innopay

Triport 3
Westelijke Randweg 43
1118 CR Amsterdam Airport
The Netherlands

PO Box 75643
1118 ZR Amsterdam Airport
The Netherlands

+31 20 6580651
info@innopay.com
www.innopay.com

Member of European
Payments Consulting
Association, EPCA
www.epca.de

National Institute of Standards and Technology

Att. of Mr P. Gallagher

100 Bureau Drive, Mailstop 8930

Gaithersburg, MD 20899

USA

Amsterdam Airport, 22 July 2011

Subject: Response to Notice of Inquiry on NSTIC Governance

Dear Mr Gallagher,

Innopay is grateful for the opportunity to respond to the Notice of Inquiry on governance models for the NSTIC.

Our expertise gained in this specific domain in recent years seems very relevant. We have been -and still are- active in promoting a 2-sided market approach to the e-identity challenge. We recognize many aspects of such an approach in the underlying vision, positioning and guiding principles as set out in the NSTIC, and in many of your questions as formulated in the Notice of Inquiry, albeit implicitly.

You may be aware that in the Netherlands we have been deeply involved in the conception, development and implementation of an e-identity ecosystem called 'eHerkenning' (in English 'eRecognition'), an initiative of our Ministry of Economic Affairs, Agriculture & Innovation. The eRecognition scheme (live since April 2010) is an inclusive model for (existing) e-identity providers and e-identity brokers to provide e-identity services to end users on both sides of the e-identity market, based on a level playing field. All private sector participants work together on agreements on the inter-related topics that a scheme entails: Business/governance, application/functionality, infrastructure/technology.

A first observation we would like to make is the excellent way the NSTIC is scoped and positioned. We commend the holistic and national positioning (C2G,C2B, B2G, B2B), as well as the fact that the ownership and lead is so clearly put in the hands of the private sector. Starting with consumer use makes sense, as it unlocks the volume that providers seek: a prerequisite for the market to take off. We also share the view of not taking a National ID card as a starting point, but rather create an ecosystem for (existing) ID solutions of which a national ID card can become one. In our opinion this is exactly the right scope and positioning. It also is ambitious.

A second observation is that the e-identity ecosystem as described in the NSTIC, has all the characteristics of a '2-sided market'. Our suggestion would be to review the NSTIC along the principles of 2-sided markets. The NSTIC has already implicitly included many of these principles, but we suggest making these more explicit. This would include:

- **Defining and separating a 'collaborative' and a 'competitive' domain**, where a scheme (or a trust framework) is agreed for the collaborative domain and participants in the scheme compete with services provided to end users on both sides in the competitive domain.
- **Adding the role of 'e-identity broker' to the ecosystem**, making the ecosystem a generic '4-party model'. This guarantees scalability of the network by aggregating all e-identity providers in the network towards relying parties, who can then connect with a broker of their choice. Vice versa, all e-identity brokers in the network are aggregated towards consumers/companies, who can use a single e-identity provider of their choice.
- **Develop a 'single scheme' rather than multiple 'trust frameworks',** as this will further minimize fragmentation, one of the key challenges in this domain, and one specifically addressed by NSTIC. It is our experience that all industry requirements can be met by introducing multiple 'levels of assurance' in a single scheme which includes multiple e-identity tokens.

When doing so, we would recommend specific attention is given to some insights the eRecognition project has provided us, Innopay:

- **Take a holistic approach, include all user segments and industries in scope,** as e-identity touches almost everything in society and cyberspace. In this respect the NSTIC is better positioned at the start than eRecognition was. However, as eRecognition started with the most complex use case of B2G, it includes many solutions (e.g. power of attorney registries) to problems that will only be encountered at a later stage when starting with consumer use. Designing for this future functionality right from the start is key, as designing it in later is almost impossible.
- **Ensure adoption by the larger government agencies**, such as the Tax Authority, and participation of the larger e-identity providers such as banks and telecom operators. In order for the network to scale and become economically sustainable, their adoption/participation is needed, and should be timed well. E-identity is a 'chicken and egg' problem!
- **Address the creation of a business model right from the start**, despite the sensitivity of the subject. It is essential for creating the right incentives for participants to join, and create network effects that drive growth and use of

the network. Be lenient in allowing exploration of such business models within the transparency of the collaborative development process. Getting a business model in later is extremely difficult.

- **Assume a guiding, monitoring and facilitating role** in the development and governance process. Leave the scheme development and governance decisions to the participating parties. Once in the process together, the participants have the incentives to reach agreements and are best positioned to evaluate the impact of such decisions and optimize accordingly. The government has a crucial role to play at the start: bringing parties together, provide 'neutral ground'.

With regard to the governance of such an ecosystem, we would like to bring forward four success factors which we have identified based on our experience in the development and subsequent governance of 4-party model based schemes for 2-sided markets, in e-identity (e.g. eRecognition), but also in adjacent areas such as e-payment (e.g. iDEAL), e-invoicing, and charging of electric vehicles. These are:

- **Accommodate the 'order of stakeholders' appropriately, without exclusion**
  - *Primary stakeholders* are participants that fulfill a defined role in the scheme (network) and offer services to end users. Without them, no network. Get them intimately involved in the development and governance process and committed to implement the results it yields.
  - *Secondary stakeholders* are users on both sides, that use services offered by participants in the scheme. Without them, no usage. Get their support for the process and buy-in on the functionality the network provides.
- **Facilitate the 'integral optimization of interests', at different levels**
  - *Content:* which solutions are there for each issue to be addressed in the scheme, which integral set of solutions is optimal for all (related) issues?
  - *Implementation:* which integral set of solutions is optimal for a participant in a role, which set integral set of solutions is optimal for all participants in that role?
  - *Network:* which integral set of solutions is optimal for the network as a whole (all participants in all roles)?
- **Organize 'pragmatic decision making', also suitable for governance phase**
  - *Expert groups:* generate options and solutions for content issues, optimize partial sets of solutions
  - *Project team:* optimize integral sets of solutions, manage consistency

- *Core team:* implementation level optimization
- *Steering group:* network level optimization

- **Iterate by definition, time-box rigorously to flush out key issues and solutions. No escape.**
  - *Spend time together physically* discussing, exploring the complexity of the subject matter and the interests, positions of the participants. Cherish advancing insights, as these are essential to reach 'common ground'.
  - *Stick with the process, timelines.* Over time (months) the participants involved in the process will become more of a team, and momentum, focus and joint commitment on what is collaborative created will build.

As a final remark we would like to point towards the Open Identity Exchange (OIX) as a candidate for the governance platform. It already has a composition and structure that seems largely fit for purpose, although reducing complexity by replacing the multiple trust frameworks approach by a single scheme approach is suggested. On the other hand, complexity will increase somewhat by adding scheme related topics such as business model structure, brand management and licensing/certification.

We think that, given our unique, specific and relevant expertise, we can contribute greatly to progressing the NSTIC, and provide substantial acceleration (years) in the development of the envisioned e-identity ecosystem.

We would welcome any opportunity to elaborate on the above, by phone, mail or a meeting, and to contribute where we can to help realise this inspiring and daring vision, so clearly set out.

Sincerely,

Chiel Liezenberg, Douwe Lycklama,

Founding partners

Innopay

Related documents provided:

- 110722 E-Scheme Development-Governance_Innopay
- 2010 A Network Approach to E-Identification_Innopay

Introducing Innopay

Who we are, what we do &
our experience with 'scheme' governance

NIST

Innopay – 2011

tomorrow's transactions today

‘We want to help create a networked world’

- Globalisation increasingly leads to a network economy and electronic infrastructures enable industries to cooperate in networks, in real-time
- (Mobile) Internet is developing into a true transaction channel, creating new transaction contexts. New contexts require new transaction services and new options emerge in existing contexts
- Transaction services are part of two-sided markets, with sophisticated dynamics and network effects
- Development of successful transaction services requires thorough understanding of the context. Development is complex and costly and asks for specialist expertise and a specific approach

Improve the transaction services industry in close, open collaboration with stakeholders

innopay. tomorrow's transactions today


Online payment

- **Innopay is an independent full service consultancy, specialised in payments and related transaction services**


E-invoicing

- **E-payment, e-invoicing, e-identity, m-payment, cards, rules**


E-identity

- **Passionate experts in innovation, products, channels, use(rs)**


Mobile payment

- **Reputed player with active contribution to development of the industry. Member of a.o. EPCA, EBA, EU-PSMEG, CA-TFPSR**


Cards

- **Truly independent from IT vendors & financial institutions**


Rules

- **Founded in 2000, employs 15 consultants, from Amsterdam**
  - Founded by Chiel Liezenberg (1968) and Douwe Lycklama (1965)
  - Extensive experience in consulting in complex organisations

INNOPAY

Our services. value propositions for everyone.

