Web Crypto (Re-) Introduction

Ryan Sleevi
Google, Inc

A "quick" charter recap...

Goals

The Web Cryptography Working Group will develop a **Recommendation-track** document that defines an API that lets developers implement secure application protocols on the level of Web applications, including message confidentiality and authentication services, by exposing trusted cryptographic primitives from the browser. This will promote higher security insofar as Web application developers will no longer have to create their own or use untrusted third-party libraries for cryptographic primitives.

Primary features

- key generation
- encryption
- decryption
- signature generation
- signature verification
- hashing
- message authentication codes
- key transport
- key agreement
- random number generation
- key derivation
- key storage

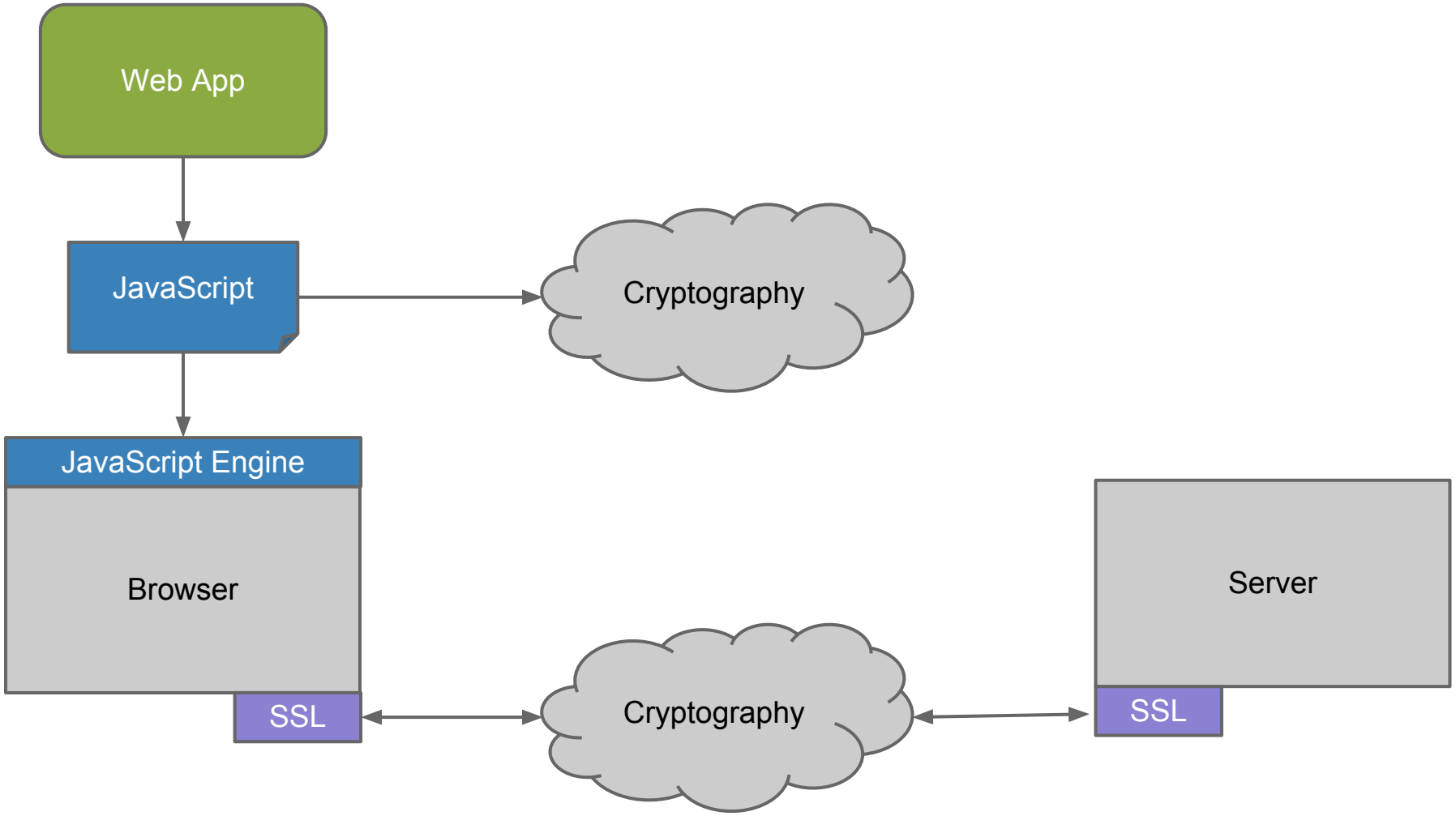
Secondary features

- TLS session login/logout
- TLS key export/derivation
- Simplified data protection function
- Multiple key containers
- Key import/export
- Key properties
- Key lifecycle management
  - Enrollment
  - Selection
  - Revocation

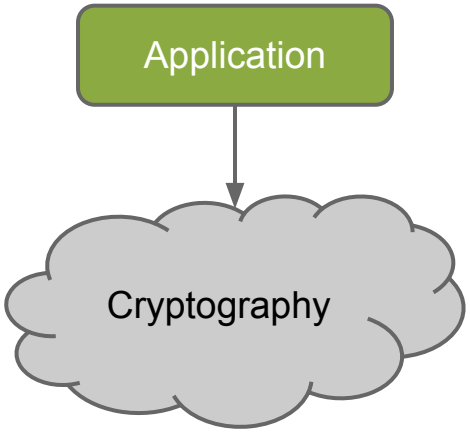
… WOW

... why?

