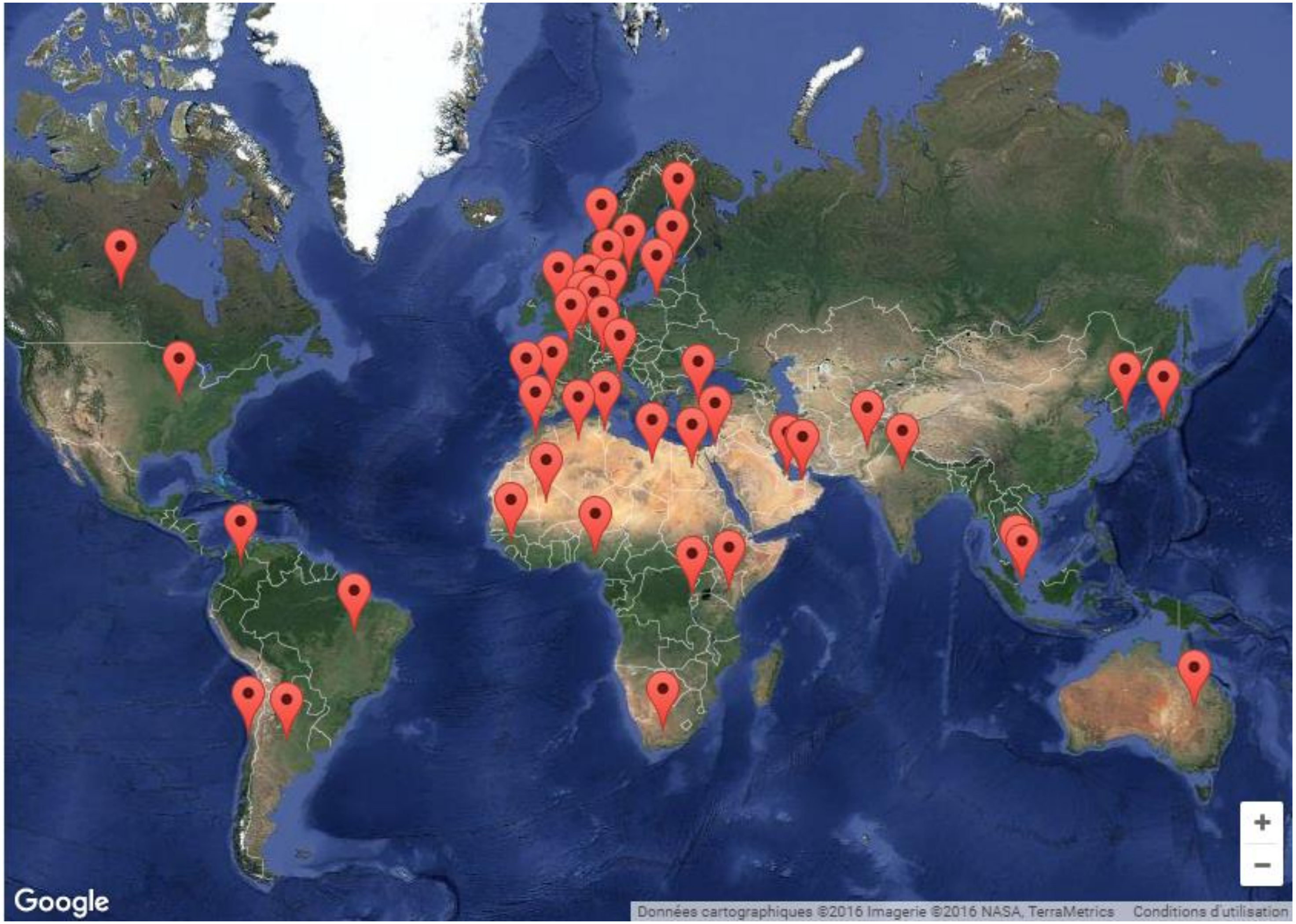
MORPHO

Hardware Security Community Group meeting in London - 26-27 April, 2016

SAFRAN

EID USE CASES IN E-CITIZENSHIP


Google
Données cartographiques ©2016 Imagerie ©2016 NASA, TerraMetrics
Conditions d'utilisation
+
−

From https://www.secureidentityalliance.org/index.php/e-services-provision-tracker

STATES MOTIVATION

- **Public safety: checking citizenship and issuing identity documents**

- **Public services: digital services 50x cheaper than user facing**

- **Digital services also provides capabilities regarding the various legal regulations**
  - Identity theft
  - Anti money laundering
  - Fraud (ghost workers, tax …)
  - Terrorism