Structure & understand™

- Help professionals to understand the transaction industry
- Facilitate focus on industry level
- Research and knowledge sharing on key industry topics

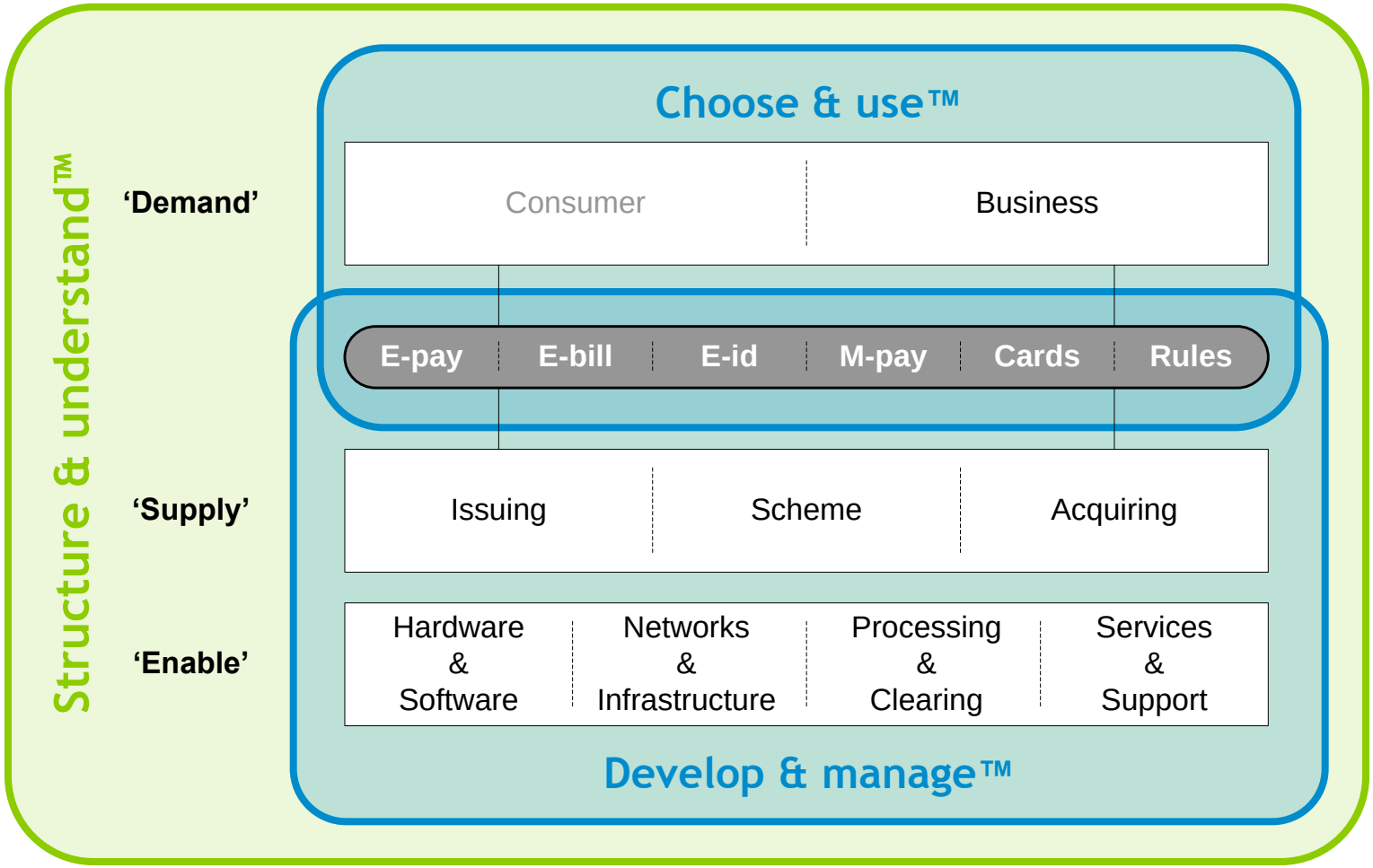
Develop & manage™

- Help providers to develop compelling transaction services
- Develop features, (new) business and/or services
- In multi-stakeholder process or for individual client

Choose & use™

- Help companies in choosing and using transaction services
- Select services that fit specific business needs of companies
- Manage implementation to deliver anticipated results

Serving all disciplines and players in the industry



Industry Level References

- **European Commission (EC):**
  - Member Payment Systems Market Expert Group (current)
  - Executive briefings (2010)
- **European Central Bank (ECB):**
  - Executive briefings (2009)
- **European Payment Council (EPC):**
  - E-Commerce Work Group (current)
  - E/M Payment Expert Group (2006-2007)
- **Euro Banking Association (EBA):**
  - E-Services Scheme Development (current)
  - E-invoicing scheme Work Group (2008/11)
- **European E-merchant Initiative:**
  - Author Position Paper (current)
- **Canadian Ministry of Finance:**
  - Task Force Payments System Review, Member Regulatory Advisory Group (current)

INNOPAY

Development of e-schemes

Specialist expertise, specific approach

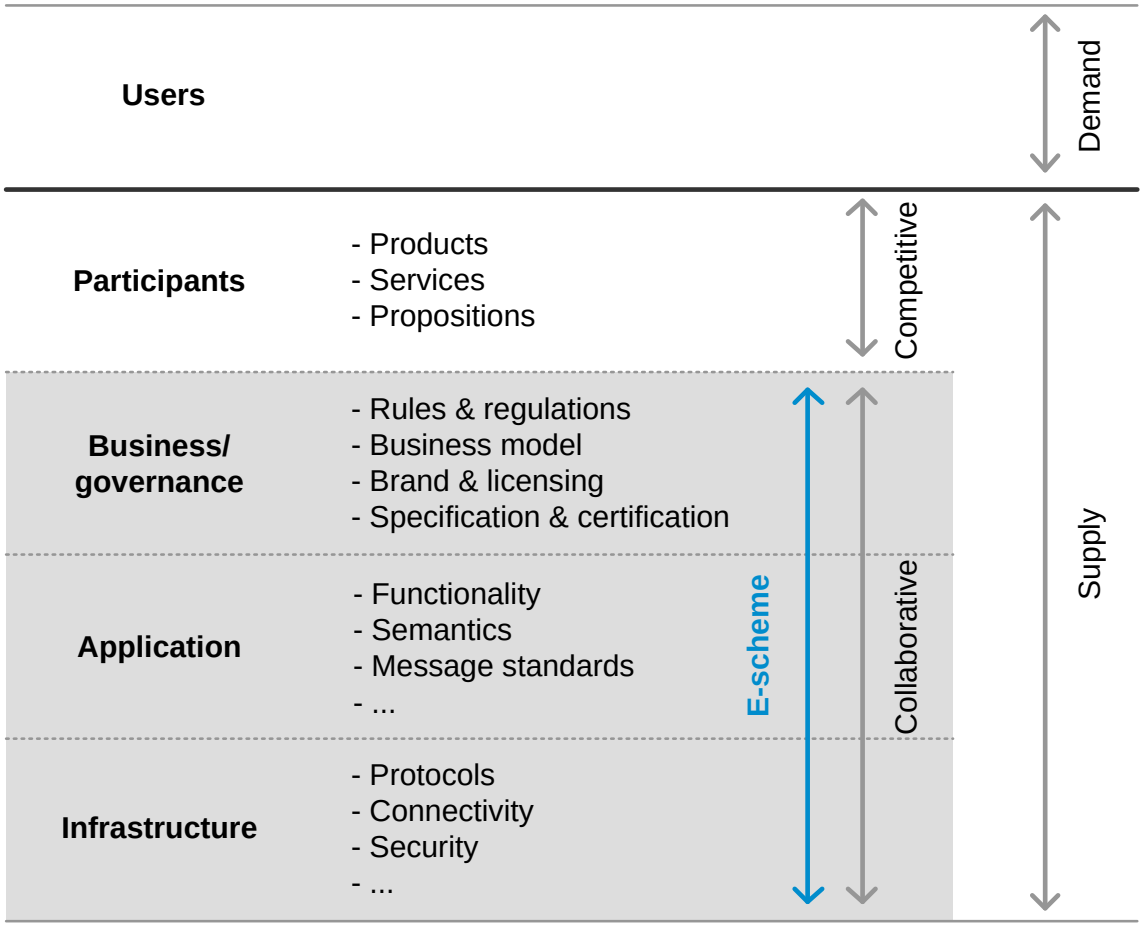
tomorrow's transactions today

Scheme Product References

- ‘iDEAL’
  - Dutch banks’ online payment scheme
  - Introduced 2005, >60% NL market share
  - Award: Thuiswinkel Innovation Award 2006
- ‘eHerkenning’
  - Dutch Government e-identity scheme
  - Introduced 2010 with B2G limitation, growing steadily
  - B2B opening up in 2012
- ‘D+B’
  - Dutch health care insurers instant claim settlement scheme, to claim health care in real time on point of sale terminal at health care provider using insurance card
  - Developed in 2007-2009, fully spec’d, piloted, certified
  - Introduction postponed, market not ready
- EBA Clearing
  - E-invoicing scheme & e-payment scheme – in progress

