**Decentralized Identifiers (DIDs) v1.0**

**Pangunahing arkitektura, modelo ng data, at mga representasyon**

[Rekomendasyon ng W3C](https://www.w3.org/standards/types#REC) 19 Hulyo 2022

**Ang bersyon na ito:**

<https://www.w3.org/TR/2022/REC-did-core-20220719/>

**Pinakabagong nai-publish na bersyon:**

<https://www.w3.org/TR/did-core/>

**Pinakabagong draft ng editor:**

<https://w3c.github.io/did-core/>

**Kasaysayan:**

<https://www.w3.org/standards/history/did-core>

[Gumawa ng kasaysayan](https://github.com/w3c/did-core/commits/main)

**Ulat sa pagpapatupad:**

<https://w3c.github.io/did-test-suite/>

**Mga editor:**

[Manu Sporny](http://manu.sporny.org/) ( [Digital Bazaar](https://digitalbazaar.com/) )

[Amy Guy](https://rhiaro.co.uk/) ( [Digital Bazaar](https://digitalbazaar.com/) )

[Markus Sabadello](https://www.linkedin.com/in/markus-sabadello-353a0821) ( [Danube Tech](https://danubetech.com/) )

[Drummond Reed](https://www.linkedin.com/in/drummondreed/) ( [Evernym/Avast](https://www.evernym.com/) )

**Mga may-akda:**

[Manu Sporny](http://manu.sporny.org/) ( [Digital Bazaar](https://digitalbazaar.com/) )

[Dave Longley](https://github.com/dlongley) ( [Digital Bazaar](https://digitalbazaar.com/) )

[Markus Sabadello](https://www.linkedin.com/in/markus-sabadello-353a0821) ( [Danube Tech](https://danubetech.com/) )

[Drummond Reed](https://www.linkedin.com/in/drummondreed/) ( [Evernym/Avast](https://www.evernym.com/) )

[Orie Steele](https://www.linkedin.com/in/or13b/) ( [Transmute](https://transmute.industries/) )

[Christopher Allen](https://www.linkedin.com/in/christophera) ( [Blockchain Commons](https://www.blockchaincommons.com/) )

**Mga Reaksyon:**

[GitHub w3c/did-core](https://github.com/w3c/did-core/) ( [pull requests](https://github.com/w3c/did-core/pulls/) , [bagong isyu](https://github.com/w3c/did-core/issues/new/choose) , [bukas na isyu](https://github.com/w3c/did-core/issues/) )

[public-did-wg@w3.org na](mailto:public-did-wg@w3.org?subject=%5Bdid-core%5D%20YOUR%20TOPIC%20HERE) may linya ng paksa ( mga [archive](https://lists.w3.org/Archives/Public/public-did-wg/) )[did-core] *… message topic …*

**Errata:**

[Umiiral ang Errata](https://w3c.github.io/did-core/errata.html) .

**Mga Kaugnay na Dokumento**

[DID Use Cases and Requirements](https://www.w3.org/TR/did-use-cases/)

[Mga Rehistro ng Detalye ng DID](https://www.w3.org/TR/did-spec-registries/)

[Ulat sa Pagpapatupad ng DID Core](https://w3c.github.io/did-test-suite/)

Tingnan din [**ang mga pagsasalin**](https://www.w3.org/Translations/?technology=did-core) .

[Copyright](https://www.w3.org/Consortium/Legal/ipr-notice#Copyright) © 2022 [W3C](https://www.w3.org/)® ( [MIT](https://www.csail.mit.edu/) , [ERCIM](https://www.ercim.eu/) , [Keio](https://www.keio.ac.jp/) , [Beihang](https://ev.buaa.edu.cn/) ). [Nalalapat ang pananagutan](https://www.w3.org/Consortium/Legal/ipr-notice#Legal_Disclaimer) ng W3C , [trademark](https://www.w3.org/Consortium/Legal/ipr-notice#W3C_Trademarks) at pinahihintulutang mga panuntunan sa [lisensya ng dokumento .](https://www.w3.org/Consortium/Legal/2015/copyright-software-and-document" \o "Paunawa at Lisensya ng W3C Software at Dokumento)

## Abstract

[Ang mga decentralized identifier](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) (DIDs) ay isang bagong uri ng identifier na nagbibigay-daan sa nabe-verify at desentralisadong digital na pagkakakilanlan. Ang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay tumutukoy sa anumang paksa (hal., isang tao, organisasyon, bagay, modelo ng data, abstract entity, atbp.) na tinutukoy ng controller ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) . Sa kaibahan sa mga karaniwang, federated identifier, [ang mga DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay idinisenyo upang ang mga ito ay mahiwalay mula sa mga sentralisadong rehistro, tagapagbigay ng pagkakakilanlan, at mga awtoridad sa sertipiko. Sa partikular, habang ang ibang mga partido ay maaaring gamitin upang tumulong na paganahin ang pagtuklas ng impormasyong nauugnay sa isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) , ang disenyo ay nagbibigay-daan sa controller ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na patunayan ang kontrol dito nang hindi nangangailangan ng pahintulot mula sa anumang ibang partido. [DIDs](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers)ay mga [URI](https://www.w3.org/TR/did-core/#dfn-uri) na nag-uugnay ng [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) sa isang [dokumento](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ng DID na nagpapahintulot sa mga mapagkakatiwalaang pakikipag-ugnayan na nauugnay sa paksang iyon.

Ang bawat [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay maaaring magpahayag ng cryptographic na materyal, mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) , o mga [serbisyo](https://www.w3.org/TR/did-core/" \l "dfn-service) , na nagbibigay ng isang hanay ng mga mekanismo na nagbibigay-daan sa isang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) na patunayan ang kontrol ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) . [Pinapagana ng mga serbisyo](https://www.w3.org/TR/did-core/" \l "dfn-service) ang mga pinagkakatiwalaang pakikipag-ugnayan na nauugnay sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) . Maaaring magbigay ang isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ng paraan upang ibalik ang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) mismo, kung ang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ay isang mapagkukunan ng impormasyon tulad ng modelo ng data.

Tinutukoy ng dokumentong ito ang syntax ng DID, isang karaniwang modelo ng data, mga pangunahing katangian, mga serialized na representasyon, mga pagpapatakbo ng DID, at isang paliwanag sa proseso ng paglutas ng mga DID sa mga mapagkukunang kinakatawan ng mga ito.

## Katayuan ng Dokumentong Ito

Inilalarawan ng seksyong ito ang katayuan ng dokumentong ito sa oras ng paglalathala nito. Ang isang listahan ng kasalukuyang mga publikasyong W3C at ang pinakabagong rebisyon ng teknikal na ulat na ito ay makikita sa [*W3C technical reports index*](https://www.w3.org/TR/) sa https://www.w3.org/TR/.

Sa oras ng paglalathala, mayroong [103 pang-eksperimentong pagtutukoy](https://w3c.github.io/did-spec-registries/#did-methods) ng Paraan ng DID , 32 pang-eksperimentong DID Method na pagpapatupad ng driver, isang [test suite](https://w3c.github.io/did-test-suite/) na tumutukoy kung ang isang ibinigay na pagpapatupad ay naaayon o hindi sa detalyeng ito at 46 na pagpapatupad na isinumite sa conformance test suite. Pinapayuhan ang mga mambabasa na sundin ang mga [isyu sa DID Core](https://github.com/w3c/did-core/issues) at [DID Core Test Suite](https://github.com/w3c/did-test-suite/issues) na ang bawat isa ay naglalaman ng pinakabagong listahan ng mga alalahanin at iminungkahing pagbabago na maaaring magresulta sa mga pagbabago sa detalyeng ito. Sa panahon ng paglalathala, walang inaasahang karagdagang mahahalagang isyu, pagbabago, o pagbabago.

Ang mga komento tungkol sa dokumentong ito ay malugod na tinatanggap. Mangyaring direktang maghain ng mga isyu sa [GitHub](https://github.com/w3c/did-core/issues/) , o ipadala ang mga ito sa [public-did-wg@w3.org](mailto:public-did-wg@w3.org) ( mag [-subscribe](mailto:public-did-wg-request@w3.org?subject=subscribe) , [archives](https://lists.w3.org/Archives/Public/public-did-wg/) ).

Ang dokumentong ito ay nai-publish ng [Decentralized Identifier Working Group](https://www.w3.org/groups/wg/did) bilang isang Rekomendasyon gamit ang [track ng Rekomendasyon](https://www.w3.org/2021/Process-20211102/#recs-and-notes) .

Inirerekomenda ng W3C ang malawak na pag-deploy ng detalyeng ito bilang pamantayan para sa Web.

Ang Rekomendasyon ng W3C ay isang detalye na, pagkatapos ng malawakang pagbuo ng pinagkasunduan, ay ineendorso ng W3C at ng mga Miyembro nito, at may mga pangako mula sa mga miyembro ng Working Group sa [walang royalty na paglilisensya](https://www.w3.org/Consortium/Patent-Policy/" \l "sec-Requirements) para sa mga pagpapatupad.

Ang dokumentong ito ay ginawa ng isang pangkat na tumatakbo sa ilalim ng [W3C Patent Policy](https://www.w3.org/Consortium/Patent-Policy/) . Ang W3C ay nagpapanatili ng isang [pampublikong listahan ng anumang mga pagsisiwalat ng patent na](https://www.w3.org/groups/wg/did/ipr) ginawa kaugnay ng mga naihatid ng grupo; Kasama rin sa page na iyon ang mga tagubilin para sa pagsisiwalat ng patent. Ang isang indibidwal na may aktwal na kaalaman sa isang patent na pinaniniwalaan ng indibidwal na naglalaman ng [(mga) Mahahalagang Claim](https://www.w3.org/Consortium/Patent-Policy/#def-essential) ay dapat ibunyag ang impormasyon alinsunod sa [seksyon 6 ng Patakaran sa Patent ng W3C](https://www.w3.org/Consortium/Patent-Policy/" \l "sec-Disclosure) .

Ang dokumentong ito ay pinamamahalaan ng [2 Nobyembre 2021 W3C Process Document](https://www.w3.org/2021/Process-20211102/) .

1.Panimula

*Ang seksyong ito ay hindi normatibo.*

Bilang mga indibidwal at organisasyon, marami sa atin ang gumagamit ng mga pandaigdigang natatanging identifier sa iba't ibang uri ng konteksto. Nagsisilbi ang mga ito bilang mga address ng komunikasyon (mga numero ng telepono, email address, username sa social media), mga numero ng ID (para sa mga pasaporte, lisensya sa pagmamaneho, mga tax ID, insurance sa kalusugan), at mga tagatukoy ng produkto (mga serial number, barcode, RFID). Ang mga URI (Uniform Resource Identifiers) ay ginagamit para sa mga mapagkukunan sa Web at ang bawat web page na tinitingnan mo sa isang browser ay may natatanging URL sa buong mundo (Uniform Resource Locator).

Ang karamihan sa mga natatanging identifier na ito sa buong mundo ay wala sa aming kontrol. Ang mga ito ay inisyu ng mga panlabas na awtoridad na nagpapasya kung sino o ano ang kanilang tinutukoy at kung kailan sila maaaring bawiin. Ang mga ito ay kapaki-pakinabang lamang sa ilang mga konteksto at kinikilala lamang ng ilang partikular na katawan na hindi natin pinili. Maaaring mawala ang mga ito o hindi na maging wasto sa pagkabigo ng isang organisasyon. Maaaring hindi nila kailangang magbunyag ng personal na impormasyon. Sa maraming kaso, maaari silang mapanlinlang na gayahin at igiit ng isang malisyosong third-party, na mas karaniwang kilala bilang "pagnanakaw ng pagkakakilanlan."

Ang Decentralized Identifiers (DIDs) na tinukoy sa detalyeng ito ay isang bagong uri ng globally unique identifier. Idinisenyo ang mga ito upang bigyang-daan ang mga indibidwal at organisasyon na makabuo ng kanilang sariling mga pagkakakilanlan gamit ang mga sistemang pinagkakatiwalaan nila. Ang mga bagong identifier na ito ay nagbibigay-daan sa mga entity na patunayan ang kontrol sa kanila sa pamamagitan ng pag-authenticate gamit ang mga cryptographic na patunay gaya ng mga digital na lagda.

Dahil ang pagbuo at paggigiit ng Mga Desentralisadong Identifier ay kinokontrol ng entity, ang bawat entity ay maaaring magkaroon ng maraming DID hangga't kinakailangan upang mapanatili ang kanilang gustong paghihiwalay ng mga pagkakakilanlan, persona, at pakikipag-ugnayan. Ang paggamit ng mga identifier na ito ay maaaring saklawin nang naaangkop sa iba't ibang konteksto. Sinusuportahan nila ang mga pakikipag-ugnayan sa ibang tao, institusyon, o system na nangangailangan ng mga entity na kilalanin ang kanilang mga sarili, o mga bagay na kinokontrol nila, habang nagbibigay ng kontrol sa kung gaano karaming personal o pribadong data ang dapat ibunyag, lahat nang hindi umaasa sa isang sentral na awtoridad upang magarantiya ang patuloy na pagkakaroon ng ang identifier. Ang mga ideyang ito ay ginalugad sa dokumento ng DID Use Cases [ [DID-USE-CASES](https://www.w3.org/TR/did-core/#bib-did-use-cases) ].

Hindi ipinapalagay ng detalyeng ito ang anumang partikular na teknolohiya o kriptograpiya upang suportahan ang pagbuo, pagpapatuloy, paglutas, o interpretasyon ng mga DID. Halimbawa, ang mga tagapagpatupad ay maaaring lumikha ng mga Desentralisadong Identifier batay sa mga pagkakakilanlan na nakarehistro sa federated o sentralisadong mga sistema ng pamamahala ng pagkakakilanlan. Sa katunayan, halos lahat ng uri ng mga identifier system ay maaaring magdagdag ng suporta para sa mga DID. Lumilikha ito ng interoperability na tulay sa pagitan ng mga mundo ng mga sentralisadong, federated, at desentralisadong mga identifier. Binibigyang-daan din nito ang mga tagapagpatupad na magdisenyo ng mga partikular na uri ng mga DID upang gumana sa imprastraktura ng pag-compute na kanilang pinagkakatiwalaan, tulad ng mga distributed ledger, desentralisadong file system, distributed database, at peer-to-peer network.

Ang pagtutukoy na ito ay para sa:

* Sinuman na gustong maunawaan ang mga pangunahing prinsipyo ng arkitektura na siyang pundasyon para sa Mga Desentralisadong Identifier;
* Mga developer ng software na gustong gumawa at gumamit ng Mga Desentralisadong Identifier at ang kanilang nauugnay na mga format ng data;
* Mga system integrator na gustong maunawaan kung paano gamitin ang Decentralized Identifiers sa kanilang software at hardware system;
* Mga may-akda ng detalye na gustong gumawa ng mga bagong imprastraktura ng DID, na kilala bilang mga pamamaraan ng DID, na umaayon sa ecosystem na inilarawan ng dokumentong ito.

Bilang karagdagan sa detalyeng ito, maaaring makita ng mga mambabasa na kapaki-pakinabang ang dokumento ng Mga Use Case at Mga Kinakailangan para sa Mga Desentralisadong Identifier [ [DID-USE-CASES ].](https://www.w3.org/TR/did-core/#bib-did-use-cases)

### **1.1Isang Simpleng Halimbawa**

Ang seksyong ito ay hindi normatibo.

Ang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay isang simpleng text string na binubuo ng tatlong bahagi: 1) ang didURI scheme identifier, 2) ang identifier para sa [DID method](https://www.w3.org/TR/did-core/#dfn-did-methods) , at 3) ang DID method-specific na identifier.

A picture containing diagram

Description automatically generated

(img src: https://www.w3.org/TR/did-core/diagrams/parts-of-a-did.svg)  
Pigura1 Isang simpleng halimbawa ng decentralized identifier (DID)

Ang halimbawang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) sa itaas ay lumulutas sa isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) . Ang isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) ay naglalaman ng impormasyong nauugnay sa [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) , tulad ng mga paraan para sa cryptographically [authenticate](https://www.w3.org/TR/did-core/#dfn-authenticated) ang isang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) .

[HALIMBAWA1](https://www.w3.org/TR/did-core/#example-a-simple-did-document): Isang simpleng dokumento ng DID

{

"@context": [

"https://www.w3.org/ns/did/v1",

"https://w3id.org/security/suites/ed25519-2020/v1"

]

"id": "did:example:123456789abcdefghi",

"authentication": [{

// ginagamit upang patotohanan gaya ng ginawa:...fghi

"id": "did:example:123456789abcdefghi#keys-1",

"type": "Ed25519VerificationKey2020",

"controller": "did:example:123456789abcdefghi",

"publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"

}]

}

### **1.2Mga Layunin sa Disenyo**

Ang seksyong ito ay hindi normatibo.

[Ang Decentralized Identifiers](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay isang bahagi ng mas malalaking system, gaya ng Verifiable Credentials ecosystem [ [VC-DATA-MODEL](https://www.w3.org/TR/did-core/#bib-vc-data-model) ], na nakaimpluwensya sa mga layunin sa disenyo para sa detalyeng ito. Ang mga layunin sa disenyo para sa Mga Desentralisadong Identifier ay buod dito.

| **Layunin** | **Paglalarawan** |
| --- | --- |
| Desentralisasyon | Tanggalin ang pangangailangan para sa mga sentralisadong awtoridad o single point failure sa pamamahala ng identifier, kabilang ang pagpaparehistro ng mga pandaigdigang natatanging identifier, mga pampublikong verification key, [serbisyo](https://www.w3.org/TR/did-core/" \l "dfn-service) , at iba pang impormasyon. |
| Kontrolin | Bigyan ang mga entity, kapwa tao at hindi tao, ng kapangyarihan na direktang kontrolin ang kanilang mga digital na pagkakakilanlan nang hindi kinakailangang umasa sa mga panlabas na awtoridad. |
| Pagkapribado | Paganahin ang mga entity na kontrolin ang privacy ng kanilang impormasyon, kabilang ang minimal, pumipili, at progresibong pagsisiwalat ng mga katangian o iba pang data. |
| Seguridad | Paganahin ang sapat na seguridad para sa paghiling sa mga partido na umasa sa mga [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) para sa kanilang kinakailangang antas ng kasiguruhan. |
| Nakabatay sa patunay | I- enable ang [DID controllers](https://www.w3.org/TR/did-core/#dfn-did-controllers) na magbigay ng cryptographic proof kapag nakikipag-ugnayan sa ibang entity. |
| Kakayahang matuklasan | Gawing posible para sa mga entity na tumuklas ng [mga DID](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers) para sa iba pang mga entity, upang matuto nang higit pa tungkol sa o makipag-ugnayan sa mga entity na iyon. |
| Interoperability | Gumamit ng mga interoperable na pamantayan upang magamit ng imprastraktura ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ang mga kasalukuyang tool at software library na idinisenyo para sa interoperability. |
| Portability | Maging system-at network-independent at paganahin ang mga entity na gamitin ang kanilang mga digital identifier sa anumang system na sumusuporta [sa mga DID](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers) at [DID na pamamaraan](https://www.w3.org/TR/did-core/#dfn-did-methods) . |
| pagiging simple | Paboran ang isang pinababang hanay ng mga simpleng feature para gawing mas madaling maunawaan, ipatupad, at i-deploy ang teknolohiya. |
| Extensibility | Kung posible, paganahin ang pagpapalawak sa kondisyon na hindi ito lubos na humahadlang sa interoperability, portability, o pagiging simple. |

### **1.3 Pangkalahatang-ideya ng Arkitektura**

Ang seksyong ito ay hindi normatibo.

Nagbibigay ang seksyong ito ng pangunahing pangkalahatang-ideya ng mga pangunahing bahagi ng arkitektura ng Decentralized Identifier.

Diagram

Description automatically generated

(img src: <https://www.w3.org/TR/did-core/diagrams/did_brief_architecture_overview.svg>)

*Pigura*2*Pangkalahatang-ideya ng arkitektura ng DID at ang kaugnayan ng mga pangunahing bahagi. Tingnan din ang: [paglalarawan ng salaysay](https://www.w3.org/TR/did-core/" \l "brief-architecture-overview-longdesc) .*

**Mga URL ng DID at DID**

Ang Decentralized Identifier, o [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) , ay isang [URI](https://www.w3.org/TR/did-core/#dfn-uri) na binubuo ng tatlong bahagi: ang scheme did:, isang method identifier, at isang natatanging, method-specific na identifier na tinukoy ng [DID method](https://www.w3.org/TR/did-core/#dfn-did-methods) . [Ang mga DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay malulutas sa mga [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) . Pinapalawak ng [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) ang syntax ng isang pangunahing [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) upang isama ang iba pang karaniwang bahagi ng [URI](https://www.w3.org/TR/did-core/#dfn-uri) gaya ng path, query, at fragment upang mahanap ang isang partikular na [mapagkukunan](https://www.w3.org/TR/did-core/" \l "dfn-resources) —halimbawa, isang cryptographic na pampublikong key sa loob ng isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) , o isang [mapagkukunang](https://www.w3.org/TR/did-core/" \l "dfn-resources) panlabas sa [DID dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) . Ang mga konseptong ito ay inilalarawan sa[3.1DID Syntax](https://www.w3.org/TR/did-core/#did-syntax) at[3.2DID URL Syntax](https://www.w3.org/TR/did-core/#did-url-syntax) .

**Mga paksa ng DID**

Ang paksa ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay, ayon sa kahulugan, ang entity na tinukoy ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) . Ang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ay maaari ding ang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) . Anuman ay maaaring maging paksa ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) : tao, grupo, organisasyon, bagay, o konsepto. Ito ay karagdagang tinukoy sa[5.1.1DID Paksa](https://www.w3.org/TR/did-core/#did-subject) .

**DID controllers**

Ang [controller](https://www.w3.org/TR/did-core/#dfn-controller) ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay ang entity (tao, organisasyon, o autonomous na software) na may kakayahan—gaya ng tinukoy ng isang [DID method](https://www.w3.org/TR/did-core/#dfn-did-methods) —na gumawa ng mga pagbabago sa isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) . Ang kakayahang ito ay karaniwang iginiit ng kontrol ng isang hanay ng mga cryptographic key na ginagamit ng software na kumikilos sa ngalan ng controller, bagama't maaari rin itong igiit sa pamamagitan ng iba pang mga mekanismo. Tandaan na ang isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay maaaring magkaroon ng higit sa isang controller, at ang [DID na paksa](https://www.w3.org/TR/did-core/#dfn-did-subjects) ay maaaring ang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) , o isa sa mga ito. Ang konseptong ito ay nakadokumento sa[5.1.2DID Controller](https://www.w3.org/TR/did-core/#did-controller) .

**Na-verify na mga rehistro ng data**

Upang malutas sa mga [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) , ang mga [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay karaniwang naitala sa isang pinagbabatayan na sistema o network ng ilang uri. Anuman ang partikular na teknolohiyang ginamit, ang anumang ganoong sistema na sumusuporta sa pagtatala ng [mga DID](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers) at pagbabalik ng data na kinakailangan upang makagawa ng mga [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay tinatawag na isang [nabe-verify na data registry](https://www.w3.org/TR/did-core/#dfn-verifiable-data-registry) . Kasama sa mga halimbawa ang mga [distributed ledger](https://www.w3.org/TR/did-core/#dfn-distributed-ledger-technology) , desentralisadong file system, database ng anumang uri, peer-to-peer network, at iba pang anyo ng pinagkakatiwalaang imbakan ng data. Ang konseptong ito ay higit na pinaliwanag sa [8.Pamamaraan](https://www.w3.org/TR/did-core/#methods) .

**Mga dokumento ng DID**

[Ang mga dokumento ng DID](https://www.w3.org/TR/did-core/#dfn-did-documents) ay naglalaman ng impormasyong nauugnay sa isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) . Karaniwang ipinapahayag nila ang mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) , gaya ng mga cryptographic na pampublikong key, at mga [serbisyong](https://www.w3.org/TR/did-core/" \l "dfn-service) nauugnay sa mga pakikipag-ugnayan sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) . Ang mga generic na katangian na sinusuportahan sa isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) ay tinukoy sa[5.Mga Pangunahing Katangian](https://www.w3.org/TR/did-core/#core-properties) . Ang isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) ay maaaring i-serialize sa isang byte stream (tingnan ang[6.Mga Kinatawan](https://www.w3.org/TR/did-core/#representations) ). Maaaring ma-update ang mga property na nasa isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ayon sa mga naaangkop na operasyong nakabalangkas sa[8.Pamamaraan](https://www.w3.org/TR/did-core/#methods) .

**Mga pamamaraan ng DID**

[Ang mga pamamaraan ng DID](https://www.w3.org/TR/did-core/#dfn-did-methods) ay ang mekanismo kung saan ang isang partikular na uri ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) at ang nauugnay na [dokumento](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ng DID nito ay nilikha, niresolba, na-update, at na-deactivate. [Ang mga pamamaraan ng DID](https://www.w3.org/TR/did-core/#dfn-did-methods) ay tinukoy gamit ang hiwalay na mga detalye ng pamamaraan ng DID tulad ng tinukoy sa[8.Pamamaraan](https://www.w3.org/TR/did-core/#methods) .

**DID solvers at DID resolution**

Ang isang solver ng [DID](https://www.w3.org/TR/did-core/#dfn-did-resolvers) ay isang bahagi ng system na kumukuha ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) bilang input at gumagawa ng isang naaayon na [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) bilang output. Ang prosesong ito ay tinatawag na [DID resolution](https://www.w3.org/TR/did-core/#dfn-did-resolution) . Ang mga hakbang para sa paglutas ng isang partikular na uri ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay tinukoy ng nauugnay na detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) . Ang proseso ng [paglutas ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-resolution) ay inilalarawan sa[7.Resolusyon](https://www.w3.org/TR/did-core/#resolution) .

**DID URL dereferencers at DID URL dereferencing**

Ang [DID URL dereferencer](https://www.w3.org/TR/did-core/#dfn-did-url-dereferencers) ay isang bahagi ng system na kumukuha ng [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) bilang input at gumagawa ng [resource](https://www.w3.org/TR/did-core/#dfn-resources) bilang output. Ang prosesong ito ay tinatawag na [DID URL dereferencing](https://www.w3.org/TR/did-core/#dfn-did-url-dereferencing) . Ang proseso ng [DID URL dereferencing](https://www.w3.org/TR/did-core/#dfn-did-url-dereferencing) ay inilalarawan sa[7.2DID URL Dereferencing](https://www.w3.org/TR/did-core/#did-url-dereferencing) .

### **1.4Pagsunod**

Pati na rin ang mga seksyon na minarkahan bilang non-normative, lahat ng mga alituntunin sa pag-akda, diagram, halimbawa, at mga tala sa detalyeng ito ay hindi normatibo. Ang lahat ng iba pa sa detalyeng ito ay normatibo.

Ang mga susing salita ay MAY , DAPAT , HINDI DAPAT , OPSYONAL , INIREREKOMENDASYON , KINAKAILANGAN , DAPAT , at HINDI DAPAT sa dokumentong ito ay dapat bigyang-kahulugan tulad ng inilarawan sa [BCP 14](https://datatracker.ietf.org/doc/html/bcp14) [ [RFC2119](https://www.w3.org/TR/did-core/#bib-rfc2119) ] [ [RFC8174](https://www.w3.org/TR/did-core/#bib-rfc8174) ] kung kailan, at kailan lamang, makikita ang mga ito sa lahat ng mga capitals. , gaya ng ipinapakita dito.

Ang dokumentong ito ay naglalaman ng mga halimbawa na naglalaman ng JSON at JSON-LD na nilalaman. Ang ilan sa mga halimbawang ito ay naglalaman ng mga character na hindi wasto, tulad ng mga inline na komento ( //) at ang paggamit ng ellipsis ( ...) upang tukuyin ang impormasyon na nagdaragdag ng maliit na halaga sa halimbawa. Ang mga nagpapatupad ay binabalaan na alisin ang nilalamang ito kung nais nilang gamitin ang impormasyon bilang wastong JSON o JSON-LD.

Ang ilang mga halimbawa ay naglalaman ng mga termino, parehong mga pangalan ng property at mga halaga, na hindi tinukoy sa detalyeng ito. Ang mga ito ay ipinahiwatig ng komento ( // external (property name|value)). Ang mga naturang termino, kapag ginamit sa isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) , ay inaasahang mairehistro sa DID Specification Registries [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ] na may mga link sa parehong pormal na kahulugan at JSON-LD na konteksto.

Ang interoperability ng mga pagpapatupad para sa mga dokumento ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) at [DID](https://www.w3.org/TR/did-core/#dfn-did-documents) ay sinusubok sa pamamagitan ng pagsusuri sa kakayahan ng isang pagpapatupad na gumawa at mag-parse ng mga dokumento ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) at [DID](https://www.w3.org/TR/did-core/#dfn-did-documents) na sumusunod sa detalyeng ito. Ang interoperability para sa mga producer at consumer ng mga [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) at [DID na mga dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) ay ibinibigay sa pamamagitan ng pagtiyak na ang mga [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) at [DID na mga dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) ay sumusunod. Ang interoperability para sa mga detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ay ibinibigay ng mga detalye sa bawat detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) . Nauunawaan na, sa parehong paraan na ang isang web browser ay hindi kinakailangan na ipatupad ang lahat ng kilalang [URI](https://www.w3.org/TR/did-core/" \l "dfn-uri)mga scheme, ang conformant software na gumagana sa [mga DID](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers) ay hindi kinakailangan upang ipatupad ang lahat ng kilalang [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) . Gayunpaman, ang lahat ng pagpapatupad ng isang ibinigay na [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ay inaasahang interoperable para sa pamamaraang iyon.

Ang **umaayon sa DID** ay anumang konkretong pagpapahayag ng mga panuntunang tinukoy sa [3.Identifier](https://www.w3.org/TR/did-core/#identifier) na sumusunod sa mga nauugnay na normative statement sa seksyong iyon.

Ang isang **sumusunod na dokumento ng DID** ay anumang konkretong pagpapahayag ng modelo ng data na inilarawan sa detalyeng ito na sumusunod sa mga nauugnay na normatibong pahayag sa[4.Modelo ng Data](https://www.w3.org/TR/did-core/#data-model) at[5.Mga Pangunahing Katangian](https://www.w3.org/TR/did-core/#core-properties) . Ang isang serialization na format para sa sumusunod na dokumento ay deterministiko, bi-directional, at lossless, tulad ng inilarawan sa[6.Mga representasyon](https://www.w3.org/TR/did-core/#representations) .

Ang isang tumutugon na **producer** ay anumang algorithm na natanto bilang software at/o hardware na bumubuo [ng mga sumusunod na DID](https://www.w3.org/TR/did-core/#dfn-conforming-did) o [umaayon sa mga Dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-conforming-did-document) at sumusunod sa mga nauugnay na normatibong pahayag sa[6.Mga representasyon](https://www.w3.org/TR/did-core/#representations) .

Ang **conforming consumer** ay anumang algorithm na naisasakatuparan bilang software at/o hardware na [gumagamit ng mga DID](https://www.w3.org/TR/did-core/" \l "dfn-conforming-did) o [umaayon sa mga dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-conforming-did-document) at sumusunod sa mga nauugnay na normative statement sa[6.Mga representasyon](https://www.w3.org/TR/did-core/#representations) .

Ang isang **tumutugmang DID na solver** ay anumang algorithm na natanto bilang software at/o hardware na sumusunod sa mga nauugnay na normatibong pahayag sa[7.1DID Resolution](https://www.w3.org/TR/did-core/#did-resolution) .

Ang isang **sumusunod na DID URL dereferencer** ay anumang algorithm na natanto bilang software at/o hardware na sumusunod sa mga nauugnay na normative statement sa[7.2DID URL Dereferencing](https://www.w3.org/TR/did-core/#did-url-dereferencing) .

Ang isang **sumusunod na pamamaraan ng DID** ay anumang detalye na sumusunod sa mga nauugnay na normatibong pahayag sa[8.Pamamaraan](https://www.w3.org/TR/did-core/#methods) .

2.Terminolohiya

*Ang seksyong ito ay hindi normatibo.*

Tinutukoy ng seksyong ito ang mga terminong ginamit sa detalyeng ito at sa buong imprastraktura ng [desentralisadong identifier .](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers)Ang isang link sa mga tuntuning ito ay kasama sa tuwing lalabas ang mga ito sa detalyeng ito.

***pag-atake ng amplification***

Isang klase ng pag-atake kung saan sinusubukan ng attacker na ubusin ang CPU, storage, network, o iba pang mapagkukunan ng target na system sa pamamagitan ng pagbibigay ng maliliit at wastong input sa system na nagreresulta sa mga nakakapinsalang epekto na maaaring mas magastos sa proseso kaysa sa mga input mismo.

***patotohanan***

Ang pagpapatunay ay isang proseso kung saan mapapatunayan ng isang entity na mayroon itong partikular na katangian o kinokontrol ang isang partikular na lihim gamit ang isa o higit pang [mga paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) . Sa [mga DID](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers) , ang isang karaniwang halimbawa ay ang pagpapatunay ng kontrol sa cryptographic na pribadong key na nauugnay sa isang pampublikong key na na-publish sa isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) .

***cryptographic suite***

Isang detalye na tumutukoy sa paggamit ng mga partikular na cryptographic primitives upang makamit ang isang partikular na layunin sa seguridad. Ang mga dokumentong ito ay kadalasang ginagamit upang tukuyin ang mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) , mga uri ng digital na lagda, mga pagkakakilanlan ng mga ito, at iba pang nauugnay na katangian.

***decentralized identifier* (DID)**

Isang globally unique persistent identifier na hindi nangangailangan ng sentralisadong awtoridad sa pagpaparehistro at kadalasang nabuo at/o nakarehistro sa cryptographically. Ang generic na format ng isang DID ay tinukoy sa[3.1DID Syntax](https://www.w3.org/TR/did-core/#did-syntax) . Ang isang partikular na [scheme ng DID](https://www.w3.org/TR/did-core/#dfn-did-schemes) ay tinukoy sa isang detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) . Marami—ngunit hindi lahat—ang mga pamamaraan ng DID ay gumagamit ng [distributed ledger technology](https://www.w3.org/TR/did-core/#dfn-distributed-ledger-technology) (DLT) o ilang iba pang anyo ng desentralisadong network.

***desentralisadong pamamahala ng pagkakakilanlan***

[Pamamahala ng pagkakakilanlan](https://en.wikipedia.org/wiki/Identity_management) na batay sa paggamit ng mga [desentralisadong identifier](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers) . Pinapalawak ng desentralisadong pamamahala ng pagkakakilanlan ang awtoridad para sa pagbuo ng identifier, pagpaparehistro, at pagtatalaga nang higit sa tradisyonal na pinagkakatiwalaan gaya ng mga serbisyo ng [direktoryo ng X.500](https://en.wikipedia.org/wiki/X.500) , [Domain Name System](https://en.wikipedia.org/wiki/Domain_Name_System) , at karamihan sa mga national ID system.

***DID controller***

Isang entity na may kakayahang gumawa ng mga pagbabago sa isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) . Ang isang [DID ay](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) maaaring magkaroon ng higit sa isang DID controller. Ang (mga) DID controller ay maaaring tukuyin ng opsyonal na controllerproperty sa tuktok na antas ng [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) . Tandaan na ang isang DID controller ay maaaring ang [DID na paksa](https://www.w3.org/TR/did-core/#dfn-did-subjects) .

***DID delegate***

Isang entity kung kanino ang isang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) ay binigyan ng pahintulot na gumamit ng isang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) na nauugnay sa isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) sa pamamagitan ng isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) . Halimbawa, ang isang magulang na kumokontrol sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ng isang bata ay maaaring pahintulutan ang bata na gamitin ang kanilang personal na device upang ma- [authenticate](https://www.w3.org/TR/did-core/#dfn-authenticated) . Sa kasong ito, ang bata ay ang [DID delegate](https://www.w3.org/TR/did-core/#dfn-did-delegate) . Ang personal na device ng bata ay maglalaman ng pribadong cryptographic na materyal na nagbibigay-daan sa bata na mag- [authenticate](https://www.w3.org/TR/did-core/#dfn-authenticated) gamit ang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) . Gayunpaman, maaaring hindi payagan ang bata na magdagdag ng iba pang mga personal na device nang walang pahintulot ng magulang.

***dokumento ng DID***

Isang set ng data na naglalarawan sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) , kabilang ang mga mekanismo, gaya ng mga cryptographic na pampublikong key, na magagamit ng [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) o isang [delegado](https://www.w3.org/TR/did-core/" \l "dfn-did-delegate) ng DID upang [patotohanan](https://www.w3.org/TR/did-core/" \l "dfn-authenticated) ang sarili nito at patunayan ang kaugnayan nito sa [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) . Ang isang DID na dokumento ay maaaring magkaroon ng isa o higit pang magkakaibang [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) gaya ng tinukoy sa[6.Mga Representasyon](https://www.w3.org/TR/did-core/#representations) o sa W3C DID Specification Registries [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ].

***DID fragment***

Ang bahagi ng isang [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) na sumusunod sa unang karakter ng hash sign ( #). Ang DID fragment syntax ay kapareho ng URI fragment syntax.

***paraan ng DID***

Isang kahulugan kung paano ipinapatupad ang isang partikular na [pamamaraan ng DID .](https://www.w3.org/TR/did-core/" \l "dfn-did-schemes)Ang isang paraan ng DID ay tinukoy ng isang detalye ng pamamaraan ng DID, na tumutukoy sa mga tumpak na operasyon kung saan [ang mga DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) at mga [dokumento](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ng DID ay nilikha, naresolba, na-update, at na-deactivate. Tingnan mo[8.Pamamaraan](https://www.w3.org/TR/did-core/#methods) .

***DID landas***

Ang bahagi ng isang [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) na nagsisimula sa at kasama ang unang forward slash ( /) na character at nagtatapos sa alinman sa isang tandang pananong ( ?) na character, isang fragment hash sign ( #) na character, o sa dulo ng [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) . DID path syntax ay kapareho ng URI path syntax. Tingnan [ang Landas](https://www.w3.org/TR/did-core/#path) .

***DID query***

Ang bahagi ng isang [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) na sumusunod at kasama ang unang character na tandang pananong ( ?). DID query syntax ay kapareho ng URI query syntax. Tingnan [ang Query](https://www.w3.org/TR/did-core/#query) .

***DID resolution***

Ang prosesong kumukuha bilang input nito ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) at isang hanay ng mga opsyon sa paglutas at nagbabalik ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) sa isang naaayon na [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) at karagdagang metadata. Ang prosesong ito ay umaasa sa "Basahin" na pagpapatakbo ng naaangkop na [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) . Ang mga input at output ng prosesong ito ay tinukoy sa[7.1DID Resolution](https://www.w3.org/TR/did-core/#did-resolution) .

***DID solver***

Ang [DID resolver](https://www.w3.org/TR/did-core/#dfn-did-resolvers) ay isang software at/o hardware na bahagi na gumaganap ng [DID resolution](https://www.w3.org/TR/did-core/#dfn-did-resolution) function sa pamamagitan ng pagkuha ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) bilang input at paggawa ng isang naaayon na [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) bilang output.

***DID scheme***

Ang pormal na syntax ng isang [desentralisadong identifier](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers) . Ang generic na DID scheme ay nagsisimula sa prefix did:gaya ng tinukoy sa[3.1DID Syntax](https://www.w3.org/TR/did-core/#did-syntax) . Ang bawat detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ay tumutukoy sa isang partikular na pamamaraan ng DID na gumagana sa partikular na [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) na iyon . Sa isang partikular na pamamaraan ng DID method, ang pangalan ng DID method ay sumusunod sa unang colon at nagtatapos sa pangalawang colon, hal,did:example:

***DID subject***

Ang entity na kinilala ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) at inilarawan ng isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) . Ang anumang bagay ay maaaring isang paksa ng DID: tao, grupo, organisasyon, pisikal na bagay, digital na bagay, lohikal na bagay, atbp.

***DID URL***

Isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) kasama ang anumang karagdagang bahagi ng syntactic na umaayon sa kahulugan sa[3.2DID URL Syntax](https://www.w3.org/TR/did-core/#did-url-syntax) . Kabilang dito ang isang opsyonal [na landas ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-paths) (kasama ang nangungunang /karakter nito), opsyonal [na query sa DID](https://www.w3.org/TR/did-core/" \l "dfn-did-queries) (kasama ang nangungunang ?karakter nito), at opsyonal [na fragment ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-fragments) (kasama ang nangungunang #karakter nito).

***DID URL dereferencing***

Ang prosesong kumukuha bilang input nito ng [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) at isang set ng input metadata, at nagbabalik ng [resource](https://www.w3.org/TR/did-core/#dfn-resources) . Ang mapagkukunang ito ay maaaring isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) at karagdagang metadata, isang pangalawang mapagkukunan na nasa loob ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) , o isang mapagkukunang ganap na panlabas sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) . Gumagamit ang proseso ng [resolusyon ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-resolution) upang kumuha ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) na ipinahiwatig ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na nasa loob ng [URL ng DID](https://www.w3.org/TR/did-core/#dfn-did-urls) . Ang proseso ng dereferencing ay maaaring magsagawa ng karagdagang pagproseso sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) upang maibalik ang na-dereference na mapagkukunan na ipinahiwatig ng [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls). Ang mga input at output ng prosesong ito ay tinukoy sa [7.2DID URL Dereferencing](https://www.w3.org/TR/did-core/#did-url-dereferencing) .

***DID URL dereferencer***

Isang software at/o hardware system na gumaganap ng [DID URL dereferencing](https://www.w3.org/TR/did-core/#dfn-did-url-dereferencing) function para sa isang ibinigay na [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) o [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) .

***distributed ledger* (DLT)**

Isang hindi sentralisadong sistema para sa pagtatala ng mga kaganapan. Ang mga system na ito ay nagtatatag ng sapat na kumpiyansa para sa mga kalahok na umasa sa data na naitala ng iba upang makagawa ng mga pagpapasya sa pagpapatakbo. Karaniwang gumagamit sila ng mga distributed database kung saan ang iba't ibang node ay gumagamit ng consensus protocol upang kumpirmahin ang pag-order ng mga transaksyong nilagdaan ng cryptographic. Ang pag-link ng mga digitally sign na transaksyon sa paglipas ng panahon ay kadalasang ginagawang epektibong hindi nababago ang kasaysayan ng ledger.

***paglalarawan ng pampublikong susi***

Isang data object na nasa loob ng isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) na naglalaman ng lahat ng metadata na kinakailangan para gumamit ng pampublikong key o isang verification key.

***mapagkukunan***

Tulad ng tinukoy ng [ [RFC3986](https://www.w3.org/TR/did-core/#bib-rfc3986) ]: "...ang terminong 'resource' ay ginagamit sa pangkalahatang kahulugan para sa anumang maaaring matukoy ng isang URI." Katulad nito, ang anumang mapagkukunan ay maaaring magsilbi bilang isang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) na tinukoy ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) .

***representasyon***

Tulad ng tinukoy para sa HTTP ng [ [RFC7231](https://www.w3.org/TR/did-core/#bib-rfc7231) ]: "impormasyon na nilalayong ipakita ang nakaraan, kasalukuyan, o nais na estado ng isang ibinigay na mapagkukunan, sa isang format na madaling maiparating sa pamamagitan ng protocol, at binubuo ng isang set ng metadata ng representasyon at isang potensyal na walang hangganang stream ng data ng representasyon." Ang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay isang representasyon ng impormasyong naglalarawan sa isang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) . Tingnan mo[6.Mga representasyon](https://www.w3.org/TR/did-core/#representations) .

***mga entry na partikular sa representasyon***

Mga entry sa isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) na ang kahulugan ay partikular sa isang partikular na [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) . Tinukoy sa[4.Modelo ng Data](https://www.w3.org/TR/did-core/#data-model) at [6.Mga representasyon](https://www.w3.org/TR/did-core/#representations) . Halimbawa, [@context](https://www.w3.org/TR/did-core/#dfn-context)sa [representasyon ng JSON-LD](https://www.w3.org/TR/did-core/" \l "json-ld) ay isang *entry na tukoy sa representasyon* .

