TRAPEZE

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

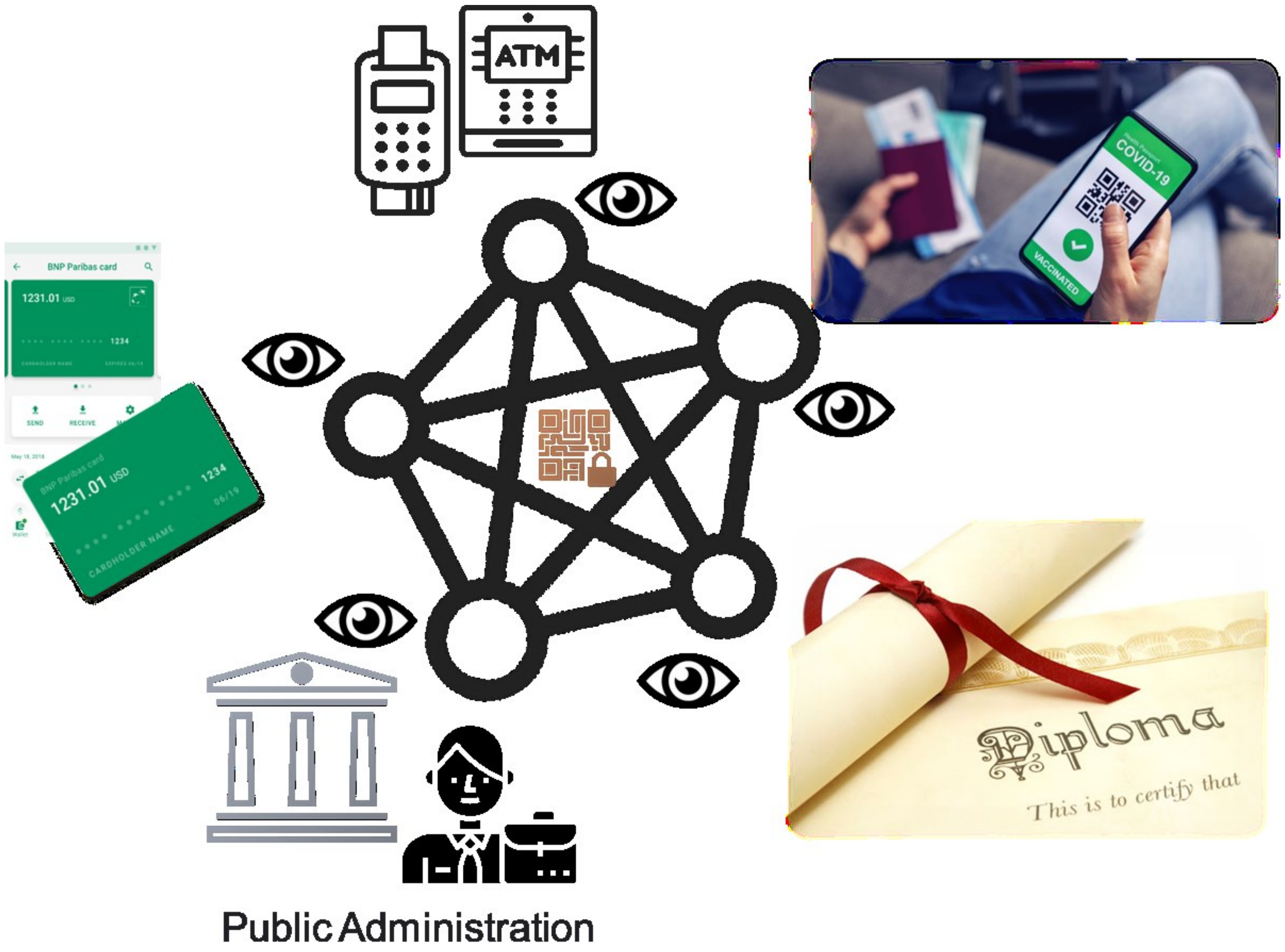
Workshop on Privacy, Transparency, Sovereignty and Security

Ramon Martín de Pozuelo, CaixaBank
Martin Kurze, Deutsche Telekom
Lauro Vanderborght, Digitaal Flanders

28 April 2023

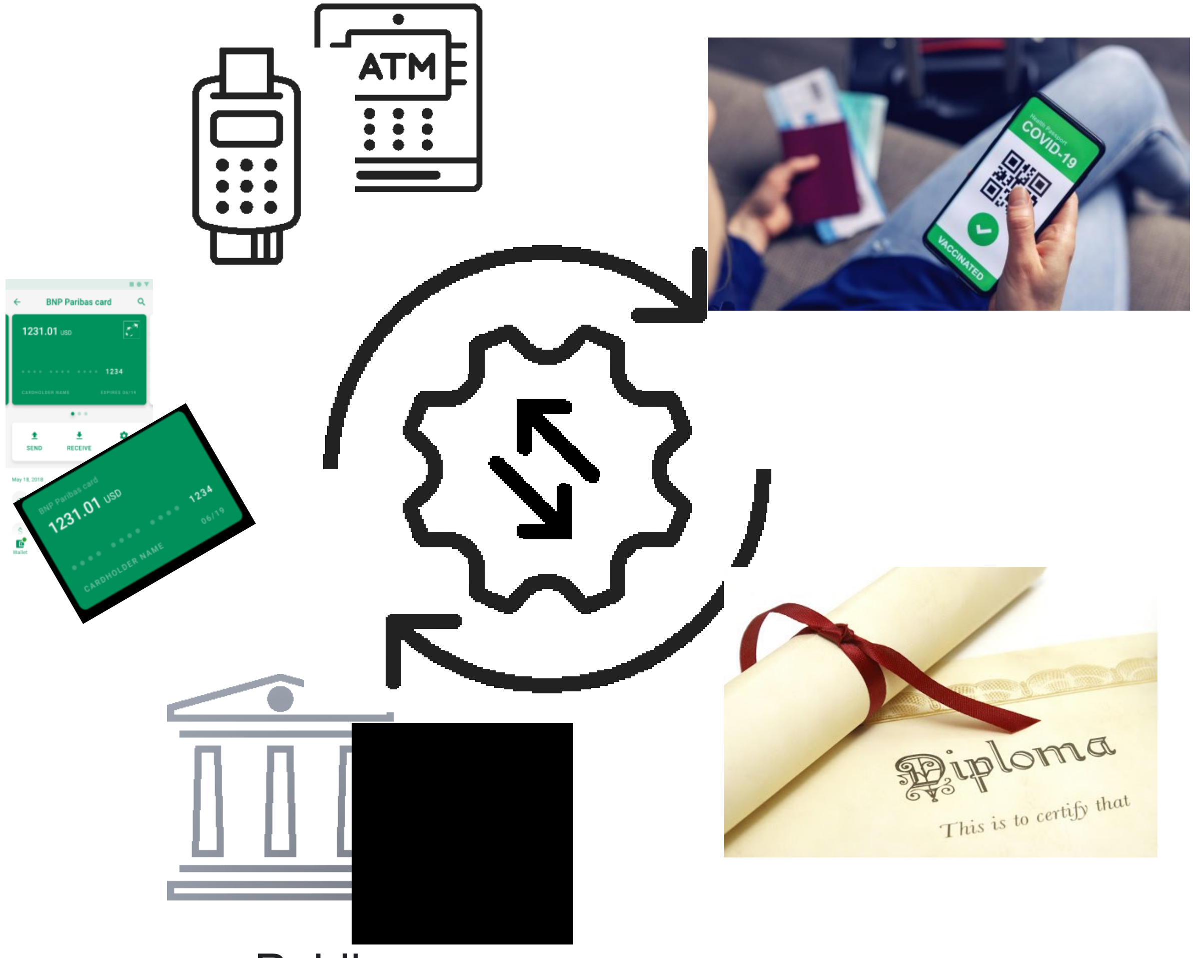
This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 883464.

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.

