An overview of the TRAPEZE use cases & their impact on society

Workshop on Privacy, Transparency, Sovereignty and Security

Ramon Martín de Pozuelo, CaixaBank
Martin Kurze, Deutsche Telekom
Lauro Vanderborght, Digitaal Flanders
28 April 2023
Transparent & Citizen-controlled Interconnectedness
Transparent & Citizen-controlled Interconnectedness

- Right to be informed,
- Right to access,
- Right to rectification,
- Right to erasure,
- Right to restriction of processing,
- Right to data portability,
- Right to object,
- Rights regarding automated decision making.
Pilot the TRAPEZE solution in 3 distinct personal data processing scenarios, demonstrating its potential for real-world applicability, scalability and replicability.
Sharing personal data with enhanced transparency and consent check

- Client
- 3rd-party service provider
- CaixaBank
- ID Wallet
- TRAPEZE platform

Client allows 3rd-party service provider to visualize ID wallet data.

ID wallet informs about the changes to CaixaBank, client and 3rd party service provider.

TRAPEZE platform includes 'Bank B' data reading policies.

DT customers
DT NatCos & 3rd parties
DT Group

Policies editing and management (export and import)

DV
Flemish citizen
Employer (3rd party)
Digitaal Vlaanderen

Combination with MyCitizen Profile

Digitaal Vlaanderen
Employer (3rd party)
Flemish citizen
DT customers
DT NatCos & 3rd parties
DT Group

DATA INTELLIGENCE HUB

Use cases
Policy language
GDPR
Customer ID Wallet

CaixaBank

Ramon Martin de Pozuelo, CAIXABANK
(rmartindepozuelo@caixabank.com)
Customer ID Wallet - Introduction

Example of customer story: “As a customer I want to be able to provide my Know Your Customer (KYC) information once, be verified, securely stored and be able to reuse it with any other financial institution or third-party service provider, having a high-level of control of who is accessing my data and for what purpose.”

1. Improving transparency and control of the personal data by citizens in general and Financial services’ clients in particular.

2. Proposed solution facilitates the control of its own data by the client, and by doing so it will simplify processes where this information can be reused or shared.

3. Main actors include:
   - The customer.
   - The bank.
   - Third-party (e.g. another bank).
   - TRAPEZE platform.
Customer ID Wallet - Stakeholders and Interests

1. First of all, customers can benefit by improving management and enforce of their personal data usage policies more easily, while keeping an overview of all processing activities even when such information temporarily leaves the company borders.

2. For CaixaBank is an opportunity to study how the usage of the wallet could improve in a critic and complex process like KYC acquisition and maintenance, which is extremely expensive for bank and at the same time difficult for the customer.

3. Once the customer can have a transparent control of his data, it is easier to grant permission to share it with third parties, simplifying enormously critic and complex mechanism of personal data acquisition, which is on the other hand source of security and privacy problems.

4. At the same time, it presents an opportunity to create new services, or for example simplify onboarding to banks in all the European Space in a simpler way, in fact Customer ID Wallet pilot aims at developing and identity wallet that can work as a technical reference or complement the future EU Digital wallet, by combining the digital identity verification means provided by the EU and Member States (when available) or any other trusted entity that works as an identity provider.

5. It presents clear benefits to controllers/processors/protection authorities since this transparent control of the privacy data is is perfect to simplify the management to comply with GDPR regulation.
Customer ID Wallet - High-level Solution Diagram

The following diagram represents an overview of the stakeholders' interactions in the Digital ID Wallet pilot.

- Policy definition
- Consent management
- Secured Distributed data storage
Customer ID Wallet - Self-sovereign identity and consent management tool

- Centralized (PKI) Vs decentralized identity management
  - The main difference is the way the data is stored and shared with others.

<table>
<thead>
<tr>
<th>Data Storage</th>
<th>Centralized identity</th>
<th>Decentralized identity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Centralized database</td>
<td>User devices</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data ownership</th>
<th>Data is owned by the organization with whom user share the data</th>
<th>Data is owned by the user</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Data disclosure</th>
<th>Full disclosure of data available for each identity credential</th>
<th>Selective disclosure at user consent</th>
</tr>
</thead>
</table>
Customer ID Wallet - Self-sovereign identity and consent management tool

• Decentralized identity management

• Exchange of data based on user consent
  • Complete control over the data, with the freedom to decide exactly what information to share, with whom, and when.

• Hierarchical deterministic (HD) Wallet
  • Having single master key (BIP39).
  • Single master key derives unique child key pairs, which can further drive their own unique children’s key pairs (BIP32).
  • Auth key used to identify the user. No derivation from this key.
  • Keys are stored in a user device.
  • User need to backup only single master seed instead of hundreds of keys.
  • Single master key can restore the exact same tree of keys.
  • User friendly keys backup and restore process
Privacy Policy Language & Tools for Data Based Telco Products

Deutsche Telekom

Martin Kurze, DT
(martin.kurze@telekom.de)
Introduction: synergies of (legally) using personal data by DT (business units), DT partners (3rd parties) & DT customers

Deutsche Telekom

• is an extremely valuable brand, based (among other features) on customer trust.