DIGITAL SECTORS AND USE CASES

Digital identity sectors			Exemplary use cases for digital identity system
Public sector	1	Public services/health	Self-service, automation, personalized medicine, tax collection, digital signature
Manufacturing industries	2	Traditional production	Personalized products, consumer insight, subscription-based services
Services industries	3	Retail	Loyalty programs, marketing, service enhancements
	4	Financial services	Automization, personalized products, risk management, secure transaction
	5	Telco and media	Personalized services, monetization of consumer insight, marketing, automation
Internet industry	6	Web 2.0 communities	Service enhancements, monetization of user-generated content, marketing
	7	eCommerce	Secure transaction, monetizing consumer insight, marketing, fraud prevention
	8	Info/ entertainment	Personalized products, monetization of consumer insight, marketing

TRUST SERVICE PROVIDERS

→ Level of Assurance defined by the lowest security level of

- Identity proofing
- Authentication factor
- Identity & authenticator lifecycle

→ Existing identity issuance models relies upon segregation of duties

- Certificate authorities check identities and delivers strong authentication factors with self contained identity link: DN of the certificate
- SP including banks, governments and other services rely upon the strong Level of Assurance that is provided by complete process

- With any non X509 based authentication factor (including OATH, FIDO …) the link to the identity should be reestablished with every SP

BANKS MATTERS OF INTEREST

→ Banks are switching to a digital world with several issues:

- Streamlined customer acquisition with on-the-fly registration
- Support various LoA to satisfy regulation, provide end-user convenience but also secure all sensitive operations
- Provide additional services, including Digital IDP for governments

→ Sensitive operations relying on strong authentication factors

- High: Smartcard (or USB token) with certificate for operation signature
- Middle:
  - 2FA mobile based credential
  - OTP or challenge / response based on banking cards (EMV/CAP)
  - OTP or challenge / response based on OATH token
  - Smartcard (or USB token) with certificate (mostly for corporate users) for authentication
  - SMS OTP
- Low: password, cookie based, FB …

BANKS ISSUES

- **Even if they don’t communicate about it, they are already facing complex attacks with combined:**
  - Social engineering
  - PC & mobile malware
  - Even with the strongest authentication factor

- **Only the smartcards (or usb token) have not or less been attacked on a large scale basis**

- **Not ready to deploy FIDO because of :**
  - the moving standards
  - the move to the full control of the OS/browser makers on the authenticators on FIDO 2.0
  - the need to change the user experience:
    - Either accept BYOC
    - Or deploy non exclusive FIDO authenticators

UNDERSTANDING THE EXISTING STANDARDS

→ Existing standards at the browser level:

- PC/SC ~ send/recv(apdu)
- PKCS#11 ~ getCert(), sign(#hash)
- (SSL)/TLS: authentication only

→ Additional vendor features:

- Why ? Post-issuance & trust services:
  - secure remote profile updated
  - certificate renewal
  - credits reload
  - identity attributes delivery
  - …
- How ? Remote middleware to remove the need of a local middleware, rely upon PCSC thanks to Java applet capability (javax.smartcard)
- But ? NP-API deprecated, no Java applet on mobile => dead end

OUR UNDERSTANDING OF THE PROBLEM

- **The browser makers point of vue: provide secure and reliant features in the user agent on behalf of the end-user**

- **No APDU API: the security relies upon the server interfaced through a Web UI which is too risky even with SOP**

- **Target is functional API which can be managed by a secure UI on the user agent**

- **Issue: apart from “standard” APIs like payment, how can we manage extended use cases like**
  - transaction confirmation (not payment)
  - post-issuance
  - identity attribute

MORPHO’S PROPOSAL

➔ Transaction confirmation API first

- This is the element a end-user could be liable
- It would fit all use cases where a business API will be too limited:
  - Authentication
  - Transaction confirmation: including
  - Signature

➔ But still to define vertically how to manage:

