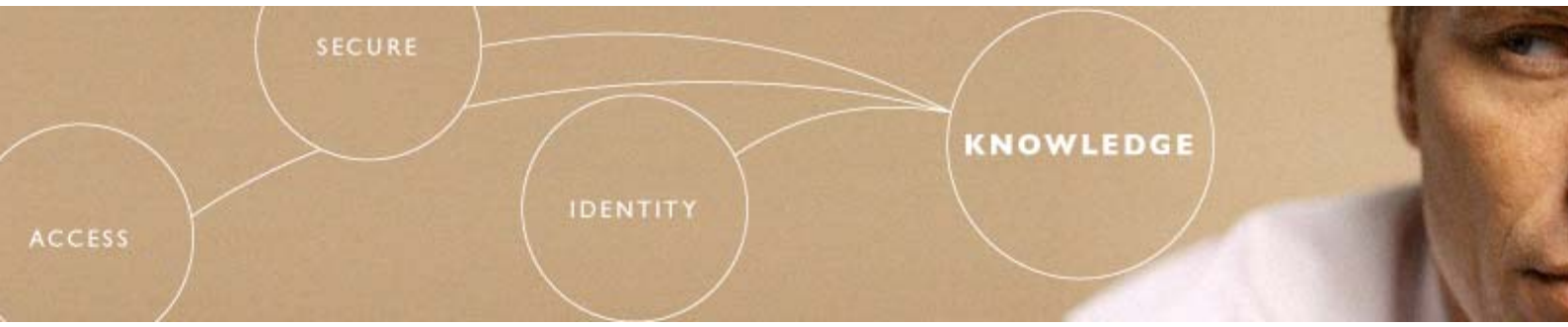
everett.
TRUSTED TO KNOW




# Federated Identity

## enabling the service chain

Thomas van Vooren, Everett

Whitepaper

# Federated Identity

## enabling the service chain

Author: Thomas van Vooren
Editor: Peter Valkenburg

# Contents

# 1 Introduction

In today's business world, enabling integrated access to services across business domains for clients, suppliers and partners has increasingly become a critical factor for success. The adoption of federated identity is the key to establishing a cost-effective and security and privacy aware solution for integrated service in the supply chain.

Today, most organisations have implemented – or are currently working on the deployment of – internally focused identity and access management solutions. These solutions may vary from streamlining account provisioning processes up to the enablement of centrally governed access control to (web based) applications for employees.

As these solutions are internally focused, organisations hold their own user data along with the management of access the user is privileged to. Once access to services across business domains comes in to play, this traditional identity silo approach inhibits access to users for an integrated service offering.

Federated identity provides the means to step away from this identity silo approach. It does so by introducing concepts and solutions to simplify transporting identity related information across organisational boundaries, addressing management, security and privacy concerns as an integral part of any federated solution.

The federation landscape contains many different concepts and related initiatives and solutions. This paper introduces these federative concepts and initiatives and provides an approach for organisations to get started with federated solutions. As such, this paper is intended for program managers, project manager and business and IT architects alike.

In the next chapter, the paper starts with outlining the business case for federated identity. The following chapter describes the federation architecture, introducing several key concepts and components. These are subsequently used in chapter four on the available technology enabling federative solutions. After two real life cases are presented, chapter six provides an approach on how to get started with federated identity. This paper ends with answers to seven frequently asked questions about identity federation.

# 2 The case for federated identity

Integration throughout the service chain raises certain challenges. What these are and how federated identity addresses these challenges is explained in this chapter.

## 2.1 The cooperative business model

Enabling integrated access to services across business domains for clients, suppliers and partners has increasingly become a critical factor for success. For instance, this is the case in the financial industry where banking institutions partner with pension funds and insurance firms. Also in other segments of the market such as higher education and manufacturing new business development is increasingly dominated by cooperation and collaboration.

The figure below depicts a simplified business process in which a customer from a bank is interested in buying travel insurance. In this example, the bank offers a variety of insurance packages through a number of insurance partners. Recently, the bank has teamed with a new insurance company to offer travel insurances.

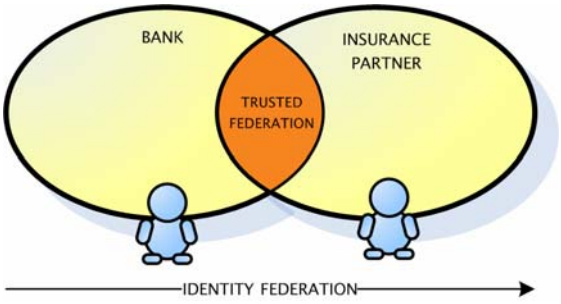



*Figure 1, Business process and federation*

In this scenario, the collaboration between the bank and insurance company intends to leverage the insurer's existing service offering while still maintaining the banks identity through corporate branding.

Note that the scenario does not necessarily imply the bank and insurer belong to different legal entities. It can also apply to organisations collaborating as a result of a mergers or acquisitions where federated identity is a model for (identity) integration through the disparate IT systems.

In any case, this scenario requires the service to be delivered quickly and cost efficient while still providing a coherent user experience. The realisation of such a requirement is faced with several challenges, to which federated identity management is key. The next paragraph discusses these challenges and how federated identity is involved.

## 2.2 Challenges

Organisations developing and marketing service chain integration will be faced with a series of challenges. These challenges are to provide the right *user experience* as the business enabler with *efficiency and time to service* as a prerequisite while maintaining respect for *legal and privacy* concerns.

- **User experience**

  On the Internet, patience is not one of your customer's virtues. Research has shown that on average an internet broadband user waits only 4 seconds for a service to load after which he will move on. This behavioural property is joined with one of any user's great annoyances – the requirement to enter identity data over and over again. This user acceptance threshold is something which will determine the appreciation of the quality of service and thus the service's success. Ensuring a common understanding of the user throughout the service chain is key to establishing a seamless user experience. This requires a trust model in which business domains or organisations throughout the chain rely on statements about users issued by one of its partners so that a user is only required to identify himself once.

- **Efficiency and time to service**

  Product or service innovation is increasingly undertaken in partnership where the strengths of individual service providers are combined into new services or the existing services improved through an integral user experience of the service chain (also see the paragraph on user experience). Linking services from different business domains together requires the services throughout the chain to share the same understanding about the customer, varying from the type of services it is requesting throughout the chain up to the information required to process transactions such as credit limits or simply a username.

  End users are becoming more demanding each day, including pressure on the timely delivery of services. Previously, new and dedicated solutions were put in place to enable multiple services from various organisations to be grouped into a new service in order to offer a cohesive user experience. Part of these solutions was the traditional identity silo approach in order to establish a common understanding of the user. Today, federated identity provides the means for standards based exchange of user information enabling federated single-sign-on between services through the chain.