***mga serbisyo***

Paraan ng pakikipag-ugnayan o pakikipag-ugnayan sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) o mga nauugnay na entity sa pamamagitan ng isa o higit pang mga [endpoint ng serbisyo](https://www.w3.org/TR/did-core/#dfn-service-endpoints) . Kasama sa mga halimbawa ang mga serbisyo sa pagtuklas, mga serbisyo ng ahente, mga serbisyo sa social networking, mga serbisyo sa pag-iimbak ng file, at mga nabe-verify na serbisyo ng imbakan ng kredensyal.

***endpoint ng serbisyo***

Isang address ng network, tulad ng isang HTTP URL, kung saan gumagana ang mga [serbisyo](https://www.w3.org/TR/did-core/" \l "dfn-service) sa ngalan ng isang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) .

***Uniform Resource Identifier* (URI)**

Ang karaniwang format ng identifier para sa lahat ng mapagkukunan sa World Wide Web gaya ng tinukoy ng [ [RFC3986](https://www.w3.org/TR/did-core/#bib-rfc3986) ]. Ang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay isang uri ng URI scheme.

***mapapatunayang kredensyal***

Isang karaniwang modelo ng data at format ng representasyon para sa mga digital na kredensyal na nabe-verify sa cryptographically gaya ng tinukoy ng detalye ng W3C Verifiable Credentials [ [VC-DATA-MODEL](https://www.w3.org/TR/did-core/#bib-vc-data-model) ].

***napapatunayan na pagpapatala ng data***

Isang system na nagpapadali sa paggawa, pag-verify, pag-update, at/o pag-deactivate ng mga [desentralisadong identifier](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers) at mga [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) . Ang isang nabe-verify na registry ng data ay maaari ding gamitin para sa iba pang mga istruktura ng data na nabe-verify sa pamamagitan ng cryptographic gaya ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/did-core/#dfn-verifiable-credentials) . Para sa higit pang impormasyon, tingnan ang detalye ng W3C Verifiable Credentials [ [VC-DATA-MODEL](https://www.w3.org/TR/did-core/#bib-vc-data-model) ].

***nabe-verify na timestamp***

Ang isang nabe-verify na timestamp ay nagbibigay-daan sa isang third-party na i-verify na ang isang data object ay umiral sa isang partikular na sandali sa oras at na ito ay hindi nabago o nasira mula noong sandaling iyon. Kung ang integridad ng data ay maaaring makatwirang nabago o nasira mula noong sandaling iyon, hindi mabe-verify ang timestamp.

***paraan ng pagpapatunay***

Isang hanay ng mga parameter na maaaring gamitin kasama ng isang proseso para independiyenteng i-verify ang isang patunay. Halimbawa, ang isang cryptographic na pampublikong key ay maaaring gamitin bilang isang paraan ng pag-verify na may kinalaman sa isang digital na lagda; sa ganitong paggamit, bini-verify nito na ang lumagda ay nagtataglay ng nauugnay na cryptographic na pribadong key.

Ang "Pagpapatunay" at "patunay" sa kahulugang ito ay nilayon upang mailapat nang malawakan. Halimbawa, ang isang cryptographic na pampublikong key ay maaaring gamitin sa panahon ng Diffie-Hellman key exchange upang makipag-ayos sa isang nakabahaging symmetric key para sa pag-encrypt. Tinitiyak nito ang integridad ng proseso ng pangunahing kasunduan. Ito ay isa pang uri ng paraan ng pag-verify, kahit na ang mga paglalarawan ng proseso ay maaaring hindi gumamit ng mga salitang "pag-verify" o "patunay."

***relasyon sa pagpapatunay***

Isang pagpapahayag ng kaugnayan sa pagitan ng [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) at isang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) . Ang isang halimbawa ng isang relasyon sa pagpapatunay ay [5.3.1Pagpapatunay](https://www.w3.org/TR/did-core/#authentication) .

***Universally Unique Identifier* (UUID)**

Isang uri ng globally unique identifier na tinukoy ng [ [RFC4122](https://www.w3.org/TR/did-core/#bib-rfc4122) ]. Ang mga UUID ay katulad ng mga DID dahil hindi sila nangangailangan ng isang sentralisadong awtoridad sa pagpaparehistro. Ang mga UUID ay naiiba sa mga DID dahil ang mga ito ay hindi malulutas o cryptographically-verify.

Bilang karagdagan sa terminolohiya sa itaas, ang detalyeng ito ay gumagamit din ng terminolohiya mula sa detalye ng [ [INFRA](https://www.w3.org/TR/did-core/#bib-infra) ] upang pormal na tukuyin ang [modelo ng data](https://www.w3.org/TR/did-core/" \l "data-model) . Kapag ginamit ang terminolohiya ng [ [INFRA](https://www.w3.org/TR/did-core/#bib-infra) ], gaya ng [string](https://infra.spec.whatwg.org/#strings) , [set](https://infra.spec.whatwg.org/#ordered-set) , at [map](https://infra.spec.whatwg.org/#maps) , direktang naka-link ito sa detalyeng iyon.

## 3.Identifier

Inilalarawan ng seksyong ito ang pormal na syntax para sa [mga DID](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers) at [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) . Ang terminong "generic" ay ginagamit upang ibahin ang syntax na tinukoy dito mula sa syntax na tinukoy ng mga partikular na [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) sa kani-kanilang mga detalye. Ang mga proseso ng paglikha, at ang kanilang timing, para sa [mga DID](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers) at [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) ay inilalarawan sa[8.2Mga Operasyon ng Pamamaraan](https://www.w3.org/TR/did-core/#method-operations) at [B.2Paglikha ng isang DID](https://www.w3.org/TR/did-core/#creation-of-a-did) .

### **3.1DID Syntax**

Ang generic na [DID scheme](https://www.w3.org/TR/did-core/#dfn-did-schemes) ay isang [URI](https://www.w3.org/TR/did-core/#dfn-uri) scheme na umaayon sa [ [RFC3986](https://www.w3.org/TR/did-core/#bib-rfc3986) ]. Ang kahulugan ng ABNF ay matatagpuan sa ibaba, na gumagamit ng syntax sa [ [RFC5234](https://www.w3.org/TR/did-core/#bib-rfc5234) ] at ang mga kaukulang kahulugan para sa ALPHAat DIGIT. Ang lahat ng iba pang pangalan ng panuntunan na hindi tinukoy sa ABNF sa ibaba ay tinukoy sa [ [RFC3986](https://www.w3.org/TR/did-core/#bib-rfc3986) ]. DAPAT sumunod ang lahat ng DID sa Mga Panuntunan ng [ABNF Syntax ng DID.](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers)

| **Ang DID Syntax ABNF Rules** |
| --- |
| did = "did:" method-name ":" method-specific-id  method-name = 1\*method-char  method-char = %x61-7A / DIGIT  method-specific-id = \*( \*idchar ":") 1\*idchar  idchar = ALPHA / DIGIT / "." / "-" / "\_" / pct-encoded  pct-encoded = "%" HEXDIG HEXDIG |

Para sa mga kinakailangan sa mga [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) na nauugnay sa syntax ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) , tingnan ang Seksyon[8.1Syntax ng Paraan](https://www.w3.org/TR/did-core/#method-syntax) .

### **3.2DID URL Syntax**

Ang [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) ay isang network location identifier para sa isang partikular na [mapagkukunan](https://www.w3.org/TR/did-core/" \l "dfn-resources) . Maaari itong magamit upang kunin ang mga bagay tulad ng mga representasyon ng mga [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) , mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) , mga [serbisyo](https://www.w3.org/TR/did-core/" \l "dfn-service) , mga partikular na bahagi ng isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) , o iba pang mapagkukunan.

Ang sumusunod ay ang kahulugan ng ABNF gamit ang syntax sa [ [RFC5234](https://www.w3.org/TR/did-core/#bib-rfc5234) ]. Bumubuo ito sa didscheme na tinukoy sa[3.1DID Syntax](https://www.w3.org/TR/did-core/#did-syntax) . Ang [path-abempty](https://www.rfc-editor.org/rfc/rfc3986#section-3.3), [query](https://www.rfc-editor.org/rfc/rfc3986#section-3.4), at [fragment](https://www.rfc-editor.org/rfc/rfc3986" \l "section-3.5)mga bahagi ay tinukoy sa [ [RFC3986](https://www.w3.org/TR/did-core/#bib-rfc3986) ]. DAPAT sumunod ang lahat ng [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) sa DID URL Syntax ABNF Rules. Maaaring higit pang paghigpitan ng mga [pamamaraan ng DID ang mga panuntunang ito, gaya ng inilarawan sa](https://www.w3.org/TR/did-core/" \l "dfn-did-methods)[8.1Syntax ng Paraan](https://www.w3.org/TR/did-core/#method-syntax) .

| **Ang DID URL Syntax ABNF Rules** |
| --- |
| did-url = ba ang path-abempty [ "?" query ] [ "#" fragment ] |

TANDAAN : Ang karakter na semicolon ay nakalaan para magamit sa hinaharap

Bagama't maaaring gamitin ang semicolon ( ;) na character ayon sa mga panuntunan ng syntax ng [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) , maaaring gamitin ito ng mga susunod na bersyon ng detalyeng ito bilang sub-delimiter para sa mga parameter tulad ng inilarawan sa [ [MATRIX-URIS](https://www.w3.org/TR/did-core/#bib-matrix-uris) ]. Upang maiwasan ang mga salungatan sa hinaharap, dapat na iwasan ng mga developer ang paggamit nito.

#### Daan

Ang isang [DID path](https://www.w3.org/TR/did-core/#dfn-did-paths) ay kapareho ng isang generic na [URI](https://www.w3.org/TR/did-core/#dfn-uri) path at umaayon sa path-abemptypanuntunan ng ABNF sa [RFC 3986, seksyon 3.3](https://www.rfc-editor.org/rfc/rfc3986#section-3.3) . Tulad ng sa mga [URI](https://www.w3.org/TR/did-core/#dfn-uri) , ang path semantics ay maaaring tukuyin ng [DID Methods](https://www.w3.org/TR/did-core/#dfn-did-methods) , na kung saan ay maaaring paganahin ang [DID controllers](https://www.w3.org/TR/did-core/#dfn-did-controllers) upang higit pang maging dalubhasa sa mga semantikong iyon.

[HALIMBAWA2](https://www.w3.org/TR/did-core/#example-2)

ginawa:halimbawa:123456/path

#### Tanong

Ang isang [DID na query](https://www.w3.org/TR/did-core/#dfn-did-queries) ay kapareho ng isang generic na query sa [URI](https://www.w3.org/TR/did-core/#dfn-uri) at umaayon sa querypanuntunan ng ABNF sa [RFC 3986, seksyon 3.4](https://www.rfc-editor.org/rfc/rfc3986#section-3.4) . Ang tampok na syntax na ito ay inilalarawan sa[3.2.1Mga Parameter ng DID](https://www.w3.org/TR/did-core/#did-parameters) .

[HALIMBAWA3](https://www.w3.org/TR/did-core/#example-3)

did:example:123456?versionId=1

#### Fragment

[Ang DID fragment](https://www.w3.org/TR/did-core/#dfn-did-fragments) syntax at semantics ay magkapareho sa isang generic na [URI](https://www.w3.org/TR/did-core/#dfn-uri) fragment at tumutugma sa fragmentpanuntunan ng ABNF sa [RFC 3986, seksyon 3.5](https://www.rfc-editor.org/rfc/rfc3986#section-3.5) .

Ang isang [DID fragment](https://www.w3.org/TR/did-core/#dfn-did-fragments) ay ginagamit bilang isang method-independent reference sa isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) o panlabas na [mapagkukunan](https://www.w3.org/TR/did-core/" \l "dfn-resources) . Ang ilang mga halimbawa ng DID fragment identifier ay ipinapakita sa ibaba.

[HALIMBAWA4](https://www.w3.org/TR/did-core/#example-a-unique-verification-method-in-a-did-document): Isang natatanging paraan ng pag-verify sa isang DID Document

did:example:123#public-key-0

[HALIMBAWA5](https://www.w3.org/TR/did-core/#example-a-unique-service-in-a-did-document): Isang natatanging serbisyo sa isang DID Document

ginawa:halimbawa:123#agent

[HALIMBAWA6](https://www.w3.org/TR/did-core/#example-a-resource-external-to-a-did-document): Isang mapagkukunang panlabas sa isang DID Document

did:example:123?service=agent&relativeRef=/credentials#degree

TANDAAN : I-fragment ang semantics sa mga representasyon

Upang mapakinabangan ang interoperability, hinihimok ang mga tagapagpatupad na tiyaking ang mga [fragment ng DID](https://www.w3.org/TR/did-core/#dfn-did-fragments) ay binibigyang kahulugan sa parehong paraan sa mga [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) (tingnan ang[6.Mga Kinatawan](https://www.w3.org/TR/did-core/#representations) ). Halimbawa, habang ang JSON Pointer [ [RFC6901](https://www.w3.org/TR/did-core/#bib-rfc6901) ] ay maaaring gamitin sa isang [DID fragment](https://www.w3.org/TR/did-core/#dfn-did-fragments) , hindi ito bibigyang-kahulugan sa parehong paraan sa mga hindi JSON na [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) .

Ang mga karagdagang semantika para sa mga pagkakakilanlan ng fragment, na tugma at naka-layer sa mga semantika sa seksyong ito, ay inilalarawan para sa mga representasyon ng JSON-LD sa[E.2application/did+ld+json](https://www.w3.org/TR/did-core/#application-did-ld-json) . Para sa impormasyon tungkol sa kung paano i-dereference ang isang [DID fragment](https://www.w3.org/TR/did-core/#dfn-did-fragments) , tingnan[7.2DID URL Dereferencing](https://www.w3.org/TR/did-core/#did-url-dereferencing) .

#### 3.2.1Mga Parameter ng DID

[Sinusuportahan ng syntax ng DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) ang isang simpleng format para sa mga parameter batay sa querybahaging inilarawan sa [Query](https://www.w3.org/TR/did-core/#query) . Ang pagdaragdag ng parameter ng DID sa isang [URL](https://www.w3.org/TR/did-core/#dfn-did-urls) ng DID ay nangangahulugan na ang parameter ay nagiging bahagi ng identifier para sa isang [mapagkukunan](https://www.w3.org/TR/did-core/" \l "dfn-resources) .

[HALIMBAWA7](https://www.w3.org/TR/did-core/#example-a-did-url-with-a-versiontime-did-parameter): Isang DID URL na may parameter na 'versionTime' DID

did:example:123?versionTime=2021-05-10T17:00:00Z

[HALIMBAWA8](https://www.w3.org/TR/did-core/#example-a-did-url-with-a-service-and-a-relativeref-did-parameter): Isang DID URL na may 'service' at isang 'relativeRef' DID parameter

did:example:123?service=files&relativeRef=/resume.pdf

Ang ilang mga parameter ng DID ay ganap na independiyente sa anumang partikular na [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) at gumagana sa parehong paraan para sa lahat ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) . Ang iba pang mga parameter ng DID ay hindi sinusuportahan ng lahat ng mga [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) . Kung saan sinusuportahan ang mga opsyonal na parameter, inaasahang gagana ang mga ito nang pantay-pantay sa mga [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) na sumusuporta sa kanila. Ang sumusunod na talahanayan ay nagbibigay ng mga karaniwang parameter ng DID na gumagana sa parehong paraan sa lahat ng mga [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) . Ang suporta para sa lahat ng [DID Parameter](https://www.w3.org/TR/did-core/#did-parameters) ay OPTIONAL .

TANDAAN

Karaniwang inaasahan na ang mga pagpapatupad ng DID URL dereferencer ay sumangguni sa [ [DID-RESOLUTION](https://www.w3.org/TR/did-core/#bib-did-resolution) ] para sa mga karagdagang detalye ng pagpapatupad. Ang saklaw ng detalyeng ito ay tumutukoy lamang sa kontrata ng mga pinakakaraniwang parameter ng query.

| **Pangalan ng Parameter** | **Paglalarawan** |
| --- | --- |
| [service](https://www.w3.org/TR/did-core/#dfn-service) | Kinikilala ang isang serbisyo mula sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) sa pamamagitan ng ID ng serbisyo. Kung mayroon, ang nauugnay na halaga ay DAPAT na isang [ASCII string](https://infra.spec.whatwg.org/#ascii-string) . |
| relativeRef | Isang kamag-anak na sanggunian ng [URI](https://www.w3.org/TR/did-core/#dfn-uri) ayon sa [RFC3986 Seksyon 4.2](https://www.rfc-editor.org/rfc/rfc3986#section-4.2) na tumutukoy sa isang [mapagkukunan](https://www.w3.org/TR/did-core/" \l "dfn-resources) sa isang [endpoint ng serbisyo](https://www.w3.org/TR/did-core/#dfn-service-endpoints) , na pinili mula sa isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) sa pamamagitan ng paggamit ng serviceparameter. Kung mayroon, ang nauugnay na value ay DAPAT na isang [ASCII string](https://infra.spec.whatwg.org/#ascii-string) at DAPAT gumamit ng percent-encoding para sa ilang partikular na character gaya ng tinukoy sa [RFC3986 Seksyon 2.1](https://www.rfc-editor.org/rfc/rfc3986#section-2.1) . |
| versionId | Tinutukoy ang isang partikular na bersyon ng isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) na lulutasin (ang bersyon ID ay maaaring sunud-sunod, o isang [UUID](https://www.w3.org/TR/did-core/#dfn-uuid) , o partikular sa pamamaraan). Kung mayroon, ang nauugnay na halaga ay DAPAT na isang [ASCII string](https://infra.spec.whatwg.org/#ascii-string) . |
| versionTime | Kinikilala ang isang partikular na bersyon ng timestamp ng isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) na lutasin. Ibig sabihin, ang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) na wasto para sa isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) sa isang partikular na oras. Kung mayroon, ang nauugnay na value ay DAPAT na isang [ASCII string](https://infra.spec.whatwg.org/#ascii-string) na isang wastong XML datetime value, gaya ng tinukoy sa seksyon 3.3.7 ng [W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes](https://www.w3.org/TR/xmlschema11-2/) [ [XMLSCHEMA11-2](https://www.w3.org/TR/did-core/#bib-xmlschema11-2) ]. DAPAT gawing normal ang halaga ng datetime na ito sa UTC 00:00:00 at walang sub-second decimal precision. Halimbawa: 2020-12-20T19:17:47Z. |
| hl | Isang mapagkukunang hash ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) upang magdagdag ng proteksyon sa integridad, gaya ng tinukoy sa [ [HASHLINK](https://www.w3.org/TR/did-core/#bib-hashlink) ]. Ang parameter na ito ay hindi normatibo. Kung mayroon, ang nauugnay na halaga ay DAPAT na isang [ASCII string](https://infra.spec.whatwg.org/#ascii-string) . |

Ang mga tagapagpatupad pati na rin ang mga may-akda ng detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ay maaaring gumamit ng mga karagdagang parameter ng DID na hindi nakalista dito. Para sa maximum na interoperability, INIREREKOMENDA na gamitin ng mga parameter ng DID ang mekanismo ng DID Specification Registries [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ], upang maiwasan ang banggaan sa iba pang paggamit ng parehong parameter ng DID na may magkakaibang semantika.

Maaaring gamitin ang mga parameter ng DID kung mayroong malinaw na kaso ng paggamit kung saan ang parameter ay kailangang maging bahagi ng isang [URL](https://url.spec.whatwg.org/#concept-url) na tumutukoy sa isang [mapagkukunan](https://www.w3.org/TR/did-core/" \l "dfn-resources) nang mas tumpak kaysa sa paggamit ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) lamang. Inaasahan na ang mga parameter ng DID ay hindi ginagamit kung ang parehong functionality ay maaaring ipahayag sa pamamagitan ng pagpasa ng input metadata sa isang [DID resolver](https://www.w3.org/TR/did-core/#dfn-did-resolvers) . Ang mga karagdagang pagsasaalang-alang para sa pagproseso ng mga parameter na ito ay tinalakay sa [ [DID-RESOLUTION](https://www.w3.org/TR/did-core/#bib-did-resolution) ].

TANDAAN : Mga parameter ng DID at resolution ng DID

Ang [DID resolution](https://www.w3.org/TR/did-core/#dfn-did-resolution) at ang [DID URL dereferencing](https://www.w3.org/TR/did-core/#dfn-did-url-dereferencing) function ay maaaring maimpluwensyahan sa pamamagitan ng pagpasa ng input metadata sa isang [DID resolver](https://www.w3.org/TR/did-core/#dfn-did-resolvers) na hindi bahagi ng [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) (tingnan ang[7.1.1Mga Opsyon sa Resolusyon ng DID](https://www.w3.org/TR/did-core/#did-resolution-options) ). Ito ay maihahambing sa HTTP, kung saan maaaring isama ang ilang partikular na parameter sa isang HTTP URL, o ipasa bilang mga header ng HTTP sa panahon ng proseso ng dereferencing. Ang mahalagang pagkakaiba ay ang mga parameter ng DID na bahagi ng [URL ng DID](https://www.w3.org/TR/did-core/#dfn-did-urls) ay dapat gamitin upang tukuyin kung anong *[mapagkukunan](https://www.w3.org/TR/did-core/" \l "dfn-resources)* ang tinutukoy , samantalang ang input ng metadata na hindi bahagi ng [URL ng DID](https://www.w3.org/TR/did-core/#dfn-did-urls) ay dapat gamitin upang kontrolin kung paano niresolba o na-dereference ang *[mapagkukunang](https://www.w3.org/TR/did-core/" \l "dfn-resources)* iyon.

#### 3.2.2Mga kamag-anak na DID URL

Ang isang kamag-anak na [URL ng DID](https://www.w3.org/TR/did-core/#dfn-did-urls) ay anumang halaga ng URL sa isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) na hindi nagsisimula sa did:<method-name>:<method-specific-id>. Higit na partikular, ito ay anumang halaga ng URL na hindi nagsisimula sa ABNF na tinukoy sa [3.1DID Syntax](https://www.w3.org/TR/did-core/#did-syntax) . Ang URL ay inaasahang magre-refer ng isang [mapagkukunan](https://www.w3.org/TR/did-core/" \l "dfn-resources) sa parehong [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) . MAAARING naglalaman ang mga kaugnay [na URL ng DID ng mga](https://www.w3.org/TR/did-core/" \l "dfn-did-urls)kaugnay na bahagi ng path, mga parameter ng query, at mga pagkakakilanlan ng fragment.

Kapag niresolba ang isang kamag-anak na reference ng [DID URL ,](https://www.w3.org/TR/did-core/#dfn-did-urls)DAPAT gamitin ang algorithm na tinukoy sa [RFC3986 Seksyon 5: Reference Resolution .](https://www.rfc-editor.org/rfc/rfc3986#section-5)Ang **batayang halaga ng URI** ay ang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na nauugnay sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) , tingnan mo[5.1.1DID Paksa](https://www.w3.org/TR/did-core/#did-subject) . Ang **scheme** ay did. Ang **awtoridad** ay kumbinasyon ng <method-name>:<method-specific-id>, at ang **path** , **query** , at **fragment** na mga halaga ay ang mga tinukoy sa [Path](https://www.w3.org/TR/did-core/#path) , [Query](https://www.w3.org/TR/did-core/#query) , at [Fragment](https://www.w3.org/TR/did-core/#fragment) , ayon sa pagkakabanggit.

Ang mga kaugnay na [URL ng DID](https://www.w3.org/TR/did-core/#dfn-did-urls) ay kadalasang ginagamit upang i-reference ang mga paraan at [serbisyo sa pag-](https://www.w3.org/TR/did-core/" \l "dfn-service)[verify](https://www.w3.org/TR/did-core/#dfn-verification-method) sa isang [DID Document](https://www.w3.org/TR/did-core/#dfn-did-documents) nang hindi kinakailangang gumamit ng mga ganap na URL. [Ang mga pamamaraan ng DID](https://www.w3.org/TR/did-core/#dfn-did-methods) kung saan ang laki ng imbakan ay isang pagsasaalang-alang ay maaaring gumamit ng mga kaugnay na URL upang bawasan ang laki ng imbakan ng mga [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) .

[HALIMBAWA9](https://www.w3.org/TR/did-core/#example-an-example-of-a-relative-did-url): Isang halimbawa ng isang kamag-anak na DID URL

{

"@context": [

"https://www.w3.org/ns/did/v1",

"https://w3id.org/security/suites/ed25519-2020/v1"

]

"id": "did:example:123456789abcdefghi",

"paraan ng pagpapatunay": [{

"id": "did:example:123456789abcdefghi#key-1",

"type": "Ed25519VerificationKey2020", // panlabas (property value)

"controller": "did:example:123456789abcdefghi",

"publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"

}, ...],

"authentication": [

// isang kamag-anak na URL ng DID na ginamit upang sumangguni sa isang paraan ng pag-verify sa itaas ng

" **#key-1** "

]

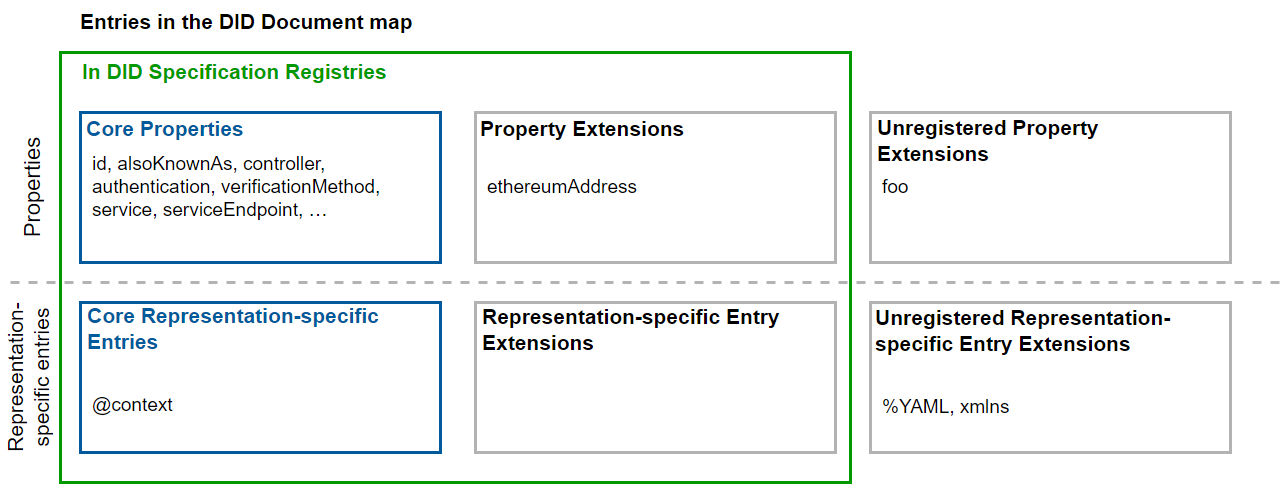
}

Sa halimbawa sa itaas, ang kaugnay na halaga ng [URL ng DID](https://www.w3.org/TR/did-core/#dfn-did-urls) ay gagawing ganap na halaga ng [URL ng DID](https://www.w3.org/TR/did-core/#dfn-did-urls)did:example:123456789abcdefghi#key-1 na .

## 4.Modelo ng Data

Tinutukoy ng detalyeng ito ang isang modelo ng data na maaaring magamit upang ipahayag ang [mga dokumento](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ng DID at mga istruktura ng data ng dokumento ng DID, na pagkatapos ay maaaring i-serialize sa maraming konkretong [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) . Nagbibigay ang seksyong ito ng mataas na antas na paglalarawan ng modelo ng data, mga paglalarawan ng mga paraan kung paano ipinahayag ang iba't ibang uri ng mga katangian sa modelo ng data, at mga tagubilin para sa pagpapalawak ng modelo ng data.

Ang isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) ay binubuo ng isang [mapa](https://infra.spec.whatwg.org/" \l "maps) ng mga [entry](https://infra.spec.whatwg.org/#map-entry) , kung saan ang bawat entry ay binubuo ng isang key/value pair. Ang modelo ng data ng [dokumento ng DID ay](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) naglalaman ng hindi bababa sa dalawang magkaibang klase ng mga entry. Ang unang klase ng mga entry ay tinatawag na mga katangian, at tinukoy sa seksyon[5.Mga Pangunahing Katangian](https://www.w3.org/TR/did-core/#core-properties) . Ang pangalawang klase ay binubuo ng mga [entry na tukoy sa representasyon](https://www.w3.org/TR/did-core/#dfn-representation-specific-entry) , at tinukoy sa seksyon[6.Mga representasyon](https://www.w3.org/TR/did-core/#representations) .



(img src: <https://www.w3.org/TR/did-core/diagrams/diagram-did-document-entries.svg>)

*Pigura*3*Ang mga entry sa isang DID na dokumento. Tingnan din ang: [paglalarawan ng salaysay](https://www.w3.org/TR/did-core/" \l "did-document-entries-longdesc) .*

Ang lahat ng entry key sa modelo ng data ng [dokumento ng DID ay mga](https://www.w3.org/TR/did-core/" \l "dfn-did-documents)[string](https://infra.spec.whatwg.org/#strings) . Ang lahat ng mga halaga ng entry ay ipinahayag gamit ang isa sa mga abstract na uri ng data sa talahanayan sa ibaba, at ang bawat [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) ay tumutukoy sa kongkretong serialization na format ng bawat uri ng data.

| **Uri ng datos** | **Mga pagsasaalang-alang** |
| --- | --- |
| [mapa](https://infra.spec.whatwg.org/#maps) | Isang may hangganan na pagkakasunud-sunod ng mga key/value pairs, na walang key na lumalabas nang dalawang beses gaya ng tinukoy sa [ [INFRA](https://www.w3.org/TR/did-core/#bib-infra) ]. Ang isang mapa ay minsang tinutukoy bilang isang [nakaayos na mapa](https://infra.spec.whatwg.org/" \l "maps) sa [ [INFRA](https://www.w3.org/TR/did-core/#bib-infra) ]. |
| [listahan](https://infra.spec.whatwg.org/#list) | Isang may hangganan na pagkakasunod-sunod ng mga item gaya ng tinukoy sa [ [INFRA](https://www.w3.org/TR/did-core/#bib-infra) ]. |
| [itakda](https://infra.spec.whatwg.org/#ordered-set) | Isang may hangganan na pagkakasunud-sunod ng mga item na hindi naglalaman ng parehong item nang dalawang beses tulad ng tinukoy sa [ [INFRA](https://www.w3.org/TR/did-core/#bib-infra) ]. Ang isang set ay minsang tinutukoy bilang isang [ordered set](https://infra.spec.whatwg.org/#ordered-set) sa [ [INFRA](https://www.w3.org/TR/did-core/#bib-infra) ]. |
| ***datetime*** | Isang halaga ng petsa at oras na may kakayahang ipahayag nang walang pagkawala ang lahat ng mga halaga na maipapahayag ng a dateTimegaya ng tinukoy sa [ [XMLSCHEMA11-2](https://www.w3.org/TR/xmlschema11-2/#dateTime) ]. |
| [string](https://infra.spec.whatwg.org/#string) | Isang pagkakasunud-sunod ng mga unit ng code na kadalasang ginagamit upang kumatawan sa nababasang wika ng tao gaya ng tinukoy sa [ [INFRA](https://www.w3.org/TR/did-core/#bib-infra) ]. |
| ***integer*** | Isang tunay na numero na walang fractional component gaya ng tinukoy sa [ [XMLSCHEMA11-2](https://www.w3.org/TR/xmlschema11-2/#decimal) ]. Upang mapakinabangan ang interoperability, hinihimok ang mga tagapagpatupad na sundin ang payo tungkol sa mga integer sa [RFC8259, Seksyon 6: Mga Numero](https://www.rfc-editor.org/rfc/rfc8259#section-6) . |
| ***doble*** | Isang halaga na kadalasang ginagamit upang tantiyahin ang mga arbitrary na tunay na numero gaya ng tinukoy sa [ [XMLSCHEMA11-2](https://www.w3.org/TR/xmlschema11-2/#double) ]. Upang i-maximize ang interoperability, hinihimok ang mga tagapagpatupad na sundin ang payo tungkol sa mga doble sa [RFC8259, Seksyon 6: Mga Numero](https://www.rfc-editor.org/rfc/rfc8259#section-6) . |
| [boolean](https://infra.spec.whatwg.org/#boolean) | Isang value na tama o mali gaya ng tinukoy sa [ [INFRA](https://www.w3.org/TR/did-core/#bib-infra) ]. |
| [wala](https://infra.spec.whatwg.org/#nulls) | Isang halaga na ginagamit upang ipahiwatig ang kakulangan ng isang halaga tulad ng tinukoy sa [ [INFRA](https://www.w3.org/TR/did-core/#bib-infra) ]. |

Bilang resulta ng pagtukoy sa [modelo ng data](https://www.w3.org/TR/did-core/" \l "data-model) gamit ang terminolohiya mula sa [ [INFRA](https://www.w3.org/TR/did-core/#bib-infra) ], ang mga value ng property na maaaring maglaman ng higit sa isang item, tulad ng mga [listahan](https://infra.spec.whatwg.org/" \l "list) , [mapa](https://infra.spec.whatwg.org/" \l "ordered-map) at [set](https://infra.spec.whatwg.org/#ordered-set) , ay tahasang iniutos. Ang lahat ng mga istraktura ng halaga na tulad ng listahan sa [ [INFRA](https://www.w3.org/TR/did-core/#bib-infra) ] ay nakaayos, mahalaga man o hindi ang pagkakasunud-sunod na iyon. Para sa mga layunin ng pagtutukoy na ito, maliban kung iba ang nakasaad, hindi mahalaga ang [mapa](https://infra.spec.whatwg.org/" \l "ordered-map) at [set](https://infra.spec.whatwg.org/#ordered-set) na pag- order at ang mga pagpapatupad ay hindi inaasahang makakagawa o makakakonsumo ng mga deterministikong order na halaga.

### **4.1Pagpapalawig**

Sinusuportahan ng modelo ng data ang dalawang uri ng pagpapalawak.

1. Para sa maximum na interoperability, inirerekumenda na gamitin ng mga extension ang mekanismo ng W3C DID Specification Registries [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ]. Ang paggamit ng mekanismong ito para sa mga bagong pag-aari o iba pang mga extension ay ang tanging tinukoy na mekanismo na nagsisiguro na ang dalawang magkaibang [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) ay magagawang magtulungan.
2. MAAARING tukuyin ng mga [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) ang iba pang mga mekanismo ng pagpapalawak, kabilang ang mga hindi nangangailangan ng paggamit ng DID Specification Registry. DAPAT suportahan ng gayong mga mekanismo ng extension ang lossless na conversion sa anumang iba pang conformant na [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) . DAPAT tukuyin ng mga mekanismo ng extension para sa isang [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) ang pagmamapa ng lahat ng mga katangian at syntax ng [representasyon sa](https://www.w3.org/TR/did-core/" \l "dfn-representations)[modelo ng data](https://www.w3.org/TR/did-core/#data-model) at sistema ng uri nito.

TANDAAN : Hindi gaanong maaasahan ang mga hindi nakarehistrong extension  
  
Palaging posible para sa dalawang partikular na pagpapatupad na sumang-ayon sa labas ng banda na gumamit ng isang nauunawaang extension o [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) na hindi nakatala sa DID Specification Registries [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ]; Ang interoperability sa pagitan ng mga naturang pagpapatupad at ang mas malaking ecosystem ay hindi gaanong maaasahan.

## 5.Mga Pangunahing Katangian

Ang isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay nauugnay sa isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) . [Ang mga dokumento ng DID](https://www.w3.org/TR/did-core/#dfn-did-documents) ay ipinahayag gamit ang [modelo ng data](https://www.w3.org/TR/did-core/" \l "data-model) at maaaring i-serialize sa isang [representasyon](https://www.w3.org/TR/did-core/" \l "representations) . Tinutukoy ng mga sumusunod na seksyon ang mga katangian sa isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) , kabilang ang kung kinakailangan o opsyonal ang mga katangiang ito. Inilalarawan ng mga katangiang ito ang mga ugnayan sa pagitan ng [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) at ang halaga ng ari-arian.

Ang mga sumusunod na talahanayan ay naglalaman ng mga impormasyong sanggunian para sa mga pangunahing katangian na tinukoy ng detalyeng ito, na may mga inaasahang halaga, at kung kinakailangan o hindi ang mga ito. Naka-link ang mga pangalan ng property sa mga talahanayan sa mga normatibong kahulugan at mas detalyadong paglalarawan ng bawat property.

TANDAAN : Mga pangalan ng ari-arian na ginagamit sa mga mapa ng iba't ibang uri

Ang mga pangalan ng ari-arian id, type, at controllermaaaring naroroon sa mga mapa ng iba't ibang uri na may posibleng pagkakaiba sa mga hadlang.

### **DID Document properties**

| **Ari-arian** | **Kailangan?** | **Mga hadlang sa halaga** |
| --- | --- | --- |
| [id](https://www.w3.org/TR/did-core/#dfn-id) | oo | Isang [string](https://infra.spec.whatwg.org/#string) na umaayon sa mga panuntunan sa [3.1DID Syntax](https://www.w3.org/TR/did-core/#did-syntax) . |
| [alsoKnownAs](https://www.w3.org/TR/did-core/#dfn-alsoknownas) | hindi | Isang [hanay](https://infra.spec.whatwg.org/" \l "ordered-set) ng mga [string](https://infra.spec.whatwg.org/#string) na umaayon sa mga panuntunan ng [ [RFC3986](https://www.w3.org/TR/did-core/#bib-rfc3986) ] para sa mga [URI](https://www.w3.org/TR/did-core/#dfn-uri) . |
| [controller](https://www.w3.org/TR/did-core/#dfn-controller) | hindi | Isang [string](https://infra.spec.whatwg.org/#string) o isang [hanay](https://infra.spec.whatwg.org/" \l "ordered-set) ng mga [string](https://infra.spec.whatwg.org/#string) na sumusunod sa mga panuntunan sa [3.1DID Syntax](https://www.w3.org/TR/did-core/#did-syntax) . |
| [verificationMethod](https://www.w3.org/TR/did-core/#dfn-verificationmethod) | hindi | Isang [hanay](https://infra.spec.whatwg.org/" \l "ordered-set) ng mga [mapa ng](https://infra.spec.whatwg.org/" \l "ordered-map)[Paraan ng Pag-verify](https://www.w3.org/TR/did-core/#dfn-verification-method) na sumusunod sa mga panuntunan sa mga [katangian ng Paraan ng Pag-verify](https://www.w3.org/TR/did-core/" \l "verification-method-properties) . |
| [authentication](https://www.w3.org/TR/did-core/#dfn-authentication) | hindi | Isang [hanay](https://infra.spec.whatwg.org/" \l "ordered-set) ng alinman sa mga [mapa ng](https://infra.spec.whatwg.org/" \l "ordered-map)[Paraan ng Pag-verify](https://www.w3.org/TR/did-core/#dfn-verification-method) na sumusunod sa mga panuntunan sa mga [katangian ng Paraan ng Pag-verify](https://www.w3.org/TR/did-core/" \l "verification-method-properties) ) o mga [string](https://infra.spec.whatwg.org/#string) na umaayon sa mga panuntunan sa [3.2DID URL Syntax](https://www.w3.org/TR/did-core/#did-url-syntax) . |
| [assertionMethod](https://www.w3.org/TR/did-core/#dfn-assertionmethod) | hindi |
| [keyAgreement](https://www.w3.org/TR/did-core/#dfn-keyagreement) | hindi |
| [capabilityInvocation](https://www.w3.org/TR/did-core/#dfn-capabilityinvocation) | hindi |
| [capabilityDelegation](https://www.w3.org/TR/did-core/#dfn-capabilitydelegation) | hindi |
| [service](https://www.w3.org/TR/did-core/#dfn-service) | hindi | Isang [hanay](https://infra.spec.whatwg.org/" \l "ordered-set) ng mga [mapa ng](https://infra.spec.whatwg.org/" \l "ordered-map)[Endpoint ng Serbisyo](https://www.w3.org/TR/did-core/#dfn-service-endpoints) na sumusunod sa mga panuntunan sa mga [property ng Serbisyo](https://www.w3.org/TR/did-core/#service-properties) . |

### **Mga katangian ng Paraan ng Pag-verify**

| **Ari-arian** | **Kailangan?** | **Mga hadlang sa halaga** |
| --- | --- | --- |
| id | oo | Isang [string](https://infra.spec.whatwg.org/#string) na umaayon sa mga panuntunan sa [3.2DID URL Syntax](https://www.w3.org/TR/did-core/#did-url-syntax) . |
| [controller](https://www.w3.org/TR/did-core/#dfn-controller) | oo | Isang [string](https://infra.spec.whatwg.org/#string) na umaayon sa mga panuntunan sa [3.1DID Syntax](https://www.w3.org/TR/did-core/#did-syntax) . |
| type | oo | Isang [string](https://infra.spec.whatwg.org/#string) . |
| [publicKeyJwk](https://www.w3.org/TR/did-core/#dfn-publickeyjwk) | hindi | Isang [mapa](https://infra.spec.whatwg.org/" \l "maps) na kumakatawan sa isang JSON Web Key na tumutugma sa [ [RFC7517](https://www.w3.org/TR/did-core/#bib-rfc7517) ]. Tingnan [ang kahulugan ng publicKeyJwk](https://www.w3.org/TR/did-core/#dfn-publickeyjwk) para sa karagdagang mga hadlang. |
| [publicKeyMultibase](https://www.w3.org/TR/did-core/#dfn-publickeymultibase) | hindi | Isang [string](https://infra.spec.whatwg.org/#string) na tumutugma sa isang [ [MULTIBASE](https://www.w3.org/TR/did-core/#bib-multibase) ] na naka-encode na pampublikong key. |

### **Mga katangian ng serbisyo**

| **Ari-arian** | **Kailangan?** | **Mga hadlang sa halaga** |
| --- | --- | --- |
| id | oo | Isang [string](https://infra.spec.whatwg.org/#string) na umaayon sa mga panuntunan ng [ [RFC3986](https://www.w3.org/TR/did-core/#bib-rfc3986) ] para sa mga [URI](https://www.w3.org/TR/did-core/#dfn-uri) . |
| type | oo | Isang [string](https://infra.spec.whatwg.org/#string) o isang [hanay](https://infra.spec.whatwg.org/" \l "ordered-set) ng mga [string](https://infra.spec.whatwg.org/#string) . |
| [serviceEndpoint](https://www.w3.org/TR/did-core/#dfn-serviceendpoint) | oo | Isang [string](https://infra.spec.whatwg.org/#string) na umaayon sa mga panuntunan ng [ [RFC3986](https://www.w3.org/TR/did-core/#bib-rfc3986) ] para sa mga [URI](https://www.w3.org/TR/did-core/#dfn-uri) , isang [mapa](https://infra.spec.whatwg.org/" \l "string) , o isang [set](https://infra.spec.whatwg.org/#ordered-set) na binubuo ng isa o higit pang mga [string](https://infra.spec.whatwg.org/#string) na sumusunod sa mga panuntunan ng [ [RFC3986](https://www.w3.org/TR/did-core/#bib-rfc3986) ] para sa mga [URI](https://www.w3.org/TR/did-core/#dfn-uri) at/o mga [mapa](https://infra.spec.whatwg.org/" \l "string) . |

### **5.1Mga Identifier**

Inilalarawan ng seksyong ito ang mga mekanismo kung saan kasama sa mga [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ang mga identifier para sa mga [paksa](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ng DID at mga [controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) ng DID .

#### 5.1.1DID Paksa

Ang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) para sa isang partikular na [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ay ipinahayag gamit ang ari- [id](https://www.w3.org/TR/did-core/" \l "dfn-id)arian sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) .

**id**

Ang halaga ng id DAPAT ay isang [string](https://infra.spec.whatwg.org/#string) na sumusunod sa mga panuntunan sa[3.1DID Syntax](https://www.w3.org/TR/did-core/#did-syntax) at DAPAT umiiral sa root [map](https://infra.spec.whatwg.org/#ordered-map) ng [data model](https://www.w3.org/TR/did-core/#data-model) para sa [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) .

[HALIMBAWA10](https://www.w3.org/TR/did-core/#example-10)

{

"id": "did:example:123456789abcdefghijk"

}

Tinutukoy idlamang ng property ang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ng [paksa](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ng DID kapag naroroon ito sa pinakamataas na [mapa](https://infra.spec.whatwg.org/" \l "ordered-map) ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) .

