everett TRUSTED TO KNOW

innoPAY

E-identity as a business

Case studies and lessons learned in networked identity

Peter Valkenburg, Wouter Meijers (Everett)

Douwe Lycklama, Vincent Jansen (Innopay)

Sponsored by

eema
www.eema.org

Table of Contents

Reviewed by Kick Willemse (Evidos)

1 Management summary

After many trials, pilots, successes and failures the identity market is still finding its shape and size. Its crucial role in the development of e-business is not disputed and more and more the subject is coming out of the 'technology geek scene'. Business people become interested, since networked e-identity, which we define as "identity across organisational boundaries", can be regarded as 'the mother of all transactions'. In the generic end-to-end trade process, identity is at the heart of each step: contract, order, shipment, invoice, payment and tax settlement. Service providers in all forms and shapes see opportunities, also 'in the cloud', enabling previously unheard scalability.

The upshot of this is that e-identity should develop out of the positioning of a pure 'cost', 'control' and 'compliance' subject into a growth-enabling topic. E-identity develops from an enterprise identity to networked identity, were it becomes a two-sided market with two distinct user groups: end users and service providers (aka 'relying parties') who can grow revenues en lower costs by offering better e-services to their clients.

This paper aims to discuss some of today's main e-identity business propositions, including their business models. The main observations are:

a. Success is for providers and solutions who clearly serve the distinct needs of end-users, and service providers. If one of them is underserved, the solution will not scale well.

b. Governments are still a major driver for e-identity, but long term success comes when the private sector is included, simply because users then have more need for usage.

c. Different solution approaches exists, all with their own right of existence. Mass adoption and success will only come when interoperability is secured, enabling more rapid growth.

The document starts with an explanation of the business of e-identity (chapter 2) and a generic framework with which networked e-identity solutions can be analysed (chapter 3). Based on various cases in the public and private sector including cloud services (chapter 4), the most critical issues are addressed for those having to take business decisions in the field of e-identity (chapter 5).

2 Understanding networked e-identity

2.1 Why e-identity?

Business transactions involve people. Irrespective of whether the activity is about a contract, order, shipment, invoice, payment or tax settlement, it involves individuals who initiate, perform tasks and sign them off. Most business activities are nowadays supported in some sense by IT, and increasingly transactions are available as end-to-end services over the Internet separating time and distance. Figure 1 shows the generic description of the end-to-end trade process.

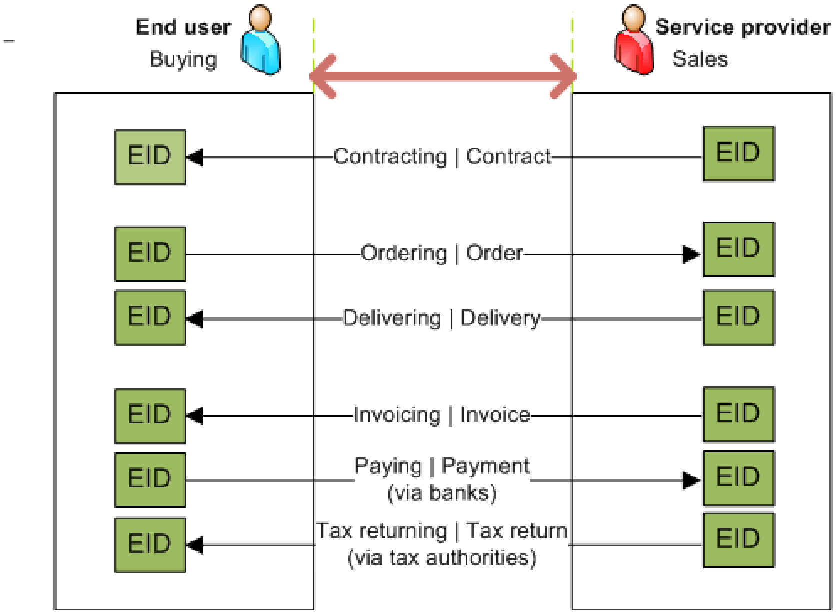


Figure 1: Trust in each step of the end-to-end trade process

For these electronic transactions trust is required on an increasingly large scale. This trust makes it possible to order, pay, deliver and provide reliable communications and trustworthy information. Trust in the digital world hinges on electronic identity (e-identity), where two interacting parties achieve enhanced trust through e-identity.

In generic terms: the end user is able to prove (relevant parts of) his identity to the 'service provider' and the service provider is able to demonstrate he is the authentic source of its services. In the natural world, a person has an identity which can be defined according to a series of attributes, or specific properties such as sex, age, hair and eye colour, profession, location etc. A person's online e-identity is an often-similar set of attributes that are kept in IT systems and can be related to a person's natural, physical identity.

Identity information of end users is kept in many places in today's world and is often made available to various organisations and individuals through the Internet, providing the trust to do e.g. online banking. This kind of *networked e-identity* is a crucial enabler for large-scale transactions, both in the public and private sectors. Increasingly, e-identity is being offered as a service and in that respect it can be said to be the 'mother of all transactions'.

Organisational digital identity versus networked e-Identity

The digital identity of a person has, up to a few years ago, mostly been restricted to the use for services within a single organisation. Nowadays, an employee or client of an organisation often has an electronic identity within each organisation the person is involved in. The need to use a single identity for seamless and cost effective access to increasing amounts of services on the Internet has led to the growing use of cross-organisational electronic identities, which in this paper is addressed as 'networked e-identity', often abbreviated to just 'e-identity'. The major difference between an intra-organisational identity and networked e-identity lies in the fact that the latter needs to be provided by a network of organisations that must be aligned to create the business and trust needed. The various parties involved make setting up networked e-identity a different endeavour than the nowadays well-understood and often straightforward hierarchical setup of intra-organisational digital identity.

2.2 What is the problem?

The problem is on two sides:

1. *End user*: the scattering of identity information of individuals over numerous organisations does lead to privacy issues and user burden to remember and maintain identities.
2. *Service provider*: for organisations the scattering of identities does not add to the required trust. Every organisation provides its own identity mechanism online, varying from passwords to advanced certificate infrastructure, leading to cost and management burden.

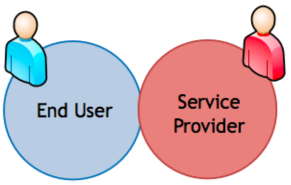
E-identity is a (so far) under-recognised two-sided market, where two distinct users groups (end users and providers) interact with each other. There is a business opportunity for parties in the facilitation of these two users groups. Dealing with the aforementioned two basic problems will prove essential.

Networked e-identity is identity, which is re-usable over multiple organisations, thereby reducing the two-sided problem.

2.3 How is e-identity provided?

With more and more services being offered online, ranging from e-commerce to e-government and banking, service providers need to know whom they are dealing with and consumers must be assured they deal with an authentic partner and that access to their personal information is assured. But how do you know whom you are dealing with?

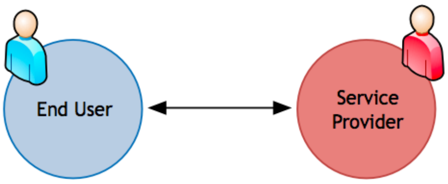
When dealing with people in the offline world, identity is easier to asses because of the physical interaction between these individuals. A person's face coupled with a picture ID is usually sufficient. A signature, matched to that on the ID, can add security. In addition, assessments of a person's trustworthiness can be made based on appearance or intuition.



A specific example to illustrate this is age verification. In many countries there is a legal age limit for purchasing alcohol. Here the attribute 'age' is verified. In this situation, age verification can be based on a visual assessment of the person's age. A general assessment that the person is over the legal age limit may be sufficient and the person's exacted date of birth may not be required. Alternatively, age can be determined on the basis of an identity document bearing a date of birth and a picture such as a passport or a driver's license. The identity document is a tangible document with certain standard characteristics that prove its authenticity. The picture on the document is compared to the visual appearance of the person offering the document to match the two. In both cases there is an immediate visual assessment by one individual of the other individual.

This relatively simple situation is complicated when it is carried out online. In an online transaction, the two parties, the end user and the service provider, are separated by time and space, rendering visual means of authentication unusable.

In the past two decades many technologies have been developed to make identities usable in the digital domain. Think of e.g. user names/ passwords, tokens, certificates and biometrics, all tools for making e-identity happen. Many initiatives are available now with all distinct characteristics. In the next chapter e-identity will be introduced and a generic framework will be presented.



3 Introducing e-identity solutions

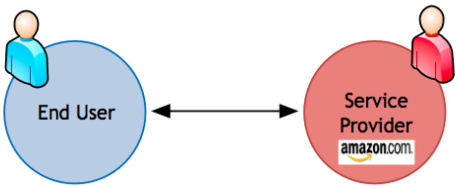
In this chapter we discuss e-identity solutions in a systematic way to allow the next chapter to discuss different examples in a structured manner. First we introduce the evolution of e-identity solutions from a closed model to an open service provider model. From this introduction we derive a description of a generic model for e-identity solutions.

3.1 A world of two-party networks

As an example to demonstrate the evolution of e-identity, let us consider Amazon.com. Amazon.com was founded in 1994 as an online bookstore. It later diversified its product range and grew into a leading global online retailer.

At Amazon.com, like at many other web shops, end users create an account with a username and password. The account contains payment and shipping details (identity attributes) and can be used to give product reviews. Amazon.com only accepts orders from account holders that are properly authenticated, e.g. through a successful credit-card payment.

In this solution there are only two parties involved: the end user and Amazon.com. We call this a two-party solution (or closed model). Amazon.com has all the information and provides all functionality necessary to authenticate the end user.



Identity solutions have started as purely technical solutions, where the end user has a relation with the service provider. The service provider stores the (relevant) identity (attributes) of the end user and gives out authentication means to end-users. Only two parties are involved.

Having (many) two party solutions is far from ideal for three main reasons:

1. End users have to create accounts for each service provider they visit ending up with a great amount of identities (often usernames and passwords).
2. End users have to maintain their profiles (identities) at every service provider they visit. Apart from the burden of having to maintain this information, a potential privacy risk is introduced by having personal data scattered over all service providers.
3. Service providers have to implement and maintain their own identity solution. This is a cost and time-consuming operation that keeps service providers away from their core business.

In two party solutions the identity solution is often positioned as a cost to the service provider.

3.2 Towards an open model: three-corner networks

The solution to the described drawbacks of the two-party solutions is actually quite simple: introduce a third corner. Often this is referred to as 'three party model', but the same party can fill in the two corners. An identity provider (the third corner) can focus on implementing and maintaining an identity solution that it offers to both the end user and the service providers. This results in less credentials to remember and profiles to maintain for end users and focus on core business for service providers while increasing profile accuracy. The figure below shows a generic model for e-identity:

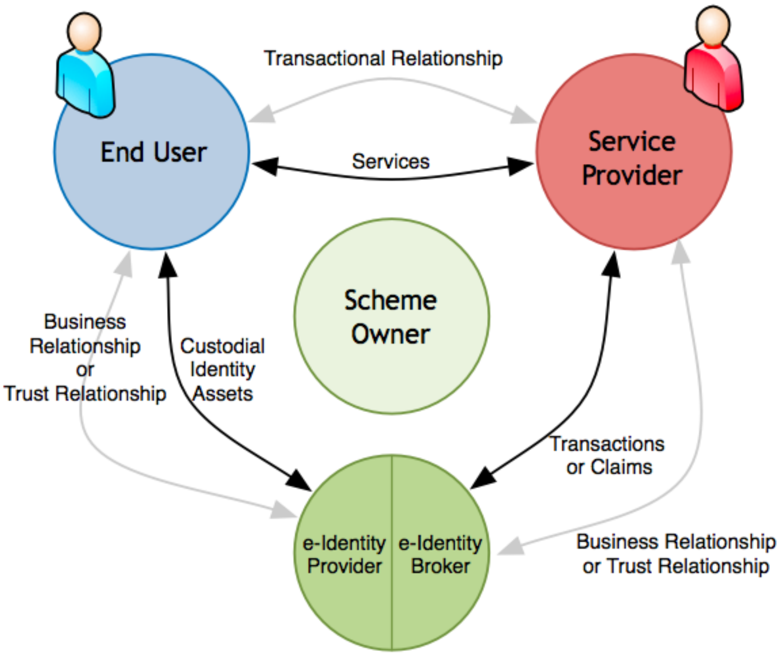

Transactional Relationship
End User
Services
Service Provider
Scheme Owner
Business Relationship or Trust Relationship
Custodial Identity Assets
Transactions or Claims
e-Identity Provider
e-Identity Broker
Business Relationship or Trust Relationship

Figure 2: A generic three-corner model for e-Identity

It should be noted the needs of the two distinct user groups (end user and provider) are catered for by only one provider. Therefore the service provider has two propositions: one for the end user and one for the service provider.

