methics

Mobile Identity Service integration with Identity Provider

ENISA Track - Session 2D

11.6.2008

Jarmo Miettinen
Methics Ltd

Content

- Methics Ltd
- Business case
  - The Business Problem
- RepRo project
  - Solution
  - Use case
- Conclusion

Methics Ltd

- Methics Ltd is a privately held consulting company
  - Established 2002. The company is specialized in subscriber management and data communication infrastructure development for security, subscriber and service management and business intelligence.
  - Chairman of the board: Stefan Engel-Flechsig
  - CEO: Jarmo Miettinen
  - Product development: Asko Saura
- Turnover 2007: 800.000 EUR
  - Dun & Bradstreet AAA (2006, 2007)
- Kiuru-product family
  - Kiuru MSSP Release 3

methics

The Business case

There are thousands of bank brance offices. We would like to reduce number of these offices.

To be able do this End User must be able to open a new bank account over the Internet.

Business case is real and simple.

Why are we not opening bank accounts over the net?

methics

What is the Problem?

Money laundering is illegal. Money laundering is the practice of **engaging in financial transactions** in order to

conceal the identity of source or destination of money.

The prime method of anti-money laundering is the requirement on financial intermediaries to know their customers.

Opening a bank account has one prime requirement:

Know your customer (KYC)

KYC Definitions

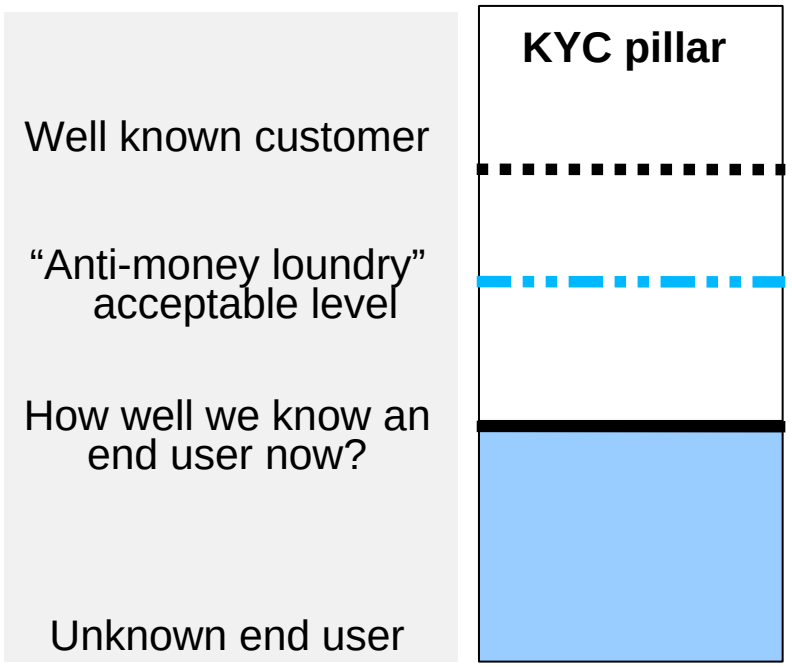
- Due diligence and bank regulation
- Financial institutions and other regulated companies must perform to identify their clients and ascertain relevant information before doing financial business with them.
  - Verify that the customer is not in known money launderers list
  - Collect reasonable assurance information
- What is reasonable information
  - Factors including jurisdiction, risk and resources.
  - The common knowledge - civil standard of proof
- ETC

Our Definition for KYC

- Collect Relevant unfavorable information from several sources
- Collect Relevant favorable information from several sources
- Analyze the data and make a “Accept or Reject” decission

