

Case Study:

Deutsche Telekom Lowers Implementation Barriers for Online IP Based Services

The Organization

Deutsche Telekom AG offers millions of private and corporate customers all over the world the entire spectrum of modern information technology and telecommunications services – whether fixed-network, wireless and broadband or complex IT and telecommunications (ICT) solutions for business customers.

There are three customer brands under the global umbrella brand “T”: T-Home for all products and services at home; T-Mobile for products and services while on the go; and the brand T-Systems offers medium to large-sized customers ICT solutions around the world. Deutsche Telekom AG is represented in about 50 countries around the globe. More than half of the revenue from the first half-year of 2007 was generated outside Germany.

Key Objectives

Deutsche Telekom AG sought to build on its existing strengths as an identity provider by lowering the implementation barriers for the delivery of online/IP-based services. In this case, the primary implementation barrier was due to the fact that different services used different standards and protocols. So Deutsche Telekom decided to develop a solution that supports a range of protocols.

Wins Second IDDY Award



Netzausweis was so innovative it won 2006 IDDY Award. The IDDY Award recognizes digital identity deployments and up-and-coming identity-enabled enterprise, social networking and Web 2.0 applications that incorporate identity specifications and policy frameworks from Liberty Alliance. The enhanced multi-protocol solution was then awarded a 2008 IDDY as well.

“The IDDY Awards showcases some of the best digital identity management solutions in the global marketplace today, ” said Brett McDowell, executive director of the Liberty Alliance.

“Deutsche Telekom is unique in being the only organization to date to be honored twice. Their new solution is significant to the market because it supports multiple protocols and this represents where the industry must go.”

Deployment Background

To best understand Deutsche Telekom AG's new work, it's necessary to go back a few years. In 2005, Deutsche Telekom AG launched what is called in German "Netzausweis" or Net ID-Card. Net ID-Card is a Liberty-enabled federated system that provides consumers with easy, secure and privacy-respecting access to applications, services, and partners.

The solution has been steadily enhanced to offer new multi-protocol capabilities for service provider interfaces as well as for authentication methods and automatic user identification.

Netzausweis was so innovative it won 2006 IDNY Award. The IDNY Award recognizes digital identity deployments and up-and-coming identity-enabled enterprise, social networking and Web 2.0 applications that incorporate identity specifications and policy frameworks from Liberty Alliance. The enhanced multi-protocol solution was then awarded a 2008 IDNY as well.

"The IDNY Awards showcase some of the best digital identity management solutions in the global marketplace today," said Brett McDowell, executive director of the Liberty Alliance. "Deutsche Telekom is unique in being the only organization to date to be honored twice. "Their new solution is significant to the market because it supports multiple protocols, opening the solution up to new customers and partners."

Business Impact

In practice, the application is designed to serve mass market requirements for online/IP-based consumer applications by providing fundamental functionalities such as Single Login, Automatic Identification, Single Sign On and Single Logout. Today it supports more than 15 million consumers using various applications across multiple devices. (e.g. PC, mobile phone, handheld, TV set top-box).

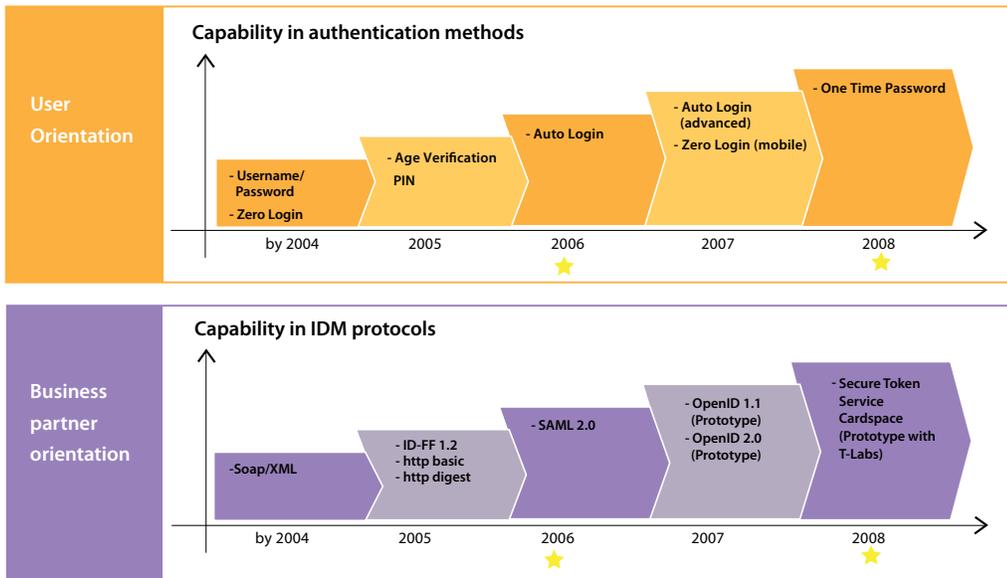
The impact of the multi-protocol capability is significant both for businesses and consumers. On the business side, the application ensures easy implementation of consumer services and shortens the time-to-market for new service offerings. It allows quick and cost-efficient link-up with partners using the identity standard protocol that fits best and reduces the complexity of the IT-architecture.