Three party models come in two ways:

1. *Government sponsored*. Government gives out authentication means, mainly for use with their own services
2. *Service providers re-use*. Service providers with large customer bases (e.g. Amazon.com, PayPal, Google, Face book) re-use their credentials over each other's services. A specific scheme has been created, which is called OpenID.

The business model of three corner models is still unclear. Either they do not have a business model (e.g. OpenID or government issued ID cards) or they provide authentication as part of a payment service (e.g. Amazon, Google and PayPal).

Three corner models overcome some of the drawbacks of two party models, because it increases the re-usability of the credentials for the end user and reduces the integration efforts for the service providers. The main problem however is that there is a multitude of three corner models. Every initiative strives for ‘world domination’ and becoming the ‘de facto’ solution. As a result, service providers do not reside all with the same three-corner identity provider and therefore the end user is left with the management of multiple identities.

This can only be overcome when all service providers and all end users concentrate at a few identity providers. For competition and privacy reasons this could not be a preferable situation.

3.3 The generic e-identity model explained further

In the previous paragraphs we saw a closed model evolve into a more open model. Within this model we clearly can distinguish four core roles:

1. **End users**

   End users request identity services from the e-identity provider. With such a service the end user can transact on-line real-time. End users can be individuals acting on their own behalf or on behalf of organisation.

2. **Service providers**

   A service provider can be a private or public party who offers on-line services. Think of e.g. tax filing, permit request, bookshop, airline ticket and banking. When using these services the end user has to identify himself during the process. Also certain relevant attributes might be checked, such as e.g. age or gender.

3. **e-identity provider and broker**

   These two roles are often combined in one corner or party.

   An e-identity provider role is the proposition towards the end user, whose identity elements are managed by the e-identity provider. Therefore there must be a trust relationship of some form. The level of trust is depending on the purpose. The identity provider also facilitates the actual checking of the identity by service providers through their e-identity broker. This is always triggered by the use of credentials issued to the end user. Credential can be e.g. passwords, tokens, phones and certificates. One of the core processes of the e-identity provider is the registration or issuing of identities. The trust level towards the service providers is often determined by the registration process (e.g. physical appearance is regarded as more reliable) in combination with the security level of the tokens.

   The e-identity broker role is the proposition to the service provider. Through the e-identity broker one or more e-identity providers can become part of the service towards the service provider.

In order to assure that the interaction between the four roles (end user, service providers, e-Identity Providers) proceeds smoothly, securely and according to a prearranged set of policies and regulations, one or more scheme owner organisations can be established. Typically in a three corner set up, the party offering the central platform can be regarded as the scheme entity.

In situations where the two proposition roles (e-identity provider and broker) can be offered by different parties (four corner model), the scheme entity lays down the ground rules upon which the various transactions take place. Also compliance with these rules is governed by the scheme organisation. Scheme owners typically consist of a number of cooperating parties that have a common interest in the creation and exploitation of a particular identity management scheme.

3.4 Key characteristics of an e-identity service

With the generic e-identity model in mind, we will discuss in the following chapters various e-identity initiatives. The analysis will be done according to certain characteristics. These characteristics are chosen for the purpose of this white paper. Many more characteristics exist, but they are not considered relevant for this paper.

Any e-identity service has two distinct aspects:

1. First is the registration phase where individuals register and are issued the e-identity by the identity provider. The registration procedure, the process by which the e-identity is issued and the integrity of the e-identity provider are fundamental for the integrity of the e-identity service as a whole. If the registration phase is susceptible to fraud, the integrity of the entire service is compromised.
2. Following registration is usage phase where the claimed identity of an individual is authenticated, authorised, etc. Important aspects in this phase are the process by which information regarding the identity is transacted between parties, the purpose of this transaction process and who has control over the credentials.

   Additionally, the working of the business model as well as issues regarding privacy and trust are important elements in the authentication phase.

Different e-identity services can be described according to a number of key characteristics. These include:

- ✓ *Registration* – The registration process describes the procedure of initial registration and the issuing of the e-identity.
- ✓ *Transaction* – The authentication transaction process and the model of the service are described.
- ✓ *Business model* – The fees and revenues are described.
- ✓ *Privacy and trust* – Any issues relating to privacy and trust such as the exchange of attributes and the integrity of parties in the network.

In the next chapter a selection of current e-identity initiatives are discussed, along the lines of the four characteristics.

4 Case studies

This chapter will present a number of case studies of e-identity services and standards in use today. We have selected a wide range of services from e-commerce to online banking and e-government and from different countries. We can learn a great deal from the way these services are set up and how they operate.

The first two cases, OpenID and CardSpace, are technology driven but vendor-neutral approaches[1]and have been selected because of their potential impact on the e-identity marketplace. The remainder of the cases are business oriented and have been chosen to depict how commercial, governmental or educational organisations have implemented various technologies to solve specific business issues. Some of these solutions (e.g. Google Apps, SURFfederatie) utilize open standards such as OpenID; some are based on proprietary technology (e.g. DigiD).

[1] We can argue whether CardSpace is in fact vendor-neutral, given the dominant role of Microsoft in the development of the standard. However, Microsoft has stated to be committed turning the associated InfoCard standard into a true open standard and has released all specifications and actively cooperates with third-parties to make the standard a success.

4.1 OpenID

The power of OpenID is based on the explicit lack of a pre-existing relationship between the service provider and the identity provider (in this particular case called the *OpenID Provider*). Instead, the scheme relies on the user providing a claim of ownership of a URL to the service provider. The service provider verifies this claim by establishing a shared secret in cooperation with the server hosting the claimed URL (identity provider). The user must be able to represent this shared secret when obtaining access to a resource owned by the service provider. Because the scheme is entirely based on self-issued claims, OpenID is only suitable for low-risk transactions. In practice, the scheme is mainly used to provide access to social networking sites[2].

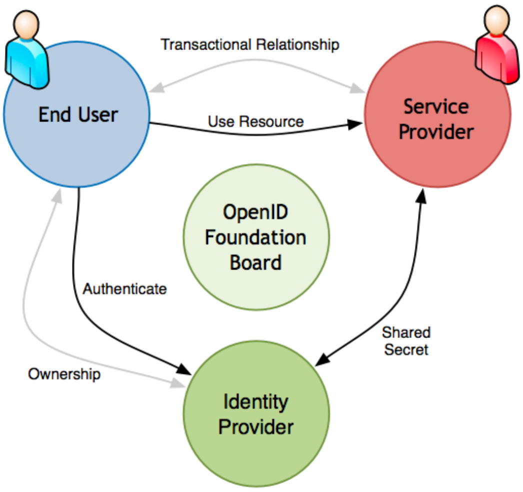


Figure 3: the OpenID authentication scheme

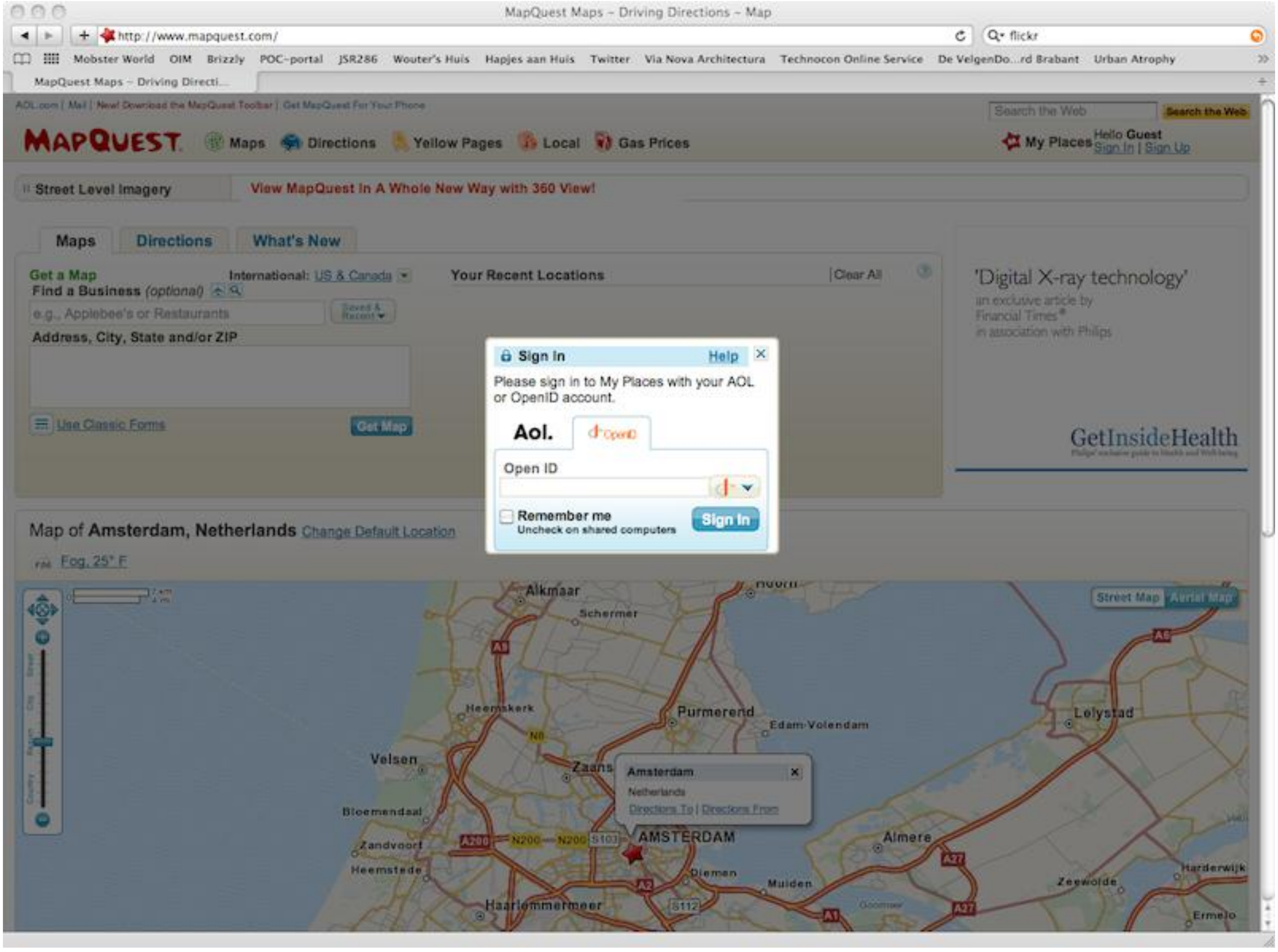
4.1.1 Registration

A user can simply create an OpenID account by registering a URL on a server that can act as an OpenID provider. This can be any one of the public OpenID servers but it can also be a server owned and operated by the user. Example of an OpenID:
`http://usermike.myopenid.com`

Currently, many of the popular social networking sites have implemented the OpenID protocol, allowing people with an account on one of these sites to login to any site supporting OpenID. A non-comprehensive list of participating sites is: Google, Yahoo, LiveJournal, Facebook, Hyves, Blogger, Flickr, Orange, MySpace, WordPress.com and AOL. Apart from these, the user can also register a free account with any of the public OpenID Providers such as Chi.mp, ClaimID, myID.net, myOpenID, VeriSign or yiid.