E-schemes consist of multiple inter-related topics

and need to be carefully scoped and positioned



E-schemes have a multi-layer structure, with delicate inter-relations

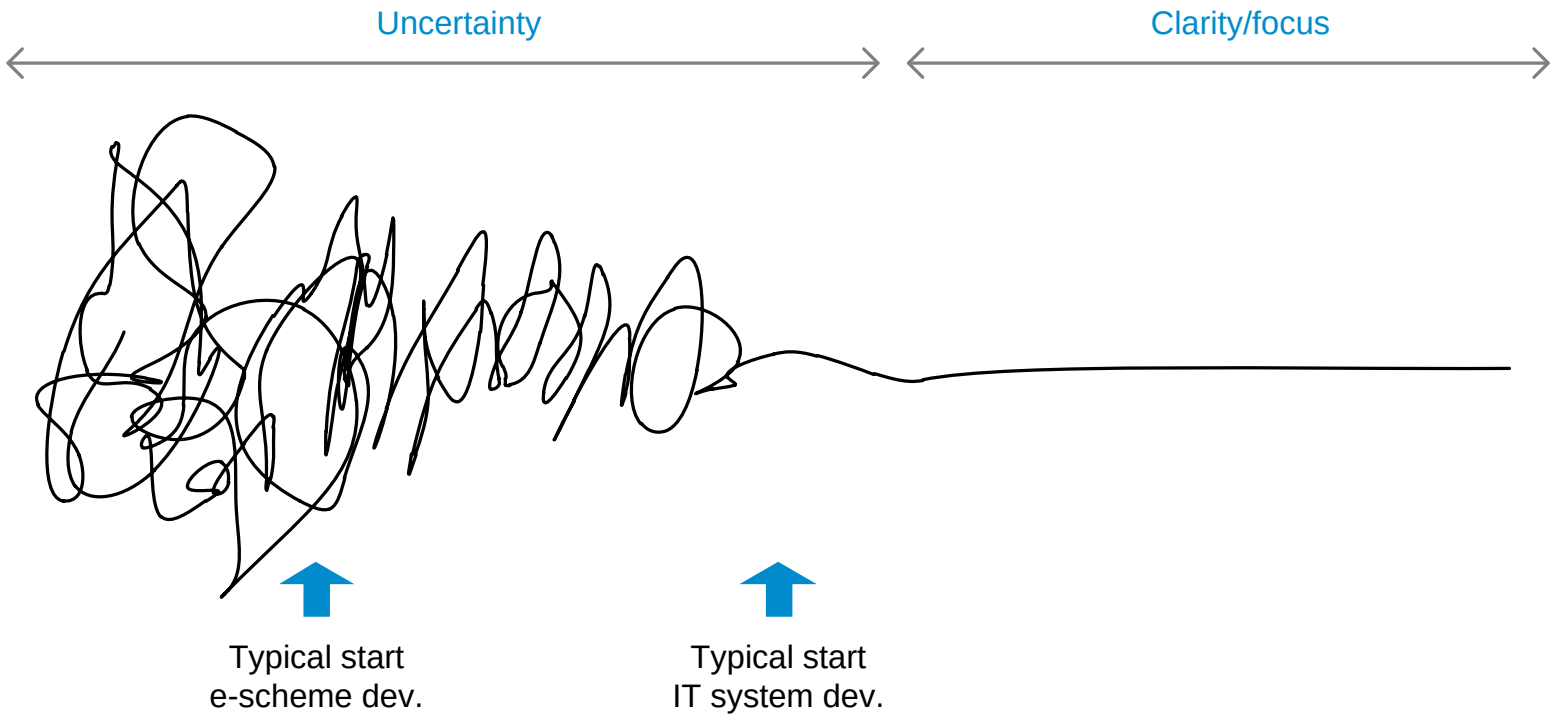
- **Separate competitive and collaborative domain**
  - Collaborate on non-value added components of the solution ('the network' as enabling commodity)
  - Assure enough space for value added components of the solution remains

- **Within collaborative domain, agreements of different nature are required:**
  - **Business/governance:** Under which business conditions do we operate, what are roles and responsibilities/liabilities and how do we handle change
  - **Application/functionality:** what value add needs to be provided, what functionality needs to be supported, what industry standards apply
  - **Infrastructure:** how do we discover participants, how do we connect, how do we exchange information securely

- **Development and governance phase require similar organization structure**
  - Subject matter complexity does not change,
  - Frequency of changes and scale/impact do change

INNOPAY

E-scheme development is a blurry design process



Research & understand

Design business model prototypes

Implement business model design

E-scheme development & governance

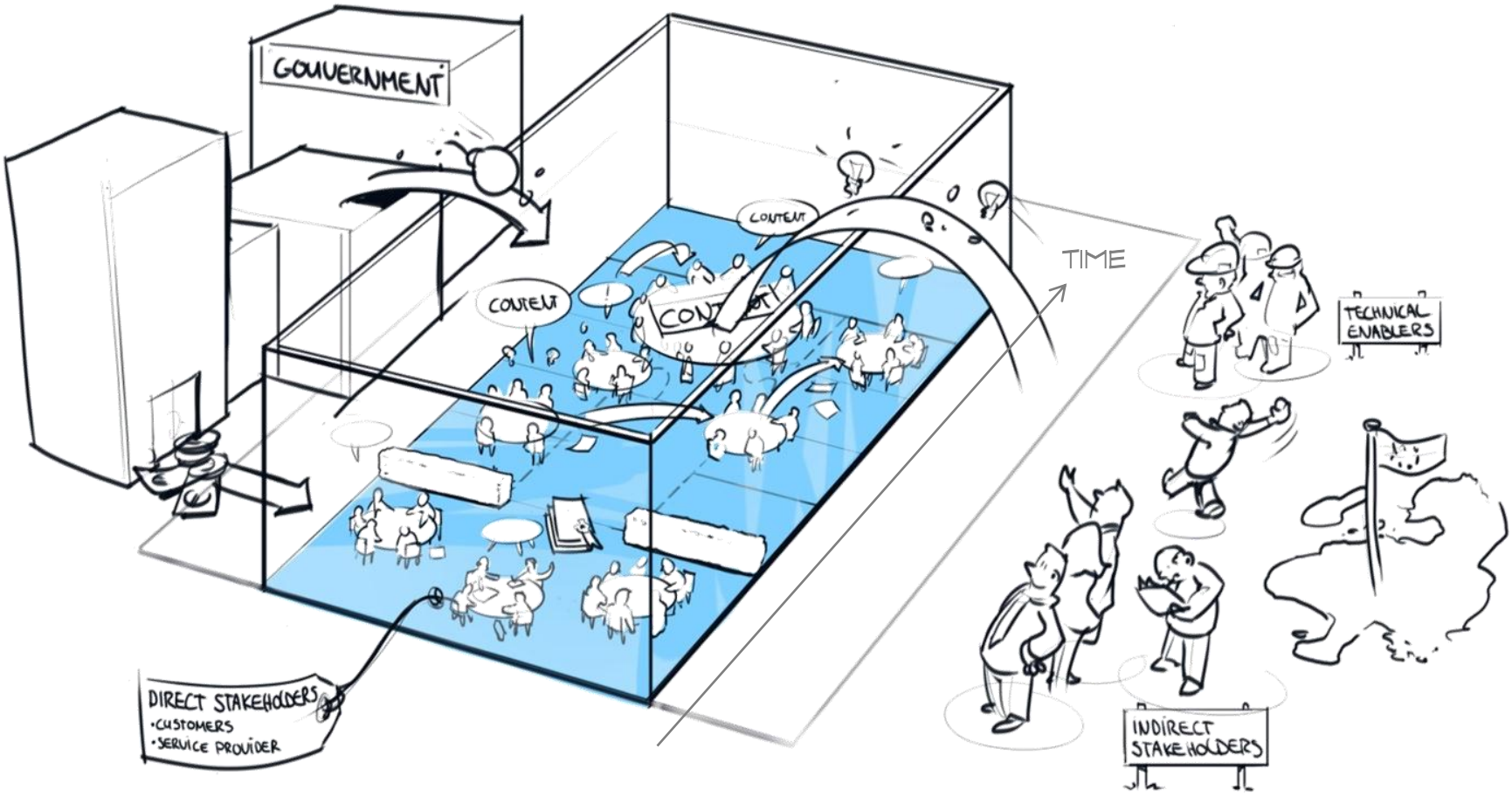
success factors

- **Accomodate the 'order of stakeholders' appropriately, without exclusion**
  - **Primary stakeholders** are participants that fulfill a defined role in the scheme (network) and offer services to end users. Without them, no network. Get them intimately involved in the development and governance process and committed to implement the end results it yields.
  - **Secondary stakeholders** are users on both sides, that use services offered by participants in the scheme. Without them, no usage. Get their support for the process and buy-in on functionality the network provides.
- **Facilitate the 'integral optimization of interests', at different levels**
  - **Content:** which solutions are there for each issue to be addressed in the scheme, which integral set of solutions for all the (related) issues is optimal?
  - **Implementation:** which integral set of solutions is optimal for a participant in a role, which set integral set of solutions is optimal for all participants in that role?
  - **Network:** which integral set of solutions is optimal for the network as a whole (all participants, all roles)?
- **Organize 'pragmatic decision making', also suitable for governance phase**
  - **Expert groups:** generate options and solutions for content issues, optimize partial sets of solutions
  - **Project team:** optimize integral sets of solutions, manage consistency
  - **Core team:** implementation level optimization
  - **Steering group:** network level optimization
- **Iterate by definition, time-box rigorously to flush out key issues and solutions. No escape.**

INNOPAY

Scheme development is like…

working in a glass box



Interested?

Feel free to contact us

Innopay - info@innopay.com, +31 20 6580651

tomorrow's transactions today

innopay

A Network Approach to E-identification

This is an introduction and explanation of a network approach for e-identification in the EU carried out by Innopay (Leendert Bottelberghs, Cassandra Hensen and Chiel Liezenberg) at the request of the Ministry of Economic Affairs of The Netherlands.