• does not (yet) monetize personal data that it has (collected legally during telco service provisioning).

• needs a secure, standardized, scalable and legal way to collect and manage enduser consent* to use personal data for new products.

• implements an internal version of TRAPEZE (called “Magenta Hyper Consent”, MHC) using TRAPEZE language and concepts (and a compatible policy format)

• uses these tools and language to define & offer APIs to 3rd parties, providing telco specific (personal) data, e.g. SIM-Card serial number

* We define “consent” as a privacy policy that both data controller and data subject agreed to
Interoduction: synergies of (legally) using personal data by DT (business units), DT partners (3rd parties) & DT customers

Deutsche Telekom  
- is an extremely valuable brand, based (among other features) on customer trust.
- does not (yet) monetize personal data that it has (collected legally during telco service provisioning).
- needs a secure, standardized, scalable & legal way to collect and manage enduser consent* using personal data.
- implements an internal version of TRAPEZE (called “Magenta Hyper Consent”, MHC) using TRAPEZE language and concepts (and a compatible policy format)
- uses these tools and language to define & offer APIs to 3rd parties, providing telco specific data, e.g. SIM-Card S/N

Today

Tomorrow

* We define “consent” as a privacy policy that both data controller and data subject agreed to
DT adopted conceptual aspects of architecture from TRAPEZE and the policy format for interoperability

DT developed its own policy toolset, based on technology and components developed in TRAPEZE, called MHC (Magenta Hyper Consent)

AND: using the same policy language and open interfaces

- TRAPEZE platform components
- 3rd party components
- Use Case partner’s components
- Privacy policy
- Privacy policy
- Privacy policy
- Privacy policy
- 3rd party services
TRAPEZE/MHC was tested to give/control „Groupwide Consent“ (KEK = Konzern-Einwilligungs-Klausel)
KEK as TRAPEZE/MHC-Policy (human & machine readable)
Deployment and Validation

The deployment activities includes **setting up the Policy Language specification** (based on dpv and TRAPEZE/Piero Bonnati’s work).

**Deployment:**
- Compliance Engine will be interpreted and implemented as “MHC Gate-Keeper”. DT systems use same policy language.
- Identity Management (via OpenID) plays a crucial role. DT already uses OpenID, so compatibility is granted.
- “Consent Management” is a key task/component for DT. Using TRAPEZE technology helps to minimize DT-internal effort.
- Transparency Dashboard was designed in close alignment with TRAPEZE/TUB to also fit DT’s plans.

These activities were carried out mainly by TF, IMP and CXB including the main activities listed.

**Use case evaluation** focusing on DT’s main “target group”: DT-internal Product managers, developing new data based products.
DT use case - Conclusions

• TRAPEZE (and DPVWG) *policy language* is an excellent means to exchange, enforce and manage privacy policies

• TRAPEZE *architecture and tools* are used as samples for DT internal components

• *Product owners* of new telco products appreciate the new way of “consent management”

• *New business* based on telco specific data is expected from API-exposition to 3rd parties.
My Citizen Profile - Diploma Use Case

Digital Flanders

Lauro Vanderborght, Digital Flanders (AIV)
(lauro.vanderborght@vlaanderen.be)
<table>
<thead>
<tr>
<th>Diploma in Flanders = Paper</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diploma is issued on paper</td>
</tr>
<tr>
<td>Cumbersome to share</td>
</tr>
<tr>
<td>Digitized copies are being used</td>
</tr>
<tr>
<td>Authenticity is difficult to verify</td>
</tr>
<tr>
<td>Diploma get lost</td>
</tr>
</tbody>
</table>
Goal

By relying on the (1) foundations of the **Solid standards and the ecosystem** being developed in Flanders and (2) the control & privacy functionalities of the **TRAPEZE platform**

We can effectively enable data reusage in a secure application which enables

- Compliance with the SDGR
- Value creation for the citizen and institutions (public/private)
- Strengthening of My Citizen Profile
Solid

Mijn Burgerprofiel

Solid Data vault

Trapeze

Data Provider

Data Consumer

controls

controls
The citizen is offered an interface to:

- **My Citizen Profile** where he/she can manage data stored in his/her pod and determine which organization can access/use what data.

- **TRAPEZE platform** in the form of a privacy dashboard to get an aggregated overview of consent to use data and how the data was used by these organizations.
Solution
Thank you!

Raising Citizen’s Security & Privacy Awareness and Competence