"Time to market is very important and we want identity to be an opportunity not an obstacle," explained Michael Gärtner, senior expert at Deutsche Telekom AG, Products and Innovation. "When marketing has a new idea or service that has to be implemented quickly by means of IP services, it's important that we can use existing frameworks and don't keep recreating solutions."

From the consumer perspective, the application also provides a unique and consistent user-interface that is easy-to-use, transparent and secure.

"With this capability, we can tie in applications and services delivered from different partners using different protocols," said Gärtner. "This way the user can use these services with one password and one login. The identity management experience is seamless and simplified."

IDENTITY MANAGEMENT CAPABILITY EVOLUTION



IDDY AWARDS

★
2006: Netzausweis was awarded for IDM deployment

★
2008: Identity application was awarded for its multi-protocol support.

How It Works: Multi-Protocol Support

So how does the multi-protocol support work? The application’s multi-protocol support means that Deutsche Telekom AG acts as an Identity Provider and can tie a broad variety of online/IP-based consumer services together by means of a common identity management (IDM) experience. Specifically, the application supports the following protocols:

- SOAP/XML (own protocol suite)
- Secure Token Service (own protocol suite)
- ID-FF 1.2
- SAML 2.0
- HTTP Basic
- HTTP Digest

In addition, the application and its underlying architectural guidelines make it possible to integrate further IDM protocols very easily. The latest enhancements provide support of the following protocols for demonstration purposes:

- OpenID 1.1
- OpenID 2.0
- Microsoft CardSpace

Multi-Protocol support also extends to authentication methods/automatic user identification. The application lowers the usage barriers by providing scenario-focused login methods and supports different authentication methods, also combining methods from different protocol layers (e.g. network layer).

In other words, when a consumer wants to access a service, the identity application simply chooses the authentication method that fits the current user-scenario best and also takes the security requirements of the service into account.

The Technology

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

- The functionalities have been implemented within the existing overall architecture. A separate layer encapsulates the Identity Management-functionalities: the so-called "AAA-domain".
- Opening the IDM-functionalities to different implementation partners in distributed system environments becomes reality through well-defined interfaces or "reference points".
- The implementations of these "reference points" are based on open standards, like SOAP/XML, ID-FF 1.2, SAML 2.0, etc.

The solution also leverages Open Source technologies:

- Standard LAMP (Linux, Apache, MySQL, PHP / Java) technologies.
- SourceID 2.0 (for ID-FF 1.2 protocol)
- OpenSAML 2.0 C++ (for SAML 2.0 protocol)
- SXIP OpenID4Java (for OpenID 1.1/2.0 protocol)

"Having the highest degree of interoperability was critically important to maximize reach", said Jochen Hiller, senior expert at Deutsche Telekom AG, Products and Innovation. "Without product interoperability, the reach of IDM solution would be limited, as the implementation partners for the online/IP-based services are using very heterogeneous technologies," he explained. "At the same time, the support of standard IDM protocols facilitates the connection to existing IDM-environments, which are also standard-compliant."

Addressing Identity Theft and Privacy

The application makes it easier for the Deutsche Telekom AG customer to manage and use his credentials. With this solution, customers have one set of credentials. That's it. This means the need to write down all sorts of logins and password data is eliminated.

In addition, a standard-based implementation makes the handling of personal data more transparent. In the past a user often would not be aware of all the data he submitted to his numerous accounts. Now, the consumer is assured that his credentials are stored only with the Identity Provider and only provided to other entities by specified and consistent processes that are transparent to him.



IDDY Award-Winning Deployment

User Orientation

Authentication Methods

- Username / Password
- Zero Login (fixed-line network)
- Zero Login (mobile network)
- Auto Login (persistent cookie)
- Auto Login (persistent cookie + network access)
- Age Verification PIN
- One Time Password

I want services everywhere. I want to access them easily and secure when i need it.

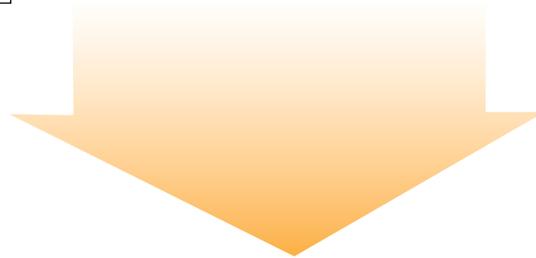
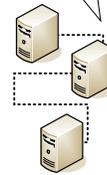


I offer an Online IP-based service. I want to choose the IDM protocol that I like most."