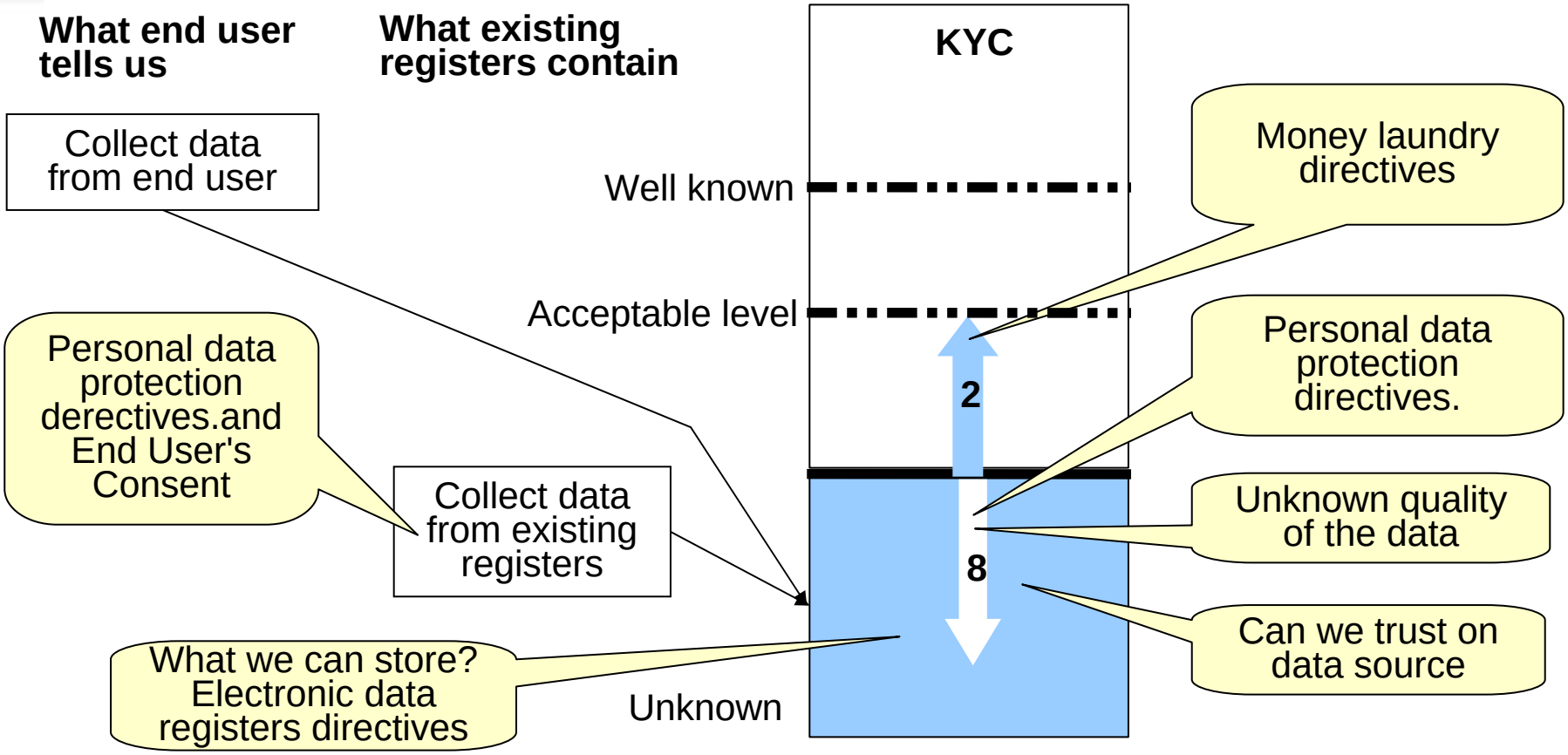
Process must be

- Rigorous and robust, consistent, thorough and accurate, documented and auditable, scalable and proportionate to the risk and resources ...
- Based on open standards