Ministerie van Economische Zaken

Contents

Preface

The users and providers of services on the internet need to be certain of the identity of the party they are dealing with. This is an essential condition to be met if our economy is to be able to conduct improved electronic business at both a national and an international level.

The current methods used to identify service providers and users have their limitations. There are too many different solutions that are often inconvenient, of limited scope, difficult to use and/or insufficiently secure. This jumbled 'bunch of digital keys' is causing problems: fraud is increasing, users are becoming distrustful, and the security of electronic traffic is declining. This is in turn hampering the further development of electronic business. Electronic business can and must be improved and made more sophisticated: it is time to take the next steps.

This exploratory study carried out by Innopay presents an appealing approach. Mobile telephones, bank cards and a variety of company systems can be used to sign a tax return, apply for a licence or deal with numerous issues on the internet – and all in a reliable manner. Consequently, no new solutions are introduced. Instead, the company proposes the use of existing systems to provide for the secure and reliable completion of transactions on the internet. This way, the existing solutions of a number of parties can be linked together in an open system.

The Dutch government introduced DigiD several years ago - a means of authentication that enables the authorities to provide digital services to citizens. This was an important step forward. However, how to proceed? In requesting this exploratory study the Ministry of Economic Affairs makes a contribution to the discussion on the next steps. The business community and the major government service providers, in particular, urgently need to implement widely applicable and broadly supported solutions which guarantee that they know precisely who they are dealing with on the Internet. We have assigned this challenge a high priority.

M.J.A. van der Hoeven
Minister of Economic Affairs

1

Management Summary

The recognition of users in digital environments is becoming increasingly challenging: the various parties involved in e-business and e-government have been struggling for many years with the lack of sufficient available options for the digital recognition of users. As all EU member states face adherence to the Services Directive by the end of 2009, the need for a reliable e-identity solution is becoming urgent. This book presents a new approach to e-identification (e-ID) that could support pan-European interoperable e-identification.

Several initiatives have been deployed, both at national as well as European level, to overcome the challenge of electronic identification. Some countries have implemented advanced and successful e-ID solutions within their borders, but all of the existing solutions lack full pan-European interoperability. In order to create an EU-wide recognition of electronic identity, two important initiatives were started. First, the 'e-ID Roadmap' outlines the European e-ID goals to be met by 2010 at a policy level and sets out specific objectives. Second, the STORK project aims at creating infrastructural interoperability by starting cross-border pilots and developing common rules and specifications for electronic authentication. In addition to the initiatives above, the EU is working on interoperability of the digital signature. The digital signature is, due to differences in implementation of the Electronic Signature Directive, not yet interoperable across Europe. 'In January 2010 the European Commission has published a central list with links to national "trusted lists" of certification-service providers issuing qualified certificates in order to improve the interoperability of electronic signatures.'

This report presents a network approach for creating a sustainable e-ID infrastructure. In this approach e-ID is regarded as a service in a two-sided network, instead of a technical infrastructure or a security problem. By applying a solution to e-ID that has proven its success in the electronic payments domain, a highly scalable and interoperable network can rapidly evolve due to low barriers in user acceptance. In the network approach to e-ID, End Users can make use of existing means of authentication to access all E-service Providers in the network (see figure 1-1).

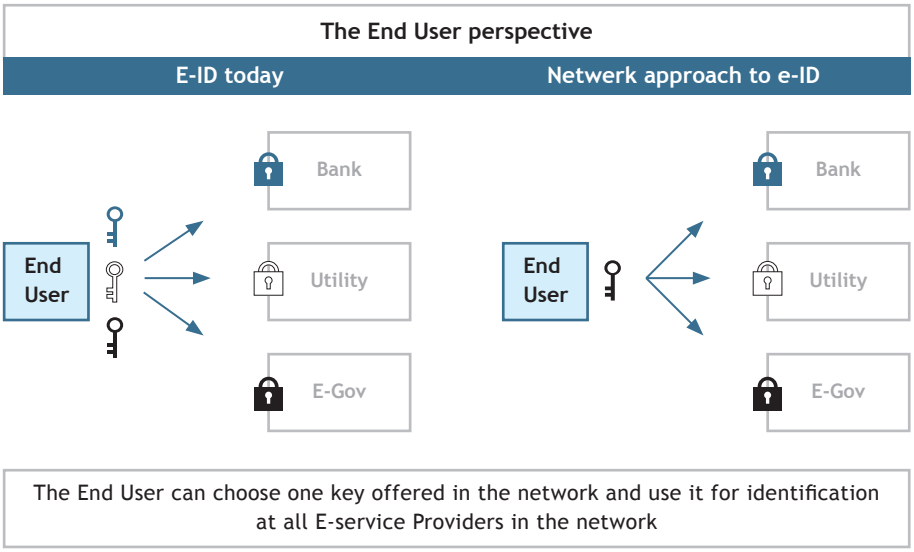


Figure 1-1: The End User perspective of a network approach to e-ID infrastructure

The E-service Providers in the e-ID network can each accept all the means of authentication issued in the network, to identify their End Users. As a result there is no need for them to issue these (costly) means of authentication themselves (see figure 1-2).

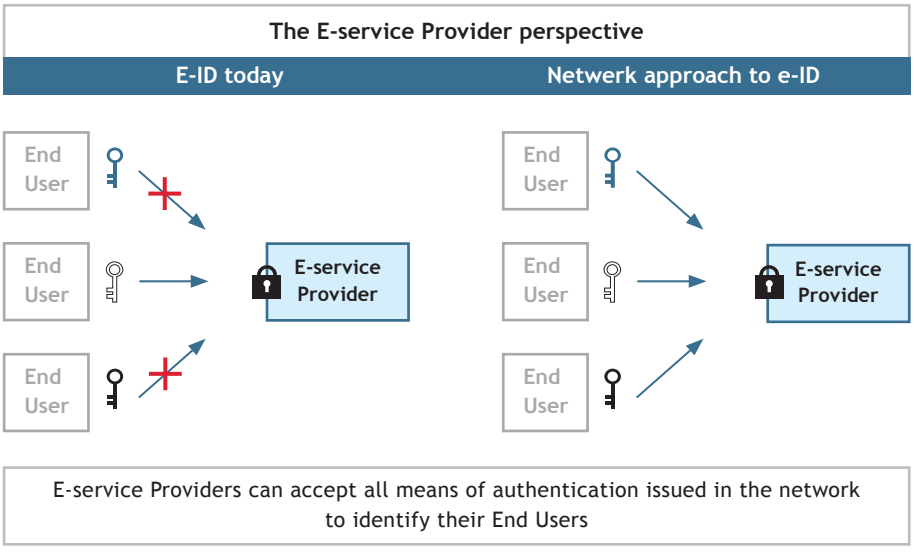


Figure 1-2: The E-service Provider perspective of a network approach to e-ID infrastructure

The approach to realise this e-ID network is twofold. In the first place, this new e-ID solution consists of a decentralised 4-party model instead of a centralised 3-party model. In the e-ID network the issuing of means of authentication and the acquiring (routing) of these means are separated in two different roles (see figure 1-3). The 4-party model connects existing means of authentication or keys (e.g. cards, mobile phones, tokens, passwords) to E-service Providers. This way a level playing field is created in which various players and solutions can co-exist.

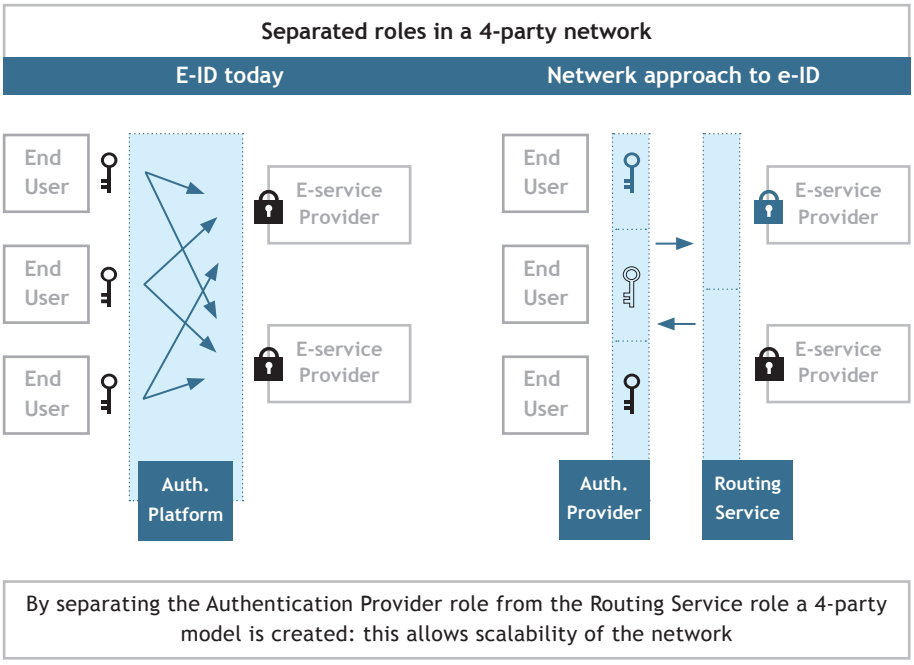


Figure 1-3: In an e-ID network Authentication Provider and Routing Service become separated roles

Secondly, a set of agreements is made that describes and defines the roles of the different parties in the 4-party model. These agreements that ensure the interoperability of the network are referred to as a 'scheme'. Parties that adhere to the scheme can join the e-ID network. This creates scalability of the network.

