2006 IDDY AWARD WINNER

# Deutsche Telekom AG, T-Com: Raising the Service Performance Bar with Federation

## Case Study:

## Deutsche Telekom AG, T-Com, dramatically improves the way services are accessed, simplifies Internet usage and reaches nearly 12 million customers with a new federated system.

IDDY winner, Michael Gaertner from Deutsche Telecom AG, T-Com, Business Unit T-Online with Liberty's George Goodman

### Project Background

T-Com launched "Netzausweis" (Net ID-Card) in 2005 to bring the benefits of federated identity management to its customers and partners. This Liberty enabled federated system provides consumers with easy, secure and privacy-respecting access to applications, services, and partners with new opportunities for reducing costs and increasing revenues. The deployment supports nearly 12 million customers and over 200 products in the telecom and Internet service provider sector in areas such as gaming, Web-hosting, IP-TV and IP-Telephony. The "Netzausweis" requires a Circle of Trust across all its partners: established in the context of the exchange of a user's personal data between the parties. Features include single log-in/sign-on, auto identification, overview, data vault, age verification and single log-out.

## Objectives

To provide consumers with easy, secure and privacy-respecting access to applications and services. To provide partners with new opportunities for reducing costs and increasing revenues.

## Bringing Identity Management to the Mass Market

With "Netzausweis" T-Com brings the concepts and ideas of identity management to its partners and customers.

**From the user's point of view this means:**

- Easy-to-use
- Transparent
- Highly secure

**From the content and service provider's point of view this means:**

- Easy implementation
- Retention of customer ownership
- Reach is extended

**From the identity provider's point of view this includes:**

- Enabling T-Com to be an Identity Provider in Germany by means of introducing the "Netzausweis" as a service and authentication product for the end customer
- Introducing innovative identity management functionalities, such as service- and division-wide single log-in and single log-out, federation of accounts, and age verification for third parties
- The "Netzausweis" shall be based upon the "Liberty Alliance Project" standard, and embed business partners of T-Com as well as third parties

## Definition of Terms

**Identity** (n) 1. the most basic element in a high value relationship 2. the individual characteristics by which a person, business, business partner, government agency or other entity is recognized or known

**Single sign-on** (n) 1. having the capability of accessing an online system once and having that authentication honored by other system entities, often service providers 2. sometimes called SSO

**Identity Provider (IdP)** (n) 1. a service that authenticates identity; often a trusted party such as a bank, mobile operator, or an

**Internet Service Provider (ISP)**
**Service Provider (SP)** (n) 1. a federation partner that provides services to an end user; service providers typically do not authenticate users but instead request authentication decisions from an identity provider

**Federation** (n) 1. an association comprising of any number of service providers or organizations 2. a model based upon trust in which user identities and security are individually managed and distributed by the service providers or member organizations 3. where the individual organization is responsible for vouching for the identity of its own users and the users are able to transparently interact with other trusted partners based on this first authentication 4. resembles the credit card model in that vendors accept an individual's ability to pay and then that ability is authenticated/verified through a single location

**Circle of Trust** (n) 1. a trusted group of identity and service providers who share linked identities and have pertinent agreements in place 2. where an individual or a business inputs a password once and minimal necessary credentials are shared among the Circle of Trust's members 3. a step strongly linked to federation, where multiple entities are involved, and there are business, policy and technical relationships in place 4. also known as "trust circle"

## The Technology

The technologies used in the deployment are based on a well-defined architecture and standards:

- The "Netzausweis" functionalities have been implemented within the existing system architecture. Within that existing architecture a separate layer encapsulates the identity management functionalities called "AAA-platform."
- Opening the IDM functionalities to different partners and their systems in distributed system environments becomes a reality through defined interfaces called "reference points."
- The implementations of the "reference points" are based on open standards—Web-services based on SOAP/XML.
- In 2005 existing authentication interfaces were extended according to the Liberty Alliance standard ID-FF 1.2 (Identity Federation Framework).