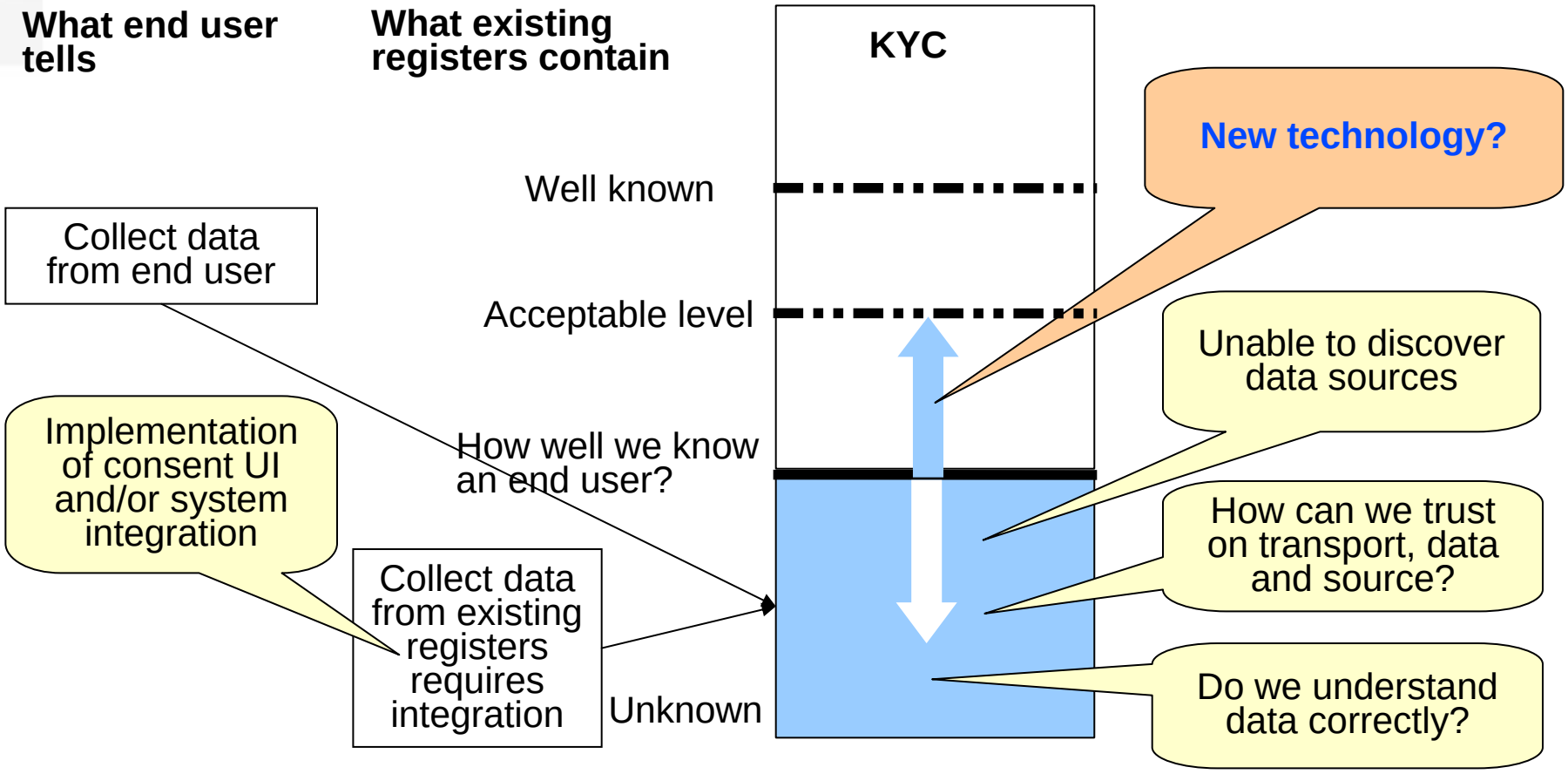
Know Your Customer

Legal perspective – Competition between privacy and money laundry regulations.



Know Your Customer

Technical perspective – Where from we can get the KYC data and can we trust on it?



methics

RePro Project

- **Re**gistering and **Pro**file distribution
- Repro project tries to create a model where MSS combined with IdP technologies can provide a simple and robust technical solution for the KYC problem.

- Financed by Methics and TEKES
- Duration 1.1-31.12.2008
- Research partner: Helsinki University

Technology

- The Identity Provider Discovery **Problem**
- The identity Framework **Problem**
- The identity InterCoT **Problem**
- Application complexity **Problem**
- MSS has **complicated** infrastructure, SIM cards etc
- MSS has **complicated** business models etc
- MSS has **limited** functionality

