W3C Web Crypto activity

Virginie GALINDO

30th of Oct 2014

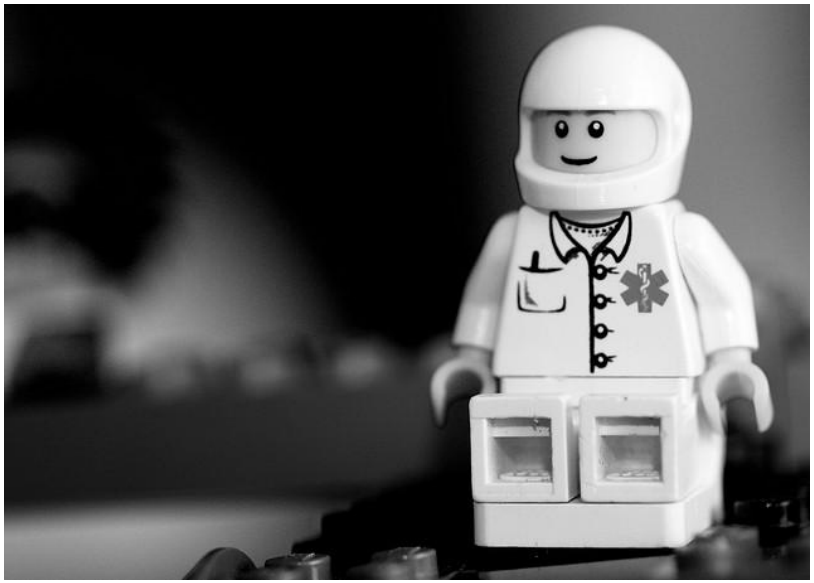
Menu ? 30 minutes to taste web, standard and security cocktail

(no drone, no demo, no hack, no code, just gossips)

gemalto

Virginie Galindo …

#gemalto / #web / #standard



gemalto

Web Security ?

Cumulating hardware, firmware, software , and servers holes

gemalto

Protecting business on the web is a real job, and a bit of coordinated effort may help...

gemalto

There is a security roadmap in W3C

gemalto

Snowden effect...

gemalto

Business on the web …

gemalto

The W3C groups dealing with security

XML Security WG
Web App Sec WG
Web Crypto WG
Web Security IG

All is here http://www.w3.org/Security/wiki/Main_Page

Web Crypto WG – crypto trolls

Trying to make available crypto to web apps

Web Crypto API

http://dvcs.w3.org/hg/webcrypto-api/raw-file/tip/spec/Overview.html

Web Crypto Key Discovery

https://dvcs.w3.org/hg/webcrypto-keydiscovery/raw-file/tip/Overview.html

Web Crypto WG

Web Crypto API

Recommendation

Candidate Recommendation

Web Crypto Key Discovery

Last Call Working Draft

Public Working Draft

gemalto

Web Crypto API : first implementations

Netflix – NfWebCrypto project blog and github

Google – statement and corresponding issue by the Chromium team.

Internet Explorer – Developer documentation for IE11 preview and plugin for other browsers

WebKit – Implementation is tracked as bug 122679

Firefox – Implementation is tracked under bug 865789

Web Crypto API in few lines

With the Web Crypto API one can

- Generate a random
- Generate a key
- Derive key (or bits)
- Import or export a key
- Encrypt, decrypt, sign, verify a signature, create a digest

A key is characterized by

- Key type
- Key usage (encrypt, sign, ...)
- Key algorithm (from registered algorithms)
- Extractable or not

Recommended algorithms

The specification describes how to manage operations with a large number of algorithms

https://dvcs.w3.org/hg/webcrypto-api/raw-file/tip/spec/Overview.html#algorithms

But recommends some of them to be implemented by UA – while this not being normative

HMAC using SHA-1

HMAC using SHA-256

RSASSA-PKCS1-v1_5 using SHA-1

RSA-PSS using SHA-256 and MGF1 with SHA-256.

RSA-OAEP using SHA-256 and MGF1 with SHA-256.

ECDSA using P-256 curve and SHA-256

AES-CBC

But this is not the end...

The WG started to think about next features...

A workshop was organized in September, calling for use cases and ideas...

http://www.w3.org/2012/webcrypto/wiki/WG_Future_Work

web crypto . NEXT

Workshop

25 program committee members, 44 papers received, 70 attendees

Discussion

Involved all actors of the value chain, from device makers (mobile, chipset, secure element, trusted execution environment) to browser makers and service providers

Covered next features of web crypto (to make it better), new services such as authentication or reuse of secure token applications

web crypto . NEXT snapshot

Web Crypto API new features

More algorithms

Key storage (including with secure storage)

Certificate

Dynamicity

New services

Authentication

Access to services located in secure token (secure element, TPM, trusted execution environment)

Report is available

Everyone clicks on http://www.w3.org/2012/webcrypto/webcrypto-next-workshop/report.html

web crypto . NEXT next steps

Follow up on public Web Security IG mailing list

http://lists.w3.org/Archives/Public/public-web-security/

Find a place in W3C to develop nice elected features

Web Crypto WG, WebAppSec WG, new WG...

Recruit participants

What about you ?

Charter or re-charter what is needed by Q1 2015

[Short advertising for Security Activity]

Interested in web security !?!

Look at the W3C security activity area
https://www.w3.org/Security/wiki/Main_Page

Pick you battle!

Thanks!

Keep in touch

@poulpita
virginie.galindo@gemalto.com

gemalto

Credit photos

Lake by Stephane (slide 28)
Trees and Circle by Naty (slide 27)
Pupils protest (slide 13), techno parad (slide 30) by Philipe Leroyer
Grubling of the tigers (slide 7) by Yoann
Caffeinated (slide 2) by Ross Pollack
L'enfant au chapeau (slide 4) by Martine Lanchec Girard
On the road (slide 12) by Ki2
Alignement de cabine de plage (slide 15) by Nomad Photography
Lego (slide 14) by Josselin Lioust
L'indémodable (slide 3) by EquinoxeFr
Parc du boisé de Saint Sulpice (slide 26) , Hamac (slide 33) by Bob August
Mortel (slide 5) by Angelus Yodasson
Jardin des Plantes Nantes (slide 6) by Gwen
Lettres (slide 31) by Daoro

Source : Flickr, all pictures in Creative Commons

gemalto