Business partner orientation

IDM protocols

- SOAP/XML
- ID-FF 1.2
- SAML 2.0
- http basic/digest
- Secure Token Service
- OpenID 1.1/2.0 (Prototype)
- Cardspace (Prototype)



Flexibility in highest user experience in IDM

Flexibility in providing wide range of protocols & methods

User benefits: Use a broad scope of internet and mobile applications with the same login and single sign on. No unnecessary login dialogs. Usage barriers vanish.

Business partner benefits: Easy integration and connection based on favourite partner technology. Partner automatically benefits from client scenario best fitting login mechanisms - respecting the security demand level of the partner service.

Looking at the ROI

Because the application is a key business enabler for offering online/IP-based services to the consumers of Deutsche Telekom AG it enables the following:

- Quick and cost-efficient link-up with partners using the IDM standard protocol that fits best
- Reduction in the complexity of the IT-architecture through the use of modular software components
- The use of seamless services based on one single IDM platform rather than implementing them separately within consumer services offered by Deutsche Telekom AG

Innovation and Liberty Alliance Support

At Deutsche Telekom AG, the R&D department (T-Labs) devotes considerable time to studying all the different IDM protocols and authentication protocols. Jörg Heuer, Senior Manager Identity and AAA at T-Labs, says that one of the benefits of being a Liberty Alliance member is having the opportunity to take part in meetings and planning sessions in which new architectural issues are introduced and discussed.

Heuer also points to Liberty's support and interest in identity initiatives like the Concordia Program, an open community initiative designed as an umbrella initiative to drive harmonization and interoperability of identity specifications and protocols.

"Liberty's support of Concordia shows that Liberty is not isolated in its own protocol world, but instead is looking at ways to create a platform of the future." said Heuer.

Benefits to Enterprises and Organizations

From Deutsche Telekom's point of view as an IDM provider for its consumer online/IP-based services—the application ensures:

- Easy implementation in online/IP-based consumer services
- Lowering the usage barriers of the consumers, anshortening the time-to-market for new service offerings

Benefits to consumers/users

From the consumer's point of view the application provides through its unique user-interface a consistent IDM solution, which is

- easy-to-use
- transparent
- secure

This solution was honored with a multi-protocol IDNY for several reasons.

From the customer's/consumer's point of view:

- The application enables Internet users to use a Single sign on across several platforms and applications.
- It lowers the usage barriers to a minimum and facilitates the daily usage of online/IP-based services of Deutsche Telekom AG significantly.

From the online/IP-based service implementation partner's (Service Provider's) point of view:

- Connection of IT-systems could happen quickly and cost-efficiently on the basis of standardized protocols.
- Long time gained experience in many realized partner implementations for a broad variety of online/IP-based-service offering.

"It's important to implement protocols that have a certain kind of reach or that may achieve a certain level of reach because we are talking about attaching different services, and it doesn't make sense that we implement IDM protocols which no one else in the world would implement. That's why the Liberty Alliance community is so valuable. It's a great framework to exchange ideas on identity management with other organizations."

**-Michael Gärtner
Senior Expert
Deutsche Telekom AG,
Products and Innovation**

From the identity provider's (Deutsche Telekom AG) point of view:

- The application is a mass-market capable IDM solution—by means of using of the most modern technologies.
- The application enables Deutsche Telekom AG to offer new online/IP-based services to its consumers in a shortened time-to-market.
- The application enables Deutsche Telekom AG to integrate new protocols and further authentication methods in a short timeframe, relying on Open-Source developments picked as useful.

From the standardization (Liberty Alliance Project) point of view:

- The application supports the Liberty Alliance IDM protocols ID-FF 1.2 and SAML 2.0 and makes them interact with different authentication methods and other IDM standards.
- By demonstrating the interaction with online/IP-based services implemented by user-centric protocols (OpenID and Microsoft-CardSpace in a demonstration implementation) the application shows how these different IDM approaches could be linked together to provide the consumer a consistent IDM user experience.
- It builds on an award-winning solution and takes it to the next level.

About Liberty Alliance

Liberty Alliance is the only global identity community with a membership base that includes technology vendors, consumer service providers and educational and government organizations working together to build a more trust-worthy Internet by addressing the technology, policy and privacy aspects of digital identity management. Liberty Alliance is also the only identity organization with a history of testing vendor products for true interoperability of identity specifications. Nearly 80 products and identity solutions from vendors around the world have now passed Liberty Interoperable™ testing. Liberty Alliance works with identity organizations worldwide to ensure all voices are included in the global identity discussion and regularly holds and participates in public events designed to advance the harmonization and interoperability of CardSpace, Liberty SAML 2.0 Federation, Liberty Web Services, OpenID and WS-* specifications. More information about Liberty Alliance as well as information about how to join many of its public groups and mail lists is available at www.projectliberty.org.