The scheme entails a multidisciplinary set of specifications in three categories: business governance, application and infrastructure. A scheme basically addresses the 'cooperative domain' between participating parties, while at the same time creating a 'competitive domain' in which the parties can develop and offer their own propositions and products.

This network approach to e-ID could also be used in the challenge to create cross-border interoperable e-ID models. The authorities' role of the Member States in the design of such an e-ID scheme could primarily be related to the specification of the framework. The authorities can also continue to issue means of authentication and, at the same time, be a user of already existing means of authentication issued by commercial parties such as banks, telecom operators and other token providers.

The scheme can result in network effects combined with freedom of choice, market forces, free competition and innovation. This can result in rapid growth and a dynamic market. Currently this network approach is being deployed in The Netherlands, in the e-Recognition project where companies and their acting representatives are identified when doing electronic business with the authorities. The basic principles of this approach could be broadened from business-to-government, to citizen-to-government, business-to-business and business-to consumer markets.

Introduction

2.1 Objective of this document

EU Member States are all undertaking efforts to adhere to the Services Directive[1] as adopted in 2006. The main challenge for Member States is to develop a solution that identifies users of online services with a high level of certainty. As a result, in several EU Member States initiatives are underway to secure electronic identification (e-ID) for public services. While this is a positive development, the inevitable diversity of these initiatives complicates cross-border use of secure e-identification systems. In short, there is a need for an interoperability framework to address e-ID requirements at an EU level.

In this report a possible approach to e-identity developed by The Netherlands is explained. The approach is based on the principles used in several successful payment systems such as debit and credit cards and online payments. Their success was achieved by re-using existing infrastructures leading to high user acceptance. The Ministry of Economic Affairs of The Netherlands believes that this network approach to e-ID could provide a workable solution for the national e-ID challenge and possibly for cross-border e-ID in Europe as well.

This document is of interest to policy and decision makers in the field of e-ID at both the national and European level, and to any person interested in e-ID solutions in general.

2.2 'e-Recognition': Beyond identification and authentication

In the ongoing discussion regarding the subject of electronic identification, ambiguity about the terminology is still present. The introduction of organisations engaging in electronic transactions makes matters even more complex, since it is always a person that acts on behalf of an organisation. In order to be assured that the person carrying out the transaction is authorised to do so by the organisation, an extra verification has to be carried out. In the Netherlands the concept of e-Recognition was introduced to cover this issue. Within this process extra information is obtained so that the relying party is assured that the transaction is valid. This can be regarded as extra services on top of identification and authentication services.

1 Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market

Because the concept of e-Recognition is relatively new and can be carried out on top of e-identification we will use the term e-identity throughout this document.
This is also more in line with existing documentation addressing the subject and will avoid confusion for the reader. To avoid any confusion, we give our definitions of identification and authorization as they are used within this document. Identification is generally defined as linking a set of specific data to a person to distinguish that person from other persons. Authentication is the verification of a claimed identity with the objective of recognising a person or user.

2.3 Outline of this document

In the next chapter the importance and urgency of a pan-European approach to e-ID is explained. The current situation in Europe with regard to the implementation of the Services Directive is given and lessons learned are identified. In Chapter 4 the basic principles of the network approach to e-ID are explained. Chapter 5 shows an example of how the network approach could work for cross-border e-ID. The final chapter provides the conclusions and opportunities.

Importance and Urgency

3.1 The need for electronic identification

Both governments and businesses are offering more and more electronic services, aiming to increase efficiency and accuracy, reduce costs, and improve End User experience. With the increasing amount of services offered electronically, the need for reliable electronic identification is becoming more apparent.

3.1.1 E-ID in the Netherlands

In 2003 the Dutch government launched the 'DigiD' platform that enables identification of citizens for online services. This solution made it possible for Dutch citizens to, for example, confirm tax registrations or claim unemployment benefits online. After experiencing a growing user base and successful usage in the past years, DigiD is facing several challenges for further growth:

- Use is restricted to interaction with organisations with a public task.
- Frequency of usage is low (on average 1.2 times a year) compared to other online services such as online banking or telephone, leading to many repeat requests for DigiD usernames and passwords.
- Cost efficiency (cost per login) is difficult to attain as a result of low usage compared to high back office costs due to password resets.
- Electronic identification does not meet the highest security requirements.
- System is for domestic use (the Netherlands only).

For communication at a higher security level, the Dutch government also enabled a Public Key Infrastructure (PKI) according to EU directives. This PKI, called 'PKIoverheid' uses Qualified Electronic Signatures and is available for both citizens and organisations in the Netherlands. It enables highly secure identification and verification in electronic communication, and can be used to e.g. digitally sign documents. Due to a lack of infrastructure that enables easy usage of this technology, the infrastructure is not utilised to its full potential.

Another challenge is the use of electronic identities for transactions between government and businesses. In acknowledgement of these challenges the Ministry of Economic Affairs is searching for creative and innovative ideas to develop new solutions for electronic identification.

3.1.2 E-ID in Europe: The Services Directive

As the European community is striving for a closer relation between Member States and for social and economical prosperity, the development of a cross-border e-identification framework is essential for the European economy. This need is emphasized by the European Commission (EC) through the Services Directive (2006/123/EC). The Services Directive aims to achieve a better internal market for enterprises by guaranteeing two freedoms: 1) the freedom of establishment and 2) the freedom to provide services throughout the entire EU. It aims to eliminate the existing barriers to cross-border business, including administrative burdens, legislative uncertainty and lack of mutual trust. To be able to achieve this goal, the Services Directive describes the following three main requirements to be met by each of the EU Member States:

- Development of fair national requirements for enterprises.
- Development of a single point of contact for enterprises.
- Development of a solution to identify users (with a high level of security) of electronic services and to process requests of enterprises online.

The latter requires a pan-European e-identity solution. The EC expects these deliverables to be in place in every Member State by December 2009.

3.1.3 Europe on the road towards securing electronic services

Over the past decade, European Member States have developed e-ID systems that were best suited to their national needs. In recent years, efforts have been made at different levels to seek solutions for the European interoperability of these domestic e-ID solutions. Three main milestones have been reached [2]:

- The e-ID Roadmap [3].
- The STORK project [4].
- The Services Directive.

At a policy level, the e-ID Roadmap has been developed. This document outlines the European e-ID goals to be reached by 2010 and defines specific objectives. At the infrastructural level, the STORK project has recently been initiated.

---

2 Report on the state of Pan-European eIDM initiatives, ENISA (2009)

3 A Roadmap for a pan-European eIDM Framework by 2010, see http://ec.europa.eu/information_society/activities/egovernment/docs/pdf/eidm_roadmap_paper.pdf

4 The ICT-PSP project Secure idenTity acrOss boRders linKed (STORK)

This project is aimed at developing a series of pilot projects for several European countries, using the authentication means favored by the respective national governments. Both the e-ID Roadmap and the STORK project have a long-term scope.

The Services Directive deadline of December 2009 is forcing the Member States to create functioning applications that require e-identification of users. Forced by this short-term deadline, the EC decided to make use of the electronic signature as a means to securely identify users. But, due to a lack of interoperability of the electronic signature between Member States, this has so far not resulted in a working cross-border solution.
With the development of the e-ID Roadmap and the Services Directive, the EC has imposed ambitious short-term goals on itself and on the Member States. In addition to the STORK project and the electronic signature developments, this has resulted in even more relevant initiatives in the EU. The different solutions that Member States have developed form a knowledge base in the field of secure e-identity. Altogether they have the potential to act as a catalyst in furthering the desired e-ID interoperability in the EU.

3.2 Lessons learned so far

From both the EU and Member States' initiatives (e-ID Roadmap and the STORK project), several lessons can be learned to ensure the successful implementation of a cross-border e-identification system in Europe.

The e-ID Roadmap states that an interoperable e-ID infrastructure should *ensure that administrations trust each other's identification and authentication methods*. With regard to the level of security, it further states that since several levels of secure authentication are needed, an e-ID solution should be *multi-level*. This way the authentication requirements for each electronic service can be tailored to the security needs of that service. Further the roadmap emphasises that a solution should *enable private sector uptake*. This allows Member States to rely on private sector partners (e.g. financial institutions) for the provision of e-ID services. Moreover this will enlarge the scope of the e-ID solution, not limiting it to government services alone. This widened scope may be necessary to ensure sufficient return on investment.

From the experience with the Dutch DigiD solution, the use of the electronic signature and the other initiatives mentioned several additional lessons can be learned:

- Uptake of any e-ID solution is largely dependent on the creation of trust and usability. This means that it should not only be safe, but also be perceived as such to meet the 'user friendly' requirements, including privacy protection.
- An additional aspect of user friendliness is the minimization of the 'digital key ring'. This refers to the multitude of 'digital keys' that users obtain to identify themselves online at different services.
- A sustainable cost structure is needed to finance the e-identification solution. Many governments now face high costs developing and maintaining e-ID systems themselves.
- Consensus at the technical level of e-ID solutions is needed to create interoperability.
- Scalability of the solution is required so it can be used by governments and enterprises in a broader geographical area.

