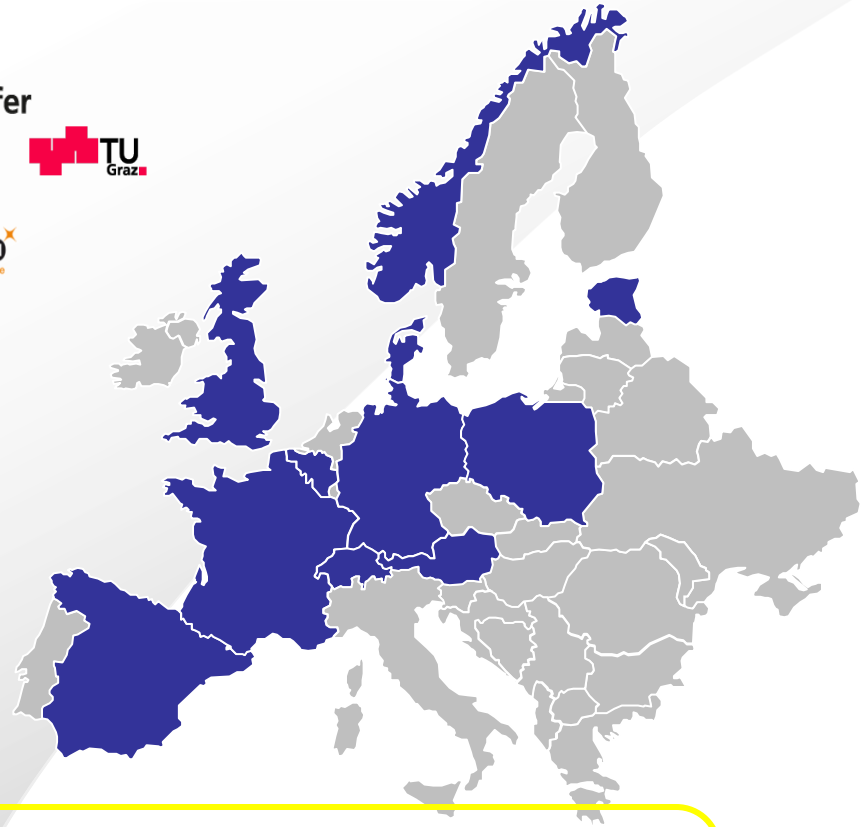
FutureID - Shaping the Future of Electronic Identity

Heiko Roßnagel, Jan Camenisch, Lothar Fritsch, Thomas Gross, Detlef Houdeau, Detlef Hühnlein, Anja Lehmann, Jon Shamah



Annual Privacy Forum 2012, October 11th, Limassol, Cyprus

FutureID is partly funded by EU FP7 under GA n°318424

Introduction

- Combination of eID and federated identity management technology promises a major improvement of security on the web
  - providing secure and user-friendly authentication
  - leading to a significant increase of confidence and trust in the use of ICT by EU citizens and business

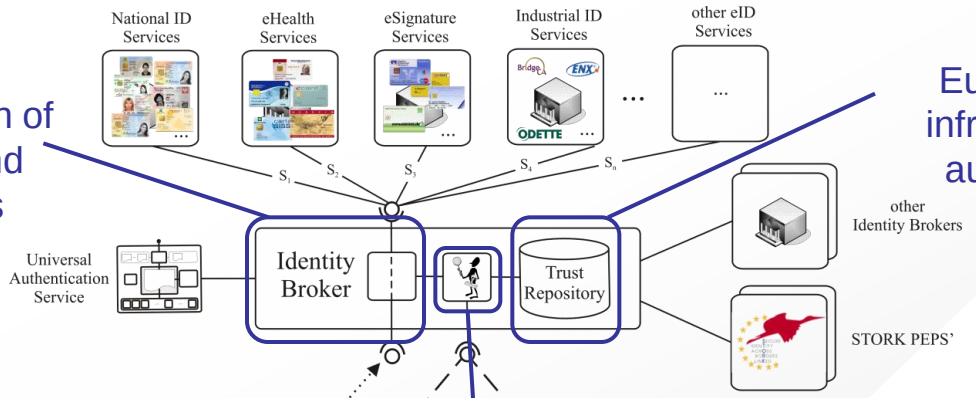
- However, there are many unsolved challenges, which prevent the interoperable, secure, ubiquitous, easy and privacy-friendly use of strong authentication mechanisms across Europe
  - no standardized, trustworthy and ubiquitously usable eID client
  - complex and costly integration of authentication and identity services
  - no coherent European trust infrastructure for authentication
  - privacy threats of real world authentication solutions
  - non-technical problems

