CREDENTIAL’s PSbD approach

Nicolás Notario McDonnell (Atos)
Summary

• CREDENTIAL
  – Summary
  – PbD Technologies
    • Re-encryption
    • Redactable signatures
    • 2Factor authentications
  – PbD Process
    • PRIPARE
    • Outcomes
CREDENTIAL

- **Duration**: Oct 2015 – Sept 2018
- **Estimated Project Cost**: 6‘645‘185.00€
- **Call**: DS-02-2014: Access Control
- **Consortium**:
  - 6 Industry partners
  - 3 Universities
  - 2 Applied research institutions

20.09.2016
CREDENTIAL Project overview
CREDENTIAL & PbD

- CREDENTIAL is a privacy/security-oriented project
- PbD in the core technologies
- PbD at process level
Minimize levels of trust required towards the cloud
Technology Pillars

CREDENTIAL Wallet

- Proxy Re-Encryption
- Redactable Signatures
- Authentication
Proxy Re-Encryption

- Example Application: Data Sharing
Proxy Re-Encryption

- Extends public key encryption
- Allows to transform ciphertext for user A to ciphertext for user B
  → Secure end-to-end encryption

[Diagram]

Alice controls re-encryption
- Generates re-encryption key from her private key

KeyGen

Alice

pk_A

sk_A

Alice

pk_B

sk_B

Bob

Enc

ReEnc

Dec

M

C_A

C_B

rk_A→B
Conditional Proxy Re-Encryption

Example: Email forwarding

- **Enc**
- **ReEnc**
- **ReKeyGen**
- **Dec**

**Mail Gateway**

- **Alice**
- **Bob**
- **Charlie**

Bob → Charlie for urgent mail during July
Redactable Signatures

- Example Application: Selective Disclosure

Service needs to check user’s attributes
Redactable Signatures

• Black-out parts of a signed document
• Signature stays valid for remaining parts
→ Selective Disclosure
Two Factor Authentication

- Hardware-based authentication
- With two different factors of:
  - Knowledge, Possession, Inherence
- FIDO specification (local authenticators)
  - supported by many OSs and hardware
- Focus on
  - Biometrics, National eID solutions
PbD at a methodological level

- Map existing CREDENTIAL work structure with PRIPARE
- Recommend practices identified by PRIPARE as tools for CREDENTIAL tasks
- Ensure CREDENTIAL has a solid approach to PSbD ensuring that all processes considered by PRIPARE as essential are present
PRIPARE project and its objectives

- PRIPARE (http://pripareproject.eu) was a 2-year FP7 Coordination and support Action which ended in October 2015.

- Objectives
  - facilitate the application of a privacy and security-by-design methodology
  - foster risk management culture

- Outcomes
  - Methodology Handbook
  - Educational material
  - Gaps and recommendations on privacy and security-by-design practices

- PRIPARE is one of the seeds of recently approved ISO 21879 Work Item “privacy engineering"
PRIPARE methodology sources

- **Ontario IPC PbD principles**
  - Full Functionality – Positive-Sum, not Zero-Sum

- **Privacy Impact Assessments**
  - More than a compliance check

- **Privacy Management Reference Model (PMRM)**
  - Understanding and analyzing privacy policies and their management requirements; selecting technical services which must be implemented to support privacy controls

- **Microsoft Security Development Lifecycle**
  - Build more secure software and address security compliance requirements

- **Risk management (CNIL, BSI, STRIDE, EBIOS...)**
  - Remove, minimise, transfer or accept identified risks

- **Privacy Enhancing Architectures**
  - Making the right architectural choices

- **ISO Standards (29100, 29101, 24760, 29140)**
PRIPARE Methodology Features

– Easy-to-understand and easy-to-use;
– Integrated with risk assessment standards;
– Designed to cover the whole system lifecycle;
– Flexible so it can adapt depending on the nature of the project and the information collected;
– Useful for different stakeholders;
– Engaged with engineering practices.
– Principles-based;
Each process is described using a standard SIPOC notation

<table>
<thead>
<tr>
<th>Process name</th>
<th>Suppliers</th>
<th>Inputs</th>
<th>Process</th>
<th>Outputs</th>
<th>Customers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tools &amp; Techniques</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Knowledge</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Responsible</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CREDENTIAL – PRIPARE mapping

- High level privacy analysis as part of the requirement elicitation phase
- Legal analysis integrated with the requirement elicitation phase
- Detailed privacy analysis
- Risk analysis (privacy and security)
- Privacy requirements operationalization
- Privacy enhancing architecture
- Privacy enhancing detailed design
PbD process outcomes

• For now... requirements, ideas and discussions
  – Multiple accounts
  – Server-side vs client-side document index
  – Log information
  – SAML improvement to carry encrypted data with re-encryption scheme
  – Mix FIDO local authenticator approach with identity federation concepts
  – Metadata encryption/recryption
    • Do we need/want the cloud to know that the encrypted value are medical data or identity data?
Privacy and Usability Requirements

• What privacy issues do you observe that might concern users, and thereby affecting the adoption of the CREDENTIAL technology?

• What usability issues do you observe that might create hurdles for users to operate CREDENTIAL technology?
Privacy and Usability Requirements II

• Are you concerned that the wallet may be a privacy risk to the user?
• Is having multiple accounts a good idea? or rather a usability and privacy challenge?
Credential Partners
Contact

Nicolás Notario
(nicolas.notario@atos.net)

Further Information

Website: http://credential.eu
Twitter: https://twitter.com/CredentialH2020 (@CredentialH2020)
LinkedIn: https://at.linkedin.com/in/credential

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 653454
Thank you very much for your attention!