‘Identity Management in Telcos’

Jörg Heuer, Deutsche Telekom AG, Laboratories.
Munich, April 2008
Agenda.

- Introduction
- User-centric Identity and Telcos
- Comprehensive Identity Models
- IDM Reference Architecture
- Selected Concepts, Projects, Results
Introduction
TU Berlin Brings Inspired Research, Deutsche Telekom Contributes Engineering Skills and Business Experience.

“University Industry Research Center” of Deutsche Telekom and TU Berlin

1. Building excellence and reputation as a world class R&D institution in telecommunication

2. Value creation for DT by substantial contributions to the product roadmap

**Technical University Berlin**
- Scientific community
- Establishment of professorships
- Integration into TU curriculum
- Attraction of aspiring young scientists

**Deutsche Telekom AG**
- Links to customers and industry
- Funding
- Private sector management
Deutsche Telekom Laboratories’ Innovation Framework.

<table>
<thead>
<tr>
<th>Focus fields (5i)</th>
<th>Innovation guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intuitive Usability</td>
<td>Simplify your life.</td>
</tr>
<tr>
<td>Integrative Service Components</td>
<td>Always best served.</td>
</tr>
<tr>
<td>Intelligent Access</td>
<td>Always best connected.</td>
</tr>
<tr>
<td>Infrastructure Development</td>
<td>High quality at reasonable cost.</td>
</tr>
<tr>
<td>Inherent Security</td>
<td>Trusted IP networks and services.</td>
</tr>
</tbody>
</table>

Focus fields (5i) for Innovation guidelines:
- Intuitive Usability
- Integrative Service Components
- Intelligent Access
- Infrastructure Development
- Inherent Security

Innovation guidelines:
- Simplify your life.
- Always best served.
- Always best connected.
- High quality at reasonable cost.
- Trusted IP networks and services.
User-centric Identity and Telcos
User-centrism in Identity Transactions – a Taxonomy (by Paul Madsen of NTT/LAP)

**User centric**
- User interaction always required
- Identity flow always through User
- People always in the protocol

**User controlled**
- User interaction is an option, but not mandatory
- Identity flow is user controlled by means of policies
- Users have identity agents

**User consented**
- User interaction is no option
- Identity flow is controlled by authorities
- Users have consented by means of contracting (e.g. employment contract)

Source: http://connectid.blogspot.com/2006/06/protocolfor-people.html
Company centric Identity vs. User centric Identity.

**Company centric Identity**
- Identities issued by the company
- Liability is with the company

**User centric Identity**
- Identities are issued by the user itself
- Liability is with the user
Concept of Claims vs. Concept of Assertion.

User centric Identity: Claims

- Identity Issuer
- Identity Agent

- Authoritative Site

Claim (in doubt)

- Identity Consumer
- Relying Party

Claim (proven to be true)

Company centric Identity: Assertion

- Identity and Role Provider
- Trust Broker

Assertion

- Service Provider
User-centrism Transcends Beyond Identity Management.

User-centric identities cannot replace corporate-centric identity management.

- Customer data bases
- Public/ governmental registers
- Financial institutions' accounts and records
- ... even your address book...

User-centrism puts power into the hand of the user – but also liabilities.

- User-centrism can help saving users from advertisement-based harassment
- Changing service contracts on the fly is a cumbersome – and expensive undertaking
- Users can mash-up services in a user-centric way much easier
- User-centric solutions introduces new complexities to the ‘normal’ user

There is a large gap between mash-ups and ‘mess-ups’
Identities in a Telco Organization.

**User/Consumption**
- Using access
- Reading eMail
- Sending SMS
- ...

**CRM/Customer Care**
- Ordering/upgrading products
- Contract administration
- Complaints

**Resource/Delivery**
- Provisioning/creation of mailboxes
- Storage allocation

Consistent Identity handling
Our Telco Identity Reference Model.

- User-Centric
- Directories
- Federation
- E-Mail Addresses
- MSISDNs
- Network Addresses

User

Gov't

Service

Enabler

Network

Web 2.0

Service Cloud

SIM/UICC

AuthN

NGN/IMS
IDM Reference Architecture
AAA & IdM Reference Architecture – Challenges of Telcos.
AAA & IdM Reference Architecture – Essentials.