FutureID is partly funded by EU FP7 under GA n°318424

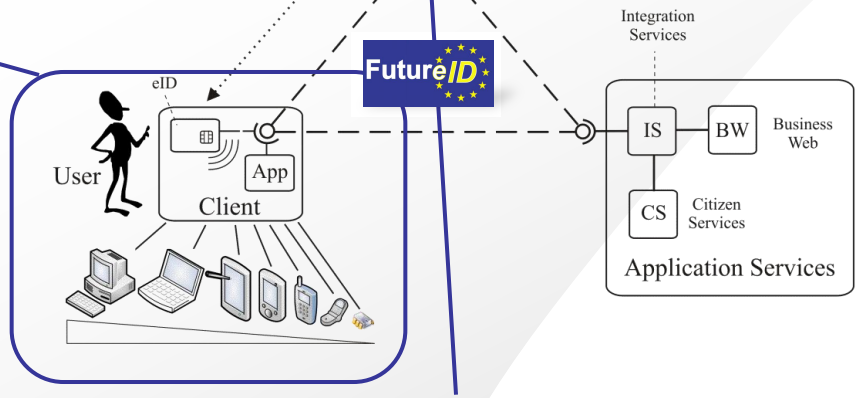
FutureID – Addressing the Challenges

Easy and cost effective integration of authentication and identity services

Coherent European trust infrastructure for authentication



Standardized, trustworthy and ubiquitously usable eID client



