Cross-Operator Identity Services.

Ingo.Friese@telekom.de

13. January 2012, Telekom Innovation Laboratories

Introduction.
Successful Telco Identity needs joint R&D.

- We believe that IdM is one of the most important application enabler, implementing IdM core functionalities for all services.

- The identity backbones of the Internet today are formed by Google, Facebook and other big OTT player.

- Telcos in addition could provide unique features and complementary services attached to identities (e.g. network-based authentication or dedicated identity attributes).

- Although a single Telco has a broad customer base it is too small to attain success in the identity market. A joint operator approach is necessary in order to be appealing for developers, communities and 3rd party services.

- The Wholesale Application Community (WAC) is already a joint effort of the Telco industry, but WAC has a clear focus on payment and identity enabler. There are not too many capacities for R&D and topics beyond the WAC scope.

- Furthermore there are many cross-operator IdM topics to be investigated before leveraging them to WAC.

- This Deutsche Telekom initiated R&D project "Cross-Operator Identity Services" focuses on future cross-operator IdM topics in the field of authentication, attribute exchange and trust relationships.

Introduction.
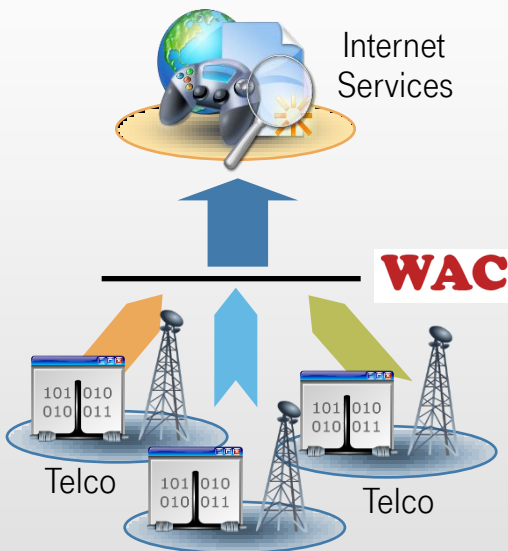## Three ways to expose a Telco asset.

Telco Originated Services
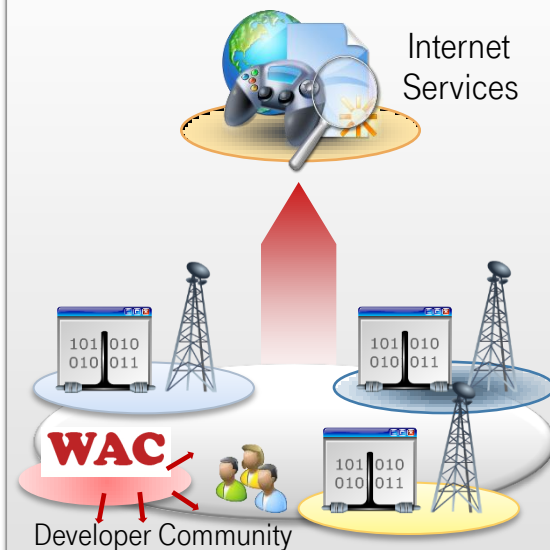
Internet Services

Telco

Telco

Telco

- Telcos offer their own assets to the Internet.
- A first approach of enabling.
- Offering for own and 3rd party services.

Centralized Telco Services

Internet Services

WAC

Telco

Telco

- Telcos offer their assets to the Internet via one common interface or platform.
- One interface broadens the customer base.

Mashed Telco Services

Internet Services

WAC

Developer Community

- Telcos provide their assets in a more scalable and standardized way. Protocols, interfaces and agreements could be handled by a "Club of Telcos" (e.g. WAC).

Cross-Operator Identity Services.
Identity Eco System – Where's the benefit?

Service Provider

Cross-Operator IdM

Users

Easy IdM Integration
Standardized solution for many Telcos

Broad potential User Base
Hundreds of millions of mobile users could be handled via one WAC interface.