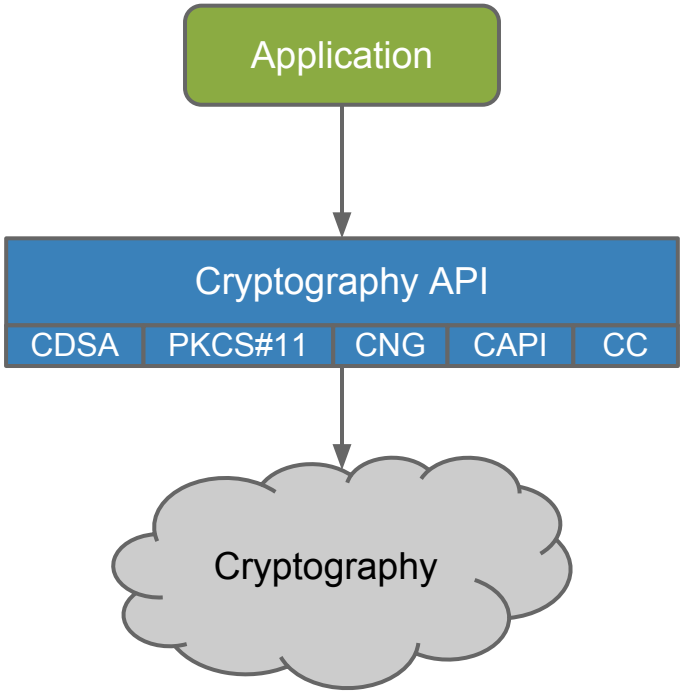
Web Apps Today



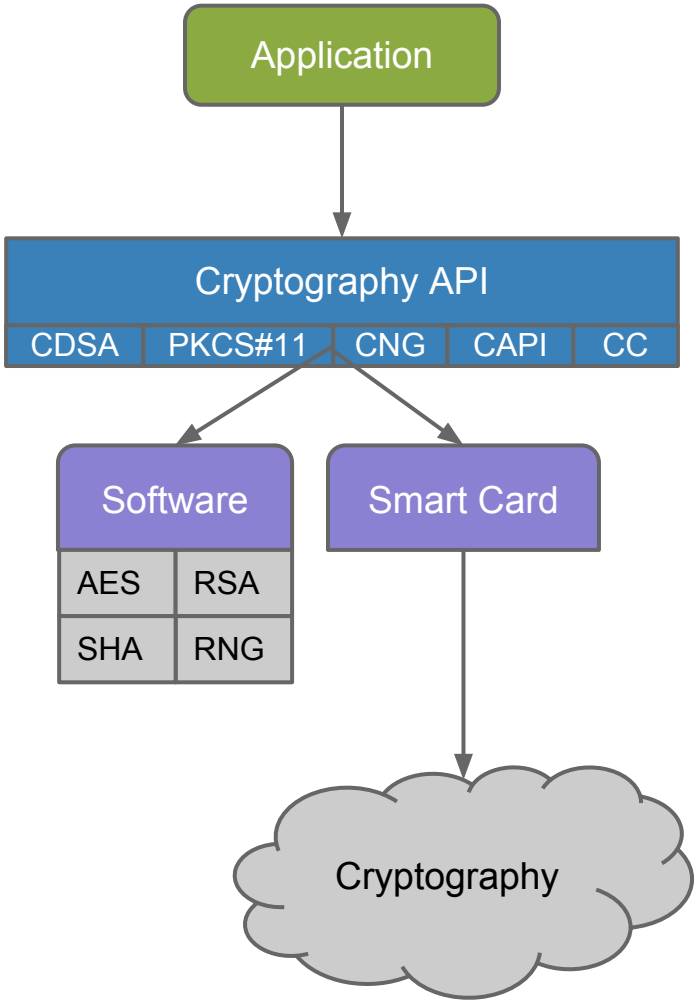
Native Apps Today