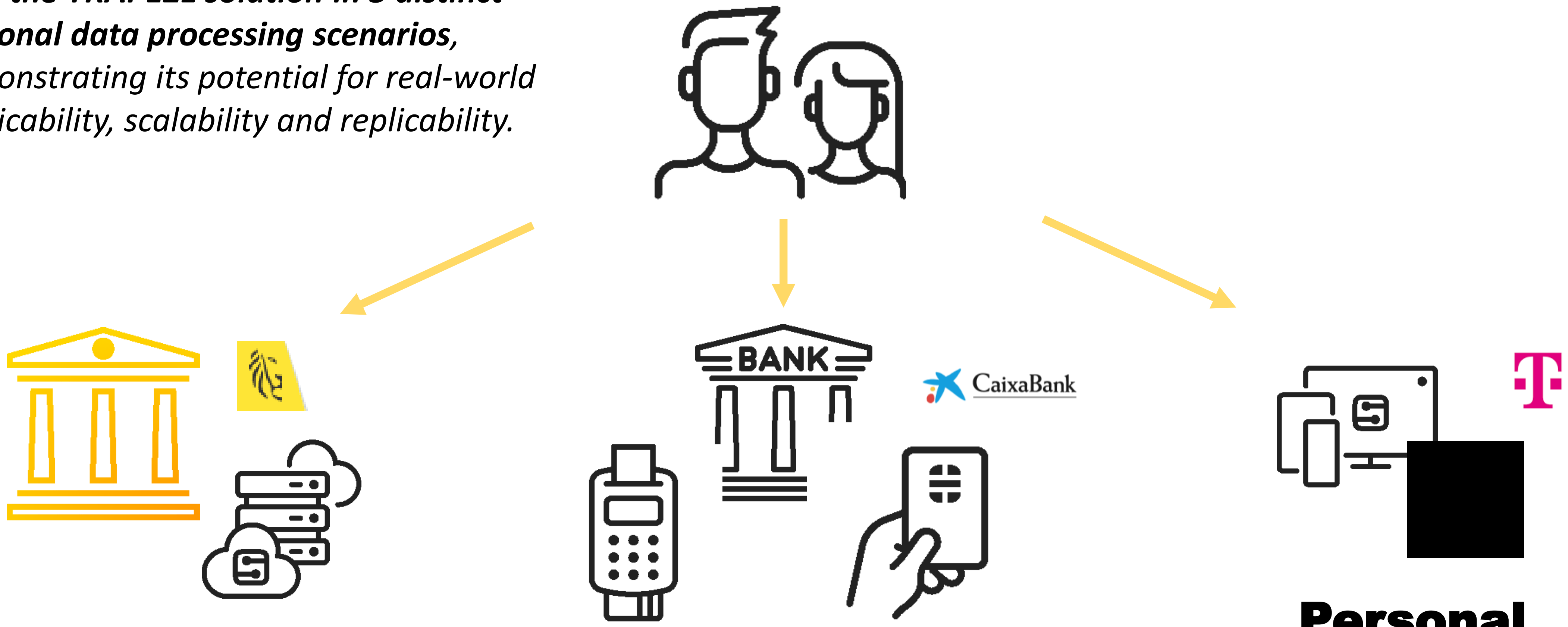


[redacted]

Public Administration

Transparent & Citizen-controlled Interconnectedness

Pilot the TRAPEZE solution in 3 distinct personal data processing scenarios, *demonstrating its potential for real-world applicability, scalability and replicability.*



[redacted]

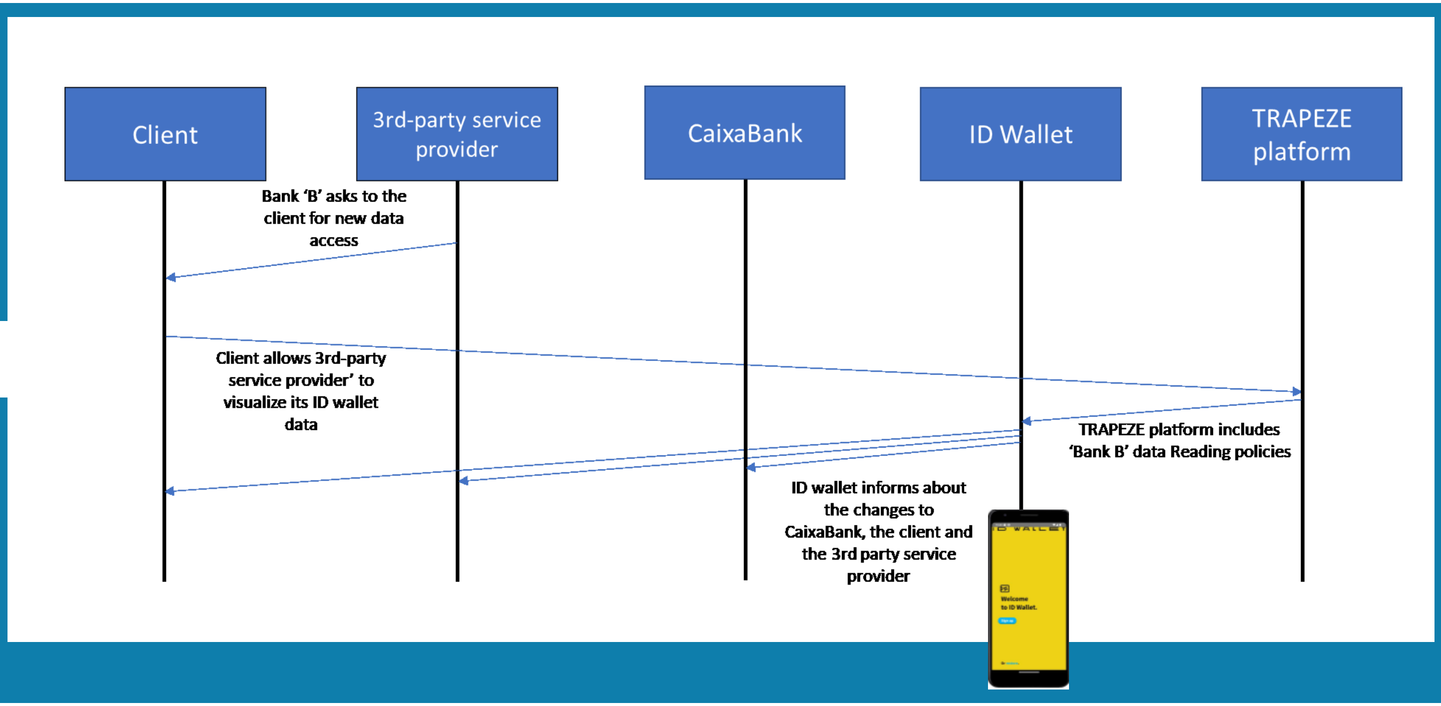
Authoritative Data

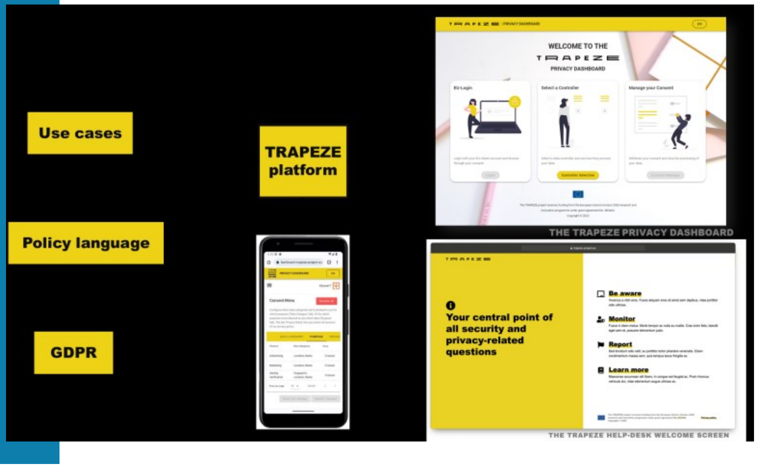
Finance and Reputational

Personal (privacy sensitive) Data

Sharing personal data with enhanced transparency and consent check

CaixaBank


Client
3rd-party service provider
CaixaBank
ID Wallet
TRAPEZE platform
Bank 'B' asks to the client for new data access
Client allows 3rd-party service provider' to visualize its ID wallet data
TRAPEZE platform includes 'Bank B' data Reading policies
ID wallet informs about the changes to CaixaBank, the client and the 3rd party service provider
Welcome to ID Wallet.


Use cases
Policy language
GDPR
TRAPEZE platform
WELCOME TO THE TRAPEZE PRIVACY DASHBOARD
EU-Login
Select a Controller
Manage your Consent
Controller Selection
Consent Menu
Your central point of all security and privacy-related questions
Be aware
Monitor
Report
Learn more
THE TRAPEZE PRIVACY DASHBOARD
THE TRAPEZE HELP-DESK WELCOME SCREEN

DT	DT customers	DT NatCos & 3rd parties	DT Group	DATA INTELLIGENCE HUB	Policies editing and management (export and import)
DV	Flemish citizen	Employer (3rd party)	Digitaal Vlaanderen		Combination with MyCitizen Profile

