



Large Scale Authentication Architecture

White Paper and Pilot

TDL | Trust in
Digital
Life

Agenda

- What is Trust in Digital Life?
- The large scale authentication infrastructure white paper
- The pilot



Introduction to TDL


TDL | Trust in
Digital
Life

Trustworthy ICT leading to innovation and growth in Europe

- Consumers have repeatedly stated that their main reasons for not buying online include concerns regarding payment security, privacy and trust.
- Eurobarometer on Attitudes on Data Protection and Electronic Identity report that Europe can develop a more productive, innovative and competitive economy that provides its people with more knowledge than ever before.
- People will have social and economic benefit from a broader provision and selection of goods and services, but lack of trust and incidents are hampering acceptance.
- Not all commercial or state actors respect the rule of law and some present a serious threat to fundamental rights. "Accountability" is insufficient – scrutiny is necessary

Trust in Digital Life shared vision

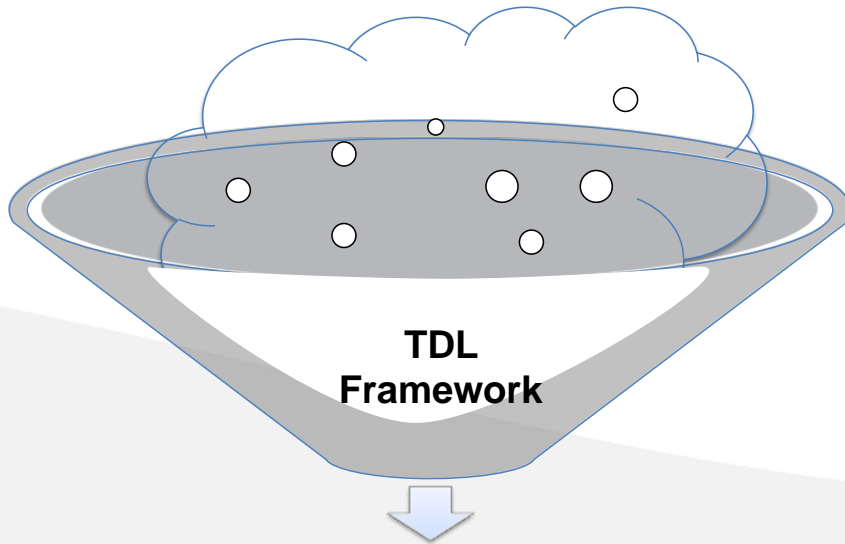
Trust in Digital Life is a **challenging ecosystem** bringing **tangible trust** in digital services supporting new ways of living and working.
Trust will become an intrinsic property of any transaction.
People should be able to recognize trustworthy services, transactions and data.

TDL Promise  4 step action plan

- 1. Consumer and industry needs:** TDL bundles multidisciplinary and cross-sectoral expertise and provides knowledge via **public and industry debates**
- 1. Challenging Strategic Research and Innovation Agenda:** with reference platforms and architectures, user stories, use cases, white papers and research questions until 2020
- 2. Innovation project portfolio:** with short and long term projects on the innovation lines Trusted Stack, Service Integrity, Data life cycle management
- 3. Short term pilot projects:** Applied research & test bed focusing on the introduction of innovative solutions in consumer domains, taking away barriers, creating trust and awareness through tangible trust/health indicators.

