gemalto
security to be free

The web will be secured or will not be …

Virginie GALINDO

@ParisWeb

18/19 October 2012

Who is on stage ?

"leader in digital security"

virginie.galindo@gemalto.com

from south ...

Sharing the world ... ... and the web services

… and the web services

#sharethelove

#sharemyfriends

#sharemyopinion

#sharemywallet

#sharemyhealthcare

#sharemydata

The open bar model

… and the web services

#TLS

#same-origin-policy

#DNT

#CORS

#CSP

#WebCryptoAPI

#protectyourself

The controled model

… and the web services

#TLS

#same-origin-policy

#DNT

#CORS #CSP

#WebCryptoAPI

#protectyourself

The controled model

W3C Web Crypto WG objective

Deliver a **standard javascript API** to help developers and service providers to build a **custom and interoperable security model**.

Example of targeted use cases
- Peer to peer communication
- Signing legal document
- Protecting video content
- Checking authenticity of code/library
- Secured cloud data backup
- User authentication

W3C Web Crypto WG features

- Generate a random number (a real one)
- Create a key (any size)
- Make it temporarily or permanent
- Choose algorithm (any algorithm, old ones, new ones)
- Sign or cipher with that key
- … and do it again !

Workforce !


ETRI
Google
DeutscheTelekom
Intel
EmilyStark
RedHat
Gemalto
FutureWebTechnologyLabs
TommyKromer
ChannyYun
ChristopherKula
Qihoo360
Microsoft
Mozilla
Baidu
Cisco
MITRE
JohnBradley
DavidDahl
Zooko
Netflix
RyanSleevi
MobileWebForum
CableTelevisionLaboratories
WendySeltzer
RichardBarnes
JarredNicholls
IBBT
Opera
NadimKobeissi
HarryHalpin
DavidRogers

When will the dream become real ?

Everything is gathered to deliver something in the W3C standard in **summer 2013** (promis, juré, craché).

At the moment we are in the First Public Working Draft, meaning that **we are expecting your comments** !

Some of the problems we have to solve…

-The **one click button** to protect data versus the **super low level API** where you can parameter and fine-tune everything

- **Sharing** the keys among webapps

-Re-using **key in a smart card** (instead of relying on dynamic key creation and local storage by the browser)

Curious to see if we will succeed ?

- Spy the W3C Web Crypto WG wiki
http://www.w3.org/2012/webcrypto/

- Subscribe to our mailing list
http://lists.w3.org/Archives/Public/public-webcrypto/

- Follow the chair @poulpita

- And help us…

Thanks !