  The challenge is to agree upon the mechanisms required that prevent one off integration for a particular service chain or partnership within a particular business domain. In order to be efficient, a federated identity model must be put in place which can be leveraged time and time again.

- **Legal and privacy**

  Enabling integration of services throughout a service chain raises several legal implications. In the example of the bank and insurance company in the previous paragraph, the responsibility for access to the insurance company's services may be ambiguous as it relies on the bank to provide the necessary user details. Federated identity solves these types of legal aspects through various enabling technologies available allowing for the appropriate mechanisms on security and privacy to be implemented. This is most apparent in the various mechanisms that exist in the standards and specifications put forward in the next chapter on how the exchange of identity information is handled.

  Additionally, establishing a common understanding of the user's identity across services is required in order to offer a coherent user experience and enable for instance single-sign-on and personalised services. This however requires the exchange of identity data that in most cases is subject to government privacy regulations or internal policies. Federated identity in general is aware to these types of privacy issues and many federation technologies and solutions support various mechanisms to address these issues. These mechanisms vary from anonymising user identifiers to explicit requests for the user's consent in the dialogue with the service.

These challenges – whether it is the capability to efficiently integrate services throughout the chain or doing so while maintaining security and ensuring privacy – all revolve around one thing: an architecture for identity federation.

## 2.3 User centric services

User centric services or Identity 2.0 is the term often used to indicate (federated) identity initiatives where the scenarios or use cases place the end user as the entity in charge when selecting the identity provider to handle authentication or manage subsequent attribute releases when accessing a specific service.

This implies that with federated identity initiatives, a distinction between two main types of control on identity based decisions exists: organisation driven federation and user driven federation. Organisation driven federation is the process where the organisation dictates the available federative process by restricting the available identity providers whereas with user driven federation the end user himself decides on how to identify and release his digital identity.

Even though both types of control are complementary to each other, this paper focuses on organisation driven federation.

# 3 Federation Architecture

Typically, two main topologies can be adopted in which federation members can enable service chain integration with identity federation. Prior to describing these topologies in the second paragraph, a number of key concepts are addressed in the first paragraph, essential to understanding the federation architecture put forward in this chapter and the client cases and enabling technology in subsequent chapters.

## 3.1 Key concepts

- **Federated identity and access management**

  The concept of identity and access management refers to all processes and underlying technology for the creation, life cycle management and application of digital identity data. In the context of this paper, *federated* identity (and access) management are all processes and underlying technology which make it possible to exchange identity data *across organisational boundaries* in a *secure* and *controlled* manner.

  The life cycle management of users consists of all processes and enabling technology for the creation, enrichment, management and use of digital identity data. Digital identity data often has a scope of – but is not limited to – the following types of use:

  - ✓ Authentication: is the user really who he says he is. A user identifying himself is only trusted after he has 'proven' his identity.
  - ✓ Authorisation: is the user entitled to accessing a requested resource. For instance, is this user a premium subscriber or does he only receive the base service offering?
  - ✓ Personalisation: how can the service offering be targeted based on user specifics such as parent organisation, job title in the case of business-to-employee environments or personal interests in the case of business-to-consumer.

- **Federated single-sign-on**

  Single-sign-on (SSO) is the process where a user gains access to a set of services during a session after a single successful authentication. The expanded term Enterprise-SSO is often used to indicate SSO of a corporate user for services within the boundaries of his own organisation.

  A related term is single-log-on (SLO) referring to the existence of a single username and password. SLO is often prerequisite to SSO within a single organisation, if not possible otherwise due to for instance other attribute exchange mechanisms or identity abstraction.

SSO across organisational boundaries is where federated SSO comes into play. It is obvious the implementation of SSO across organisational boundaries with the prerequisite of a SLO is not feasible. Inhibited by local security policies or external regulation and legislation such as various privacy acts, SSO across organisational boundaries brings new challenges to the table and thus becomes the domain of federation.

- **Federated provisioning**

Provisioning is the process of automatically managing digital identity attributes, login accounts and credentials throughout the lifecycle of a subject's relationship with the organisation. An example is the well known hire-fire scenario in which a user obtains all his (network) accounts automatically after registration in the personnel system on hire and automatic revocation of these accounts upon contract termination.

Services tied into federation scenarios often depend on the existence of accounts or user profiles in the underlying applications or systems. As integration of provisioning systems across organisations is not feasible (span of control), federated provisioning is required to solve this provisioning challenge. It does so by combining data exchange protocols (thus avoiding integration issues on interface level) with privacy aware attribute release scenarios common to federation architectures.

## 3.2 Federation components

- **Identity provider**

An identity provider (IDP) is typically the service or organisation in a federation scenario that is responsible for the authentication of a user's identity for locally integrated services as well as services owned and controlled by external parties. Based on this role, the IDP is entitled to issue statements (often referred to as *assertions*) about the user's identity (who), in which context the authentication has taken place (authentication), what the user is allowed to (authorisation) and what else is know about the user (attributes for personalisation).

An example of an identity provider may be a bank portal that holds identity data on users and performs the authentication of users on behalf of a service offered by one of its insurance partners.

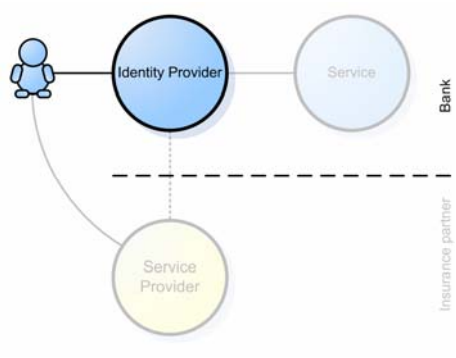



*Figure 2, Identity provider*

Technically, the identity provider is the entity responsible for the authentication of a user's identity on others behalf. On a more logical level however, the identity provider is the *organisation* holding the identity data. In addition, this organisation may also offer services to internal and external users and therefore equally well qualifies as a service provider (see next paragraph)[1].

- Service provider

A service provider is a specific service offered to users that relies on an identity provider for the authentication, authorisation (or authorisation properties) and attribute retrieval on its behalf.

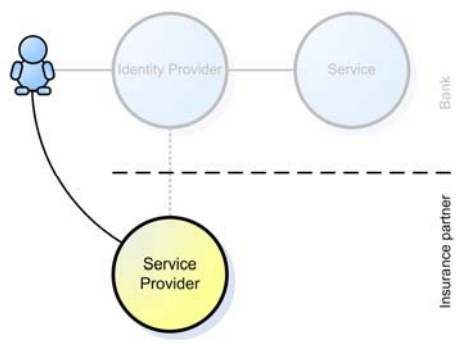



*Figure 3, Service provider*

Technically, the service provider is the entity providing the service based on underlying applications or systems. On a more logical level however, the service provider is the *organisation* as a whole offering one or more services to users. This organisation may also act as – or contain – an identity provider for the authentication of its own users to internal or external services (see previous paragraph) or those of other (service) partners.

