W3C UPDATE MEETING #4
OCT. 16, 2014

WebCrypto

Axel Nennker, Telekom Innovation Laboratories

LIFE IS FOR SHARING.

W3C UPDATE MEETING #4
WEBCRYPTO

- WebCrypto WG Status
- WebCrypto Next Steps Workshop

W3C UPDATE MEETING #4
WEBCRYPTO WG STATUS

- WebCrypto Standard is in Last Call
- Heated discussion about W3C standardization process

- Collaboration with IETF JOSE WG on key formats and algorithm names
  - Common members in both WGs
  - JOSE is in IETF App Dir review
- Browser implementations by Google and Mozilla (and Microsoft)
  - https://bugzilla.mozilla.org/show_bug.cgi?id=865789

http://www.w3.org/2012/webcrypto/
http://www.w3.org/TR/WebCryptoAPI/

W3C UPDATE MEETING #4
WEBCRYPTO NEXT STEPS WORKSHOP

W3C

Web Cryptography Next Steps

W3C Workshop on Authentication, Hardware Tokens and Beyond

10-11 September 2014, Silicon Valley (Mountain View), California

Workshop report anticipated early October 2014.

Home | Agenda | Papers | How to Participate | Logistics | Program Committee

Many projects and companies are now requiring high security Web applications with improved authentication, and the W3C is positioned to enable technologies ranging from simple multi-factor authentication to full-blown smartcard-based authentication available to Web applications. For an example of new relevant work, the Web Cryptography API will soon expose standardized cryptographic functionality to Web applications across all major browsers.

Before re-chartering Web Cryptography Working Group or any new Working Group, the W3C believes that consensus around a long-term strategy should be solidified, and so the W3C is holding a workshop [1] to

1 Important Dates

31 July 2014:
Deadline for submission of Position Papers

9 August 2014:
Acceptance notification and registration in-

http://www.w3.org/2012/webcrypto/webcrypto-next-workshop/Overview.html

W3C UPDATE MEETING #4

WEBCRYPTO NEXT STEPS WORKSHOP DAY 1

- Intercede Position Paper by Peter Cattaneo (Intercede)
- Mozilla Position Paper by Richard Barnes (Mozilla)
- A Position Paper for the W3C Workshop on Web Cryptography Next Steps by Dirk Balfanz (Google)
- Web Cryptography API vNext should add BigNum support by Brian LaMacchia (Microsoft)
- WebCrypto Analysis Highlights by Kelsey Cairns (Washington State University)
- Using the W3C WebCrypto API for Document Signing by Nick Van den Bleeken (Inventive Designers)
- Digital Certificate and Beyond by Sangrae Cho and Soo-Hyung Kim (ETRI)
- Proposal for a discovery and connection API for Proximity Security Devices by Philip Hoyer (HID Global)
- **Strong Authentication In and Beyond the Browser by Brad Hill (Paypal), Jeff Hodges (Paypal), Davit Baghdasaryan (NokNok Labs), Christiaan Brand (Entersekt), and Rob Philpott (RSA)**
- **Towards harmonizing ISO24727 FIDO and Web Crypto API by Detlef Hühnlein (ECSEC)**
- **Use of SIM Card Authentication in the Open Web Platform by John Mattsson (Ericsson)**
- **ARM Submission by Hannes Tschofenig (ARM)**
- **Beyond Online Authentication: An e-banking and e-government perspective by Sean Wykes (Nascent Technology Consultants)**

W3C UPDATE MEETING #4

WEBCRYPTO NEXT STEPS WORKSHOP DAY 2

- Why W3C needs to Remain Neutral and Endorse 'Brand-free' Hardware Security by Siva Narendra (Tyfone)
- Accessing GlobalPlatform Secure Component from a Web Application by Gil Bernabeu (GlobalPlatform)
- Secure Element Access from a Web browser by Bruno Javary, Florian Recape and Cedric Barreau (Oberthur Technologies)
- Hardware Tokens: SIM Applets for use in Mobile Connect by Natasha Rooney (GSMA)
- Enhancing Web Application Security with Secure Hardware Tokens by Karen Lu (Gemalto)
- Web Cryptography & utilizing ARM TrustZone based TEE (Trusted Execution environment) for authentication, cryptography and beyond by Ilhan Gurel (Trustonic)
- Multifactor Authentication based on User Contextual Data and the Mobile Web by Jon Azen, Ian Brettell, Laurence Lundblade, Giridhar Mandyam and Mike Milikich (Qualcomm)
- The Increasing Importance of Proof-of-Possession to the Web by Mike Jones (Microsoft)
- Cloud Service Privacy in a Pervasive Monitoring Landscape by Stefan Håkansson (Ericsson)
- Enhancing privacy in token based electronic identity schemes by Jonas Andersson (Fingerprints)

W3C UPDATE MEETING #4

WEBCRYPTO NEXT STEPS WORKSHOP SUMMARY

- Hardware Crypto (methods and key storage) will be included in the next phase of the work
- SIM/UICC are accepted “targets”
  - T-Mobile / PD as stakeholder
- µSD-cards as authenticator
  - T-Systems as stakeholder / FIDO Alliance

- WebCrypto is the basis for higher level APIs like payment and authentication

- FIDO Alliance and U2F is the next big thing.
  - DT should become a member of the FIDO alliance

- eCard API not yet dead
- GBA not yet dead (Ericsson)

- The GSMA is an important partner for DT to bring Mobile Connect and WebCrypto together
- Web Permissions need to be addressed