TDL Innovation funnel

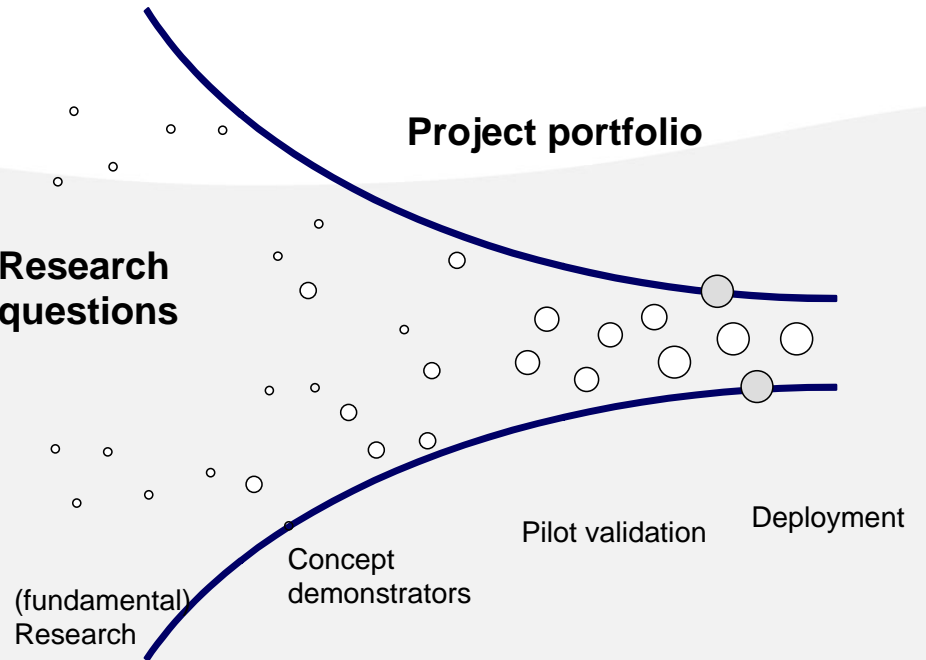
End-2-End Trust Challenges Landscape



Research & Innovation building blocks



Research questions





Authentication White Paper

TDL | Trust in
Digital
Life

White Paper Goals

- The paper is intended to provide the bigger picture when addressing Identity
 - Technologies are available from multiple vendors and OSS
 - Open standards
- Provide a blueprint to build more scalable, secure services with respect to privacy
 - What are the key points to reflect on when adding authentication infrastructures
 - And what can go wrong if you don't reflect on these points
 - Define general principles for designing authentication infrastructures on a global scale

- Introduction
- Identity Architecture Principles
 1. Composable Architecture
 2. Open to Technology and Standards evolution
 3. Attributes remain with the owner of the data
 4. User Consent
 5. Privacy
 6. Correctness and accountability

- Introduction
- Identity Architecture Principles
- Claims-based Application Architecture
 - Design Pattern
 - Externalizing Authentications
 - Moving authentication out of development increases scalability and flexibility

- Introduction
- Identity Architecture Principles
- Claims-based Application Architecture
- Architecture
 - Learn about the different components of the architecture
 - And how these components interact with each other
 - See the huge opportunity to turn legacy systems into components of the architecture as e.g. Attribute Providers

Storyline

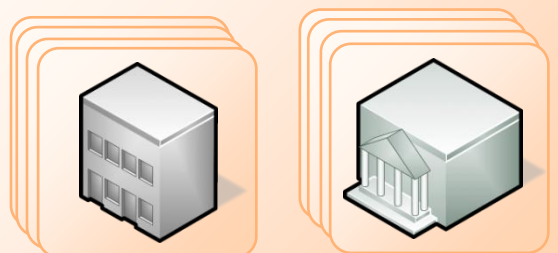
- Introduction
- Identity Architecture Principles
- Claims-based Application Architecture
- Architecture
- Threat Analysis
 - Security, Privacy and Availability threats

Storyline

- Introduction
- Identity Architecture Principles
- Claims-based Application Architecture
- Architecture
- Threat Analysis
- Relationship between existing infrastructures and the proposed architecture
 - Governments have invested in PKI and Federation Infrastructures
 - Should we start all over again?
 - Learn how the existing infrastructures fit into the proposed architecture

Trust Framework Provider

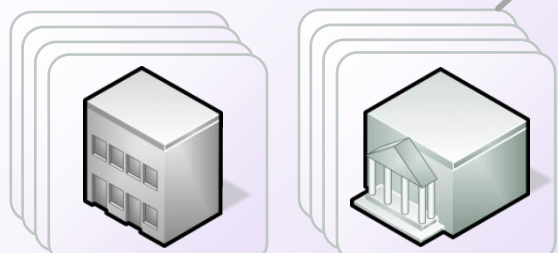
Attribute Providers



Commercial Attribute Providers

Government Attribute Providers

Identity Providers



Commercial Identity Providers

Government Identity Providers

User Identity Agent Provider

User Identity Agent



Service

3. Evaluate Policy

Client



5. User consent

Computing Devices

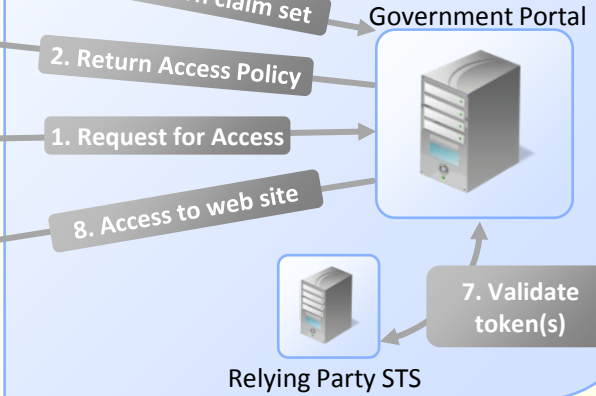
Service Providers (Relying Parties)