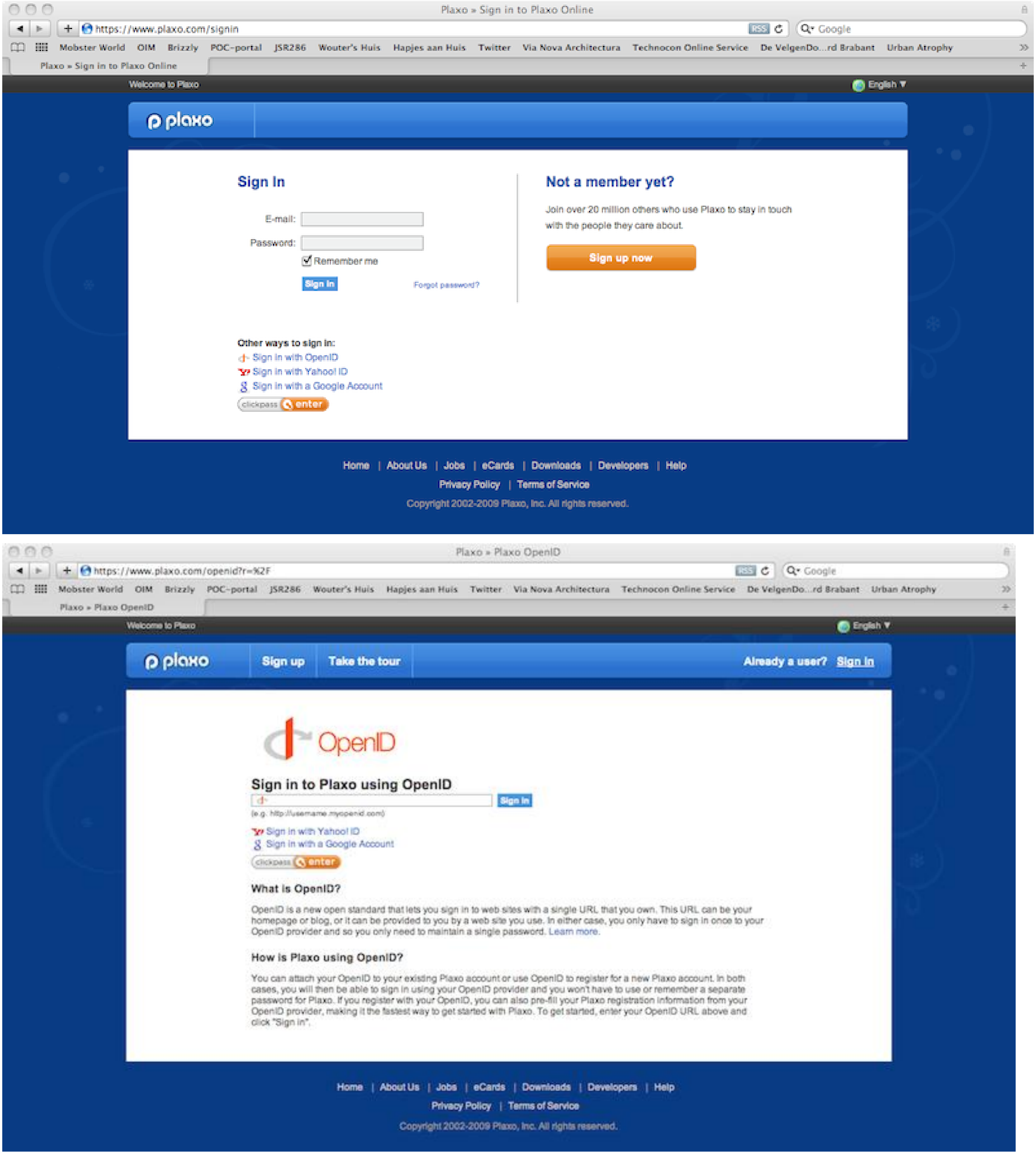
The following screenshots show a number of popular sites that offer OpenID as an authentication method:

[2] However, this situation might change in the future as more and more providers are adding extensions in-and-around OpenID. One example is Google, who combined OpenID with the OAuth authorisation protocol (see chapter 4.3). Another example is the Japanese telecom giant NTT Docomo (over 55 million subscribers), who facilitate an interface that providers can use to obtain additional identity information in the context of an OpenID authentication and which can be used (among other things) to perform on-line payments.



Please sign in to My Places with your AOL or OpenID account.

Figure 4: MapQuest provides either an AOL or an OpenID login box



Sign In

E-mail:

Password:

☑ Remember me

Sign In

Forgot password?

Not a member yet?

Join over 20 million others who use Plaxo to stay in touch with the people they care about.

Sign up now

Other ways to sign in:

- Sign in with OpenID
- Sign in with Yahoo! ID
- Sign in with a Google Account

clickpass enter

Home | About Us | Jobs | eCards | Downloads | Developers | Help
Privacy Policy | Terms of Service

Copyright 2002-2009 Plaxo, Inc. All rights reserved.

Sign in to Plaxo using OpenID

Sign In

(e.g. http://username.myopenid.com)

- Sign in with Yahoo! ID
- Sign in with a Google Account

clickpass enter

What is OpenID?

OpenID is a new open standard that lets you sign in to web sites with a single URL that you own. This URL can be your homepage or blog, or it can be provided to you by a web site you use. In either case, you only have to sign in once to your OpenID provider and so you only need to maintain a single password. Learn more.

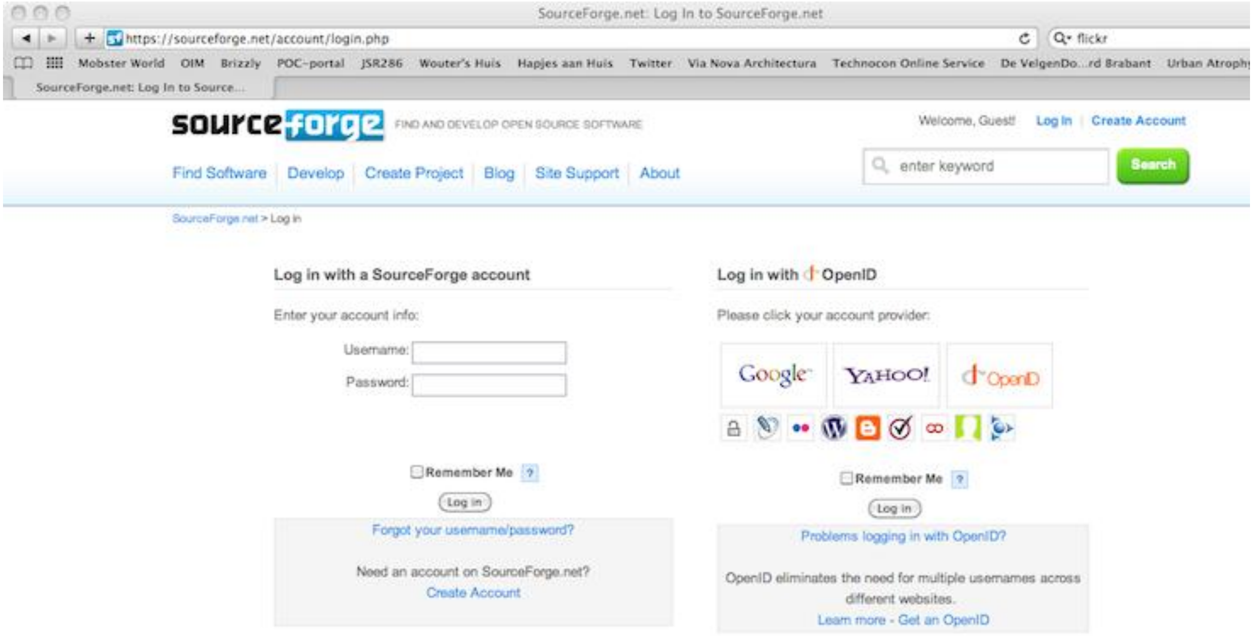
How is Plaxo using OpenID?

You can attach your OpenID to your existing Plaxo account or use OpenID to register for a new Plaxo account. In both cases, you will then be able to sign in using your OpenID provider and you won't have to use or remember a separate password for Plaxo. If you register with your OpenID, you can also pre-fill your Plaxo registration information from your OpenID provider, making it the fastest way to get started with Plaxo. To get started, enter your OpenID URL above and click "Sign in".

Home | About Us | Jobs | eCards | Downloads | Developers | Help
Privacy Policy | Terms of Service

Copyright 2002-2009 Plaxo, Inc. All rights reserved.

Figure 5: Plaxo provides a number of external authentication mechanisms, including OpenID



SourceForge.net: Log In to SourceForge.net

https://sourceforge.net/account/login.php

Mobster World OIM Brizzly POC-portal JSR286 Wouter's Huis Hapjes aan Huis Twitter Via Nova Architectura Technocon Online Service De VelgenDo...rd Brabant Urban Atrophy

SourceForge.net: Log In to Source...

sourceforge FIND AND DEVELOP OPEN SOURCE SOFTWARE

Welcome, Guest! Log In | Create Account

Find Software | Develop | Create Project | Blog | Site Support | About

enter keyword Search

SourceForge.net > Log in

Log in with a SourceForge account

Enter your account info:

Username:

Password:

□ Remember Me ?

Log in

Forgot your username/password?

Need an account on SourceForge.net?
Create Account

Log in with OpenID

Please click your account provider:

Google YAHOO! OpenID

□ Remember Me ?

Log in

Problems logging in with OpenID?

OpenID eliminates the need for multiple usernames across different websites.
Learn more - Get an OpenID

Figure 6: SourceForge offers an extensive range of external authentication methods, including OpenID

4.1.2 Transaction

OpenID entirely depends on existing and well-established Internet protocols and standards such as HTTP and XML. The figure below depicts what happens when a user attempts to access a site that supports the OpenID protocol:

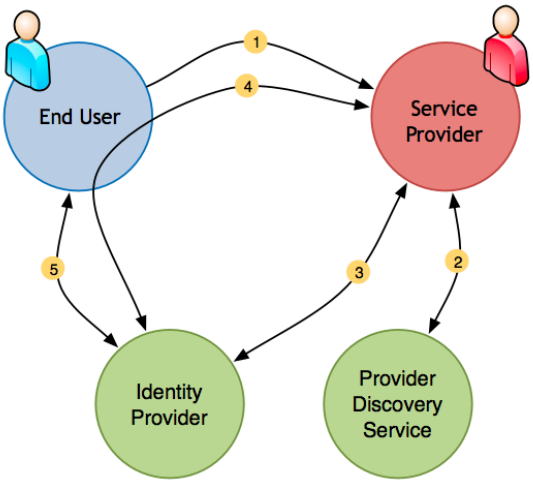


Figure 7: The OpenID authentication sequence

The user enters his/her OpenID URL in the “OpenID login” box at the service provider (step 1). The service provider uses a discovery protocol (such as *Yadis*[3]) to find the location of the Identity provider, based on the contents of the provided URL (step 2). The protocol might

[3] The Yadis protocol (located at http://yadis.org) is closely related to OpenID, but can also be used by other authentication schemes. Yadis translates the user-specified URL (the *Yadis-ID*) into an *eXtensible Resource Descriptor* (XRD) document that provides a list of service identifiers applicable to this user-specified URL.

use a separate discovery service, depending on the format of the OpenID URL provided by the user. Once discovered, the service provider and identity provider establish a “shared secret” (step 3).

The discovery service can be considered the “e-identity broker” from our generic model. The discovery service selects an identity provider based on the structure and content of the URL provided by the user and thus allows the service provider to utilise a potentially large number of different identity providers.

The user is now redirected to the identity provider (step 4) and is requested to authenticate using any method supported by this provider. The authentication mechanism can be anything from simple username/password to certificates, tokens or Info Cards (see: chapter 4.2, CardSpace). The identity provider asks the user whether he/she trusts the service provider to receive the user’s credentials and identity details (step 5). This is an important step since it provides the user with a mechanism to control which information is disclosed to the service provider.

If the user is satisfied with the requested information, he/she is redirected back to the service provider, which verifies the received user credentials against the “shared secret” established earlier. If all is satisfactory, the user is granted access to the requested information.

Note that the exact set of credentials that can be exchanged varies between service providers. When registering ones OpenID, the identity provider typically facilitates the creation of user profiles and negotiates with a service provider regarding the attributes to be returned as part of the credential request. In a typical case, the user is shown the list of attributes that the relying party requests and the user can accept or refuse any of these attributes before being redirected back to the service provider.

4.1.3 Business Model

The roots of OpenID are in the social networking domain where users expressed a desire to obtain access to Blogs, Wiki’s and other social networking sites without the need to register and authenticate separately for each and every site. Instead, OpenID provides one, easy to remember, URL-based user identity and associated profile that can be used to obtain access to a large number of different sites.