open source

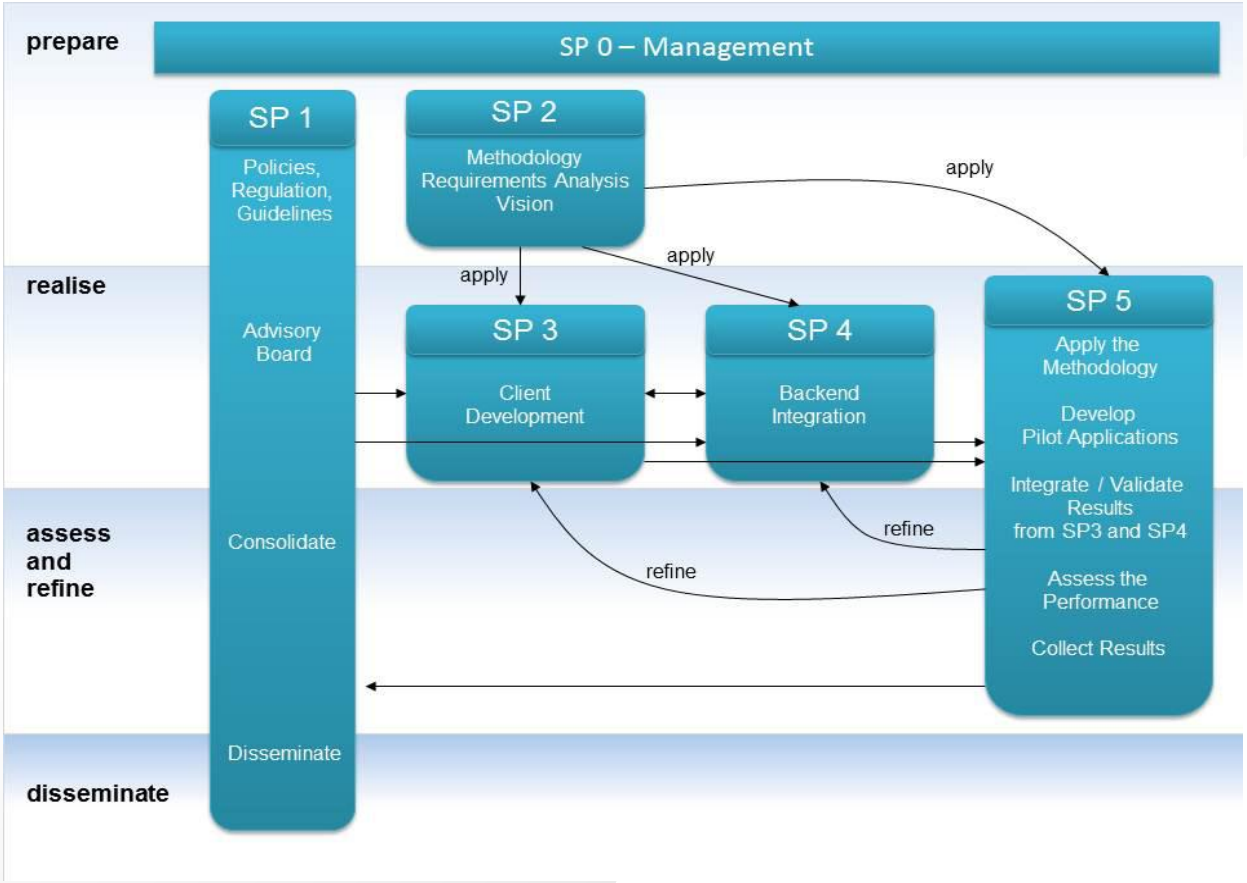
policy
law
economics

Addressing non-technical requirements

Privacy enhancing authentication protocols for the real world

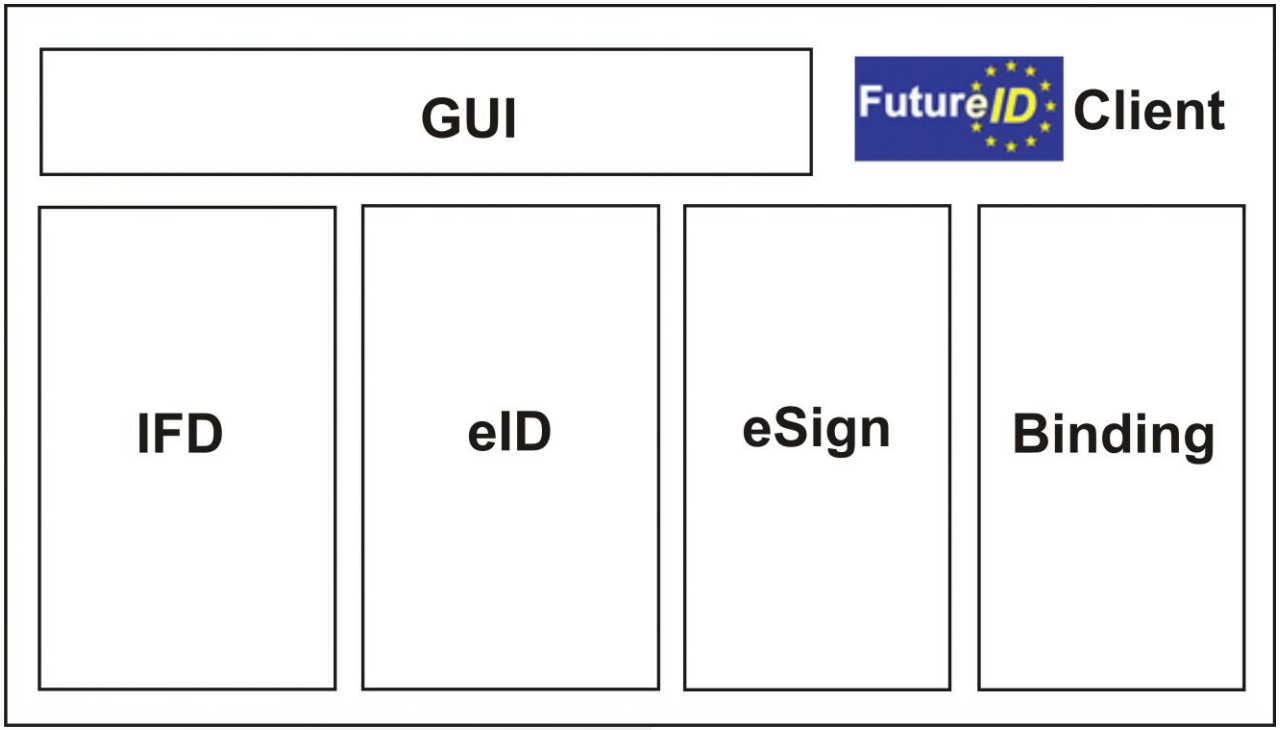
FutureID is partly funded by EU FP7 under GA n°318424