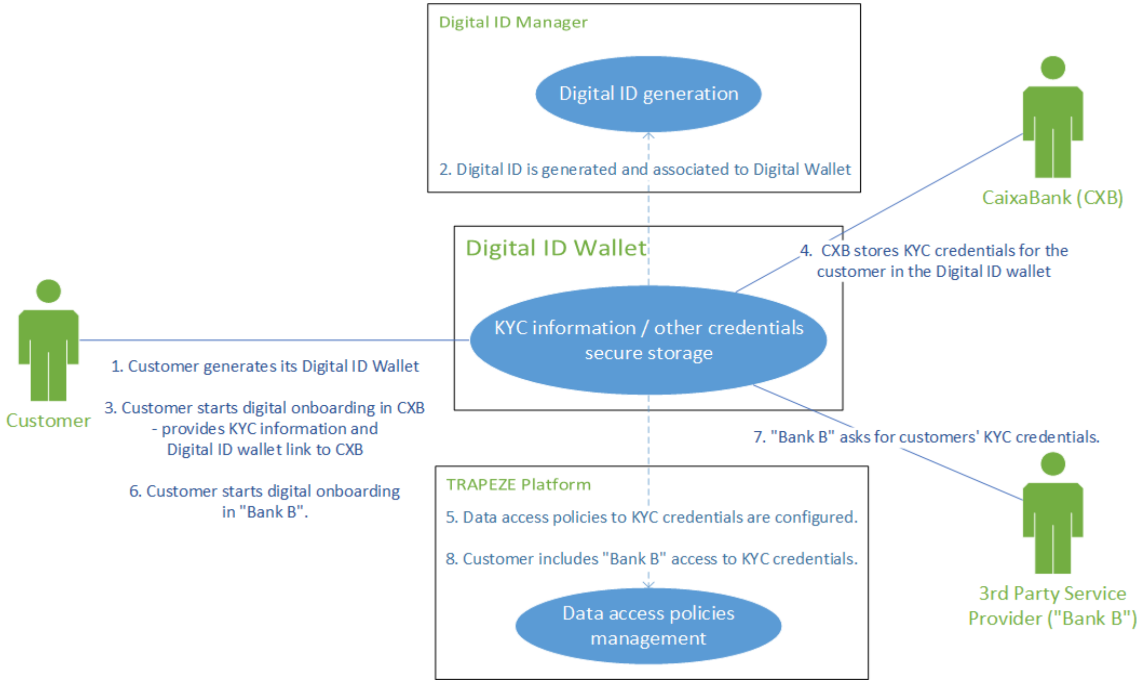
Customer ID Wallet

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.”



Digital ID Manager

Digital ID generation

2. Digital ID is generated and associated to Digital Wallet

Digital ID Wallet

KYC information / other credentials secure storage

Customer

1. Customer generates its Digital ID Wallet

3. Customer starts digital onboarding in CXB - provides KYC information and Digital ID wallet link to CXB

6. Customer starts digital onboarding in "Bank B".

CaixaBank (CXB)

4. CXB stores KYC credentials for the customer in the Digital ID wallet

7. "Bank B" asks for customers' KYC credentials.

3rd Party Service Provider ("Bank B")

TRAPEZE Platform

5. Data access policies to KYC credentials are configured.

8. Customer includes "Bank B" access to KYC credentials.

Data access policies management

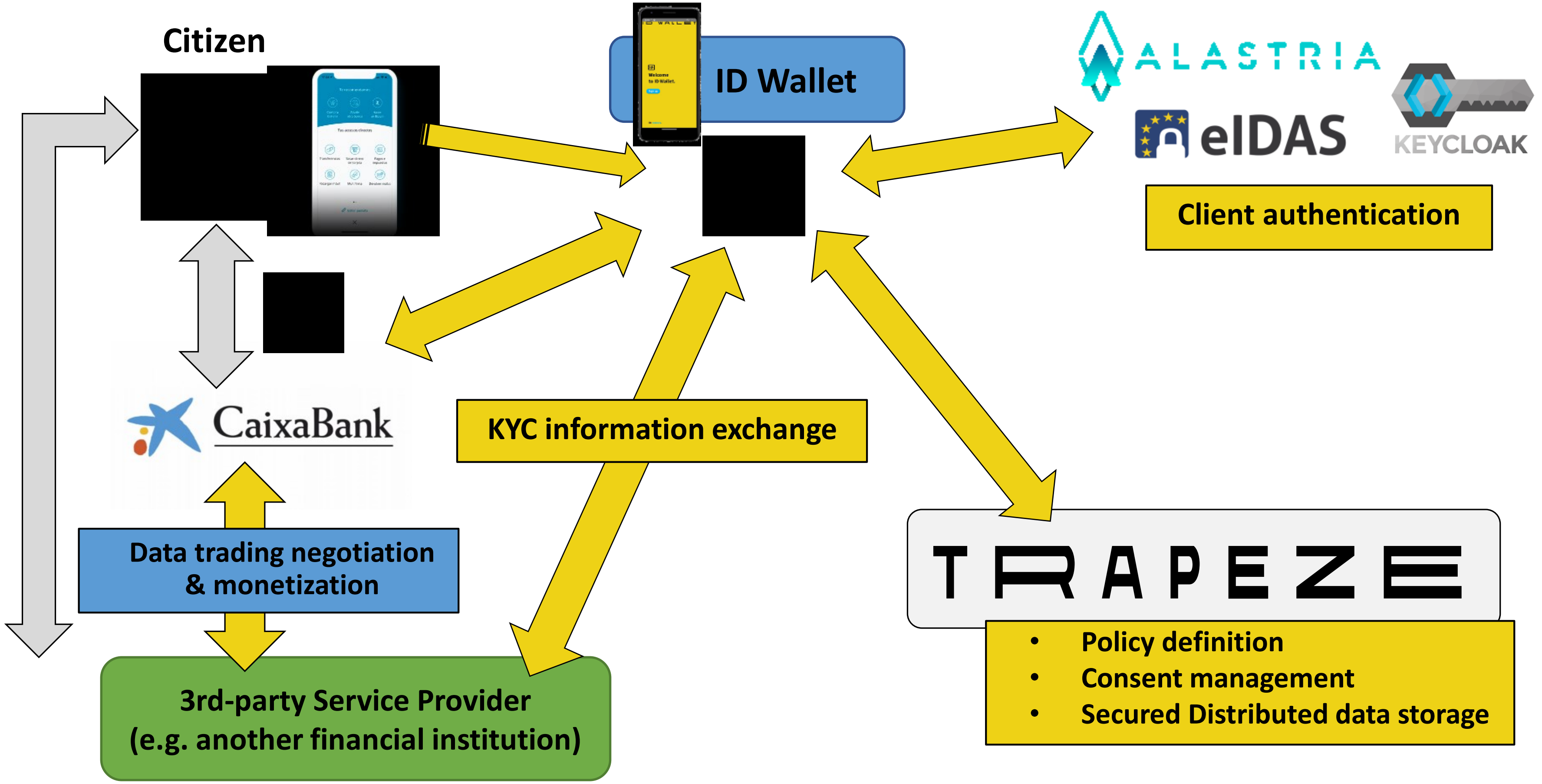
1. **Improving transparency and control of the personal data** by citizens in general and Financial services’ clients in particular.
2. Proposed solution **facilitates the control of its own data by the client**, and by doing so it will **simplify processes where this information can be reused or shared**.
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 aquisition 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.


Citizen
ID Wallet
ALASTRIA
eIDAS
KEYCLOAK
Client authentication
CaixaBank
KYC information exchange
Data trading negotiation & monetization
3rd-party Service Provider (e.g. another financial institution)
TRAPEZE
Policy definition
Consent management
Secured Distributed data storage

TRAPEZE

3rd-parties

Use Case

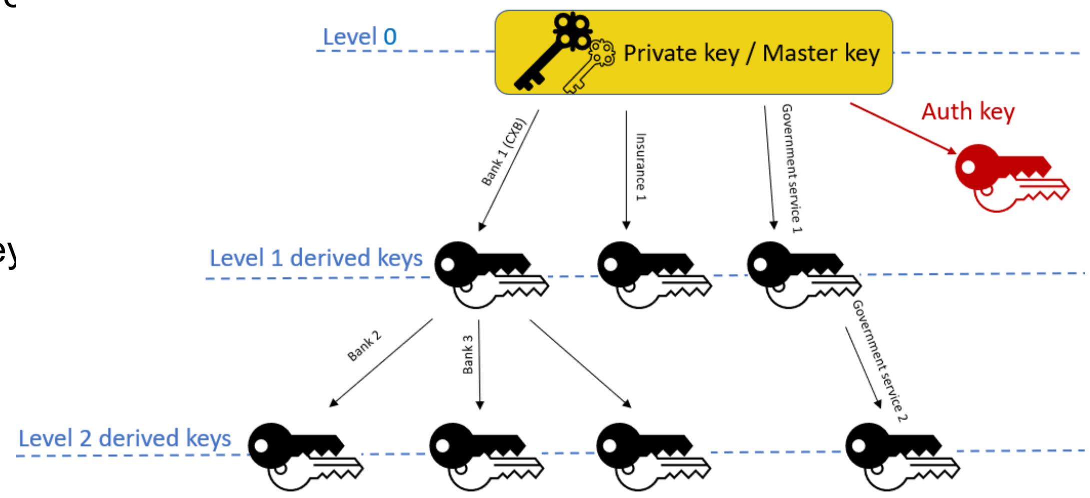
Customer ID Wallet - Self-sovereign identity and consent management tool