Cloud Services



Consumer Sites



Online

Physical World

Identity "Proofing"



Commercial Service

Government Service



User

Authentication Device Providers



IP

AP

4. Obtain token(s)

IP

IP

AP

6. Return claim set

2. Return Access Policy

1. Request for Access

8. Access to web site

7. Validate token(s)

- Paper is completed and under final review within TDL
- Will soon be published on the TDL website:
www.trustindigitallife.eu
- Obtain a link when the paper is published or queries on TDL and the pilot:
 - TDLoffice@bicore.nl



Pilot

TDL | Trust in
Digital
Life

Moving into the next steps

- Go beyond paper and implement the architecture applied in different domains
- Identity claims provide assurance on the identity of the user
 - This can be done with state of the art technology available today providing big opportunities for success
- The pilot will combine authentication with Cyber security
 - Device Health – Deliver claims about the health state of the user's device with respect to the user's privacy
 - If the user is authentication from an unhealthy device, how can one be sure about the delivered claims?
- Device Health claims provide assurance of the device
 - Device Health is a novel concept

Identity Provider

Relying Party

<p>Public Sector as Identity Provider</p> <p>Public Sector as Relying Party</p>	<p>Private Sector as Identity Provider</p> <p>Public Sector as Relying Party</p>
<p>Public Sector as Identity Provider</p> <p>Private Sector as Relying Party</p>	<p>Private Sector as Identity Provider</p> <p>Private Sector as Relying Party</p>

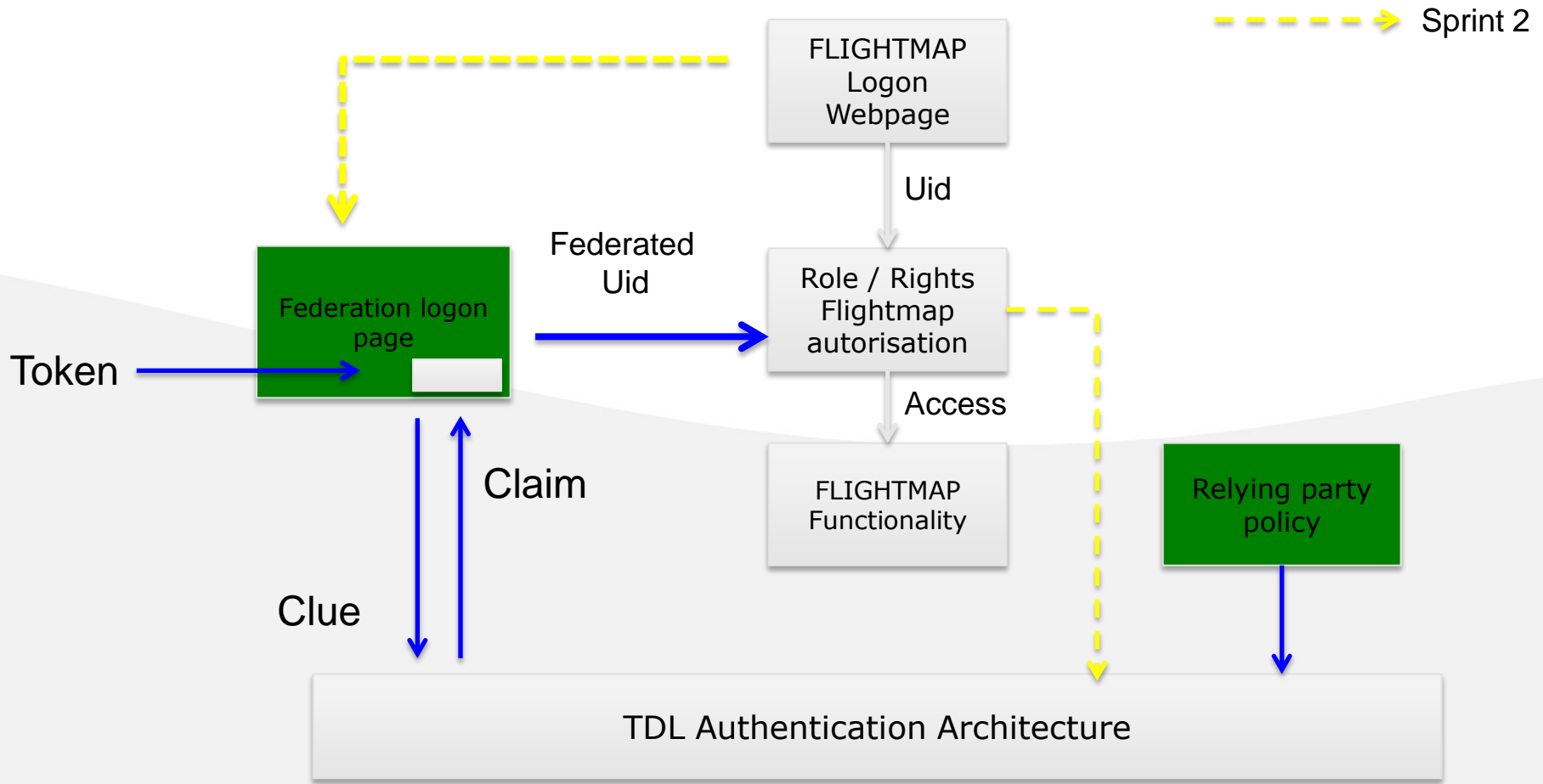
- In 2012, 4 sprints are planned
- Each sprint takes 3 months for preparation, implementation and execution
- Each sprint has one or two new applications (relying party service provision)
- Sprint one is defined:
 - Federation services for cloud service FLIGHTMAP (Bicore)
 - Health service from Philips
- Theme for Sprint 2
 - Cybercrime
 - Mobile and smart card authentication
- The E-authentication Trust framework is implemented in parallel with the 4 sprints
- Demonstration, results and feedback is provided at the end of each sprint