Overview of FutureID Workplan



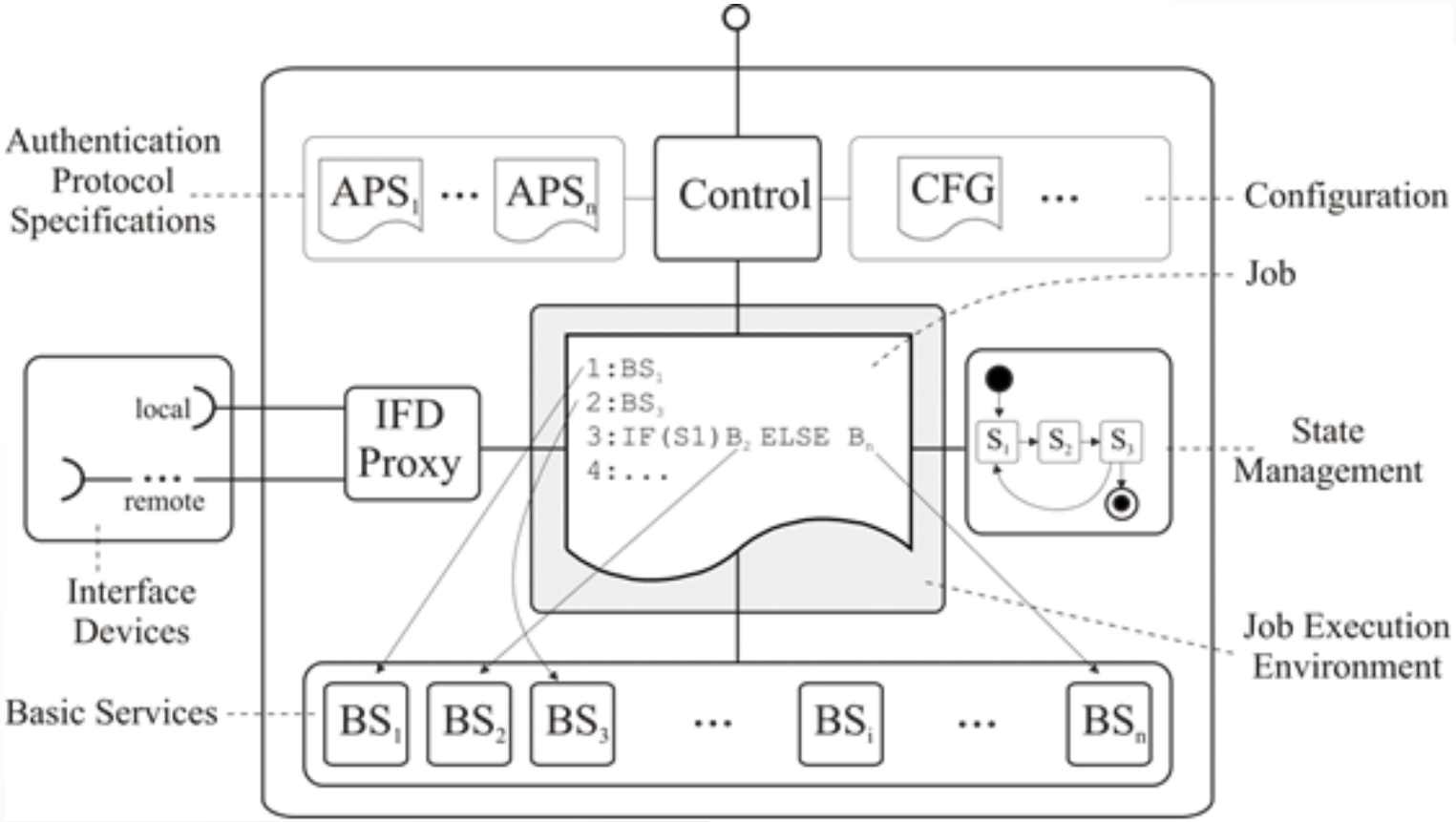
FutureID is partly funded by EU FP7 under GA n°318424