Since users can run their own OpenID provider, they have maximum control over the identity attributes that are used for authentication. Even when using a public provider (such as MyOpenID), the user still has to maintain only a single shared profile that can be used to obtain access to a large number of different sites. This central profile provides a good incentive to users to keep the information up-to-date, which in turn is a benefit to the service providers, which are more likely to receive accurate information.

The second advantage for the service providers is the delegation of user registration information and authentication to the identity provider. Instead of having separate registration forms, local authentication schemes and associated data stores, user properties are maintained at the identity providers and are obtained during authentication by a user-controlled process. Note that there exists *no* explicit trust relationship between service providers and identity providers. This facilitates a federated authentication network that can scale almost infinitely.

On the downside, this lack of trust relationship combined with the use of self-issued claims means that services provided by service providers to the users are limited to relatively low-risk service types, such as the aforementioned access to Blogs or other social networking sites.

4.1.4 Privacy & Trust

The OpenID scheme is based on self-issued claims. Users maintain their own OpenID profile (either at one of the many public OpenID identity providers, or at a provider managed and operated by the user). During authentication, users can manage the properties that are passed from the identity provider to the service provider. While this scheme provides a high level of privacy protection from the user's point of view, the lack of explicit trust relationships between the service provider and the identity providers, combined with the fact that the service provider has no control over the strength and quality of the authentication scheme implemented by the identity provider, also implies that the service providers cannot depend on the quality and accuracy of the received user credentials.

The OpenID protocol relies heavily on redirection, in which the user is sent from service provider to identity provider and back. This particular behaviour makes the OpenID protocol vulnerable to "phishing" attacks (e.g. the introduction of rogue providers that insert themselves into the authentication chain, thereby facilitating digital identity theft).

4.2 CardSpace

CardSpace, (otherwise known as “*Info Cards*”) is an identity management scheme originally devised by Microsoft as a means to provide more control to the end user compared to the more traditional schemes. CardSpace basically routes *all* traffic through the end user’s device and thereby provides maximum control of the identifying properties that are exchanged between service provider and identity provider (in this particular case called the *Security Token Provider)*.

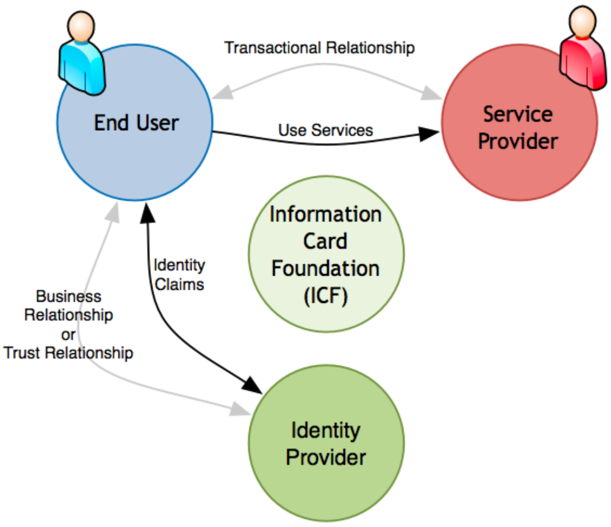

End User
Transactional Relationship
Use Services
Service Provider
Information Card Foundation (ICF)
Identity Claims
Business Relationship or Trust Relationship
Identity Provider

Figure 8: the CardSpace identity management scheme

Apart from being integrated in Windows Vista and Windows 7, CardSpace is currently supported by a number of Identity Management software suppliers. Examples are the Bandit project, IBM, FuGen solutions, the Higgins project, Ping Identity, the Shibboleth project, Siemens, Sun, Oracle, VeriSign, WSO2 and the XMLDAP project. Since CardSpace is build upon a set of open standards4, any application that supports these standards can integrate with CardSpace. Microsoft actively promotes the standard and works together with the open-source community to ensure that coexisting and interoperable implementations are created.

4.2.1 Registration

The end user maintains a “wallet” of Info Cards that is maintained on the user’s device (desktop PC, laptop or mobile device). This wallet can be compared directly with a physical wallet, containing any number of credit cards, debit cards or identity cards. Info Cards basically come in two flavours:

1) *Personal Cards*, or “self-issued” cards, are created by the user and can contain any information that the user desires to disclose about him/her. Since these are self-issued claims, they have value only for low-security scenarios such as providing user-profile information to web sites or an OpenID transaction (see chapter 4.1).

[4] In particular, CardSpace uses the Web Services protocol stack, which consists of a number of open standards (WS-Security, WS-Trust, WS-MetadataExchange and WS-SecurityPolicy).

2) *Managed Cards* are created and maintained by an external identity provider and have to be verified by a third-party. These can be considered “digital credit cards” or “digital identity cards”. Managed Cards can be used as a secure authentication or electronic-signature mechanism.

4.2.2 Transaction

The Info Card “wallet” is otherwise known as a “card selector” and plays an important role in any CardSpace authentication transaction. The figure below depicts such a transaction:

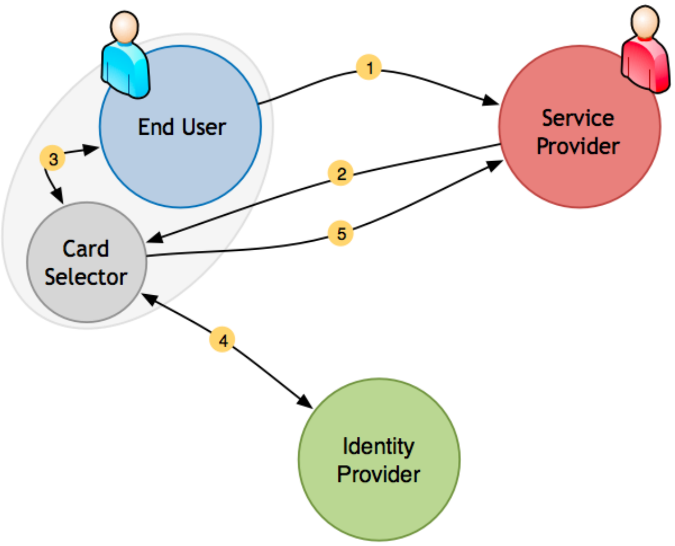


Figure 9: The CardSpace authentication sequence

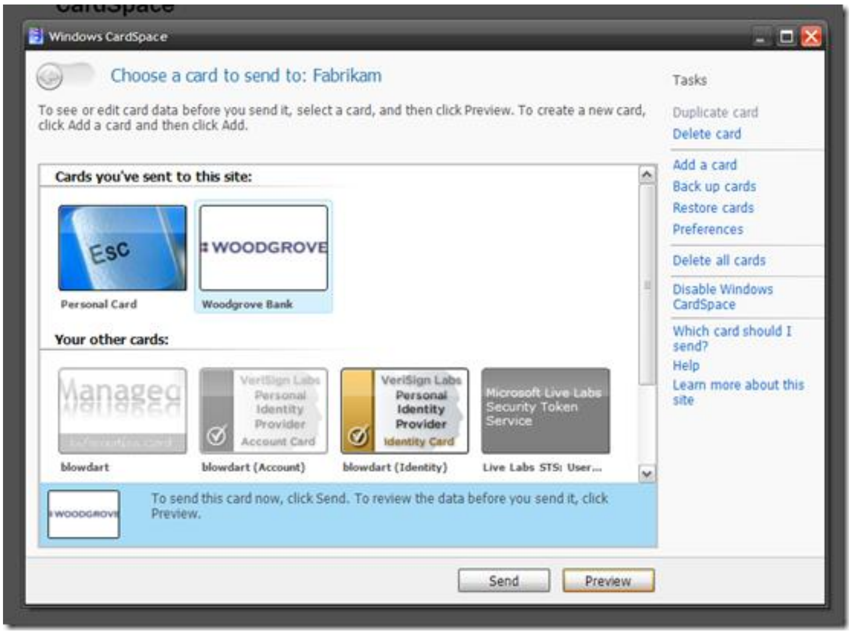
The CardSpace authentication sequence starts when the user attempts to access a protected resource at the service provider’s web site (step 1). In order to allow access, the service provider requests a number of claims from the end user. The relying party informs the card selector of these claims (step 2).

Based on the requested claims, the card selector determines which Info Cards, present in the wallet, are suitable to fulfil these claims and presents a list of these cards to the user. The user subsequently picks a card to be used in the transaction (step 3).

The selected card determines which identity provider must be consulted to validate the claims present on the card. The card selector requests an encrypted and signed message containing these validated claims. This message is called a “*security token*”. The token, holding the claims, is returned to the service provider for verification and subsequently allows the user access to the requested resource.

CardSpace does not recognize a separate “e-identity broker”, since all traffic is routed through the user device. One could thus state that the user himself acts as a broker, since it is the user who selects the appropriate identity provider by selecting a specific card. Microsoft has attempted to act as “the mother of all brokers” in the Microsoft Passport project (now ‘renamed’ Windows Live ID). However, this initiative has failed completely since the market did not want to trust Microsoft in such an important role. Microsoft has learned from this experience and designed CardSpace around the user instead of attempting yet another broker function.

The card selector is available in Windows as an integrated feature (see figure below). The open-source community provides some card selectors for the Firefox browser, Apple OS/X and Linux.



Windows CardSpace

Choose a card to send to: Fabrikam

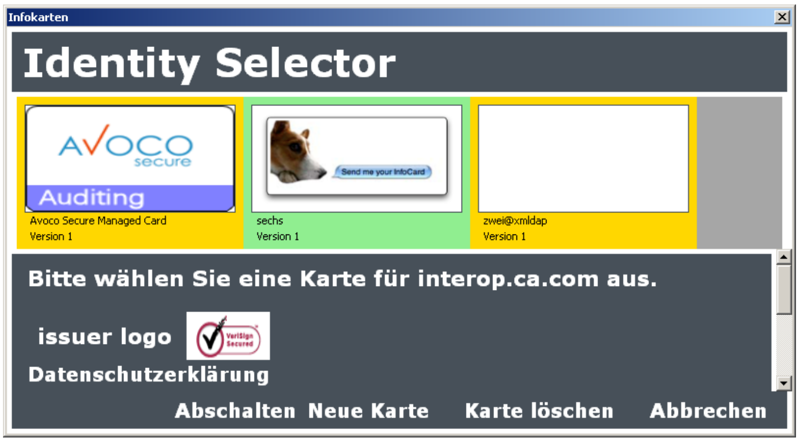
To see or edit card data before you send it, select a card, and then click Preview. To create a new card, click Add a card and then click Add.

Cards you've sent to this site:

Your other cards:

To send this card now, click Send. To review the data before you send it, click Preview.

Figure 10: Windows CardSpace card selector.

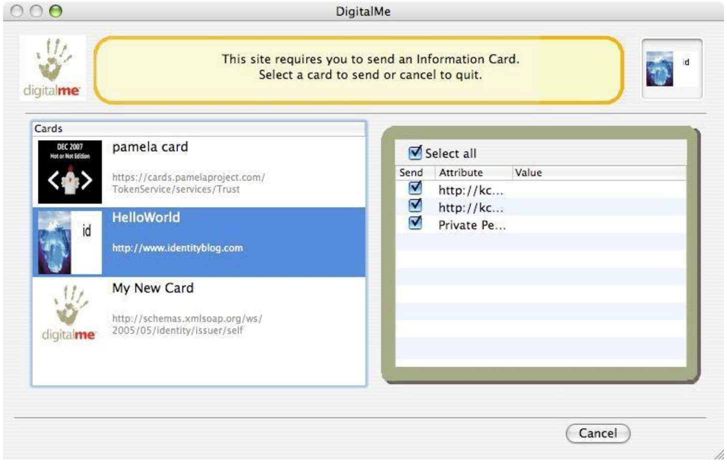


Infokarten

Identity Selector

Bitte wählen Sie eine Karte für interop.ca.com aus.

Figure 11: Card selector for Firefox



This site requires you to send an Information Card.
Select a card to send or cancel to quit.

pamela card
https://cards.pamelaproject.com/TokenService/services/Trust

HelloWorld
http://www.identityblog.com

My New Card
http://schemas.xmlsoap.org/ws/2005/05/identity/issuer/self

☑ http://kc...
☑ http://kc...
☑ Private Pe...