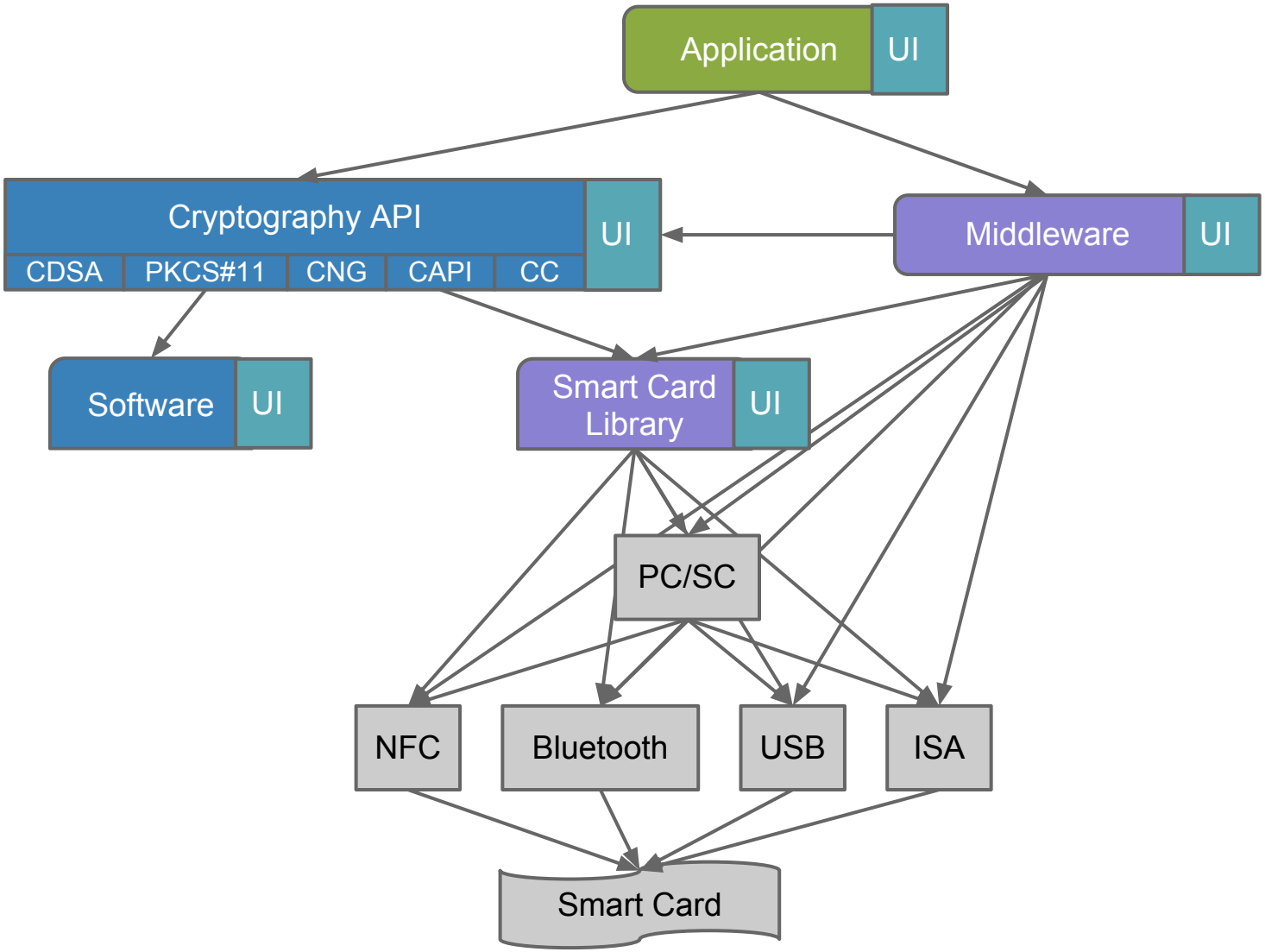
Native Apps Today



Native Apps Today



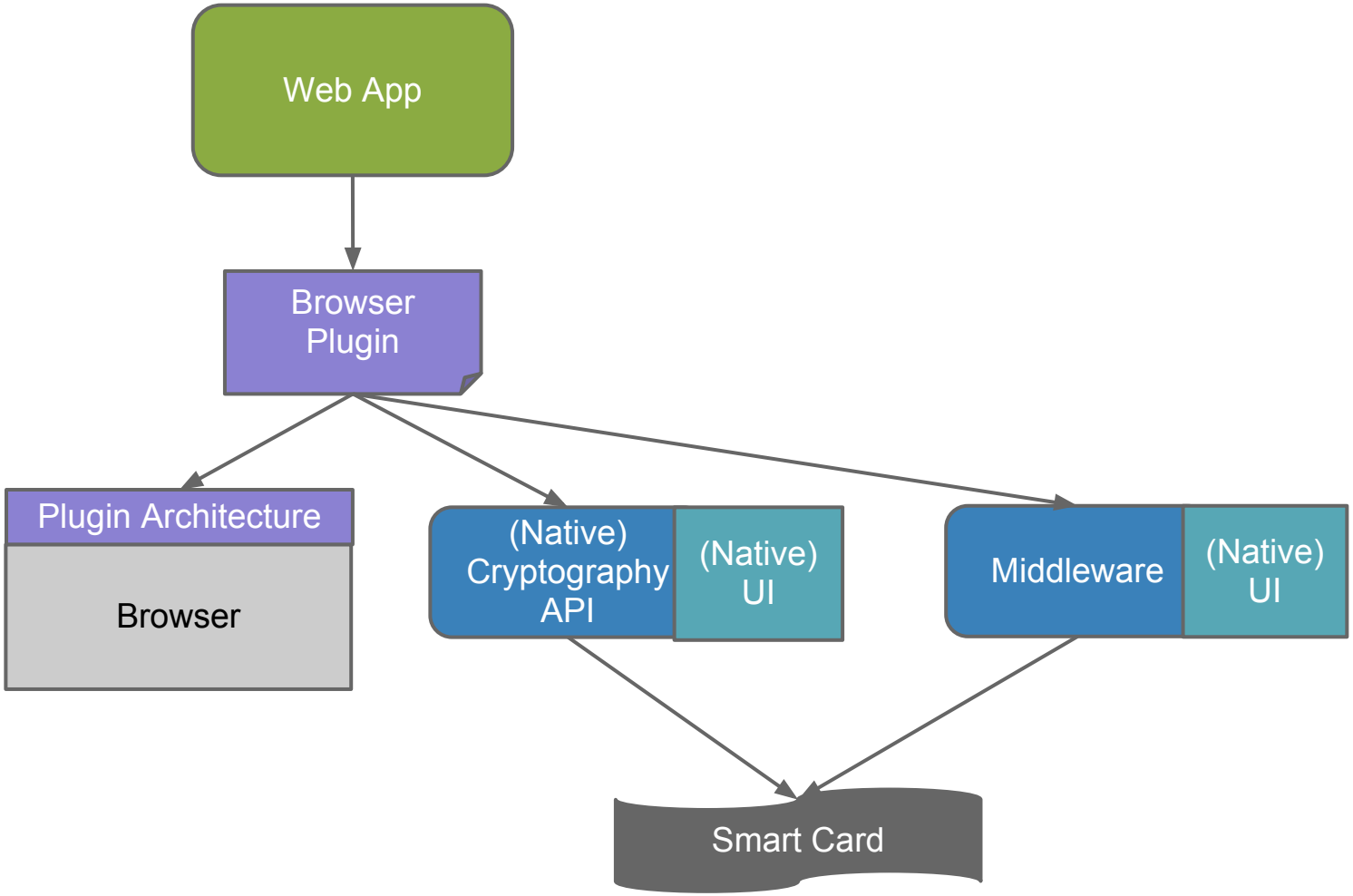
Native Apps Today



... but wait