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

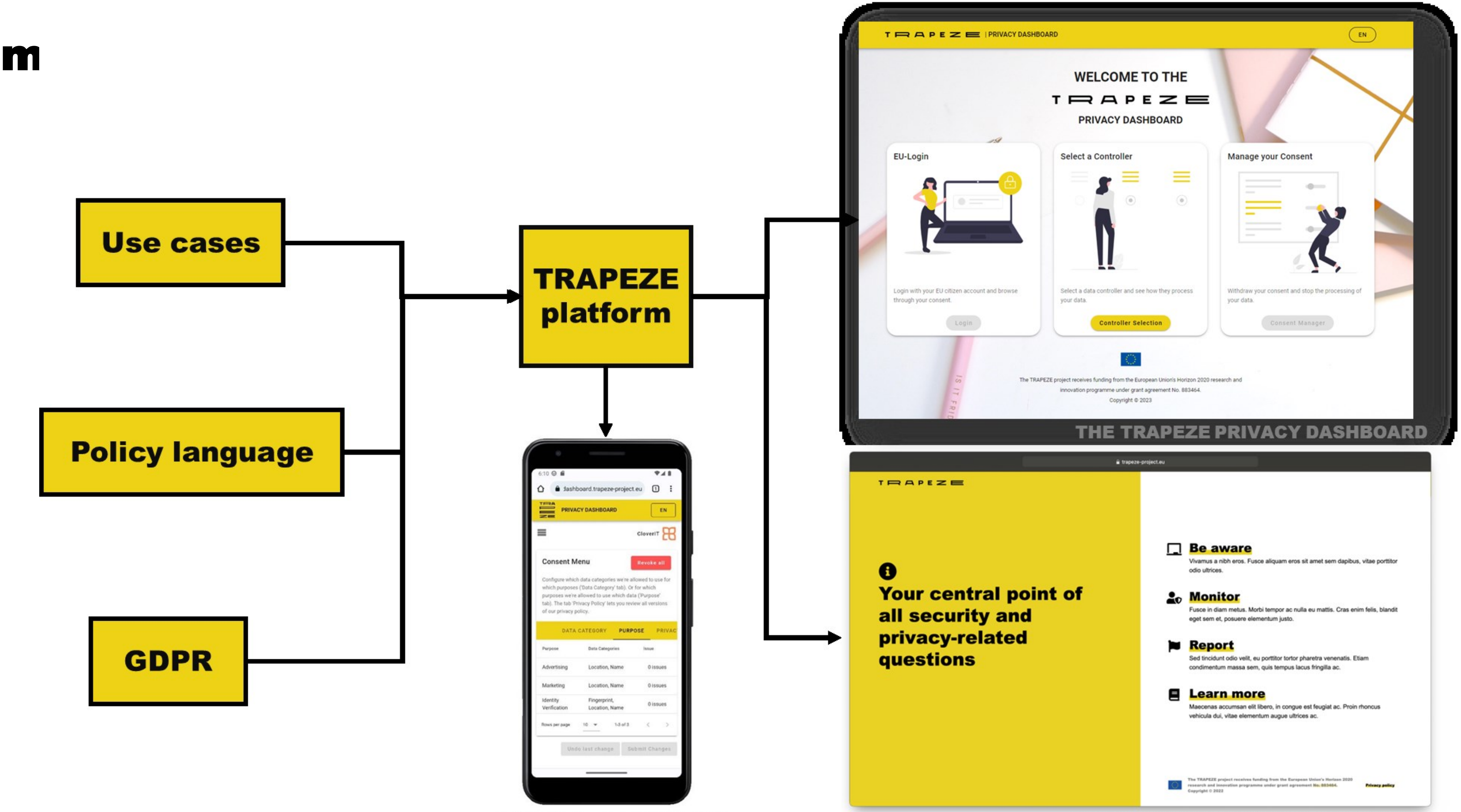
	Centralized identity	Decentralized identity
Data Storage	Centralized database	User devices
Data ownership	Data is owned by the organization with whom user share the data	Data is owned by the user
Data disclosure	Full disclosure of data available for each identity credential	Selective disclosure at user consent

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 key
  - Single master key can restore the exact same tree of keys keys.
  - User friendly keys backup and restore process



Custom



TRAPEZE | PRIVACY DASHBOARD EN

WELCOME TO THE TRAPEZE PRIVACY DASHBOARD

EU-Login

Login with your EU citizen account and browse through your consent.

Login

Select a Controller

Select a data controller and see how they process your data.

Controller Selection

Manage your Consent

Withdraw your consent and stop the processing of your data.

Consent Manager

The TRAPEZE project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883464.
Copyright © 2023

THE TRAPEZE PRIVACY DASHBOARD

6:10

dashboard.trapeze-project.eu

PRIVACY DASHBOARD EN

CloverIT

Consent Menu Revoke all

Configure which data categories we're allowed to use for which purposes ('Data Category' tab). Or for which purposes we're allowed to use which data ('Purpose' tab). The tab 'Privacy Policy' lets you review all versions of our privacy policy.

DATA CATEGORY | PURPOSE | PRIVAC

Purpose	Data Categories	Issue
Advertising	Location, Name	0 issues
Marketing	Location, Name	0 issues
Identity Verification	Fingerprint, Location, Name	0 issues

Rows per page 10 ▾ 1-3 of 3

Undo last change | Submit Changes

ID WALLET APPLICATION

trapeze-project.eu

TRAPEZE

Your central point of all security and privacy-related questions

Be aware

Vivamus a nibh eros. Fusce aliquam eros sit amet sem dapibus, vitae porttitor odio ultrices.

Monitor

Fusce in diam metus. Morbi tempor ac nulla eu mattis. Cras enim felis, blandit eget sem et, posuere elementum justo.

Report

Sed tincidunt odio velit, eu porttitor tortor pharetra venenatis. Etiam condimentum massa sem, quis tempus lacus fringilla ac.

Learn more

Maecenas accumsan elit libero, in congue est feugiat ac. Proin rhoncus vehicula dui, vitae elementum augue ultrices ac.

The TRAPEZE project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883464.
Copyright © 2022

Privacy policy

THE TRAPEZE HELP-DESK WELCOME SCREEN

Privacy Policy Language & Tools for Data Based Telco Products

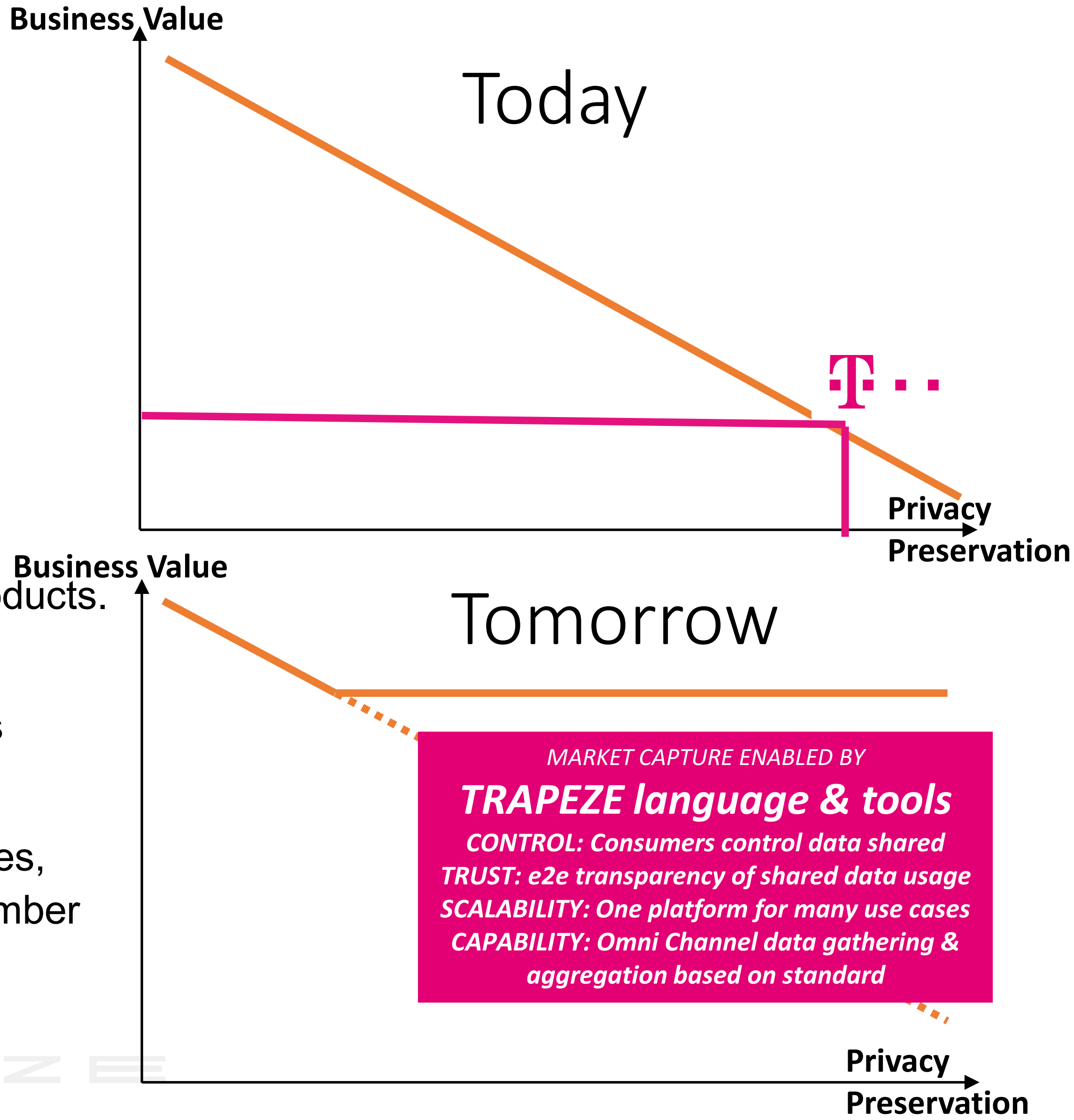
Deutsche Telekom

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 servce 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