[1] Sometimes the term identity provider is also referred to as the *authentication authority* or *source site* (origin of the user). Lately, the term source site is used less frequently as the origin of a user in federation scenarios is potentially more ambiguous.

- **Identity selector**

Identity selectors are used in scenarios or use cases where the end user is in control when selecting the appropriate identity provider to meet the requirement for identity imposed by the service provider. These requirements are in most cases about the release of attributes required to provide the service.

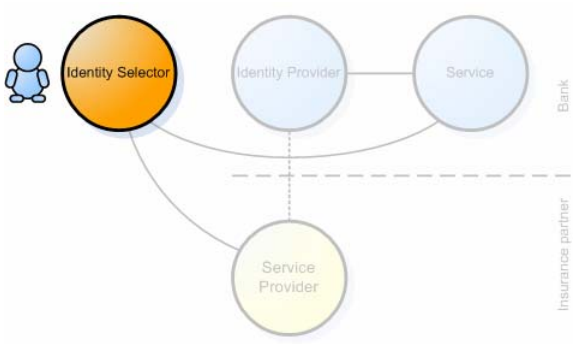



*Figure 4, Identity selector*

Although leaving the choice of identity provider to the user is significantly different from organisation driven federation, both put the users identity at the core of their concepts and both address user control and privacy with equal importance although be it in different manners.

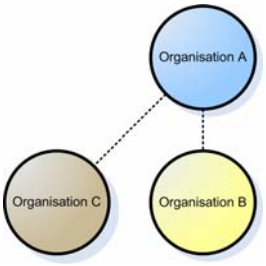
So how does 'Identity 2.0' fit in to a federated architecture? Bottom line is that this depends on the prerequisites imposed on identity providers and the required trust by the service providers in the service chain. While in some scenarios service providers may be comfortable to rely on identity information asserted by user selected identity providers – usually in low security scenarios such as blog access – in other more high security scenarios, the service providers may want to be in charge when it comes down the identity provider selection. This is for instance the case in the banking and insurance examples included throughout this whitepaper.

Both offer unique possibilities and will coexist or even complement each other in some federation scenarios. For completeness, chapter four on enabling technology provides an overview of the most important identity selector solutions; information cards and URL based identity.

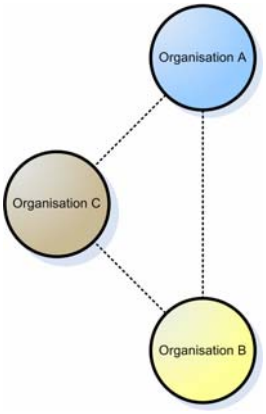
### 3.3 Federation topologies

Once a role as an identity or service provider (or both) is established, several topologies exist in which organisations can decide to participate in a federation.

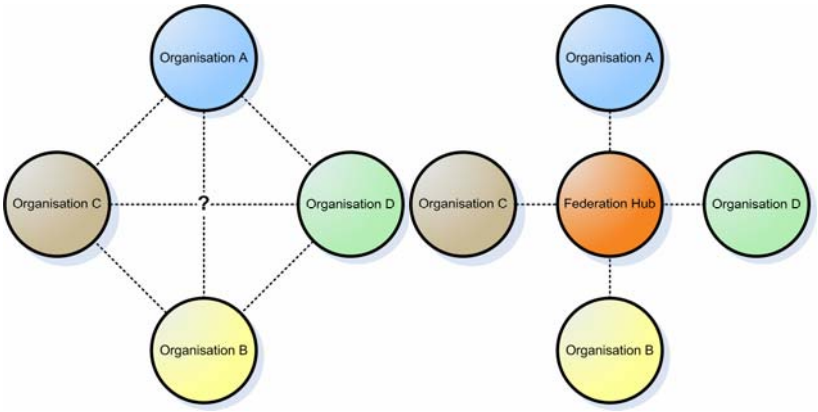
The simplest one is when two organisations decide to cooperate in the service chain and establish a direct trust in order to federate. This model is often referred to as the *point* model as depicted below.




In this example, organisation A has two processes in which it requires federation with different organisations, organisation B and organisation C. Hence, a trust is established with both organisations and no knowledge of the other trust is visible to either organisation. In the event that organisations B and C also wish to cooperate in the service chain in a different context, both establish a trust of their own.




However, if the number of services increases and more importantly, if access across services between all organisations is required, the scale of federation introduces the need for a common platform for federation: the federation *hub*.




A federation hub prevents one-off federation between organisations and the related cost ineffectiveness. Typically, a federation hub not only enables organisations to focus on the effort of a single integration but also often provides the legal and organisational framework required by federation in general.

Hubs are generally the topology of choice when cooperation and collaboration in a particular market segment transcends the relationship between individual organisations. Such is for instance the case in higher education as outlined by the case in paragraph 5.2 where multiple institutes of higher education wish to cooperate and use services provided by multiple organisations such as publishers and libraries across the market segment.

# 4 Enabling Technology

The federation architecture put forward in chapter three and the example client cases in the chapter after rely on standards and initiatives for a scalable execution of federation scenarios. Common challenges in federation scenarios include security and privacy concerns and scale of interoperability. These challenges in itself are not new when it comes to system or service chain integration, but become more apparent and critical to address when transcending organisational boundaries.

In order to address the issues raised by these challenges, a number of standards and initiatives have been developed over the last few years, they are still developing and have been incorporated in most of the larger vendor software stacks as well as various open source initiatives today. Each of these standards and initiatives have developed their own traits by addressing different issues, varying from user empowerment scenarios (privacy and user centric identity) to data exchange protection (security).

As standards and initiatives continue to develop, some merge and incorporate other standards in the process as the following paragraphs will illustrate. Please also note that the technology put forward in this chapter is not a finite list, but an overview of the most important current standards and initiatives which according to Everett will determine the federation market for the next few years to come.

As a guide through this chapter, consider standards to be low level specifications addressing identity message exchange formats as well as some simple scenarios (user to system dialogue sequences), whereas initiatives may incorporate these standards but add the ability to implement more complex user scenarios.

## 4.1 Standards

- **SAML**

  The Security Assertion Markup Language (SAML, pronounce as sammul) is a standard based on XML, defined by the standards body OASIS[2] to facilitate the exchange of identity data between domains. The message in which the identity data is wrapped is referred to as an assertion, hence the standard's name.

[2] http://www.oasis-open.org/committees/security

An assertion is a statement an identity provider issues about a particular user and is used by a service provider to determine entitlements if a user requests access for a specific resource. The statements such an assertion may contain are divided into three categories.