Figure 12: And a card selector for Apple OS/X

4.2.3 Business Model

The CardSpace scheme places the user in the driver seat. Instead of requiring the user to keep track of multiple authentication profiles at various sites (each with possibly conflicting requirements), the user can select the most suitable Info Card for each authentication request. Although the need to remember usernames and passwords does not go away, the entire authentication process becomes more transparent from the user's point of view. Even better, the user has the option to mix and match the best fit for each authentication request, thereby remaining in full control at all times.

Even though the user might be requested to authenticate when contacting an identity provider, the number of different authentication mechanisms to manage is now directly related to the set of Info Cards that the user holds and is no longer a function of the service providers that the user attempts to access. This scheme can be compared directly with the use of "physical" Credit Cards or Bank Cards: even though each card requires a separate PIN code, the user relies on a limited number of cards to conduct transactions at a large number of different facilities.

The seven laws of Identity

Following the failure of Microsoft Passport as an infrastructure for Internet-wide authentication and identity management, Kim Cameron, a security architect working for Microsoft, has devised a set of rules applicable to an Internet-wide identity ecosystem. Following is a summary of these rules, which are otherwise known as "*the seven laws of identity*":

1 *User control and consent*: the user must be able to self-manage the use of his or her identity information.

2 *Minimal disclosure for a constrained use*: the user does not have to provide any more information than required for successful execution of the service requested by that user.

3 *Justifiable parties*: identity information must only be provided to relevant and trusted parties.

4 *Directed identity*: an identity system must support identities for large-scale, general use as well as specific, directed use.

5 *Pluralism of operators and technologies*: the identity system can be implemented and supported by different parties.

6 *Human integration*: the presentation and use of identity related information must be unambiguous and user-friendly.

7 *Consistent experience across contexts*: the identity system must provide a consistent user experience, independent of technologies and services.

The CardSpace scheme facilitates loose coupling between users, service providers and identity providers by means of the broker function of the card selector. Service providers simply have to issue a set of required claims and do not depend on a particular mechanism in order to fulfil these claims. The card selector, in combination with the identity providers, perform the role of translating claims into security tokens and provide an open standards based, secure token verification facility which is independent of any particular combination of service provider and identity provider. Authentication is effectively “externalized” from the service providers.

CardSpace seems to be designed with the user strongly in mind. It is unclear how the service provider fits in: does he have an attractive enough proposition? Does he have to contract with Info Card provider, similar to credit cards or banks? That aspect gives Info Card limited network scalability since the service provider is never sure he can address every end user who uses CardSpace. As of this moment, there are no major Card Space implementations present on the Internet. Even Microsoft does not offer it as an option on their community sites. Although some implementations were attempted back in 2007 (e.g. the German retailing giant OTTO used to have a CardSpace implementation), most of these initiatives are no longer active today.

The STORK project

The aim of the STORK project is to establish a European eID Interoperability Platform that will allow citizens to do transactions and communication across borders, by presenting national eIDs.

Cross-border user authentication for such e-relations takes place in the project by means of five pilot projects using existing government services in EU Member States. In time however, additional service providers should become connected to the platform thereby increasing the number of cross-border services available to European users.

Thus in the future, a citizen should be able to start a company, get a tax refund, or obtain university papers without physical presence. To access these services one enters personal data using the national eID, and the STORK platform obtains the required guarantee (authentication) from the respective government.

The role of the STORK platform is to identify a user who is in a session with a service provider, at a defined (and cross-national) trust level, and to send the identification to this service. Whilst the service provider may request various data items, the user should be in control of the data to be sent. The explicit consent of the owner of the data, the user, is always required before data can be sent to the service provider, which fits various EU privacy regulation. In this respect STORK can be said to be user centric, since the user acts as the broker of identity data.

More information: *www.eid-stork.eu*

4.2.4 Privacy & Trust

The advantage of the CardSpace model is that it almost perfectly fulfils all of the seven laws of Identity (see frame “*The seven laws of Identity*” on the previous page). By putting the user in the middle of the transaction, he/she has optimal control over privacy and can determine exactly which information to disclose to service providers.

CardSpace offers two levels of trust:

1. *Personal Cards* provide a low-level of trust in return for user convenience and can be used to provide e.g. profile information in low-security contexts, such as the provisioning of customisation information to social networking sites.

2. The concept of *Managed Cards* provides the required level of trust to conduct business transactions between service providers, the user and identity providers.

It is striking to notice that to date there are few e-Identity services that actually use CardSpace although cases in which privacy is considered paramount would seem logical applications. A case in point here may be the EU STORK project which addresses cross-national eID subject to privacy regulation; see the text box on STORK.

4.3 Google Apps

Back in 2006, Google introduced their cloud-computer offering, Google Apps, as an evolution of the popular Gmail webmail application. Google Apps offers a growing number of business productivity tools (mail, calendar, documents, groups and more). Google Apps are "true" cloud applications, meaning that the applications are hosted by Google, including all associated data and are offered as a set of services, accessible by means of only a web browser. Users need a subscription from Google and in return receive the rights to use the services. Thus, Google Apps can be considered a service provider in a two-party network.

Since Google has made the underlying Google Apps engine available to software developers, the number of available applications that run on the Google Apps framework is growing rapidly. Starting from March, 2010, Google provides an on-line marketplace of available applications at http://www.google.com/enterprise/marketplace. At the time of opening this marketplace, approximately 50 vendors had application offerings available, targeted at the 2 million organisations using Google Apps (with a total of over 25 million users).

What makes the Google solution interesting in the scope of this document is an associated service, Google Accounts, which utilises the Google account database to act as an identity provider as well as a service provider. Google Accounts utilises the OpenID protocol (see chapter 4.1) for this purpose and can thus be considered a "regular" identity provider in an OpenID network. Furthermore, Google combines OpenID with the OAuth protocol, which allows a user (with a Google account) to authorise a third-party service provider to use Google services on behalf of that user. The key feature of OAuth is that this authorisation process does not disclose any account information to the third-party service provider.

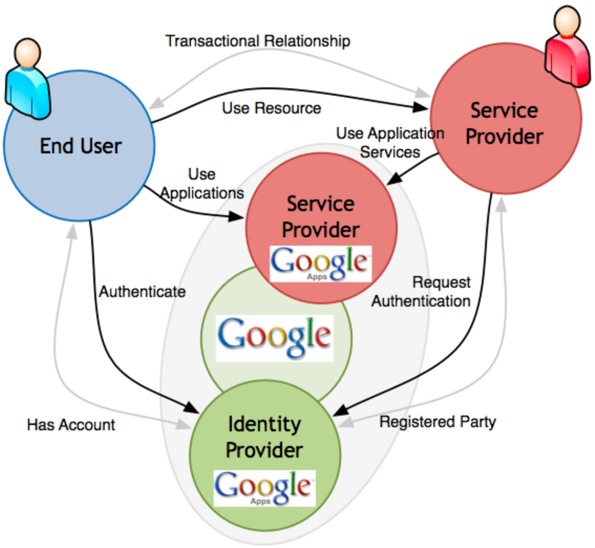


Figure 13: the Google Apps combined authentication and authorisation model

The solution depicted above positions Google as an identity provider, in which case access to Google Apps (or services provided by third-party service providers) is governed by the Google Accounts database. Google offers a second solution, based on the SAML open standard, in which case the roles are reversed: Google acts as the service provider and a third-party has the identity provider role. Users trying to access a Google Apps application are now authenticated against an external identity store, managed by a third-party identity provider. In the scope of this paper, we only consider the case in which Google acts as an identity provider.

4.3.1 Registration

Google differentiates between Google Apps “Standard Edition” and “Premier Edition” (as well as some special editions for the educational, governmental and non-profit markets). Standard Edition is free and is targeted towards individuals or home users and offers basic messaging, collaboration and document processing. The Premier Edition requires an annual subscription fee and provides access to the full suite of applications, provides large amounts of storage space and is targeted to commercial users. All Google Apps subscriptions are acquired on a per Internet domain basis (e.g. “mycompany.com”). Google facilitates self-service of domain accounts and prevents domains from accessing each other’s information.

Any user with a Google account (either Standard or Premier Edition) can utilize Google Accounts as an OpenID identity provider, e.g. they can authenticate to any web site that utilizes the OpenID protocol by providing their Google account identifier as an Open ID. Also, any user with a Google account can request service access from third-party service providers by means of combined OpenID authentication and OAuth authorization. For the OAuth authorization to work, the third-party service provider has to be registered at Google. Registration implies that certificates and shared secrets have been exchanged beforehand since these are required by the OAuth protocol to establish the necessary trust between identity provider and third-party service provider.

4.3.2 Transaction

Assuming the user wants to access services provided by a third-party service provider and these services in turn require Google Apps services then the transaction might look as depicted below:

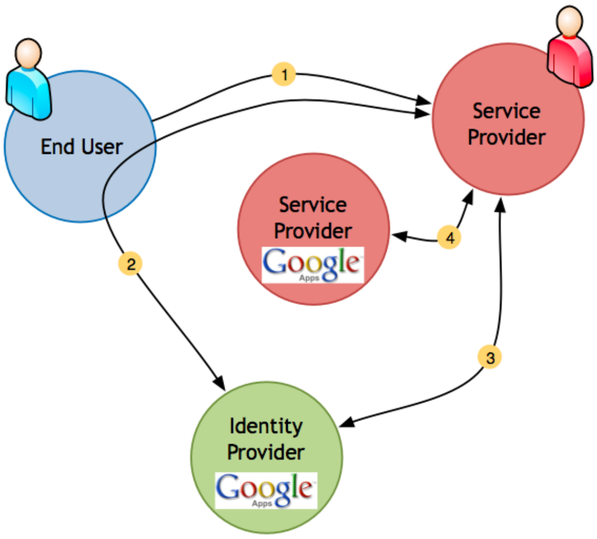


Figure 14: The Google authentication + authorisation transaction

The authentication sequence starts when the user attempts to access a resource at the third-party service provider's web site that requires additional services from Google Apps (step 1).

The user selects the OpenID protocol to authenticate, using his Google account. The service provider redirects the user to Google for authentication (step 2). This process utilises the standard OpenID protocol as described in chapter 4.1.2. However, as part of the "shared secret" information exchange (step 3 in the OpenID transaction), the third-party service provider requests an OAuth "Request Token". The OAuth protocol uses these tokens to validate the credentials of the third-party service provider, based on pre-registered certificates. Assuming that validation proves to be successful, the request token is returned to the third-party service provider together with the user identity (the result of the OpenID authentication).

Request tokens do not provide access to resources, they are only used to authenticate the third-party service provider in the context of the user session and typically have a limited validity time (e.g. 1 hour). Within this time period, the third-party service provider has to ask the identity provider to swap the request token for an "Access Token" (step 3). Access tokens have (at least with Google) an unlimited validity time and can only be revoked through the Google Apps management interface for the domain that initially requested the token. Token revocation implies that the third-party service provider has to go through the complete sequence again (authenticating the user, obtaining a request token and exchange this token for an access token). This process assures that no tokens are exchanged without the proper user consent.

Once the third-party service provider has obtained the access token, the token can be used to request Google Apps services, in which case the token acts as a "valet key", e.g. it provides limited access to a specific set of services defined by the contents of the token (step 4).

4.3.3 Business Model

Today's Google business model relies heavily on advertising services. E-identity services are currently just 'a cost of doing business'. However, in the long term this could change, when cloud-computing takes off and Google start selling to large amounts of organisations and end users. Currently, the income from Google's cloud computing ventures is minimal compared to the other sources of income. However, Google expects a massive growth of revenue in the coming 5 to 10 years, since the potential savings for end users is very high. By investing heavily in the underlying technologies, pushing standards, giving away the "Standard Edition" for free and opening the underlying Apps engine to the software developers community, Google expects to become a major player in the cloud computing arena within a couple of years.

Since the Google Accounts database is tightly integrated with the Apps engine and contains tens of millions of accounts, it makes sense for Google to use the contents of this database for additional purposes besides simple authentication for their own applications. Opening the accounts database to the Internet as an identity provider places Google in a favourable position compared to many other identity providers, given the sheer number of accounts (as an example, by mid 2009 there were over 140 million GMail users, all of whom are in the Google Accounts database).