Secure & Open IdM
Currently Telcos work with web standards; Telco standards (e.g. SIM-based AuthN) are more secure. Telco IdM data and processes are of higher quality due to regulation and specific business.

Convenient IdM Solution
Easier registration and login processes through user data exchange/verification; Zero/seamless login through SIM AuthN.

WAC and others

Club of Telcos (e.g. WAC)
allows for faster and easier adaption and integration of new central services and prevents policy and privacy issues.

Convenience
Easier login and registration through SIM-based AuthN / no need for login / password. Telco identity is also usable in foreign countries, networks and services.

Secure & Privacy ensured IdM
User ID and data are handled by trusted brands controlled by regulation and "Club of Telcos" (WAC) defined privacy policies.

Telco Operator(s)

Business Relevance
Customer retention, increased usage, user convenience.

Supplementary Service
Door opener for value added services like operator billing, trust services, recommendations and profiling.

Project Objectives.
Seamless and strong authentication are unique assets Telcos could bring to the Internet.

Telco Authentication

- "Zero login" authentication for web services of different carriers using SIM card over different access technologies
- Strong / 2 factor authentication (e.g. SIM + password) as a trust anchor for lost passwords etc.
- Mobile phone as universal authentication tool (e.g. for banking, IPTV etc.)

Telco Attributes

- Trusted Telco user attributes for web services in a standardized way and a harmonized semantic
- Privacy ensured way to roam user data in a Telco community

Trust Frameworks

- Defining common criteria for classifying a service / identity provider as a trustful 3rd party
- Defining / Developing an architecture to onboard 3rd party services automatically (hundreds and thousands of services)
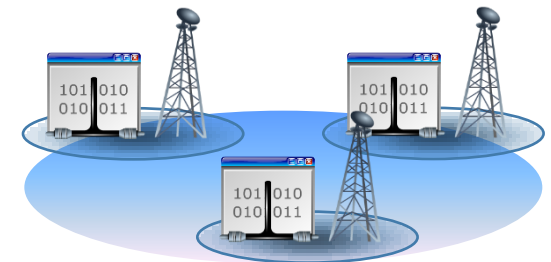
Project Objectives.
Telco Authentication.

- **Using SIM card not only for mobile network authentication**
- Promote, foster and develop "Zero login" seamless authentication for web services for different carriers using SIM card over different access technologies (e.g. cross-operator GBA)

- **SIM-based authentication could be used as an additional factor for strong authentication**
- Definition of authentication as a cross-operator service (business models with WAC)
- Definition and demo of a dedicated service for password reset based on phone number / SIM that is applicable for different Telcos

- **Mobile phone could be used as a universal authentication tool**
- Mobile phone could be used to authenticate in split device scenarios (e.g. mobile phone and set top box) for value added services and different device classes in a cross-operator context

Project Objectives.
Trusted Attributes.

- **Telcos could offer trusted user attributes to the web in a standardized way and a harmonized semantic**

- Develop a common cross-operator set of user attributes

- Investigate and develop a smart address and discover mechanism for user attributes

- **Telcos could roam identity and user attributes within the Telco community in a user-controlled and privacy ensured way**

- Develop an architecture design for cross-operator attribute transfer

- Provide a user-centric, privacy ensured exchange of user attributes

- Provide different (also lightweight) levels of "age verification"

- Provide further user attributes for validation
  (e.g. "call is originated in city xyz")

Project Objectives.
Trust Frameworks.

- **Defining common criteria for classifying a service / identity provider as a trustful 3rd party**

- How to establish a trust relationship between Telcos and service providers?