Product interoperability is important, as it is fundamental to broaden the "Netzausweis" partner community:

- Without product interoperability the reach of the "Netzausweis" partner community would be limited by technical implementation needs.
- The extension of existing authentication interfaces according to the Liberty Alliance standard ID-FF 1.2 facilitates the connection to existing IDM-environments which are also ID-FF 1.2 conformant. For instance, connecting a partner who uses Sun Access/ Identity Manager ID-FF 1.2 implementation to the Source ID-based ID-FF 1.2 implementation is NOT about complete integration, rather just configure-and-play.
- Liberty Alliance is a standard that helps T-Com's partners and itself to manage identities in distributed environments.

## Benefits to Consumers

As an IDM solution designed for consumers, the "Netzausweis" delivers various benefits to the consumers—with one primary goal: "Simplify daily Internet usage."

**From the consumer's point of view the benefits include:**

- Single Log-in, Single Sign-on and Auto Identification: A user can then easily browse a large range of Internet sites
- Overview: Meaning having the capability to view all interesting information in one place—and navigate through a "personal Internet" with fewer clicks
- Data Vault: Type in personal information only once—and distribute it as liked and needed
- Age Verification: Access age sensitive content or services registering only once and using a known system—without special software/hardware
- Login Status: View actual login status—anytime
- Secure Single Log-out: Spanning all Netzausweis sites

**The benefits could be summarized by the following statement:**
"With Netzausweis everything will be just a mouse click away."

## The ROI

The "Netzausweis" is a key business enabler:

- It allows quick and cost-efficient link-up with partners by usage of Liberty Alliance Project standards.
- It reduces the complexity of the IT-architecture, last but not least by use of modular software components.
- It allows the use of seamless services within the group Deutsche Telekom AG, the parent company of its business unit T-Online, as well as centralization of AAA-services on one single platform rather than implementing them separately within each business unit of Deutsche Telekom.

## Addressing Privacy Concerns

This project improves privacy in a number of key ways:

- The Liberty Alliance specifications enable the storage of personal data transparent to the user. In the past, a user often was not aware of all the data he submitted to his numerous accounts.
- The user is assured that his credentials are stored only with the ID provider he trusts and only provided to other providers by specified and consistent processes he can manage himself.
- Using one-off services a user does not need to reveal all his personal data as trust providers don't necessarily give away personal details in the Liberty Alliance context.

## Exceeding Deployment Objectives

By establishing an IDM-solution package (not just single sign-on/log-in) the key objectives were exceeded—bringing additional value to T-Com and its partners:

- The "Netzausweis" enables partners to lower the hurdle of utilization for their end-customer's offers.
- At the same time, traffic can be raised and costs can be reduced. Through the "Netzausweis Überblick" (Overview) the partner gets the possibility to make available specific information to its users, without the user having to directly access the services of the partner.
- Based on a completed authentication solution, services can be used even better seamlessly and be connected with each other.

## Protection Against Identity Theft

Protection against identity theft also improves with the new capabilities:

- The IDM based on Liberty Alliance makes it easier for the user to manage and use his credentials, most of which are either insecure and easy to hack, or cryptic and easy to forget.

- The problem of remembering different passwords has been addressed by only needing one set of credentials per customer. Therefore fewer identities and passwords will be written down. The danger of the passwords being compromised is therefore reduced.
- A consistent level of security, especially with the transmission of credentials, is implemented as the interfaces to the Liberty Alliance components are specified in detail and have to be considered by each and every application. In the past, many customers used the same password for different applications, so if one of them was compromised in a certain way due to weak security implementation of one application, the others were in danger as well.

## ABOUT THE LIBERTY ALLIANCE

Liberty Alliance is a global alliance of companies, non-profit and government organizations developing open standards for federated network identity, interoperable strong authentication and Web services. Liberty Federation and Liberty Web Services provide consumers and organizations with a more convenient, privacy respecting and secure way to control online identity information. The Liberty Alliance management board currently consists of representatives from AOL, Ericsson, Fidelity Investments, France Telecom, General Motors, HP, IBM, Intel, Novell, NTT, Oracle, RSA Security and Sun Microsystems. Membership in Liberty Alliance is open to all commercial and non-commercial organizations. A full list of members, as well as information about how to become a member, is available at www.projectliberty.org /membership.