

W3C



Technology & Society @W3C / MIT CSAIL
Wendy Seltzer, wseltzer@w3.org
@wseltzer



Products[11]

state. (e.g. Line Model[12] ,X11 Uxola[13] ,
NeXTStep[14] , Servers[15] , Tools[16] , Mail
robot[17] , Library[18])

Technical[19]

Details of protocols, formats, program internals
etc



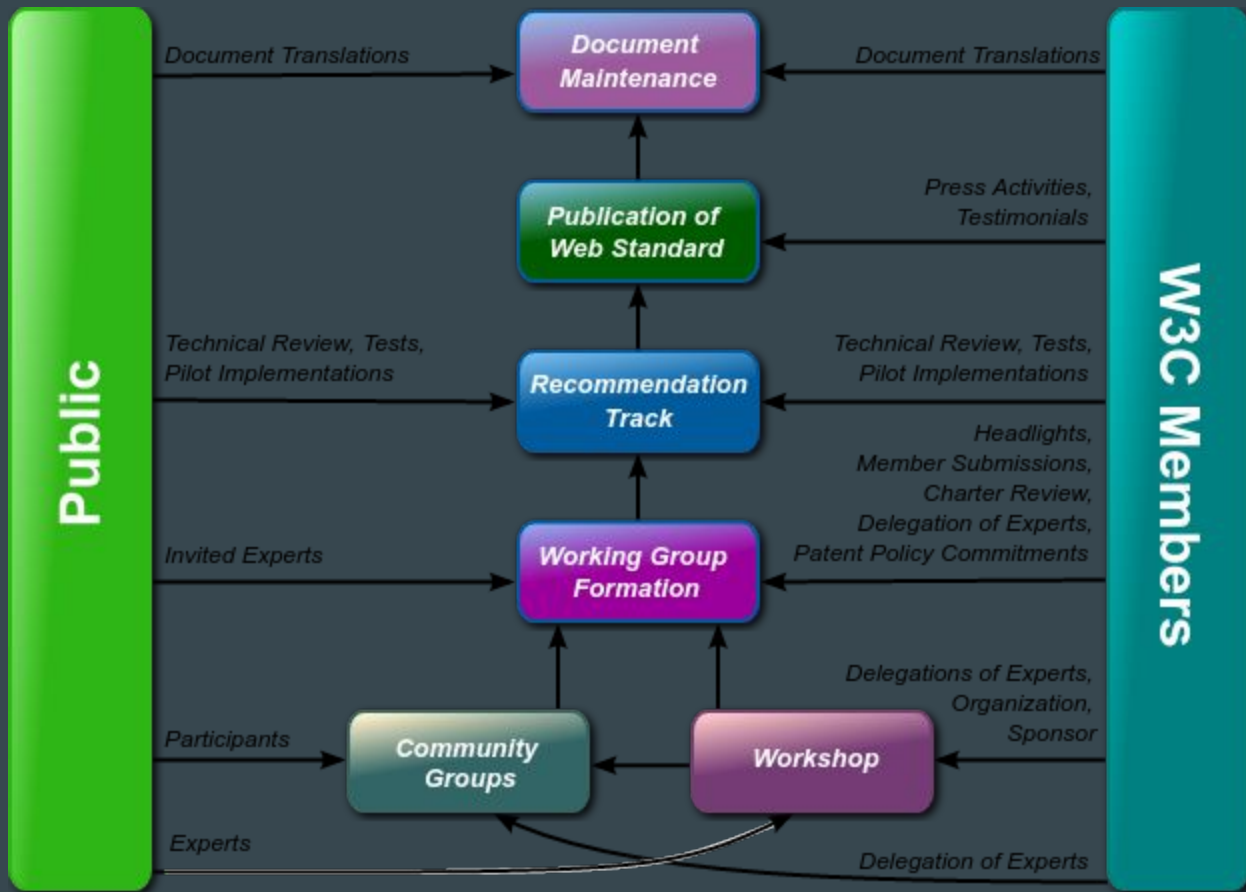
SIR TIM BERNERS-LEE
INVENTOR OF THE WORLD WIDE WEB
Director, W3C

World Wide Web Consortium (W3C)



Voluntary standard-setting. Stewarding the Open Web Platform.