Web Apps Today

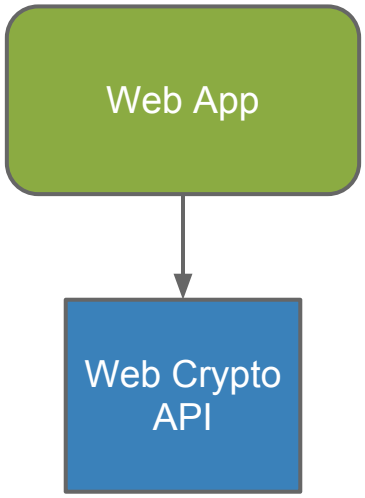
(in Asia and Europe)



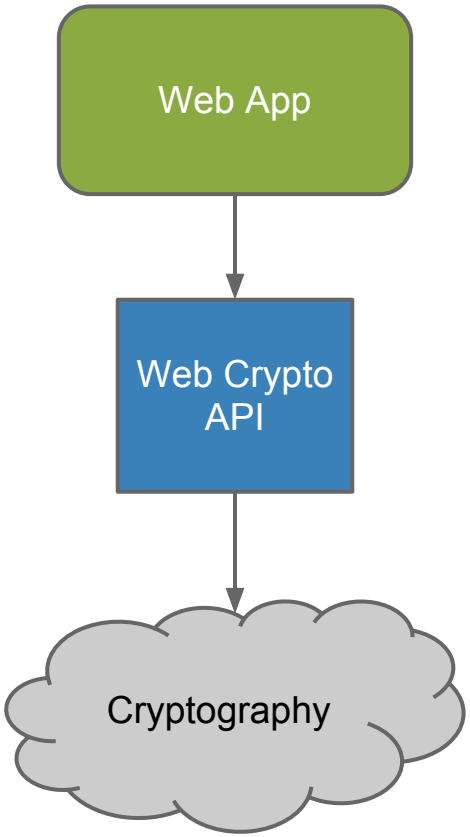
Plugins are *not* the Web App Way

The (possible) future with Web Crypto API

Web Apps Tomorrow, Case 1



Web Apps Tomorrow, Case 2



Web Apps Tomorrow, Case 3