- Analyzing / adapting existing trust frameworks from Kantara Initiative and Open Identity Exchange for cross-operator use

- Defining common criteria and missing parts

- Defining / developing an architecture to onboard 3rd party services automatically (hundreds and thousands of services)

Source: OIX at http://openidentityexchange.org/what-is-a-trust-framework
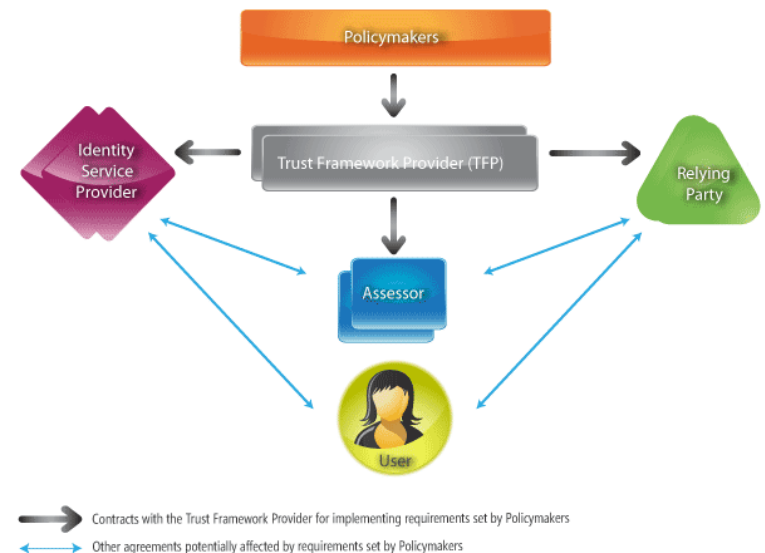
Project Scope.
R&D view to cross-operator IdM topics in the field of authentication, attribute exchange and trust relationships.

In scope

- Is an R&D project in the field of IdM, authentication, privacy ensured attribute exchange and trust relationships
- Are R&D studies, concepts, technical papers, whitepapers and proof-of-concept demos
- Are joint conference papers, input for standardization or recommendations for organizations (WAC)

Out of scope

- Is a product or service development
- Is to form a new standardization body
- Is a legal investigation

Key Questions and Key Deliverables.
Identity in a cross-operator context.

Key questions

- What is the key differentiator for Telco IdM in the Internet?
- What can be handled in the regional context of each Telco; what should be done in a cross-operator context?
- What is the optimal architectural approach for cross-operator IdM?
- How to ensure a privacy respecting and transparent exchange of Telco user attributes?
- What could a "Telco-based trust anchor service" (e.g. password reset) for Internet service provider look like?
- In 3rd party business: How to onboard 100's or 1000's services a day automatically?
- How to establish trust between Telco IdP and 100's or 1000's of service providers?

Key deliverables

- Concept of a Telco trust framework
- Technical paper for a Telco trust architecture
- Concept of a cross-operator authentication architecture (seamless authentication / strong authentication / mobile phone as a universal authentication tool)
- Concept of a cross-operator user attribute service in a privacy respecting and user-centric way
- Proof-of-concept of a "Telco-based trust anchor service"

Relevance for Cross-Operator R&D.
Join the Telco Identity R&D Community.

- Although a single Telco has a broad customer base, a cross-operator approach is necessary to be appealing for developers, communities and 3rd party services.

- Developers and 3rd party services don't want to use different interfaces for every single Telco – they look for a common API, trust relationship and deployment and business process when using Telco identity services.

- WAC was set up as a joint operational unit and several standardization bodies address Telco IdM issues with different scope and level of detail.

- These organizations don't spend much effort in R&D.

- This project intends to fill this gap as a joint cross-operator R&D project initiated by Deutsche Telekom.

Model of Procedure.
Multi-lateral R&D project.

1. Project proposal is circulated among different companies and organizations and discussed with potential project partners (additional topics may be proposed).

2. Deutsche Telekom is initiator of the project and invites to a kick off meeting in Feb/Mar 2012 in Berlin.

3. Each participating company or organization chooses one or more topics it is interested in and to which it wants to contribute.

4. Partners meet for a project preparation meeting and draw up a project organization, plan and further regulations (who wants to contribute what, how to handle IPRs, etc.)

5. Main points will be written in a multi-lateral one-time cooperation / R&D contract.

6. Project start is planned for April 2012 (pending).

Multi-lateral R&D project.
Potential Partners.

- If you are interested in participating or in case of questions please contact:

Ingo.Friese@telekom.de

- Companies and Organizations that already indicated interest:

Back up.

Thank you for your attention!