3.3 A network approach

At this moment the EU and its Member States are at a crossroad concerning the development of pan-European e-ID solutions. It is clear that as of yet many solutions have enabled online identification, but no single initiative has provided the definitive solution to the European e-ID issues. The challenge is to combine the benefits of existing initiatives and integrate these into an interoperable e-ID solution for Europe.

The network approach as currently developed in the Netherlands aims to re-use existing means of authentication such as bank tokens, national e-ID cards and digital certificates. End Users can make use of these existing means of authentication to access all E-service Providers in the network. The End User perspective of the network approach to e-ID infrastructure is shown in figure 3-1.

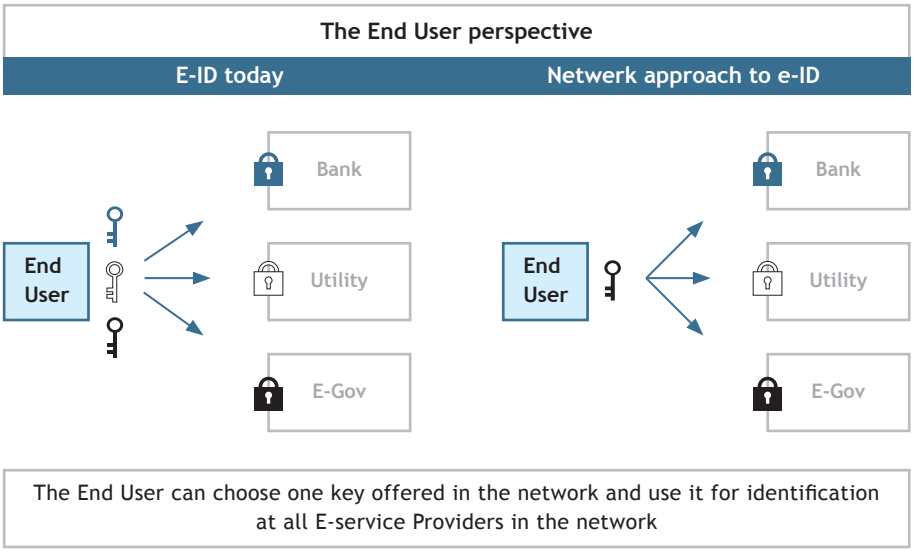


Figure 3-1: The End User perspective of a network approach to e-ID infrastructure

The E-service Providers that are part of the e-ID network can each accept all the means of authentication issued in the network to identify their End Users. This is shown in figure 3-2.

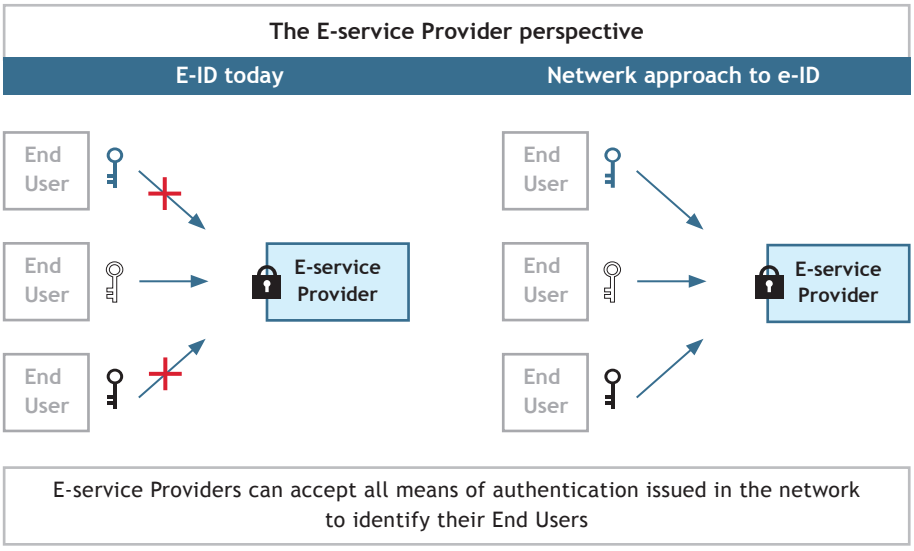


Figure 3-2: The E-service Provider perspective of a network approach to e-ID infrastructure

To achieve this, a set of rules and agreements is created allowing parties to join the network as long as they meet the requirements. Since this approach is not a system as such, but rather a framework, it does not have one central node but allows for participating parties to communicate directly. Naturally this leads to interoperability and scalability, and it has several other benefits:

- High End User friendliness: already known and trusted means of authentication are used.
- No enlargement of the 'digital key ring'.
- Market participation is enabled, which means that it allows for the use of 'digital keys' that are not issued by the public sector.
- Cooperative creation and use of the infrastructure leads to a sustainable cost structure.
- Multi-level: existing means of authentication already enable different security levels.

In the next chapter the network approach to an interoperable e-ID solution will be presented and explained in more detail.

4

A Network Approach: ‘E-ID as a Scheme’

The network approach we present in this document is not a new approach, but an existing solution applied to e-ID. It is based on the ‘scheme’ approach used in the past to solve network and scale problems that arose with global payment networks. Currently this network approach is being developed in the Netherlands. To explain how this network approach can help to develop secure e-identification, we will start to explain the concept of the two-sided network and the basic elements of a scheme. Then we show how the concept of a scheme can be applied to create an e-ID scheme. In the last section we show what value added services the scheme concept can bring, in order to meet existing needs and stimulate further innovation.

4.1 Two-sided networks

A two-sided network distinguishes two types of users that interact with each other, using a common infrastructure. Examples of two-sided networks can be found in the area of electronic payments, as for instance credit card networks. With credit card payments, consumers (cardholders) and merchants (acceptants) both use a common infrastructure that facilitates the transaction, while the two types of users have distinct requirements regarding the services that are offered to them. What they have in common is that they both benefit from the size of the other side of the network. In other words: cardholders benefit from the number of merchants that accept their card, and merchants benefit if many consumers hold the credit card that they accept. This is what is called a cross-sided network effect[5]. In a network paradigm, electronic identification can be considered as a two-sided network with cross-sided network effects [6].

The evolution of global payment systems in the 1970’s was supported by the implementation of 4-party model schemes. The 4-party model implies that the two sides of the market, the consumer side and the merchant side, obtain their required services from different parties. These parties offer their services in competition with each other while giving the users access to the same network. This provides scalability, a competitive market and network effects. This is opposed to a 3-party model, where there is a single central party to which both consumers and merchants have to connect.

5 Opposed to the cross-sided network effect is the same-sided network effect. This refers to the benefits gained from the growth of the same side of the network.

6 Examples of international credit card schemes include Visa and MasterCard.

For the 4-party model to work, a set of agreements is necessary that allows the participants to share a common infrastructure and offer the same basic services. This set of agreements is referred to as a 'scheme'.

4.2 A scheme: allowing both competition and cooperation

So how did these schemes provide the fertile ground for these two-sided markets to grow so successfully? The strength of such a scheme lies in the separation of the cooperative and the competitive domain in the market. This way a scheme addresses two objectives of the network. Firstly, *a scheme promotes cooperation between the parties by the creation of a joint infrastructure*. This cooperative domain achieves a reduction of various costs (such as development and admission costs) resulting from the parties' collaboration in these fields. Secondly, the network *promotes competition at the product level by offering market players an opportunity to distinguish themselves in terms of added value*. This is the competitive domain were the parties involved can develop their specific propositions on top of the joint infrastructure.

The separation of the cooperative and competitive domains is essential to enable market competition and sort network effects. Moreover, since cooperation at the infrastructure level is mandatory, *this prevents competition between different infrastructures* that raises cost and offers no extra benefits to End Users or participating parties in the network.

4.2.1 Layers of a scheme

A scheme consists of a set of agreements, rules and regulations that ensure the separation of domains. The cooperative domain of a scheme is primarily comprised of three layers:

- Business and Governance: defining on what basis the participants in the scheme participate and their mutual rights and obligations in the scheme.
- Application: defining the scheme's scope, application and functionality.
- Infrastructure: defining how participating parties communicate and exchange information.

The competitive domain exists on top of this collaborative domain as is shown in Figure 3-1. The competitive domain now offers the participants in the scheme a level playing field in which they can develop propositions for the two-sided market.

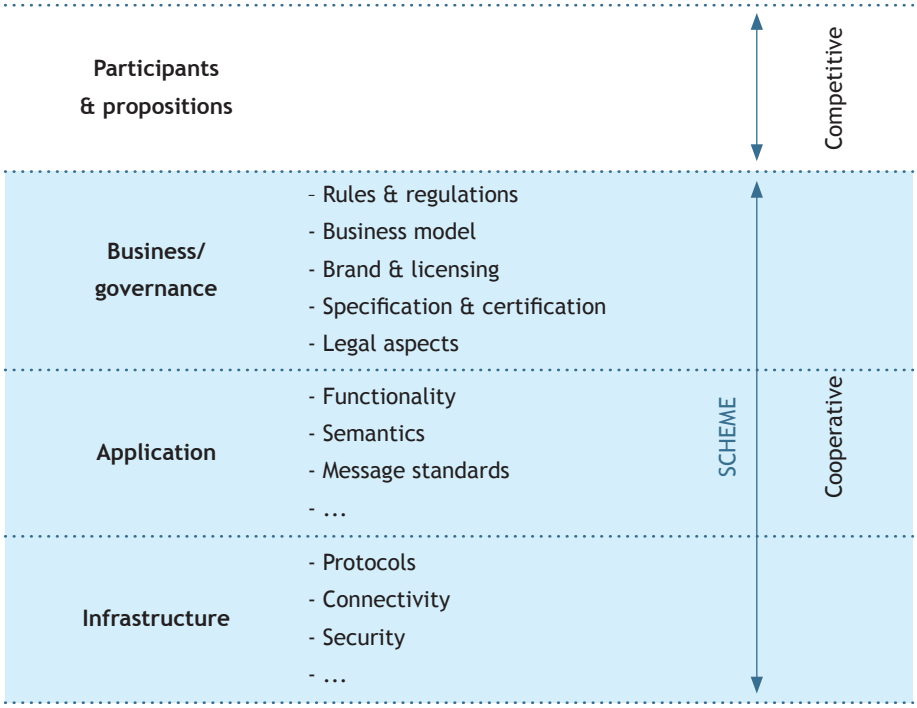


Figure 4-1: Separation of domains in a scheme, broken down into different layers.