MARKET CAPTURE ENABLED BY

TRAPEZE language & tools

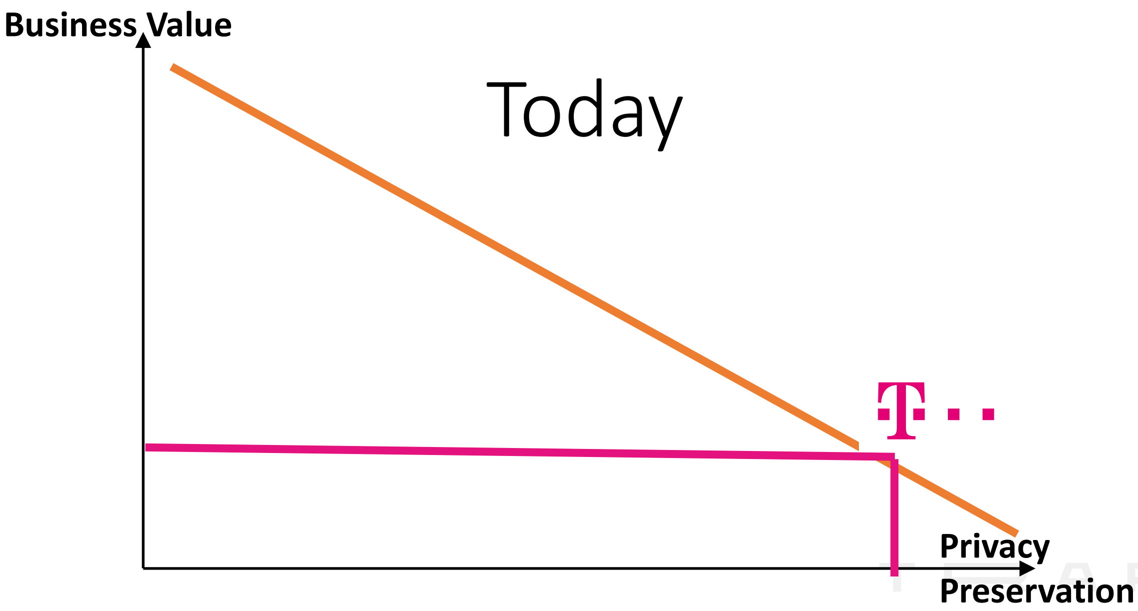
CONTROL: Consumers control data shared
TRUST: e2e transparency of shared data usage
SCALABILITY: One platform for many use cases
CAPABILITY: Omni Channel data gathering & aggregation based on standard

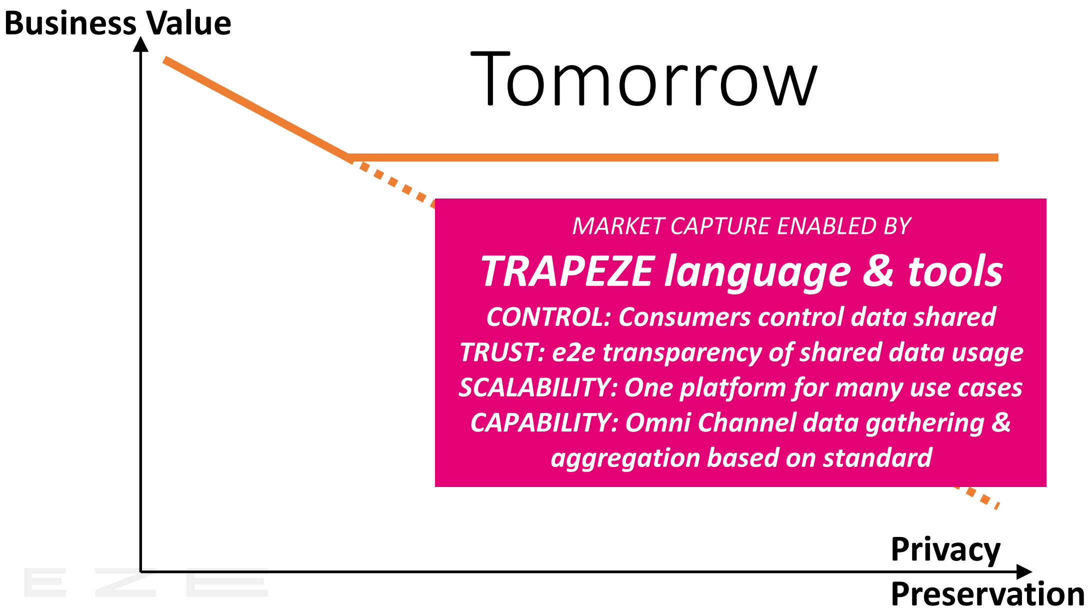
* We define “consent” as a privacy policy that both data controller and data subject agreed to

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 servce 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





MARKET CAPTURE ENABLED BY

TRAPEZE language & tools

CONTROL: Consumers control data shared
TRUST: e2e transparency of shared data usage
SCALABILITY: One platform for many use cases
CAPABILITY: Omni Channel data gathering & aggregation based on standard

* 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

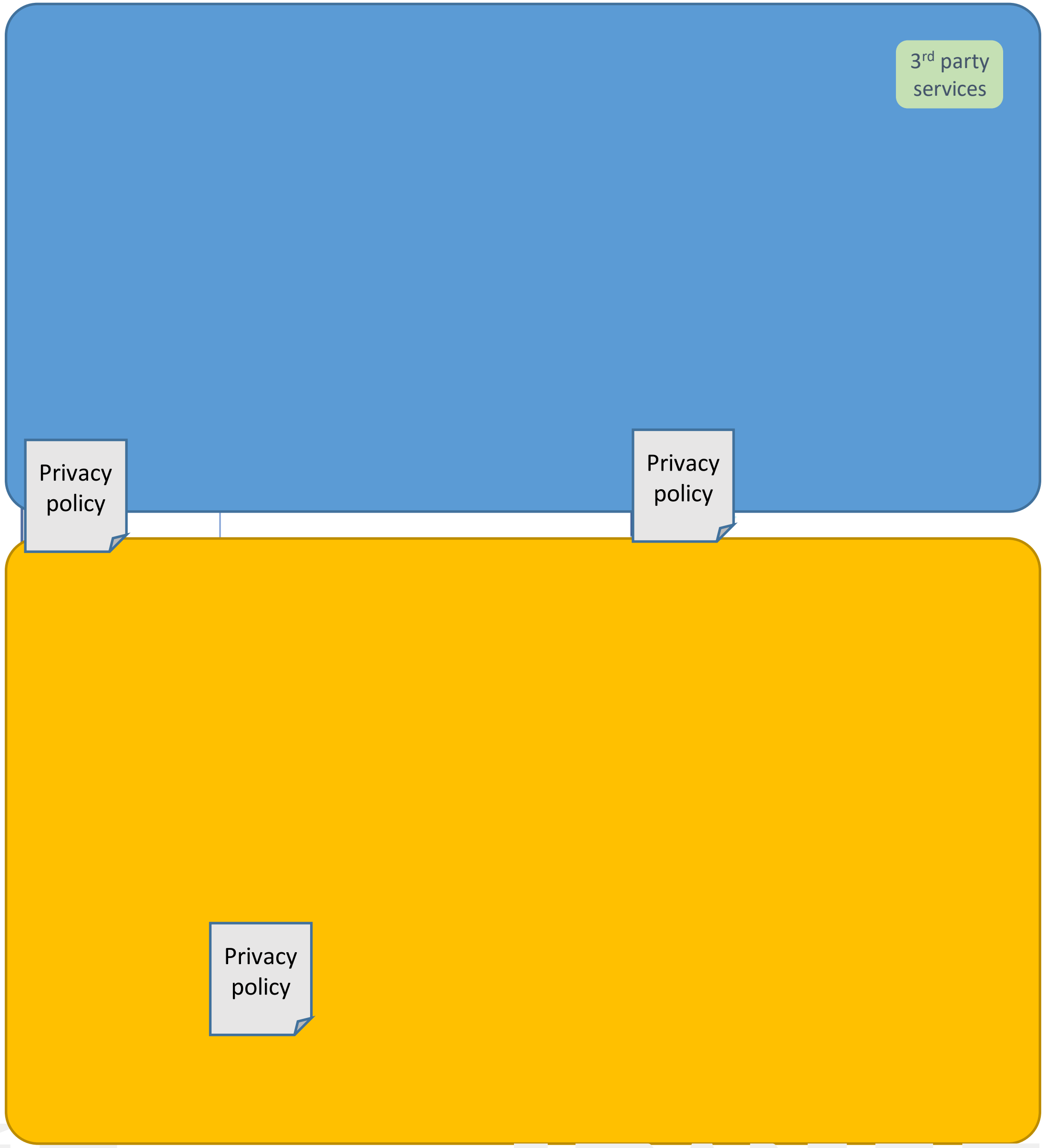
DT developed its own policy toolset, based on technology and components developed in TRAPEZE, called MHC (Magenta Hyper Consent)