TANDAAN : Mga intermediate na representasyon

[Ang mga detalye ng paraan ng DID](https://www.w3.org/TR/did-core/#dfn-did-methods) ay maaaring lumikha ng mga intermediate na representasyon ng isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) na hindi naglalaman ng [id](https://www.w3.org/TR/did-core/" \l "dfn-id)property, gaya ng kapag ang isang [DID resolver](https://www.w3.org/TR/did-core/#dfn-did-resolvers) ay gumaganap ng [DID resolution](https://www.w3.org/TR/did-core/#dfn-did-resolution) . Gayunpaman, ang ganap na nalutas na [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay palaging naglalaman ng isang wastong ari- [id](https://www.w3.org/TR/did-core/" \l "dfn-id)arian.

#### 5.1.2DID Controller

Ang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) ay isang entity na pinahintulutan na gumawa ng mga pagbabago sa isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) . Ang proseso ng pagpapahintulot sa isang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) ay tinukoy ng [DID method](https://www.w3.org/TR/did-core/#dfn-did-methods) .

**controller**

OPTIONAL ang controllerproperty . Kung mayroon, ang value ay DAPAT na isang [string](https://infra.spec.whatwg.org/#string) o isang [hanay](https://infra.spec.whatwg.org/" \l "ordered-set) ng mga [string](https://infra.spec.whatwg.org/#string) na sumusunod sa mga panuntunan sa[3.1DID Syntax](https://www.w3.org/TR/did-core/#did-syntax) . Ang katumbas na (mga) [dokumento ng DID ay](https://www.w3.org/TR/did-core/" \l "dfn-did-documents)DAPAT maglaman ng mga [ugnayan sa pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship) na tahasang nagpapahintulot sa paggamit ng ilang mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) para sa mga partikular na layunin.

Kapag ang isang [controller](https://www.w3.org/TR/did-core/" \l "dfn-controller)property ay naroroon sa isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) , ang halaga nito ay nagpapahayag ng isa o higit pang [mga DID](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers) . Ang anumang mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) na nilalaman sa mga [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) para sa mga [DID na iyon ay](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers)DAPAT tanggapin bilang may awtoridad, upang ang mga patunay na nakakatugon sa mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ay maituturing na katumbas ng mga patunay na ibinigay ng [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) .

[HALIMBAWA11](https://www.w3.org/TR/did-core/#example-did-document-with-a-controller-property): DID dokumento na may controller property

{

"@context": "https://www.w3.org/ns/did/v1",

"id": "did:example:123456789abcdefghi",

"controller": "did:example:bcehfew7h32f32h7af3",

}

TANDAAN : Awtorisasyon vs authentication

Tandaan na ang pahintulot na ibinigay ng halaga ng controlleray hiwalay sa pagpapatunay tulad ng inilarawan sa[5.3.1Pagpapatunay](https://www.w3.org/TR/did-core/#authentication) . Ito ay partikular na mahalaga para sa key recovery sa kaso ng cryptographic key loss, kung saan ang [DID subject](https://www.w3.org/TR/did-core/#dfn-did-subjects) ay wala nang access sa kanilang mga key, o key compromise, kung saan ang mga pinagkakatiwalaang third party ng [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) ay kailangang i-override ang nakakahamak na aktibidad ng isang attacker. Tingnan mo[9.Mga Pagsasaalang- alang sa Seguridad](https://www.w3.org/TR/did-core/#security-considerations) para sa impormasyong nauugnay sa mga modelo ng pagbabanta at mga vector ng pag-atake.

#### 5.1.3Kilala rin sa

Ang isang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ay maaaring magkaroon ng maraming identifier para sa iba't ibang layunin, o sa iba't ibang oras. Ang pagsasabi na ang dalawa o higit pang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) (o iba pang uri ng [URI](https://www.w3.org/TR/did-core/#dfn-uri) ) ay tumutukoy sa parehong [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ay maaaring gawin gamit ang [alsoKnownAs](https://www.w3.org/TR/did-core/" \l "dfn-alsoknownas)property.

**kilala rin sa**

OPTIONAL ang alsoKnownAsproperty . Kung mayroon, ang value ay DAPAT na isang [set](https://infra.spec.whatwg.org/#ordered-set) kung saan ang bawat item sa set ay isang [URI](https://www.w3.org/TR/did-core/#dfn-uri) na tumutugma sa [ [RFC3986](https://www.w3.org/TR/did-core/#bib-rfc3986) ].

Ang kaugnayang ito ay isang pahayag na ang paksa ng identifier na ito ay kinilala rin ng isa o higit pang mga identifier.

TANDAAN : Pagtutumbas at Kilala rin Bilang

Maaaring piliin ng mga application na isaalang-alang ang dalawang pagkakakilanlan na nauugnay ni [alsoKnownAs](https://www.w3.org/TR/did-core/" \l "dfn-alsoknownas)upang maging katumbas *kung* ang [alsoKnownAs](https://www.w3.org/TR/did-core/" \l "dfn-alsoknownas)relasyon ay ginagantihan sa baligtad na direksyon. Pinakamabuting kasanayan na *huwag* isaalang-alang ang mga ito na katumbas sa kawalan ng kabaligtaran na relasyon na ito. Sa madaling salita, ang pagkakaroon ng isang [alsoKnownAs](https://www.w3.org/TR/did-core/" \l "dfn-alsoknownas)assertion ay hindi nagpapatunay na ang assertion na ito ay totoo. Samakatuwid, mahigpit na ipinapayo na ang humihiling na partido ay kumuha ng independiyenteng pag-verify ng isang alsoKnownAsassertion.

Dahil ang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ay maaaring gumamit ng iba't ibang mga identifier para sa iba't ibang layunin, ang pag-asa ng malakas na pagkakapareho sa pagitan ng dalawang pagkakakilanlan, o pagsasama-sama ng impormasyon ng dalawang kaukulang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) , ay hindi kinakailangang naaangkop, *kahit na may* katumbas na relasyon.

### **5.2Mga Paraan ng Pagpapatunay**

Ang isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay maaaring magpahayag ng mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) , tulad ng mga cryptographic na pampublikong key, na maaaring magamit upang [patotohanan](https://www.w3.org/TR/did-core/" \l "dfn-authenticated) o pahintulutan ang mga pakikipag-ugnayan sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) o mga nauugnay na partido. Halimbawa, ang isang cryptographic na pampublikong key ay maaaring gamitin bilang isang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) na may kinalaman sa isang digital na lagda; sa ganitong paggamit, bini-verify nito na maaaring gamitin ng lumagda ang nauugnay na cryptographic na pribadong key. Maaaring tumagal ng maraming parameter [ang mga paraan ng pag-verify .](https://www.w3.org/TR/did-core/#dfn-verification-method)Ang isang halimbawa nito ay isang hanay ng limang cryptographic key kung saan ang alinman sa tatlo ay kinakailangang mag-ambag sa isang cryptographic threshold signature.

**paraan ng pagpapatunay**

OPTIONAL ang verificationMethodproperty . Kung mayroon, ang halaga ay DAPAT na isang [hanay](https://infra.spec.whatwg.org/" \l "ordered-set) ng mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) , kung saan ang bawat [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ay ipinahayag gamit ang isang [mapa](https://infra.spec.whatwg.org/" \l "ordered-map) . DAPAT kasama sa [mapa ng](https://infra.spec.whatwg.org/" \l "ordered-map)[paraan](https://www.w3.org/TR/did-core/#dfn-verification-method) ng pag - verify ang , , , at mga partikular na katangian ng materyal sa pagpapatunay na tinutukoy ng halaga ng at tinukoy sa idtypecontrollertype[5.2.1Materyal sa Pagpapatunay](https://www.w3.org/TR/did-core/#verification-material) . MAAARING may kasamang mga karagdagang property ang isang [paraan ng pag-verify .](https://www.w3.org/TR/did-core/" \l "dfn-verification-method)DAPAT nakarehistro ang mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) sa DID Specification Registries [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ].

**id**

Ang halaga ng [id](https://www.w3.org/TR/did-core/" \l "dfn-id)property para sa isang [paraan ng pag-verify ay](https://www.w3.org/TR/did-core/" \l "dfn-verification-method)DAPAT na isang [string](https://infra.spec.whatwg.org/#string) na sumusunod sa mga panuntunan sa Seksyon[3.2DID URL Syntax](https://www.w3.org/TR/did-core/#did-url-syntax) .

**uri**

Ang value ng typeproperty ay DAPAT na isang [string](https://infra.spec.whatwg.org/#string) na eksaktong tumutukoy sa isang uri ng [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) . Upang ma-maximize ang pandaigdigang interoperability, DAPAT na nakarehistro ang uri ng [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) sa DID Specification Registries [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ].

**controller**

Ang halaga ng controllerproperty ay DAPAT na isang [string](https://infra.spec.whatwg.org/#string) na sumusunod sa mga panuntunan sa[3.1DID Syntax](https://www.w3.org/TR/did-core/#did-syntax) .

[HALIMBAWA12](https://www.w3.org/TR/did-core/#example-example-verification-method-structure): Halimbawang istraktura ng paraan ng pag-verify

{

"@context": [

"https://www.w3.org/ns/did/v1",

"https://w3id.org/security/suites/jws-2020/v1"

"https://w3id.org/security/suites/ed25519-2020/v1"

]

"id": "did:example:123456789abcdefghi",

...

"verificationMethod": [{

"id": ...,

"type": ...,

"controller": ...,

"publicKeyJwk": ...

}, {

"id": ...,

"type": ...,

"controller": ...,

"publicKeyMultibase": ...

}]

}

TANDAAN : (mga) controller ng paraan ng pag-verify at (mga) DID controller

Ang semantics ng controllerproperty ay pareho kapag ang paksa ng relasyon ay ang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) at kapag ang paksa ng relasyon ay isang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) , gaya ng isang cryptographic na pampublikong key. Dahil hindi makokontrol ng isang key ang sarili nito, at hindi mahihinuha ang key controller mula sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) , kinakailangan na tahasang ipahayag ang pagkakakilanlan ng controller ng key. Ang pagkakaiba ay ang halaga ng controllerpara sa isang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ay *hindi* nangangahulugang isang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) . [Ang mga controller ng DID](https://www.w3.org/TR/did-core/#dfn-did-controllers) ay ipinahayag gamit ang [controller](https://www.w3.org/TR/did-core/" \l "dfn-controller)property sa pinakamataas na antas ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) (ang pinakamataas[mapa](https://infra.spec.whatwg.org/#ordered-map) sa [modelo ng data](https://www.w3.org/TR/did-core/" \l "data-model) ); tingnan mo[5.1.2DID Controller](https://www.w3.org/TR/did-core/#did-controller) .

#### 5.2.1Materyal ng Pagpapatunay

Ang materyal sa pag-verify ay anumang impormasyon na ginagamit ng isang proseso na naglalapat ng [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) . Ang paraan typeng pag- [verify](https://www.w3.org/TR/did-core/#dfn-verification-method) ay inaasahang gagamitin upang matukoy ang pagiging tugma nito sa mga naturang proseso. Ang mga halimbawa ng mga katangian ng materyal sa pagpapatunay ay [publicKeyJwk](https://www.w3.org/TR/did-core/" \l "dfn-publickeyjwk)o [publicKeyMultibase](https://www.w3.org/TR/did-core/" \l "dfn-publickeymultibase). Ang isang detalye ng [cryptographic suite](https://www.w3.org/TR/did-core/#dfn-cryptosuite) ay responsable para sa pagtukoy sa [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) type at sa nauugnay nitong materyal sa pag-verify. Halimbawa, tingnan ang [JSON Web Signature 2020](https://w3c-ccg.github.io/lds-jws2020/) at [Ed25519 Signature 2020](https://w3c-ccg.github.io/lds-ed25519-2020/) . Para sa lahat ng nakarehistrong uri ng [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) at nauugnay na materyal sa pag-verify na available para sa [mga DID](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers), pakitingnan ang DID Specification Registries [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ].

Upang mapataas ang posibilidad ng mga interoperable na pagpapatupad, nililimitahan ng detalyeng ito ang bilang ng mga format para sa pagpapahayag ng materyal sa pag-verify sa isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) . Ang mas kaunting mga format na kailangang ipatupad ng mga nagpapatupad, mas malamang na susuportahan nila ang lahat ng ito. Sinusubukan ng diskarteng ito na magkaroon ng maselan na balanse sa pagitan ng kadalian ng pagpapatupad at pagsuporta sa mga format na dati nang nagkaroon ng malawak na deployment. Dalawang sinusuportahang katangian ng materyal sa pag-verify ang nakalista sa ibaba:

**publicKeyJwk**

OPTIONAL ang publicKeyJwkproperty . Kung mayroon, ang value ay DAPAT na isang [mapa](https://infra.spec.whatwg.org/" \l "ordered-map) na kumakatawan sa isang JSON Web Key na tumutugma sa [ [RFC7517](https://www.w3.org/TR/did-core/#bib-rfc7517) ]. Ang [mapa](https://infra.spec.whatwg.org/" \l "ordered-map)ay HINDI DAPAT maglaman ng "d", o anumang iba pang miyembro ng klase ng pribadong impormasyon tulad ng inilarawan sa [Registration Template](https://tools.ietf.org/html/rfc7517#section-8.1.1) . Inirerekomenda na ang mga paraan ng pag-verify na gumagamit ng mga JWK [ [RFC7517](https://www.w3.org/TR/did-core/#bib-rfc7517) ] upang kumatawan sa kanilang mga pampublikong susi ay gumagamit ng halaga ng bilang kanilang [fragment identifier](https://www.w3.org/TR/did-core/#fragment) . Inirerekomenda na ang mga halaga ng JWK ay nakatakda sa pampublikong key fingerprint [ [RFC7638](https://www.w3.org/TR/did-core/#bib-rfc7638) ]. Tingnan ang unang key in kidkid[Halimbawa13](https://www.w3.org/TR/did-core/#example-various-verification-method-types)para sa isang halimbawa ng pampublikong key na may compound key identifier.

**publicKeyMultibase**

OPTIONAL ang publicKeyMultibaseproperty . Non-normative ang feature na ito. Kung mayroon, ang value ay DAPAT na isang [string](https://infra.spec.whatwg.org/#string) na representasyon ng isang [ [MULTIBASE](https://www.w3.org/TR/did-core/#bib-multibase) ] na naka-encode na pampublikong key.

Tandaan na ang detalye ng [ [MULTIBASE](https://www.w3.org/TR/did-core/#bib-multibase) ] ay hindi pa isang pamantayan at maaaring magbago. Maaaring may ilang mga kaso ng paggamit para sa format ng data na ito kung saan **public**KeyMultibasetinukoy, upang payagan ang pagpapahayag ng mga pampublikong key, ngunit **private**KeyMultibase hindi tinukoy, upang maprotektahan laban sa hindi sinasadyang pagtagas ng mga lihim na susi.

Ang isang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method)ay HINDI DAPAT maglaman ng maraming katangian ng materyal sa pag-verify para sa parehong materyal. Halimbawa, ipinagbabawal ang pagpapahayag ng pangunahing materyal sa isang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) gamit ang pareho publicKeyJwkat publicKeyMultibasesa parehong oras.

Ang isang halimbawa ng isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) na naglalaman ng mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) gamit ang parehong mga katangian sa itaas ay ipinapakita sa ibaba.

[HALIMBAWA13](https://www.w3.org/TR/did-core/#example-various-verification-method-types): Mga paraan ng pag-verify gamit ang publicKeyJwk at publicKeyMultibase

{

"@context": [

"https://www.w3.org/ns/did/v1",

"https://w3id.org/security/suites/jws-2020/v1",

"https://w3id.org/security/suites/ed25519-2020/v1"

]

"id": "did:example:123456789abcdefghi",

...

"paraan ng pagpapatunay": [{

"id": "did:example:123#\_Qq0UL2Fq651Q0Fjd6TvnYE-faHiOpRlPVQcY\_-tA4A",

"type": "JsonWebKey2020", // panlabas (property value)

"controller": "did:example:123",

"publicKeyJwk": {

"crv": "Ed25519", // panlabas (pangalan ng ari-arian)

"x": "VCpo2LMLhn6iWku8MKvSLg2ZAoC-nlOyPVQaO3FxVeQ", // panlabas (pangalan ng ari-arian)

"kty": "OKP", // panlabas (pangalan ng ari-arian)

"bata" : "\_Qq0UL2Fq651Q0Fjd6TvnYE-faHiOpRlPVQcY\_-tA4A" // panlabas (pangalan ng ari-arian)

}

}, {

"id": "did:example:123456789abcdefghi#keys-1",

"type": "Ed25519VerificationKey2020", // panlabas (property value)

"controller": "did:example:pqrstuvwxyz0987654321",

"publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"

}],

...

}

#### 5.2.2Pagtukoy sa Mga Paraan ng Pagpapatunay

[Maaaring i-embed o i-reference ang mga paraan ng pag-verify](https://www.w3.org/TR/did-core/#dfn-verification-method) mula sa mga property na nauugnay sa iba't ibang [ugnayan sa pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship) gaya ng inilalarawan sa[5.3Mga Relasyon sa Pagpapatunay](https://www.w3.org/TR/did-core/#verification-relationships) . Ang pagre -refer sa [mga paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ay nagbibigay-daan sa mga ito na magamit ng higit sa isang [ugnayan sa pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship) .

Kung ang halaga ng isang property ng [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ay isang [mapa](https://infra.spec.whatwg.org/" \l "ordered-map) , ang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ay na-embed at ang mga katangian nito ay maaaring direktang ma-access. Gayunpaman, kung ang halaga ay isang [string](https://infra.spec.whatwg.org/#string) ng URL , ang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ay isinama sa pamamagitan ng sanggunian at ang mga katangian nito ay kailangang makuha mula sa ibang lugar sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) o mula sa isa pang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) . Ginagawa ito sa pamamagitan ng pag-dereference sa URL at paghahanap sa nagreresultang [mapagkukunan](https://www.w3.org/TR/did-core/" \l "dfn-resources) para sa isang [mapa ng](https://infra.spec.whatwg.org/" \l "ordered-map)[paraan ng pag-verify](https://www.w3.org/TR/did-core/#dfn-verification-method) na may property na ang halaga ay tumutugma sa URL. id

[HALIMBAWA14](https://www.w3.org/TR/did-core/#example-embedding-and-referencing-verification-methods): Pag-embed at pagtukoy ng mga paraan ng pag-verify

{

...

"authentication": [

// ang key na ito ay isinangguni at maaaring gamitin ng

// higit sa isang ugnayan sa pag-verify

"did:example:123456789abcdefghi#keys-1",

// ang key na ito ay naka-embed at maaaring \*lamang\* gamitin para sa authentication

{

"id": "did:example:123456789abcdefghi#keys-2",

"type": "Ed25519VerificationKey2020", // panlabas (property value)

"controller": "did:example:123456789abcdefghi",

"publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"

}

],

...

}

### **5.3Mga Relasyon sa Pagpapatunay**

Ang isang ugnayan sa pag- [verify](https://www.w3.org/TR/did-core/#dfn-verification-relationship) ay nagpapahayag ng kaugnayan sa pagitan ng [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) at isang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) .

Ang magkakaibang mga [ugnayan sa pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship) ay nagbibigay -daan sa mga nauugnay na [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) na magamit para sa iba't ibang layunin. Nasa isang verifier na tiyakin ang bisa ng isang pagsubok sa pag-verify sa pamamagitan ng pagsuri na ang ginamit na [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ay nasa naaangkop na pag- aari ng [kaugnayan sa pag-verify ng](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship)[DID Document](https://www.w3.org/TR/did-core/#dfn-did-documents) .

Ang [ugnayan sa pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship) sa pagitan ng [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) at ng [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ay tahasan sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) . [Ang mga paraan ng pag-verify](https://www.w3.org/TR/did-core/#dfn-verification-method) na hindi nauugnay sa isang partikular na [kaugnayan sa pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship) ay hindi maaaring gamitin para sa [kaugnayan sa pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship) na iyon . Halimbawa, ang isang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) sa halaga ng [authentication](https://www.w3.org/TR/did-core/" \l "dfn-authentication)property ay hindi maaaring gamitin para makipag-ugnayan sa mga pangunahing protocol ng kasunduan sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) —ang halaga ng [keyAgreement](https://www.w3.org/TR/did-core/" \l "dfn-keyagreement)property ay kailangang gamitin para doon.

Ang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay hindi nagpapahayag ng mga binawi na susi gamit ang isang [kaugnayan sa pagpapatunay](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship) . Kung ang isang isinangguni na paraan ng pag-verify ay wala sa pinakabagong [DID na Dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) na ginamit upang i-dereference ito, ang paraan ng pag-verify ay ituring na hindi wasto o binawi. Ang bawat detalye [ng pamamaraan ng DID](https://www.w3.org/TR/did-core/#dfn-did-methods) ay inaasahang magdetalye kung paano isinasagawa at sinusubaybayan ang pagbawi.

Tinutukoy ng mga sumusunod na seksyon ang ilang kapaki-pakinabang [na ugnayan sa pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship) . MAAARING kasama sa isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ang alinman sa mga ito, o iba pang mga pag-aari, upang ipahayag ang isang partikular na [kaugnayan sa pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship) . Upang ma-maximize ang pandaigdigang interoperability, DAPAT na nakarehistro ang anumang naturang property na ginamit sa DID Specification Registries [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ].

#### 5.3.1Pagpapatunay

Ginagamit ang authentication [kaugnayan sa pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship) upang tukuyin kung paano inaasahang maa- [authenticate ang](https://www.w3.org/TR/did-core/#dfn-authenticated)[paksa ng DID](https://www.w3.org/TR/did-core/#dfn-did-subjects) , para sa mga layunin tulad ng pag-log in sa isang website o pagsali sa anumang uri ng protocol sa pagtugon sa hamon.

**pagpapatunay**

OPTIONAL ang authenticationproperty . Kung mayroon, ang nauugnay na halaga ay DAPAT na isang [hanay](https://infra.spec.whatwg.org/" \l "ordered-set) ng isa o higit pang mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) . Ang bawat [paraan ng pag-verify ay](https://www.w3.org/TR/did-core/" \l "dfn-verification-method)MAAARING naka -embed o sumangguni.

[HALIMBAWA15](https://www.w3.org/TR/did-core/#example-authentication-property-containing-three-verification-methods): Pag-aari ng pagpapatunay na naglalaman ng tatlong paraan ng pag-verify

{

"@context": [

"https://www.w3.org/ns/did/v1",

"https://w3id.org/security/suites/ed25519-2020/v1"

],

"id": "did:example:123456789abcdefghi",

...

"authentication": [

// ang pamamaraang ito ay maaaring gamitin upang patotohanan tulad ng ginawa:...fghi

"did:example:123456789abcdefghi#keys-1",

// ang pamamaraang ito ay \*lamang\* na inaprubahan para sa pagpapatunay, maaaring hindi ito

// gamitin para sa anumang iba pang layunin ng patunay, kaya ang buong paglalarawan nito ay

// naka-embed dito sa halip na gumamit lamang ng isang sanggunian

{

"id": "did:example:123456789abcdefghi#keys-2",

"type": "Ed25519VerificationKey2020",

"controller": "did:example:123456789abcdefghi",

"publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"

}

],

...

}

Kung naitatag ang pagpapatunay, nasa [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) o iba pang aplikasyon ang pagpapasya kung ano ang gagawin sa impormasyong iyon. Ang isang partikular na [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ay maaaring magpasya na ang pagpapatotoo bilang isang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) ay sapat upang, halimbawa, i-update o tanggalin ang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) . Ang isa [pang paraan ng DID](https://www.w3.org/TR/did-core/#dfn-did-methods) ay maaaring mangailangan ng iba't ibang mga susi, o ganap na ibang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) , na iharap upang i-update o tanggalin ang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) kaysa sa ginamit sa [pagpapatunay](https://www.w3.org/TR/did-core/" \l "dfn-authenticated) . Sa madaling salita, ang ginagawa pagkatapos ng pagsusuri sa pagpapatunay ay wala sa saklaw para sa [modelo ng data](https://www.w3.org/TR/did-core/" \l "data-model) ; [Mga pamamaraan ng DID](https://www.w3.org/TR/did-core/#dfn-did-methods)at ang mga aplikasyon ay inaasahang tutukuyin ito mismo.

Ito ay kapaki-pakinabang sa anumang verifier ng pagpapatotoo na kailangang suriin upang makita kung ang isang entity na sumusubok na [magpatotoo](https://www.w3.org/TR/did-core/" \l "dfn-authenticated) ay, sa katunayan, ay nagpapakita ng wastong patunay ng pagpapatunay. Kapag ang isang verifier ay nakatanggap ng ilang data (sa ilang format na partikular sa protocol) na naglalaman ng isang patunay na ginawa para sa layunin ng "pagpapatotoo", at nagsasabing ang isang entity ay kinilala ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) , pagkatapos ay ang verifier na iyon ay nagsusuri upang matiyak na ang patunay maaaring ma-verify gamit ang [paraan](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ng pag-verify (hal., public key) na nakalista sa ilalim [authentication](https://www.w3.org/TR/did-core/" \l "dfn-authentication)ng [DID Document](https://www.w3.org/TR/did-core/#dfn-did-documents) .

Tandaan na ang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) na ipinahiwatig ng pag- [authentication](https://www.w3.org/TR/did-core/" \l "dfn-authentication)aari ng isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay magagamit lamang upang [patotohanan](https://www.w3.org/TR/did-core/" \l "dfn-authenticated) ang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) . Upang [patotohanan](https://www.w3.org/TR/did-core/" \l "dfn-authenticated) ang ibang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) , ang entity na nauugnay sa halaga ng controller, gaya ng tinukoy sa[5.1.2Ang DID Controller](https://www.w3.org/TR/did-core/#did-controller) , ay kailangang [magpatotoo](https://www.w3.org/TR/did-core/" \l "dfn-authenticated) gamit ang sarili nitong [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) at nauugnay na kaugnayan sa [authentication](https://www.w3.org/TR/did-core/#dfn-authentication) [pagpapatunay](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship) .

#### 5.3.2Paninindigan

Ginagamit ang assertionMethod [kaugnayan sa pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship) upang tukuyin kung paano inaasahang ipahayag ng [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ang mga claim, tulad ng para sa mga layunin ng pag-isyu ng isang Nabe-verify na Kredensyal [ [VC-DATA-MODEL](https://www.w3.org/TR/did-core/#bib-vc-data-model) ].

**assertionParaan**

OPTIONAL ang assertionMethodproperty . Kung mayroon, ang nauugnay na halaga ay DAPAT na isang [hanay](https://infra.spec.whatwg.org/" \l "ordered-set) ng isa o higit pang mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) . Ang bawat [paraan ng pag-verify ay](https://www.w3.org/TR/did-core/" \l "dfn-verification-method)MAAARING naka -embed o sumangguni.

Kapaki-pakinabang ang property na ito, halimbawa, sa panahon ng pagproseso ng isang [nabe-verify na kredensyal](https://www.w3.org/TR/did-core/#dfn-verifiable-credentials) ng isang verifier. Sa panahon ng pag-verify, ang isang verifier ay nagsusuri upang makita kung ang isang [nabe-verify na kredensyal](https://www.w3.org/TR/did-core/#dfn-verifiable-credentials) ay naglalaman ng isang patunay na ginawa ng [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) sa pamamagitan ng pagsuri na ang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) na ginamit upang igiit ang patunay ay nauugnay sa [assertionMethod](https://www.w3.org/TR/did-core/" \l "dfn-assertionmethod)property sa kaukulang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) .

[HALIMBAWA16](https://www.w3.org/TR/did-core/#example-assertion-method-property-containing-two-verification-methods): Pag-aari ng paraan ng assertion na naglalaman ng dalawang paraan ng pag-verify

{

"@context": [

"https://www.w3.org/ns/did/v1",

"https://w3id.org/security/suites/ed25519-2020/v1"

],

"id": "did:example:123456789abcdefghi",

...

"AssertionMethod": [

// ang pamamaraang ito ay maaaring gamitin upang igiit ang mga pahayag gaya ng ginawa:...fghi

"did:example:123456789abcdefghi#keys-1",

// ang paraang ito ay \*lamang\* na inaprubahan para sa paggigiit ng mga pahayag, hindi ito

// ginagamit para sa anumang iba pang kaugnayan sa pag-verify, kaya ang buong paglalarawan nito ay

// naka-embed dito sa halip na gumamit ng reference

{

"id": "did:example:123456789abcdefghi#keys-2",

"type": "Ed25519VerificationKey2020", // panlabas (property value)

"controller": "did:example:123456789abcdefghi",

"publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"

}

],

...

#### 5.3.3Pangunahing Kasunduan

Ginagamit ang keyAgreement [kaugnayan sa pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship) upang tukuyin kung paano makakabuo ang isang entity ng materyal sa pag-encrypt upang maihatid ang kumpidensyal na impormasyong nilalayon para sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) , tulad ng para sa mga layunin ng pagtatatag ng isang secure na channel ng komunikasyon sa tatanggap.

**keyAgreement**

OPTIONAL ang keyAgreementproperty . Kung mayroon, ang nauugnay na halaga ay DAPAT na isang [hanay](https://infra.spec.whatwg.org/" \l "ordered-set) ng isa o higit pang mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) . Ang bawat [paraan ng pag-verify ay](https://www.w3.org/TR/did-core/" \l "dfn-verification-method)MAAARING naka -embed o sumangguni.

Ang isang halimbawa kung kailan kapaki-pakinabang ang property na ito ay kapag nag-e-encrypt ng mensaheng nilayon para sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) . Sa kasong ito, ginagamit ng counterparty ang cryptographic public key na impormasyon sa [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) para i-wrap ang isang decryption key para sa tatanggap.

[HALIMBAWA17](https://www.w3.org/TR/did-core/#example-key-agreement-property-containing-two-verification-methods): Pag-aari ng pangunahing kasunduan na naglalaman ng dalawang paraan ng pag-verify

{

"@context": "https://www.w3.org/ns/did/v1",

"id": "did:example:123456789abcdefghi",

...

"keyAgreement": [

// ang pamamaraang ito ay maaaring gamitin upang maisagawa ang pangunahing kasunduan gaya ng ginawa:...fghi

"did:example:123456789abcdefghi#keys-1",

// ang pamamaraang ito ay \*lamang\* na inaprubahan para sa paggamit ng pangunahing kasunduan, hindi ito

// gagamitin para sa anumang iba pang kaugnayan sa pag-verify, kaya ang buong paglalarawan nito ay

// naka-embed dito sa halip na gumamit lamang ng reference

{

"id": "did:example:123#zC9ByQ8aJs8vrNXyDhPHHHNNMSHPcaSgNpjjsBYpMMjsTdS",

"type": "X25519KeyAgreementKey2019", // panlabas (property value)

"controller": "did:example:123",

"publicKeyMultibase": "z9hFgmPVfmBZwRvFEyniQDBkz9LmV7gDEqytWyGZLmDXE"

}

],

...

}

#### 5.3.4Panawagan sa Kakayahang

Ang capabilityInvocation [kaugnayan sa pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship) ay ginagamit upang tumukoy ng [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) na maaaring gamitin ng [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) upang mag-invoke ng kakayahan sa cryptographic, gaya ng pahintulot na i-update ang [DID Document](https://www.w3.org/TR/did-core/#dfn-did-documents) .

**kakayahanInvocation**

OPTIONAL ang capabilityInvocationproperty . Kung mayroon, ang nauugnay na halaga ay DAPAT na isang [hanay](https://infra.spec.whatwg.org/" \l "ordered-set) ng isa o higit pang mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) . Ang bawat [paraan ng pag-verify ay](https://www.w3.org/TR/did-core/" \l "dfn-verification-method)MAAARING naka -embed o sumangguni.

Ang isang halimbawa kung kailan kapaki-pakinabang ang property na ito ay kapag ang isang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ay kailangang mag-access ng isang protektadong HTTP API na nangangailangan ng pahintulot upang magamit ito. Upang makapagbigay ng pahintulot kapag ginagamit ang HTTP API, ang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ay gumagamit ng kakayahan na nauugnay sa isang partikular na URL na nakalantad sa pamamagitan ng HTTP API. Ang invocation ng kakayahan ay maaaring ipahayag sa maraming paraan, hal, bilang isang digitally signed message na inilalagay sa HTTP Header.

Ang server na nagbibigay ng HTTP API ay ang verifier ng kakayahan at kakailanganin nitong i-verify na ang [paraan](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ng pag-verify na tinutukoy ng na-invoke na kakayahan ay umiiral sa pag- [capabilityInvocation](https://www.w3.org/TR/did-core/" \l "dfn-capabilityinvocation) aari ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) . Susuriin din ng verifier upang matiyak na wasto ang pagkilos na ginagawa at naaangkop ang kakayahan para sa mapagkukunang ina-access. Kung matagumpay ang pag-verify, natukoy ng server sa cryptographically na awtorisado ang invoker na i-access ang protektadong mapagkukunan.

[HALIMBAWA18](https://www.w3.org/TR/did-core/#example-capability-invocation-property-containing-two-verification-methods): Capability invocation property na naglalaman ng dalawang paraan ng pag-verify

{

"@context": [

"https://www.w3.org/ns/did/v1",

"https://w3id.org/security/suites/ed25519-2020/v1"

],

"id": "did:example:123456789abcdefghi",

...

"capabilityInvocation": [

// ang pamamaraang ito ay maaaring gamitin upang mag-invoke ng mga kakayahan tulad ng ginawa:...fghi

"did:example:123456789abcdefghi#keys-1",

// ang pamamaraang ito ay \*lamang\* na inaprubahan para sa paggamit ng capability invocation, hindi ito

// gagamitin para sa anumang iba pang kaugnayan sa pag-verify, kaya ang buong paglalarawan nito ay

// naka-embed dito sa halip na gumamit lang ng reference

{

"id": "did:example:123456789abcdefghi#keys-2",

"type": "Ed25519VerificationKey2020", // panlabas (property value)

"controller": "did:example:123456789abcdefghi",

"publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"

}

],

...

}

#### 5.3.5Delegasyon ng Kakayahan

Ang capabilityDelegation [kaugnayan sa pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship) ay ginagamit upang tukuyin ang isang mekanismo na maaaring gamitin ng [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) upang italaga ang isang cryptographic na kakayahan sa isa pang partido, tulad ng pagtatalaga ng awtoridad upang ma-access ang isang partikular na HTTP API sa isang subordinate.

**kakayahanPagdelegasyon**

OPTIONAL ang capabilityDelegationproperty . Kung mayroon, ang nauugnay na halaga ay DAPAT na isang [hanay](https://infra.spec.whatwg.org/" \l "ordered-set) ng isa o higit pang mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) . Ang bawat [paraan ng pag-verify ay](https://www.w3.org/TR/did-core/" \l "dfn-verification-method)MAAARING naka -embed o sumangguni.

Ang isang halimbawa kung kailan kapaki-pakinabang ang property na ito ay kapag pinili ng isang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) na italaga ang kanilang kakayahang mag-access ng isang protektadong HTTP API sa isang partido maliban sa kanilang sarili. Upang maitalaga ang kakayahan, gagamit ang [paksa ng DID ng](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects)[paraan ng pag-verify](https://www.w3.org/TR/did-core/#dfn-verification-method) na nauugnay sa kaugnayan sa pag- capabilityDelegation [verify](https://www.w3.org/TR/did-core/#dfn-verification-relationship) upang pirmahan nang cryptographic ang kakayahan sa isa pang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) . Gagamitin ng delegado ang kakayahan sa paraang katulad ng halimbawang inilarawan sa[5.3.4Panawagan sa Kakayahang](https://www.w3.org/TR/did-core/#capability-invocation) .

[HALIMBAWA19](https://www.w3.org/TR/did-core/#example-capability-delegation-property-containing-two-verification-methods): Capability Delegation property na naglalaman ng dalawang paraan ng pag-verify

{

"@context": [

"https://www.w3.org/ns/did/v1",

"https://w3id.org/security/suites/ed25519-2020/v1"

],

"id": "did:example:123456789abcdefghi",

...

"capabilityDelegation": [

// ang pamamaraang ito ay maaaring gamitin upang maisagawa ang pagtatalaga ng kakayahan tulad ng ginawa:...fghi

"did:example:123456789abcdefghi#keys-1",

// ang paraang ito ay \*lamang\* naaprubahan para sa pagbibigay ng mga kakayahan; hindi ito

// gagamitin para sa anumang iba pang kaugnayan sa pag-verify, kaya ang buong paglalarawan nito ay

// naka-embed dito sa halip na gumamit lang ng reference

{

"id": "did:example:123456789abcdefghi#keys-2",

"type": "Ed25519VerificationKey2020", // panlabas (property value)

"controller": "did:example:123456789abcdefghi",

"publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"

}

],

...

}

### **5.4Mga serbisyo**

Ginagamit ang mga [serbisyo sa mga](https://www.w3.org/TR/did-core/" \l "dfn-service)[dokumento ng DID](https://www.w3.org/TR/did-core/#dfn-did-documents) upang ipahayag ang mga paraan ng pakikipag-usap sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) o mga nauugnay na entity. Ang isang [serbisyo](https://www.w3.org/TR/did-core/" \l "dfn-service) ay maaaring maging anumang uri ng serbisyo na gustong i-advertise ng [paksa ng DID , kabilang ang mga](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects)[desentralisadong](https://www.w3.org/TR/did-core/#dfn-decentralized-identity-management) serbisyo sa pamamahala ng pagkakakilanlan para sa karagdagang pagtuklas, pagpapatunay, awtorisasyon, o pakikipag-ugnayan.

Dahil sa mga alalahanin sa privacy, ang pagbubunyag ng pampublikong impormasyon sa pamamagitan ng mga [serbisyo](https://www.w3.org/TR/did-core/" \l "dfn-service) , tulad ng mga social media account, personal na website, at email address, ay hindi hinihikayat. Ang karagdagang pag-explore ng mga alalahanin sa privacy ay matatagpuan sa[10.1Panatilihing Pribado ang Personal na Data](https://www.w3.org/TR/did-core/#keep-personal-data-private) at[10.6Privacy ng Serbisyo](https://www.w3.org/TR/did-core/#service-privacy) . Ang impormasyong nauugnay sa mga [serbisyo](https://www.w3.org/TR/did-core/" \l "dfn-service) ay kadalasang partikular sa serbisyo. Halimbawa, ang impormasyong nauugnay sa isang naka-encrypt na serbisyo sa pagmemensahe ay maaaring magpahayag kung paano simulan ang naka-encrypt na link bago magsimula ang pagmemensahe.

[Ang mga serbisyo](https://www.w3.org/TR/did-core/#dfn-service) ay ipinahayag gamit ang [service](https://www.w3.org/TR/did-core/" \l "dfn-service)property, na inilalarawan sa ibaba:

**serbisyo**

*OPTIONAL* ang serviceproperty . Kung mayroon, ang nauugnay na halaga ay *DAPAT* na isang [hanay](https://infra.spec.whatwg.org/" \l "ordered-set) ng mga [serbisyo](https://www.w3.org/TR/did-core/" \l "dfn-service) , kung saan ang bawat serbisyo ay inilalarawan ng isang [mapa](https://infra.spec.whatwg.org/" \l "ordered-map) . Ang bawat [mapa ng](https://infra.spec.whatwg.org/" \l "ordered-map)[serbisyo ay](https://www.w3.org/TR/did-core/#dfn-service)*DAPAT* maglaman ng , , at mga katangian. Ang bawat extension ng serbisyo *ay MAAARING* magsama ng mga karagdagang property at *MAY* higit pang paghigpitan ang mga property na nauugnay sa extension. [id](https://www.w3.org/TR/did-core/" \l "dfn-id)type[serviceEndpoint](https://www.w3.org/TR/did-core/#dfn-serviceendpoint)

**id**

Ang halaga ng idproperty ay *DAPAT* na isang [URI](https://www.w3.org/TR/did-core/#dfn-uri) na tumutugma sa [ [RFC3986](https://www.w3.org/TR/did-core/#bib-rfc3986) ]. HINDI [DAPAT](https://www.w3.org/TR/did-core/#dfn-conforming-producer)*gumawa* ng maramihang servicemga entry na may parehong id. *DAPAT* gumawa ng error ang isang [sumusunod na mamimili](https://www.w3.org/TR/did-core/" \l "dfn-conforming-consumer) kung makakita ito ng maramihang mga entry na may parehong . serviceid

**uri**

Ang value ng typeproperty ay *DAPAT* na isang [string](https://infra.spec.whatwg.org/#string) o isang [set](https://infra.spec.whatwg.org/#ordered-set) ng mga [string](https://infra.spec.whatwg.org/#string) . Upang ma-maximize ang interoperability, ang uri ng [serbisyo](https://www.w3.org/TR/did-core/" \l "dfn-service) at ang mga nauugnay na katangian nito ay *DAPAT* na nakarehistro sa DID Specification Registries [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ].

***serviceEndpoint***

Ang halaga ng serviceEndpointproperty ay *DAPAT* na isang [string](https://infra.spec.whatwg.org/#string) , isang [mapa](https://infra.spec.whatwg.org/" \l "string) , o isang [set](https://infra.spec.whatwg.org/#ordered-set) na binubuo ng isa o higit pang mga [string](https://infra.spec.whatwg.org/#string) at/o mga [mapa](https://infra.spec.whatwg.org/" \l "string) . Ang lahat ng mga [string](https://infra.spec.whatwg.org/#string) value ay *DAPAT* na wastong mga [URI](https://www.w3.org/TR/did-core/#dfn-uri) na tumutugma sa [ [RFC3986](https://www.w3.org/TR/did-core/#bib-rfc3986) ] at na-normalize ayon sa mga [panuntunan sa Normalization at Comparison sa RFC3986](https://www.rfc-editor.org/rfc/rfc3986" \l "section-6) at sa anumang mga panuntunan sa normalization sa naaangkop nitong [URI](https://www.w3.org/TR/did-core/#dfn-uri) scheme specification.

Para sa higit pang impormasyon tungkol sa privacy at mga pagsasaalang-alang sa seguridad na may kaugnayan sa [mga serbisyo](https://www.w3.org/TR/did-core/" \l "dfn-service) tingnan[10.6Privacy ng Serbisyo](https://www.w3.org/TR/did-core/#service-privacy) ,[10.1Panatilihing Pribado ang Personal na Data](https://www.w3.org/TR/did-core/#keep-personal-data-private) ,[10.3DID Document Correlation Risks](https://www.w3.org/TR/did-core/#did-document-correlation-risks) , at[9.3Mga Endpoint ng Serbisyo sa Pagpapatunay](https://www.w3.org/TR/did-core/#authentication-service-endpoints) .

[HALIMBAWA20](https://www.w3.org/TR/did-core/#example-usage-of-the-service-property): Paggamit ng service property

{

"serbisyo": [{

"id":"did:example:123#linked-domain",

"type": "LinkedDomains", // panlabas (property value)

"serviceEndpoint": "https://bar.example.com"

}]

}

6.Mga representasyon

Ang isang konkretong serialization ng isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) sa detalyeng ito ay tinatawag na [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) . Ang isang [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) ay nilikha sa pamamagitan ng pagse-serialize ng [modelo ng data](https://www.w3.org/TR/did-core/" \l "data-model) sa pamamagitan ng isang proseso na tinatawag na **produksyon** . Ang isang [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) ay binago sa [modelo ng data](https://www.w3.org/TR/did-core/" \l "data-model) sa pamamagitan ng isang proseso na tinatawag na **pagkonsumo** . Ang mga proseso ng produksyon at pagkonsumo ay nagbibigay-daan sa pag-convert ng impormasyon mula sa isang [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) patungo sa isa pa. Tinutukoy ng detalyeng ito ang mga [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) para sa JSON at JSON-LD, at maaaring gumamit ang mga developer ng anumang iba pang [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations), tulad ng XML o YAML, na may kakayahang ipahayag ang [modelo ng data](https://www.w3.org/TR/did-core/" \l "data-model) . Tinutukoy ng mga sumusunod na seksyon ang mga pangkalahatang tuntunin para sa [produksyon](https://www.w3.org/TR/did-core/" \l "dfn-production) at [pagkonsumo](https://www.w3.org/TR/did-core/" \l "dfn-consumption) , pati na rin ang mga [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) ng JSON at JSON-LD .