Client Components



FutureID is partly funded by EU FP7 under GA n°318424

High Level Design of the Universal Authentication Service



FutureID is partly funded by EU FP7 under GA n°318424

FutureID Consortium

19 Partners from 11 European Countries

Research Organisations

Fraunhofer

Norsk Regnesentral

Small and Medium Enterprises

esec

trustable

SK

AGETO

Data Protection Agency / NPO

ULD

eema

Industry Participants

gemalto

Atos

IBM

infineon

COMARCH

Giesecke & Devrient

Creating Confidence.

Universities

DTU

TU Graz

Newcastle University

KATHOLIEKE UNIVERSITEIT LEUVEN

TECHNISCHE UNIVERSITÄT DARMSTADT

FutureID is partly funded by EU FP7 under GA n°318424

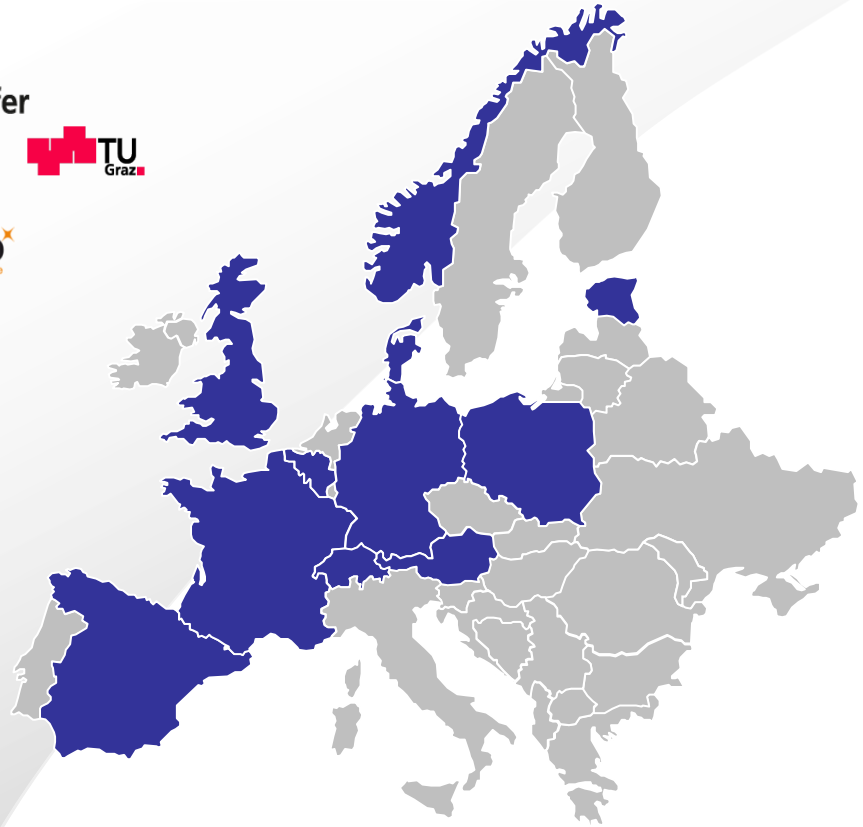
Impact

FutureID will provide benefits to all stakeholders involved

- **Users** will benefit from ubiquitously usable open source eID client
  - Running on desktop PCs, tablets and smartphones.
  - Special attention to ensure the user-friendliness of this client.
  - Removing a major barrier towards the wide application of eID
- **Application and service providers** will be enabled to use trustworthy authentication services
  - Reducing up-front investments in eID
  - Providing new business opportunities
  - Addressing new consumers segments by mitigating trust issues or privacy concerns.
- For the **e-government** domain FutureID will enable new online services
  - By combination of identity management systems with the strong authentication and signature functionality
  - Provide the necessary security infrastructure elininating security or legal constraints.
- FutureID will reduce cost for **businesses** to setup or migrate to use of eID
  - in their standard business activities
  - avoid high (prohibitive) transaction costs
- **Identity service providers** will benefit from the increased pool of potential customers
  - easy integration of existing identity services into the universal authentication service.