Let's try something else.
How about
MSS and IdP technologies together

Solution in Principle

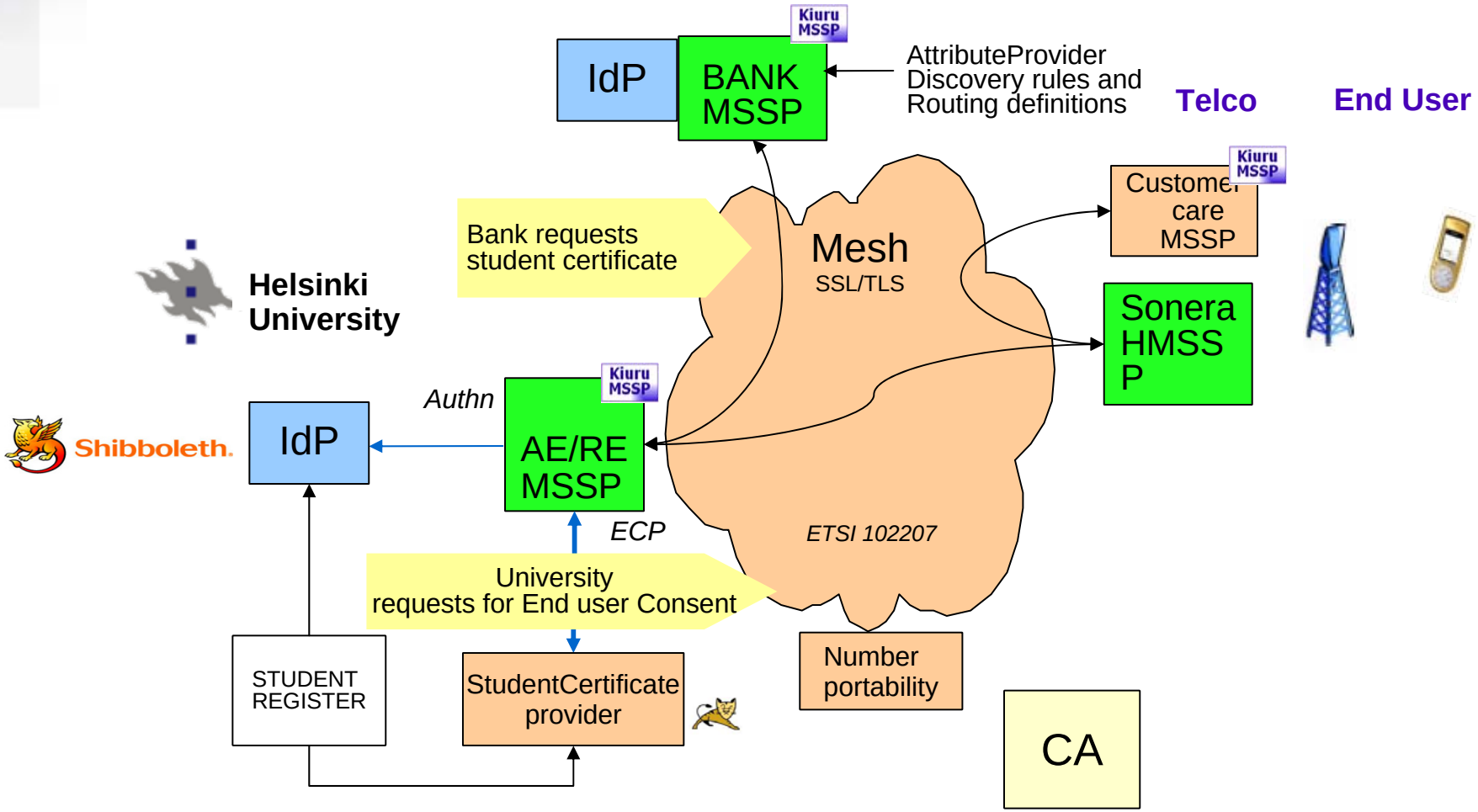
1. **Select well-known target customer group**
   - ✓ New students in Helsinki University
2. **Enable MSS service with the target group**
   - ✓ University knows Students. New students can register in the University IT-services by using MSS service.
3. **Define favorable data sets of the customer group and containers for that data**
   - ✓ Student certificate - (SAML2 Assertion)
   - ✓ Population registration center – (X.509+ WS=>Assertion)
   - ✓ Mobile operator's customer certificate - (SAML2 Assertion)
   - ✓ End User's input with legally binding electronic signature - (PKCS#7)
4. **Enable Student's profile discovery and reliable distribution**
   - ✓ Implement Consent
   - ✓ Transport over MSS roaming network