### **6.1Produksyon at Pagkonsumo**

Bilang karagdagan sa mga [representasyong](https://www.w3.org/TR/did-core/" \l "dfn-representations) tinukoy sa ispesipikasyong ito, maaaring gumamit ang mga tagapagpatupad ng iba pang mga [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) , kung ang bawat naturang [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) ay wastong tinukoy (kabilang ang mga panuntunan para sa interoperable na pangangasiwa ng mga ari-arian na hindi nakalista sa DID Specification Registries [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ]). Tingnan mo[4.1Extensibility](https://www.w3.org/TR/did-core/#extensibility) para sa karagdagang impormasyon.

Ang mga kinakailangan para sa lahat ng mga [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) ay ang mga sumusunod:

1. DAPAT tukuyin ng isang representasyon ang tiyak na mga panuntunan sa produksyon at pagkonsumo para sa lahat ng uri ng data na tinukoy [sa](https://www.w3.org/TR/did-core/" \l "dfn-representations) [4.Modelo ng Data](https://www.w3.org/TR/did-core/#data-model) .
2. DAPAT na natatanging nauugnay ang isang representasyon sa isang Uri ng Media na nakarehistro sa IANA [.](https://www.w3.org/TR/did-core/#dfn-representations)
3. DAPAT tukuyin ng isang [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) ang mga panuntunan sa pagpoproseso ng fragment para sa Uri ng Media nito na naaayon sa mga panuntunan sa pagproseso ng fragment na tinukoy sa [Fragment](https://www.w3.org/TR/did-core/#fragment) .
4. DAPAT gamitin ng isang [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) ang lexical na representasyon ng mga uri ng data ng [data model](https://www.w3.org/TR/did-core/#data-model) . Halimbawa, ginagamit ng JSON at JSON-LD ang XML Schema lexical serialization upang kumatawan sa mga [datetime](https://www.w3.org/TR/did-core/#dfn-datetime) . MAAARING piliin ng isang representasyon na i-serialize ang mga uri [ng data ng](https://www.w3.org/TR/did-core/#dfn-representations)[data model](https://www.w3.org/TR/did-core/#data-model) gamit ang ibang lexical na serialization hangga't ang proseso ng [pagkonsumo](https://www.w3.org/TR/did-core/" \l "dfn-consumption) pabalik sa [data model](https://www.w3.org/TR/did-core/#data-model) ay walang pagkawala. Halimbawa, ang ilang representasyong batay sa CBOR ay [nagpapahayag](https://www.w3.org/TR/did-core/" \l "dfn-representations) ng mga halaga ng [datetime](https://www.w3.org/TR/did-core/#dfn-datetime) gamit ang mga integer upang kumatawan sa bilang ng mga segundo mula noong panahon ng Unix. dateTime
5. MAAARING tukuyin ng isang [representasyon ang mga](https://www.w3.org/TR/did-core/" \l "dfn-representations)[entry](https://www.w3.org/TR/did-core/#dfn-representation-specific-entry) na partikular sa representasyon na naka-imbak sa isang [mapa ng mga](https://infra.spec.whatwg.org/" \l "maps)[entry na partikular sa representasyon](https://www.w3.org/TR/did-core/#dfn-representation-specific-entry) para gamitin sa proseso ng [produksyon](https://www.w3.org/TR/did-core/" \l "dfn-production) at [pagkonsumo](https://www.w3.org/TR/did-core/" \l "dfn-consumption) . Ang mga entry na ito ay ginagamit kapag kumonsumo o gumagawa upang tumulong sa pagtiyak ng walang pagkawalang conversion.
6. Upang ma-maximize ang interoperability, DAPAT irehistro ng mga may- akda ng detalye ng [representasyon ang kanilang](https://www.w3.org/TR/did-core/" \l "dfn-representations)[representasyon](https://www.w3.org/TR/did-core/#dfn-representations) sa DID Specification Registries [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ].

Ang mga kinakailangan para sa lahat ng [umaayon sa mga producer](https://www.w3.org/TR/did-core/" \l "dfn-conforming-producer) ay ang mga sumusunod:

1. DAPAT kumuha ng [modelo ng data ng](https://www.w3.org/TR/did-core/" \l "data-model)[dokumento ng DID](https://www.w3.org/TR/did-core/#dfn-did-documents) at isang [mapa ng mga](https://infra.spec.whatwg.org/" \l "maps)[entry na partikular sa representasyon](https://www.w3.org/TR/did-core/#dfn-representation-specific-entry) ang isang [producer](https://www.w3.org/TR/did-core/#dfn-conforming-producer) bilang input sa proseso ng [produksyon](https://www.w3.org/TR/did-core/" \l "dfn-production) . MAAARING tumanggap ng mga karagdagang opsyon ang [umaayon sa producer](https://www.w3.org/TR/did-core/" \l "dfn-conforming-producer) bilang input sa proseso ng [produksyon](https://www.w3.org/TR/did-core/" \l "dfn-production) .
2. DAPAT i-serialize ng isang naaayon na producer ang lahat ng mga entry sa modelo ng data ng dokumento ng DID [,](https://www.w3.org/TR/did-core/#dfn-conforming-producer)[at](https://www.w3.org/TR/did-core/#data-model)[ang](https://www.w3.org/TR/did-core/#dfn-did-documents) mapa ng mga [entry](https://infra.spec.whatwg.org/#maps)[na partikular sa representasyon](https://www.w3.org/TR/did-core/#dfn-representation-specific-entry) , na walang tahasang mga panuntunan sa pagproseso para sa [representasyong](https://www.w3.org/TR/did-core/" \l "dfn-representations) ginagawa gamit lamang ang mga panuntunan sa pagpoproseso ng uri ng data ng [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) at ibalik ang serialization pagkatapos ng natapos ang proseso ng [produksyon](https://www.w3.org/TR/did-core/" \l "dfn-production) .
3. DAPAT ibalik ng isang [tumutugmang producer](https://www.w3.org/TR/did-core/" \l "dfn-conforming-producer) ang Media Type [string](https://infra.spec.whatwg.org/#string) na nauugnay sa [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) pagkatapos makumpleto ang proseso ng [produksyon](https://www.w3.org/TR/did-core/" \l "dfn-production) .
4. HINDI DAPAT gumawa ng mga hindi sumusunod [na DID](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers) o [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) ang isang tumutugon na producer .

Ang mga kinakailangan para sa lahat ng [umaayon sa mga mamimili](https://www.w3.org/TR/did-core/" \l "dfn-conforming-consumer) ay ang mga sumusunod:

1. DAPAT kumuha ng [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) at Media Type [string](https://infra.spec.whatwg.org/#string) bilang input ang isang [conforming consumer sa proseso ng](https://www.w3.org/TR/did-core/#dfn-conforming-consumer)[pagkonsumo](https://www.w3.org/TR/did-core/#dfn-consumption) . MAAARING tumanggap ng mga karagdagang opsyon ang isang [sumusunod na mamimili](https://www.w3.org/TR/did-core/" \l "dfn-conforming-consumer) bilang input sa proseso ng [pagkonsumo](https://www.w3.org/TR/did-core/" \l "dfn-consumption) .
2. DAPAT tukuyin ng isang sumusunod na consumer ang representasyon [ng](https://www.w3.org/TR/did-core/#dfn-conforming-consumer)[isang](https://www.w3.org/TR/did-core/#dfn-representations) DID na [dokumento](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) gamit ang Media Type input [string](https://infra.spec.whatwg.org/#string) .
3. DAPAT tuklasin ng isang sumusunod na consumer ang anumang entry [na](https://www.w3.org/TR/did-core/" \l "dfn-conforming-consumer)[partikular](https://www.w3.org/TR/did-core/#dfn-representation-specific-entry) sa representasyon sa lahat ng kilalang [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) at ilagay ang entry sa isang [mapa ng mga](https://infra.spec.whatwg.org/" \l "maps)[entry na partikular sa representasyon](https://www.w3.org/TR/did-core/#dfn-representation-specific-entry) na ibinalik pagkatapos makumpleto ang proseso ng [pagkonsumo](https://www.w3.org/TR/did-core/" \l "dfn-consumption) . Ang isang listahan ng lahat ng kilalang mga [entry na tukoy sa representasyon](https://www.w3.org/TR/did-core/#dfn-representation-specific-entry) ay makukuha sa DID Specification Registries [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ].
4. DAPAT idagdag ng isang sumusunod na consumer ang lahat ng [mga](https://www.w3.org/TR/did-core/" \l "dfn-conforming-consumer)[entry](https://www.w3.org/TR/did-core/#dfn-representation-specific-entry) na hindi partikular sa representasyon na walang tahasang mga panuntunan sa pagproseso para sa [representasyong](https://www.w3.org/TR/did-core/" \l "dfn-representations) ginagamit sa [modelo ng data ng](https://www.w3.org/TR/did-core/" \l "data-model)[dokumento ng DID](https://www.w3.org/TR/did-core/#dfn-did-documents) gamit lamang ang mga panuntunan sa pagproseso ng uri ng data ng [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) at ibalik ang modelo ng data ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) pagkatapos ng [pagkonsumo](https://www.w3.org/TR/did-core/" \l "dfn-consumption) kumpleto ang proseso.
5. DAPAT gumawa ng mga error ang isang sumusunod na consumer kapag gumagamit ng mga hindi sumusunod na dokumento [ng DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) o [DID](https://www.w3.org/TR/did-core/#dfn-did-documents) .

Graphical user interface, diagram, application

Description automatically generated

(img scr: <https://www.w3.org/TR/did-core/diagrams/diagram-production-consumption.svg>)

*Pigura*4*Produksyon at pagkonsumo ng mga representasyon. Tingnan din ang: [paglalarawan ng salaysay](https://www.w3.org/TR/did-core/" \l "production-consumption-longdesc) .*

TANDAAN : Conversion sa pagitan ng mga representasyon

Inaasahang magko-convert ang isang pagpapatupad sa pagitan ng mga [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) sa pamamagitan ng paggamit ng mga panuntunan sa *pagkonsumo* sa pinagmulang representasyon na nagreresulta sa [modelo ng data](https://www.w3.org/TR/did-core/" \l "data-model) at pagkatapos ay paggamit ng mga panuntunan sa *produksyon* para i-serialize ang [modelo ng data](https://www.w3.org/TR/did-core/" \l "data-model) sa target na representasyon, o anumang iba pang mekanismo na nagreresulta sa parehong target na representasyon.

### **6.2JSON**

Tinutukoy ng seksyong ito ang mga panuntunan sa [produksyon](https://www.w3.org/TR/did-core/" \l "dfn-production) at [pagkonsumo para sa](https://www.w3.org/TR/did-core/" \l "dfn-consumption)[representasyon](https://www.w3.org/TR/did-core/#dfn-representations) ng JSON .

#### 6.2.1Produksyon

Ang [DID document](https://www.w3.org/TR/did-core/#dfn-did-documents) , DID document data structures, at [representation-specific entries](https://www.w3.org/TR/did-core/#dfn-representation-specific-entry)[map](https://infra.spec.whatwg.org/#maps)DAPAT naka -serialize sa JSON [representation](https://www.w3.org/TR/did-core/#dfn-representations) ayon sa mga sumusunod na panuntunan sa [produksyon :](https://www.w3.org/TR/did-core/" \l "dfn-production)

| **Uri ng datos** | **Uri ng Representasyon ng JSON** |
| --- | --- |
| [mapa](https://infra.spec.whatwg.org/#maps) | Isang [JSON Object](https://www.rfc-editor.org/rfc/rfc8259#section-4) , kung saan ang bawat entry ay naka-serialize bilang isang miyembro ng JSON Object na may entry key bilang pangalan ng miyembro ng [JSON String](https://www.rfc-editor.org/rfc/rfc8259#section-7) at ang entry value ayon sa uri nito, gaya ng tinukoy sa talahanayang ito. |
| [listahan](https://infra.spec.whatwg.org/#list) | Isang [JSON Array](https://www.rfc-editor.org/rfc/rfc8259#section-5) , kung saan ang bawat elemento ng listahan ay naka-serialize, sa pagkakasunud-sunod, bilang isang halaga ng array ayon sa uri nito, gaya ng tinukoy sa talahanayang ito. |
| [itakda](https://infra.spec.whatwg.org/#ordered-set) | Isang [JSON Array](https://www.rfc-editor.org/rfc/rfc8259#section-5) , kung saan ang bawat elemento ng set ay idinaragdag, sa pagkakasunud-sunod, bilang isang halaga ng array ayon sa uri nito, gaya ng tinukoy sa talahanayang ito. |
| [datetime](https://www.w3.org/TR/did-core/#dfn-datetime) | Isang [JSON String](https://www.rfc-editor.org/rfc/rfc8259#section-7) na na-serialize bilang [XML Datetime](https://www.w3.org/TR/xmlschema11-2/#dateTime) na na-normalize sa UTC 00:00:00 at walang sub-second decimal precision. Halimbawa: 2020-12-20T19:17:47Z. |
| [string](https://infra.spec.whatwg.org/#string) | Isang [JSON String](https://www.rfc-editor.org/rfc/rfc8259#section-7) . |
| [integer](https://www.w3.org/TR/did-core/#dfn-integer) | Isang [JSON Number na](https://www.rfc-editor.org/rfc/rfc8259#section-6) walang decimal o fractional na bahagi. |
| [doble](https://www.w3.org/TR/did-core/#dfn-double) | Isang [JSON Number na](https://www.rfc-editor.org/rfc/rfc8259#section-6) may decimal at fractional na bahagi. |
| [boolean](https://infra.spec.whatwg.org/#boolean) | Isang [JSON Boolean](https://www.rfc-editor.org/rfc/rfc8259#section-3) . |
| [wala](https://infra.spec.whatwg.org/#nulls) | Isang [JSON null literal](https://www.rfc-editor.org/rfc/rfc8259#section-3) . |

Ang lahat ng mga tagapagpatupad na lumilikha ng mga [producer na tumutugma na gumagawa ng mga](https://www.w3.org/TR/did-core/#dfn-conforming-producer)[representasyon](https://www.w3.org/TR/did-core/#dfn-representations) ng JSON ay pinapayuhan na tiyaking ang kanilang mga algorithm ay nakahanay sa mga [panuntunan ng serialization ng JSON](https://infra.spec.whatwg.org/" \l "serialize-an-infra-value-to-json-bytes) sa detalye ng [ [INFRA](https://www.w3.org/TR/did-core/#bib-infra) ] at sa mga payo sa [katumpakan hinggil sa Mga Numero](https://www.rfc-editor.org/rfc/rfc8259" \l "section-6) sa detalye ng JSON [ [RFC8259](https://www.w3.org/TR/did-core/#bib-rfc8259) ].

Ang lahat ng mga entry ng isang [DID na dokumento ay](https://www.w3.org/TR/did-core/#dfn-did-documents)*DAPAT* kasama sa root na [JSON Object](https://www.rfc-editor.org/rfc/rfc8259#section-4) . *MAAARING* maglaman ang mga entry ng karagdagang mga substructure ng data na napapailalim sa mga panuntunan sa representasyon ng halaga sa listahan sa itaas. Kapag nagse-serialize ng isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) , *DAPAT tumukoy ang isang*[tumutugmang producer](https://www.w3.org/TR/did-core/" \l "dfn-conforming-producer) ng uri ng media ng mga downstream na application tulad ng inilarawan saapplication/did+json[7.1.2Metadata ng DID Resolution](https://www.w3.org/TR/did-core/#did-resolution-metadata) .

[HALIMBAWA21](https://www.w3.org/TR/did-core/#example-example-did-document-in-json-representation): Halimbawa ng DID na dokumento sa representasyon ng JSON

{

"id": "did:example:123456789abcdefghi",

"authentication": [{

"id": "did:example:123456789abcdefghi#keys-1",

"type": "Ed25519VerificationKey2018",

"controller": "did:example:123456789abcdefghi",

"publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"

}]

}

#### 6.2.2Pagkonsumo

DAPAT i -deserialize ang DID document at DID document data structures na representasyon ng JSON sa data [model](https://www.w3.org/TR/did-core/#dfn-did-documents) ayon [sa](https://www.w3.org/TR/did-core/" \l "dfn-representations)[mga](https://www.w3.org/TR/did-core/#data-model) sumusunod na panuntunan sa [pagkonsumo :](https://www.w3.org/TR/did-core/" \l "dfn-consumption)

| **Uri ng Representasyon ng JSON** | **Uri ng datos** |
| --- | --- |
| [JSON Object](https://www.rfc-editor.org/rfc/rfc8259#section-4) | Isang [mapa](https://infra.spec.whatwg.org/" \l "maps) , kung saan idinaragdag ang bawat miyembro ng JSON Object bilang isang entry sa mapa. Ang bawat entry key ay nakatakda bilang pangalan ng miyembro ng JSON Object. Ang bawat halaga ng entry ay itinakda sa pamamagitan ng pag-convert ng halaga ng miyembro ng JSON Object ayon sa uri ng representasyon ng JSON gaya ng tinukoy sa talahanayang ito. Dahil ang order ay hindi tinukoy ng JSON Objects, walang insertion order ang magagarantiya. |
| [JSON Array](https://www.rfc-editor.org/rfc/rfc8259#section-5) kung saan ang [data model](https://www.w3.org/TR/did-core/#data-model) entry value ay isang [listahan](https://infra.spec.whatwg.org/" \l "list) o hindi alam | Isang [listahan](https://infra.spec.whatwg.org/" \l "list) , kung saan ang bawat value ng JSON Array ay idinaragdag sa listahan sa pagkakasunud-sunod, na na-convert batay sa uri ng representasyon ng JSON ng array value, gaya ng tinukoy sa talahanayang ito. |
| [JSON Array](https://www.rfc-editor.org/rfc/rfc8259#section-5) kung saan ang [data model](https://www.w3.org/TR/did-core/#data-model) entry value ay isang [set](https://infra.spec.whatwg.org/#ordered-set) | Isang [set](https://infra.spec.whatwg.org/#ordered-set) , kung saan ang bawat value ng JSON Array ay idinaragdag sa set sa pagkakasunud-sunod, na na-convert batay sa uri ng representasyon ng JSON ng array value, gaya ng tinukoy sa talahanayang ito. |
| [JSON String](https://www.rfc-editor.org/rfc/rfc8259#section-7) kung saan ang value ng entry ng [data model ay isang](https://www.w3.org/TR/did-core/#data-model)[datetime](https://www.w3.org/TR/did-core/#dfn-datetime) | Isang [datetime](https://www.w3.org/TR/did-core/#dfn-datetime) . |
| [JSON String](https://www.rfc-editor.org/rfc/rfc8259#section-7) , kung saan ang uri ng value ng entry ng [data model ay](https://www.w3.org/TR/did-core/#data-model)[string](https://infra.spec.whatwg.org/#string) o hindi alam | Isang [string](https://infra.spec.whatwg.org/#string) . |
| [Numero ng JSON na](https://www.rfc-editor.org/rfc/rfc8259#section-6) walang decimal o fractional na bahagi | Isang [integer](https://www.w3.org/TR/did-core/#dfn-integer) . |
| [JSON Number](https://www.rfc-editor.org/rfc/rfc8259#section-6) na may decimal at fractional na bahagi, o kapag ang entry value ay [doble](https://www.w3.org/TR/did-core/#dfn-double) anuman ang pagsasama ng fractional na bahagi | Isang [doble](https://www.w3.org/TR/did-core/#dfn-double) . |
| [JSON Boolean](https://www.rfc-editor.org/rfc/rfc8259#section-3) | Isang [boolean](https://infra.spec.whatwg.org/" \l "boolean) . |
| [JSON null literal](https://www.rfc-editor.org/rfc/rfc8259#section-3) | Isang [null na](https://infra.spec.whatwg.org/#nulls) halaga. |

Ang lahat ng mga nagpapatupad na lumilikha ng mga [sumusunod na consumer na gumagawa ng mga](https://www.w3.org/TR/did-core/" \l "dfn-conforming-consumer)[representasyon](https://www.w3.org/TR/did-core/#dfn-representations) ng JSON ay pinapayuhan na tiyaking ang kanilang mga algorithm ay nakahanay sa mga [panuntunan sa conversion ng JSON](https://infra.spec.whatwg.org/" \l "parse-json-bytes-to-an-infra-value) sa detalye ng [ [INFRA](https://www.w3.org/TR/did-core/#bib-infra) ] at sa mga payo sa [katumpakan hinggil sa Mga Numero](https://www.rfc-editor.org/rfc/rfc8259" \l "section-6) sa detalye ng JSON [ [RFC8259](https://www.w3.org/TR/did-core/#bib-rfc8259) ].

Kung ang impormasyon ng uri ng media ay magagamit sa isang [sumusunod na mamimili](https://www.w3.org/TR/did-core/" \l "dfn-conforming-consumer) at ang halaga ng uri ng media ay application/did+json, kung gayon ang istraktura ng data na ginagamit ay isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) , at ang root element ay DAPAT na isang [JSON Object](https://www.rfc-editor.org/rfc/rfc8259#section-4) kung saan ang lahat ng miyembro ng object ay mga entry ng [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) . Ang isang [sumusunod na consumer para sa isang](https://www.w3.org/TR/did-core/" \l "dfn-conforming-consumer)[representasyon](https://www.w3.org/TR/did-core/#dfn-representations) ng JSON na gumagamit ng isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) na may root element na hindi isang [JSON Object ay](https://www.rfc-editor.org/rfc/rfc8259#section-4)DAPAT mag-ulat ng isang error.

### **6.3JSON-LD**

Ang JSON-LD [ [JSON-LD11](https://www.w3.org/TR/did-core/#bib-json-ld11) ] ay isang JSON-based na format na ginagamit para i-serialize ang [Linked Data](http://www.w3.org/TR/ld-glossary/#linked-data) . Tinutukoy ng seksyong ito ang mga panuntunan sa [produksyon](https://www.w3.org/TR/did-core/" \l "dfn-production) at [pagkonsumo para sa](https://www.w3.org/TR/did-core/" \l "dfn-consumption)[representasyon](https://www.w3.org/TR/did-core/#dfn-representations) ng JSON-LD .

Tinutukoy ng [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) ng JSON-LD ang sumusunod na mga [entry na tukoy](https://www.w3.org/TR/did-core/#dfn-representation-specific-entry) sa representasyon :

**@konteksto**

Ang [Konteksto ng JSON-LD](https://www.w3.org/TR/json-ld11/" \l "the-context) ay alinman sa isang [string](https://infra.spec.whatwg.org/#string) o isang [listahan](https://infra.spec.whatwg.org/" \l "list) na naglalaman ng anumang kumbinasyon ng mga [string](https://infra.spec.whatwg.org/#string) at/o mga [nakaayos na mapa](https://infra.spec.whatwg.org/" \l "maps) .

#### 6.3.1Produksyon

Ang [dokumento](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ng DID , mga istruktura ng data ng dokumento ng DID, at [mapa ng mga](https://infra.spec.whatwg.org/" \l "maps)[entry na partikular sa representasyon ay](https://www.w3.org/TR/did-core/#dfn-representation-specific-entry)DAPAT na naka-serialize sa [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) ng JSON-LD ayon sa mga panuntunan sa [produksyon ng](https://www.w3.org/TR/did-core/" \l "dfn-production)[representasyon](https://www.w3.org/TR/did-core/#dfn-representations) ng JSON gaya ng tinukoy sa [6.2JSON](https://www.w3.org/TR/did-core/#json) .

Bilang karagdagan sa paggamit ng mga panuntunan sa [produksyon ng](https://www.w3.org/TR/did-core/#dfn-production)[representasyon ng JSON,](https://www.w3.org/TR/did-core/#dfn-representations)DAPAT isama ng produksyon ng JSON-LD ang entry [na tukoy sa representasyon .](https://www.w3.org/TR/did-core/#dfn-representation-specific-entry)Ang serialized na halaga ng DAPAT ay ang [JSON String](https://www.rfc-editor.org/rfc/rfc8259#section-7) , o isang [JSON Array](https://www.rfc-editor.org/rfc/rfc8259#section-5) kung saan ang unang item ay ang [JSON String](https://www.rfc-editor.org/rfc/rfc8259#section-7) at ang mga kasunod na item ay naka-serialize ayon sa mga panuntunan sa [produksyon ng](https://www.w3.org/TR/did-core/#dfn-production)[representasyon ng JSON.](https://www.w3.org/TR/did-core/#dfn-representations) [@context](https://www.w3.org/TR/did-core/#dfn-context)@context https://www.w3.org/ns/did/v1 https://www.w3.org/ns/did/v1

[HALIMBAWA22](https://www.w3.org/TR/did-core/#example-a-valid-serialization-of-a-simple-context-entry): Isang wastong serialization ng isang simpleng @context entry

{

"@context": "https://www.w3.org/ns/did/v1",

...

}

[HALIMBAWA23](https://www.w3.org/TR/did-core/#example-a-valid-serialization-of-a-layered-context-entry): Isang wastong serialization ng isang layered @context entry

{

"@context": [

"https://www.w3.org/ns/did/v1",

"https://did-method-extension.example/v1"

],

...

}

Ang lahat ng mga nagpapatupad na gumagawa ng mga [sumusunod na producer na gumagawa ng mga](https://www.w3.org/TR/did-core/" \l "dfn-conforming-producer)[representasyon](https://www.w3.org/TR/did-core/#dfn-representations) ng JSON-LD ay pinapayuhan na tiyaking ang kanilang mga algorithm ay gumagawa ng mga wastong JSON-LD [ [JSON-LD11](https://www.w3.org/TR/did-core/#bib-json-ld11) ] na mga dokumento. Ang mga di-wastong dokumento ng JSON-LD ay magdudulot sa mga JSON-LD na processor na huminto at mag-ulat ng mga error.

Upang makamit ang interoperability sa iba't ibang [representasyon ,](https://www.w3.org/TR/did-core/" \l "dfn-representations)DAPAT na mairehistro ang lahat ng JSON-LD Contexts at ang kanilang mga termino sa DID Specification Registries [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ].

Ang isang [tumutugon na producer](https://www.w3.org/TR/did-core/" \l "dfn-conforming-producer) na bumubuo ng isang JSON-LD na [representasyon ay](https://www.w3.org/TR/did-core/" \l "dfn-representations)HINDI DAPAT gumawa ng isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) na naglalaman ng mga terminong hindi tinukoy sa pamamagitan ng @contextbilang [sumusunod na mga mamimili](https://www.w3.org/TR/did-core/" \l "dfn-conforming-consumer) ay inaasahang mag-aalis ng mga hindi kilalang termino. Kapag nagse-serialize ng JSON-LD na [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) ng isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) , DAPAT tumukoy ang isang [tumutugmang producer](https://www.w3.org/TR/did-core/" \l "dfn-conforming-producer) ng uri ng media ng mga downstream na application tulad ng inilarawan saapplication/did+ld+json[7.1.2Metadata ng DID Resolution](https://www.w3.org/TR/did-core/#did-resolution-metadata) .

#### 6.3.2Pagkonsumo

Ang [dokumento ng DID at anumang istruktura ng data ng dokumento ng DID na ipinahayag ng isang](https://www.w3.org/TR/did-core/" \l "dfn-did-documents)[representasyon](https://www.w3.org/TR/did-core/#dfn-representations) ng JSON-LD ay DAPAT na i-deserialize sa [modelo ng data](https://www.w3.org/TR/did-core/" \l "data-model) ayon sa mga panuntunan sa [pagkonsumo ng](https://www.w3.org/TR/did-core/" \l "dfn-consumption)[representasyon](https://www.w3.org/TR/did-core/#dfn-representations) ng JSON gaya ng tinukoy sa[6.2JSON](https://www.w3.org/TR/did-core/#json) .

Ang lahat ng mga nagpapatupad na lumilikha ng mga [sumusunod na consumer](https://www.w3.org/TR/did-core/" \l "dfn-conforming-consumer) na gumagamit ng mga [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) ng JSON-LD ay pinapayuhan na tiyaking ang kanilang mga algorithm ay tumatanggap lamang ng mga wastong dokumento ng JSON-LD [ [JSON-LD11](https://www.w3.org/TR/did-core/#bib-json-ld11) ]. Ang mga di-wastong dokumento ng JSON-LD ay magdudulot sa mga JSON-LD na processor na huminto at mag-ulat ng mga error.

[Ang pagsunod sa mga consumer](https://www.w3.org/TR/did-core/#dfn-conforming-consumer) na nagpoproseso ng isang JSON-LD na [representasyon ay](https://www.w3.org/TR/did-core/" \l "dfn-representations)DAPAT na alisin ang lahat ng mga tuntunin mula sa isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) na hindi tinukoy sa pamamagitan ng @context.

## 7.Resolusyon

Tinutukoy ng seksyong ito ang mga input at output ng [DID resolution](https://www.w3.org/TR/did-core/#dfn-did-resolution) at [DID URL dereferencing](https://www.w3.org/TR/did-core/#dfn-did-url-dereferencing) . Ang kanilang eksaktong pagpapatupad ay wala sa saklaw para sa pagtutukoy na ito, ngunit ang ilang mga pagsasaalang-alang para sa mga nagpapatupad ay tinalakay sa [ [DID-RESOLUTION](https://www.w3.org/TR/did-core/#bib-did-resolution) ].

DAPAT ipatupad ng lahat ng conformant [DID resolver ang mga function ng](https://www.w3.org/TR/did-core/#dfn-did-resolvers)[DID resolution](https://www.w3.org/TR/did-core/#dfn-did-resolution) para sa kahit isang [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) at DAPAT makapagbalik ng [dokumento](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ng DID sa kahit isang conformant na [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) .

### **7.1DID Resolution**

Ang mga function ng [DID resolution](https://www.w3.org/TR/did-core/#dfn-did-resolution) ay nagre-resolve ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) sa isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) sa pamamagitan ng paggamit ng "Read" operation ng naaangkop na [DID method](https://www.w3.org/TR/did-core/#dfn-did-methods) gaya ng inilarawan sa[8.2Mga Operasyon ng Pamamaraan](https://www.w3.org/TR/did-core/#method-operations) . Ang mga detalye kung paano naisasagawa ang prosesong ito ay nasa labas ng saklaw ng detalyeng ito, ngunit ang lahat ng umaayon sa [DID na mga solver](https://www.w3.org/TR/did-core/#dfn-did-resolvers) ay nagpapatupad ng mga function sa ibaba, na mayroong mga sumusunod na abstract na form:

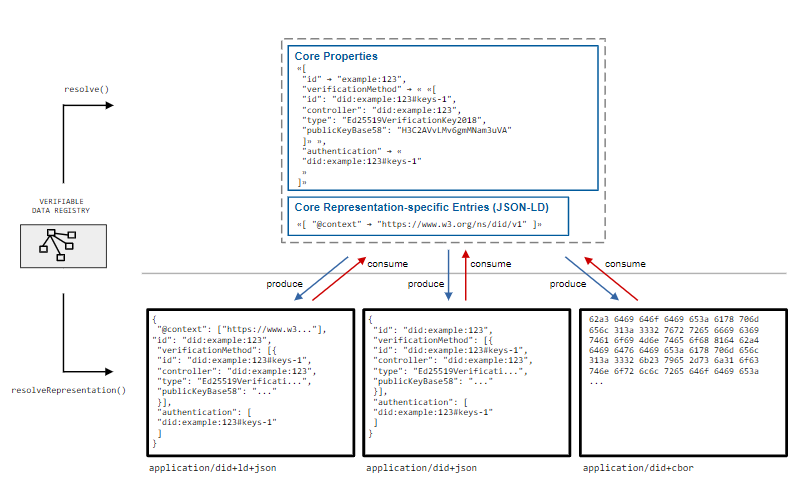
resolve(did, resolutionOptions) →

« didResolutionMetadata, didDocument, didDocumentMetadata »

resolveRepresentation(did, resolutionOptions) →

« didResolutionMetadata, didDocumentStream, didDocumentMetadata »

resolveIbinabalik ng function ang dokumento ng [DID](https://www.w3.org/TR/did-core/#dfn-did-documents) sa abstract form nito (isang [mapa](https://infra.spec.whatwg.org/" \l "maps) ). Ang resolveRepresentationfunction ay nagbabalik ng isang byte stream ng [DID Document](https://www.w3.org/TR/did-core/#dfn-did-documents) na naka-format sa kaukulang representasyon.



(imgsrc: <https://www.w3.org/TR/did-core/diagrams/diagram-resolve-resolverepresentation.svg>)

*Pigura*5*Ang mga function ay nagresolve() at resolveRepresentation(). Tingnan din ang: [paglalarawan ng salaysay](https://www.w3.org/TR/did-core/" \l "resolve-resolverepresentation-longdesc) .*

ng mga variable ng input ng resolveat mga resolveRepresentationfunction ay ang mga sumusunod:

**ginawa**

Ito ang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na lutasin. Ang input na ito ay *KINAKAILANGAN* at ang value ay *DAPAT* na isang conformant [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) gaya ng tinukoy sa[3.1DID Syntax](https://www.w3.org/TR/did-core/#did-syntax) .

**resolutionOptions**

Isang [istruktura ng metadata na](https://www.w3.org/TR/did-core/" \l "metadata-structure) naglalaman ng mga katangian na tinukoy sa[7.1.1Mga Opsyon sa Resolusyon ng DID](https://www.w3.org/TR/did-core/#did-resolution-options) . Ang input na ito ay *KINAKAILANGAN , ngunit MAAARING* walang laman ang istraktura .

Ang bawat function na ito ay nagbabalik ng maramihang mga halaga, at walang mga limitasyon na inilalagay sa kung paano ibinabalik ang mga halagang ito nang magkasama. Ang mga return value ng resolveay [didResolutionMetadata](https://www.w3.org/TR/did-core/" \l "dfn-didresolutionmetadata) , [didDocument](https://www.w3.org/TR/did-core/" \l "dfn-diddocument) , at [didDocumentMetadata](https://www.w3.org/TR/did-core/" \l "dfn-diddocumentmetadata) . Ang mga return value ng resolveRepresentationay [didResolutionMetadata](https://www.w3.org/TR/did-core/#dfn-didresolutionmetadata) , [didDocumentStream](https://www.w3.org/TR/did-core/#dfn-diddocumentstream) , at [didDocumentMetadata](https://www.w3.org/TR/did-core/" \l "dfn-diddocumentmetadata) . Ang mga halagang ito ay inilarawan sa ibaba:

***didResolutionMetadata***

Isang [istruktura ng metadata](https://www.w3.org/TR/did-core/" \l "metadata-structure) na binubuo ng mga value na nauugnay sa mga resulta ng proseso ng [paglutas ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-resolution) na karaniwang nagbabago sa pagitan ng mga invocation ng resolveat mga resolveRepresentationfunction, dahil kinakatawan nito ang data tungkol sa mismong proseso ng paglutas. Ang istrakturang ito ay *KINAKAILANGAN* , at sa kaso ng isang error sa proseso ng paglutas, *HINDI ito DAPAT* walang laman. Ang metadata na ito ay tinukoy ng[7.1.2DID Resolution Metadata](https://www.w3.org/TR/did-core/#did-resolution-metadata) . Kung tinawag, *DAPAT* maglaman resolveRepresentationang istrukturang ito ng isang property na naglalaman ng Uri ng Media ng representasyong makikita sa . Kung hindi matagumpay ang resolution, *DAPAT* maglaman ang istrukturang ito ng property na naglalarawan sa error. contentTypedidDocumentStreamerror

***didDocument***

Kung matagumpay ang resolution, at kung resolvetinawag ang function, *DAPAT* itong [DID document](https://www.w3.org/TR/did-core/#dfn-did-documents) abstract data model (isang [mapa](https://infra.spec.whatwg.org/" \l "maps) ) gaya ng inilarawan sa[4.Modelo ng Data](https://www.w3.org/TR/did-core/#data-model) na may kakayahang ma-transform sa isang [naaayon na DID Document](https://www.w3.org/TR/did-core/" \l "dfn-conforming-did-document) (representasyon), gamit ang mga panuntunan sa produksyon na tinukoy ng representasyon. Ang halaga ng [id](https://www.w3.org/TR/did-core/" \l "dfn-id)sa naresolbang [dokumento ng DID ay](https://www.w3.org/TR/did-core/" \l "dfn-did-documents)*DAPAT* tumugma sa [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na nalutas. Kung hindi matagumpay ang resolution, *DAPAT* walang laman ang value na ito.

***didDocumentStream***

Kung matagumpay ang resolution, at kung resolveRepresentation tinawag ang function, *DAPAT* itong byte stream ng naresolbang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) sa isa sa mga conformant na [representasyon](https://www.w3.org/TR/did-core/" \l "representations) . Ang byte stream ay maaaring ma-parse ng tumatawag ng resolveRepresentationfunction sa isang [modelo ng data](https://www.w3.org/TR/did-core/" \l "data-model) , na maaari namang ma-validate at maproseso. Kung hindi matagumpay ang resolution, *DAPAT* na walang laman na stream ang value na ito.

***didDocumentMetadata***

Kung matagumpay ang resolution, *DAPAT* itong [metadata structure](https://www.w3.org/TR/did-core/#metadata-structure) . Naglalaman ang istrukturang ito ng metadata tungkol sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) na nasa didDocument property. Karaniwang hindi nagbabago ang metadata na ito sa pagitan ng mga invocation ng resolveat mga resolveRepresentationfunction maliban kung magbabago ang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) , dahil kinakatawan nito ang metadata tungkol sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) . Kung ang resolution ay hindi matagumpay, ang output na ito ay *DAPAT* na isang walang laman na [istraktura ng metadata](https://www.w3.org/TR/did-core/" \l "metadata-structure) . Ang mga katangiang tinukoy ng pagtutukoy na ito ay nasa[7.1.3DID Document Metadata](https://www.w3.org/TR/did-core/#did-document-metadata) .

Ang pagsunod sa mga pagpapatupad ng [DID resolver ay](https://www.w3.org/TR/did-core/#dfn-did-resolvers) hindi nagbabago sa lagda ng mga function na ito sa anumang paraan. Maaaring imapa ng mga pagpapatupad ng [DID resolver](https://www.w3.org/TR/did-core/#dfn-did-resolvers)resolve ang at mga resolveRepresentationfunction sa isang internal na function na tukoy sa pamamaraan upang maisagawa ang aktwal na proseso ng [paglutas ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-resolution) . [Ang mga pagpapatupad ng DID resolver ay](https://www.w3.org/TR/did-core/#dfn-did-resolvers) maaaring magpatupad at maglantad ng mga karagdagang function na may iba't ibang mga lagda bilang karagdagan sa resolveat mga resolveRepresentationfunction na tinukoy dito.

#### 7.1.1Mga Opsyon sa Resolusyon ng DID

Ang mga posibleng pag-aari sa loob ng istrukturang ito at ang mga posibleng halaga nito ay nakarehistro sa DID Specification Registry [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ]. Tinutukoy ng detalyeng ito ang mga sumusunod na karaniwang katangian.

**tanggapin**

Ang Uri ng Media ng gustong [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) ng tumatawag sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) . DAPAT ipahayag ang Uri ng Media bilang isang [ASCII string](https://infra.spec.whatwg.org/#ascii-string) . DAPAT gamitin ng pagpapatupad ng [DID resolver](https://www.w3.org/TR/did-core/#dfn-did-resolvers) ang halagang ito upang matukoy ang [representasyong](https://www.w3.org/TR/did-core/" \l "dfn-representations) nakapaloob sa ibinalik kung sinusuportahan at available ang naturang [representasyon .](https://www.w3.org/TR/did-core/" \l "dfn-representations)Ang property na ito ay OPTIONAL para sa function at HINDI DAPAT gamitin kasama ng function. didDocumentStreamresolveRepresentationresolve

#### 7.1.2Metadata ng DID Resolution

Ang mga posibleng pag-aari sa loob ng istrukturang ito at ang mga posibleng halaga nito ay nakarehistro sa DID Specification Registry [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ]. Tinutukoy ng detalyeng ito ang mga sumusunod na katangian ng metadata ng DID resolution:

**uri ng nilalaman**

Ang Uri ng Media ng ibinalik na didDocumentStream. Ang property na ito ay KINAKAILANGAN kung matagumpay ang resolution at kung resolveRepresentationtinawag ang function. HINDI DAPAT naroroon ang property na resolveito kung tinawag ang function. Ang halaga ng property na ito ay DAPAT na isang [ASCII string](https://infra.spec.whatwg.org/#ascii-string) na Uri ng Media ng mga conformant na [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) . DAPAT gamitin ng tumatawag ng resolveRepresentationfunction ang halagang ito kapag tinutukoy kung paano i-parse at iproseso ang ibinalik ng function na ito sa [modelo ng data](https://www.w3.org/TR/did-core/" \l "data-model) . didDocumentStream

**pagkakamali**

Ang error code mula sa proseso ng paglutas. Ang property na ito ay KINAKAILANGAN kapag may error sa proseso ng pagresolba. Ang halaga ng property na ito ay DAPAT na iisang keyword na [ASCII string](https://infra.spec.whatwg.org/#ascii-string) . Ang mga posibleng value ng property ng field na ito ay DAPAT na nakarehistro sa DID Specification Registry [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ]. Tinutukoy ng detalyeng ito ang mga sumusunod na karaniwang halaga ng error:

**invalidDid**

Ang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na ibinigay sa [DID resolution](https://www.w3.org/TR/did-core/#dfn-did-resolution) function ay hindi sumusunod sa wastong syntax. (Tingnan[3.1DID Syntax](https://www.w3.org/TR/did-core/#did-syntax) .)

**hindi mahanap**

Hindi mahanap ng [DID resolver ang](https://www.w3.org/TR/did-core/#dfn-did-resolvers)[dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) ng DID na nagreresulta mula sa kahilingang ito ng resolusyon.

**representationNotSupported**

Ibinabalik ang error code na ito kung ang [representasyong](https://www.w3.org/TR/did-core/" \l "dfn-representations) hiniling sa pamamagitan ng acceptinput metadata property ay hindi sinusuportahan ng [DID method](https://www.w3.org/TR/did-core/#dfn-did-methods) at/o [DID resolver na](https://www.w3.org/TR/did-core/#dfn-did-resolvers) pagpapatupad.

#### 7.1.3DID Document Metadata

Ang mga posibleng pag-aari sa loob ng istrukturang ito at ang kanilang mga posibleng halaga ay DAPAT na mairehistro sa DID Specification Registries [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ]. Tinutukoy ng detalyeng ito ang mga sumusunod na karaniwang katangian.

**nilikha**

DAPAT bang may kasamang property ang metadata ng [dokumento](https://www.w3.org/TR/did-core/" \l "dfn-did-documents)created upang ipahiwatig ang timestamp ng [operasyong Lumikha](https://www.w3.org/TR/did-core/" \l "method-operations) . Ang value ng property ay DAPAT na isang [string](https://infra.spec.whatwg.org/#string) na naka- format bilang [XML Datetime](https://www.w3.org/TR/xmlschema11-2/#dateTime) na na-normalize sa UTC 00:00:00 at walang sub-second decimal precision. Halimbawa: 2020-12-20T19:17:47Z.

**na-update**

DAPAT bang may kasamang property ang metadata ng [dokumento](https://www.w3.org/TR/did-core/" \l "dfn-did-documents)updated upang isaad ang timestamp ng huling [pagpapatakbo ng Update](https://www.w3.org/TR/did-core/" \l "method-operations) para sa bersyon ng dokumento na nalutas. DAPAT sundin ng halaga ng property ang parehong mga panuntunan sa pag-format gaya ng created property. Ang ari- updatedarian ay tinanggal kung ang isang Update operation ay hindi pa kailanman naisagawa sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) . Kung mayroong isang updated property, maaari itong maging kapareho ng value ng createdproperty kapag ang pagkakaiba sa pagitan ng dalawang timestamp ay mas mababa sa isang segundo.

**na-deactivate**

Kung ang isang DID ay na- [deactivate](https://www.w3.org/TR/did-core/#method-operations) , [DID document](https://www.w3.org/TR/did-core/#dfn-did-documents) metadata DAPAT isama ang property na ito na may boolean value true. Kung ang isang DID ay hindi na-deactivate, ang property na ito ay OPTIONAL , ngunit kung kasama, DAPAT mayroong boolean value false.

**nextUpdate**

MAAARING magsama ng property ang metadata ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents)nextUpdate kung ang nalutas na bersyon ng dokumento ay hindi ang pinakabagong bersyon ng dokumento. Ipinapahiwatig nito ang timestamp ng susunod na [pagpapatakbo ng Update](https://www.w3.org/TR/did-core/" \l "method-operations) . DAPAT sundin ng halaga ng property ang parehong mga panuntunan sa pag-format gaya ng createdproperty.

