

Wanna secure your webapp ?



Virginie GALINDO

June 2013

Who's on stage ?

- ✦ Virginie GALINDO with gemalto, a security company
- ✦ gemalto standardization crew, since 8 years
- ✦ Tags : security, mobile, innovation, smart card, trusted execution environment, standard, french, traveler, writer, ...
- ✦ My best friends : mobile network operators, banks, governments, public transportation, device makers, ...
- ✦ Chair of the W3C Web Crypto WG

News from Paris !




Paris mayor in 2014 will necessarily be a lady

The little story ...

- ✦ Right party decided to make Parisian electors choosing their unique candidate to run the election
 - ✦ Elections were relying on e-voting
- ✦ After few hours the electronic vote opened, first security failures were detected
- ✦ When the voted closed the participation rate was 86%.

Primaire UMP à Paris : un vote électronique faillible

🏠 > ACTUALITE > POLITIQUE Par  lefigaro.fr | Mis à jour le 31/05/2013 à 17:39 | Publié le 31/05/2013 à 12:14

	▾
ÈME SUJET	▾
(74)	▾



ACCUSE DE RECEPTION

Election primaire ouverte pour l'alternance à Paris en 2014



ACCUSE DE RECEPTION

Election primaire ouverte pour l'alternance à Paris en 2014

Primaire UMP à Paris : "Un simulacre d'élection"

Créé le 03-06-2013 à 20h14 - Mis à jour le 04-06-2013 à 12h25



Par Boris Manenti



"L'UMP a créé une lessiveuse à voix qui accepte les fausses identités", critique l'Observatoire du vote, vent debout contre le vote par internet.

Mots-clés : Paris, UMP, internet, scrutin, election, Nathalie Kosciusko-Morizet, candidat, vote, municipales, mairie

 Recommander

26

 +1

2

PARTAGER



RÉAGIR

9

Abonnez-vous au
Nouvel Observateur

de vote a bien été enregistré.

: C

Election primaire ouverte pour l'alternance à Paris
internet

réception : 31/05/2013 à

numérique d'emargement :

merci d'avoir voté par Internet.

Fait le 31/05/2013 à



Post mortem ...

- ✦ User experience was a pain
 - ✦ Visit the site
 - ✦ Load a plug-in
 - ✦ Enter name, birth, phone number
 - ✦ Pay with credit card
- ✦ Security failures were soooo obvious
 - ✦ Identity could be faked
 - ✦ Same person could vote several time
 - ✦ No risk management

Crypto could have helped !

- ✧ Implementing **Security** relies on very few valuable things !
- ✧ **Operations** such as user identification, device authentication, service and client authentication, ciphering of exchanges, integrity of messages
 - ✧ In other word : cryptographic operations
- ✧ Included during the service **Design**
 - ✧ Don't even think about improvising security
- ✧ This is why we need a **standard and robust crypto API** in browsers available to webapp

Savers of the web



On Monday night...

- ✦ Web Crypto WG meets on irc #crypto
- ✦ You can spy us <http://www.w3.org/2012/webcrypto/>
 - ✦ We argue about the best algorithms to reference
 - ✦ We finetune means for creating keys

Serious stuff

- ✧ Use cases
 - ✧ To explain W3C management what we wanna do
- ✧ Web Crypto API
 - ✧ To let web dev generate a random number, create a key and use it
- ✧ Web Crypto Key Discovery
 - ✧ To let web apps retrieving their key – and only their key
- ✧ Web Crypto High Level API
 - ✧ To make the web dev dream that crypto will be a one click button one day...

Use cases

- ✦ Banking transaction
- ✦ Files synchronization and cloud backup
- ✦ Code signing
- ✦ Content protection (Who said DRM ?)

(We need to ask the future Paris mayor to sponsor the e-voting use case)

Seriously ! Serious, like what ?

- ✧ Web Crypto APIs are not only a mercury repository
- ✧ You can play with it
 - ✧ Polycrypt by BBN
 - ✧ <http://polycrypt.net/>
- ✧ Some people claim to use it already
 - ✧ Netflix, in combination with Encrypted Media Extension (Who said DRM ?)
 - ✧ <http://www.webmonkey.com/2013/04/netflix-plans-to-ditch-silverlight-for-html5/>
 - ✧ Inventive Designers, experimental, combined with a smart card
 - ✧ <http://www.inventivedesigners.com/>
- ✧ Product Announcement
 - ✧ Mozilla : https://bugzilla.mozilla.org/show_bug.cgi?id=865789
 - ✧ Google : <https://groups.google.com/a/chromium.org/forum/#!msg/blink-dev/iEz5GOuM4eU/nl6NSQV4YWUJ>

Ok, we have interoperable crypto. What is next ?

- ✦ A super complex Key is cool !
- ✦ But a Key protected in a tamper resistant, is even more cool !
- ✦ SysApp WG will be working on letting web apps accessing secure element
 - ✦ Those little chips that you can attack, it will never unveil their secret – actually it may die to preserve it

Thanks !

I am more talkative than the smart card my
company sells !

You can ask questions...

Keep in touch...



@poulpita



fr.linkedin.com/in/viriniegalindo/



virinie.galindo@gemalto.com



<http://poulpitablog.wordpress.com>