- ✓ Authentication statement: this statement declares the status on the verification of a user's identity at the identity provider. Examples of requests that can lead to an authentication statement include 'do you know this user' and 'what time did this user successfully authenticate with you';
- ✓ Authorisation statement: this statement states to which parts of the service provider the user has access to. In this case a service provider will trust the identity provider authorisation statement entirely without applying any authorisation rules itself. An example of a request that leads to an authorisation statement is 'does this user have access to the restricted premium services of car insurance';
- ✓ Attribute statement: this statement provides the service provider one or more user attributes and its respective value. In this case the service provider may use the statement to apply access control policies itself or use the attributes to personalise content. One example of a request that leads to an attribute statement is 'what is this user's credit level'?

The SAML standard initially focused on the standardisation of assertion messages (its format) and some simple and limited user scenarios describing the interaction between a user, identity provider and service provider in order to establish SSO. These user scenarios are called *profiles* and determine – next to assertions – the main content of the specification together with *bindings* (message carriers such as SOAP) and *protocols* (request response models). The first significant release of SAML was version 1.1 that was soon adopted by the larger identity and access management vendors and software solution providers over the course of 2004 into 2005.

At the beginning of 2005, OASIS released SAML 2.0 that incorporated new profiles (scenarios), broadening the standard's scope beyond SSO to include single sign off and adding privacy and security features previously lacking in the 1.1 version. Most of these new features were incorporated from two other major federation initiatives: Shibboleth and Liberty. As both Shibboleth and Liberty extended SAML 1.0 and SAML 1.1, incorporation of these initiatives' work into the SAML 2.0 standard has changed the risk of evolving disparate standards to convergence.

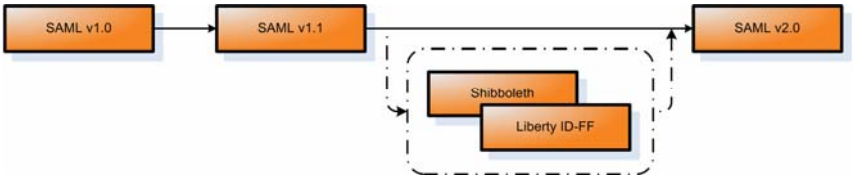



*Figure 5, SAML and Shibboleth*

- **XACML**

The abbreviation XACML stands for eXtensible Access Control Markup Language. This is also an XML based standard defined by OASIS in an attempt to standardise the exchange format of authorisation statements between domains. Where SAML focuses on how to exchange identity data without the need to know each others identity and access management structures, XACML focuses on how to interpret the exchanged data. These standards are complementary to each other especially as the SAML standard defines a XACML profile, but that the entire XACML specification can be used without SAML as well.

- **SPML**

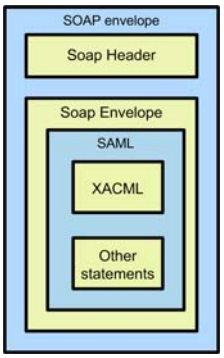
With SAML and XACML, federation is enabled with standards that define how to exchange authentication, authorisation and attribute statements which enables SSO across organisational boundaries. However, service providers often require local user profiles to exist in order for the underlying application or system to function.

Federations usually don't allow for the unbridled exchange of (privacy sensitive) data for use as provisioning data by the underlying application or system to mitigate this issue. Even when the federation would allow the data exchange required for account creation, there are no mechanisms informing the application of events relating to the life cycle management of the user's account at the identity provider.

These privacy and security considerations have provided the industry standard for provisioning with a drive to incorporate new specifications for use in federation scenarios. This standard is called the Service Provider Markup Language (SPML) and although it has become more aware to federation aspects in its latest 2.0 release from 2006 after its initial 1.0 release in 2003, federation is still a very small portion of the standard. The current landscape of federation solutions does very well at federated authentication and federated SSO but is troubled in its implementation as it often lacks mature federated provisioning support. Further development of the SPML standard is crucial to federation scenarios in order to capture user life cycle events across those organisational boundaries.

- **SOAP**

Finally, SOAP is the Simple Object Access Protocol that defines how XML based messages must be transported across a network in terms of its format (envelope and body). Although the standard does not prescribe a carrier, in practice, SOAP is usually transported over HTTP.




The figure on the right depicts how SOAP and the standards from the previous paragraphs correspond to each other.

## 4.2 Initiatives

- **Shibboleth**

Shibboleth is an initiative led by the Internet2[3] platform for the development of both a specification and its implementation where the emphasis is on the privacy of the user as well as extensions on the scenarios (profiles) of the SAML standard on which it is largely based.

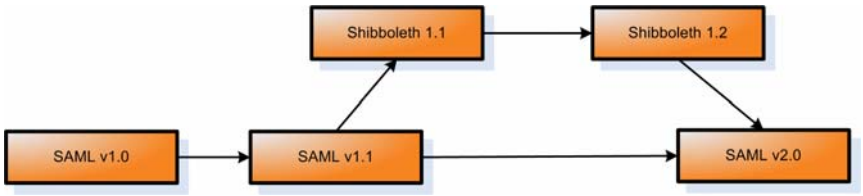



*Figure 6, Convergence SAML and Shibboleth*

The Shibboleth initiative distincts itself from other initiatives such as the Liberty specification and the WS-* (pronounce as WS-Star) due to the fact it not only drafts the specification, but at the same time provides a reference implementation framework to lower the adoption threshold.

This initiative is primarily used in the educational sector, but is nevertheless of significant importance as it has provided input to recent releases of the SAML standard (more specifically SAML 2.0). The developments in the field of higher education such as these have not only been important to the development of the standards. Given the early adopter attitude of higher education worldwide driven by a natural disposition to work together between institutions, most of the lessons learned in federation we have higher education to thank for.

[3] http://shibboleth.internet2.edu

## Liberty Alliance

Also known as Project Liberty, the Liberty Alliance is a specifications body consisting of large players in the software industry and both commercial and public sector. A few names are Sun Microsystems, Novell, RSA, General Motors, France Telecom and the French government.

Liberty is an organisation that strives to define and standardise the specifications to achieve federated identity in the broadest sense. Whereas the previously discussed scenarios (or profiles) as well as the Shibboleth initiative focus on federation for 'real life' users in a web based (browser) context, both the WS-* initiatives described in the next paragraph as well as the Liberty Alliance maintain a much broader scope by aiming for federation specifications in scenarios where for instance federation across web services is addressed.

In order to distinct these specifications, the Liberty Alliance has created several programs of which two are most prominent:

- ID-FF: Identity Federation Framework
- ID-WSF: Identity Web Services Framework

The development of the ID-FF specification of the Liberty Alliance is based on SAML standard version 1.0 and version 1.1 up to the release of ID-FF version 1.1. The SAML standard has been expanded by the Liberty Alliance in the ID-FF specification to include more complex scenarios such as opt-in and opt-out where the user can intervene attribute exchange and explicitly indicate whether he wants to federate his account or (a subset of) his identity data. Furthermore, Liberty alliance has included several privacy mechanism that enable organisations to link identity data between them without exposing account identifiers.

