Distributed Identity Management

The intention of Distributed Identity Management is the advancement of the electronic communication infrastructure in justice with the goal of defining open, interoperable and internationally standardized interfaces for the participants. It allows secure access to communication services as well as secure and reliable electronic communication.

The D.I.M. concept aims at defining standards for secure registration, authentication and authorization for the use of E-Justice communication applications and also for secure access to the communication participants personal data.

- D.I.M. is designed to provide a highly scalable and distributed solution to registration for any e-Justice user.
- D.I.M. is based on modern web service standards and can therefore function as an identification service both for any specialised procedure and for purely information services on the Internet.
- D.I.M. administers and distributes identity attributes and roles in a trust domain.
- Subject to all checks, D.I.M. should be able to cope with the full range of data protection demands since in the D.I.M. context signature certificates and current encryption procedures have to be used every time data are consulted.
- D.I.M. gives the registered user a convenient single sign-on for all linked e-Justice and e-Government services with a trusted identity provider.
- A number of identity providers form a circle of trust based on contractual arrangements.
- D.I.M. allows different authentication procedures, from simple e-mail confirmation to electronic ID.

Functional requirements

The main goals of D.I.M. are to provide an open and highly scalable architecture for Federated Identity Management in E-Justice and E-Government.

To increase the reusability of the components of a D.I.M.-based E-Justice application D.I.M. is consequently built on open international standards from the field of Identity-Management. These were profiled to meet the needs of E-Government and E-Justice applications. D.I.M. only defines interfaces and the modular architecture. The design of the individual components is left to the developer. In particular D.I.M. supports platform independence of the interoperating components. It is absolutely possible to develop single components using the .NET-technology while developing other parts with JAVA. D.I.M. can achieve interoperability of different Identity-Management scenarios and enables identity federation. The identities of all D.I.M.-based E-Government applications are stored using a common scheme. It is thereby possible to interpret and accept iden-
entities from other applications. Federated Identity-Management makes Single-Sign-On possible. This means that a user has the possibility to register only once to a trusted site and uses this identity to apply for different D.I.M.-based services.

The main goal of the D.I.M.-concept is the registration and usage of identities from a rich client application, because these were the concrete requirements for the E-Justice communication scenario. The concept also contains a sketch of how to use the D.I.M.-based identities for a web-based browser scenario.

**Standards**

Currently there are two competing international standards in the field of digital identity management, SAML 2.0/Liberty Alliance and WS-Trust/WS-Federation. So far it is unknown, which of the two standard families will have greater acceptance in the future. D.I:M. is based on the WS-Trust/WS-Federation standards family and therefore is able to use main parts of the very established WS-* standards family for Web-Service interoperability. On the other hand D.I:M. is designed in a way that it is possible for the architectural components of D.I:M. in a future version to also support SAML/Liberty Alliance. This would turn D.I:M. into a so called “Identity Metasystem”.
D.I.M. Showcase

To show the core concepts of D.I.M. and to prototype an early realisation a showcase application was developed. This showcase implements parts of the D.I.M. concept exemplarily and shows concrete application scenarios. The showcase application consists of two parts:

1. The first part shows browser based access to the German business register as a federated Single-Sign-On scenario. It is thus an outlook on possibilities for a different specialisation of the D.I.M. core concept from document [1].

2. The second part shows an authentication to a web-service using a software certificate. By the included role-attribute the service is able to set the user rights. This scenario in parts already implements the E-Justice communication scenario that is specified in document [2].

It is maybe interesting that a user who is registered at a trustworthy home organisation and has his certificate as well as his username and password information stored there could use both services without registering twice. He could use the web-based business register service as well as take part in an E-Justice communication. This is not implemented in the showcase but would be possible if both services were implemented D.I.M.-based.

1.1 Showcase Part 1

1.1.1 Explanation

In this part of the showcase a web-based “German Commercial Registry Information” service is simulated. This service is provided by the justice portal of the federal ministry of justice. To use the service a user has to sign on with a username and password. The Federal Justice Portal is supporting a user registration according to the D.I.M.-concept. Thus it is possible to register at the German Federal Justice Portal in order to apply for service usage.

In addition to the German Federal Justice Portal there are Justice Portals of the ‘Länder’, which might offer their own services and also their own user registration according to the D.I.M.-concept. To make up a federation the state portals have to support a trust relationship to the Federal Justice Portal. They then form a so-called “circle of trust”.

A lawyer, who e.g. is from Bremen, can decide if he wants to register as a user of the Federal Justice Portal or as a user of the Bremen Justice Portal, supplied by the state of Bremen. If these two Portals support a trust relationship according to the D.I.M.-concept (as shown below), a registration at either of the portals is enables the lawyer to access services published at the Federal Justice Portal as well as services published at the Bremen Justice Portal.