AND: using the same policy language and open interfaces ↔ Privacy policy

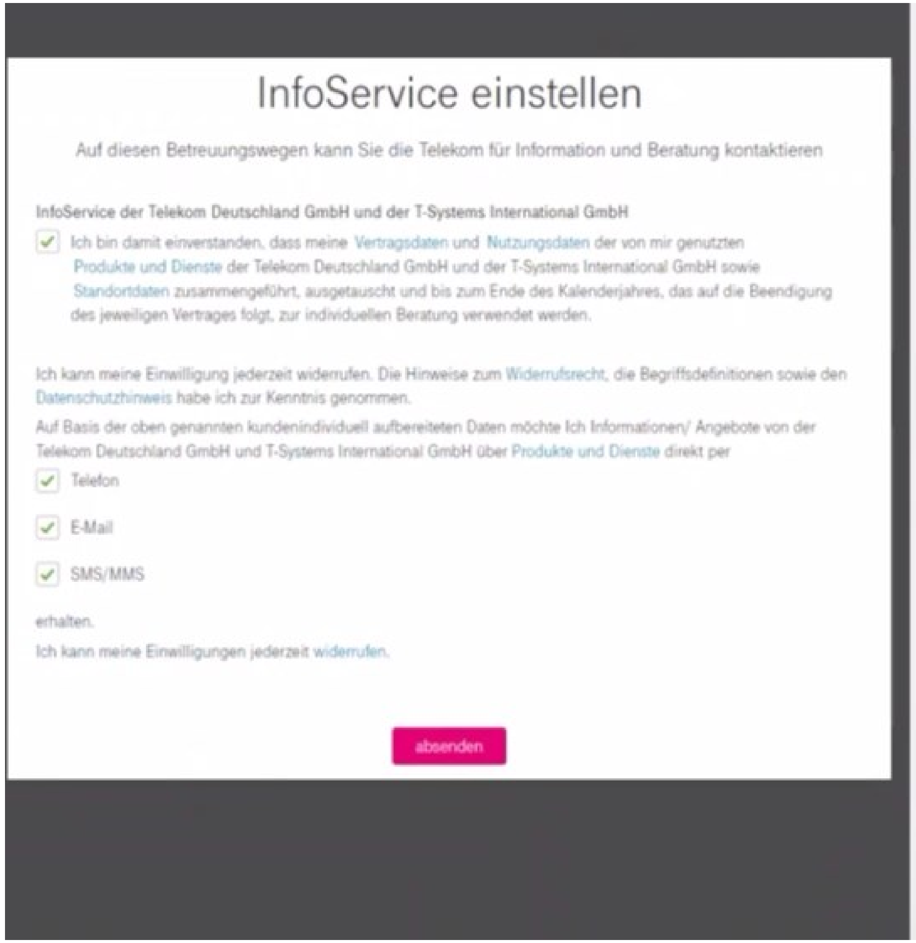
TRAPEZE platform components

3rd party components

Use Case partner's components



TRAPEZE/MHC was tested to give/control „Groupwide Consent“ (KEK = Konzern-Einwilligungs-Klausel)



InfoService einstellen

Auf diesen Betreuungswegen kann Sie die Telekom für Information und Beratung kontaktieren

InfoService der Telekom Deutschland GmbH und der T-Systems International GmbH

☑ Ich bin damit einverstanden, dass meine Vertragsdaten und Nutzungsdaten der von mir genutzten Produkte und Dienste der Telekom Deutschland GmbH und der T-Systems International GmbH sowie Standortdaten zusammengeführt, ausgetauscht und bis zum Ende des Kalenderjahres, das auf die Beendigung des jeweiligen Vertrages folgt, zur individuellen Beratung verwendet werden.

Ich kann meine Einwilligung jederzeit widerrufen. Die Hinweise zum Widerrufsrecht, die Begriffsdefinitionen sowie den Datenschutzhinweis habe ich zur Kenntnis genommen.

Auf Basis der oben genannten kundenindividuell aufbereiteten Daten möchte Ich Informationen/ Angebote von der Telekom Deutschland GmbH und T-Systems International GmbH über Produkte und Dienste direkt per

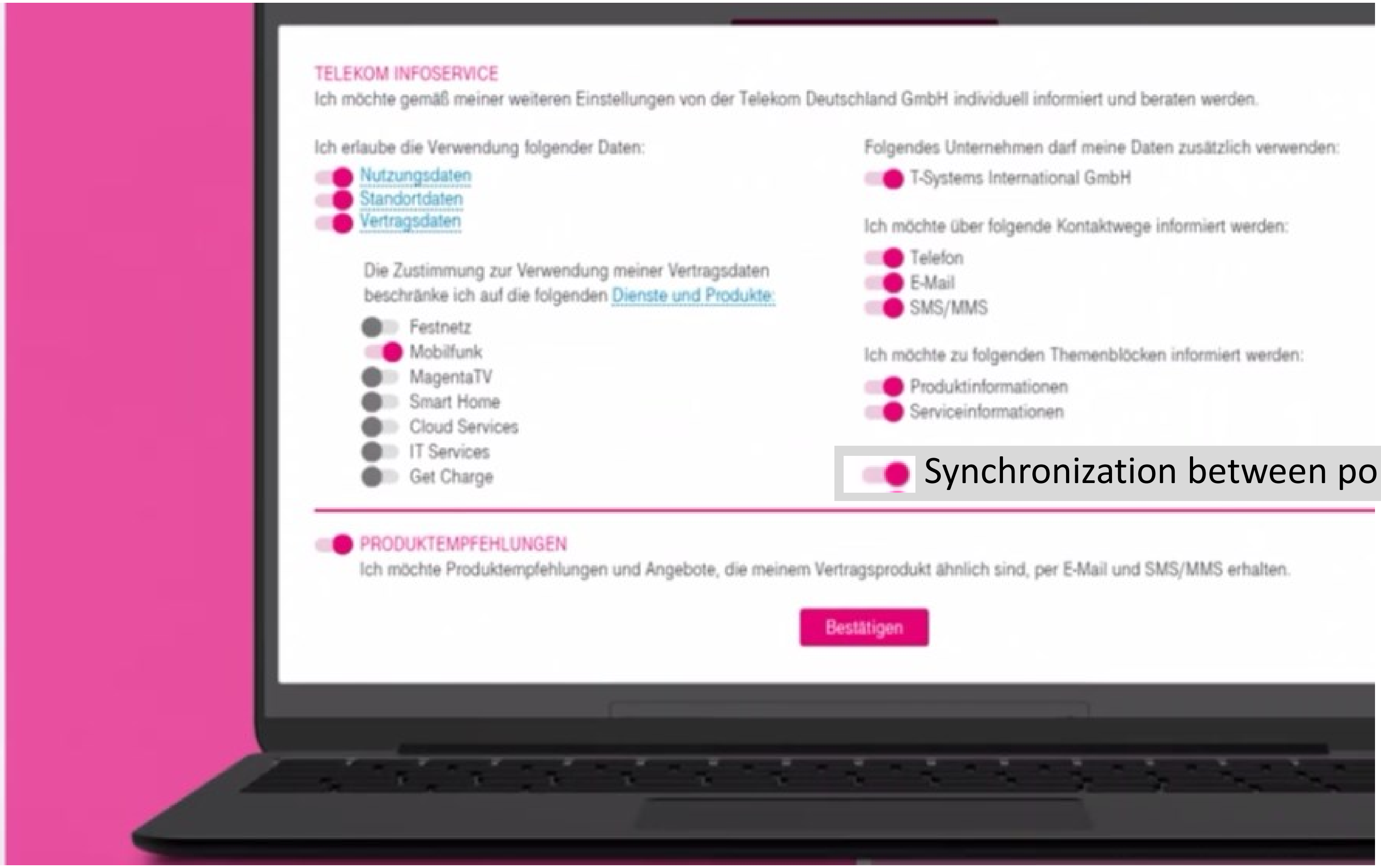
☑ Telefon

☑ E-Mail

☑ SMS/MMS

erhalten.