Each and every transaction that involves Google services (e.g. accessing Google search, Google Apps, GMail, YouTube, OpenID authentication, etc.) is logged and processed by Google to produce valuable marketing information, telling Google exactly what their users do and what their areas of interest are). As of 2006, the Google logging databases, not counting all applications, contained over 1 Petabytes (1.048.576 GByte) of information. By opening the accounts database to the Internet for third-party authentication and authorisation, even more valuable marketing information will be collected.

For the end user, the advantages of using only a single account for accessing cloud applications as well as logging in to hundreds (or even thousands) of web sites supporting the OpenID and/or the OAuth protocol are evident.

For third-party service providers, utilizing the massive Google Accounts database offers a unique authentication resource with a number of available accounts that would be very difficult, or even impossible, to establish by themselves.

4.3.4 Privacy & Trust

Google utilises the OpenID protocol for authentication. As stated in chapter 4.1, there is a limitation to the level of trust related to this protocol. Given that the majority of accounts that are present in the Google Accounts database are free accounts, established by the users and used to obtain access to free services such as GMail or Apps “Standard Edition”, the trust level offered by Google is currently limited to low-trust types of services.

The OAuth protocol offers a reasonable level of trust, given that all messages exchanged between service provider and identity provider are encrypted and signed by pre-registered certificates and shared secrets. The integration of OAuth with the OpenID protocol creates a higher level of trust compared to “plain-vanilla” OpenID. Also, OAuth requires service providers to be pre-registered at the identity provider, which implies that the service providers know in advance the quality and the strength of the authentication facilities offered by Google, which is an improvement over the standard OpenID protocol.

Regarding privacy: users perform “self-registration” with Google in order to obtain a Google account. With the exception of paid accounts (which are still a minority), there is hardly any guarantee that provided information is correct. Also, given that Google logs all information that flows through their systems for purpose of analysis (and potential marketing), there is a high potential for privacy violations. In their privacy statement, Google explicitly states that it claims the right to combine user information with data collected from other services with the purpose to improve products and services provided by Google to the end users. The privacy statement also states that no personal information will ever be disclosed or used, either within Google or to third parties, without the proper user consent[5]. However, it is still

[5] “Google considers the privacy of its customers important and is serious regarding data protection. Google adheres to the US Safe Harbor Privacy Principles of Notice, Choice, Onward Transfer, Security, Data Integrity, Access and Enforcement and is registered with the U.S. Department of Commerce’s Safe Harbor Program. The processes and systems related to data security and privacy protection have been successfully audited for SAS 70 Type II compliance.”

difficult (if impossible) for end users to verify that all information flowing through the Google systems is indeed protected properly against privacy violations, identity misuse or theft. This is a serious issue for organisations that consider the use of cloud applications, since they have to trust the service provider to treat the, potentially sensitive, corporate information properly according to pre-defined service level agreements (in which Google explicitly denies any responsibility beforehand and explicitly states that the services are not meant to be used for “high-risk” activities).

The OAuth protocol that is used to grant third-party service providers access to Google services offers a fair amount of privacy protection, since no account information is ever disclosed to these third-party providers. Also, OAuth assures that any user-related information that needs to be exchanged between Google and the third-party provider has to be approved by the end-user in order for the transaction to succeed.

4.4 DigiD

DigiD is a single sign-on and authentication service launched in 2003 by the Dutch government that enables legal residents of the Netherlands to use e-government services. It is mostly used to file income tax statements online with most users using it only 1.2 times a year on average. From an end user perspective it is not a great success, because the relevance in a person’s life is limited. From the identity provider point of view it is more of a success since at least 8 million people have enrolled for DigiD, because of the obligation to use DigiD for tax filing. The figure below depicts the scheme:

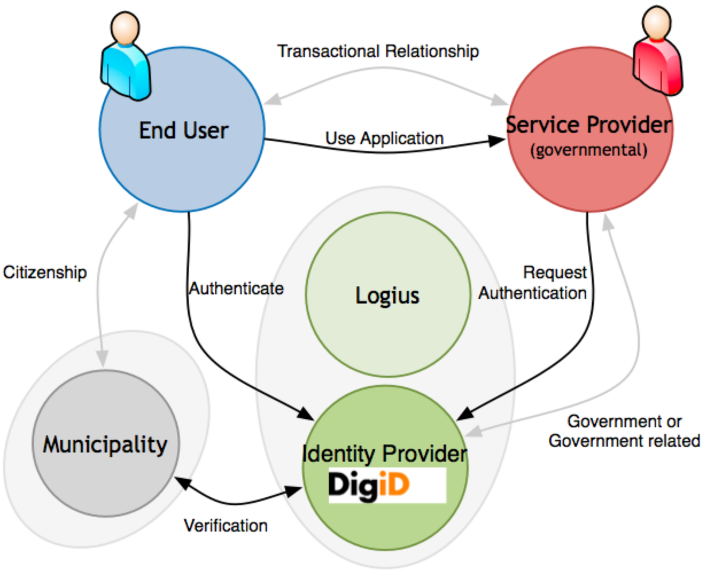


Figure 15: The DigiD authentication scheme

The DigiD Scheme operator is “Logius”, a Dutch Government Agency that is also responsible for hosting and exploitation of the DigiD application itself.

4.4.1 Registration: leveraging citizenship

Users request a DigiD through the DigiD website. The DigiD is based on the Citizens Service Number (BSN) that is issued to each legal resident of the Netherlands by the municipality in which they live and on the Municipal Basic Administration (GBA) to which the BSN refers. The GBA is regulated by Dutch law, which stipulates how the information can be acquired, altered and used. An independent body, the Dutch Data Protection Authority (CPB), oversees the GBA and its compliancy to national and international law.

The picture below depicts the registration procedure:

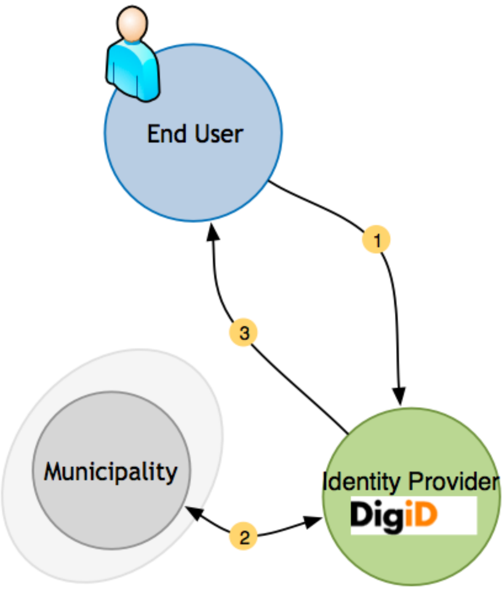


Figure 16: DigiD Registration

1) A DigiD can be requested from the DigiD website. End-users fill in their BSN, postal address and email address and can then select a username and temporary password. The account can be used from here on, but with severely limited functionality (security level “temporary”).

2) DigiD verifies the provided information against the Municipal Basic Administration (GBA) and if proved to be correct, creates the account.

3) On correct registration, an activation code is sent to the End-user’s home address by mail. This activation code has to be used at the DigiD website to activate the account. At this time, the user also has to select a permanent password. The account is now ready to be used for authentication transactions.

A key point is that the DigiD identifier is the Citizens Service Number (BSN). Only legal residents of the Netherlands are issued a BSN and only government organization are allowed to use the BSN for authentication purposes. Because DigiD is based on the BSN, any restriction applying to issuing or the use of BSN applies to DigiD as well.

Only government organizations can be service providers. This means that DigiD cannot be used for non-governmental e-services such as financial services, e-commerce or social networks. However, Dutch law is able to designate exemption and it has done so for medical insurance companies providing the mandatory basic health care insurance. Thanks to this exemption, DigiD can be used to apply for this service online or login at insurance companies.

4.4.2 Transaction

DigiD can only be used as an authentication facility. These authentication transactions are stateless, which implies that DigiD does not "remember" whether a specific user has authenticated earlier within the same browser session. The net-result is that the user will have to re-authenticate for each and every government site that the user is visiting in the same session.

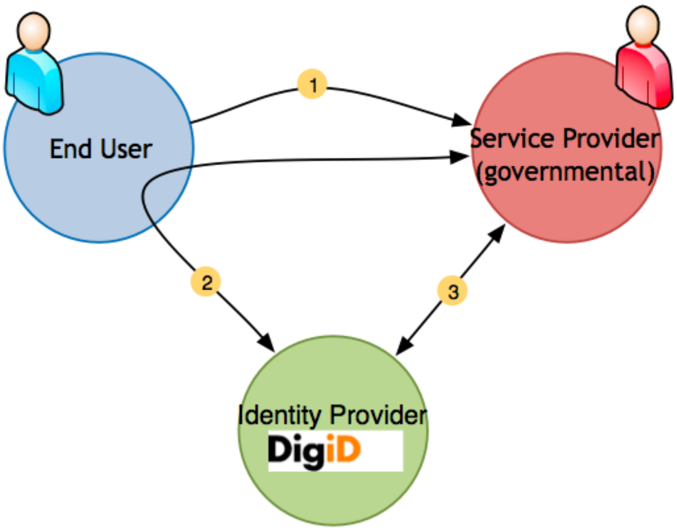


Figure 17: DigiD authentication sequence

The DigiD authentication sequence is invoked when the user visits a government web site and selects the "DigiD login" button (step 1). Selecting "DigiD login" will redirect the user to the DigiD web site for authentication using username/password (step 2). If required, the user can select a "stronger" authentication level, in which case a one-time code is sent as an SMS to the mobile number provided during registration. The user has to enter this number as part of the authentication transaction.

Assuming that authentication has been successful, the user is now redirected to the requested web resource at the service provider. In case of unsuccessful authentication, the user is left at the DigiD site to try again.

The service provider invokes a DigiD service in order to verify the authentication transaction data that has been received from DigiD and finally grants access (step 3).

Since the DigiD scheme only contains a single identity provider, there is no use for a separate e-identity broker in this case.

4.4.3 Business model: not-for-profit

DigiD is free for end users as well as service providers to use. As a government service it is a not-for-profit initiative, which is subsidized by the Dutch Ministry of Internal Affairs.

The main purpose of DigiD is to replace the many different username/password combinations that citizens required to obtain access to government web sites. Since DigiD only provides a user identifier (authentication only), these web sites still have to maintain local profiles to store all additional information they require. DigiD thus only solves part of the problem (authentication) and leaves the issues of maintaining identity assets to the local government sites.

Also, although penetration of DigiD is high, use of DigiD is limited for most users to a few occasions per year for government transactions only.

Against this background the Dutch government has started developing a new network called eRecognition[6] that allows private sector employees to access government services based on an open market for identity services. eRecognition is a based on a 4 corner model, of which the government supports the scheme, and is expected to also support B2B services.

4.4.4 Privacy and trust

DigiD differentiates between three security levels that are to be used for different types of services:

- ✓ The first level requires only a username and password (one factor authentication), and is suitable for services that require a limited level of security, privacy and trust.
- ✓ The second level requires the username and password in addition to a One Time Password (OTP) sent by SMS to the End-user's mobile phone (two-factor authentication). This level is intended to be used for services that require a high level of security, privacy and trust.
- ✓ A third level was planned and would involve a physical electronic identity card that is yet to be introduced and a face-to-face registration process. However, this program has been put on hold indefinitely.

DigiD provides limited trust, since each authentication session is only based on a transaction between the DigiD identity provider and a single service provider. Users still have to authenticate repeatedly when visiting other identity providers, even if these are also supporting DigiD. A new initiative called “mijnoverheid.nl” (my-government.nl) will improve on this situation by establishing a federation of cooperating, trusted, parties. In this case, a user who authenticated (using DigiD) with “any” service provider within this federation is allowed to travel between all service providers that are member of the federation, without the need to re-authenticate.