After the release of ID-FF 1version 1.1, the Liberty Alliance has handed the specification to OASIS for incorporation into the SAML 2.0 standard as the figure below illustrates.

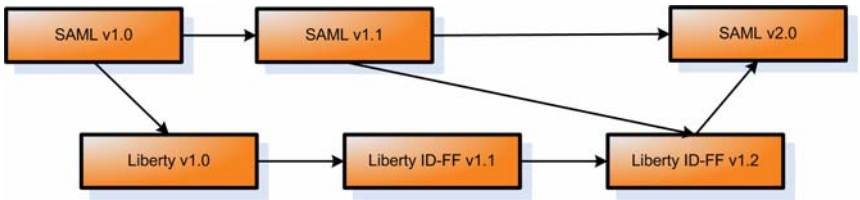



*Figure 7, Convergence SAML and Liberty ID-FF*

Now, the Liberty Alliances does no new development on the ID-FF standard on its own. The ongoing development is governed by OASIS, an explicit decision made by the Liberty Alliance members to promote convergence of standards and in order to focus on the development of the ID-WSF specifications.

This also illustrates the maturity of federation standard from a web based end user perspective. SAML 2.0 – together with the help from Shibboleth and the Liberty Alliance – has reached its adolescence and will now move to maturity on its own.

It also indicates where the development of federation standards other then those in the end user's web based context stands: childhood to early adolescence. Until recently, the development – to a certain extent – but certainly the adoption of federation web services standards has been meagre in comparison. Industry trends such as SOA (Service Oriented Architecture) and the position therein held by web services and composite application development are enormous drivers for federation web services standards in the next two years to come.

The latest ID-WSF release from Liberty already builds on top of the SAML 2.0 specification – which it helped create – in combination with some of the WS-* initiatives.

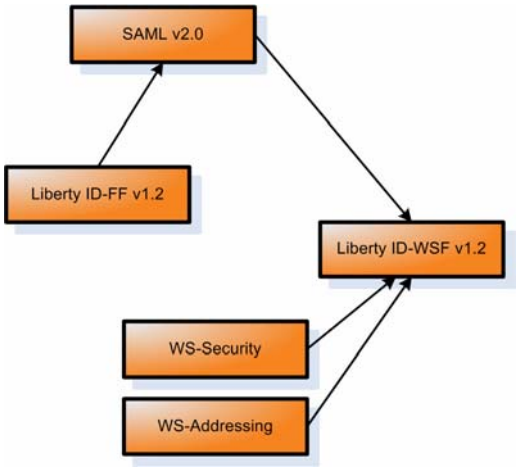



*Figure 8, Convergence Liberty ID-WSF, SAML and WS-* initiatives*

## WS-* and WS-Federation

Pronounced as WS-Star, WS-* is a set of web services specifications varying in purpose and certainly varying in the parties involved. As WS-* is nothing more then a collective name and not so much an initiative or collection governed by a standards body, anyone can define a specification and name it WS-Something. This makes it difficult to filter out the relevant and stable specifications at first glance.

However, there are a few WS-* specifications that are drafted by leading players in the software industry of which Microsoft and IBM are most prominent. Together they are responsible for the most important WS-* specifications around today.

These specifications do not all address federation in particular, although a few do. An important specification that applies to web services in general for instance is WS-Security (which is used by Liberty's ID-WSF as well). WS-Security is a protocol providing the mechanisms for applying security to web services and has been submitted by Microsoft and IBM to OASIS. As such, WS-Security is also part of a specification with has a more direct relation with this paper's topic: WS-Federation.

WS-Federation is developed by Microsoft and IBM and is positioned as sort of a competitor to the Liberty Alliance specifications and SAML 2.0. The specification actually consists of three sub specifications of which WS-Security is one as stated before:

- ✓ WS-Security is a communications protocol providing mechanisms to secure web services. In this context, it adds the mechanisms required to secure messages carried by SOAP. Hence the low threshold for Liberty to adopt this specification after the submission to OASIS;
- ✓ WS-Trust goes on to define the way security tokens need to be constructed when exchanging them between trust domains. In essence, the key properties of the security tokens defined by WS-Trust are similar to the early definition of assertions by SAML. As a result, WS-Federation does not use SAML;
- ✓ WS-Policy is a specification that aims to standardise the way policy messages are defined, where a policy is a set of rules to which an entity must conform in order to use the web-service.

WS-Federation is the above mentioned set of specifications, expanded with a set of directives how to use the specifications coherently in order to create a federative model. It also adds two sub specifications - WS-FederationActive and WS-FederationPassive, which model the execution of specific scenarios and the interaction between user, identity provider and service provider.

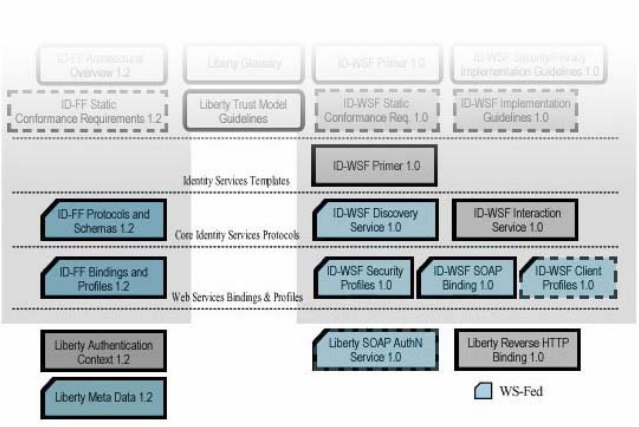



*Figure 9, WS-Federation versus Liberty ID-FF* [4]

## 4.3 User centric initiatives

The next two paragraphs provide an overview of the most important Identity 2.0 initiatives existing today; information cards and URL based identity.

- **Information cards**

  Information cards are user managed 'cards' containing identity information or references to identity providers able to assert that identity information as configured by the end user. In essence, it contains pointers to identity providers and information on what these identity providers are allowed to assert about the user as governed by that user.

  In the landscape of information cards, two main frameworks are worthwhile highlighting: CardSpace and Higgins. It is worth noting that both initiatives have adopted a similar approach, differences however do exist once a lower level comparison is performed. This is not in scope for this whitepaper and therefore not discussed in further detail.

  CardSpace is a technology included in the Windows operating system by Microsoft and enables end users to organise and use the aforementioned information cards when accessing service providers in a web context. Based on WS-Trust, CardSpace is the successor of the failed Passport initiative. As a client, CardSpace is currently only supported on the Windows platform, however Microsoft's involvement in the open source industry through the OSIS (Open Source Identity System) discussion platform allows optimism for support on the Linux platform.

  In turn, Higgins is a fully open source initiative by the Eclipse[5] foundation and supports the major components of the SAML and Project

[4] From http://www.projectliberty.org

[5] Please refer to http://www.eclipse.org/org/ for more information on the Eclipe foundation.