**versionId**

DAPAT bang may kasamang property ang metadata ng [dokumento](https://www.w3.org/TR/did-core/" \l "dfn-did-documents)versionId upang isaad ang bersyon ng huling [pagpapatakbo ng Update](https://www.w3.org/TR/did-core/" \l "method-operations) para sa bersyon ng dokumento na nalutas. Ang value ng property ay DAPAT na isang [ASCII string](https://infra.spec.whatwg.org/#ascii-string) .

**nextVersionId**

MAAARING magsama ng property ang metadata ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents)nextVersionId kung ang nalutas na bersyon ng dokumento ay hindi ang pinakabagong bersyon ng dokumento. Ipinapahiwatig nito ang bersyon ng susunod na [pagpapatakbo ng Update](https://www.w3.org/TR/did-core/" \l "method-operations) . Ang value ng property ay DAPAT na isang [ASCII string](https://infra.spec.whatwg.org/#ascii-string) .

**katumbasId**

Maaaring tukuyin ng isang paraan ng DID ang iba't ibang anyo ng isang [DID](https://www.w3.org/TR/did-core/#dfn-did-methods)[na](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) lohikal na katumbas. Ang isang halimbawa ay kapag ang isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay kumuha ng isang form bago ang pagpaparehistro sa isang [nabe-verify na data registry](https://www.w3.org/TR/did-core/#dfn-verifiable-data-registry) at isa pang form pagkatapos ng naturang pagpaparehistro. Sa kasong ito, maaaring kailanganin ng detalye ng [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) na ipahayag ang isa o higit pang [mga DID](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers) na lohikal na katumbas ng nalutas na [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) bilang isang pag-aari ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) . Ito ang layunin ng ari- [equivalentId](https://www.w3.org/TR/did-core/" \l "dfn-equivalentid)arian.

MAAARING may kasamang equivalentIdproperty ang metadata [ng dokumento ng DID .](https://www.w3.org/TR/did-core/#dfn-did-documents)Kung mayroon, ang value ay DAPAT na isang [set](https://infra.spec.whatwg.org/#ordered-set) kung saan ang bawat item ay isang [string](https://infra.spec.whatwg.org/#string) na sumusunod sa mga panuntunan sa Seksyon[3.1DID Syntax](https://www.w3.org/TR/did-core/#did-syntax) . Ang relasyon ay isang pahayag na ang bawat [equivalentId](https://www.w3.org/TR/did-core/" \l "dfn-equivalentid)halaga ay lohikal na katumbas ng idhalaga ng ari-arian at sa gayon ay tumutukoy sa parehong [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) . Ang bawat [equivalentId](https://www.w3.org/TR/did-core/" \l "dfn-equivalentid)halaga ng DID ay DAPAT gawin ng, at isang anyo ng, parehong [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) bilang idhalaga ng ari-arian. (hal., did:example:abc== did:example:ABC)

DAPAT ginagarantiyahan ng isang sumusunod na detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) na ang bawat halaga ay lohikal na katumbas ng halaga ng ari-arian. [equivalentId](https://www.w3.org/TR/did-core/" \l "dfn-equivalentid)id

Inaasahang mapapanatili ng isang humihiling na partido ang mga halaga mula sa idat mga pag- [equivalentId](https://www.w3.org/TR/did-core/" \l "dfn-equivalentid)aari upang matiyak na ang anumang kasunod na pakikipag-ugnayan sa alinman sa mga halagang naglalaman ng mga ito ay tama na pinangangasiwaan bilang lohikal na katumbas (hal., panatilihin ang lahat ng mga variant sa isang database upang ang isang pakikipag-ugnayan sa alinmang isa ay nagmamapa sa pareho pinagbabatayan na account).

TANDAAN : Mas malakas na katumbas

[equivalentId](https://www.w3.org/TR/did-core/#dfn-equivalentid) ay isang mas malakas na anyo ng equivalence kaysa [alsoKnownAs](https://www.w3.org/TR/did-core/" \l "dfn-alsoknownas)dahil DAPAT na garantisado ang equivalence ng namamahala na [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) . [equivalentId](https://www.w3.org/TR/did-core/" \l "dfn-equivalentid)kumakatawan sa isang buong pagsasanib ng graph dahil ang parehong [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay naglalarawan sa [equivalentId](https://www.w3.org/TR/did-core/" \l "dfn-equivalentid) [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) at sa idproperty na [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) .

Kung ang isang humihiling na partido ay hindi nagpapanatili ng mga halaga mula sa idat mga pag- [equivalentId](https://www.w3.org/TR/did-core/" \l "dfn-equivalentid)aari at matiyak na ang anumang kasunod na pakikipag-ugnayan sa alinman sa mga halagang naglalaman ng mga ito ay wastong pinangangasiwaan bilang lohikal na katumbas, maaaring may mga negatibo o hindi inaasahang isyu na lumabas. Lubos na pinapayuhan ang mga nagpapatupad na sundin ang mga direktiba na nauugnay sa metadata property na ito.

**canonicalId**

Ang [canonicalId](https://www.w3.org/TR/did-core/" \l "dfn-canonicalid)property ay kapareho ng [equivalentId](https://www.w3.org/TR/did-core/" \l "dfn-equivalentid)property maliban sa: a) ito ay nauugnay sa isang value sa halip na isang set, at b) ang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay tinukoy bilang ang canonical ID para sa [DID na paksa](https://www.w3.org/TR/did-core/#dfn-did-subjects) sa loob ng saklaw ng naglalaman ng [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) .

MAAARING may kasamang canonicalIdproperty ang metadata ng [dokumento ng DID .](https://www.w3.org/TR/did-core/" \l "dfn-did-documents)Kung mayroon, ang value ay DAPAT na isang [string](https://infra.spec.whatwg.org/#string) na sumusunod sa mga panuntunan sa Seksyon[3.1DID Syntax](https://www.w3.org/TR/did-core/#did-syntax) . Ang relasyon ay isang pahayag na ang [canonicalId](https://www.w3.org/TR/did-core/" \l "dfn-canonicalid)halaga ay lohikal na katumbas ng halaga ng ari- idarian at ang [canonicalId](https://www.w3.org/TR/did-core/" \l "dfn-canonicalid) halaga ay tinukoy ng [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) upang maging canonical ID para sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) sa saklaw ng naglalaman ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) . DAPAT gawin ang isang [canonicalId](https://www.w3.org/TR/did-core/" \l "dfn-canonicalid)halaga ng, at isang anyo ng, parehong [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) bilang halaga ng ari-arian. (hal., == ). iddid:example:abcdid:example:ABC

DAPAT ginagarantiyahan ng isang sumusunod na detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) na ang halaga ay lohikal na katumbas ng halaga ng ari-arian. [canonicalId](https://www.w3.org/TR/did-core/" \l "dfn-canonicalid)id

Inaasahang gagamitin ng humihiling na partido ang [canonicalId](https://www.w3.org/TR/did-core/" \l "dfn-canonicalid)value bilang pangunahing ID value nito para sa [DID subject](https://www.w3.org/TR/did-core/#dfn-did-subjects) at ituring ang lahat ng iba pang katumbas na value bilang pangalawang alias (hal, i-update ang mga kaukulang pangunahing reference sa kanilang mga system para ipakita ang bagong canonical ID directive).

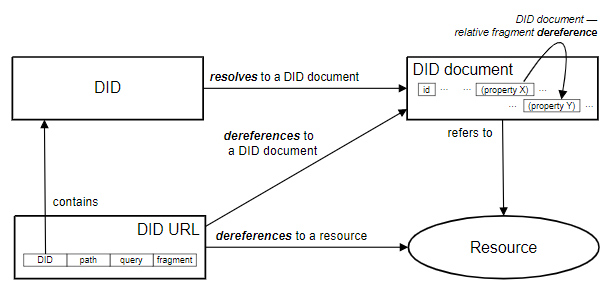
TANDAAN : Canonical equivalence

[canonicalId](https://www.w3.org/TR/did-core/#dfn-canonicalid)ay ang parehong pahayag ng equivalence bilang [equivalentId](https://www.w3.org/TR/did-core/" \l "dfn-equivalentid)maliban kung ito ay napipilitan sa isang solong halaga na tinukoy na canonical para sa [DID paksa](https://www.w3.org/TR/did-core/#dfn-did-subjects) sa saklaw ng [DID dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) . Tulad ng [equivalentId](https://www.w3.org/TR/did-core/" \l "dfn-equivalentid), [canonicalId](https://www.w3.org/TR/did-core/" \l "dfn-canonicalid)ay kumakatawan sa isang buong pagsasama ng graph dahil ang parehong [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) ay naglalarawan sa [canonicalId](https://www.w3.org/TR/did-core/" \l "dfn-canonicalid)DID at sa idproperty [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) .

Kung hindi ginagamit ng isang nagre-resolve na partido ang [canonicalId](https://www.w3.org/TR/did-core/" \l "dfn-canonicalid)value bilang pangunahing ID value nito para sa DID subject at ituturing ang lahat ng iba pang katumbas na value bilang pangalawang alias, maaaring may mga negatibo o hindi inaasahang isyu na lumitaw na nauugnay sa karanasan ng user. Lubos na pinapayuhan ang mga nagpapatupad na sundin ang mga direktiba na nauugnay sa metadata property na ito.

### **7.2DID URL Dereferencing**

Ang [DID URL dereferencing](https://www.w3.org/TR/did-core/#dfn-did-url-dereferencing) function ay nagde-dereference sa isang [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) sa isang [resource](https://www.w3.org/TR/did-core/#dfn-resources) na may mga content depende sa mga bahagi ng [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) , kabilang ang [DID method](https://www.w3.org/TR/did-core/#dfn-did-methods) , method-specific identifier, path, query, at fragment. Ang prosesong ito ay nakadepende sa [DID resolution](https://www.w3.org/TR/did-core/#dfn-did-resolution) ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na nilalaman sa [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) . [DID URL dereferencing](https://www.w3.org/TR/did-core/#dfn-did-url-dereferencing)maaaring may kasamang maraming hakbang (hal., kapag ang DID URL na inaalis sa sanggunian ay may kasamang fragment), at ang function ay tinukoy upang ibalik ang panghuling mapagkukunan pagkatapos makumpleto ang lahat ng hakbang. Ang mga detalye kung paano isinasagawa ang prosesong ito ay nasa labas ng saklaw ng detalyeng ito. Ang sumusunod na figure ay naglalarawan ng relasyon na inilarawan sa itaas.



(imgsrc: <https://www.w3.org/TR/did-core/diagrams/did_url_dereference_overview.svg>)

*Pigura*6*Pangkalahatang-ideya ng DID URL dereference Tingnan din ang: [pagsasalaysay ng paglalarawan](https://www.w3.org/TR/did-core/" \l "did-url-dereference-overview-longdesc) .*

Ang lahat ng umaayon sa [DID resolver](https://www.w3.org/TR/did-core/#dfn-did-resolvers) ay nagpapatupad ng sumusunod na function na mayroong sumusunod na abstract form:

dereference(didUrl, dereferenceOptions) →

« dereferencingMetadata, contentStream, contentMetadata »

Ang mga variable ng input ng dereferencefunction ay ang mga sumusunod:

**didUrl**

Isang conformant [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) bilang isang [string](https://infra.spec.whatwg.org/#string) . Ito ang [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) upang i-dereference. Upang i-dereference ang isang [DID fragment ,](https://www.w3.org/TR/did-core/#dfn-did-fragments)*DAPAT* gamitin ang kumpletong [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) kasama ang [DID fragment .](https://www.w3.org/TR/did-core/#dfn-did-fragments)Ang input na ito ay *KINAKAILANGAN* .

TANDAAN : DID URL dereferencer patterns

Bagama't may bisa para sa anuman didUrlna maipasa sa isang DID URL dereferencer, ang mga tagapagpatupad ay inaasahang sumangguni sa [ [DID-RESOLUTION](https://www.w3.org/TR/did-core/#bib-did-resolution) ] upang higit na maunawaan ang mga karaniwang pattern para sa kung paano inaasahang made-dereference ang isang [DID URL .](https://www.w3.org/TR/did-core/#dfn-did-urls)

**dereferencingOptions**

Isang [istruktura ng metadata](https://www.w3.org/TR/did-core/#metadata-structure) na binubuo ng mga opsyon sa pag-input sa dereferencefunction bilang karagdagan sa didUrlsarili nito. Ang mga katangiang tinukoy ng pagtutukoy na ito ay nasa[7.2.1DID URL Dereferencing Options](https://www.w3.org/TR/did-core/#did-url-dereferencing-options) . Ang input na ito ay *KINAKAILANGAN , ngunit MAAARING* walang laman ang istraktura .

Ang function na ito ay nagbabalik ng maramihang mga halaga, at walang mga limitasyon na inilalagay sa kung paano ibinabalik ang mga halagang ito nang magkasama. Ang mga return value ng dereferenceinclude dereferencingMetadata, contentStream, at contentMetadata:

**dereferencingMetadata**

Isang [istruktura ng metadata](https://www.w3.org/TR/did-core/" \l "metadata-structure) na binubuo ng mga halagang nauugnay sa mga resulta ng proseso ng pagtukoy sa [URL ng DID](https://www.w3.org/TR/did-core/#dfn-did-url-dereferencing) . Ang istrakturang ito ay *KINAKAILANGAN* , at sa kaso ng isang error sa proseso ng dereferencing, *HINDI ito DAPAT* na walang laman. Ang mga katangiang tinukoy ng pagtutukoy na ito ay nasa[7.2.2DID URL Dereferencing Metadata](https://www.w3.org/TR/did-core/#did-url-dereferencing-metadata) . Kung hindi matagumpay ang dereferencing, *DAPAT* maglaman ang istrukturang ito ng errorproperty na naglalarawan sa error.

**contentStream**

Kung dereferencingtinawag at matagumpay ang function, *DAPAT* itong maglaman ng [mapagkukunan](https://www.w3.org/TR/did-core/" \l "dfn-resources) na tumutugma sa [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) . Ang contentStream *MAY* ay isang [mapagkukunan](https://www.w3.org/TR/did-core/" \l "dfn-resources) tulad ng isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) na maaaring i-serialize sa isa sa mga conformant na [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) , isang [Paraan ng Pag-verify](https://www.w3.org/TR/did-core/" \l "verification-methods) , isang [serbisyo](https://www.w3.org/TR/did-core/" \l "services) , o anumang iba pang format ng mapagkukunan na maaaring matukoy sa pamamagitan ng Uri ng Media at makuha sa pamamagitan ng proseso ng paglutas. Kung hindi matagumpay ang dereferencing, *DAPAT* walang laman ang value na ito.

**contentMetadata**

Kung matagumpay ang dereferencing, *DAPAT* itong [metadata structure](https://www.w3.org/TR/did-core/#metadata-structure) , ngunit *MAAARING* walang laman ang structure. Ang istrukturang ito ay naglalaman ng metadata tungkol sa contentStream. Kung ang contentStream ay isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) , *DAPAT* itong isang [didDocumentMetadata](https://www.w3.org/TR/did-core/" \l "dfn-diddocumentmetadata) na istraktura tulad ng inilarawan sa [DID Resolution](https://www.w3.org/TR/did-core/#dfn-did-resolution) . Kung ang dereferencing ay hindi matagumpay, ang output na ito ay *DAPAT* na isang walang laman na [istraktura ng metadata](https://www.w3.org/TR/did-core/" \l "metadata-structure) .

Ang pagsunod sa mga pagpapatupad ng [DID URL dereferencing ay](https://www.w3.org/TR/did-core/#dfn-did-url-dereferencing) hindi nagbabago sa lagda ng mga function na ito sa anumang paraan. Maaaring i-map ng mga pagpapatupad ng [DID URL dereferencing](https://www.w3.org/TR/did-core/#dfn-did-url-dereferencing)dereference ang function sa isang internal na function na partikular sa pamamaraan upang maisagawa ang aktwal na proseso ng pagde- [dereferencing ng DID URL](https://www.w3.org/TR/did-core/#dfn-did-url-dereferencing) . Maaaring ipatupad at ilantad ng [DID URL dereferencing](https://www.w3.org/TR/did-core/#dfn-did-url-dereferencing)dereference ang mga karagdagang function na may iba't ibang lagda bilang karagdagan sa function na tinukoy dito.

#### 7.2.1DID URL Dereferencing Options

Ang mga posibleng pag-aari sa loob ng istrukturang ito at ang kanilang mga posibleng halaga ay DAPAT na mairehistro sa DID Specification Registries [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ]. Tinutukoy ng detalyeng ito ang mga sumusunod na karaniwang katangian para sa mga opsyon sa dereferencing:

**tanggapin**

Ang Uri ng Media na mas gusto ng tumatawag para sa contentStream. DAPAT ipahayag ang Uri ng Media bilang isang [ASCII string](https://infra.spec.whatwg.org/#ascii-string) . DAPAT gamitin ng pagpapatupad ng [DID URL dereferencing](https://www.w3.org/TR/did-core/#dfn-did-url-dereferencing) ang value na ito upang matukoy ang representasyong [nakapaloob](https://www.w3.org/TR/did-core/" \l "dfn-representations) sa ibinalik na halaga kung sinusuportahan at available ang naturang [representasyon .](https://www.w3.org/TR/did-core/" \l "dfn-representations)contentType

#### 7.2.2DID URL Dereferencing Metadata

Ang mga posibleng pag-aari sa loob ng istrukturang ito at ang mga posibleng halaga nito ay nakarehistro sa DID Specification Registry [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ]. Tinutukoy ng detalyeng ito ang mga sumusunod na karaniwang katangian.

**uri ng nilalaman**

Ang Uri ng Media ng ibinalik ay contentStream DAPAT na ipahayag gamit ang property na ito kung matagumpay ang dereferencing. DAPAT ipahayag ang halaga ng Uri ng Media bilang isang [ASCII string](https://infra.spec.whatwg.org/#ascii-string) .

**pagkakamali**

Ang error code mula sa proseso ng dereferencing. KINAKAILANGAN ang property na ito kapag may error sa proseso ng dereferencing. Ang halaga ng property na ito ay DAPAT na iisang keyword na ipinahayag bilang [ASCII string](https://infra.spec.whatwg.org/#ascii-string) . Ang mga posibleng value ng property ng field na ito ay DAPAT na nakarehistro sa DID Specification Registry [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ]. Tinutukoy ng detalyeng ito ang mga sumusunod na karaniwang halaga ng error:

**invalidDidUrl**

Ang [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) na ibinigay sa [DID URL dereferencing](https://www.w3.org/TR/did-core/#dfn-did-url-dereferencing) function ay hindi sumusunod sa wastong syntax. (Tingnan[3.2DID URL Syntax](https://www.w3.org/TR/did-core/#did-url-syntax) .)

**hindi mahanap**

Hindi mahanap ng [DID URL dereferencer](https://www.w3.org/TR/did-core/#dfn-did-url-dereferencers) ang contentStreamresulta mula sa kahilingang ito sa dereferencing.

### **7.3Istraktura ng Metadata**

Ang input at output metadata ay kadalasang kasama sa panahon ng [DID Resolution](https://www.w3.org/TR/did-core/#dfn-did-resolution) , [DID URL dereferencing](https://www.w3.org/TR/did-core/#dfn-did-url-dereferencing) , at iba pang mga prosesong nauugnay sa DID. Ang istraktura na ginamit upang ipaalam ang metadata na ito ay DAPAT na isang [mapa](https://infra.spec.whatwg.org/" \l "maps) ng mga katangian. Ang bawat pangalan ng property ay DAPAT na isang [string](https://infra.spec.whatwg.org/#string) . Ang bawat value ng property ay DAPAT na isang [string](https://infra.spec.whatwg.org/#string) , [mapa](https://infra.spec.whatwg.org/" \l "maps) , [list](https://infra.spec.whatwg.org/#list) , [set](https://infra.spec.whatwg.org/#ordered-set) , [boolean](https://infra.spec.whatwg.org/" \l "boolean) , o [null](https://infra.spec.whatwg.org/#nulls) . Ang mga halaga sa loob ng anumang kumplikadong istruktura ng data gaya ng mga mapa at listahan ay DAPATmaging isa rin sa mga uri ng data na ito. Dapat tukuyin ng lahat ng mga kahulugan ng property ng metadata na nakarehistro sa DID Specification Registry [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ] ang uri ng halaga, kabilang ang anumang karagdagang mga format o paghihigpit sa value na iyon (halimbawa, isang string na naka-format bilang petsa o bilang decimal integer). Inirerekomenda na ang mga kahulugan ng ari-arian ay gumagamit ng mga string para sa mga halaga. DAPAT maging serializable ang buong istraktura ng metadata ayon sa mga [panuntunan ng serialization ng JSON](https://infra.spec.whatwg.org/" \l "serialize-an-infra-value-to-json-bytes) sa detalye ng [ [INFRA](https://www.w3.org/TR/did-core/#bib-infra) ]. MAAARING i-serialize ng mga pagpapatupad ang istruktura ng metadata sa iba pang mga format ng data.

Ang lahat ng pagpapatupad ng mga function na gumagamit ng mga istruktura ng metadata bilang input o output ay ganap na makakatawan sa lahat ng mga uri ng data na inilalarawan dito sa isang tiyak na paraan. Dahil ang mga input at output na gumagamit ng mga istruktura ng metadata ay tinukoy sa mga tuntunin ng mga uri ng data at hindi ang kanilang serialization, ang paraan para sa [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) ay panloob sa pagpapatupad ng function at wala sa saklaw ng detalyeng ito.

Ang sumusunod na halimbawa ay nagpapakita ng JSON-encoded metadata structure na maaaring gamitin bilang [DID resolution input metadata](https://www.w3.org/TR/did-core/#did-resolution-options) .

[HALIMBAWA24](https://www.w3.org/TR/did-core/#example-json-encoded-did-resolution-input-metadata-example): Halimbawa ng metadata ng input ng metadata ng input ng resolution ng JSON na naka-encode

{

"accept": "application/did+ld+json"

}

Ang halimbawang ito ay tumutugma sa isang istruktura ng metadata ng sumusunod na format:

[HALIMBAWA25](https://www.w3.org/TR/did-core/#example-did-resolution-input-metadata-example): Halimbawa ng metadata ng pag-input ng DID resolution

«[

"accept" → "application/did+ld+json"

]»

Ang susunod na halimbawa ay nagpapakita ng JSON-encoded metadata structure na maaaring gamitin bilang [DID resolution metadata](https://www.w3.org/TR/did-core/#did-resolution-options) kung ang isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay hindi nahanap.

[HALIMBAWA26](https://www.w3.org/TR/did-core/#example-json-encoded-did-resolution-metadata-example): Halimbawa ng metadata ng resolution ng DID na naka-encode ng JSON

{

"error": "notFound"

}

Ang halimbawang ito ay tumutugma sa isang istruktura ng metadata ng sumusunod na format:

[HALIMBAWA27](https://www.w3.org/TR/did-core/#example-did-resolution-metadata-example): Halimbawa ng metadata ng paglutas ng DID

«[

"error" → "notFound"

]»

Ang susunod na halimbawa ay nagpapakita ng JSON-encoded metadata structure na maaaring gamitin bilang [DID document metadata](https://www.w3.org/TR/did-core/#did-document-metadata) upang ilarawan ang mga timestamp na nauugnay sa [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) .

[HALIMBAWA28](https://www.w3.org/TR/did-core/#example-json-encoded-did-document-metadata-example): Halimbawa ng metadata ng dokumento ng DID na naka-encode ng JSON

{

"created": "2019-03-23T06:35:22Z",

"updated": "2023-08-10T13:40:06Z"

}

Ang halimbawang ito ay tumutugma sa isang istruktura ng metadata ng sumusunod na format:

[HALIMBAWA29](https://www.w3.org/TR/did-core/#example-did-document-metadata-example): Halimbawa ng metadata ng dokumento ng DID

«[

"created" → "2019-03-23T06:35:22Z",

"updated" → "2023-08-10T13:40:06Z"

]»

## 8.Paraan

Tinutukoy ng isang [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) kung paano napagtanto ng mga nagpapatupad ang mga tampok na inilarawan ng detalyeng ito. [Ang mga pamamaraan ng DID](https://www.w3.org/TR/did-core/#dfn-did-methods) ay kadalasang nauugnay sa isang partikular na [nabe-verify na registry ng data](https://www.w3.org/TR/did-core/#dfn-verifiable-data-registry) . Ang mga bagong [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ay tinukoy sa kanilang sariling mga detalye upang paganahin ang interoperability sa pagitan ng iba't ibang mga pagpapatupad ng parehong [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) .

Sa konsepto, ang ugnayan sa pagitan ng detalyeng ito at isang detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ay katulad ng ugnayan sa pagitan ng pangkalahatang detalye ng [URI](https://www.w3.org/TR/did-core/#dfn-uri) ng IETF [ [RFC3986](https://www.w3.org/TR/did-core/#bib-rfc3986) ] at isang partikular na [URI](https://www.w3.org/TR/did-core/#dfn-uri) scheme [ [IANA-URI-SCHEMES](https://www.w3.org/TR/did-core/#bib-iana-uri-schemes) ], gaya ng httpscheme [ [RFC7230](https://www.w3.org/TR/did-core/#bib-rfc7230) ]. Bilang karagdagan sa pagtukoy ng isang partikular na [scheme](https://www.w3.org/TR/did-core/#dfn-did-schemes) ng [DID](https://www.w3.org/TR/did-core/#dfn-did-methods) , tinutukoy din ng isang detalye ng pamamaraan ng DID ang mga mekanismo para sa paggawa, paglutas, pag-update, at pag-deactivate ng mga dokumento ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) at [DID](https://www.w3.org/TR/did-core/#dfn-did-documents) gamit ang isang partikular na uri ng [registry ng data na nabe](https://www.w3.org/TR/did-core/#dfn-verifiable-data-registry) -verify . Dinodokumento din nito ang lahat ng pagsasaalang-alang sa pagpapatupad na may kaugnayan sa[Mga DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) pati na rin ang Mga Pagsasaalang-alang sa Seguridad at Privacy.

Tinutukoy ng seksyong ito ang mga kinakailangan para sa pag-akda ng mga detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) .

### **8.1Syntax ng Pamamaraan**

Ang mga kinakailangan para sa lahat ng pagtutukoy ng [pamamaraan ng DID kapag tinutukoy ang Syntax ng DID na tukoy sa pamamaraan ay ang mga sumusunod:](https://www.w3.org/TR/did-core/" \l "dfn-did-methods)

1. DAPAT tukuyin ng isang detalye ng pamamaraan ng DID ang eksaktong isang scheme ng DID na tukoy sa pamamaraan [na](https://www.w3.org/TR/did-core/" \l "dfn-did-methods)[tinutukoy](https://www.w3.org/TR/did-core/#dfn-did-schemes) ng eksaktong isang pangalan ng pamamaraan na tinukoy ng panuntunan samethod-name[3.1DID Syntax](https://www.w3.org/TR/did-core/#did-syntax) .
2. DAPAT tukuyin ng detalye ng [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods)kung paano bumuo ng method-specific-idbahagi ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) .
3. DAPAT tukuyin ng detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ang pagiging sensitibo at normalisasyon ng halaga ng . method-specific-id
4. DAPAT natatangi ang method-specific-idvalue sa loob ng isang [DID method](https://www.w3.org/TR/did-core/#dfn-did-methods) . Ang halaga mismo ay maaaring natatangi sa buong mundo. method-specific-id
5. Ang anumang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na nabuo sa pamamagitan ng isang [DID na pamamaraan ay](https://www.w3.org/TR/did-core/#dfn-did-methods)DAPAT na kakaiba sa buong mundo.
6. Upang mabawasan ang mga pagkakataon ng mga method-namesalungatan, DAPAT na irehistro ang isang detalye ng [pamamaraan ng DID sa Mga Rehistro ng Detalye ng DID [](https://www.w3.org/TR/did-core/" \l "dfn-did-methods)[DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ].
7. MAAARING tumukoy ang isang [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ng maraming format. method-specific-id
8. Ang method-specific-idformat ay MAY may kasamang mga tutuldok. Ang paggamit ng mga tutuldok ay DAPAT sumunod sa syntactically sa method-specific-idtuntunin ng ABNF.
9. MAAARING tukuyin ng isang detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ang mga panuntunan ng ABNF para sa mga [path ng DID](https://www.w3.org/TR/did-core/#dfn-did-paths) na mas mahigpit kaysa sa mga pangkalahatang panuntunan sa [Path](https://www.w3.org/TR/did-core/#path) .
10. MAAARING tukuyin ng isang detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ang mga panuntunan ng ABNF para sa mga [query sa DID](https://www.w3.org/TR/did-core/#dfn-did-queries) na mas mahigpit kaysa sa mga pangkalahatang tuntunin sa seksyong ito.
11. MAAARING tukuyin ng isang detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ang mga panuntunan ng ABNF para sa mga [fragment ng DID](https://www.w3.org/TR/did-core/#dfn-did-fragments) na mas mahigpit kaysa sa mga pangkalahatang tuntunin sa seksyong ito.

TANDAAN : Mga colon sa method-specific-id

Ang kahulugan ng mga tutuldok sa method-specific-iday ganap na tukoy sa pamamaraan. Maaaring gamitin ang mga colon ng mga [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) para sa pagtatatag ng mga namespace na nahati ayon sa hierarchy, para sa pagtukoy ng mga partikular na pagkakataon o bahagi ng [rehistro ng nabe-verify na data](https://www.w3.org/TR/did-core/" \l "dfn-verifiable-data-registry) , o para sa iba pang mga layunin. Ang mga tagapagpatupad ay pinapayuhan na iwasang ipagpalagay ang anumang mga kahulugan o gawi na nauugnay sa isang colon na karaniwang naaangkop sa lahat ng mga [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) .

### **8.2Mga Operasyon ng Pamamaraan**

Ang mga kinakailangan para sa lahat ng mga detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) kapag tinutukoy ang mga pagpapatakbo ng pamamaraan ay ang mga sumusunod:

1. DAPAT tukuyin ng detalye [ng paraan ng DID kung paano](https://www.w3.org/TR/did-core/#dfn-did-methods)isinasagawa ang awtorisasyon upang maisagawa ang lahat ng operasyon, kabilang ang anumang kinakailangang proseso ng cryptographic.
2. DAPAT tukuyin ng isang detalye ng paraan ng DID kung paano lumikha ang [isang](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) DID [controller ng isang](https://www.w3.org/TR/did-core/#dfn-did-controllers)[DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) at ang nauugnay [na dokumentong DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) nito .
3. DAPAT tukuyin ng isang detalye ng paraan ng DID kung paano gumagamit ng [DID](https://www.w3.org/TR/did-core/#dfn-did-methods)[ang](https://www.w3.org/TR/did-core/#dfn-did-resolvers) isang solver ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) upang malutas ang isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) , kabilang ang kung paano mabe-verify ng solver ng [DID](https://www.w3.org/TR/did-core/#dfn-did-resolvers) ang pagiging tunay ng tugon.
4. DAPAT tukuyin ng isang detalye ng paraan ng DID kung ano ang bumubuo sa isang pag-update sa isang dokumento ng [DID](https://www.w3.org/TR/did-core/#dfn-did-methods)[at](https://www.w3.org/TR/did-core/#dfn-did-documents) kung paano maaaring i -update ng isang [DID controller ang isang](https://www.w3.org/TR/did-core/#dfn-did-controllers)[dokumento ng DID](https://www.w3.org/TR/did-core/#dfn-did-documents)o sabihin na ang mga pag-update ay hindi posible.
5. DAPAT tukuyin ng detalye ng [pamamaraan](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ng DID kung paano maaaring i -deactivate ng [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) ang isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers)o sabihin na hindi posible ang pag-deactivate.

Ang awtoridad ng isang partido na nagsasagawa ng awtorisasyon upang isagawa ang mga operasyon ay partikular sa isang [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) . Halimbawa, ang isang [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ay maaaring -

* gamitin ang ari- [controller](https://www.w3.org/TR/did-core/" \l "dfn-controller)arian.
* gamitin ang mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) na nakalista sa ilalim ng [authentication](https://www.w3.org/TR/did-core/#dfn-authentication).
* gumamit ng iba pang mga konstruksyon sa [DID Document](https://www.w3.org/TR/did-core/#dfn-did-documents) tulad ng [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) na tinukoy sa pamamagitan ng [capabilityInvocation](https://www.w3.org/TR/did-core/" \l "dfn-capabilityinvocation) [relasyon sa pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship) .
* hindi gamitin ang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) para sa desisyong ito, at sa halip ay umaasa sa isang out-of-band na mekanismo.

### **8.3Mga Kinakailangan sa Seguridad**

Ang mga kinakailangan para sa lahat ng mga detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) kapag nag-akda ng seksyong Mga Pagsasaalang-alang sa Seguridad ay ang mga sumusunod:

1. DAPAT sundin ng mga detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ang lahat ng mga alituntunin at normatibong wika na ibinigay sa RFC3552 [: Pagsusulat ng Mga Seksyon ng Mga Pagsasaalang-alang sa Seguridad](https://www.rfc-editor.org/rfc/rfc3552#section-5) para sa mga pagpapatakbo ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na tinukoy sa detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) .
2. DAPAT idokumento ng seksyong Mga Pagsasaalang-alang sa Seguridad ang mga sumusunod na paraan ng pag-atake para sa mga pagpapatakbo ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na tinukoy sa detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) : eavesdropping, replay, pagpasok ng mensahe, pagtanggal, pagbabago, pagtanggi sa serbisyo, [amplification](https://www.w3.org/TR/did-core/#dfn-amplification) , at man-in-the-middle. DAPAT ding idokumento ang iba pang kilalang paraan ng pag-atake .
3. DAPAT talakayin ng seksyong Mga Pagsasaalang-alang sa Seguridad ang mga natitirang panganib, gaya ng mga panganib mula sa kompromiso sa isang nauugnay na protocol, maling pagpapatupad, o cipher pagkatapos na mai-deploy ang pagbabanta ng pagbabanta.
4. Ang seksyong Mga Pagsasaalang-alang sa Seguridad ay DAPAT magbigay ng proteksyon sa integridad at pagpapatunay ng pag-update para sa lahat ng operasyong kinakailangan ng Seksyon[8.2Mga Operasyon ng Pamamaraan](https://www.w3.org/TR/did-core/#method-operations) .
5. Kung kasangkot ang pagpapatunay, partikular ang pagpapatunay ng user-host, DAPAT na malinaw na naidokumento ang mga katangian ng seguridad ng paraan ng pagpapatunay.
6. DAPAT talakayin ng seksyong Mga Pagsasaalang-alang sa Seguridad ang mekanismo ng patakaran kung saan ang mga [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay napatunayang natatanging itinalaga.
7. DAPAT talakayin ang pagpapatunay ng endpoint na tukoy sa pamamaraan . Kung saan ang mga [pamamaraan](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ng DID ay gumagamit ng mga [DLT](https://www.w3.org/TR/did-core/#dfn-distributed-ledger-technology) na may iba't ibang topology ng network, kung minsan ay inaalok bilang light node o [*thin client*](https://en.bitcoin.it/wiki/Thin_Client_Security) na mga pagpapatupad upang mabawasan ang mga kinakailangang mapagkukunan ng computing, DAPAT talakayin ang mga pagpapalagay sa seguridad ng topology na magagamit sa mga pagpapatupad ng [pamamaraan ng DID .](https://www.w3.org/TR/did-core/" \l "dfn-did-methods)
8. Kung isinasama ng isang protocol ang mga mekanismo ng proteksyon ng cryptographic, DAPAT malinaw na ipahiwatig ng detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) kung aling mga bahagi ng data ang pinoprotektahan at sa pamamagitan ng kung anong mga proteksyon, at DAPAT itong magbigay ng indikasyon ng mga uri ng pag-atake kung saan ang proteksyon ng cryptographic ay madaling kapitan. Ang ilang mga halimbawa ay integridad lamang, pagiging kumpidensyal, at pagpapatunay ng endpoint.
9. DAPAT malinaw na lagyan ng label ang data na dapat panatilihing lihim (keying material, random seeds, at iba pa) .
10. DAPAT ipaliwanag at tukuyin ng mga detalye ng [paraan ng DID ang pagpapatupad ng mga lagda sa mga](https://www.w3.org/TR/did-core/" \l "dfn-did-methods)[dokumento ng DID](https://www.w3.org/TR/did-core/#dfn-did-documents) , kung naaangkop.
11. Kung saan ang mga [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ay gumagamit ng mga mapagkukunan ng peer-to-peer na computing, tulad ng lahat ng kilalang [DLT ,](https://www.w3.org/TR/did-core/#dfn-distributed-ledger-technology)DAPAT talakayin ang mga inaasahang pasanin ng mga mapagkukunang iyon kaugnay ng pagtanggi sa serbisyo.
12. [Mga pamamaraan ng DID](https://www.w3.org/TR/did-core/#dfn-did-methods) na nagpapakilala ng mga bagong uri ng [serbisyo](https://www.w3.org/TR/did-core/" \l "dfn-service) sa pagpapatotoo , tulad ng inilarawan sa[5.4Mga Serbisyo](https://www.w3.org/TR/did-core/#services) , DAPAT isaalang-alang ang mga kinakailangan sa seguridad ng sinusuportahang protocol ng pagpapatunay.

### **8.4Mga Kinakailangan sa Privacy**

Ang mga kinakailangan para sa lahat ng mga detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) kapag nag-author ng seksyong Mga Pagsasaalang- alang sa Privacy ay:

1. DAPAT talakayin ng seksyong Mga Pagsasaalang-alang sa Privacy ng detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ang anumang subseksiyon ng Seksyon 5 ng [ [RFC6973](https://www.w3.org/TR/did-core/#bib-rfc6973) ] na maaaring ilapat sa paraang partikular sa pamamaraan. Ang mga subsection na isasaalang-alang ay: pagsubaybay, naka-imbak na kompromiso ng data, hindi hinihinging trapiko, maling pag-atribusyon, ugnayan, pagkakakilanlan, pangalawang paggamit, pagsisiwalat, at pagbubukod.

## 9.Mga Pagsasaalang-alang sa Seguridad

Ang seksyong ito ay hindi normatibo.

Naglalaman ang seksyong ito ng iba't ibang pagsasaalang-alang sa seguridad na pinapayuhan ng mga taong gumagamit ng Mga Desentralisadong Identifier na isaalang-alang bago i-deploy ang teknolohiyang ito sa isang setting ng produksyon. [Ang mga DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay idinisenyo upang gumana sa ilalim ng modelo ng pagbabanta na ginagamit ng maraming pamantayan ng IETF at nakadokumento sa [ [RFC3552](https://www.w3.org/TR/did-core/#bib-rfc3552) ]. Ang seksyong ito ay nagpapaliwanag ng ilang mga pagsasaalang-alang sa [ [RFC3552](https://www.w3.org/TR/did-core/#bib-rfc3552) ], pati na rin ang iba pang mga pagsasaalang-alang na natatangi sa arkitektura ng [DID .](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers)

### **9.1Pagpili ng DID Resolvers**

Ang DID Specification Registries [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ] ay naglalaman ng isang impormasyong listahan ng mga pangalan ng [DID method](https://www.w3.org/TR/did-core/#dfn-did-methods) at ang kanilang kaukulang mga detalye ng [DID method](https://www.w3.org/TR/did-core/#dfn-did-methods) . Kailangang tandaan ng mga nagpapatupad na walang sentral na awtoridad na mag-utos kung aling detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ang gagamitin sa anumang partikular na pangalan [ng pamamaraan ng DID](https://www.w3.org/TR/did-core/#dfn-did-methods) . Kung may pagdududa kung ang isang partikular na [DID resolver](https://www.w3.org/TR/did-core/#dfn-did-resolvers) ay nagpapatupad o hindi ng isang [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) , ang DID Specification Registries ay maaaring gamitin upang hanapin ang nakarehistrong detalye at gumawa ng matalinong desisyon tungkol sa kung aling [DID resolver](https://www.w3.org/TR/did-core/#dfn-did-resolvers) ang gagamitin na pagpapatupad.

### **9.2Pagpapatunay ng Kontrol at Pagbubuklod**

Ang pagbubuklod ng isang entity sa digital world o ang pisikal na mundo sa isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) , sa isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) , o sa cryptographic na materyal ay nangangailangan, ang paggamit ng mga protocol ng seguridad na pinag-isipan ng detalyeng ito. Ang mga sumusunod na seksyon ay naglalarawan ng ilang posibleng mga sitwasyon at kung paano maaaring patunayan ng isang entity na naroroon ang kontrol sa isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) o isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) para sa mga layunin ng pagpapatunay o awtorisasyon.

#### Pagpapatunay ng Kontrol ng isang DID at/o DID na Dokumento

Ang pagpapatunay ng kontrol sa isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) at/o isang [DID na Dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) ay kapaki-pakinabang kapag nag-a-update alinman sa isang [nabe-verify na registry ng data](https://www.w3.org/TR/did-core/#dfn-verifiable-data-registry) o nagpapatotoo sa mga malalayong system. Ang mga cryptographic na digital na lagda at mga [nabe-verify na timestamp](https://www.w3.org/TR/did-core/#dfn-verifiable-timestamp) ay nagbibigay -daan sa ilang partikular na protocol ng seguridad na nauugnay sa mga [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) upang maging cryptographically verifiable. Para sa mga layuning ito, tinutukoy ng detalyeng ito ang mga kapaki-pakinabang [na ugnayan sa pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship) sa[5.3.1Pagpapatunay](https://www.w3.org/TR/did-core/#authentication) at[5.3.4Panawagan sa Kakayahang](https://www.w3.org/TR/did-core/#capability-invocation) . Ang lihim na materyal na cryptographic na nauugnay sa mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ay maaaring gamitin upang bumuo ng isang cryptographic na digital na lagda bilang bahagi ng isang authentication o authorization security protocol.

TANDAAN : Mga nilagdaang dokumento ng DID

Ang ilang mga [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ay nagpapahintulot sa mga digital na lagda at iba pang mga patunay na maisama sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) o a[7.3Istraktura ng Metadata](https://www.w3.org/TR/did-core/#metadata-structure) . Gayunpaman, ang gayong mga patunay sa kanilang sarili ay hindi kinakailangang patunayan ang kontrol sa isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) , o ginagarantiyahan na ang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) ay ang tama para sa [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) . Upang makuha ang tamang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) at mapatunayan ang kontrol sa isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) , kinakailangan na gawin ang proseso ng [paglutas ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-resolution) gaya ng tinukoy ng [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) .

#### Nagbubuklod sa Pisikal na Pagkakakilanlan

Ang isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) at [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) ay hindi likas na nagdadala ng anumang [personal na data](https://en.wikipedia.org/wiki/Personal_data) at ito ay lubos na pinapayuhan na ang mga hindi pampublikong entity ay hindi mag-publish ng personal na data sa [mga dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) .

Maaari itong maging kapaki-pakinabang upang ipahayag ang isang pagbubuklod ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) sa pisikal na pagkakakilanlan ng isang tao o organisasyon sa paraang mapapatunayang iginiit ng isang pinagkakatiwalaang awtoridad, gaya ng isang pamahalaan. Ang pagtutukoy na ito ay nagbibigay ng[5.3.2Relasyon sa](https://www.w3.org/TR/did-core/#assertion)[pagpapatunay](https://www.w3.org/TR/did-core/#dfn-verification-relationship) ng paninindigan para sa mga layuning ito. Maaaring paganahin ng feature na ito ang mga pakikipag-ugnayan na pribado at maaaring ituring na legal na maipapatupad sa ilalim ng isa o higit pang mga hurisdiksyon; ang pagtatatag ng gayong mga pagbubuklod ay dapat na maingat na balanse laban sa mga pagsasaalang-alang sa privacy (tingnan [10.Mga Pagsasaalang- alang sa Privacy](https://www.w3.org/TR/did-core/#privacy-considerations) ).

Ang proseso ng pagbubuklod ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) sa isang bagay sa pisikal na mundo, tulad ng isang tao o isang organisasyon — halimbawa, sa pamamagitan ng paggamit ng mga [nabe-verify na kredensyal](https://www.w3.org/TR/did-core/#dfn-verifiable-credentials) na may parehong paksa tulad ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na iyon — ay pinag-iisipan ng detalyeng ito at higit pang tinukoy sa Modelo ng Data ng Mga Na-verify na Kredensyal [ [VC-DATA-MODEL](https://www.w3.org/TR/did-core/#bib-vc-data-model) ].