Use case relying party Flightmap

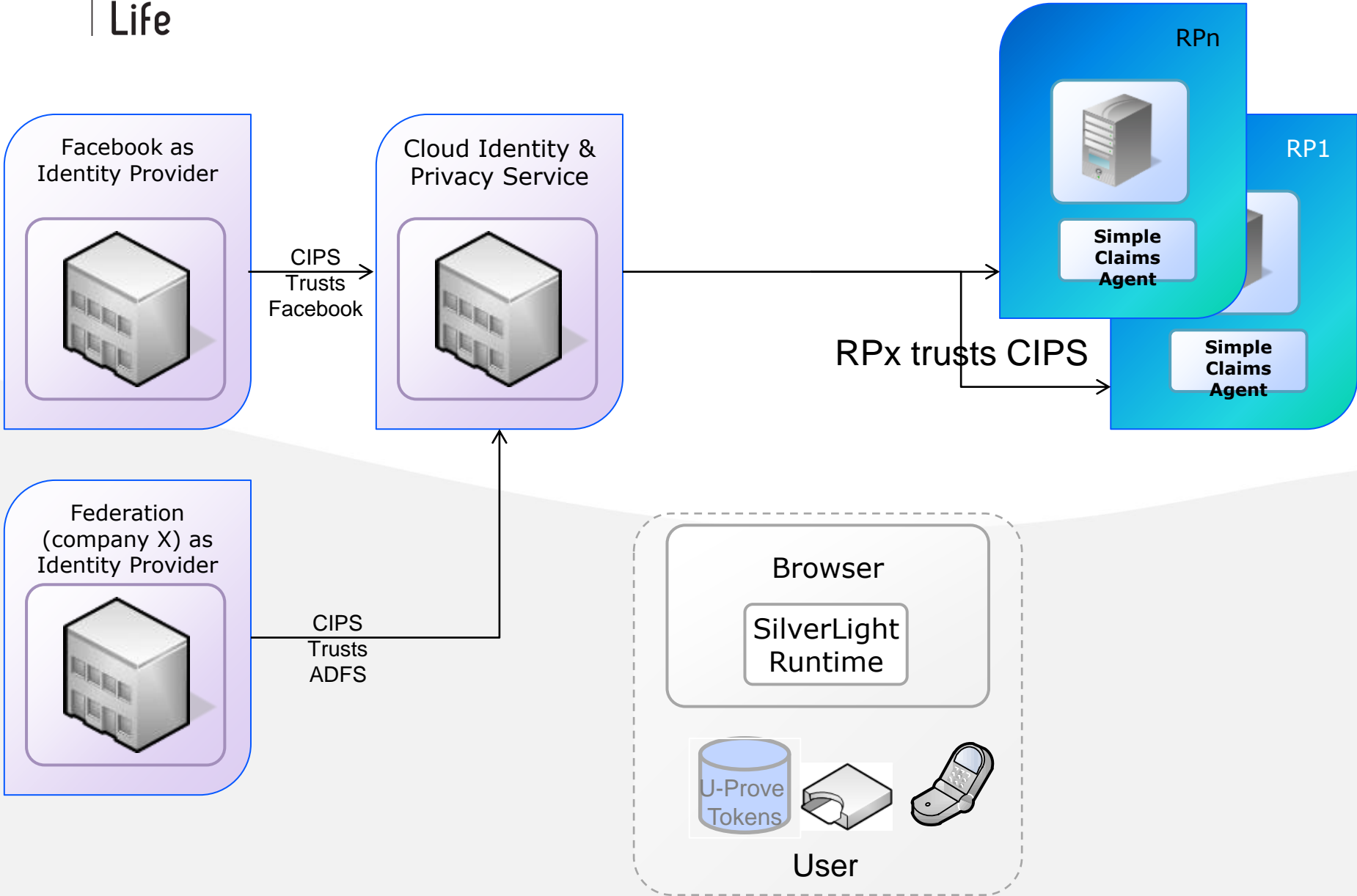
USE CASE 2: Secure access to cloud service FLIGHTMAP via single logon

