WEBCRYPTO API

De la cryptographie dans le navigateur

Jean-Christophe Sirot

@jcsirot

fr.linkedin.com/in/jcsirot/

Paris JUG - 13/01/2015

POURQUOI UNE API CRYPTO ?

BIBLIOTHÈQUES

- sjcl (https://crypto.stanford.edu/sjcl/)
- crypto-js (https://code.google.com/p/crypto-js/)
- forge (https://github.com/digitalbazaar/forge)
- digest.js (https://github.com/jcsirot/digest.js)

PROBLÈMES...

PROBLÈMES...

- Pas d'entier de 64 bits natifs, pas de *big integer*, pas de tableaux performants

PROBLÈMES...

- Pas d'entier de 64 bits natifs, pas de *big integer*, pas de tableaux performants
- Impossibilité des «calculs longs» (thread unique)

PROBLÈMES...

- Pas d'entier de 64 bits natifs, pas de *big integer*, pas de tableaux performants
- Impossibilité des «calculs longs» (thread unique)
- Pas de générateur de nombres aléatoires de qualité (PRNG)

SOLUTIONS ?

- Applet Java
- Source d'aléa : https://random.org

SOLUTIONS ?

- Applet Java
- Source d'aléa : https://random.org

WebCrypto API : http://www.w3.org/TR/WebCryptoAPI/

GÉNÉRATEUR ALÉATOIRE

```
var array = new Uint8Array(16);
window.crypto.getRandomValues(array);
```

- Représentation des données : *ArrayBufferView*
- Fonction synchrone, non bloquante
- Utilise une source d'aléa «sûre» du système (par exemple `/dev/urandom`)

WINDOW.CRYPTO.SUBTLE

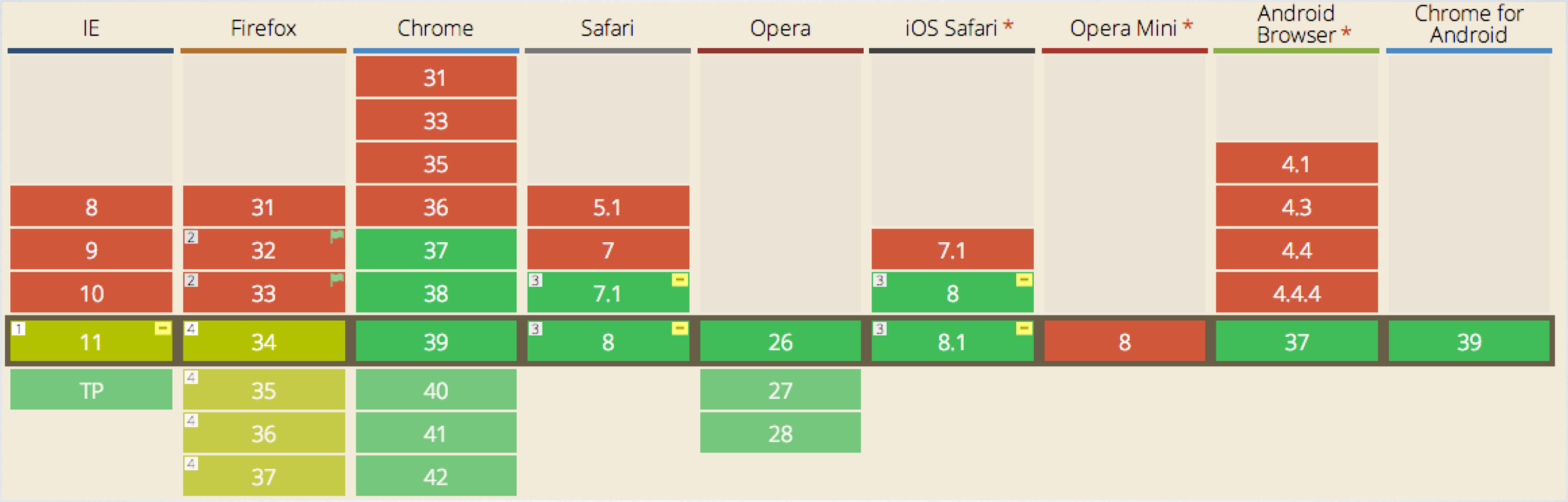
- Interface avec les primitives cryptographiques : encrypt, decrypt, sign, digest, generateKey...
- Données sont passées sous forme de *ArrayBufferView*
- Retourne une *Promise* javascript

PROMISE

```
var data = toArrayBufferView("Hello World!");
var algorithm = {
    name: "SHA-256"
};
window.crypto.subtle.digest(algorithm, data)
    .then(function(result) {
        console.log(result);
    })
    .catch(function(error) {
        console.error(error);
    });
```

DEMO

CAN I USE ?



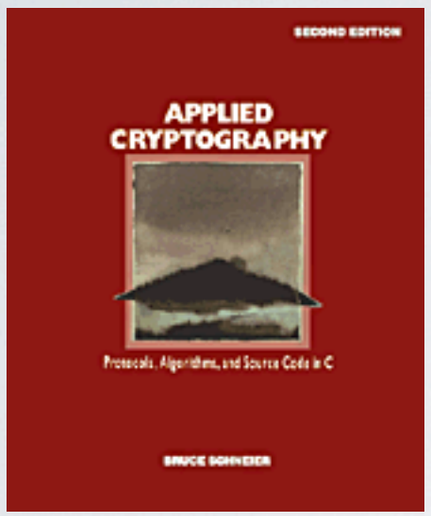
http://caniuse.com/#feat=cryptography

LIMITATIONS

- Faire confiance aux applications web
- Pas encore disponible partout, tous les algorithmes ne sont pas disponibles
- version 1 de l'API n'est pas parfaite (pas d'API *update/finish*, pas d'API de streaming, pas d'API pour utiliser les clés déjà présentes sur le système...)

QUESTIONS

POUR ALLER PLUS LOIN

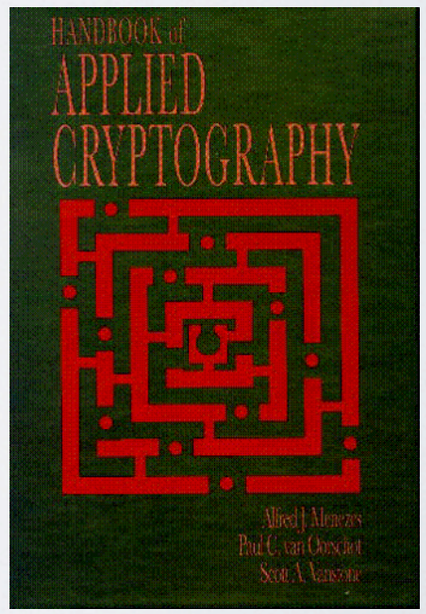


Applied Cryptography

https://www.schneier.com/book-applied.html

Handbook of Applied Cryptography

http://cacr.uwaterloo.ca/hac/



CRÉDITS

- https://www.flickr.com/photos/110751683@N02/13334048894/
- https://www.flickr.com/photos/derek_b/3046770021