Liberty standards in an information card architecture. Its architecture however allows for identity information cards to be developed based on other protocols as well, such as some of the WS-* initiatives. As a client, Higgins is currently supported on both the Windows and Linux platform and can be used when accessing web based and non web based services.

- **URL based identity**

  The term URL based identity is used in the scenario where a user accessing a service provider does not identify him self through the traditional username and password but rather through the submission of a URL or URI (for instance everett.some-url-identity-provider.org).

  Generally, this URL points to an identity service, which the service provider can query to retrieve the identity provider(s) maintained by the user and where this identity provider resides. The service provider can redirect the user to this identity provider for authentication and identity attribute retrieval, as required by the service provider to provide access.

  Much like the information card initiatives from the previous paragraph, in this scenario the user is in control when selecting the appropriate identity provider. The underlying technology however differs from information cards, as it uses specifications from (open source) initiatives such as OpenID, Sxip or LID. These are all URL based identity programs, but they vary in their complexity and offered functionality (discovery services for multiple identity providers offered by Yadis for example) or even overlap and converge (OpenID and Sxip).

  There are several URL based identity initiatives and along with Microsoft's intended support for OpenID with CardSpace, will see ongoing convergence in the future.

# 5 Cases

The previous chapters have introduced federated identity as the key to integration throughout the service chain followed by a description of a federated architecture and its enabling technology. Moving on from these more or less abstract concepts, this chapter describes two real life cases to provide the required context.

## 5.1 Postal Services

This case is an example based of the hub topology from chapter 3 in which throughout the service chain three 'service columns' exist: online banking service providers acting as identity providers, the postal services as the trusted intermediate (hub) and its subscribing service providers designated as 'billers'. In this example, the phone company is used as an example of a biller but it could be any type of organisation. The three service columns create a process through the service chain as depicted by the figure below.

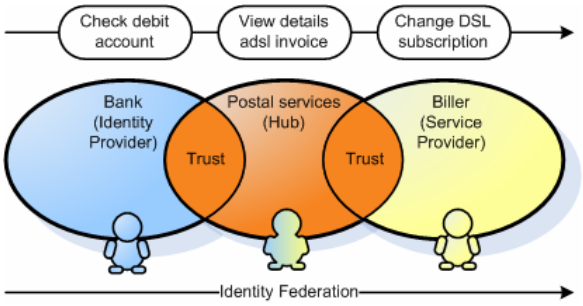
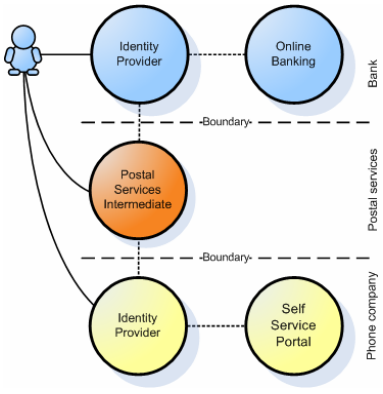



*Figure 10, Case 'postal services' identity federation*

The process is started when a user logs in to the bank portal to do some online banking. From there the user is able to view all his transactions and view details of these transactions. These details are served by a service located at the site of the postal services. This service is made possible through the earlier exchange of billing data between the phone company and the postal services. Based on a common identifier exchanged between the bank and the postal services, the appropriate information is presented to the user.

A user may then decide to upgrade his DSL account, for instance because he requires a subscription allowing him to transfer more data with his DSL account. Based on the SAML 1.1 protocol, further identity federation occurs allowing the user to seamlessly login to his personalised phone company portal account. The identity federation in this example is the postal service asserting the customer code and the phone



company trusting the postal service to have properly verified the user's account and his customer code previously. In this example, the actual user authentication occurred at the bank's site on which the postal service in turn relies.

This case is an example of trust and identity federation throughout the chain, where the end points of the service chain process are unaware of the start points in the chain responsible for the user's authentication.

This allows billers to potentially provide all banking users with an integrated user experience without the need for integration effort with various banking institutions. The same is true for all banks to provide richer service to end users without the need to integrate with numerous billers. This very principle is the business case for all three columns involved in the service chain and is depicted by the figure below.

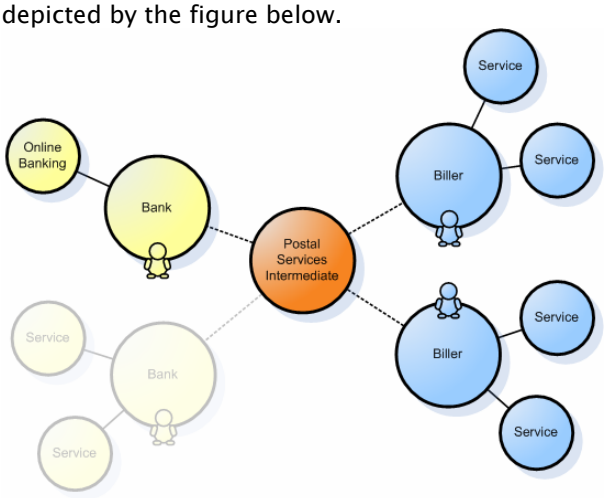



*Figure 11, Postal services federation hub*

## 5.2 Higher education

Much like the case in the previous paragraph, this higher education case is an example of federation using a hub topology. Here, the hub is called the SURF federation, an initiative of the SURF foundation with the mission to innovate higher education in the Netherlands through advanced shared ICT infrastructure as to promote cooperation and collaboration, both nationally as well as internationally.

The SURF federation supports and promotes cooperation and collaboration through its function as an intermediate between universities and colleges as well as other organisations active in the segment of higher educations such as libraries and publishers.

A typical end user process involving these parties is depicted by the figure below.

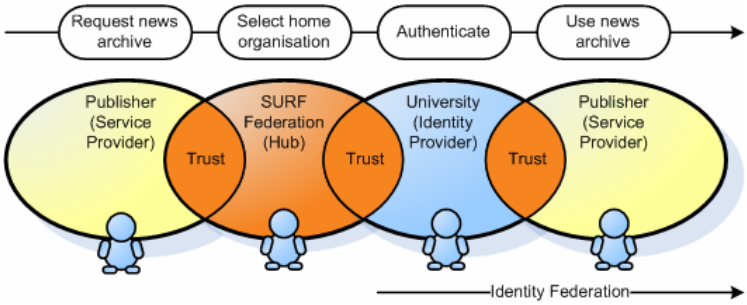
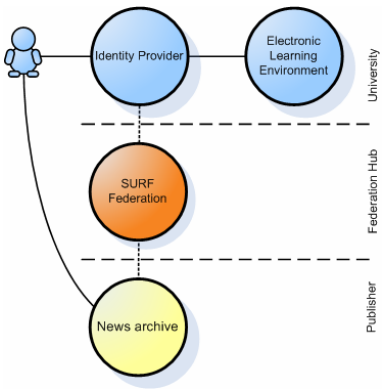



*Figure 12, Case 'SURF Federation' identity federation*

In the above example, it is assumed an end user (a student) is already logged in at his home organisation, a university at which he follows a masters in journalism. As part of his study program, the student requires access to an online news archive to support articles in his thesis.