4.5 Estonian e-ID card

The Estonian e-ID card is a national identification card that can also be used for a whole range of online authentication services including e-government services, online banking, online financial services and e-commerce. A single ID card can be used for offline as well as

[6] See http://www.eoverheidvoorbedrijven.nl/afsprakenstelseleherkenning/english/english.html; a whitepaper on the eRecognition network approach can be downloaded at http://innopay.com/publications

online authentication. Online, the card can also be used for digital signatures while offline the card can also be used at a ticket in public transportation. The digital version of the Estonian ID card is provided by Sertifitseerimiskeskus (SK, www.sk.ee) as a certificate issuing and validation service.

Around 80% of Estonians have an e-ID card and they each use it for online authentication 25 times a year on average. Compared to other Estonian authentication methods, such as those offered by banks, this figure is relatively low. The power of the Estonian e-ID service is that it leverages the identity card already mandatory for all legal residents over 15 years old. For those already owning a card, using it for online authentication is a small step.

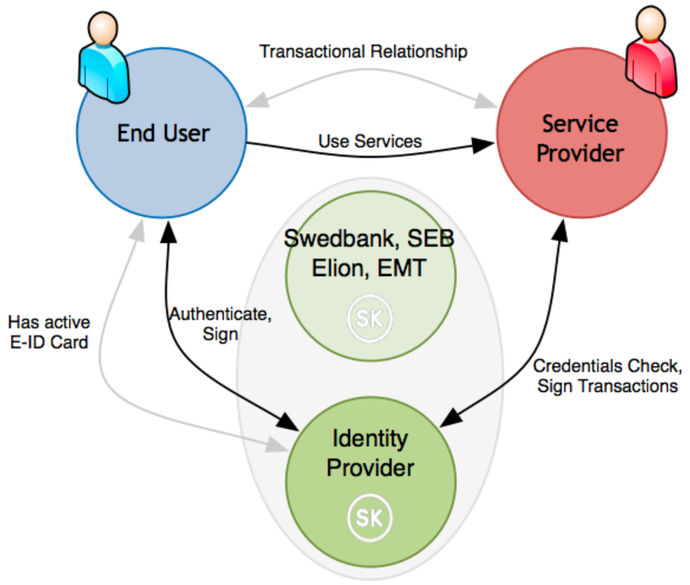


Figure 18: E-identity provider SK using the Estonian ID card

4.5.1 Registration: leveraging the ID card

Registration for the Estonian e-ID card has two parts: the issuing of the card and the issuing of the information needed for online authentication. Most often both parts will be carried out simultaneously but they can also be carried out independently.

1. **Issuing the card.** In the first part of registration the physical identity card is issued to the End user through the Citizenship and Migration Board (CMB) after a request made by the End user. The card is picked up and activated at a bank branch. The card is a standard polycarbonate card containing the end user's name, date of birth and other information in addition to a photograph of the end user. Every Estonian citizen and legal resident of the country over the age of 15 is required to have such an identity card. The card is linked to the 11-digit Personal Identification Code (PIC) that uniquely identifies each Estonian legal resident and is provided to the CMB by the Population Register of Estonia. The card also contains a microchip that can be used for electronic authentication online as well as at terminals. The creation of the card is outsourced to TRÜB Baltic, a company that personalizes cards.

2. **Issuing the digital content.** In the second phase of registration, the information on the chip in addition to other information needed for online authentication is issued. The information issued is: the digital content of the chip, PIN and PUK codes, and a national e-mail address. There are three pieces of digital content stored on the chip: basic personal data equivalent to that printed on the card, a digital certificate for online authentication, and a digital certificate for digital signatures. Both certificates contain only the End user's name and their PIC, with the certificate for online authentication also including the End user's national e-mail address. The card thus carries little authentication data and function primarily as a key to access the databases where the information is stored. Each certificate is protected by a different PIN.

   The digital content of the card is added by TRÜB Baltic. TRÜB forwards the end user's personal information to SK in order to create a database entry. Once the content is loaded onto the card, and the PIN and PUK codes have been generated, everything is sent to a bank branch for pickup.

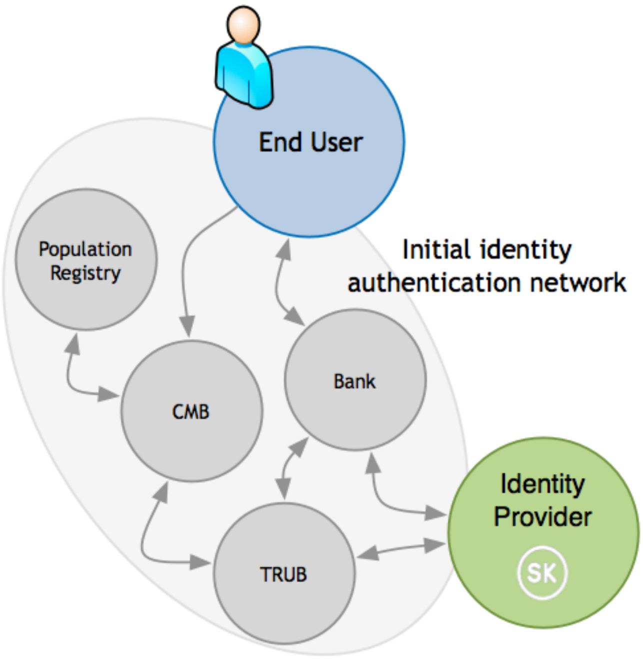


Figure 19: The registration of e-identity for SK

4.5.2 Transaction

SK serves as a certificate provider, a validation authority, maintains the technical infrastructure and develops the necessary services and software. All authentication transactions carried out by End users are routed through SK and the central directory containing all authentication data. SK is a private organization owned by banks Swedbank and SEB and telecommunication companies Elion and EMT.

All service providers connect directly to SK. To facilitate this connection, SK provides downloadable applications and requires little further technical integration.

For end users to use the Estonian e-ID card for online identification, several things are required:

- ✓ the physical e-ID card
- ✓ a PIN code (self chosen)
- ✓ a username (self-chosen, can vary across services)
- ✓ a card reader connected to the computer
- ✓ software installed on the computer.

An end user can initiate a transaction on any website connected to the service.

4.5.3 Business model

For End users, acquiring the physical e-ID card costs approximately EUR 10. Updating or changing authentication related information such as PIN codes or certificates is free of charge at the Citizenship and Migration Board while SEB and Swedbank bank branches charge a small fee of approximately EUR 2-4. Card readers can be purchased at SEB and Swedbank branches for approximately EUR 6. Aside from these small set-up fees, the service is free for End users.

Service providers pay a monthly fee for the service. This fee ranges from EUR 25 for 400 transactions per month to EUR 6,000 for 750,000 transactions per month. The price is therefore between 0.008 and 0.06 EUR per transaction, which is substantially lower than other electronic transaction services such as online payments. A six-month 8.000 transaction starter's package is free of charge.

4.5.4 Privacy and trust

With the exception of the CMB, all parties involved in the issuing of the card and digital content are private entities. This may raise concerns over security and trust. In Estonia, all public and private organizations are subject to the Personal Data Protection Act that regulates the use of personal data and databases containing personal data. Adherence to the Act is overseen and enforced by the Estonian Data Protection Inspection.

The Estonian e-ID card uses two factor authentications: the combination of the PIN and the card. As the personal information contained on the card is considered public information in Estonia, the card does not contain any private data. It functions only as a key to access the central database. Thanks to the two factor authentication, a stolen card does not give access to online services. The PIN code is self-chosen but cannot be easily altered.

4.6 BankID

BankID is a Swedish e-identity solution developed by Swedish banks that was subsequently expanded to become an authentication mechanism for a variety of e-services. These e-services range from online banking to e-commerce and e-government. BankID is issued by banks to their internet customers. Today 10 banks are issuing BankID and 2 million BankID's have been issued of a potential market of 5 million online bank users.

BankID's main usage is for financial transactions (around 50% of the transactions) and e-government transactions (40% of the transactions). The remainder is for transactions with private companies and this percentage is growing. Today BankID has 10 million transactions monthly. BankID has two usage modes: authentication and digital signing.

The power of BankID is that it is an open and scalable network allowing any consumer and any type of e-service provider to easily get access to the service and the entire network. Also, it leverages existing and trusted credentials.

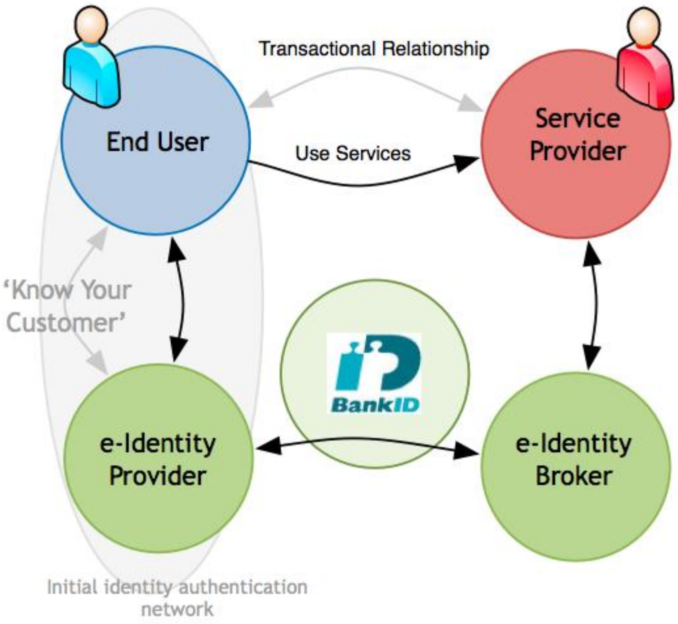


Figure 20: The four corner network of BankID

Figure 20 shows clearly that the roles are similar to the ones depicted in the generic e-identity three-corner model, but that one corner is split in two. Since there can be multiple e-identity providers and e-identity brokers, interoperability and scalability needs to be ensured by the independent scheme organisation.

4.6.1 Registration: leveraging an existing relationship

One of the most important aspects of BankID is the way the identities are provided; by banks to their account holders. This enables secure authentication, the leveraging of an existing infrastructure and enabled the achievement of critical mass.

Banks generally have long lasting relationships with their account holders and know a great deal about them. Users can only open a bank account after making a physical appearance at a bank and offering some form of identification. Banks are also required to comply with 'Know Your Customer' (KYC) and anti-money laundering regulations that requires banks to know who they are dealing with. These regulations were put in place to prevent financial crime and to prevent financing of terrorism.

Since most Swedish banks participate, critical mass has been reached for further growth.

4.6.2 Transaction: scalable 4-corner model

In BankID, the role of identity provider has been decentralized to create a quickly scalable four-corner model. The transactions are routed from the end user to the service provider, via the e-identity broker and the e-identity provider.

The role of the single identity provider has been split into three roles. The reason for this is scalability. In a three-corner model, all end users and relying parties must maintain a technical connection and legal relationship with the same party. In small markets this may not pose a problem, but it can stifle growth.

In a four-corner model, the role of the identity provider is split allowing end users to receive their credential from their identity provider of choice. The service providers forwards the credentials received from the end user to the e-identity broker for authentication. The service provider only has a relationship with the e-identity broker and not with the e-identity provider.

The advantage of the four-corner model is that each actor in the network only needs to connect to one other actor, even if the service grows very rapidly. The network is therefore highly scalable.

The BankID network runs on a single infrastructure owned by the major banks. The Swedish Payments Clearing Housing BGC handles the operations of BankID.

4.6.3 Business model

For banks the services strengthen their position as trusted party for end users and service providers. Banks do not need to maintain their owned identity infrastructure, once they issue BankID's. The end user does not pay for the basic service separately; it is part of the online banking service. However, additional services are charged to the user. The service provider pays- and the e-identity provider receives a fee for each transaction. It is a 4-party model with bilaterally agreed interchange fees.

4.6.4 Privacy and trust

BankID is based on electronic signatures. Transactions with BankID are legally binding throughout the EU, since BankID issuers serve as certificate authorities who are bound to strong legal requirements regarding security, privacy and trust.

BankID certificates come on USB devices, smart cards and just recently on mobile phones.

4.7 SURFfederatie

SURFfederatie is an initiative of the Dutch organisation SURFnet. SURFnet is a subsidiary of the SURF foundation, in which Dutch universities, universities for applied sciences and research centres collaborate nationally and internationally on innovative ICT facilities.

The SURFfederatie is a federative, multi-protocol[7], authentication facility, which has been established to facilitate students and staff to access services provided by various educational institutions as well as a selection of third-party service providers.