4.2.2 E-ID in a 4-party model

Currently most e-ID models exist as 3-party models. Although this can function very well for certain markets, this model also has some limitations. The benefits of using a 4-party model over a 3-party model are discussed in paragraph 4.3.

Within a 3-party model, the party that provides the central platform for the market can readily be split into two roles to achieve the transition from a 3-party into a 4-party model. This is shown in figure 4-2.

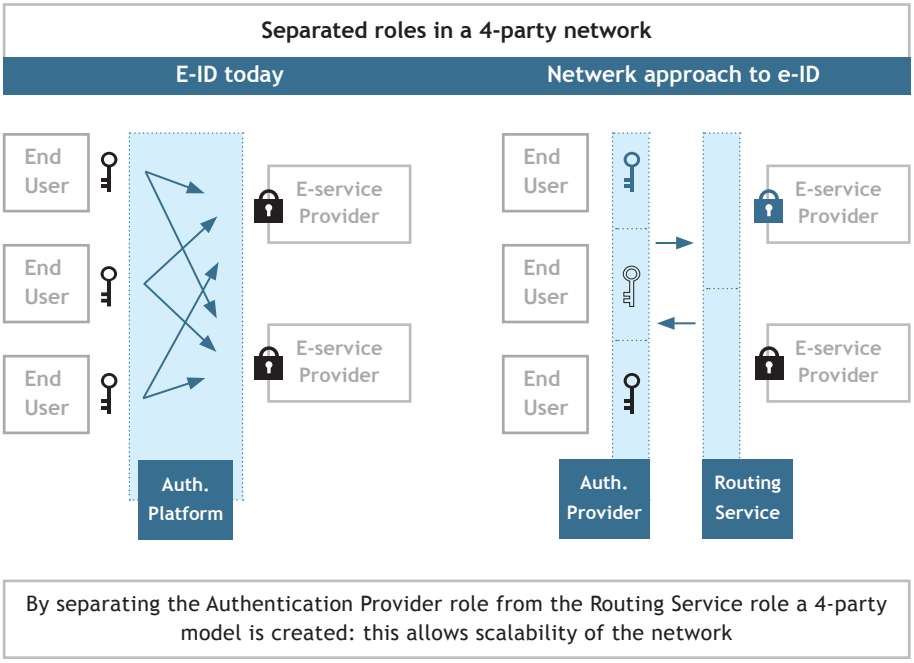


Figure 4-2: In an e-ID network Authentication Provider and Routing Service become separated roles

In the 3-party model the central party both issues the authentication means and connects the (governmental) E-service Providers. In the 4-party model, the component that issues the authentication means is transformed into an Authentication Provider, and the e-ID component linking the governmental E-service Providers is transformed into a Routing Service.

A scheme with a 4-party network model ensures that all players have pure bilateral relationships and fulfil an explicitly specified role in the chain:

- **End User - E-service Provider:** the End User concludes an agreement with an E-service Provider which requires the authentication of the End User. The authentication can be used for various purposes, such as secure login or digital signing (see paragraph 5.4 – Value added services for e-ID).
- **E-service Provider – Routing Service:** the Routing Service offers the E-service Provider a connection to the network in order to obtain authentication of the End User.
- **Routing Service – Authentication Provider:** the Routing Service and Authentication Provider exchange real-time messages and data during the authentication process. Within the e-ID scheme, all Routing Services are connected to all Authentication Providers.
- **Authentication Provider - End User:** the End User has an account with an Authentication Provider. The End User can select his Authentication Provider for an authentication. The Authentication Provider will handle the authentication and return the result to the Routing Service.

The roles played by the 4 parties in an e-ID model as a scheme are shown in figure 4-3.

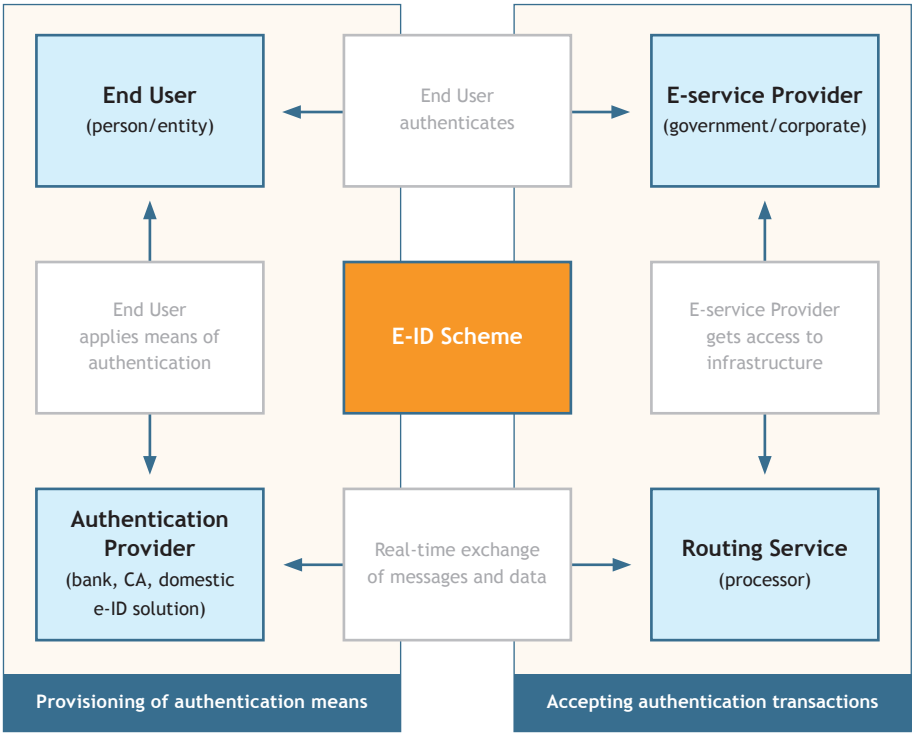


Figure 4-3: The roles played by the 4 parties in an e-ID model as a scheme.

The roles of the Authentication Provider and the Routing Service can each be filled in by multiple parties simultaneously. This gives the End User a choice where to obtain his authentication means. It could even be possible for the End User to have accounts at multiple Authentication Providers, as long as the scheme allows for this. The same applies to the E-service Provider who can choose where to obtain access to the e-ID network, since every Routing Service is connected to all Authentication Providers. The bilateral relationships between these parties are essential for the scalability of the network.

A Scheme Management Organisation manages the rules and regulations. The manage ment of the brand of the e-ID solution can be part of the Scheme Management Organisation as well.

Adopting this approach immediately results in a 4-party model that is ready for kick-off. Other solutions or parties can then be invited to play a role within the scheme if they comply with the scheme's rules and regulations – thereby promoting further network effects.

4.2.3 Management and governance of the scheme

The authorities' role in this scheme can be the initiation of the cooperation and assistance with the specification of the framework. However, the authorities do not need to be the owners of the scheme. The most important motivation for authority involvement is to have influence on the functionality as well as oversight. Influence on functionality could be organised via a customer reference board. Oversight could be organised through existing oversight bodies for example for telecom operators or financial services. A variety of alternatives is conceivable in which the stakeholders receive an interest in the organisation managing the scheme. This will achieve broad support for the scheme. In addition to managing and possibly the further development of the scheme, this organisation also performs a number of other duties:
the organisation issues licences to participants and certifies participants that are eligible for taking part in the scheme. The e-ID Scheme Management Organization is responsible for:

- **General management** of the rules and regulations of the scheme.
- **Certification and licensing** of Authentication Providers and Routing Services participating in the scheme.
- **Specification** of commercial (model) agreements and, possibly, provide for the mutual settlement of accounts. This will depend on the chosen business model for the scheme.
- **Mediation** in case of disputes that may arise between the Authentication Providers and Routing Services that cannot be settled bilaterally.
- **Product management** of the common e-ID functionality offered by the network. This also includes further (functional) development of the scheme.
- **Brand management** of the e-ID network. The e-ID scheme will be recognisable as a brand focussed on the End Users. This creates long-term trust and will help further growth of the network.