Using SAML2 and MSS

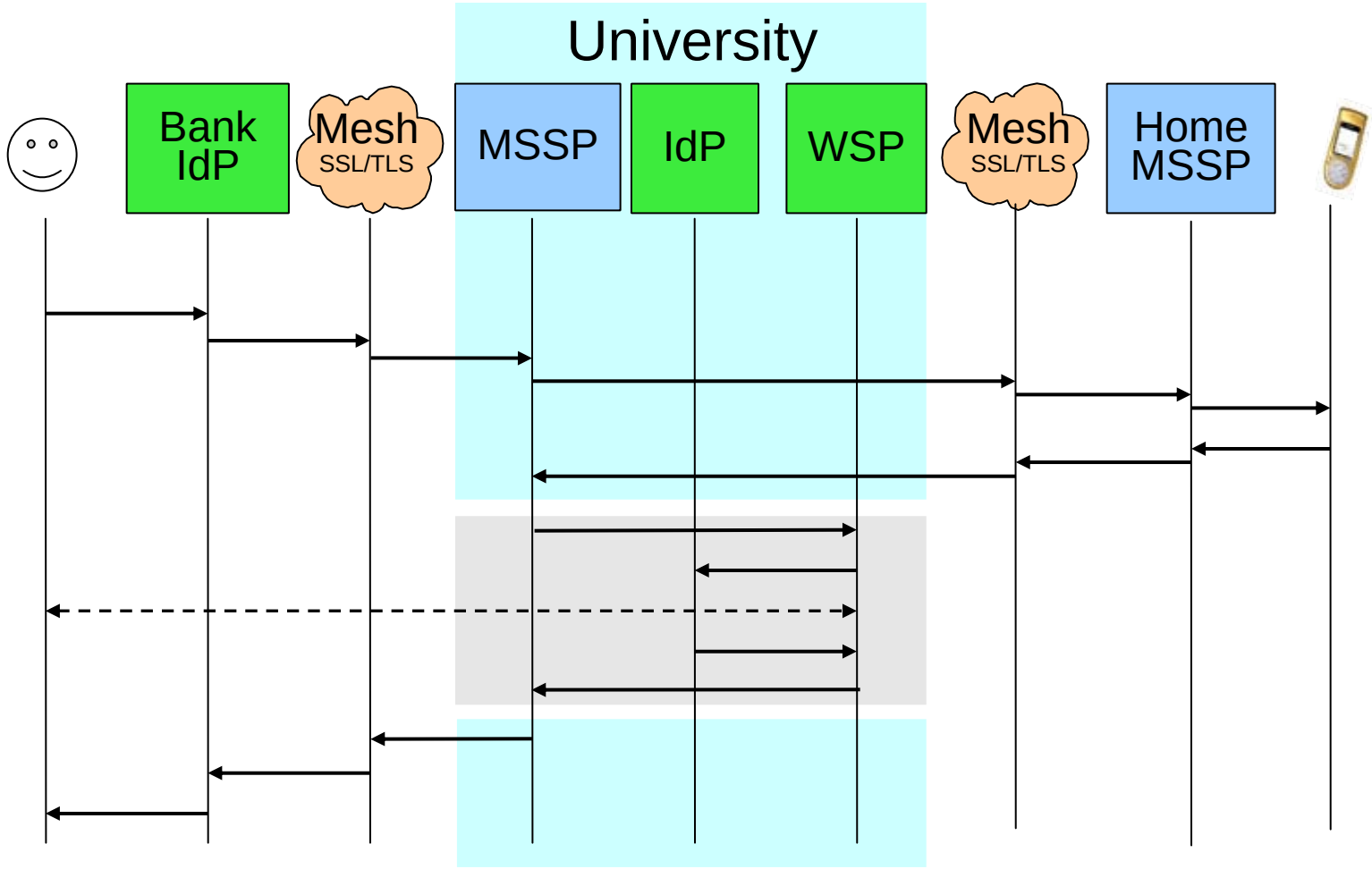
1. **Mobile Signature Service as an Authentication Provider**
   - IdP model contains methods to integrate Authn-servers
   - ETSI TS 102 204 interface can be used
2. **Mobile Signature Service connection with Attribute Provider**
   - MSS contains simple methods for AdditionalService request
   - MSS roaming model contains routing by AdditionalService
   - MSS provides simple methods for transporting End user Identity and assertions
   - Every IdP model has a method for accessing End User's Attributes, Authorizing Attibute Queries and creating Assertions

   Interface between MSS and IdP:
   - MSSP use SAML2 Attribute Query or Liberty ECP profile
   - Standard Assertions, IdP services, RPs etc
3. **Transport between organizations**
   - Use Mobile Signature Service Roaming Mesh, ETSI TS 102 207
   - No need for direct connections between organizations (10 x 10 connections)
   - Message integrity: XML Signatures in SAML assertions

Use case: Helsinki University



Message Flow



Conclusions

- Our solution Weaknesses
  - Works with target customer groups
  - Requires Mobile operators, MSS infrastructure and PKI etc
  - There is no real WPKI infrastructure available today
  - Attribute Provider discovery is based on operator managed rules or local routing rules
- Our solution Strengths
  - It is “OK” for Finnish financial regulator
  - It is based on existing open IDM standards
  - It is public

methics

Thank You

Live demo:	http://demo.methics.fi/consentdemo
user:	consentdemo
password:	student

Jarmo Miettinen
Methics Ltd

jarmo.miettinen@methics.fi
www.methics.fi