Ich kann meine Einwilligungen jederzeit widerrufen.



TELEKOM INFOSERVICE

Ich möchte gemäß meiner weiteren Einstellungen von der Telekom Deutschland GmbH individuell informiert und beraten werden.

Ich erlaube die Verwendung folgender Daten:

- ● Nutzungsdaten
- ● Standortdaten
- ● Vertragsdaten

Die Zustimmung zur Verwendung meiner Vertragsdaten beschränke ich auf die folgenden Dienste und Produkte:

- ○ Festnetz
- ● Mobilfunk
- ○ MagentaTV
- ○ Smart Home
- ○ Cloud Services
- ○ IT Services
- ○ Get Charge

Folgendes Unternehmen darf meine Daten zusätzlich verwenden:

- ● T-Systems International GmbH

Ich möchte über folgende Kontaktwege informiert werden:

- ● Telefon
- ● E-Mail
- ● SMS/MMS

Ich möchte zu folgenden Themenblöcken informiert werden:

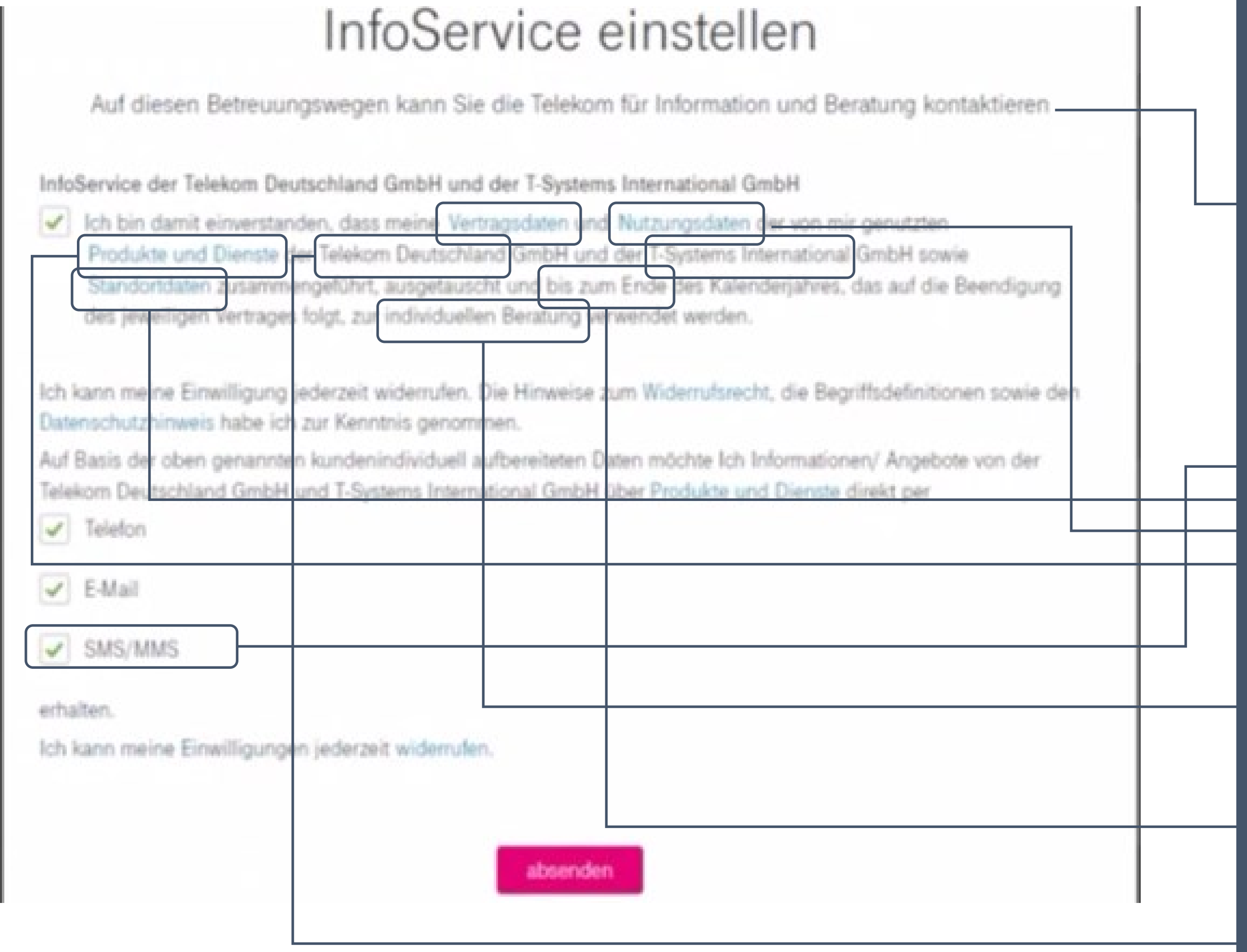
- ● Produktinformationen
- ● Serviceinformationen

● Synchronization between policies

● PRODUKTEMPFEHLUNGEN

Ich möchte Produktempfehlungen und Angebote, die meinem Vertragsprodukt ähnlich sind, per E-Mail und SMS/MMS erhalten.

KEK as TRAPEZE/MHC-Policy (human & machine readable)



InfoService einstellen

Auf diesen Betreuungswegen kann Sie die Telekom für Information und Beratung kontaktieren

InfoService der Telekom Deutschland GmbH und der T-Systems International GmbH

☑ Ich bin damit einverstanden, dass meine Vertragsdaten und Nutzungsdaten der von mir genutzten Produkte und Dienste der Telekom Deutschland GmbH und der T-Systems International GmbH sowie Standortdaten zusammengeführt, ausgetauscht und bis zum Ende des Kalenderjahres, das auf die Beendigung des jeweiligen Vertrages folgt, zur individuellen Beratung verwendet werden.

Ich kann meine Einwilligung jederzeit widerrufen. Die Hinweise zum Widerrufsrecht, die Begriffsdefinitionen sowie den Datenschutzhinweis habe ich zur Kenntnis genommen.

Auf Basis der oben genannten kundenindividuell aufbereiteten Daten möchte Ich Informationen/ Angebote von der Telekom Deutschland GmbH und T-Systems International GmbH über Produkte und Dienste direkt per

☑ Telefon

☑ E-Mail

☑ SMS/MMS

erhalten.

Ich kann meine Einwilligungen jederzeit widerrufen.

Deployment and Validation

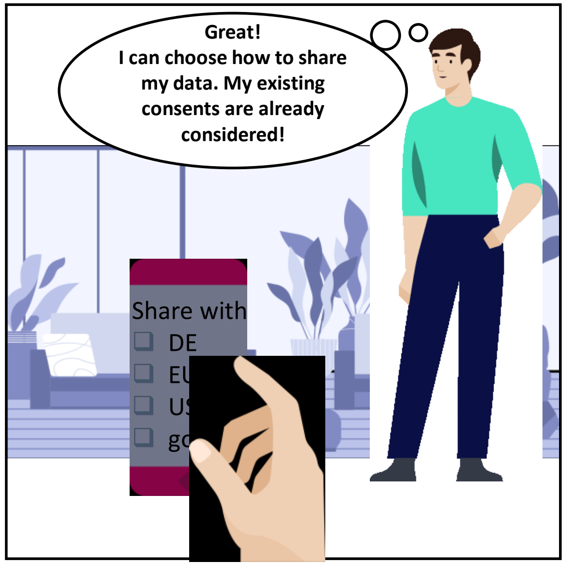
The deployment activities includes **setting up the Policy Language specification** (based on dpv and TRAPEZE/Piero Bonnati's work).

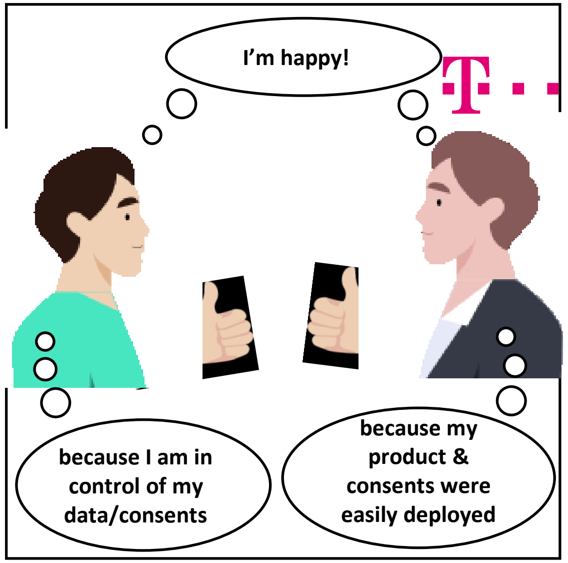
Deployment:

- 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 ft 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


Great! I can choose how to share my data. My existing consents are already considered!
Share with
□ DE
□ EU
□ US
□ go


I'm happy!
because I am in control of my data/consents
because my product & consents were easily deployed

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)