In the past, students who wanted to use services from different institutions were required to have multiple accounts, one at each institution they wanted to access. Since students are increasingly using facilities of different educational institutions, this situation needed to improve. The SURFfederatie facilitates access to various service providers (including third-party commercial organisations, educational organisations and research centres), using only one single account. The role of identity provider is assigned to the "native" institution of the student, e.g. the institution at which the student is registered.

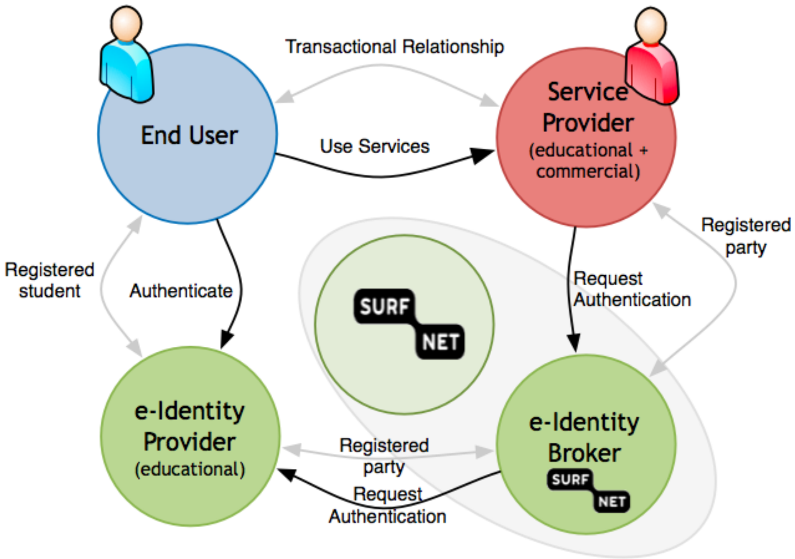


Figure 21: The four corner network of the SURFfederatie

Similar to BankID, the SURFfederatie is implemented as a four-corner model, in which SURFnet acts as a broker and protocol translator. The SURFfederatie allows different federation protocols to be used by both the service providers and identity providers.

4.7.1 Registration: leveraging an existing relationship

The federation utilizes the existing relationships between the student and the educational institution at which the student is registered. The advantage of this approach is the availability of critical mass, utilization of existing trust relationships between student and educational institution and reuse of existing infrastructure (especially important given the large amounts of changes occurring each year as students graduate and new students arrive).

In order to connect to the federation, all providers are required to establish a contract between the provider and SURFdiensten (a subsidiary of SURF and responsible for all products and services provided by the SURF organisation). When the contract is in place, the

[7] Since different service providers and identity providers might utilize different protocols, a unique feature of the SURFfederatie is its capability to act as a broker and protocol translator. Currently, the federation supports the SAML 2.0, WS-Federation, A-Select and Shibboleth federated authentication protocols.

provider can utilize one of the supported protocols to establish the technical connection. By supporting multiple protocols, the barrier for providers to connect to the federation is kept low.

4.7.2 Transaction: scalable 4-corner model

The SURFfederatie utilizes an award winning[8], decentralised, distributed model for identity providers and service providers. This approach facilitates a scalable four-corner model (see also chapter 4.6.2 for a description of the advantages of this model). The transactions are routed from the end user to the service provider, via the e-identity broker and the e-identity provider. The e-identity broker also performs protocol translation, thereby facilitating providers to connect using different protocols.

4.7.3 Business model

Educational institutions leverage their existing infrastructure and position as trusted party for end users and service providers. Without extensive changes in account management, students can access services from multiple service providers. The federation thus provides a compelling business proposition to both the educational institutions (who can offer a large set of services to students) as well as third-party service providers (who get access to a large potential customer base without the need to invest in an expensive identity management infrastructure).

By supporting multiple protocols, the extra cost for providers to establish a connection to the federation is kept low, thereby providing an extra stimulus for providers to connect and thus pushing both the number of potential customers as well as the services offered to those customers[9].

Connected parties (service providers and identity providers) pay a fee to SURFdiensten for services obtained. These services include the use of the federation and development of new and/or updated features.

4.7.4 Privacy and trust

The federation builds on the existing trust relationship between students and educational institutions. In many cases, identity information does not need to leave the institution (e.g. the fact that a student is registered at an institution might be sufficient proof to obtain access to a service).

An additional level of trust is provided by the contracts between providers and the SURF foundation, which assures that all communication between providers and the federation adheres to the strict policies implemented by SURF. A high level of trust exists between the institutions and the SURF foundation, given that the joint universities founded this

[8] In 2008, SURFnet and Everett have received the eema Award for Excellence for the SURFfederatie solution.

[9] To illustrate the success of this approach, in February 2010, Google has signed a 3-year agreement with SURFdiensten to connect to the federation and make available the Educational Edition of Google Apps, as well as all third-party applications offered through the Google Applications Marketplace, to all connected educational institutions. Google uses their SAML-based single sign-on facility (see chapter 4.3) to establish the role of service provider with external identity providers.

foundation in 1987. Today, the foundation represents over sixty institutions (academic universities, universities of applied sciences, research centres and centres for documentary information services).

5 Conclusions

The e-Identity business is still in its infancy and it has often been a case of trial and error when starting a service in this area. For achieving success, it is clear that scale, in terms of the number of transactions and number of participants, is a major factor. In that sense most initiatives discussed can be said to be successful, although the usage of dedicated government initiatives and of the pure user centric approach of Cardspace is, to date, limited.

Based on the analysis of e-identity as a two sided market, serving end users on one side and service providers on the other, various aspects appear crucial in setting up a successful e-identity network. We have listed the cases of this report in the table below to provide an overview of key aspects.

	OpenID	CardSpace	DigiD	Estonian e-ID	Google	BankID	SURFfederatie
	OpenID		DigiD Digitale Identificatie	SK	Google Apps	BankID	SURF NET
Domain	Technology, web 2.0 / social	Technology, user centric	Government, easy to use, only for citizens	Government, trusted transactions	Cloud computing, SaaS	Re-use what's already there, private and government sector	Re-use what's already there. Educational sector
Network model	4 corner, Internet DNS acts as broker	3 corner, user acts as broker	3 corner	3 corner	3 corner	4 corner	4 corner
Registration	Mostly self registration	Depending on InfoCard scheme	Local government	Local government, certificates	Self registration	Bank issued	Issued by educational institutions
Transaction	Authentication, profiling	Card dependent	Authentication	Authentication, signing	Authentication, authorisation	Authentication, signing	Authentication
Business Model	Low-cost trust, more traffic	Currently only technology	Subsidised, government only	Wide range of transactions	Advertisement, generating more traffic	Wide range of transactions	Wide range of transactions
Privacy & Trust	Minimal trust	User centric, privacy control	Government controlled	Government controlled	Google policy regulated privacy	Government and bank regulated	Educational sector regulated
Take away	Fits well for large-scale, limited trust networks.	User centric, technology driven, still to be proven	High penetration, limited usage for citizens	Re-use government-ID for private transactions	World domination through attractive applications	Re-use bank-ID for private and public transactions	Restricted to education, high usage.

Figure 22: Overview of e-Identity initiatives

Conclusions that can be drawn from the various cases investigated are

1. In terms of solutions, there is no one size fits all. E-identity is used for many situations with different risks, trust and user profiles. From a privacy point of view it makes sense to have multiple identities, per usage context. Hard privacy guarantees cannot be given from a technology point of view only. This is why the scheme holder must be a trusted party. What lacks in terms of convincing end users about their security and privacy may be solved by technology only if the transactional stake is limited. This is exemplified by the loose coupling between service providers and identity providers in common OpenID and CardSpace scenarios where little trust exists between the parties in the network and consequently the transactions served are perceived to be of limited risk.
2. The cost of the identity administration process and the handing out of means of authentication, needed to establish trust for individual transactions, is a major factor in the business model. Successful sharing or transferral of that cost is key in any e-identity network. This is illustrated in some of the cases that reuse existing administration processes and authentication means, e.g. by government (DigiD, Estonian e-ID Card), banks (BankID) or the educational sector (SURFfederatie).
3. E-identity seems to be underestimated as a two sided market serving end users on one-end and service providers on the other. An important aspect of a two-sided market is that the propositions should be attractive to stakeholders at both ends. Successful larger scale solutions do address this aspect and these can be, in the context of the framework proposed, 3 or 4 corner models. In contrast, an initiative such as CardSpace seems to focus on the end user only, providing a less clear business case to service providers.
4. Interoperability of e-identity solutions is the way forward for mass adoption. End-users and service providers do not want to be bothered with the selection problem of which technology or solution is the best. They just want a service delivered. The EU STORK initiative (see text box in paragraph 4.3) clearly has this in mind from a cross border perspective. A private solution such as Google's mitigates this by providing multiple standards, including OpenID and SAML2.0, to bridge the gap between services and communities. Another good example is the SURFfederatie, which offers multiple protocols for providers to utilize, thereby significantly reducing the cost and effort to connect.

Finally, we want to propose a thesis:

> *In successful e-identity networks, the business case and the gain for each party (identity providers, service providers, users) is transparent to all parties.*

If there is widespread doubt on what gain (money or otherwise) some party in the network takes from it, trust in the network will erode and it cannot scale towards higher value transactions. This may be the reason why some of the more successful initiatives have a government supported scheme, which, at least in Europe, appears to provide the required trust. However, the amount of interaction of citizens and companies with governments is limited and involvement of the private sector is crucial for widespread adoption and growth of e-Identity.

6 About Innopay

Innopay is an independent full service consultancy firm specialised in payments and related transaction services. Our key practices include online payment, e-invoicing, e-identity, mobile payment, cards and related regulation.

Given our independent position, we work for all players in the industry. We devote research time and investments to help peer professionals ‘structure & understand’ these topics and actively facilitate industry knowledge transfer, which we consider crucial for the further development of global e-business. Our leading industry reports can be downloaded from www.innopay.com.

With our in-depth knowledge and experience gained on both the demand side and the supply side, we are ideally positioned to help our clients determine the direction of their growth. This often results in new products and/or markets that we successively help to ‘develop & manage’ and bring to market in a controlled and effective way. We do this for single clients but also for groups of clients. Consequently, we have extensive experience in developing multi-party transaction schemes and accompanying messaging standards in diverse industries such as financial services, insurance and document exchange.

On the other side, we help corporate users to ‘choose & use’ the transaction services that fit their specific business needs from the wide array of often industry tailored transaction services on offer. We use a multi-disciplinary approach covering commercial, operational and technical aspects.

Innopay is a member of the European Payments Consulting Association (EPCA) and the Payment Systems Market Expert Group (PSMEG) of the European Commission and an associate member of the Euro Banking Association (EBA).

For more information visit www.innopay.com or mail to info@innopay.com

7 About Everett

Everett (www.everett.nl) is a systems integrator and consultancy firm specialized in interaction, identity and integration. Everett has offices in Nieuwegein (Netherlands, head offices), London (UK), Milan, Rome (Italy) and Bangalore (India). Everett also provides 24x7 solution support services via its ESSC support centre. Since its inception in 1999, Everett has proven itself as a leading specialist on identity enabled services and middleware in general, and portal, secure remote access, identity & access management, IT compliance and service oriented integration technology in particular.

Our aspiration is the ‘identity enabled’ enterprise, with its strategic objective of facilitating secure, personalized and integrated ICT services with a minimal time-to-service. Implementing these identity enabled services poses a challenge for the modern day ICT organisation since it has to find a cost effective balance between user demand, organisational goals and rules and regulations. Everett’s core activity is assisting organisations in this area with consultancy, implementation skills, knowhow and solution support.

In the past ten years, Everett has realised a large number of projects. We are active in a number of different business domains such as Education, Research & Development, Telecom & Media, Finance, Transport & Logistics, Government, Energy, Manufacturing and Healthcare.

Customer projects include the whole range of identity & access management infrastructure, and the realisation of personalized web portals and composite applications, using Service Oriented Architecture and most of the of Web 2.0 technologies. At the core of all of these projects is an agile project approach aimed at producing immediate business value in the context of a long-term vision and target architecture.

For more information visit www.everett.nl, or mail info@everett.nl.