### **9.3Mga Endpoint ng Serbisyo sa Pagpapatunay**

Kung ang isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay nag- publish ng isang [serbisyo](https://www.w3.org/TR/did-core/" \l "dfn-service) na nilayon para sa pagpapatunay o awtorisasyon ng [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) (tingnan ang Seksyon[5.4Mga Serbisyo](https://www.w3.org/TR/did-core/#services) ), responsibilidad ng [service endpoint](https://www.w3.org/TR/did-core/#dfn-service-endpoints) provider, paksa, o humihiling na partido na sumunod sa mga kinakailangan ng mga protocol ng pagpapatunay na sinusuportahan sa [endpoint ng serbisyong](https://www.w3.org/TR/did-core/#dfn-service-endpoints) iyon .

### **9.4Non-Repudiation**

Ang hindi pagtanggi sa mga pag-update ng [dokumento ng DID at DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents)[ay](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) sinusuportahan kung:

* Sinusuportahan ng nabe-verify na [registry ng data](https://www.w3.org/TR/did-core/#dfn-verifiable-data-registry) ang [mga nabe-verify na timestamp](https://www.w3.org/TR/did-core/" \l "dfn-verifiable-timestamp) . Tingnan mo[7.1.3Metadata ng Dokumento ng DID](https://www.w3.org/TR/did-core/#did-document-metadata) para sa karagdagang impormasyon sa mga kapaki-pakinabang na timestamp na magagamit sa proseso ng [paglutas ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-resolution) .
* Ang paksa ay sinusubaybayan para sa mga hindi awtorisadong pag-update gaya ng ipinaliwanag sa [9.5Notification ng DID Document Changes](https://www.w3.org/TR/did-core/#notification-of-did-document-changes) .
* Ang paksa ay nagkaroon ng sapat na pagkakataon na ibalik ang mga nakakahamak na update ayon sa mekanismo ng pahintulot para sa [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) .

### **9.5Abiso ng mga Pagbabago sa Dokumento ng DID**

Ang isang pagpapagaan laban sa mga hindi awtorisadong pagbabago sa isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay ang pagsubaybay at aktibong pag-abiso sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) kapag may mga pagbabago. Ito ay kahalintulad sa pagtulong na maiwasan ang pagkuha ng account sa mga nakasanayang username/password account sa pamamagitan ng pagpapadala ng mga notification sa pag-reset ng password sa mga email address na nasa file.

Sa kaso ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) , walang tagapamagitan na registrar o provider ng account upang bumuo ng mga naturang notification. Gayunpaman, kung direktang sinusuportahan ng [nabe-verify na registry ng data](https://www.w3.org/TR/did-core/#dfn-verifiable-data-registry) kung saan nakarehistro ang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) , maaaring mag-alok ng serbisyo ng subscription sa mga [controller ng DID](https://www.w3.org/TR/did-core/#dfn-did-controllers) . Maaaring direktang ipadala ang mga notification sa mga nauugnay na [endpoint ng serbisyo](https://www.w3.org/TR/did-core/#dfn-service-endpoints) na nakalista sa isang umiiral nang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) .

Kung pipiliin ng isang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) na umasa sa isang third-party na serbisyo sa pagsubaybay (maliban sa [nabe-verify na registry ng data](https://www.w3.org/TR/did-core/#dfn-verifiable-data-registry) mismo), nagpapakilala ito ng isa pang vector ng pag-atake.

### **9.6Key at Signature Expiration**

Sa isang [desentralisadong identifier](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers) na arkitektura, maaaring walang mga sentralisadong awtoridad na magpapatupad ng mga patakaran sa pag-expire ng cryptographic na materyal o cryptographic na digital signature. Samakatuwid, ito ay sa pagsuporta sa software tulad ng mga [DID resolver](https://www.w3.org/TR/did-core/#dfn-did-resolvers) at verification library na humihiling sa mga partido na nagpapatunay na ang cryptographic na materyal ay hindi nag-expire sa oras na ginamit ang mga ito. Ang mga humihiling na partido ay maaaring gumamit ng sarili nilang mga patakaran sa pag-expire bilang karagdagan sa mga input sa kanilang mga proseso ng pag-verify. Halimbawa, ang ilang humihiling na partido ay maaaring tumanggap ng mga pagpapatotoo mula sa nakalipas na limang minuto, habang ang iba na may access sa mataas na katumpakan na mga pinagmumulan ng oras ay maaaring mangailangan ng mga pagpapatotoo na mamarkahan ng oras sa loob ng huling 500 millisecond.

May ilang humihiling na partido na may mga lehitimong pangangailangan na palawigin ang paggamit ng expired na cryptographic na materyal, gaya ng pag-verify ng legacy na cryptographic na mga digital na lagda. Sa mga sitwasyong ito, maaaring atasan ng humihiling na partido ang kanilang software sa pag-verify na huwag pansinin ang pag-expire ng cryptographic key material o tukuyin kung nag-expire na ang cryptographic key material noong ginamit ito.

### **9.7Pag-ikot ng Paraan ng Pag-verify**

Ang pag-ikot ay isang proseso ng pamamahala na nagbibigay-daan sa lihim na cryptographic na materyal na nauugnay sa isang umiiral na [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) na ma-deactivate o masira kapag may naidagdag na bagong [paraan ng pag-verify sa](https://www.w3.org/TR/did-core/" \l "dfn-verification-method)[dokumento ng DID](https://www.w3.org/TR/did-core/#dfn-did-documents) . Sa pagpapatuloy, anumang mga bagong patunay na mabubuo sana ng isang [controller](https://www.w3.org/TR/did-core/#dfn-controller) gamit ang lumang lihim na materyal na cryptographic ay maaari na ngayong mabuo gamit ang bagong materyal na cryptographic at mabe-verify gamit ang bagong [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) .

Ang pag-ikot ay isang kapaki-pakinabang na mekanismo para sa pagprotekta laban sa kompromiso sa paraan ng pag-verify, dahil ang madalas na pag-ikot ng isang paraan ng pag-verify ng controller ay nagpapababa sa halaga ng isang nakompromisong paraan ng pag-verify sa isang umaatake. Ang pagsasagawa ng pagbawi kaagad pagkatapos ng pag-ikot ay kapaki-pakinabang para sa mga paraan ng pag-verify na itinalaga ng controller para sa panandaliang pag-verify, gaya ng mga kasangkot sa pag-encrypt ng mga mensahe at pagpapatotoo.

Maaaring magamit ang mga sumusunod na pagsasaalang-alang kapag pinag-iisipan ang paggamit ng pag-ikot ng [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) :

* [Ang pag-ikot ng paraan ng pag-verify](https://www.w3.org/TR/did-core/#dfn-verification-method) ay isang aktibong hakbang sa seguridad.
* Karaniwang itinuturing na pinakamahusay na kasanayan ang regular na pagsasagawa ng pag-ikot ng [paraan ng pag-verify .](https://www.w3.org/TR/did-core/" \l "dfn-verification-method)
* Ang mga mas mataas na kapaligiran ng seguridad ay may posibilidad na gumamit ng mas madalas na pag-ikot ng paraan ng pag-verify.
* [Ang pag-ikot ng paraan ng pag-verify](https://www.w3.org/TR/did-core/#dfn-verification-method) ay nagpapakita lamang bilang mga pagbabago sa kasalukuyan o pinakabagong bersyon ng isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) .
* Kapag ang isang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ay naging aktibo sa mahabang panahon, o ginagamit para sa maraming mga operasyon, maaaring naisin ng isang controller na magsagawa ng pag-ikot.
* Ang madalas na pag-ikot ng isang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ay maaaring nakakadismaya para sa mga partidong napipilitang patuloy na mag-renew o mag-refresh ng mga nauugnay na kredensyal.
* Ang mga patunay o lagda na umaasa sa mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) na wala sa pinakabagong bersyon ng isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay hindi naaapektuhan ng pag-ikot. Sa mga kasong ito, maaaring mangailangan ng karagdagang impormasyon ang software sa pag-verify, tulad ng kung kailan inaasahang magiging wasto ang isang partikular na [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) pati na rin ang pag-access sa isang [registry ng data na nabe](https://www.w3.org/TR/did-core/#dfn-verifiable-data-registry) -verify na naglalaman ng makasaysayang tala, upang matukoy ang bisa ng patunay o lagda. Maaaring hindi available ang opsyong ito sa lahat [ng paraan ng DID](https://www.w3.org/TR/did-core/#dfn-did-methods) .
* Ang seksyon sa mga [pagpapatakbo ng pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "method-operations) ay tumutukoy sa mga pagpapatakbo ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na susuportahan ng isang detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) , kabilang ang pag- [update](https://www.w3.org/TR/did-core/#method-operations) na inaasahang gagamitin upang magsagawa ng pag-ikot ng [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) .
* Ang isang [controller](https://www.w3.org/TR/did-core/#dfn-controller) ay nagsasagawa ng pag-ikot kapag nagdagdag sila ng bagong [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) na nilalayong palitan ang isang umiiral na [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) pagkalipas ng ilang panahon.
* Hindi lahat [ng paraan ng DID ay](https://www.w3.org/TR/did-core/#dfn-did-methods) sumusuporta sa pag-ikot ng [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) .

### **9.8Paraan ng Pagpapatunay Pagbawi**

Ang pagbawi ay isang proseso ng pamamahala na nagbibigay-daan sa lihim na cryptographic na materyal na nauugnay sa isang umiiral na [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) na ma-deactivate upang hindi na ito maging isang wastong paraan ng paglikha ng mga bagong patunay ng mga digital na lagda.

Ang pagbawi ay isang kapaki-pakinabang na mekanismo para sa pagtugon sa isang kompromiso sa paraan ng pag-verify. Ang pagsasagawa ng pagbawi kaagad pagkatapos ng pag-ikot ay kapaki-pakinabang para sa mga paraan ng pag-verify na itinalaga ng controller para sa panandaliang pag-verify, gaya ng mga kasangkot sa pag-encrypt ng mga mensahe at pagpapatotoo.

Ang pagkompromiso sa mga lihim na nauugnay sa isang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ay nagbibigay-daan sa umaatake na gamitin ang mga ito ayon sa [kaugnayan sa pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship) na ipinahayag ng [controller](https://www.w3.org/TR/did-core/#dfn-controller) sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) , halimbawa, para sa pagpapatunay. Ang paggamit ng mga lihim ng umaatake ay maaaring hindi makilala mula sa paggamit ng lehitimong [controller](https://www.w3.org/TR/did-core/#did-controller) simula sa oras na nairehistro ang [paraan ng pag-verify , hanggang sa oras na ito ay binawi.](https://www.w3.org/TR/did-core/" \l "dfn-verification-method)

Maaaring magamit ang mga sumusunod na pagsasaalang-alang kapag pinag-iisipan ang paggamit ng pagbawi ng [paraan ng pag-verify :](https://www.w3.org/TR/did-core/" \l "dfn-verification-method)

* [Ang pagbawi ng paraan ng pag-verify](https://www.w3.org/TR/did-core/#dfn-verification-method) ay isang reaktibong hakbang sa seguridad.
* Ito ay itinuturing na isang pinakamahusay na kasanayan upang suportahan ang pangunahing pagbawi.
* Inaasahan na agad na bawiin ng isang controller ang anumang paraan [ng pag-](https://www.w3.org/TR/did-core/#dfn-controller)[verify](https://www.w3.org/TR/did-core/#dfn-verification-method) na kilalang nakompromiso.
* [Ang pagbawi ng paraan ng pag-verify](https://www.w3.org/TR/did-core/#dfn-verification-method) ay maaari lamang isama sa mga pagbabago sa pinakabagong bersyon ng isang [DID Document](https://www.w3.org/TR/did-core/#dfn-did-documents) ; hindi nito maaaring retroactive na isaayos ang mga nakaraang bersyon.
* Gaya ng inilarawan sa[5.2.1Materyal sa Pag-verify](https://www.w3.org/TR/did-core/#verification-material) , ang kawalan ng paraan ng pag-verify ay ang tanging paraan ng pagbawi na nalalapat sa lahat ng [Paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) na sumusuporta sa pagbawi.
* Kung ang isang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ay hindi na eksklusibong naa-access ng [controller](https://www.w3.org/TR/did-core/#dfn-controller) o mga partidong pinagkakatiwalaang kumilos sa ngalan ng [controller](https://www.w3.org/TR/did-core/#dfn-controller) , inaasahang agad itong bawiin upang mabawasan ang panganib ng mga kompromiso gaya ng pagbabalatkayo, pagnanakaw, at panloloko.
* Inaasahang mauunawaan ang pagbawi bilang isang [controller](https://www.w3.org/TR/did-core/#dfn-controller) na nagpapahayag na ang mga patunay o lagda na nauugnay sa isang binawi na [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) na ginawa pagkatapos ng pagbawi nito ay dapat ituring na hindi wasto. Maaari rin itong magpahiwatig ng pag-aalala na ang mga umiiral na patunay o lagda ay maaaring nilikha ng isang umaatake, ngunit hindi ito ang kaso. Gayunpaman, maaari pa ring piliin ng mga verifier na tanggapin o tanggihan ang anumang naturang mga patunay o lagda sa kanilang sariling paghuhusga.
* Ang seksyon sa mga [pagpapatakbo ng pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "method-operations) ay tumutukoy sa mga pagpapatakbo ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na susuportahan ng isang detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) , kabilang ang pag- [update](https://www.w3.org/TR/did-core/#method-operations) at pag- [deactivate](https://www.w3.org/TR/did-core/#method-operations) , na maaaring gamitin upang alisin ang isang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) mula sa isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) .
* Hindi lahat [ng paraan ng DID ay](https://www.w3.org/TR/did-core/#dfn-did-methods) sumusuporta sa pagbawi ng [paraan ng pag-verify .](https://www.w3.org/TR/did-core/" \l "dfn-verification-method)
* Kahit na [mayroong paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) sa isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) , maaaring gamitin ang karagdagang impormasyon, tulad ng isang sertipiko ng pagbawi ng pampublikong key, o isang listahan ng panlabas na payagan o pagtanggi, upang matukoy kung ang isang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ay binawi.
* Ang pang-araw-araw na pagpapatakbo ng anumang software na umaasa sa isang nakompromisong [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) , gaya ng operating system, antivirus, o endpoint protection software ng isang indibidwal, ay maaaring maapektuhan kapag ang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ay binawi sa publiko.

#### Mga Semantika ng Pagpapawalang-bisa

Bagama't maaaring piliin ng mga verifier na huwag tumanggap ng mga patunay o pirma mula sa isang binawi na paraan ng pag-verify, ang pag-alam kung ang isang pag-verify ay ginawa gamit ang isang binawi na [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ay mas nakakalito kaysa sa tila. Ang ilang mga [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ay nagbibigay ng kakayahang tumingin pabalik sa estado ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) sa isang punto ng oras, o sa isang partikular na bersyon ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) . Kapag ang naturang feature ay pinagsama sa isang mapagkakatiwalaang paraan upang matukoy ang oras o bersyon ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na umiral noong ginawa ang isang pahayag na nabe-verify sa pamamagitan ng cryptographic, hindi inaalis ng pagbawi ang pahayag na iyon. Ito ay maaaring maging batayan para sa paggamit ng [mga DID](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers) upang gumawa ng mga may-bisang pangako; halimbawa, upang pumirma sa isang mortgage.

Kung ang mga kundisyong ito ay natutugunan, ang pagbawi ay hindi retroaktibo; ito ay nagpapawalang-bisa lamang sa hinaharap na paggamit ng pamamaraan.

Gayunpaman, upang maging ligtas ang mga naturang semantika, ang pangalawang kundisyon — isang kakayahang malaman kung ano ang estado ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) noong panahong ginawa ang paggigiit — ay inaasahang mailalapat. Kung wala ang garantiyang iyon, maaaring matuklasan ng isang tao ang isang binawi na susi at gamitin ito para gumawa ng mga pahayag na nabe-verify sa pamamagitan ng cryptographic na may simulate na petsa sa nakaraan.

Pinapayagan lamang ng ilang [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ang pagkuha ng kasalukuyang estado ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) . Kapag ito ay totoo, o kapag ang estado ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) sa oras ng isang cryptographically verifiable na pahayag ay hindi mapagkakatiwalaang matukoy, kung gayon ang tanging ligtas na kurso ay ang hindi payagan ang anumang pagsasaalang-alang ng DID na estado na may kinalaman sa oras, maliban sa kasalukuyang sandali. [Ang mga DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ecosystem na gumagamit ng diskarteng ito ay mahalagang nagbibigay ng mga pahayag na nabe-verify sa cryptographically bilang mga ephemeral na token na maaaring ma-invalidate anumang oras ng [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) .

#### Pagbawi sa Mga Sistemang Walang Pagtitiwalaan

Ang mga walang tiwala na sistema ay ang mga kung saan ang lahat ng tiwala ay nagmula sa mga assertion na napapatunayan sa cryptographically, at mas partikular, kung saan walang metadata sa labas ng cryptographic system ang isinasali sa pagpapasiya ng tiwala sa system. Upang i-verify ang isang lagda ng patunay para sa isang [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) na binawi sa isang walang tiwala na sistema, kailangang suportahan ng isang [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods)versionId ang alinman o pareho ng o versionTime, pati na rin ang parehong updatedat nextUpdate, mga katangian ng metadata ng [dokumento ng DID .](https://www.w3.org/TR/did-core/" \l "dfn-did-documents)Maaaring patunayan ng isang verifier ang isang lagda o patunay ng isang binawi na susi kung at kung totoo lang ang lahat ng sumusunod:

* Kasama sa patunay o pirma ang versionIdo versionTimeng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) na ginamit sa puntong nilikha ang lagda o patunay.
* Maaaring matukoy ng verifier ang punto sa oras kung kailan ginawa ang lagda o patunay; halimbawa, ito ay naka-angkla sa isang blockchain.
* Para sa nalutas na metadata ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents)updated , ang timestamp ay bago, at ang nextUpdatetimestamp ay pagkatapos, ang punto sa oras kung kailan ginawa ang lagda o patunay.

Sa mga system na handang tanggapin ang metadata maliban sa mga bumubuo ng cryptographic input, maaaring makamit ang katulad na tiwala -- ngunit palaging sa parehong batayan kung saan ang isang maingat na paghuhusga ay ginawa tungkol sa kung ang nilalaman ng isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) sa sandali ng isang kaganapan sa pagpirma ang inaasahang nilalaman.

### **9.9DID Recovery**

Ang pagbawi ay isang reaktibong panukalang panseguridad kung saan ang isang [controller](https://www.w3.org/TR/did-core/#dfn-controller) na nawalan ng kakayahang magsagawa ng mga pagpapatakbo ng DID, gaya ng pagkawala ng isang device, ay makakabawi ng kakayahang magsagawa ng mga pagpapatakbo ng DID.

Ang mga sumusunod na pagsasaalang-alang ay maaaring magamit kapag pinag-iisipan ang paggamit ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) recovery:

* Ang pagsasagawa ng pagbawi nang maagap sa isang madalang ngunit regular na batayan, ay makakatulong upang matiyak na ang kontrol ay hindi nawala.
* Itinuturing na pinakamahusay na kasanayan ang hindi kailanman muling gumamit ng cryptographic na materyal na nauugnay sa pagbawi para sa anumang iba pang layunin.
* Ang pagbawi ay karaniwang ginagawa kasabay ng pag- [ikot ng paraan ng pag](https://www.w3.org/TR/did-core/" \l "verification-method-rotation) -verify at [pagbawi ng paraan ng pag](https://www.w3.org/TR/did-core/" \l "verification-method-revocation) -verify .
* Pinapayuhan ang pagbawi kapag ang isang [controller](https://www.w3.org/TR/did-core/#dfn-controller) o mga serbisyong pinagkakatiwalaang kumilos para sa kanila ay wala nang eksklusibong kakayahang magsagawa ng mga operasyon ng DID tulad ng inilarawan sa[8.2Mga Operasyon ng Pamamaraan](https://www.w3.org/TR/did-core/#method-operations) .
* [Maaaring piliin ng mga detalye ng pamamaraan ng DID](https://www.w3.org/TR/did-core/#dfn-did-methods) na paganahin ang suporta para sa isang korum ng mga pinagkakatiwalaang partido upang mapadali ang pagbawi. Iminungkahi ang ilan sa mga pasilidad para gawin ito[5.1.2DID Controller](https://www.w3.org/TR/did-core/#did-controller) .
* Hindi lahat ng mga detalye ng [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ay makikilala ang kontrol mula sa [mga DID na](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers) nakarehistro gamit ang iba pang mga [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) at maaari nilang paghigpitan ang kontrol ng third-party sa [mga DID](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers) na gumagamit ng parehong paraan.
* Ang kontrol sa pag-access at pagbawi sa isang detalye ng [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ay maaari ding magsama ng tampok na time lock upang maprotektahan laban sa pangunahing kompromiso sa pamamagitan ng pagpapanatili ng pangalawang track ng kontrol para sa pagbawi.
* Sa kasalukuyan ay walang mga karaniwang mekanismo sa pagbawi na nalalapat sa lahat ng mga [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) .

### **9.10Ang Papel ng Mga Tagatukoy na Magiliw sa Tao**

[Nakakamit ng mga DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ang pandaigdigang natatangi nang hindi nangangailangan ng isang sentral na awtoridad sa pagpaparehistro. Dumating ito sa halaga ng pagiging alaala ng tao. Ang mga algorithm na may kakayahang bumuo ng mga hindi malabong identifier sa buong mundo ay gumagawa ng mga random na string ng mga character na walang kahulugan ng tao. Ang trade-off na ito ay madalas na tinutukoy bilang [Zooko's Triangle](https://en.wikipedia.org/wiki/Zooko%27s_triangle) .

May mga kaso ng paggamit kung saan kanais-nais na matuklasan ang isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) kapag nagsisimula sa isang pantukoy na pang-tao. Halimbawa, isang natural na pangalan ng wika, isang domain name, o isang kumbensyonal na address para sa isang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) , tulad ng isang numero ng mobile na telepono, email address, username sa social media, o URL ng blog. Gayunpaman, ang problema sa pagmamapa ng mga pantukoy na madaling gamitin sa tao sa [mga DID](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers) , at paggawa nito sa paraang mabe-verify at mapagkakatiwalaan, ay nasa labas ng saklaw ng detalyeng ito.

Ang mga solusyon sa problemang ito ay tinukoy sa magkahiwalay na mga detalye, gaya ng [ [DNS-DID](https://www.w3.org/TR/did-core/#bib-dns-did) ], na tumutukoy sa detalyeng ito. Lubos na inirerekomenda na maingat na isaalang-alang ng mga naturang pagtutukoy ang:

* Maraming panseguridad na pag-atake batay sa panlilinlang sa mga user tungkol sa totoong human-friendly na identifier para sa isang target na entity.
* Mga kahihinatnan sa privacy ng paggamit ng mga pantukoy na madaling gamitin sa tao na likas na nauugnay, lalo na kung ang mga ito ay natatangi sa buong mundo.

### **9.11Mga DID bilang Mga Pinahusay na URN**

Kung ninanais ng isang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) , ang isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) o isang [DID URL](https://www.w3.org/TR/did-core/#dfn-did-urls) ay may kakayahang kumilos bilang paulit-ulit, lokasyon-independent na mapagkukunang identifier. Ang mga uri ng identifier na ito ay inuri bilang Uniform Resource Names (URNs) at tinukoy sa [ [RFC8141](https://www.w3.org/TR/did-core/#bib-rfc8141) ]. [Ang mga DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay isang pinahusay na anyo ng URN na nagbibigay ng cryptographically secure, lokasyon-independent na identifier para sa isang digital na mapagkukunan, habang nagbibigay din ng metadata na nagbibigay-daan sa pagkuha. Dahil sa di-direksyon sa pagitan ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) at ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) mismo, maaaring ayusin ng [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) ang aktwal na lokasyon ng mapagkukunan — o kahit na direktang ibigay ang mapagkukunan — nang hindi inaayos ang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers). [Ang mga DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ng ganitong uri ay maaaring tiyak na ma-verify na ang resource na nakuha ay, sa katunayan, ang resource na natukoy.

Ang isang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) na nagnanais na gumamit ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) para sa layuning ito ay pinapayuhan na sundin ang mga pagsasaalang-alang sa seguridad sa [ [RFC8141](https://www.w3.org/TR/did-core/#bib-rfc8141) ]. Sa partikular:

* Ang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) ay inaasahang pipili ng isang [DID na paraan](https://www.w3.org/TR/did-core/#dfn-did-methods) na sumusuporta sa mga kinakailangan ng controller para sa pagtitiyaga. Ang Rubric ng Desentralisadong Katangian [ [DID-RUBRIC](https://www.w3.org/TR/did-core/#bib-did-rubric) ] ay isang tool na magagamit upang matulungan ang mga tagapagpatupad na magpasya sa pinaka-angkop na [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) .
* Ang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) ay inaasahang maglathala ng mga patakaran sa pagpapatakbo nito upang ang mga humihiling na partido ay matukoy ang antas kung saan sila makakaasa sa pananatili ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na kinokontrol ng [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) na iyon . Sa kawalan ng naturang mga patakaran, ang mga humihiling na partido ay hindi inaasahang gumawa ng anumang pagpapalagay tungkol sa kung ang isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay isang patuloy na pagkakakilanlan para sa parehong [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) .

### **9.12Kawalang pagbabago**

Maraming mga pang-aabuso sa cybersecurity ang nakasalalay sa pagsasamantala sa mga puwang sa pagitan ng katotohanan at mga pagpapalagay ng mga makatuwiran, may mabuting pananampalataya na mga aktor. Ang kawalan ng pagbabago ng mga [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay maaaring magbigay ng ilang mga benepisyo sa seguridad. Ang mga indibidwal na [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ay dapat isaalang-alang ang mga hadlang na mag-aalis ng mga pag-uugali o semantika na hindi nila kailangan. Ang mas naka- lock down na paraan ng [DID](https://www.w3.org/TR/did-core/#dfn-did-methods) ay, habang nagbibigay ng parehong hanay ng mga tampok, mas mababa ito ay maaaring manipulahin ng mga malisyosong aktor.

Bilang halimbawa, isaalang-alang na ang isang solong pag-edit sa isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay maaaring magbago ng anuman maliban sa root [id](https://www.w3.org/TR/did-core/" \l "dfn-id)property ng dokumento. Ngunit ito ba ay talagang kanais-nais para sa isang [serbisyo](https://www.w3.org/TR/did-core/" \l "dfn-service) na baguhin typeito pagkatapos itong matukoy? O para sa isang susi upang baguhin ang halaga nito? O mas mabuti bang mangailangan ng bago [id](https://www.w3.org/TR/did-core/" \l "dfn-id)kapag nagbago ang ilang pangunahing katangian ng isang bagay? Ang mga nakakahamak na pagkuha sa isang website ay kadalasang naglalayon ng isang resulta kung saan pinapanatili ng site ang host name identifier nito, ngunit bahagyang binago sa ilalim. Kung ang ilang partikular na pag-aari ng site, gaya ng [ASN](https://en.wikipedia.org/wiki/Autonomous_system_(Internet)) na nauugnay sa IP address nito, ay hinihiling ng detalye na hindi nababago, ang pagtuklas ng anomalya ay magiging mas madali, at ang mga pag-atake ay magiging mas mahirap at mas mahal na isagawa.

Para sa mga [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) na nauugnay sa isang pandaigdigang pinagmumulan ng katotohanan, palaging posible ang direktang, just-in-time na paghahanap ng pinakabagong bersyon ng isang [dokumento ng DID .](https://www.w3.org/TR/did-core/" \l "dfn-did-documents)Gayunpaman, mukhang malamang na ang mga layer ng cache ay maaaring maupo sa pagitan ng isang [DID resolver](https://www.w3.org/TR/did-core/#dfn-did-resolvers) at ang pinagmulan ng katotohanan. Kung gagawin nila, ang paniniwalang ang mga katangian ng isang bagay sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay may ibinigay na estado kapag sila ay talagang banayad na naiiba ay maaaring mag-imbita ng mga pagsasamantala. Ito ay partikular na totoo kung ang ilang mga paghahanap ay isang buong [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) , at ang iba ay bahagi ng data kung saan ang mas malaking konteksto ay ipinapalagay.

### **9.13Naka-encrypt na Data sa Mga Dokumento ng DID**

Napag-alaman na nabigo ang mga algorithm ng pag-encrypt dahil sa mga pag-unlad sa cryptography at kapangyarihan sa pag-compute. Pinapayuhan ang mga tagapagpatupad na ipagpalagay na ang anumang naka-encrypt na data na inilagay sa isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay maaaring maging available sa huli sa malinaw na teksto sa parehong audience kung saan available ang naka-encrypt na data. Ito ay partikular na nauugnay kung ang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay pampubliko.

Ang pag-encrypt ng lahat o bahagi ng isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay hindi isang naaangkop na paraan upang maprotektahan ang data sa mahabang panahon. Katulad nito, ang paglalagay ng naka-encrypt na data sa isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay hindi isang naaangkop na paraan upang maprotektahan ang personal na data.

Dahil sa mga caveat sa itaas, kung ang naka-encrypt na data ay kasama sa isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) , pinapayuhan ang mga tagapagpatupad na huwag mag-ugnay ng anumang nauugnay na impormasyon na maaaring magamit upang magpahiwatig ng kaugnayan sa pagitan ng naka-encrypt na data at isang nauugnay na partido. Kasama sa mga halimbawa ng nauugnay na impormasyon ang mga pampublikong key ng isang tumatanggap na partido, mga identifier sa mga digital na asset na kilala na nasa ilalim ng kontrol ng isang tumatanggap na partido, o nababasa ng tao na paglalarawan ng isang tumatanggap na partido.

### **9.14Mga Katangian ng Pagkakapantay-pantay**

Dahil ang mga [equivalentId](https://www.w3.org/TR/did-core/" \l "dfn-equivalentid)at ang mga [canonicalId](https://www.w3.org/TR/did-core/" \l "dfn-canonicalid) katangian ay nabuo mismo ng mga [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) , ang parehong mga garantiya sa seguridad at katumpakan na nalalapat sa nalutas na [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na nasa idlarangan ng isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay nalalapat din sa mga katangiang ito. Ang [alsoKnownAs](https://www.w3.org/TR/did-core/" \l "dfn-alsoknownas)ari-arian ay hindi ginagarantiyahan na isang tumpak na pahayag ng katumbas, at hindi dapat umasa nang hindi nagsasagawa ng mga hakbang sa pagpapatunay na lampas sa resolusyon ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) .

Ang [equivalentId](https://www.w3.org/TR/did-core/" \l "dfn-equivalentid)at [canonicalId](https://www.w3.org/TR/did-core/" \l "dfn-canonicalid) mga katangian ay nagpapahayag ng katumbas na mga pahayag sa mga variant ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na ginawa ng parehong [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) at mapagkakatiwalaan hanggang sa ang humihiling na partido ay nagtitiwala sa [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) at isang tumutugon na producer at solver.

Pinapahintulutan ng [alsoKnownAs](https://www.w3.org/TR/did-core/" \l "dfn-alsoknownas)property ang isang equivalence assertion sa mga [URI](https://www.w3.org/TR/did-core/#dfn-uri) na hindi pinamamahalaan ng parehong [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) at hindi mapagkakatiwalaan nang hindi nagsasagawa ng mga hakbang sa pag-verify sa labas ng namamahala na [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) . Tingnan ang karagdagang gabay sa[5.1.3Kilala rin Bilang](https://www.w3.org/TR/did-core/#also-known-as) .

Tulad ng anumang iba pang property na nauugnay sa seguridad sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) , ang mga partidong umaasa sa anumang equivalence statement sa isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay dapat magbantay laban sa mga halaga ng mga property na ito na pinapalitan ng isang attacker pagkatapos maisagawa ang wastong pag-verify. Ang anumang write access sa isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) na nakaimbak sa memorya o disk pagkatapos maisagawa ang pag-verify ay isang attack vector na maaaring umiwas sa pag-verify maliban kung ang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) ay muling na-verify.

### **9.15Proteksyon sa Integridad ng Nilalaman**

[Ang mga dokumento ng DID](https://www.w3.org/TR/did-core/#dfn-did-documents) na may kasamang mga link sa external na content na nababasa ng makina gaya ng mga larawan, web page, o schema ay madaling maapektuhan ng pakikialam. Lubos na pinapayuhan na ang mga panlabas na link ay protektado ng integridad gamit ang mga solusyon gaya ng hashlink [ [HASHLINK](https://www.w3.org/TR/did-core/#bib-hashlink) ]. Ang mga panlabas na link ay dapat iwasan kung hindi sila maprotektahan ng integridad at ang integridad ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay nakasalalay sa panlabas na link.

Isang halimbawa ng panlabas na link kung saan maaaring maapektuhan ang integridad ng mismong [dokumento ng DID ay ang JSON-LD Context [](https://www.w3.org/TR/did-core/" \l "dfn-did-documents)[JSON-LD11](https://www.w3.org/TR/did-core/#bib-json-ld11) ]. Upang maprotektahan laban sa kompromiso, pinapayuhan ang mga consumer ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) na i-cache ang mga lokal na static na kopya ng JSON-LD na konteksto at/o i-verify ang integridad ng mga panlabas na konteksto laban sa isang cryptographic na hash na kilalang nauugnay sa isang ligtas na bersyon ng external na JSON-LD Context .

### **9.16Pagtitiyaga**

[Ang mga DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay idinisenyo upang maging paulit-ulit upang ang isang [controller](https://www.w3.org/TR/did-core/#dfn-controller) ay hindi kailangang umasa sa isang pinagkakatiwalaang third party o administrator upang mapanatili ang kanilang mga identifier. Sa isang mainam na kaso, walang administrator ang maaaring mag-alis ng kontrol mula sa [controller](https://www.w3.org/TR/did-core/#dfn-controller) , at hindi rin mapipigilan ng isang administrator ang paggamit ng kanilang mga identifier para sa anumang partikular na layunin gaya ng pagpapatunay, awtorisasyon, at pagpapatunay. Walang third party ang maaaring kumilos sa ngalan ng isang [controller](https://www.w3.org/TR/did-core/#dfn-controller) upang alisin o gawing hindi gumagana ang identifier ng isang entity nang walang pahintulot ng [controller](https://www.w3.org/TR/did-core/#dfn-controller) .

Gayunpaman, mahalagang tandaan na sa lahat ng mga [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) na nagbibigay-daan sa cryptographic proof-of-control, ang paraan ng pagpapatunay ng kontrol ay maaaring palaging ilipat sa ibang partido sa pamamagitan ng paglilipat ng sikretong cryptographic na materyal. Samakatuwid, mahalaga na ang mga system na umaasa sa pananatili ng isang identifier sa paglipas ng panahon ay regular na suriin upang matiyak na ang identifier ay, sa katunayan, nasa ilalim pa rin ng kontrol ng nilalayong partido.

Sa kasamaang palad, imposibleng matukoy mula sa cryptography lamang kung ang lihim na materyal na cryptographic na nauugnay sa isang ibinigay na [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ay nakompromiso o hindi. Maaaring ang inaasahang [controller](https://www.w3.org/TR/did-core/#dfn-controller) ay mayroon pa ring access sa sikretong cryptographic na materyal — at dahil dito ay maaaring magsagawa ng proof-of-control bilang bahagi ng proseso ng pag-verify — habang kasabay nito, ang isang masamang aktor ay may access din sa mga iyon. mga susi, o sa isang kopya nito.

Dahil dito, inaasahang gagamitin lang ang cryptographic proof-of-control bilang isang salik sa pagsusuri sa antas ng katiyakan ng pagkakakilanlan na kinakailangan para sa mga sitwasyong may mataas na stake. [Ang pagpapatunay na nakabatay sa DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay nagbibigay ng higit na higit na katiyakan kaysa sa isang username at password, salamat sa kakayahang matukoy ang kontrol sa isang cryptographic na lihim nang hindi ipinapadala ang sikretong iyon sa pagitan ng mga system. Gayunpaman, hindi ito hindi nagkakamali. Ang mga sitwasyong may kinalaman sa sensitibo, mataas na halaga, o kritikal sa buhay na operasyon ay inaasahang gagamit ng mga karagdagang salik kung naaangkop.

Bilang karagdagan sa potensyal na kalabuan mula sa paggamit ng iba't ibang mga [controller](https://www.w3.org/TR/did-core/#dfn-controller) , imposibleng magarantiya, sa pangkalahatan, na ang isang ibinigay na [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay ginagamit bilang pagtukoy sa parehong paksa sa anumang partikular na punto ng oras. Teknikal na posible para sa controller na muling gumamit ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) para sa iba't ibang paksa at, mas banayad, para sa tumpak na kahulugan ng paksa na magbago sa paglipas ng panahon o hindi maintindihan.

Halimbawa, isaalang-alang ang isang [DID na](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ginagamit para sa isang solong pagmamay-ari, na tumatanggap ng iba't ibang mga kredensyal na ginagamit para sa mga transaksyong pinansyal. Sa [controller](https://www.w3.org/TR/did-core/#dfn-controller) , tinutukoy ng identifier na iyon ang negosyo. Habang lumalaki ang negosyo, sa kalaunan ay naisasama ito bilang isang Limited Liability Company. Patuloy na ginagamit ng [controller](https://www.w3.org/TR/did-core/#dfn-controller) ang parehong [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) , dahil sa **kanila** ang [DID ay](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) tumutukoy sa negosyo. Gayunpaman, sa estado, awtoridad sa buwis, at lokal na munisipalidad, ang [DID](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers)hindi na tumutukoy sa parehong entity. Kung mahalaga o hindi ang banayad na pagbabago sa kahulugan sa isang tagapagbigay ng kredito o tagapagtustos ay kinakailangang nasa kanila ang pagpapasya. Sa maraming kaso, hangga't nababayaran ang mga bayarin at maaaring ipatupad ang mga koleksyon, ang paglilipat ay hindi materyal.

Dahil sa mga potensyal na ambiguity na ito, ang mga [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay dapat ituring na wasto ayon sa konteksto sa halip na ganap. Ang kanilang pagtitiyaga ay hindi nagpapahiwatig na sila ay tumutukoy sa eksaktong parehong paksa, o na sila ay nasa ilalim ng kontrol ng parehong [controller](https://www.w3.org/TR/did-core/#dfn-controller) . Sa halip, kailangang maunawaan ng isang tao ang konteksto kung saan nilikha ang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) , kung paano ito ginamit, at isaalang-alang ang mga malamang na pagbabago sa kanilang kahulugan, at magpatibay ng mga pamamaraan at patakaran upang matugunan ang parehong potensyal at hindi maiiwasang semantic drift.

### **9.17Antas ng Assurance**

Ang karagdagang impormasyon tungkol sa konteksto ng seguridad ng mga kaganapan sa pagpapatotoo ay kadalasang kinakailangan para sa mga dahilan ng pagsunod, lalo na sa mga kinokontrol na lugar gaya ng mga sektor ng pananalapi at pampublikong. Ang impormasyong ito ay madalas na tinutukoy bilang Level of Assurance (LOA). Kasama sa mga halimbawa ang proteksyon ng lihim na cryptographic na materyal, ang proseso ng pag-proofing ng pagkakakilanlan, at ang form-factor ng authenticator.

[Ang mga serbisyo sa pagbabayad (PSD 2)](https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en) at [eIDAS ay](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG" \t "_blank) nagpapakilala sa mga naturang kinakailangan sa konteksto ng seguridad. Ang mga framework ng antas ng assurance ay inuri at tinukoy ng mga regulasyon at pamantayan gaya ng [eIDAS](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG" \t "_blank) , [NIST 800-63-3](https://pages.nist.gov/800-63-3/sp800-63-3.html) at [ISO/IEC 29115:2013](https://www.iso.org/standard/45138.html) , kasama ang kanilang mga kinakailangan para sa konteksto ng seguridad, at paggawa ng mga rekomendasyon kung paano makamit ang mga ito. Maaaring kabilang dito ang malakas na pag-authenticate ng user kung saan matutupad ng [FIDO2](https://fidoalliance.org/fido2/) / [WebAuthn](https://www.w3.org/TR/webauthn-2/" \t "_blank) ang kinakailangan.

Ang ilang mga regulated na sitwasyon ay nangangailangan ng pagpapatupad ng isang partikular na antas ng kasiguruhan. Dahil ang mga [ugnayan sa pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-relationship) gaya ng at maaaring gamitin sa ilan sa mga sitwasyong ito, ang impormasyon tungkol sa inilapat na konteksto ng seguridad ay maaaring kailangang ipahayag at ibigay sa isang verifier . Kung at kung paano i-encode ang impormasyong ito sa modelo ng data ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay wala sa saklaw para sa detalyeng ito. Maaaring tandaan ng mga interesadong mambabasa na 1) maaaring maipadala ang impormasyon gamit ang Mga Napapatunayang Kredensyal [ [VC-DATA-MODEL](https://www.w3.org/TR/did-core/#bib-vc-data-model) ], at 2) ang modelo ng data ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay maaaring palawigin upang maisama ang impormasyong ito tulad ng inilarawan sa [assertionMethod](https://www.w3.org/TR/did-core/#dfn-assertionmethod)[authentication](https://www.w3.org/TR/did-core/#dfn-authentication)[4.1Extensibility](https://www.w3.org/TR/did-core/#extensibility) , at kung saan[10.Naaangkop ang Mga Pagsasaalang- alang sa Privacy](https://www.w3.org/TR/did-core/#privacy-considerations) para sa mga naturang extension.

## 10.Mga Pagsasaalang-alang sa Privacy

Ang seksyong ito ay hindi normatibo.

Dahil ang mga dokumento ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) at [DID](https://www.w3.org/TR/did-core/#dfn-did-documents) ay idinisenyo upang direktang pangasiwaan ng [(mga) DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) , napakahalagang ilapat ang mga prinsipyo ng Privacy by Design [ [PRIVACY-BY-DESIGN](https://www.w3.org/TR/did-core/#bib-privacy-by-design) ] sa lahat ng aspeto ng [desentralisadong identifier](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers)arkitektura. Ang lahat ng pitong prinsipyong ito ay nailapat sa buong pagbuo ng detalyeng ito. Ang disenyo na ginamit sa detalyeng ito ay hindi ipinapalagay na mayroong isang registrar, kumpanya ng pagho-host, o iba pang intermediate na service provider upang magrekomenda o maglapat ng mga karagdagang proteksyon sa privacy. Ang privacy sa detalyeng ito ay preventive, hindi remedial, at isang naka-embed na default. Ang mga sumusunod na seksyon ay sumasaklaw sa mga pagsasaalang-alang sa privacy na maaaring maging kapaki-pakinabang ng mga tagapagpatupad kapag gumagawa ng mga system na gumagamit ng [mga desentralisadong identifier](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers) .

### **10.1Panatilihing Pribado ang Personal na Data**

Kung ang isang detalye ng [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ay isinulat para sa isang [registry ng data na nabe](https://www.w3.org/TR/did-core/#dfn-verifiable-data-registry) -verify na nakaharap sa publiko kung saan ang mga kaukulang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) at mga [dokumento](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ng DID ay maaaring gawing available sa publiko, napakahalaga na ang mga [dokumentong DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) na iyon ay walang personal na data. Sa halip, ang personal na data ay maaaring ipadala sa pamamagitan ng iba pang paraan tulad ng 1) Mga Nabe-verify na Kredensyal [ [VC-DATA-MODEL](https://www.w3.org/TR/did-core/#bib-vc-data-model) ], o 2) mga [endpoint ng serbisyo](https://www.w3.org/TR/did-core/#dfn-service-endpoints) sa ilalim ng kontrol ng [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) o [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) .