FutureID is partly funded by EU FP7 under GA n°318424

Thank you for your attention!



FutureID is partly funded by EU FP7 under GA n°318424

Attribute based credentials

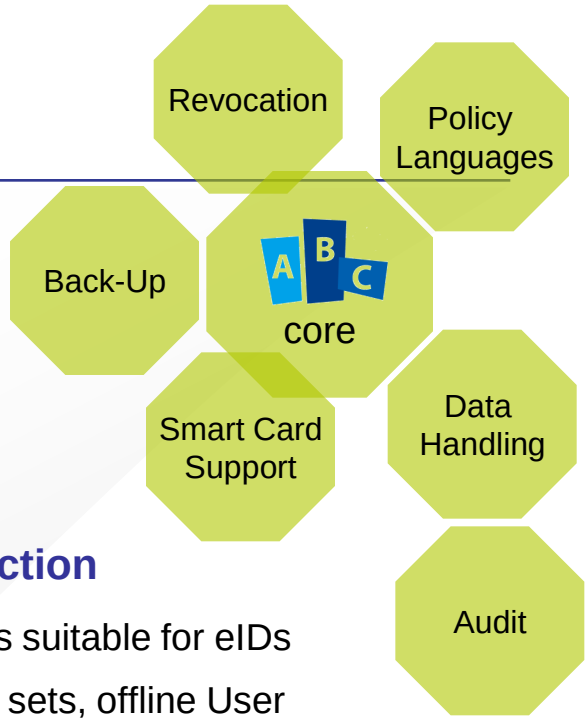
- pseudonymous authentication, unlinkable credentials, minimal attribute disclosure
- state of the art: core technology (e.g, Idemix, UProve) is mature and deployed in real-life *pilots* (PrimeLife, ABC4Trust)

- **Integrate ABCs into eID infrastructures and provide deployment roadmap to take full advantage of privacy features**
  - ABC integration and support in Identity Broker, Universal Authentication Service and FutureID client
  - approach integration into eID standards, e.g., CEN 15480, ISO/IEC 24727, ICAO, ...
- **Advance efficiency and usability of ABCs on smart cards**
  - smart card: + extra protection - limited resources, without UI
  - preliminary, technology-specific approaches to combine advantages of smartcard & PC deployment – realizable on standard smartcards

  → FutureID will **provide unified "device-binding" mode of ABCs**

FutureID is partly funded by EU FP7 under GA n°318424

Attribute based credentials



- **Provide solutions to real-life usability issues**
  - secure back-up and recovery of credentials that are stored / bound to device
- **Provide mechanisms & tools that complement ABC core technology to enable full-fledged privacy-protection**
  - developing new privacy-enhancing revocation mechanisms suitable for eIDs
    - unsolved challenges: frequent revocation, large User sets, offline User
    - open issues: ABC-specific requirements, e.g. local revocation of pseudonyms
  - developing protection and audit mechanisms for released attributes
- **Closing the gap between policy/claim languages and cryptographic realizations**
  - providing formal semantics and verification tools for ABC language

FutureID is partly funded by EU FP7 under GA n°318424