When the student requests access to the news archive, its service provider (publisher) has no knowledge of the user but does require him to identify himself in order to determine his entitlements for the news archive. In order to prevent the requirement for a dedicated user account administration and to act as an identity provider itself, the publisher is subscribed to the SURF federation so it can leverage the identity providers of SURF federation subscribed universities.

The student is directed to the SURF Federation where he is presented with a list of all organisations known to the SURF Federation[6]. As the student's university is also subscribed to the SURF Federation, he selects his home organisation redirecting the student to the identity provider at his university.




The student is recognised by the identity provider since he has logged in there previously. The identity provider directs the student with the appropriate identity information back to the publisher based on which the entitlements for the news archive can be determined and the user is granted access.

Currently, the SURF federation supports identity providers to subscribe to the federation based on the proprietary A-Select 'cross' interface whereas service providers may choose to subscribe on the basis of A-Select or the

[6] Note that the SURF federation also supports variations to this scenario which are not mentioned in this paper.

SAML 1.1 open standard based Shibboleth initiative (an open source initiative of the internet2[7] platform). The roadmap of SURF federation also foresees to support subscriptions based on WS-Federation in the near future.

This case is an example of trust and identity federation between the service providers and identity providers, where the end points of the service chain process are aware of each other only through the SURF Federation. The SURF Federation in this case not only acts as the proxy but also provides the legal framework in order to indirectly establish the trust between all subscribed parties.

In this scenario, the business case for publishers and libraries is for instance the absence of user administration and its associated cost while maintaining the ability for personalised services and licensing. To parties such as universities this is also true where jointly developed masters are available to students and access to services from more then one university is required. This business case is extended by other drivers such as a seamless user experience in order to improve the richness of service delivery driven by increased competition in the field of higher education.

As the field of higher education involves many different organisations, so do the federation scenarios. Because of the requirement to subscribe only once – that is, to the SURF Federation – organisations are able to participate in numerous federation scenarios while maintaining cost effectiveness. This is best depicted by the figure below.

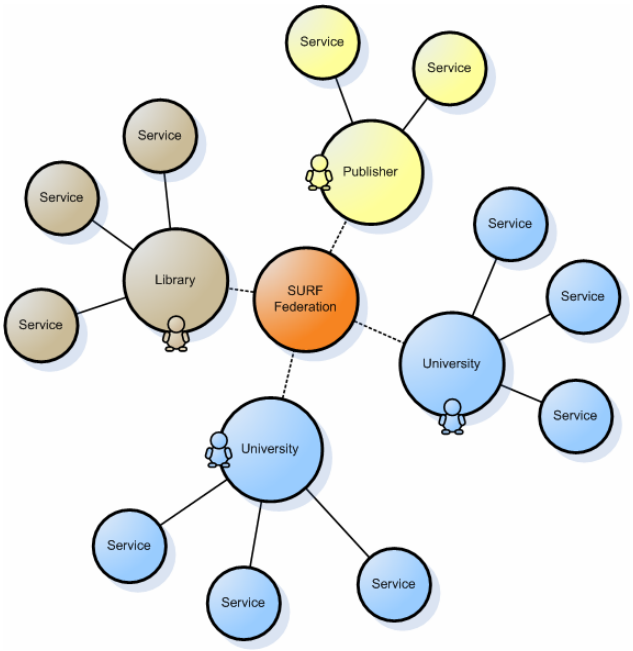



*Figure 13, SURF federation hub*

[7] Refer to http://shibboleth.internet2.edu/ for more information on internet2 and Shibboleth.

# 6 Approach

Based on Everett's experience with implementing federated identity solutions as put forward in the previous chapters, organisations have to be aware of specific areas in the delivery and deployment of federated solutions. This chapter outlines several phases where important aspects in the delivery of federated identity solutions are put forward.

## 6.1 Inception

- **Business case and architecture**

  The definition of a business case for federated identity is different to each organisation when it comes down to specifics. In general however, the business case for federation is focused around the following drivers:

  - ✓ Improve or maintain user experience;
  - ✓ Improve time to service and increase cost effectiveness;
  - ✓ Mitigate legal and privacy concerns.

- **Roadmap**

  The feasibility of a federated identity solution largely depends on the maturity of each participant's identity and access management environment. As different parties in the service chain become to rely on other's user identity statements, the reliability of these statements are crucial. This reliability is dependant on several things among which the accuracy of the digital identity data presented and the enforced restriction mechanisms (authentication and access control) are most prevalent.

  In general, participants must have their own user account life cycle processes under control through for instance the deployment of a provisioning system. Access management systems relying on these processes must also be in place, controlling access to internal services, preferably in a standards based manner to easy integration with those of other parties.

  Executing a prerequisite analysis for federation and – if required – the definition of roadmap / program on identity & access management from which projects can be derived is crucial in order to succeed. As with many things, it is important to think big, but implement in small steps.

## 6.2 Elaboration

- **Topology**

  Part of the design of any federated solution requires organisations to consider the topology in which they federate with others. If federation will only occur with a single partner, a point topology is applicable. However, it is recommended to look beyond the boundaries of just a specific partnership. In the long run your organisation may require to cooperate with multiple partners. A hub or networked topology may be more efficient if cooperation between your partners or the market segment in general is the case.

- **Supporting standards**

  The scalability of your federation capability is not only determined by the chosen topology. The choice of enabling technology to build your federation capability determines the scale of interoperability you will have with other parties now and in the future. It is recommended to adopt standards and initiatives supporting technology that supports your immediate federation needs as well as the standards that are commonly used by your potential federation partners of the future.

- **Identity attribute semantics**

  Federation scenarios depend on the reliability of the exchanged digital identity statements. However, assuring the reliability is not enough as its meaning is subject to interpretation. For this reason, all federated identity projects should pay attention to the semantics and mapping of data (attributes) in the design phase.

  This is illustrated by the example of the bank and the insurance firm where both parties will exchange information on an insurance product through an attribute called 'insuranceproductidentifier' taken from their respective back office systems. Agreeing on the digital identity information's label is not enough as its value is where both parties will need to agree when determining the type of service offered. Determining and aligning the meaning of identity attribute values is crucial for the exchange of identity statements to bear cross-organisational meaning.