Domain centric Identity Management

Federated Identity Management

SSO, SLO, Attributes

CoT

No Interop
AAA & IdM Reference Architecture – Essentials.

Mission – Provide guidance and blueprints for seamless and overarching AAA & IdM functionalities by means of defining an AAA & IdM Reference Architecture.
AAA & IdM Reference Architecture – Concepts.
Simplified version.

User Agent (Principal)

Relying Party

Identity Provider

Authentication Enforcement

Authentication Validation

Attribute Provider

Authorization Enforcement

Authorization Decision

Accounting Provider

Charging Provider

Identity Provisioning

Identity Auditing

AAA & IdM Infrastructure
AAA & IdM Reference Architecture – Concepts.

Some selected concepts with regards to Service oriented Architectures.
AAA & IdM Reference Architecture – Concepts.

Trust: Security Tokens, Claims & Assertions

Basic Building Block of an IdM & AAA infrastructure
... can be distributed over any fixed or mobile network and interchanged between network and service layer without further requirement on security

AAA & IdM Infrastructure

Security Token Service

Security Token (Issuer)

Information (about someone)

Trust Validation

Authentication

Enforcement

Authorization

Enforcement

Decision

Accounting

Provider

Charging Provider

Identity Provisioning

Identity Auditing

Attribute Provider
Selected Concepts, Projects, Results
Microsoft CardSpace - Dimensions.

**Dimensions**

- **Cardstore**: Where is the cardstore?
  Service Providers store the information cards and facilitate the use through different devices.

- **CredentialStore**: Where are the credentials?
  Storage of credentials and engine for cryptographic operations.

- **UI Generation**: Where is the UI generated?
  The UI could be generated on a server but be displayed on one of the user’s devices.

- **Identity Selector (UI)**: Where is the UI displayed and where is the Information Card selected?

- **STS**: Where is the STS?

- **STS Authentication**: Authentication Technology

- **Browser**: On which device is the authentication needed?
CardSpace Scenario.

- **A** Relying Party
- **B** Secure Token Server
- **C** IDP Website
- **D** NFC Card Driver on PC
- **E** Tools on PC
- **F** Applet on UICC
- **G** X509 Certificate on UICC
- **H** Managed Cards backed by X509 Certificate
Technology Prototype - Identity Broker.

1. Access to protected resource
2. Redirect to Identity Provider
3. Direct to login page
4. User chooses InfoCard for authentication
5. CardSpace preselects InfoCard based on tagged information by IDP
6. User logs in using chosen InfoCard
7. Security Token transfer to LA
8. Redirect to Service Provider
9. SAML assertion
10. Access to protected resource

Diagram:
- User
- Resource
- Service Provider / Relying Party
- Identity Provider
- LA
- ID-FF
- STS
Identity and Reputation – The Building Blocks of Trust.

- In-game self-provided attributes
- External self-provided attributes
- 3rd party authority provided attributes
- 3rd party community provided perceptions

“Identity is my story about me. Reputation is your story about me.”
Phil Windley
Telcos need to solve Identity Management Issues in Many places.

- Telcos are large Enterprises too, they run operational infrastructures controlled by AAA-systems (Authentication, Authorization, Accounting), and handle customer data for Millions.

- Privacy – in contrast to ad-based players, telcos are obliged to handle personal data with extreme care. In the face of increasing amounts of unsolicited communication and unprecedented opportunities to disclose personal information in Social Networks, a crucial asset – especially in conjunction with...

- Establishing trust between consumers, prosumers, and enterprises.

- Advertisement-driven ‘feels-like-free’ business models are limited – usage-based models can help especially small sites and user-generated content. AAA, Billing, and Payment will be substantial for this.
Author’s Contact Information.

Thank You for Your Kind Attention.

Dipl.-Inform.

Jörg Heuer
E-mail: joerg.heuer@telekom.de
Phone: +49 (30) 8353 58422

Ernst-Reuter-Platz 7, 18th Floor
10587 Berlin, Germany
Web: www.telekom.de/laboratories
Fax: +49 (30) 8353 58409