Context

Diploma in Flanders = Paper

- Diploma is issued on paper
- Cumbersome to share
- Digitized copies are being used
- Authenticity is difficult to verify
- Diploma get lost

Goal

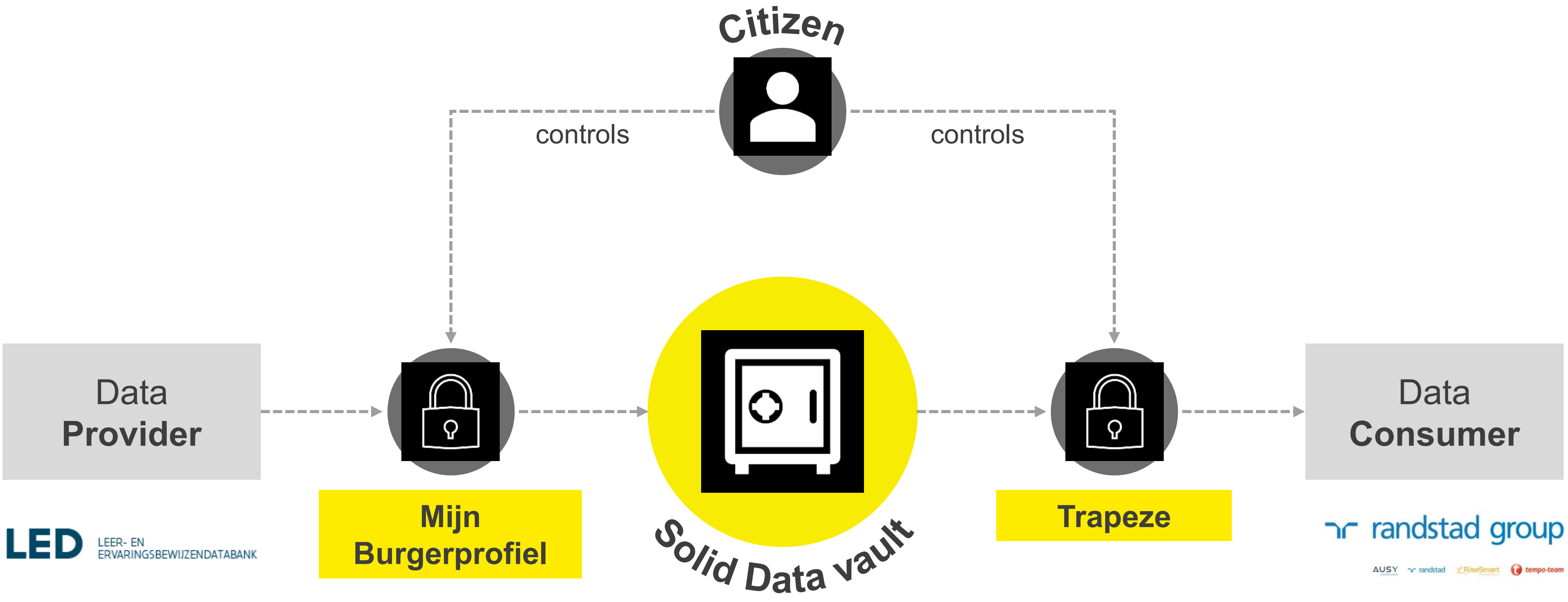
Goal

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



Citizen

controls

controls

Data
Provider

Mijn Burgerprofiel

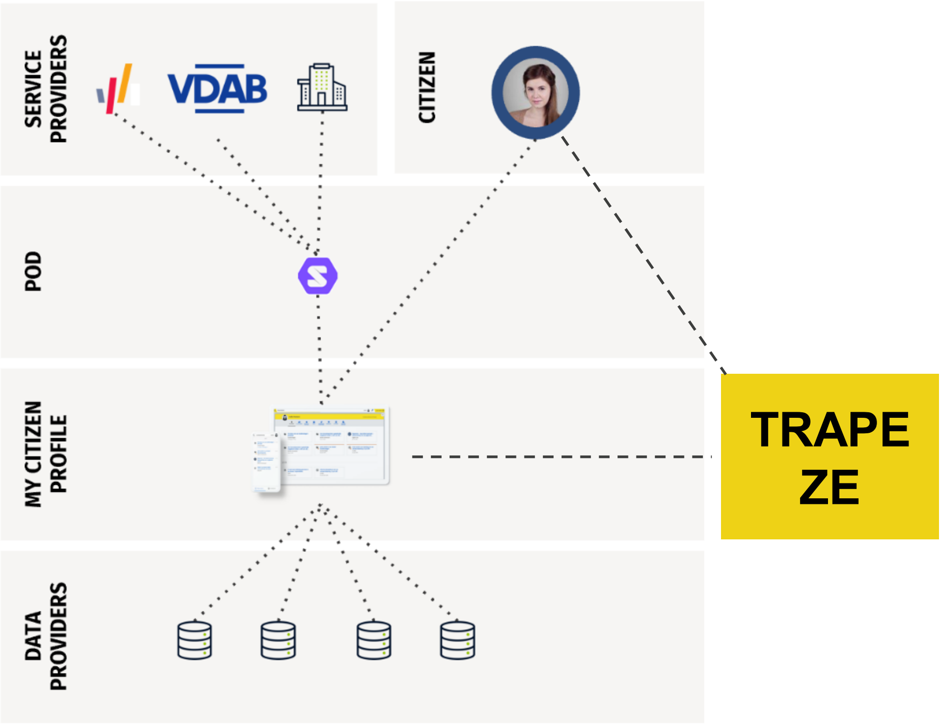
Solid Data vault

Trapeze

Data
Consumer

Solution

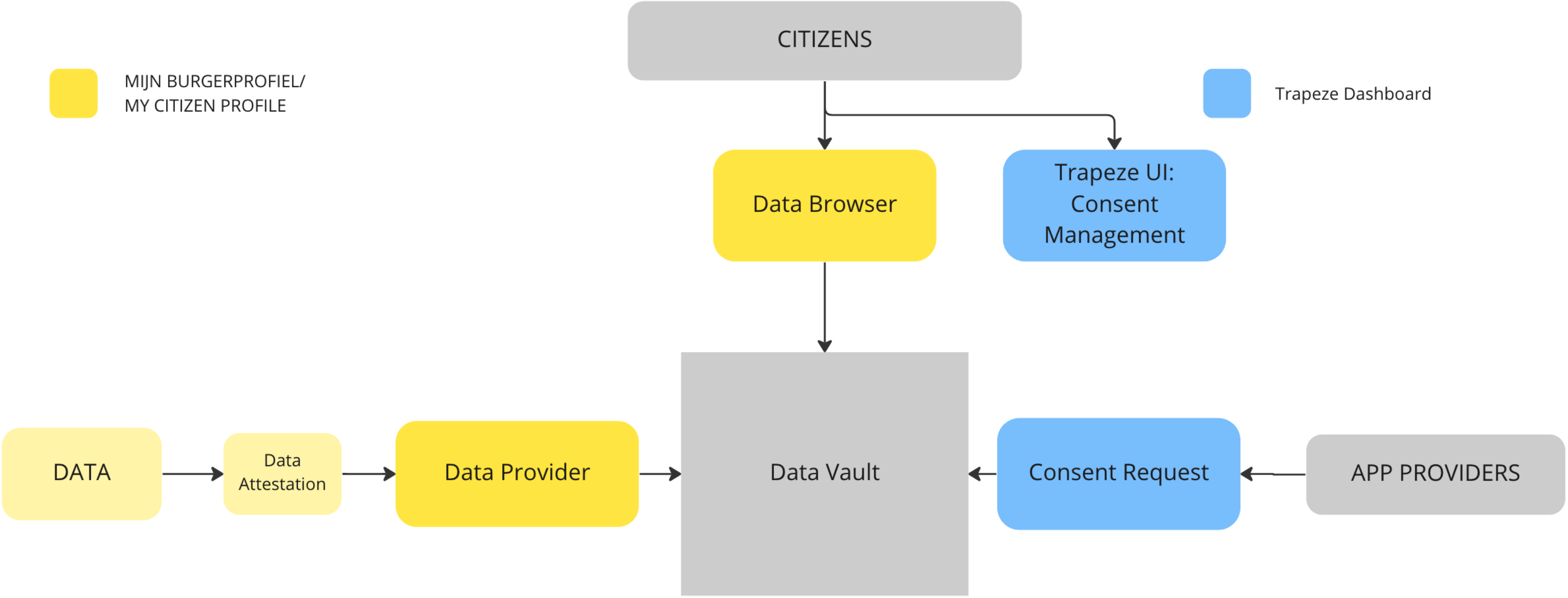
AIV (Digital Flanders) – Use case actors



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


MIJN BURGERPROFIEL/
MY CITIZEN PROFILE
CITIZENS
Trapeze Dashboard
Data Browser
Trapeze UI: Consent Management
DATA
Data Attestation
Data Provider
Data Vault
Consent Request
APP PROVIDERS

Thank you!

Raising Citizen’s Security & Privacy Awareness and Competence