Inaasahan na isasagawa ang angkop na pagsisikap sa paggamit ng mga URL sa mga [endpoint ng serbisyo](https://www.w3.org/TR/did-core/#dfn-service-endpoints) upang maiwasan ang pagtagas ng personal na data o ugnayan sa loob ng isang URL ng isang [endpoint ng serbisyo](https://www.w3.org/TR/did-core/#dfn-service-endpoints) . Halimbawa, ang isang URL na naglalaman ng isang username ay mapanganib na isama sa isang [DID Document](https://www.w3.org/TR/did-core/#dfn-did-documents) dahil ang username ay malamang na makatao sa isang paraan na maaaring magbunyag ng impormasyon na ang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ay hindi pumayag na ibahagi. Gamit ang arkitektura ng privacy na iminungkahi ng detalyeng ito, ang personal na data ay maaaring palitan sa isang pribado, peer-to-peer na batayan gamit ang mga channel ng komunikasyon na tinukoy at sinigurado ng [mga paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) sa [mga dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) . Nagbibigay-daan din [ito sa mga paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects)at humihiling sa mga partido na ipatupad ang karapatan ng [GDPR](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation)[na makalimutan](https://en.wikipedia.org/wiki/Right_to_be_forgotten) , dahil walang personal na data ang nakasulat sa isang hindi nababagong [distributed ledger](https://www.w3.org/TR/did-core/#dfn-distributed-ledger-technology) .

### **10.2Mga Panganib sa Pag-uugnay ng DID**

Tulad ng anumang uri ng hindi malabong identifier sa buong mundo, maaaring gamitin ang [mga DID para sa ugnayan.](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers)Maaaring pagaanin ng mga [controller ng DID ang panganib sa privacy na ito sa pamamagitan ng paggamit ng mga pairwise na](https://www.w3.org/TR/did-core/#dfn-did-controllers)[DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na natatangi sa bawat relasyon; sa epekto, ang bawat [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay gumaganap bilang isang pseudonym. Ang isang pairwise [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay kailangan lang ibahagi sa higit sa isang partido kapag ang ugnayan ay tahasang nais. Kung pairwise [DIDs](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ang default, ang tanging kailangan lang na mag-publish ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) nang hayagan, o ibahagi ito sa maraming partido, ay kapag ang [DID controller(s)](https://www.w3.org/TR/did-core/#dfn-did-controllers) at/o [DID subject](https://www.w3.org/TR/did-core/#dfn-did-subjects) ay tahasang nagnanais ng pampublikong pagkakakilanlan at ugnayan.

### **10.3DID Document Correlation Risks**

Ang mga anti-correlation na proteksyon ng pairwise [DIDs](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay madaling talunin kung ang data sa mga kaukulang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay maaaring maiugnay. Halimbawa, ang paggamit ng magkaparehong [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) o pasadyang mga [endpoint ng serbisyo](https://www.w3.org/TR/did-core/#dfn-service-endpoints) sa maraming [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay maaaring magbigay ng mas maraming impormasyon ng ugnayan gaya ng paggamit ng parehong [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) . Samakatuwid, ang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) para sa isang pairwise [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay kailangan ding gumamit ng pairwise na natatanging impormasyon, gaya ng pagtiyak na ang mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) ay natatangi sa pairwise na relasyon.

Maaaring natural na gumamit din ng pairwise na natatanging mga [endpoint ng serbisyo](https://www.w3.org/TR/did-core/#dfn-service-endpoints) sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) para sa isang pairwise na [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) . Gayunpaman, pinapayagan ng mga natatanging endpoint ang lahat ng trapiko sa pagitan ng dalawang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na maihiwalay nang perpekto sa mga natatanging bucket, kung saan madali ang ugnayan ng timing at katulad na pagsusuri. Samakatuwid, ang isang mas mahusay na diskarte para sa privacy ng endpoint ay maaaring magbahagi ng isang endpoint sa isang malaking bilang ng mga [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na kinokontrol ng maraming iba't ibang mga paksa (tingnan ang[10.5Privacy ng kawan](https://www.w3.org/TR/did-core/#herd-privacy) ).

### **10.4Pag-uuri ng Paksa ng DID**

Mapanganib na magdagdag ng mga katangian sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) na maaaring gamitin upang ipahiwatig, tahasan o sa pamamagitan ng hinuha, kung anong uri o katangian ng bagay ang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) , partikular na kung ang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ay isang tao.

Hindi lamang maaaring magresulta ang mga naturang property sa personal na data (tingnan [10.1Panatilihing Pribado ang Personal na Data](https://www.w3.org/TR/did-core/#keep-personal-data-private) ) o kaugnay na data (tingnan[10.2DID Mga Panganib sa Pag](https://www.w3.org/TR/did-core/" \l "did-correlation-risks) -uugnay at[10.3DID Document Correlation Risks](https://www.w3.org/TR/did-core/#did-document-correlation-risks) ) na naroroon sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) , ngunit magagamit ang mga ito para sa pagpapangkat ng mga partikular [na DID](https://www.w3.org/TR/did-core/" \l "dfn-decentralized-identifiers) sa paraan na ang mga ito ay kasama o hindi kasama sa ilang partikular na operasyon o functionality.

Ang pagsasama ng uri ng impormasyon sa isang [DID na Dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) ay maaaring magresulta sa mga personal na pinsala sa privacy kahit para sa mga [Paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) na hindi tao na mga entity, gaya ng mga IoT device. Ang pagsasama-sama ng naturang impormasyon sa paligid ng isang [DID Controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) ay maaaring magsilbi bilang isang anyo ng digital fingerprint at ito ay pinakamahusay na maiiwasan.

Upang mabawasan ang mga panganib na ito, ang lahat ng pag-aari sa isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay dapat para sa pagpapahayag ng materyal na cryptographic, mga endpoint, o mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) na nauugnay sa paggamit ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) .

### **10.5Privacy ng kawan**

Kapag ang isang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ay hindi nakikilala mula sa iba sa kawan, magagamit ang privacy. Kapag ang pagkilos ng pakikipag-ugnayan nang pribado sa ibang partido ay sa pamamagitan ng sarili nitong isang makikilalang bandila, ang privacy ay lubhang nababawasan.

[Ang mga pamamaraan ng DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) at [DID](https://www.w3.org/TR/did-core/#dfn-did-methods) ay kailangang gumana upang mapahusay ang pagkapribado ng kawan, lalo na para sa mga lehitimong nangangailangan nito. Pumili ng mga teknolohiya at mga interface ng tao na default sa pagpapanatili ng anonymity at pseudonymity. Upang bawasan ang [mga digital na fingerprint](https://en.wikipedia.org/wiki/Device_fingerprint) , magbahagi ng mga karaniwang setting sa paghiling ng mga pagpapatupad ng partido, panatilihing pinakamababa ang mga napagkasunduang opsyon sa mga wire protocol, gumamit ng mga naka-encrypt na transport layer, at pad na mga mensahe sa karaniwang haba.

### **10.6Privacy ng Serbisyo**

Ang kakayahan ng isang [controller](https://www.w3.org/TR/did-core/#dfn-controller) na opsyonal na magpahayag ng kahit isang [endpoint ng serbisyo](https://www.w3.org/TR/did-core/#dfn-service-endpoints) sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay nagpapataas ng kanilang kontrol at ahensya. Ang bawat karagdagang endpoint sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay nagdaragdag ng panganib sa privacy dahil sa ugnayan, gaya ng mga paglalarawan sa endpoint, o dahil ang mga [serbisyo](https://www.w3.org/TR/did-core/" \l "dfn-service) ay hindi protektado ng mekanismo ng awtorisasyon, o pareho.

[Ang mga dokumento ng DID](https://www.w3.org/TR/did-core/#dfn-did-documents) ay kadalasang pampubliko at, dahil naka-standardize ang mga ito, ay maiimbak at mai-index nang mahusay sa pamamagitan ng kanilang likas na batay sa pamantayan. Mas malala ang panganib na ito kung ang mga [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay nai-publish sa mga hindi nababagong [rehistro ng data na nabe](https://www.w3.org/TR/did-core/" \l "dfn-verifiable-data-registry) -verify . Ang pag-access sa isang kasaysayan ng mga [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) na isinangguni ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay kumakatawan sa isang paraan ng pagsusuri sa trapiko na ginawang mas mahusay sa pamamagitan ng paggamit ng mga pamantayan.

Ang antas ng karagdagang panganib sa privacy na dulot ng paggamit ng maraming mga [endpoint ng serbisyo](https://www.w3.org/TR/did-core/#dfn-service-endpoints) sa isang [dokumento ng DID](https://www.w3.org/TR/did-core/#dfn-did-documents) ay maaaring mahirap tantiyahin. Ang mga pinsala sa privacy ay karaniwang hindi sinasadyang mga kahihinatnan. [Maaaring sumangguni ang mga DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) sa mga dokumento, [serbisyo](https://www.w3.org/TR/did-core/#dfn-service) , schema, at iba pang bagay na maaaring nauugnay sa mga indibidwal na tao, sambahayan, club, at employer — at ang ugnayan ng kanilang mga [endpoint ng serbisyo](https://www.w3.org/TR/did-core/#dfn-service-endpoints) ay maaaring maging isang mahusay na tool sa pagsubaybay at paghihinuha. Ang isang halimbawa ng potensyal na pinsalang ito ay makikita kapag maramihang karaniwang mga domain sa pinakamataas na antas ng antas ng bansa gaya ng https://example.co.ukmaaaring gamitin upang ipahiwatig ang tinatayang lokasyon ng [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) na may mas malaking antas ng posibilidad.

#### Pagpapanatili ng Privacy ng kawan

Ang iba't ibang posibleng mga endpoint ay ginagawang partikular na mapaghamong mapanatili ang pagkapribado ng kawan, kung saan walang impormasyon tungkol sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ang na-leak (tingnan ang[10.5Privacy ng kawan](https://www.w3.org/TR/did-core/#herd-privacy) ).

Una, dahil maaaring tukuyin ang mga endpoint ng serbisyo bilang mga [URI](https://www.w3.org/TR/did-core/#dfn-uri) , maaari nilang hindi sinasadyang mag-leak ng personal na impormasyon dahil sa arkitektura ng serbisyo. Halimbawa, ang isang endpoint ng serbisyo ng http://example.com/MyFirstNameay naglalabas ng termino MyFirstNamesa lahat ng makaka-access sa [dokumento ng DID](https://www.w3.org/TR/did-core/#dfn-did-documents) . Kapag nagli-link sa mga legacy system, ito ay isang hindi maiiwasang panganib, at ang pangangalaga ay inaasahang gagawin sa mga ganitong kaso. Hinihikayat ng detalyeng ito ang mga bagong, [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) -aware na mga endpoint na gumamit ng wala nang higit pa sa [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) mismo para sa anumang pagkakakilanlan na kinakailangan. Halimbawa, kung ang isang paglalarawan ng serbisyo ay isasama ang http://example.com/did%3Aexample%3Aabc123, walang pinsalang gagawin dahil did:example:abc123nakalabas na sa DID Document; hindi ito naglalabas ng karagdagang impormasyon.

Pangalawa, dahil ang isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay maaaring maglista ng maramihang mga endpoint ng serbisyo, posible na hindi maibabalik na iugnay ang mga serbisyo na hindi nauugnay sa anumang iba pang konteksto. Ang ugnayang ito sa sarili nitong maaaring humantong sa mga pinsala sa privacy sa pamamagitan ng pagbubunyag ng impormasyon tungkol sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) , kahit na ang mga [URI](https://www.w3.org/TR/did-core/#dfn-uri) na ginamit ay walang anumang sensitibong impormasyon.

Pangatlo, dahil ang ilang uri ng mga [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ay maaaring mas malamang na maglista ng mga partikular na endpoint, ang listahan ng isang partikular na serbisyo ay maaaring, sa sarili nitong, mag-leak ng impormasyon na maaaring magamit upang magpahiwatig ng isang bagay tungkol sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) . Halimbawa, ang isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) para sa isang sasakyan ay maaaring magsama ng isang pointer sa isang pampublikong rekord ng pamagat sa Department of Motor Vehicles, habang ang isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) para sa isang indibidwal ay hindi magsasama ng impormasyong iyon.

Layunin ng herd privacy na matiyak na ang kalikasan ng mga partikular na [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ay natatakpan ng populasyon ng kabuuan. Upang i-maximize ang pagkapribado ng kawan, kailangang umasa ang mga tagapagpatupad sa isa — at isa lamang — na endpoint ng serbisyo, na ang endpoint na iyon ay nagbibigay ng proxy o tagapamagitan na serbisyo na handang umasa ang controller, para protektahan ang mga naturang asosasyon at bulagin ang mga kahilingan sa pinakahuling serbisyo.

#### Mga Alternatibo sa Endpoint ng Serbisyo

Dahil sa mga alalahanin sa nakaraang seksyon, hinihimok ang mga tagapagpatupad na isaalang-alang ang alinman sa mga sumusunod na endpoint approach ng serbisyo:

* **Endpoint ng Negotiator** — Serbisyo para sa pakikipagnegosasyon sa mga channel ng komunikasyong pinagkasunduang dalawa, mas mabuti gamit ang pribadong hanay na intersection. Ang output ng negosasyon ay isang channel ng komunikasyon at anumang mga kredensyal na maaaring kailanganin upang ma-access ito.
* **Tor Endpoint** ( [Tor Onion Router](https://www.torproject.org/about/history/) ) — Magbigay ng address na may kinalaman sa privacy para maabot ang mga endpoint ng serbisyo. Anumang serbisyo na maaaring ibigay online ay maaaring ibigay sa pamamagitan ng TOR para sa karagdagang privacy.
* **Endpoint ng**[Tagapamagitan](https://github.com/hyperledger/aries-rfcs/blob/720bdab50e2d0437fda03028c1b17c69781bdd69/concepts/0046-mediators-and-relays/README.md) — Nagbibigay ang mga tagapamagitan ng generic na endpoint, para sa maraming partido, makatanggap ng mga naka-encrypt na mensahe sa ngalan ng mga partidong iyon, at ipasa ang mga ito sa nilalayong tatanggap. Iniiwasan nito ang pangangailangang magkaroon ng isang partikular na endpoint bawat paksa, na maaaring lumikha ng panganib sa ugnayan. Ang pamamaraang ito ay tinatawag ding proxy.
* **Kumpidensyal na Imbakan** — Maaaring kailanganing itago ang pagmamay-ari o kumpidensyal na personal na impormasyon sa isang [nabe-verify na registry ng data](https://www.w3.org/TR/did-core/#dfn-verifiable-data-registry) upang magbigay ng karagdagang mga garantiya sa privacy at/o seguridad, lalo na para sa mga [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) kung saan na-publish ang mga [dokumento](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ng DID sa isang pampublikong ledger. Ang pagturo sa mga serbisyo ng panlabas na mapagkukunan ay nagbibigay ng paraan para sa mga pagsusuri at pagtanggal ng pahintulot.
* **Polymorphic Proxy** — Isang proxy endpoint na maaaring kumilos bilang anumang bilang ng mga serbisyo, depende sa kung paano ito tinatawag. Halimbawa, ang parehong URL ay maaaring gamitin para sa parehong negotiator at mediator function, depende sa isang mekanismo para sa muling pagruruta.

Ang mga uri ng endpoint ng serbisyo na ito ay patuloy na isang lugar ng pagbabago at paggalugad.

## A.Mga halimbawa

### **A.1Mga Dokumento ng DID**

Ang seksyong ito ay hindi normatibo.

Tingnan ang Mga [Uri ng Paraan ng Pag-verify](https://www.w3.org/TR/did-spec-registries/#verification-method-types) [ [DID-SPEC-REGISTRIES](https://www.w3.org/TR/did-core/#bib-did-spec-registries) ] para sa mga opsyonal na extension at iba pang uri ng paraan ng pag-verify.

TANDAAN

Ang mga halimbawang ito ay para sa mga layunin ng impormasyon lamang, ito ay itinuturing na isang pinakamahusay na kasanayan upang maiwasan ang paggamit ng parehong [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) para sa maraming layunin.

[HALIMBAWA30](https://www.w3.org/TR/did-core/#example-did-document-with-1-verification-method-type): DID Dokumento na may 1 uri ng paraan ng pag-verify

{

"@context": [

"https://www.w3.org/ns/did/v1",

"https://w3id.org/security/suites/ed25519-2020/v1"

],

"id": "did:example:123",

"authentication": [

{

"id": "did:example:123#z6MkecaLyHuYWkayBDLw5ihndj3T1m6zKTGqau3A51G7RBf3",

"type": "Ed25519VerificationKey2020", *// external (property value)*

"controller": "did:example:123",

"publicKeyMultibase": "zAKJP3f7BD6W4iWEQ9jwndVTCBq8ua2Utt8EEjJ6Vxsf"

}

],

"capabilityInvocation": [

{

"id": "did:example:123#z6MkhdmzFu659ZJ4XKj31vtEDmjvsi5yDZG5L7Caz63oP39k",

"type": "Ed25519VerificationKey2020", *// external (property value)*

"controller": "did:example:123",

"publicKeyMultibase": "z4BWwfeqdp1obQptLLMvPNgBw48p7og1ie6Hf9p5nTpNN"

}

],

"capabilityDelegation": [

{

"id": "did:example:123#z6Mkw94ByR26zMSkNdCUi6FNRsWnc2DFEeDXyBGJ5KTzSWyi",

"type": "Ed25519VerificationKey2020", *// external (property value)*

"controller": "did:example:123",

"publicKeyMultibase": "zHgo9PAmfeoxHG8Mn2XHXamxnnSwPpkyBHAMNF3VyXJCL"

}

],

"assertionMethod": [

{

"id": "did:example:123#z6MkiukuAuQAE8ozxvmahnQGzApvtW7KT5XXKfojjwbdEomY",

"type": "Ed25519VerificationKey2020", *// external (property value)*

"controller": "did:example:123",

"publicKeyMultibase": "z5TVraf9itbKXrRvt2DSS95Gw4vqU3CHAdetoufdcKazA"

}

]

}

[HALIMBAWA31](https://www.w3.org/TR/did-core/#example-did-document-with-many-different-key-types): DID Document na may maraming iba't ibang uri ng key

{

"@context": [

"https://www.w3.org/ns/did/v1",

"https://w3id.org/security/suites/jws-2020/v1"

],

"verificationMethod": [

{

"id": "did:example:123#key-0",

"type": "JsonWebKey2020",

"controller": "did:example:123",

"publicKeyJwk": {

"kty": "OKP", *// external (property name)*

"crv": "Ed25519", *// external (property name)*

"x": "VCpo2LMLhn6iWku8MKvSLg2ZAoC-nlOyPVQaO3FxVeQ" *// external (property name)*

}

},

{

"id": "did:example:123#key-1",

"type": "JsonWebKey2020",

"controller": "did:example:123",

"publicKeyJwk": {

"kty": "OKP", *// external (property name)*

"crv": "X25519", *// external (property name)*

"x": "pE\_mG098rdQjY3MKK2D5SUQ6ZOEW3a6Z6T7Z4SgnzCE" *// external (property name)*

}

},

{

"id": "did:example:123#key-2",

"type": "JsonWebKey2020",

"controller": "did:example:123",

"publicKeyJwk": {

"kty": "EC", *// external (property name)*

"crv": "secp256k1", *// external (property name)*

"x": "Z4Y3NNOxv0J6tCgqOBFnHnaZhJF6LdulT7z8A-2D5\_8", *// external (property name)*

"y": "i5a2NtJoUKXkLm6q8nOEu9WOkso1Ag6FTUT6k\_LMnGk" *// external (property name)*

}

},

{

"id": "did:example:123#key-3",

"type": "JsonWebKey2020",

"controller": "did:example:123",

"publicKeyJwk": {

"kty": "EC", *// external (property name)*

"crv": "secp256k1", *// external (property name)*

"x": "U1V4TVZVMUpUa0ZVU1NBcU9CRm5IbmFaaEpGNkxkdWx", *// external (property name)*

"y": "i5a2NtJoUKXkLm6q8nOEu9WOkso1Ag6FTUT6k\_LMnGk" *// external (property name)*

}

},

{

"id": "did:example:123#key-4",

"type": "JsonWebKey2020",

"controller": "did:example:123",

"publicKeyJwk": {

"kty": "EC", *// external (property name)*

"crv": "P-256", *// external (property name)*

"x": "Ums5WVgwRkRTVVFnU3k5c2xvZllMbEcwM3NPRW91ZzN", *// external (property name)*

"y": "nDQW6XZ7b\_u2Sy9slofYLlG03sOEoug3I0aAPQ0exs4" *// external (property name)*

}

},

{

"id": "did:example:123#key-5",

"type": "JsonWebKey2020",

"controller": "did:example:123",

"publicKeyJwk": {

"kty": "EC", *// external (property name)*

"crv": "P-384", *// external (property name)*

"x": "VUZKSlUwMGdpSXplekRwODhzX2N4U1BYdHVYWUZsaXVDR25kZ1U0UXA4bDkxeHpE", *// external (property name)*

"y": "jq4QoAHKiIzezDp88s\_cxSPXtuXYFliuCGndgU4Qp8l91xzD1spCmFIzQgVjqvcP" *// external (property name)*

}

},

{

"id": "did:example:123#key-6",

"type": "JsonWebKey2020",

"controller": "did:example:123",

"publicKeyJwk": {

"kty": "EC", *// external (property name)*

"crv": "P-521", *// external (property name)*

"x": "VTI5c1lYSmZWMmx1WkhNZ0dQTXhaYkhtSnBEU3UtSXZwdUtpZ0VOMnB6Z1d0U28tLVJ3ZC1uNzhuclduWnplRGMx", *// external (property name)*

"y": "UW5WNVgwSnBkR052YVc0Z1VqY1B6LVpoZWNaRnliT3FMSUpqVk9sTEVUSDd1UGx5RzBnRW9NV25JWlhoUVZ5cFB5" *// external (property name)*

}

},

{

"id": "did:example:123#key-7",

"type": "JsonWebKey2020",

"controller": "did:example:123",

"publicKeyJwk": {

"kty": "RSA", *// external (property name)*

"e": "AQAB", *// external (property name)*

"n": "UkhWaGJGOUZRMTlFVWtKSElBdENGV2hlU1F2djFNRXh1NVJMQ01UNGpWazlraEpLdjhKZU1YV2UzYldIYXRqUHNrZGYyZGxhR2tXNVFqdE9uVUtMNzQybXZyNHRDbGRLUzNVTElhVDFoSkluTUhIeGoyZ2N1Yk82ZUVlZ0FDUTRRU3U5TE8wSC1MTV9MM0RzUkFCQjdRamE4SGVjcHl1c3BXMVR1X0RicXhjU253ZW5kYW13TDUyVjE3ZUtobE80dVh3djJIRmx4dWZGSE0wS21DSnVqSUt5QXhqRF9tM3FfX0lpSFVWSEQxdERJRXZMUGhHOUF6c24zajk1ZC1zYU" *// external (property name)*

}

}

]

}

[HALIMBAWA32](https://www.w3.org/TR/did-core/#example-did-document-with-different-verification-method-types): DID Dokumento na may iba't ibang uri ng paraan ng pag-verify

{

"@context": [

"https://www.w3.org/ns/did/v1",

"https://w3id.org/security/suites/ed25519-2018/v1",

"https://w3id.org/security/suites/x25519-2019/v1",

"https://w3id.org/security/suites/secp256k1-2019/v1",

"https://w3id.org/security/suites/jws-2020/v1"

],

"verificationMethod": [

{

"id": "did:example:123#key-0",

"type": "Ed25519VerificationKey2018",

"controller": "did:example:123",

"publicKeyBase58": "3M5RCDjPTWPkKSN3sxUmmMqHbmRPegYP1tjcKyrDbt9J" *// external (property name)*

},

{

"id": "did:example:123#key-1",

"type": "X25519KeyAgreementKey2019",

"controller": "did:example:123",

"publicKeyBase58": "FbQWLPRhTH95MCkQUeFYdiSoQt8zMwetqfWoxqPgaq7x" *// external (property name)*

},

{

"id": "did:example:123#key-2",

"type": "EcdsaSecp256k1VerificationKey2019",

"controller": "did:example:123",

"publicKeyBase58": "ns2aFDq25fEV1NUd3wZ65sgj5QjFW8JCAHdUJfLwfodt" *// external (property name)*

},

{

"id": "did:example:123#key-3",

"type": "JsonWebKey2020",

"controller": "did:example:123",

"publicKeyJwk": {

"kty": "EC", *// external (property name)*

"crv": "P-256", *// external (property name)*

"x": "Er6KSSnAjI70ObRWhlaMgqyIOQYrDJTE94ej5hybQ2M", *// external (property name)*

"y": "pPVzCOTJwgikPjuUE6UebfZySqEJ0ZtsWFpj7YSPGEk" *// external (property name)*

}

}

]

}

### **A.2nagpapatunay**

Ang seksyong ito ay hindi normatibo.

TANDAAN

Ang mga halimbawang ito ay para sa mga layunin ng impormasyon lamang. Tingnan ang [W3C Verifiable Credentials Data Model](https://www.w3.org/TR/vc-data-model/) para sa mga karagdagang halimbawa.

[HALIMBAWA33](https://www.w3.org/TR/did-core/#example-verifiable-credential-linked-to-a-verification-method-of-type-ed25519verificationkey2020): Na-verify na Kredensyal na naka-link sa isang paraan ng pag-verify ng uri Ed25519VerificationKey2020

{ *// external (all terms in this example)*

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://w3id.org/citizenship/v1"

],

"type": [

"VerifiableCredential",

"PermanentResidentCard"

],

"credentialSubject": {

"id": "did:example:123",

"type": [

"PermanentResident",

"Person"

],

"givenName": "JOHN",

"familyName": "SMITH",

"gender": "Male",

"image": "data:image/png;base64,iVBORw0KGgo...kJggg==",

"residentSince": "2015-01-01",

"lprCategory": "C09",

"lprNumber": "000-000-204",

"commuterClassification": "C1",

"birthCountry": "Bahamas",

"birthDate": "1958-08-17"

},

"issuer": "did:example:456",

"issuanceDate": "2020-04-22T10:37:22Z",

"identifier": "83627465",

"name": "Permanent Resident Card",

"description": "Government of Example Permanent Resident Card.",

"proof": {

"type": "Ed25519Signature2018",

"created": "2020-04-22T10:37:22Z",

"proofPurpose": "assertionMethod",

"verificationMethod": "did:example:456#key-1",

"jws": "eyJjcml0IjpbImI2NCJdLCJiNjQiOmZhbHNlLCJhbGciOiJFZERTQSJ9..BhWew0x-txcroGjgdtK-yBCqoetg9DD9SgV4245TmXJi-PmqFzux6Cwaph0r-mbqzlE17yLebjfqbRT275U1AA"

}

}

[HALIMBAWA34](https://www.w3.org/TR/did-core/#example-verifiable-credential-linked-to-a-verification-method-of-type-jsonwebkey2020): Na-verify na Kredensyal na naka-link sa isang paraan ng pag-verify na may uri na JsonWebKey2020

{ *// external (all terms in this example)*

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.gov/credentials/3732",

"type": ["VerifiableCredential", "UniversityDegreeCredential"],

"issuer": { "id": "did:example:123" },

"issuanceDate": "2020-03-10T04:24:12.164Z",

"credentialSubject": {

"id": "did:example:456",

"degree": {

"type": "BachelorDegree",

"name": "Bachelor of Science and Arts"

}

},

"proof": {

"type": "JsonWebSignature2020",

"created": "2020-02-15T17:13:18Z",

"verificationMethod": "did:example:123#\_Qq0UL2Fq651Q0Fjd6TvnYE-faHiOpRlPVQcY\_-tA4A",

"proofPurpose": "assertionMethod",

"jws": "eyJiNjQiOmZhbHNlLCJjcml0IjpbImI2NCJdLCJhbGciOiJFZERTQSJ9..Y0KqovWCPAeeFhkJxfQ22pbVl43Z7UI-X-1JX32CA9MkFHkmNprcNj9Da4Q4QOl0cY3obF8cdDRdnKr0IwNrAw"

}

}

[HALIMBAWA35](https://www.w3.org/TR/did-core/#example-verifiable-credential-linked-to-a-bls12381-verification-method): Na-verify na Kredensyal na naka-link sa isang paraan ng pag-verify ng bls12381

{ *// external (all terms in this example)*

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://w3id.org/security/bbs/v1",

{

"name": "https://schema.org/name",

"birthDate": "https://schema.org/birthDate"

}

],

"id": "urn:uuid:c499e122-3ba9-4e95-8d4d-c0ebfcf8c51a",

"type": ["VerifiableCredential"],

"issuanceDate": "2021-02-07T16:02:08.571Z",

"issuer": {

"id": "did:example:123"

},

"credentialSubject": {

"id": "did:example:456",

"name": "John Smith",

"birthDate": "2021-02-07"

},

"proof": {

"type": "BbsBlsSignature2020",

"created": "2021-02-07T16:02:10Z",

"proofPurpose": "assertionMethod",

"proofValue": "o7zD2eNTp657YzkJLub+IO4Zqy/R3Lv/AWmtSA/kUlEAOa73BNyP1vOeoow35jkABolx4kYMKkp/ZsFDweuKwe/p9vxv9wrMJ9GpiOZjHcpjelDRRJLBiccg9Yv7608mHgH0N1Qrj14PZ2saUlfhpQ==",

"verificationMethod": "did:example:123#bls12381-g2-key"

}

}

[HALIMBAWA36](https://www.w3.org/TR/did-core/#example-verifiable-credential-selective-disclosure-zero-knowledge-proof-linked-to-a-bls12381-verification-method): Nabe-verify na Credential selective disclosure zero knowledge proof na naka-link sa isang bls12381 na paraan ng pag-verify

{ *// external (all terms in this example)*

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://w3id.org/security/bbs/v1",

{

"name": "https://schema.org/name",

"birthDate": "https://schema.org/birthDate"

}

],

"id": "urn:uuid:c499e122-3ba9-4e95-8d4d-c0ebfcf8c51a",

"type": "VerifiableCredential",

"issuanceDate": "2021-02-07T16:02:08.571Z",

"issuer": {

"id": "did:example:123"

},

"credentialSubject": {

"id": "did:example:456",

"birthDate": "2021-02-07"

},

"proof": {

"type": "BbsBlsSignatureProof2020",

"created": "2021-02-07T16:02:10Z",

"nonce": "OqZHsV/aunS34BhLaSoxiHWK+SUaG4iozM3V+1jO06zRRNcDWID+I0uwtPJJ767Yo8Q=",

"proofPurpose": "assertionMethod",

"proofValue": "",

"verificationMethod": "did:example:123#bls12381-g2-key"

}

}

[HALIMBAWA37](https://www.w3.org/TR/did-core/#example-verifiable-credential-as-decoded-jwt): Na-verify na Kredensyal bilang Na-decode na JWT

{ *// external (all terms in this example)*

"protected": {

"kid": "did:example:123#\_Qq0UL2Fq651Q0Fjd6TvnYE-faHiOpRlPVQcY\_-tA4A",

"alg": "EdDSA"

},

"payload": {

"iss": "did:example:123",

"sub": "did:example:456",

"vc": {

"@context": [

"https://www.w3.org/2018/credentials/v1",

"https://www.w3.org/2018/credentials/examples/v1"

],

"id": "http://example.gov/credentials/3732",

"type": [

"VerifiableCredential",

"UniversityDegreeCredential"

],

"issuer": {

"id": "did:example:123"

},

"issuanceDate": "2020-03-10T04:24:12.164Z",

"credentialSubject": {

"id": "did:example:456",

"degree": {

"type": "BachelorDegree",

"name": "Bachelor of Science and Arts"

}

}

},

"jti": "http://example.gov/credentials/3732",

"nbf": 1583814252

},

"signature": "qSv6dpZJGFybtcifLwGf4ujzlEu-fam\_M7HPxinCbVhz9iIJCg70UMeQbPa1ex6BmQ2tnSS7F11FHnMB2bJRAw"

}

### **A.3Pag-encrypt**

Ang seksyong ito ay hindi normatibo.

TANDAAN

Ang mga halimbawang ito ay para sa mga layunin ng impormasyon lamang, ito ay itinuturing na isang pinakamahusay na kasanayan upang maiwasan ang pagkawala ng hindi kinakailangang impormasyon sa mga header ng JWE.

[HALIMBAWA38](https://www.w3.org/TR/did-core/#example-jwe-linked-to-a-verification-method-via-kid): Naka-link ang JWE sa isang paraan ng pag-verify sa pamamagitan ng bata

{ *// external (all terms in this example)*

"ciphertext": "3SHQQJajNH6q0fyAHmw...",

"iv": "QldSPLVnFf2-VXcNLza6mbylYwphW57Q",

"protected": "eyJlbmMiOiJYQzIwUCJ9",

"recipients": [

{

"encrypted\_key": "BMJ19zK12YHftJ4sr6Pz1rX1HtYni\_L9DZvO1cEZfRWDN2vXeOYlwA",

"header": {

"alg": "ECDH-ES+A256KW",

"apu": "Tx9qG69ZfodhRos-8qfhTPc6ZFnNUcgNDVdHqX1UR3s",

"apv": "ZGlkOmVsZW06cm9wc3RlbjpFa...",

"epk": {

"crv": "X25519",

"kty": "OKP",

"x": "Tx9qG69ZfodhRos-8qfhTPc6ZFnNUcgNDVdHqX1UR3s"

},

"kid": "did:example:123#zC1Rnuvw9rVa6E5TKF4uQVRuQuaCpVgB81Um2u17Fu7UK"

}

}

],

"tag": "xbfwwDkzOAJfSVem0jr1bA"

}

## B.Mga Pagsasaalang-alang sa Arkitektura

### **B.1Detalyadong Arkitektura Diagram**

Ang sumusunod ay isang diagram na nagpapakita ng mga relasyon sa pagitan [4.Modelo ng Data](https://www.w3.org/TR/did-core/#data-model) ,[5.Mga Pangunahing Katangian](https://www.w3.org/TR/did-core/#core-properties) , at [8.Pamamaraan](https://www.w3.org/TR/did-core/#methods) , at[7.Resolusyon](https://www.w3.org/TR/did-core/#resolution) .

Diagram

Description automatically generated

### **B.2Paglikha ng isang DID**

Ang paglikha ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay isang proseso na tinukoy ng bawat [DID Method](https://www.w3.org/TR/did-core/#dfn-did-methods) . Ang ilang [DID Methods](https://www.w3.org/TR/did-core/#dfn-did-methods) , gaya ng did:key, ay puro generative, kung kaya't ang isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) at isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) ay nabuo sa pamamagitan ng pagbabago ng isang piraso ng cryptographic na materyal sa isang conformant na [representasyon](https://www.w3.org/TR/did-core/" \l "dfn-representations) . Maaaring kailanganin ng ibang mga [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) ang paggamit ng isang [nabe-verify na registry ng data](https://www.w3.org/TR/did-core/#dfn-verifiable-data-registry) , kung saan ang [dokumento ng](https://www.w3.org/TR/did-core/" \l "dfn-did-documents)[DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) at DID ay kinikilalang umiiral ng mga third party kapag natapos na ang pagpaparehistro, gaya ng tinukoy ng kaukulang [pamamaraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) . Ang iba pang mga proseso ay maaaring tukuyin ng kani-kanilang mga[paraan ng DID](https://www.w3.org/TR/did-core/#dfn-did-methods) .

### **B.3Pagtukoy sa paksa ng DID**

Ang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay isang partikular na uri ng URI (Uniform Resource Identifier), kaya maaaring sumangguni ang [DID sa anumang mapagkukunan.](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers)Bawat [ [RFC3986](https://www.w3.org/TR/did-core/#bib-rfc3986) ]:

ang terminong "resource" ay ginagamit sa pangkalahatang kahulugan para sa anumang maaaring matukoy ng isang URI. [...] Ang isang mapagkukunan ay hindi kinakailangang ma-access sa pamamagitan ng Internet.

Ang mga mapagkukunan ay maaaring digital o pisikal, abstract o kongkreto. Anumang mapagkukunan na maaaring italaga ng isang URI ay maaaring italaga ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) . Ang mapagkukunang tinutukoy ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay ang [paksa](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ng DID .

Tinutukoy ng [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) ang [DID subject](https://www.w3.org/TR/did-core/#dfn-did-subjects) . Hindi inaasahang posibleng matukoy ang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) mula sa pagtingin sa [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) mismo, dahil ang mga [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay karaniwang makabuluhan lamang sa mga makina, hindi sa tao. Ang isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay malamang na hindi naglalaman ng anumang impormasyon tungkol sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) , kaya ang karagdagang impormasyon tungkol sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ay matutuklasan lamang sa pamamagitan ng paglutas ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) sa [dokumento](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ng DID , pagkuha ng isang napapatunayang kredensyal tungkol sa [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) , o sa pamamagitan ng iba pang paglalarawan ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) .

Habang ang halaga ng ari- [id](https://www.w3.org/TR/did-core/" \l "dfn-id)arian sa nakuhang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay dapat palaging tumugma sa [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na niresolba, kung ang aktwal na mapagkukunan na tinutukoy ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay maaaring magbago sa paglipas ng panahon ay nakadepende sa [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) . Halimbawa, ang isang [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) na nagpapahintulot na magbago ang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ay maaaring gamitin upang makabuo ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) para sa kasalukuyang naninirahan sa isang partikular na tungkulin—gaya ng CEO ng isang kumpanya—kung saan ang aktwal na taong sumasakop sa tungkulin ay maaaring mag-iba depende sa kung kailan naresolba ang [DID .](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers)

### **B.4Nagre-refer sa dokumento ng DID**

Ang [DID ay](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) tumutukoy sa [DID na paksa](https://www.w3.org/TR/did-core/#dfn-did-subjects) at nagresolba sa DID na [dokumento](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) (sa pamamagitan ng pagsunod sa protocol na tinukoy ng [DID method](https://www.w3.org/TR/did-core/#dfn-did-methods) ). Ang [dokumento](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ng DID ay hindi hiwalay na mapagkukunan mula sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) at walang [URI](https://www.w3.org/TR/did-core/#dfn-uri) na hiwalay sa [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) . Sa halip, ang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay isang artifact ng [resolusyon ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-resolution) na kinokontrol ng controller ng [DID](https://www.w3.org/TR/did-core/#dfn-did-controllers) para sa layuning ilarawan ang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) .

Ang pagkakaibang ito ay inilalarawan ng modelo ng graph na ipinapakita sa ibaba.

Diagram

Description automatically generated

(imgsrc: <https://www.w3.org/TR/did-core/diagrams/figure-a.1-did-and-did-document-graph.svg>)

*Pigura*8*Ang*[*DID*](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers)*ay isang identifier na itinalaga ng isang*[*DID controller*](https://www.w3.org/TR/did-core/#dfn-did-controllers)*upang sumangguni sa isang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) at malutas sa a*[*DID na dokumento*](https://www.w3.org/TR/did-core/#dfn-did-documents)*na naglalarawan sa*[*DID na paksa*](https://www.w3.org/TR/did-core/#dfn-did-subjects)*. Ang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay isang artifact ng [resolusyon ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-resolution) at hindi isang hiwalay na mapagkukunan na naiiba sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) . Tingnan din ang: [paglalarawan ng salaysay](https://www.w3.org/TR/did-core/" \l "did-and-did-document-graph-longdesc) .*

### **B.5Mga pahayag sa dokumento ng DID**

Ang bawat property sa isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) ay isang pahayag ng [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) na naglalarawan ng:

* Ang string ng mga character na tumutukoy sa mga identifier para sa [DID na paksa](https://www.w3.org/TR/did-core/#dfn-did-subjects) (hal., ang [id](https://www.w3.org/TR/did-core/" \l "dfn-id)at mga [alsoKnownAs](https://www.w3.org/TR/did-core/" \l "dfn-alsoknownas) katangian)
* Paano makipag-ugnayan sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) (hal., ang [verificationMethod](https://www.w3.org/TR/did-core/" \l "dfn-verificationmethod)at mga [service](https://www.w3.org/TR/did-core/#dfn-service) katangian).
* Paano bigyang-kahulugan ang partikular na representasyon ng [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) (hal., ang @contextproperty para sa isang JSON-LD na representasyon).

Ang tanging kinakailangang ari-arian sa isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) ay [id](https://www.w3.org/TR/did-core/#dfn-id), kaya iyon ang tanging pahayag na garantisadong nasa isang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) . Ang pahayag na iyon ay inilalarawan sa [Figure8](https://www.w3.org/TR/did-core/#did-and-did-document-graph) na may direktang ugnayan sa pagitan ng[DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) at ng [DID na paksa](https://www.w3.org/TR/did-core/#dfn-did-subjects) .

### **B.6Pagtuklas ng higit pang impormasyon tungkol sa paksa ng DID**

Ang mga opsyon para sa pagtuklas ng higit pang impormasyon tungkol sa [paksa ng DID ay](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) nakasalalay sa mga katangiang nasa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) . Kung [service](https://www.w3.org/TR/did-core/" \l "dfn-service)naroroon ang property, maaaring humiling ng karagdagang impormasyon mula sa isang [endpoint ng serbisyo](https://www.w3.org/TR/did-core/#dfn-service-endpoints) . Halimbawa, sa pamamagitan ng pagtatanong sa isang [endpoint ng serbisyo](https://www.w3.org/TR/did-core/#dfn-service-endpoints) na sumusuporta sa mga nabe-verify na kredensyal para sa isa o higit pang mga claim (mga katangian) na naglalarawan sa [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) .

Ang isa pang opsyon ay gamitin ang [alsoKnownAs](https://www.w3.org/TR/did-core/" \l "dfn-alsoknownas)property kung ito ay nasa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) . [Magagamit ito ng DID controller](https://www.w3.org/TR/did-core/" \l "dfn-did-controllers) upang magbigay ng listahan ng iba pang mga URI (kabilang ang iba pang mga [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ) na tumutukoy sa parehong [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) . Ang pagresolba o pag-derefer sa mga URI na ito ay maaaring magbunga ng iba pang mga paglalarawan o representasyon ng [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) gaya ng inilalarawan sa figure sa ibaba.

Diagram

Description automatically generated

(img src: <https://www.w3.org/TR/did-core/diagrams/figure-a.2-also-known-as-graph.svg>)

*Pigura*9*Ang isang*[*DID na dokumento*](https://www.w3.org/TR/did-core/#dfn-did-documents)*ay maaaring gumamit ng alsoKnownAs property upang igiit na ang isa pang*[*URI*](https://www.w3.org/TR/did-core/#dfn-uri)*(kabilang, ngunit hindi kinakailangan, isa pang*[*DID*](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers)*) ay tumutukoy sa parehong [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) . Tingnan din ang: [paglalarawan ng salaysay](https://www.w3.org/TR/did-core/" \l "alsoKnownAs-graph-longdesc) .*

### **B.7Naghahatid ng representasyon ng paksa ng DID**

Kung ang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ay isang digital na mapagkukunan na maaaring makuha mula sa internet, maaaring piliin ng isang [paraan ng DID na bumuo ng](https://www.w3.org/TR/did-core/" \l "dfn-did-methods)[URL ng DID](https://www.w3.org/TR/did-core/#dfn-did-urls) na nagbabalik ng representasyon ng mismong [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) . Halimbawa, ang isang schema ng data na nangangailangan ng paulit-ulit, nabe-verify na cryptographic na pagkakakilanlan ay maaaring magtalaga ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) , at magpasa ng isang tinukoy na parameter ng DID (tingnan ang [3.2.1DID Parameters](https://www.w3.org/TR/did-core/#did-parameters) ) ay maaaring gamitin bilang karaniwang paraan upang makuha ang representasyon ng schema na iyon.

Katulad nito, ang isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay maaaring gamitin upang sumangguni sa isang digital na mapagkukunan (tulad ng isang imahe) na maaaring ibalik nang direkta mula sa isang [nabe-verify na registry ng data](https://www.w3.org/TR/did-core/#dfn-verifiable-data-registry) kung ang functionality na iyon ay sinusuportahan ng naaangkop na [paraan ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-methods) .