- FLIGHTMAP is a cloud service for enterprises for Portfolio management on a centralized application server.
- Current situation: users logon to the system and can use two-factor authentication (application login with SMS challenge response).
- Pilot extension: Single logon. Users login into their enterprise intranet. Federation services is used for automatic validation of users to logon in FLIGHTMAP application

Technical set-up use Flightmap



TDL Authentication Architecture

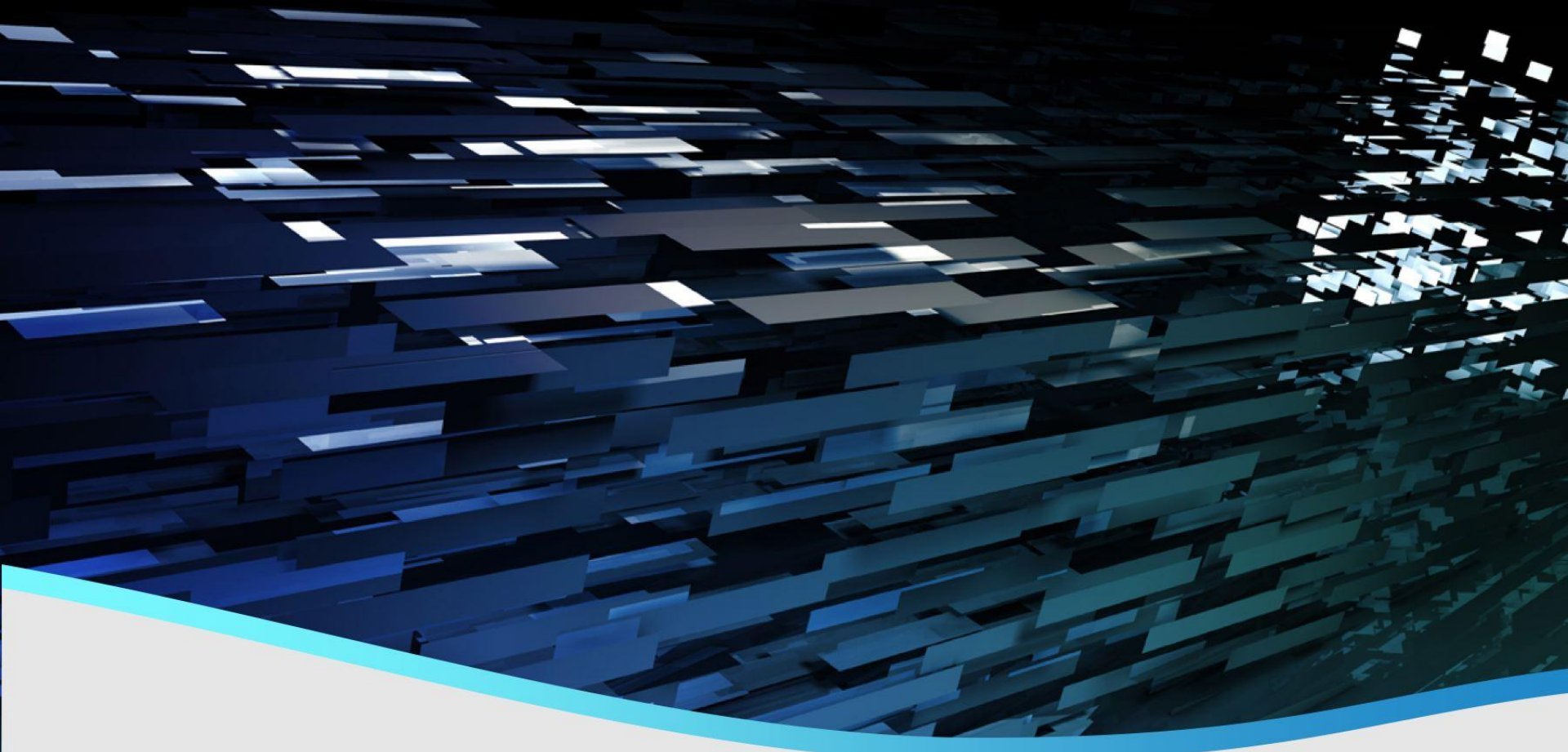


Value Proposition for members

- Based on the experiences of the industry
 - over the last ten years trying to bootstrap an identity ecosystem
 - Implementation of the six principles (white paper)
- Sustainable Infrastructure
 - To validate new ways to add identity to services
 - To validate usage of authentication methods
- Easy integration for services
 - One to two days of work
- Reach out to other partners focused on Trust
 - Knowledge institutes, government and industry

Claims based application architecture

- The best design pattern to address the listed principles
- Build-in advanced Security & Privacy
- Loosely Coupled architecture
- Supports
 - Devices
 - Multiple Identity Providers
 - Separate Attribute Providers
 - User Centric models
 - Advanced Authorization schemes



www.trustindigitallife.eu

TDL | Trust in
Digital
Life

Trust in Digital Life Ecosystem

- TDL ecosystem brings tangible trust in digital services:
 - ✓ Citizens will have the confidence to live their digital lives to the full and to unlock the latent potential of digital services, thus creating many new business opportunities.
 - ✓ TDL will bring forward new ways of living and working through innovative solutions, incorporate legal, business and technical advances, support cyber security policies, and integrate societal considerations.