- ~400 Member organizations, thousands of participants
- ~65 staff
- Working Groups develop specifications (Recommendations)
- Interest Groups, Community Groups develop use cases and requirements, incubate
- Governed by [W3C Process](#), Art of Consensus
- Royalty-Free [Patent Policy](#)



Blockchain and Web Standards

Web support for Blockchain

e.g., crypto, formats, APIs

Blockchain support for Web

e.g., cert transparency

Standards

Improvement,
harmonization, consensus

Innovation

Incubation

Some W3C Work

Security & Privacy:

Web Authentication

Web Crypto

Web Application Security

Web Payments

Privacy IG

HTML (Web Platform WG)

Web Performance

CSS

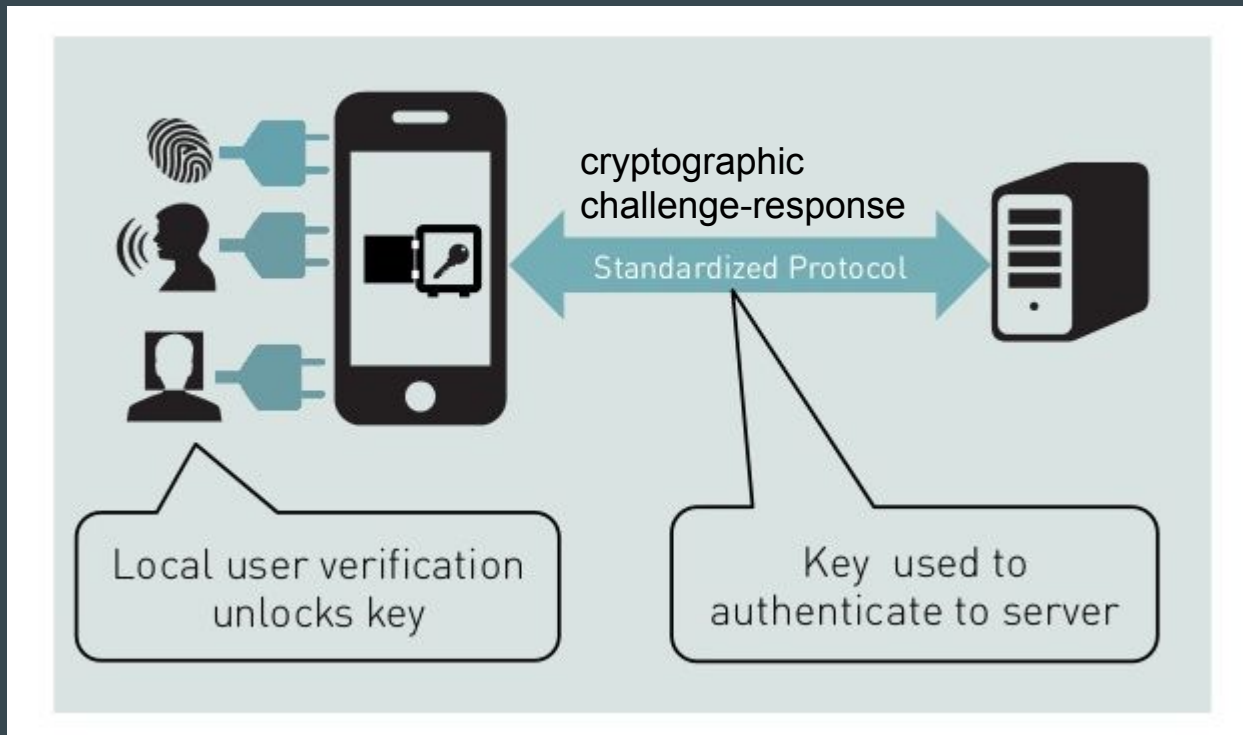
HTML Media

WebRTC

WebAuthn

WebAuthn, building a Web API for FIDO 2.0, uses a cryptographic challenge **unique** to each website and **bound** to its origin.

Local authentication such as biometrics never leaves the device.