The message flow is the following. The user tries to access the service „Commercial Registry Information“. Because the service is unable to authenticate the user it determines the users Home-Portal, where he is registered, and redirects the user there for login. The user logs onto his Home-Portal and is again automatically redirected to the service.

It could be of interest that the user login and authentication is performed by an Identity-Management standard architectural component called „Identity-Provider“, which is fur-
ther specified in the D.I.M. concept. The called service is able to authorise users and define their access rights without knowing the users personal identity. The users identity is verified and assured by the Identity-Provider; the user registration is no longer part of the service. In this showcase each user Home-Portal is hosting an Identity-Provider. Thus two identity providers exist, one at the Bremen Justice Portal and one at the Federal Justice Portal.

Because the service call then contains authentication information the user is able to use the service. The authentication information was created by the Home-Portal and was attached to the service call.

1.1.2 Sequence of the Showcase

1. A lawyer from Bremen wants to query the “Commercial Registry Information” service and calls the Federal Justice Portal, because the service is available there for registered users.
2. By choosing "Online-Services" the lawyer indicates that he wants to call a service that requires registration. Because the Federal Justice Portal supports a federation with the state portals and approves users registered there, the lawyer is asked for his Home-Portal, where his online-identity is stored.
3. If the lawyer is registered at the Federal Justice Portal he is redirected to its login-page to provide his login information.

If the lawyer is registered in Bremen, he is redirected to the Bremen Justice Portal for login. The login-page in this case is physically hosted on the Bremen Justice Portal server and supports federation with the Federal Justice Portal. This is made obvious by the page design, which is using the style of the Bremen Justice Portal.

A similar scenario would be possible for EU-services.
4. The lawyer is then automatically redirected to the web-page of the Federal Justice Portal, where the services obligatory for registration are hosted.

5. There he is able to call the „Commercial Registry Information“-Service.

The D.I.M.-concept makes it possible to use services from all state portals and the federal portal with a single registration at one of the portals. D.I.M. is designed very open and allows the portals to...

1. specify their own processes for registration and authentication. It would be possible that e.g. the Schleswig-Holstein Justice Portal demands a certificate instead of username / password for registration.

2. specify their own authorisation policies for users in federated portals. It is possible that e.g. the Schleswig-Holstein Justice Portal offers three services which can be accessed by users from an arbitrary federated portal. For two of them a username / password authentication is enough while the third requires higher
security. The user has to authenticate himself with a certificate and the associated PIN.

3. specify necessary attributes that have to be provided for a service usage. This could be e.g. a role “Lawyer” or a credit card number. This is possible because all Partners in a D.I.M.-Federation have the same understanding of attribute semantics.

These possibilities were not modelled in the showcase.

1.2 Showcase Part 2

1.2.1 Explanation

In this second part of the showcase the access to an E-Justice communication infrastructure from a JAVA-rich-client application is shown. The user authenticates to the communication service with his certificate which was supplied by the operator of the D.I.M. registration infrastructure. The implemented service is the address-book-service specified in D.I.M. document [2]. This service returns a list of users registered for E-Justice communication. In a real communication scenario the user could choose the recipient of a message from that list.

The user registration and authentication is again performed by an Identity-Provider. This Identity-Provider has different communication interfaces compared to the one from part 1 of the showcase, because it has to communicate with a rich client application. In a federation scenario it would be enough for a user to register at only one of the Identity-Providers to access the different federated services, no matter if these are web-services or browser-based services. This was not implemented for this showcase; the Identity Providers of the two showcase parts are different components.

A minimal fully functional Identity-Provider was implemented for this part 2 the showcase. This Identity-Provider operates invisible for the user.

The user provides his personal certificate to the Identity-Provider for authentication. From this user certificate the identity-Provider knows the users identity and role. The Identity-Provider supplies this information to the address-book service the user is calling. Depending on the users role the service allows different views on the data. A normal citizen is only able to see address information of courts and ministries while a ministry user can see the whole list of registered users.

The following communication is taking place:
1. The user authenticates at the Identity-Provider using his personal certificate.

2. The Identity-Provider creates a signed document which confirms the correct registration of the user and contains additional attributes as name and role.

3. With this document the user is able to use the service.

4. The service returns the requested data according to the user role.

During this communication an encrypted channel between user and service is established enabling confidential communication between the partners.

1.2.2 Sequence of the Showcase

1. Initially the user chooses his personal certificate from a certificate store. With this certificate he authenticates at an Identity-Provider running in the background. The Identity-Provider checks the certificate and reads name and role from his user database to confirm these, together with the user identity, to the service. The identity confirmation is passed on to the service by the user.
2. By knowing the role that was confirmed by the Identity-Provider the called service can determine the access rights of the user. In the shown example the user is registered as “Amtsgericht Coburg” in the role “court” and is able to search the users database without any restrictions.