 - ✓ Trust will become an intrinsic property of any transaction involving personal information, and people should be able to recognize trustworthy services, transactions and data.
 - ✓ TDL will provide user-friendly, intuitive to use, robust and self secured mechanisms for Europe's citizens that enable them to judge whether the service, data transaction or the message is trustworthy enough.
 - ✓ A social risk that seems remote today might be trivial in 15 years. TDL provides regulators with technical knowledge to act in anticipation of privacy threats when justifiable

Governance TDL Consortium

Experts from industry,
government and
knowledge institutes

Advisory Board

Executive Board

Permanent seats for founding partners:
Gemalto; Microsoft; Nokia and Philips
Elections at the general assembly

Selection of 30 members
Elections at the general assembly

Management Board

TDL Ambassadors anchoring
TDL in European research
community

TDL Mirror Group

TDL Office

Bicore: Secretary & membership mgt
Editing vision and SRA

Working Group 1

Use Cases
WG Leader: University of Luxembourg

Working Group 2

Requirements and Technology
WG Leader: Philips

Working Group 3

Law & Technology
WG Leader: Nokia

Working Group 4

Business Cases
WG Leader: Corvinus University, Hungary

- Growing membership >25 members
- Developing associations with other trust initiatives
- Investing by members in selected innovations
- Collaboration with regulators and policy makers to remove barriers
- ENISA., Digital Enlightenment forum, Effects plus

TDL Trust in Digital Life

TDL Membership status

Industrial and Service Sector ●

- Microsoft
- Nokia
- Philips
- Gemalto
- Oberthur
- Irreto
- NEC Europe
- Nokia Siemens Networks
- NXP
- Thales (New)

Knowledge Institutes ●

- Fraunhofer Institute Fokus
- Goethe University
- Privacy International
- University of Twente
- University of Murcia
- University of Luxembourg
- Waterford Institute of Technology
- KU Leuven
- Norwegian Consumer Council