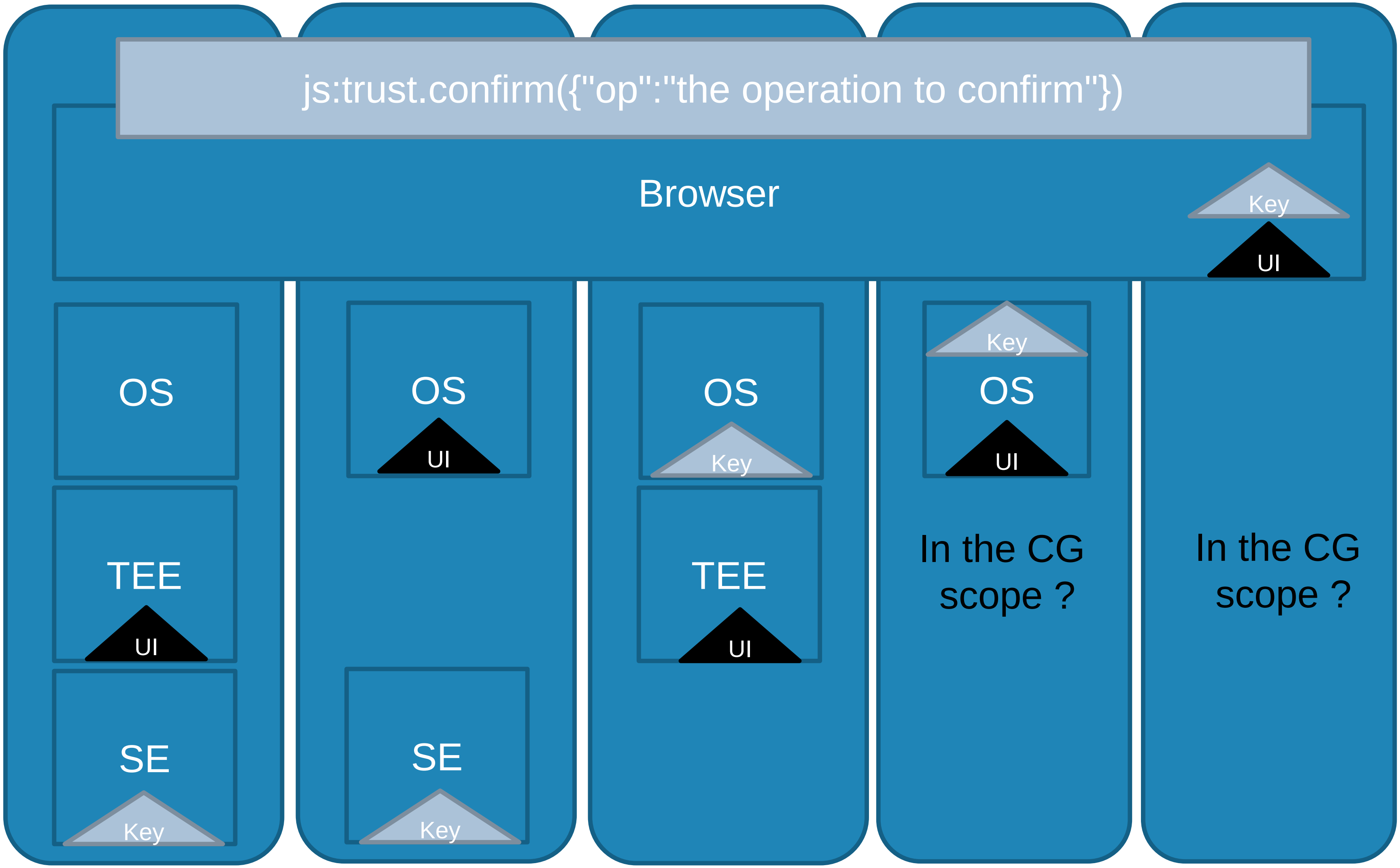
- Signature: manage the document signature on the server side (see PP Server signing)
- Identity attributes delivery
- Post issuance API

➔ Limit on the privacy:

- How to give the right subset of attributes with the required trust level ?
- How to compute additional values without delivering the original data (majority vs birthdate)

Transaction confirmation POC

ESERVICES CONFIRMATION



SAFRAN Morpho

ESERVICES CONFIRMATION

→ Generally:

- Operation: transaction confirmation only
- Security: local operation
- Accessibility: relies upon the middleware/OS => consent

→ On PC:

- Patch to the browser (plugin IE, FF & Chrome)
- Middleware based reader and certificate selection
- Patch to the middleware to present the data to sign as part of the confirmation

→ On Mobile:

- Target: patch to the browser
- According to the situation: relies upon the browser, the OS or the TEE

KEY MISSIONS, KEY TECHNOLOGIES, KEY TALENTS

Sebastien Bahloul
Senior architect – Business support & Innovation
Digital Center of Excellence

sebastien.bahloul@morpho.com

This document and the information therein are the property of Morpho, They must not be copied or communicated to a third party without the prior written authorization of Morpho.