### **B.8Pagtatalaga ng mga DID sa mga kasalukuyang mapagkukunan ng web**

Kung ang controller ng isang web page o anumang iba pang web resource ay gustong magtalaga dito ng isang tuluy-tuloy, cryptographically verifiable identifier, maaaring bigyan ito ng controller ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) . Halimbawa, ang may-akda ng isang blog na hino-host ng isang blog hosting company (sa ilalim ng domain ng hosting company na iyon) ay maaaring gumawa ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) para sa blog. Sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) , maaaring isama ng may-akda ang [alsoKnownAs](https://www.w3.org/TR/did-core/" \l "dfn-alsoknownas)property na tumuturo sa kasalukuyang URL ng blog, hal:

"alsoKnownAs": ["https://myblog.blogging-host.example/home"]

Kung pagkatapos ay inilipat ng may-akda ang blog sa ibang kumpanya ng pagho-host (o sa sariling domain ng may-akda), maaaring i-update ng may-akda ang [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) upang tumuro sa bagong URL para sa blog, hal:

"alsoKnownAs": ["https://myblog.example/"]

Ang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay epektibong nagdaragdag ng isang layer ng hindi direksyon para sa URL ng blog. Ang layer ng indidirection na ito ay nasa ilalim ng kontrol ng may-akda sa halip na nasa ilalim ng kontrol ng isang panlabas na administratibong awtoridad gaya ng blog hosting company. Ito ay kung paano epektibong gumana ang isang [DID bilang pinahusay na](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers)[URN (Uniform Resource Name)](https://tools.ietf.org/html/rfc8141) —isang patuloy na pagkakakilanlan para sa mapagkukunan ng impormasyon na ang lokasyon ng network ay maaaring magbago sa paglipas ng panahon.

### **B.9Ang ugnayan sa pagitan ng DID controllers at DID subjects**

Upang maiwasan ang pagkalito, nakakatulong na uriin ang mga [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) sa dalawang magkahiwalay na hanay batay sa kanilang kaugnayan sa [controller ng DID](https://www.w3.org/TR/did-core/#dfn-did-controllers) .

#### B.9.1Set #1: Ang DID na paksa ay ang DID controller

Ang unang kaso, na ipinakita sa[Figure10](https://www.w3.org/TR/did-core/" \l "controller-subject-equivalence" \o "Ang paksa ng DID ay kapareho ng entity ng DID controller.  Tingnan din ang: paglalarawan ng salaysay.), ay ang karaniwang senaryo kung saan ang [DID na paksa](https://www.w3.org/TR/did-core/#dfn-did-subjects) ay ang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) din . Ito ang kaso kapag ang isang indibidwal o organisasyon ay lumikha ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) upang makilala ang sarili.

Diagram

Description automatically generated

(img src: <https://www.w3.org/TR/did-core/diagrams/figure-b.1-controller-and-subject-equivalence.svg>)

Pigura10 Ang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ay ang parehong entity bilang ang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) . Tingnan din ang: [paglalarawan ng salaysay](https://www.w3.org/TR/did-core/" \l "controller-subject-equivalence-longdesc) .

Mula sa pananaw ng modelo ng graph, kahit na ang mga node ay natukoy bilang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) at [DID subject](https://www.w3.org/TR/did-core/#dfn-did-subjects) in [Figure10](https://www.w3.org/TR/did-core/#controller-subject-equivalence)ay naiiba, mayroong isang lohikal na arko na nagkokonekta sa kanila upang ipahayag ang isang semantic equivalence na relasyon.

#### B.9.2Set #2: Ang paksa ng DID ay hindi ang DID controller

Ang pangalawang kaso ay kapag ang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ay isang hiwalay na entity mula sa [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) . Ito ang kaso kapag, halimbawa, ang isang magulang ay lumikha at nagpapanatili ng kontrol ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) para sa isang bata; ang isang korporasyon ay lumilikha at nagpapanatili ng kontrol ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) para sa isang subsidiary; o ang isang manufacturer ay gumagawa at nagpapanatili ng kontrol ng isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) para sa isang produkto, isang IoT device, o isang digital na file.

Mula sa perspektibo ng modelo ng graph, ang tanging pagkakaiba mula sa Set 1 na walang katumbas na ugnayang arko sa pagitan ng [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) at mga node ng [controller ng DID.](https://www.w3.org/TR/did-core/#dfn-did-controllers)

### **B.10Maramihang DID controllers**

Ang isang [DID na dokumento ay](https://www.w3.org/TR/did-core/#dfn-did-documents) maaaring may higit sa isang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) . Ito ay maaaring mangyari sa isa sa dalawang paraan.

#### B.10.1Malayang Pagkontrol

Sa kasong ito, ang bawat isa sa mga [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) ay maaaring kumilos sa sarili nitong, ibig sabihin, ang bawat isa ay may ganap na kapangyarihan na i-update ang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) nang nakapag-iisa. Mula sa pananaw ng modelo ng graph, sa pagsasaayos na ito:

* Ang bawat karagdagang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) ay isa pang natatanging graph node (na maaaring matukoy ng sarili nitong [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ).
* Ang parehong mga arko ("kontrol" at "controller") ay umiiral sa pagitan ng bawat [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) at ng [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) .Diagram

  Description automatically generated

*Pigura*11*Maramihang independiyenteng*[*DID controllers*](https://www.w3.org/TR/did-core/#dfn-did-controllers)*na bawat isa ay maaaring kumilos nang nakapag-iisa. Tingnan din ang: [Paglalarawan ng Teksto](https://www.w3.org/TR/did-core/" \l "independent-did-controllers-longdesc)*

#### B.10.2Kontrol ng Grupo

Sa kaso ng kontrol ng grupo, ang mga [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) ay inaasahang kumilos nang magkakasama sa ilang paraan, gaya ng kapag gumagamit ng cryptographic algorithm na nangangailangan ng maramihang digital signature ("multi-sig") o isang threshold number ng digital signatures ("m-of -n"). Mula sa isang functional na pananaw, ang opsyong ito ay katulad ng isang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) dahil, bagama't ang bawat isa sa [DID controllers](https://www.w3.org/TR/did-core/#dfn-did-controllers) sa [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) group ay may sarili nitong graph node, ang aktwal na control ay bumagsak sa isang solong logical graph node na kumakatawan sa [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) group tulad ng ipinapakita . sa [Figure12](https://www.w3.org/TR/did-core/#group-did-controllers).

Diagram

Description automatically generated

(img src: <https://www.w3.org/TR/did-core/diagrams/figure-c.2-group-did-controllers.svg>)

Pigura12 Maramihang [DID controllers](https://www.w3.org/TR/did-core/#dfn-did-controllers) na inaasahang kumilos nang sama-sama bilang isang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) group. Tingnan din ang: [paglalarawan ng salaysay](https://www.w3.org/TR/did-core/" \l "group-did-controllers-longdesc) .

Ang configuration na ito ay madalas na malalapat kapag ang [paksa ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ay isang organisasyon, korporasyon, ahensya ng gobyerno, komunidad, o iba pang grupo na hindi kontrolado ng isang indibidwal.

### **B.11Pagbabago ng paksa ng DID**

Ang isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) ay may eksaktong isang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) na tumutukoy sa [DID na paksa](https://www.w3.org/TR/did-core/#dfn-did-subjects) . Ang [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) ay ipinahayag bilang ang halaga ng ari- [id](https://www.w3.org/TR/did-core/" \l "dfn-id)arian. Ang halaga ng ari-arian na ito ay hindi nababago para sa buhay ng [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) .

Gayunpaman, posible na ang mapagkukunang tinukoy ng [DID](https://www.w3.org/TR/did-core/#dfn-decentralized-identifiers) , ang [paksa](https://www.w3.org/TR/did-core/" \l "dfn-did-subjects) ng DID , ay maaaring magbago sa paglipas ng panahon. Ito ay nasa ilalim ng eksklusibong awtoridad ng [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) . Para sa higit pang mga detalye, tingnan ang seksyon [9.16Pagtitiyaga](https://www.w3.org/TR/did-core/#persistence) .

### **B.12Pagbabago ng DID controller**

Ang [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) para sa isang [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) ay maaaring magbago sa paglipas ng panahon. Gayunpaman, depende sa kung paano ito ipinatupad, ang isang pagbabago sa [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) ay maaaring hindi makita sa pamamagitan ng mga pagbabago sa mismong [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) . Halimbawa, kung ang pagbabago ay ipinatupad sa pamamagitan ng pagbabago sa pagmamay-ari ng mga pinagbabatayan na cryptographic key o iba pang mga kontrol na ginagamit para sa isa o higit pa sa mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) sa [dokumento ng DID](https://www.w3.org/TR/did-core/" \l "dfn-did-documents) , maaaring hindi ito makilala sa karaniwang pag-ikot ng key.

Sa kabilang banda, kung ang pagbabago ay ipinatupad sa pamamagitan ng pagbabago ng halaga ng ari- [controller](https://www.w3.org/TR/did-core/" \l "dfn-controller)arian, ito ay magiging transparent.

Kung mahalagang i-verify ang pagbabago ng [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) , pinapayuhan ang mga implementer na [patunayan](https://www.w3.org/TR/did-core/" \l "dfn-authenticated) ang bagong [DID controller](https://www.w3.org/TR/did-core/#dfn-did-controllers) laban sa mga [paraan ng pag-verify](https://www.w3.org/TR/did-core/" \l "dfn-verification-method) sa binagong [DID na dokumento](https://www.w3.org/TR/did-core/#dfn-did-documents) .

## C.Kasaysayan ng Pagbabago

Ang seksyong ito ay naglalaman ng mga pagbabagong ginawa mula nang mailathala ang detalyeng ito bilang isang W3C First Public Working Draft.

Ang mga pagbabago mula noong [Ikalawang Rekomendasyon ng Kandidato ay](https://www.w3.org/TR/2021/CR-did-core-20210615/) kinabibilangan ng:

* Non-normatively sumangguni sa detalye ng DID Resolution upang gabayan ang mga nagpapatupad patungo sa mga karaniwang pattern ng pagpapatupad ng DID URL.
* Ipaliwanag kung kailan ang DID Documents ay nauunawaang magsisimulang umiiral.
* I-convert ang mga PNG diagram sa mga SVG diagram.
* Muling ayusin ang pagkakasunud-sunod ng mga Appendice upang mapabuti ang pagiging madaling mabasa.
* I-update ang gabay ng IANA bilang resulta ng mga pagsisikap ng IETF Media Type Maintenance Working Group.
* Magdagdag ng mga link upang gamitin ang dokumento ng mga kaso.
* Magdagdag ng babala na nauugnay sa [ [MULTIBASE](https://www.w3.org/TR/did-core/#bib-multibase) ] at publicKeyMultibase.
* Alisin ang mga marker ng isyu sa panganib para sa mga feature na nakakuha ng sapat na karanasan sa pagpapatupad.
* I-finalize ang impormasyon ng Editors, Authors, at Acknowledgements.

Ang mga pagbabago mula noong [Rekomendasyon ng Unang Kandidato ay](https://www.w3.org/TR/2021/CR-did-core-20210318/) kinabibilangan ng:

* Pagdaragdag ng mga nasa panganib na marker sa karamihan ng Mga Parameter ng DID, ang mga datatype ng data model na inaasahang hindi ipapatupad, at ang application/did+ld+json na uri ng media. Ang pagbabagong ito ay nagresulta sa desisyon ng DID WG na magsagawa ng pangalawang yugto ng Rekomendasyon ng Kandidato. Ang lahat ng iba pang mga pagbabago ay alinman sa editoryal o hinulaang sa "nasa panganib" na mga marker ng isyu.
* Pag-alis ng nasa panganib na marker ng isyu para sa method-specific-idpanuntunan ng ABNF at para sa nextUpdateat nextVersionId.
* Paglilinaw na equivalentIdat canonicalIdopsyonal.
* Pagdaragdag ng mga kahulugan para sa "pag-atake ng amplification" at "cryptographic suite".
* Pagpapalit ng publicKeyBase58may publicKeyMultibase.
* Mga update sa seksyon ng mga halimbawa ng DID Document.
* Isang malaking bilang ng mga editoryal na paglilinis sa seksyong Mga Pagsasaalang-alang sa Seguridad.

Kasama sa mga pagbabago mula noong [First Public Working Draft](https://www.w3.org/TR/2019/WD-did-core-20191107/) ang:

* Ang pagpapakilala ng abstract data model na maaaring i-serialize sa maraming representasyon kabilang ang JSON at JSON-LD.
* Ang pagpapakilala ng isang DID Specifications Registry para sa mga layunin ng pagpaparehistro ng mga katangian ng extension, representasyon, DID Resolution input metadata at output metadata, DID Document metadata, DID parameters, at DID Methods.
* Paghihiwalay ng metadata ng DID Document, gaya ng mga ginawa at na-update na value, mula sa mga property ng DID Document.
* Ang pag-alis ng mga naka-embed na patunay sa DID Document.
* Ang pagdaragdag ng mga ugnayan sa pag-verify para sa mga layunin ng pagpapatunay, paggigiit, pangunahing kasunduan, pag-uutos ng kakayahan at pagtatalaga ng kakayahan.
* Ang kakayahang suportahan ang pag-uugnay ng maraming identifier sa DID Document, gaya ng DID controller, na kilala rin bilang, katumbas na ID, at canonical ID.
* Pagpapahusay ng privacy sa pamamagitan ng pagbabawas ng impormasyon na maaaring maglaman ng personal na nakakapagpakilalang impormasyon sa DID Document.
* Ang pagdaragdag ng isang malaking seksyon sa mga pagsasaalang-alang sa seguridad at mga pagsasaalang-alang sa privacy.
* Isang seksyon ng Representasyon na nagdedetalye kung paano magagawa at magagamit ang abstract data model sa iba't ibang format kasama ng mga pangkalahatang tuntunin para sa lahat ng representasyon, producer, at consumer.
* Isang seksyong nagdedetalye sa DID Resolution at DID URL Dereferencing interface na kahulugan na inaasahang ilantad ng lahat ng DID resolver pati na rin ang mga input at output sa mga prosesong iyon.
* Mga halimbawa ng DID Document sa isang appendix na nagbibigay ng mas kumplikadong mga halimbawa ng mga serialization ng DID Document.
* Mga Pagsasaalang-alang ng IANA para sa maraming representasyong tinukoy sa DID Core.
* Pag-aalis ng seksyong Trabaho sa Hinaharap dahil ang karamihan sa gawain ay nagawa na ngayon.
* Isang seksyon ng pagkilala.

## D.Mga Pasasalamat

Ang Working Group ay nagpaabot ng malalim na pagpapahalaga at taos-pusong pasasalamat sa aming mga Tagapangulo na sina Brent Zundel at Dan Burnett, gayundin sa aming W3C Staff Contact, Ivan Herman, para sa kanilang walang pagod na trabaho sa pagpapanatili ng Working Group na patungo sa isang produktibong direksyon at pag-navigate sa malalim at mapanganib na tubig. ng proseso ng pamantayan.

Ang Working Group ay buong pasasalamat na kinikilala ang gawain na humantong sa paglikha ng detalyeng ito, at nagpaabot ng taos-pusong pagpapahalaga sa mga indibidwal na nagtrabaho sa mga teknolohiya at mga detalye na lubos na nakaimpluwensya sa aming trabaho. Sa partikular, kabilang dito ang gawa ni Phil Zimmerman, Jon Callas, Lutz Donnerhacke, Hal Finney, David Shaw, at Rodney Thayer sa [Pretty Good Privacy (PGP)](https://en.wikipedia.org/wiki/Pretty_Good_Privacy) noong 1990s at 2000s.

Noong kalagitnaan ng 2010s, ang mga paunang pagpapatupad ng kung ano ang magiging Decentralized Identifiers ay [binuo](https://web-payments.org/minutes/2014-05-07/" \l "topic-1) sa pakikipagtulungan sa Telehash project ni Jeremie Miller at sa W3C Web Payments Community Group na pinamumunuan ni Dave Longley at Manu Sporny. [Makalipas ang isang taon, nagsimulang tuklasin](https://docs.google.com/document/d/1EP-KhH60y-nl4xkEzoeSf3DjmjLomfboF4p2umF51FA/) ng XDI.org Registry Working Group ang mga desentralisadong teknolohiya para sa pagpapalit sa dati nitong identifier registry. Ilan sa mga unang [nakasulat na](https://github.com/WebOfTrustInfo/rwot1-sf/blob/master/final-documents/dpki.pdf)[papel](https://github.com/WebOfTrustInfo/rwot2-id2020/blob/master/final-documents/requirements-for-dids.pdf) ang paggalugad sa konsepto ng Mga Desentralisadong Identifier ay maaaring masubaybayan pabalik sa unang ilang workshop sa Rebooting the Web of Trust na ipinatawag ni Christopher Allen. Ang gawaing iyon ay humantong sa isang pangunahing pakikipagtulungan sa pagitan nina Christopher Allen, Drummond Reed, Les Chasen, Manu Sporny, at Anil John. Nakita ni Anil ang pangako sa teknolohiya at inilaan ang paunang hanay ng pagpopondo ng pamahalaan upang galugarin ang espasyo. Kung wala ang suporta ni Anil John at ang kanyang patnubay sa paglipas ng mga taon, malamang na ang Decentralized Identifiers ay nasa kung nasaan sila ngayon. Ang karagdagang pagpipino sa mga workshop sa Rebooting the Web of Trust ay humantong sa [unang dokumentasyon ng mga tagapagpatupad](https://github.com/WebOfTrustInfo/rwot3-sf/blob/master/final-documents/did-implementer-draft-10.pdf), inedit ni Drummond Reed, Les Chasen, Christopher Allen, at Ryan Grant. Kasama sa mga nag-ambag sina Manu Sporny, Dave Longley, Jason Law, Daniel Hardman, Markus Sabadello, Christian Lundkvist, at Jonathan Endersby. Ang paunang gawaing ito ay pinagsama sa W3C Credentials Community Group, pinalubha pa, at pagkatapos ay inilipat sa W3C Decentralized Identifiers Working Group para sa pandaigdigang standardisasyon.

Ang mga bahagi ng trabaho sa detalyeng ito ay pinondohan ng Departamento ng Homeland Security (US DHS) Science and Technology Directorate sa ilalim ng mga kontrata HSHQDC-16-R00012-H-SB2016-1-002, at HSHQDC-17-C-00019 , pati na rin ang US DHS Silicon Valley Innovation Program sa ilalim ng mga kontratang 70RSAT20T00000010, 70RSAT20T00000029, 70RSAT20T00000030, 70RSAT20T00000045, 70RSAT20T03000, 70RSAT20T03000, 70RSAT20T03,200 at Ang nilalaman ng detalyeng ito ay hindi kinakailangang sumasalamin sa posisyon o patakaran ng US Government at walang opisyal na pag-endorso ang dapat na ipahiwatig.

Ang mga bahagi ng trabaho sa detalyeng ito ay pinondohan din ng programang StandICT.eu ng European Union sa ilalim ng numero ng kontrata ng sub-grantee na CALL05/19. Ang nilalaman ng detalyeng ito ay hindi kinakailangang sumasalamin sa posisyon o patakaran ng European Union at walang opisyal na pag-endorso ang dapat ipahiwatig.

Ang paggawa sa detalyeng ito ay sinusuportahan din ng komunidad ng [Rebooting the Web of Trust na](https://www.weboftrust.info/) pinangasiwaan ni Christopher Allen, Shannon Appelcline, Kiara Robles, Brian Weller, Betty Dhamers, Kaliya Young, Kim Hamilton Duffy, Manu Sporny, Drummond Reed, Joe Andrieu, at Heather Vescent. Ang pagbuo ng detalyeng ito ay sinusuportahan din ng [W3C Credentials Community Group](https://w3c-ccg.github.io/) , na pinangunahan nina Kim Hamilton Duffy, Joe Andrieu, Christopher Allen, Heather Vescent, at Wayne Chang. Sinuportahan din ng mga kalahok sa Internet Identity Workshop, na pinangasiwaan nina Phil Windley, Kaliya Young, Doc Searls, at Heidi Nobantu Saul, ang gawaing ito sa pamamagitan ng maraming sesyon ng pagtatrabaho na idinisenyo upang makipagdebate, pagbutihin, at turuan ang mga kalahok tungkol sa detalyeng ito.

Ang Working Group ay nagpapasalamat sa mga sumusunod na indibidwal para sa kanilang mga kontribusyon sa detalyeng ito (sa alpabetikong pagkakasunud-sunod, ang Github handle ay nagsisimula sa@at pinagsunod-sunod bilang mga apelyido): Denis Ah-Kang, Nacho Alamillo, Christopher Allen, Joe Andrieu, Antonio, Phil Archer, George Aristy, Baha, Juan Benet, BigBlueHat, Dan Bolser, Chris Boscolo, Pelle Braendgaard, Daniel Buchner, Daniel Burnett, Juan Caballero, @cabo, Tim Cappalli, Melvin Carvalho, David Chadwick, Wayne Chang, Sam Curren, Hai Dang, Tim Daubenschütz, Oskar van Deventer, Kim Hamilton Duffy, Arnaud Durand, Ken Ebert, Veikko Eeva, @ewagner70, Carson Magsasaka, Nikos Fotiou, Gabe, Gayan, @gimly-jack, @gjgd, Ryan Grant, Peter Grassberger, Adrian Gropper, Amy Guy, Daniel Hardman, Kyle Den Hartog, Philippe Le Hegaret, Ivan Herman, Michael Herman, Alen Horvat, Dave Huseby, Marcel Jackisch, Mike Jones, Andrew Jones, Tom Jones, jonnycrunch, Gregg Kellogg, Michael Klein, @kdenhartog-sybil1, Paul Knowles, @ktobich, David I. Lehn, Charles E. Lehner,Michael Lodder, @mooreT1881, Dave Longley, Tobias Looker, Wolf McNally, Robert Mitwicki, Mircea Nistor, Grant Noble, Mark Nottingham, @oare, Darrell O'Donnell, Vinod Panicker, Dirk Porsche, Praveen, Mike Prorock, @pukkamustard, Drummond Reed, Julian Reschke, Yancy Ribbens, Justin Richer, Rieks, @rknobloch, Mikeal Rogers, Evstifeev Roman, Troy Ronda, Leonard Rosenhol, Michael Ruminer, Markus Sabadello, Cihan Saglam, Samu, Rob Sanderson, Wendy Seltzer, Mehran Shakeri, Jaehoon ( Ace) Shim, Samuel Smith, James M Snell, SondreB, Manu Sporny, @ssstolk, Orie Steele, Shigeya Suzuki, Sammotic Switchyarn, @tahpot, Oliver Terbu, Ted Thibodeau Jr., Joel Thorstensson, Tralcan, Henry Tsai, Rod Vagg, Mike Varley, Kaliya "Identity Woman" Young, Eric Welton, Fuqiao Xue, @Yue, Dmitri Zagidulin, @zhanb, at Brent Zundel.Dave Longley, Tobias Looker, Wolf McNally, Robert Mitwicki, Mircea Nistor, Grant Noble, Mark Nottingham, @oare, Darrell O'Donnell, Vinod Panicker, Dirk Porsche, Praveen, Mike Prorock, @pukkamustard, Drummond Reed, Julian Reschke, Yancy Ribbens, Justin Richer, Rieks, @rknobloch, Mikeal Rogers, Evstifeev Roman, Troy Ronda, Leonard Rosenhol, Michael Ruminer, Markus Sabadello, Cihan Saglam, Samu, Rob Sanderson, Wendy Seltzer, Mehran Shakeri, Jaehoon (Ace) Shim, Samuel Smith , James M Snell, SondreB, Manu Sporny, @ssstolk, Orie Steele, Shigeya Suzuki, Sammotic Switchyarn, @tahpot, Oliver Terbu, Ted Thibodeau Jr., Joel Thorstensson, Tralcan, Henry Tsai, Rod Vagg, Mike Varley, Kaliya "Identity Babae" Young, Eric Welton, Fuqiao Xue, @Yue, Dmitri Zagidulin, @zhanb, at Brent Zundel.Dave Longley, Tobias Looker, Wolf McNally, Robert Mitwicki, Mircea Nistor, Grant Noble, Mark Nottingham, @oare, Darrell O'Donnell, Vinod Panicker, Dirk Porsche, Praveen, Mike Prorock, @pukkamustard, Drummond Reed, Julian Reschke, Yancy Ribbens, Justin Richer, Rieks, @rknobloch, Mikeal Rogers, Evstifeev Roman, Troy Ronda, Leonard Rosenhol, Michael Ruminer, Markus Sabadello, Cihan Saglam, Samu, Rob Sanderson, Wendy Seltzer, Mehran Shakeri, Jaehoon (Ace) Shim, Samuel Smith , James M Snell, SondreB, Manu Sporny, @ssstolk, Orie Steele, Shigeya Suzuki, Sammotic Switchyarn, @tahpot, Oliver Terbu, Ted Thibodeau Jr., Joel Thorstensson, Tralcan, Henry Tsai, Rod Vagg, Mike Varley, Kaliya "Identity Babae" Young, Eric Welton, Fuqiao Xue, @Yue, Dmitri Zagidulin, @zhanb, at Brent Zundel.Robert Mitwicki, Mircea Nistor, Grant Noble, Mark Nottingham, @oare, Darrell O'Donnell, Vinod Panicker, Dirk Porsche, Praveen, Mike Prorock, @pukkamustard, Drummond Reed, Julian Reschke, Yancy Ribbens, Justin Richer, Rieks, @rknobloch , Mikeal Rogers, Evstifeev Roman, Troy Ronda, Leonard Rosethol, Michael Ruminer, Markus Sabadello, Cihan Saglam, Samu, Rob Sanderson, Wendy Seltzer, Mehran Shakeri, Jaehoon (Ace) Shim, Samuel Smith, James M Snell, SondreB, Manu Sporny , @ssstolk, Orie Steele, Shigeya Suzuki, Sammotic Switchyarn, @tahpot, Oliver Terbu, Ted Thibodeau Jr., Joel Thorstensson, Tralcan, Henry Tsai, Rod Vagg, Mike Varley, Kaliya "Identity Woman" Young, Eric Welton, Fuqiao Xue , @Yue, Dmitri Zagidulin, @zhanb, at Brent Zundel.Robert Mitwicki, Mircea Nistor, Grant Noble, Mark Nottingham, @oare, Darrell O'Donnell, Vinod Panicker, Dirk Porsche, Praveen, Mike Prorock, @pukkamustard, Drummond Reed, Julian Reschke, Yancy Ribbens, Justin Richer, Rieks, @rknobloch , Mikeal Rogers, Evstifeev Roman, Troy Ronda, Leonard Rosethol, Michael Ruminer, Markus Sabadello, Cihan Saglam, Samu, Rob Sanderson, Wendy Seltzer, Mehran Shakeri, Jaehoon (Ace) Shim, Samuel Smith, James M Snell, SondreB, Manu Sporny , @ssstolk, Orie Steele, Shigeya Suzuki, Sammotic Switchyarn, @tahpot, Oliver Terbu, Ted Thibodeau Jr., Joel Thorstensson, Tralcan, Henry Tsai, Rod Vagg, Mike Varley, Kaliya "Identity Woman" Young, Eric Welton, Fuqiao Xue , @Yue, Dmitri Zagidulin, @zhanb, at Brent Zundel.Dirk Porsche, Praveen, Mike Prorock, @pukkamustard, Drummond Reed, Julian Reschke, Yancy Ribbens, Justin Richer, Rieks, @rknobloch, Mikeal Rogers, Evstifeev Roman, Troy Ronda, Leonard Rosenhol, Michael Ruminer, Markus Sabadello, Cihan Saglam, Samu , Rob Sanderson, Wendy Seltzer, Mehran Shakeri, Jaehoon (Ace) Shim, Samuel Smith, James M Snell, SondreB, Manu Sporny, @ssstolk, Orie Steele, Shigeya Suzuki, Sammotic Switchyarn, @tahpot, Oliver Terbu, Ted Thibodeau Jr. , Joel Thorstensson, Tralcan, Henry Tsai, Rod Vagg, Mike Varley, Kaliya "Identity Woman" Young, Eric Welton, Fuqiao Xue, @Yue, Dmitri Zagidulin, @zhanb, at Brent Zundel.Dirk Porsche, Praveen, Mike Prorock, @pukkamustard, Drummond Reed, Julian Reschke, Yancy Ribbens, Justin Richer, Rieks, @rknobloch, Mikeal Rogers, Evstifeev Roman, Troy Ronda, Leonard Rosenhol, Michael Ruminer, Markus Sabadello, Cihan Saglam, Samu , Rob Sanderson, Wendy Seltzer, Mehran Shakeri, Jaehoon (Ace) Shim, Samuel Smith, James M Snell, SondreB, Manu Sporny, @ssstolk, Orie Steele, Shigeya Suzuki, Sammotic Switchyarn, @tahpot, Oliver Terbu, Ted Thibodeau Jr. , Joel Thorstensson, Tralcan, Henry Tsai, Rod Vagg, Mike Varley, Kaliya "Identity Woman" Young, Eric Welton, Fuqiao Xue, @Yue, Dmitri Zagidulin, @zhanb, at Brent Zundel.Michael Ruminer, Markus Sabadello, Cihan Saglam, Samu, Rob Sanderson, Wendy Seltzer, Mehran Shakeri, Jaehoon (Ace) Shim, Samuel Smith, James M Snell, SondreB, Manu Sporny, @ssstolk, Orie Steele, Shigeya Suzuki, Sammotic Switchyarn, @tahpot, Oliver Terbu, Ted Thibodeau Jr., Joel Thorstensson, Tralcan, Henry Tsai, Rod Vagg, Mike Varley, Kaliya "Identity Woman" Young, Eric Welton, Fuqiao Xue, @Yue, Dmitri Zagidulin, @zhanb, at Brent Zundel .Michael Ruminer, Markus Sabadello, Cihan Saglam, Samu, Rob Sanderson, Wendy Seltzer, Mehran Shakeri, Jaehoon (Ace) Shim, Samuel Smith, James M Snell, SondreB, Manu Sporny, @ssstolk, Orie Steele, Shigeya Suzuki, Sammotic Switchyarn, @tahpot, Oliver Terbu, Ted Thibodeau Jr., Joel Thorstensson, Tralcan, Henry Tsai, Rod Vagg, Mike Varley, Kaliya "Identity Woman" Young, Eric Welton, Fuqiao Xue, @Yue, Dmitri Zagidulin, @zhanb, at Brent Zundel .Dmitri Zagidulin, @zhanb, at Brent Zundel.Dmitri Zagidulin, @zhanb, at Brent Zundel.

## E.Mga Pagsasaalang-alang ng IANA

Ang seksyong ito ay isusumite sa Internet Engineering Steering Group (IESG) para sa pagsusuri, pag-apruba, at pagpaparehistro sa IANA kapag ang detalyeng ito ay naging isang Iminungkahing Rekomendasyon ng W3C .

### **E.1application/did+json**

**Pangalan ng uri:**

aplikasyon

**Pangalan ng subtype:**

ginawa+json

**Mga kinakailangang parameter:**

wala

**Opsyonal na mga parameter:**

wala

**Mga pagsasaalang-alang sa pag-encode:**

Tingnan [ang RFC 8259, seksyon 11](https://www.rfc-editor.org/rfc/rfc8259#section-11) .

**Mga pagsasaalang-alang sa seguridad:**

Tingnan ang [RFC 8259, seksyon 12](https://www.rfc-editor.org/rfc/rfc8259#section-12) [ [RFC8259](https://www.w3.org/TR/did-core/#bib-rfc8259) ].

**Mga pagsasaalang-alang sa interoperability:**

Hindi maaari

**Nai-publish na detalye:**

https://www.w3.org/TR/did-core/

**Mga application na gumagamit ng ganitong uri ng media:**

Anumang application na nangangailangan ng identifier na desentralisado, nagpapatuloy, nabe-verify sa pamamagitan ng cryptographic, at nareresolba. Karaniwang binubuo ang mga application ng mga cryptographic identity system, desentralisadong network ng mga device, at mga website na naglalabas o nagbe-verify ng W3C Verifiable Credentials.

**Karagdagang impormasyon:**

**(mga) magic number:**

Hindi maaari

**(mga) extension ng file:**

.didjson

**Macintosh file type code(s):**

TEKSTO

**Tao at email address na makontak para sa karagdagang impormasyon:**

Ivan Herman <ivan@w3.org>

**Nilalayon na paggamit:**

Karaniwan

**Mga paghihigpit sa paggamit:**

wala

**(Mga) May-akda:**

Drummond Reed, Manu Sporny, Markus Sabadello, Dave Longley, Christopher Allen

**Baguhin ang controller:**

W3C

Ang mga fragment identifier na ginamit sa [application/did+json](https://www.w3.org/TR/did-core/#application-did-json) ay ginagamot ayon sa mga panuntunang tinukoy sa [Fragment](https://www.w3.org/TR/did-core/#fragment) .

### **E.2application/did+ld+json**

TANDAAN : IETF Structured Media Uri

Ang yugto ng Rekomendasyon ng Kandidato para sa detalyeng ito ay nakatanggap ng malaking bilang ng mga pagpapatupad para sa application/did+ld+jsonuri ng media. Ang pagpaparehistro ng uri ng media application/did+ld+jsonsa IANA ay nakabinbing paglutas ng isyu ng [Mga Uri ng Media na may Maramihang Suffix .](https://datatracker.ietf.org/doc/html/draft-w3cdidwg-media-types-with-multiple-suffixes)Inaasahan na magpapatuloy ang trabaho sa [IETF Media Type Maintenance Working Group](https://datatracker.ietf.org/wg/mediaman/about/) na may pagpaparehistro ng application/did+ld+jsonuri ng media sa pamamagitan ng W3C kasunod ng ilang sandali matapos ang paglalathala ng [Media Types with Multiple Suffixes](https://datatracker.ietf.org/doc/html/draft-w3cdidwg-media-types-with-multiple-suffixes) RFC.

**Pangalan ng uri:**

aplikasyon

**Pangalan ng subtype:**

ginawa+ld+json

**Mga kinakailangang parameter:**

wala

**Opsyonal na mga parameter:**

wala

**Mga pagsasaalang-alang sa pag-encode:**

Tingnan [ang RFC 8259, seksyon 11](https://www.rfc-editor.org/rfc/rfc8259#section-11) .

**Mga pagsasaalang-alang sa seguridad:**

Tingnan ang [JSON-LD 1.1, Mga Pagsasaalang-alang sa Seguridad](https://www.w3.org/TR/json-ld11/#security) [ [JSON-LD11](https://www.w3.org/TR/did-core/#bib-json-ld11) ].

**Mga pagsasaalang-alang sa interoperability:**

Hindi maaari

**Nai-publish na detalye:**

<https://www.w3.org/TR/did-core/>

Anumang application na nangangailangan ng identifier na desentralisado, nagpapatuloy, nabe-verify sa pamamagitan ng cryptographic, at nareresolba. Karaniwang binubuo ang mga application ng mga cryptographic identity system, desentralisadong network ng mga device, at mga website na naglalabas o nagbe-verify ng W3C Verifiable Credentials.  
  
**Karagdagang impormasyon:**

**(mga) magic number:**

Hindi maaari

**(mga) extension ng file:**

.didjsonld

**Macintosh file type code(s):**

TEKSTO

**Tal address na makontak para sa karagdagang impormasyon:**

Ivan Herman [ivan@w3.org](mailto:ivan@w3.org)

**Nilalayon na paggamit:**

Karaniwan  
**Mga hiht:**

Wala

**(Mga) May-akda:**

Drummond Reed, Manu Sporny, Markus Sabadello, Dave Longley, Christopher Allen  
**Baguh**W3C

Ang a

**]**

[Infra Standard](https://infra.spec.whatwg.org/) . Anne van Kesteren; Domenic Denicola. WHATWG. Pamantayan sa Pamumuhay. URL:<https://infra.spec.whatwg.org/>

**[JSON-LD11]**

[JSON-LD 1.1](https://www.w3.org/TR/json-ld11/) . Gregg Kellogg; Pierre-Antoine Champin; Dave Longley. W3C. 16 Hulyo 2020. Rekomendasyon ng W3C. URL:<https://www.w3.org/TR/json-ld11/>

**[RFC2119]**

[Mga pangunahing salita para sa paggamit sa mga RFC upang Ipahiwatig ang Mga Antas ng Kinakailangan](https://www.rfc-editor.org/rfc/rfc2119) . S. Bradner. IETF. Marso 1997. Pinakamahusay na Kasalukuyang Kasanayan. URL:<https://www.rfc-editor.org/rfc/rfc2119>

**[RFC3552]**

[Mga Alituntunin para sa Pagsulat ng RFC Text sa Mga Pagsasaalang-alang sa Seguridad](https://www.rfc-editor.org/rfc/rfc3552) . E. Rescorla; B. Korver. IETF. Hulyo 2003. Pinakamahusay na Kasalukuyang Kasanayan. URL:<https://www.rfc-editor.org/rfc/rfc3552>

**[RFC3986]**

[Uniform Resource Identifier (URI): Generic Syntax](https://www.rfc-editor.org/rfc/rfc3986) . T. Berners-Lee; R. Fielding; L. Master. IETF. Enero 2005. Internet Standard. URL:<https://www.rfc-editor.org/rfc/rfc3986>

**[RFC5234]**

[Augmented BNF para sa Syntax Specifications: ABNF](https://www.rfc-editor.org/rfc/rfc5234) . D. Crocker, Ed.; P. Sa kabuuan. IETF. Enero 2008. Internet Standard. URL:<https://www.rfc-editor.org/rfc/rfc5234>

**[RFC7517]**

[JSON Web Key (JWK)](https://www.rfc-editor.org/rfc/rfc7517) . M. Jones. IETF. Mayo 2015. Iminungkahing Pamantayan. URL:<https://www.rfc-editor.org/rfc/rfc7517>

**[RFC7638]**

[JSON Web Key (JWK) Thumbprint](https://www.rfc-editor.org/rfc/rfc7638) . M. Jones; N. Sakimura. IETF. Setyembre 2015. Iminungkahing Pamantayan. URL:<https://www.rfc-editor.org/rfc/rfc7638>

**[RFC8174]**

[Kalabuan ng Malaking titik kumpara sa Maliit na titik sa RFC 2119 Key Words](https://www.rfc-editor.org/rfc/rfc8174) . B. Leiba. IETF. Mayo 2017. Pinakamahusay na Kasalukuyang Kasanayan. URL:<https://www.rfc-editor.org/rfc/rfc8174>

**[RFC8259]**

[Ang Format ng Pagpapalitan ng Data ng JavaScript Object Notation (JSON)](https://www.rfc-editor.org/rfc/rfc8259) . T. Bray, Ed.. IETF. Disyembre 2017. Internet Standard. URL:<https://www.rfc-editor.org/rfc/rfc8259>

**[url]**

[URL Standard](https://url.spec.whatwg.org/) . Anne van Kesteren. WHATWG. Pamantayan sa Pamumuhay. URL:<https://url.spec.whatwg.org/>

**[XMLSCHEMA11-2]**

[W3C XML Schema Definition Language (XSD) 1.1 Bahagi 2: Mga Uri ng Data](https://www.w3.org/TR/xmlschema11-2/) . David Peterson; Sandy Gao; Ashok Malhotra; Michael Sperberg-McQueen; Henry Thompson; Paul V. Biron et al. W3C. 5 Abril 2012. Rekomendasyon ng W3C. URL:<https://www.w3.org/TR/xmlschema11-2/>**]**

[Desentralisadong Identifier Resolution](https://w3c-ccg.github.io/did-resolution/) . Markus Sabadello; Dmitri Zagidulin. Pangkat ng Komunidad ng Mga Kredensyal. Draft Ulat ng Grupo ng Komunidad. URL:<https://w3c-ccg.github.io/did-resolution/>

**[DID-RUBRIC]**

[Rubric ng Desentralisadong Katangian v1.0](https://w3c.github.io/did-rubric/) . Joe Andrieu. Pangkat ng Komunidad ng Mga Kredensyal. Draft Ulat ng Grupo ng Komunidad. URL:<https://w3c.github.io/did-rubric/>

**[DID-SPEC-REGISTRIES]**

[Mga Rehistro ng Detalye ng DID](https://www.w3.org/TR/did-spec-registries/) . Orie Steele; Manu Sporny; Michael Prorock. W3C. 28 Hunyo 2022. W3C Working Group Note. URL:<https://www.w3.org/TR/did-spec-registries/>

**[MGA KASO-GINAMIT]**

[Mga Kaso ng Paggamit at Mga Kinakailangan para sa Mga Desentralisadong Identifier](https://www.w3.org/TR/did-use-cases/) . Joe Andrieu; Phil Archer; Kim Duffy; Ryan Grant; Adrian Gropper. W3C. 17 Marso 2021. Tala ng W3C Working Group. URL:<https://www.w3.org/TR/did-use-cases/>

**[DNS-DID]**

[Ang Decentralized Identifier (DID) sa DNS](https://datatracker.ietf.org/doc/draft-mayrhofer-did-dns/) . Alexander Mayrhofer; Dimitrij Klesev; Markus Sabadello. Pebrero 2019. Internet-Draft. URL:<https://datatracker.ietf.org/doc/draft-mayrhofer-did-dns/>

**[HASHLINK]**

[Mga Cryptographic Hyperlink](https://tools.ietf.org/html/draft-sporny-hashlink-05) . Manu Sporny. IETF. Disyembre 2018. Internet-Draft. URL:<https://tools.ietf.org/html/draft-sporny-hashlink-05>

**[IANA-URI-SCHEMES]**

[Uniform Resource Identifier (URI) Scheme](https://www.iana.org/assignments/uri-schemes/uri-schemes.xhtml) . IANA. URL:<https://www.iana.org/assignments/uri-schemes/uri-schemes.xhtml>

**[MATRIX-URIS]**

[Matrix URIs - Mga Ideya tungkol sa Web Architecture](https://www.w3.org/DesignIssues/MatrixURIs.html) . Tim Berners-Lee. Disyembre 1996. Personal na Pananaw. URL:<https://www.w3.org/DesignIssues/MatrixURIs.html>

**[MULTIBASE]**

[Ang Multibase Encoding Scheme](https://datatracker.ietf.org/doc/html/draft-multiformats-multibase-03) . Juan Benet; Manu Sporny. IETF. Pebrero 2021. Internet-Draft. URL:<https://datatracker.ietf.org/doc/html/draft-multiformats-multibase-03>

**[PRIVACY-BY-DESIGN]**

[Pagkapribado ayon sa Disenyo](https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf) . Ann Cavoukian. Komisyoner ng Impormasyon at Pagkapribado. 2011. URL:<https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf>

**[RFC4122]**

[Isang Universally Unique IDentifier (UUID) URN Namespace](https://www.rfc-editor.org/rfc/rfc4122) . P. Leach; M. Pagkain; R. Salz. IETF. Hulyo 2005. Iminungkahing Pamantayan. URL:<https://www.rfc-editor.org/rfc/rfc4122>

**[RFC6901]**

[JavaScript Object Notation (JSON) Pointer](https://www.rfc-editor.org/rfc/rfc6901) . P. Bryan, Ed.; K. Zyp; M. Nottingham, Ed.. IETF. Abril 2013. Iminungkahing Pamantayan. URL:<https://www.rfc-editor.org/rfc/rfc6901>

**[RFC6973]**

[Mga Pagsasaalang-alang sa Privacy para sa Mga Protocol sa Internet](https://www.rfc-editor.org/rfc/rfc6973) . A. Cooper; H. Tschofenig; B. Aboba; J. Peterson; J. Morris; M. Hansen; R. Smith. IETF. Hulyo 2013. Impormasyon. URL:<https://www.rfc-editor.org/rfc/rfc6973>

**[RFC7230]**

[Hypertext Transfer Protocol (HTTP/1.1): Syntax at Routing ng Mensahe](https://httpwg.org/specs/rfc7230.html) . R. Fielding, Ed.; J. Reschke, Ed.. IETF. Hunyo 2014. Iminungkahing Pamantayan. URL:<https://httpwg.org/specs/rfc7230.html>

**[RFC7231]**

[Hypertext Transfer Protocol (HTTP/1.1): Semantics at Content](https://httpwg.org/specs/rfc7231.html) . R. Fielding, Ed.; J. Reschke, Ed.. IETF. Hunyo 2014. Iminungkahing Pamantayan. URL:<https://httpwg.org/specs/rfc7231.html>

**[RFC8141]**

[Uniform Resource Names (URNs)](https://www.rfc-editor.org/rfc/rfc8141) . P. Saint-Andre; J. Klensin. IETF. Abril 2017. Iminungkahing Pamantayan. URL:<https://www.rfc-editor.org/rfc/rfc8141>

**[VC-DATA-MODEL]**

[Modelo ng Data ng Mga Na-verify na Kredensyal v1.1](https://www.w3.org/TR/vc-data-model/) . Manu Sporny; Grant Noble; Dave Longley; Daniel Burnett; Brent Zundel; Kyle Den Hartog. W3C. 3 Marso 2022. Rekomendasyon ng W3C. URL:<https://www.w3.org/TR/vc-data-model/>