Web Crypto WG F2F meeting – 30th of October 2014

HELLO THIS IS WEB CRYPTO WG !

- *Hello, this is Web Crypto WG*
  - *We will be having fun today until 18:00, with a break between 11:00 and 15:00*
- *Please introduce yourself*
- *Enter wifi (W3C/fullpotential) and join the irc #webcrypto*
- *Volunteer to scribe*

SUGGESTED AGENDA

- *8:30 - Introduction*
- *8:45 - Web Crypto API*
- *15:00 - Test tools/repository/working method*
- *15:30 - Implementation status*
- *16:00 - Web Crypto Next Workshop*
- *16:30 - Re-chartering*
- *17:30 – Roadmap & group life*
- *17:55 - Wrap up*

What else ?

(INTRODUCTION)
THIS F2F OBJECTIVE

- *Finalize the Web Crypto API*
- *Trigger next phase : test & call for implementation*
- *Getting elements to build a common vision for what is coming next in Web Crypto WG*
  - *No decision today !*

INTRODUCTION
SOME NEWS FROM THE CONSORTIUM…

- *Security has become n°1 item for the consortium…*

- *See 8 Application Foundations announced by W3C*
  - *http://www.w3.org/blog/2014/10/application-foundations-for-the-open-web-platform/*

- *It lists potential features : web crypto, multi-authentication, smart card, biometry, strong passwords, identity management*

INTRODUCTION
W3C SECURITY AREA…

- *W3C Security Activity is large and dynamic*
  - *http://www.w3.org/Security/wiki/Main_Page*
- *It is made of*
  - *XML security WG (for specification maintenance)*
  - *WebAppSec WG*
  - *Web Crypto WG*
  - *Web Security Interest Group*
  - *Privacy Interest Group*
  - *There are some discussions to progress on a Trust and Permission Community Group (see Dave Raggett break out session during TPAC)*
- *Organized/supported this year several workshops*
  - *Pervasive monitoring*
  - *Trust and permission*
  - *Web Crypto Next*
  - *Privacy and user*

INTRODUCTION
WEB CRYPTO WG

- *Web Crypto WG is a 74 WG participants*
  - *65 participants from 27 organizations*
  - *9 Invited Experts*

- *Major deliverables are*
  - ***Use cases*** *https://dvcs.w3.org/hg/webcrypto-usecases/raw-file/tip/Overview.html*
  - ***Web Crypto API*** *https://dvcs.w3.org/hg/webcrypto-api/raw-file/tip/spec/Overview.html*
  - ***Web Crypto Key Discovery API*** *https://dvcs.w3.org/hg/webcrypto-keydiscovery/raw-file/tip/Overview.html*

INTRODUCTION
WHERE IS WEB CRYPTO ?

- *Web Crypto API is getting out of Last Call*
  - *On 3rd Nov 2014 after loooong and interesting debates*
  - *(please applaud editors **Mark Watson** from Netflix and **Ryan Sleevi** from Google)*

- *Implementations have already started*
  - *Safari, Chrome, Firefox, IE*

- *Next Web Crypto API version is already discussed*
  - *Inside the WG* http://www.w3.org/2012/webcrypto/wiki/WG_Future_Work
  - *During the Web Crypto Next Workshop held in September 2014*

INTRODUCTION
WHERE IS WEB CRYPTO DISCOVERY API?

- *Web Crypto Key Discovery API is unchanged since months*

- *What do we do ?*
  - *Transform into Technical Note*
  - *Push towards REC*
  - *Keep into the next charter*

- *Lets discuss Web Crypto API*

WHAT IS ON OUR PLATE ?

- *Bug status*
  https://www.w3.org/Bugs/Public/buglist.cgi?quicksearch=web%20crypto&list_id=46437

- *Working out details of extensibility/errata*

- *Remarkable Bugs*
  - *25198*
  - *26322*
  - *26741*
  - *26903*
- *About security recommendation from IETF CFRG*

- *Other specific bug/topic you wanna discuss ?*

- *Lets discuss Web Crypto API next milestones*

PROCESS…

- *We are still in the 2005 process*
- *We need to go through following steps*

- *Lets discuss tests and tools*

- *Lets discuss implementation*

- *Lets discuss Web Crypto Next Workshop*

WEB CRYPTO . NEXT

- *Workshop*
  - *Supported by Harry Halpin, Wendy Seltzer, Karen Myers and myself*
  - *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

- *New friends (a lots of non-W3C members interested…)*

- *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 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…*
- *Charter or re-charter what is needed by Q1 2015*

- *Lets discuss Charter …*

WEB CRYPTO WG 2015 CHARTER

- *Words from browser makers*
  - *What is your roadmap ?*

- *Some specific features have been identified during the workshop*
  - *https://www.w3.org/Security/wiki/IG/webcryptonext_workshop*
  - *Please indicate if you want to have in the charter*

- *Lets discuss WG life*

THANKS FOR THE HARD WORK !