**Legal and contractual agreements**

As parties start to collaborate throughout the chain, several legal and contractual issues arise. Attention is required specifically in the following areas:

- ✓ Auditability and liability: service providers rely on identity providers to properly verify identity authenticity and identity providers in turn expect the service provider to ensure the released identity assertions are protected from security threats. Therefore, security requirements on both ends, the auditability thereof and the end responsibility must be agreed upon;
- ✓ Service level agreements: service providers will rely on one or more identity providers and quite possibly a federation hub for identity operations. Without these available, access to the service provider is hindered, so service providers will need to establish service level agreements with the identity providers to ensure the availability of their services.

## 6.3 Construction

**Build and test coordination**

The reliability of service offered to the end user depends on federation components deployed by multiple organisations. This makes it apparent that during the build and test cycles in the construction phase require an approach considering the entire service chain rather then just the components under the span of your organisation's own control. Thus, coordination during this critical phase is required in order to ensure the quality of the service offered to the end user.

## 6.4 Transfer

**Support**

When the solution nears the stage of go-live-operations, the support for the federative process and not just its individual supporting components must be addressed. As from the end user's perspective there is a just a single service, any occurring issues or errors throughout the service chain will have to be addressed from a coordinated support organisation, both for back-end (operations) and front-end (service desk, single point of contact) support.

# 7 Seven frequently asked questions

### Why should I use federated identity?

When users require access to services but reside in different organisations or domains, the exchange of identity information needed to provide a seamless service is hindered by organisational boundaries. This varies from legal and privacy concerns to the ability to provide a sufficient time to service while still maintaining cost effectiveness. Federated identity addresses these.

### How can I maximise my federation interoperability?

Several standards exist today, and available technology and products often support multiple standards within a single product. Choosing standards and setting up appropriate policies for exchanging identity information are key to interoperability.

### What are the legal implications of federation?

Depending on the nature of trust between partner organisations in a federation, responsibility for privacy and service levels need to be addressed in the legal framework of the federation initiative.

### How do I agree on and manage exchange of user information?

Important to the exchange of user information is agreement on the measures to ensure privacy, the semantics and meaning of the exchanged user information and maximising the possibilities for exchange and transport of data through the adoption of a standards based approach.

### What is Identity 2.0? Is it for real?

Identity 2.0 is the collective term for user centric based scenarios and solutions, as opposed to organisation centric identity. In federation scenarios, this implies the user is in control when selecting the identity provider that is to release the identity information required by the requested service. Although very early in terms of adoption, identity 2.0 technologies have already become part of operational services. User centric identity, however, will often coexist with organisation driven federation where the identity or service provider determine the appropriate means of releasing and exchanging identity data between each other.

### Are there products available to implement federation?

Yes. A variety of established standards for organisation driven federation exists today including SAML, Liberty ID-WSF and WS-Federation. These are implemented by a broad range of vendors with commercial software products in their portfolio, but also in solutions provided by the open source community.

Examples of vendors are Sun, Novell and Oracle while the open source community provides, e.g., OpenSAML and Shibboleth. For Identity 2.0 user driven federation there are emerging solutions based on information cards such as Microsoft Cardspace or the open source industry's Higgins as well as URL based identity solutions such as OpenID.

### What do I need in order to start?

In order to start with federation it is important to be in control of the relevant internal identity and access management processes to ensure coherent identity can be linked into the service chain and your federation partners' infrastructure. A first step is typically to perform a preliminary analysis, involving a partner with experience in the area of provisioning, access control and auditing capabilities, as well as federation scenario's and technology.

# 8 About Everett

Everett, formerly known as Webflex, is a systems integrator and consultancy firm with highly skilled professionals and unique hands-on experience. Our inspiration is connecting individuals and ICT services in a secure, personalised and demand-triggered way.

However, 'demands' are changing ever faster, requiring ultimate flexibility of ICT-systems. Providing access is often in conflict with control, governance and privacy. Furthermore, corporate ICT should continuously reassess its past investments in the light of being potentially unique sources for new services, while balancing within the constraints of being auditable, cost-efficient and compliant. Our inspiration has therewith become a boardroom consideration, which will largely determine the success of the organisation.

Everett firmly believes in a middleware solution for this requirement for a controllable and agile ICT environment. New concepts and technologies in that area can provide your organisation with a sustainable -competitive- advantage, in terms of cost control as well as time-to-service. Over the years Everett has proven itself as a leading specialist on SOA integration frameworks and middleware in general and Portal, Secure Remote Access, Search, Identity & Access Management and Enterprise Application Integration technology in particular – an area of expertise that is subject to major new developments on a continuous basis.

We have therefore become a truly innovative company, embracing innovative concepts in the stage that they are 'fit for purpose', when they are leading edge rather than bleeding edge, however still early in their lifecycle.

We use our vision and knowledge capturing capability to identify which technologies will stand or fail, and which can contribute to an increase of the agility of your ICT services. We are organised in such a way that we know things earlier and better than others.

Since new technology and new concepts bring uncertainty we have adopted methods to absorb this while implementing. Our interactive and iterative methodology embraces change and channels it to the desired result. We will assist you in this process as your consultant, architect, project manager or engineer. As a temporary addition to your team or as a complete project team with a clear mission.

And after we deliver we will not back off. Everett's Advanced Technical Support centre will be available to assist with in-depth expertise to accommodate the appropriate SLA. We strive for thought leadership in our competence and we want to work as a trusted advisor with the early adopters in any industry.

Everett NL, Wiersedreef 5-7, 3430 ZX Nieuwegein, The Netherlands
Everett UK, 55 Station Road, Beaconsfield HP9 1QL, United Kingdom

# 9 Terminology

| | |
|---|---|
| Artifact | A reference based on which a service provider can retrieve an assertion. |
| Assertion | A claim or statement about a particular identity by an identity provider. |
| Authentication | The process of verifying an entity's claim of identification. |
| Authorisation | The process of establishing the entitlements for access. |
| Cardspace | A framework for identity selectors developed by Microsoft which stores assertions or pointers to identity providers capable of providing assertions. |
| Federated identity | All processes and underlying technology which make it possible to exchange identity data *across organisational boundaries* in a *secure* and *controlled* manner. |
| Higgins | An open source framework for identity selectors of the Eclipse foundation. |
| IAM | See 'Identity and Access Management' |
| Identity and Access Management | All processes and underlying technology for the creation, life cycle management and application of digital identity data. |
| Identity Provider | An entity providing assertions to services that rely on those assertions for providing access. |
| IDM | See 'Identity and Access Management' |
| Infocard | See 'Cardspace' |
| Provisioning | The automatic propagation of new, changed or removed identity date from authoritative sources to connected systems in order to establish efficient and consistent user management. |
| SAML | Security Assertions Markup Language |
| Service Provider | An entity relying on assertions provided by an identity provider for providing access. |
| Shibboleth | Shibboleth is standards-based, open source middleware software which provides web SSO across or within organizational boundaries. |
| SPML | Service Provisioning Markup Language |