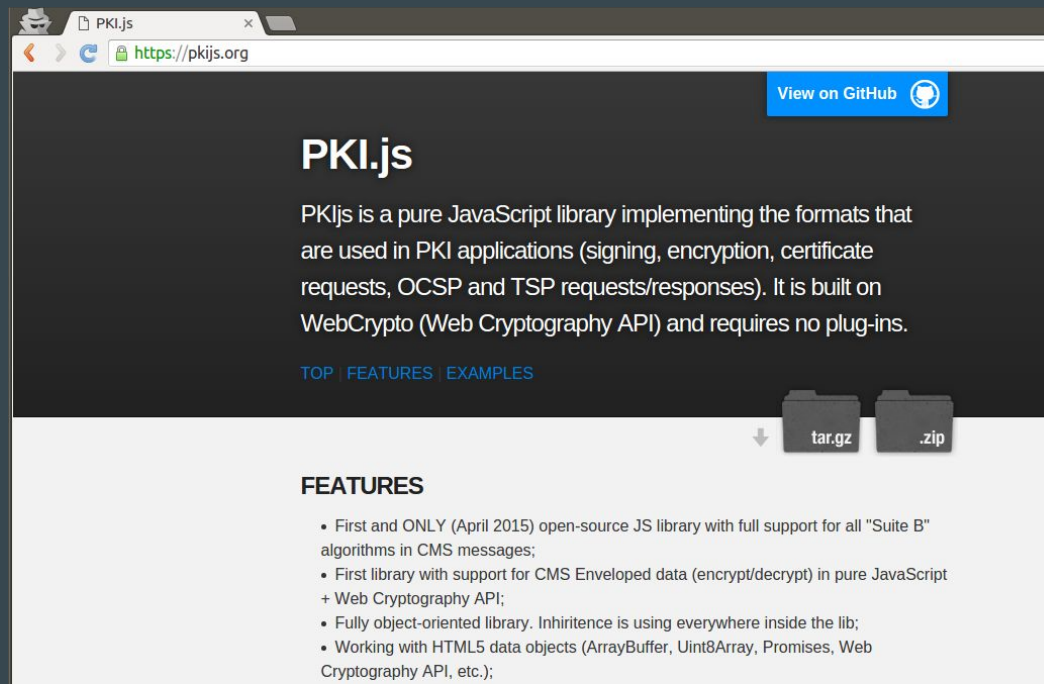


WebCrypto API

Enable web application developers to build on standard javascript crypto across browsers.

Used by, e.g.,

OpenWhisper's Signal desktop
PKI.js



The screenshot shows a web browser window with the URL <https://pkij.s.org>. The page has a dark header with a "View on GitHub" button. The main content area is dark and features the title "PKI.js" in large white text. Below the title is a paragraph describing the library as a pure JavaScript implementation of PKI formats, built on WebCrypto. There are links for "TOP", "FEATURES", and "EXAMPLES". At the bottom of the dark section, there are two download buttons labeled "tar.gz" and ".zip". The "FEATURES" section is highlighted in white and contains a bulleted list of features.

View on GitHub

PKI.js

PKI.js is a pure JavaScript library implementing the formats that are used in PKI applications (signing, encryption, certificate requests, OCSP and TSP requests/responses). It is built on WebCrypto (Web Cryptography API) and requires no plug-ins.

[TOP](#) | [FEATURES](#) | [EXAMPLES](#)

tar.gz .zip

FEATURES

- First and ONLY (April 2015) open-source JS library with full support for all "Suite B" algorithms in CMS messages;
- First library with support for CMS Enveloped data (encrypt/decrypt) in pure JavaScript + Web Cryptography API;
- Fully object-oriented library. Inheritance is using everywhere inside the lib;
- Working with HTML5 data objects (ArrayBuffer, Uint8Array, Promises, Web Cryptography API, etc.);

WebAppSec

Enlisting the User Agent in Cooperative Policy Enforcement

- Content Security Policy
- Subresource Integrity
- Mixed Content Blocking

Security Related APIs

- Permissions API
- Credential Management

Experiments in the Web Security Model / Same Origin Policy

- Confinement with Origin Web Labels (COWL)

Encryption Everywhere

WebAppSec Standardizing and Enabling HTTPS for confidentiality, integrity, and authentication

- Secure Contexts
- Upgrade Insecure Requests
- Mixed Content
- Referrer Policy
- Subresource Integrity

- Let's Encrypt

IETF

- Certificate Transparency
- HSTS, HPKP

Web Payments

Payment Request API

Payment Method Identifiers

Basic Card Payment

In-progress: Payment Apps, Payment Method Specs

Links

Overview of Security at W3C: <https://www.w3.org/Security>

WebCrypto: <https://www.w3.org/TR/WebCryptoAPI/>

WebAppSec: <https://www.w3.org/2011/webappsec/>

Web Authentication: <https://w3c.github.io/webauthn/>

Hardware-Based Secure Services: <https://www.w3.org/community/hb-secure-services/>

Payments: <https://www.w3.org/Payments/>

Thanks!



Wendy Seltzer
wseltzer@w3.org <https://wendy.seltzer.org/>
@wseltzer +1.617.715.4883