4.3 Benefits of the 4-party model

A 4-party model ensures the separation of the parties providing the services for the two sides of the network: the Authentication Provider serves the End User and the Routing Service serves the E-service Provider (see Figure 3-2). In the model, these two roles can now be played by different parties, which have the following benefits:

- The model *prevents the development of a centralised position of power.*
- The model allows the *reuse of already existing means of authentication.*
- An End User can use one authentication means of choice to identify himself at multiple organizations resulting in *high user friendliness* and *reduction of the 'digital key ring'.*
- Use of the 4-party model will *stimulate market* development since the services on both sides of the network can be provided in competition.
- Because of the infrastructural agreements in the scheme, the *e-ID propositions developed in competition are always interoperable.*
- Since a common infrastructure is part of the scheme, the 4-party model *prevents competition on an infrastructure level* This prevents investment in different e-ID infrastructures that are not interoperable.
- The 4-party model allows *freedom of choice for all users of the e-ID network.* The model ensures that every Routing Service is connected to every Authentication Provider and that these roles can be fulfilled by multiple parties simultaneously. This gives the End User the choice where to obtain his authentication means and it allows the E-service Provider to choose where to obtain access to the e-ID network.

In general, the 4-party model scheme is an inclusive model that supports scale and interoperability.

In the next chapter we will give an example of how a deployed e-ID Scheme could work for e-government services in a pan-European context.

5

Example of an E-ID Scheme

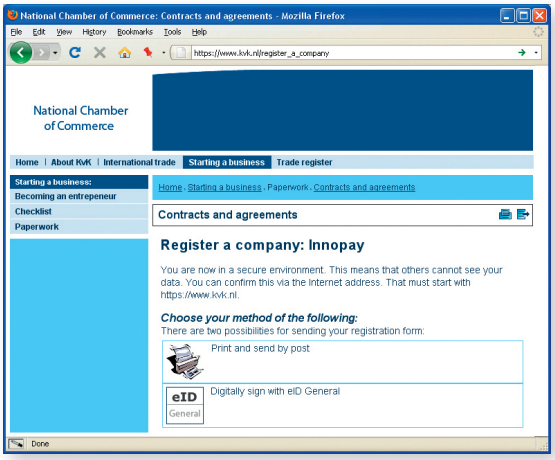
5.1 Introduction

In this chapter we present an example of how a deployed e-ID Scheme could work for a user in the EU. The intention of this example is to provide insight into its operation and possible form. This example is neither definitive nor binding: it merely serves to illustrate the roles, the players and the processes involved in a cross-border e-ID process when e-ID would be organised in a scheme. The fictitious scheme, referred to as e-ID General, is based on the 4-party model presented in paragraph 4.2.2 and shows the operation of the scheme from various perspectives: End User, E-service Provider, Authentication Provider and Routing Service.

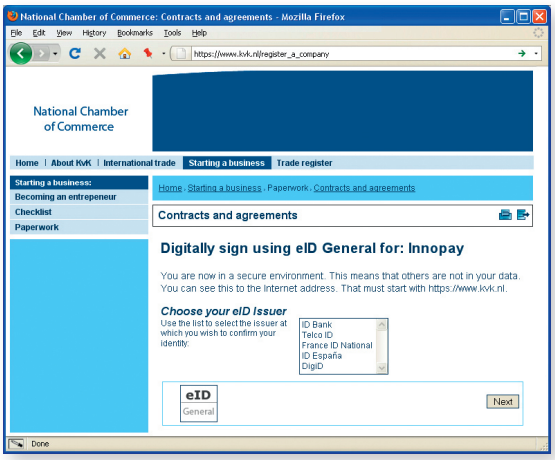
5.2 End User

A user that holds an account with an Authentication Provider (for example a participating bank which supports the e-ID General scheme), has an opportunity to use this as a means of authentication.

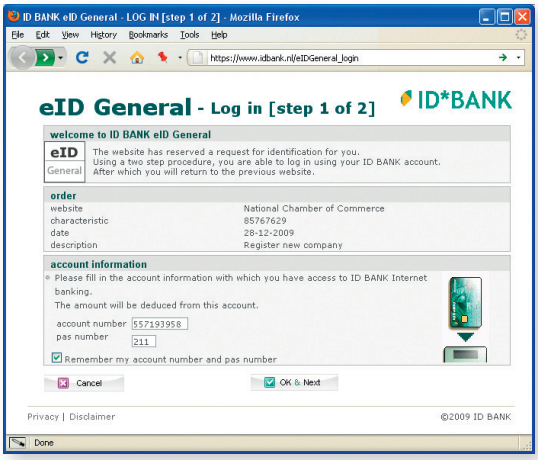
Getting an e-ID General authentication involves the completion of a number of actions on internet pages displayed to the End User. We will present the example of a EU Member State End User that wants to register at the Chamber of Commerce of another EU Member State. Again this example is fictitious, but will show the user perspective on how a domestic authentication means is used to authenticate at any European e-government service.



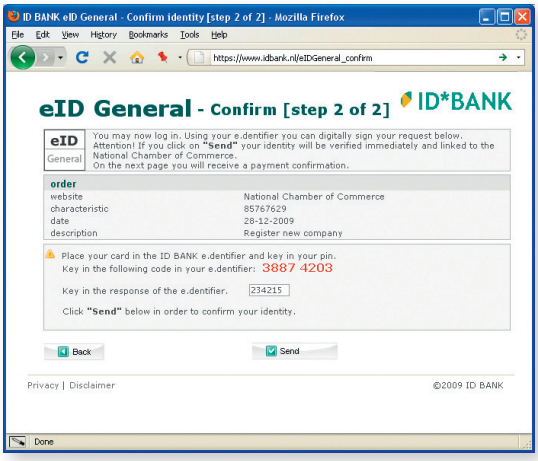
On the website of the Chamber of Commerce the End User fills in the forms that are necessary to register a company in that EU Member State. Once this is completed the user selects signing the registration using the e-ID General solution.



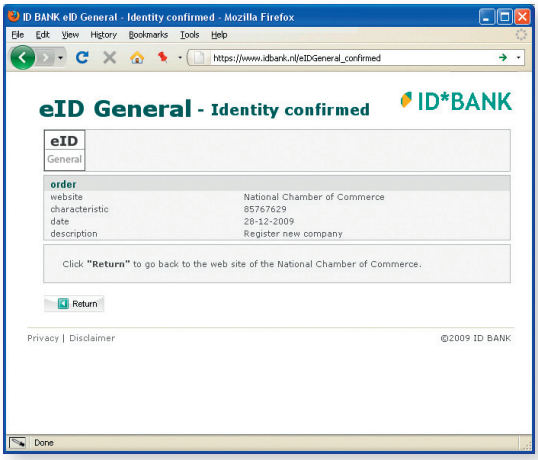
The End User can now select an Authentication Provider from the list of participating parties that offer authentication means. In this example the user selects the bank he or she uses for internet banking, although several other types of Authentication Providers can participate, as long as they comply with the scheme requirements.



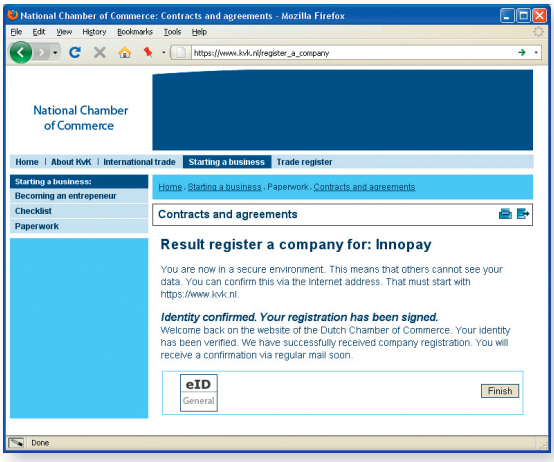
The e-ID request for authentication of the user is now routed from the E-service Provider (in this example the Chamber of Commerce) via the Routing Service to the login screen of the selected Authentication Provider (in this example, the user's bank). The user then follows the bank's standard login procedure.



The Authentication Provider displays the relevant request for authentication to the user. The request is authenticated using the standard procedure of the Authentication Provider. If the authentication succeeds then the response message is generated and...



...the End User receives confirmation. The End User can now return to the website of the E-service Provider (the Chamber of Commerce).



The E-service Provider immediately retrieves the result of the request for authentication via the Routing Service. The Authentication Provider (the bank) has issued confirmation to the End User. When the End User returns to the E-service Provider, the latter checks the integrity of the transaction result that has been received (the authentication), stores it, and continues with the requested process or service.

The process described above is just one example of an application of e-ID as a scheme. However, users will need to complete the same general procedure for other online processes.

5.3 E-service Provider

An E-service Provider wishing to accept the e-ID authentications will need to register with a Routing Service. Subsequent to registration (and further verification, as well as a risk analysis) the Routing Service will connect the E-service Provider to their system. To this end the E-service Provider will need to integrate the e-service application with the Routing Service's platform. The necessary aids and support may be provided as part of the Routing Service offerings.

Once connected, the E-service Provider can accept and process authentication requests of e-ID End Users. The E-service Provider is expected to retrieve the result of each transaction from the Routing Service immediately after the completion of requests for authentication. With a successful transaction this is the real time authentication.

The E-service Provider can receive information at the level of individual authentication requests, and can also make use of any Routing Service's supplementary services such as additional management information.

In principle, E-service Providers can connect with more than one Routing Service. This opportunity can be of interest for a number of reasons, such as the distribution of risk (redundancy) and optimisation of the fees.

5.4 Routing Service

A Routing Service wishing to join the e-ID General scheme and develop and offer e-ID routing products in the scheme will need to register with the Scheme Management Organisation and obtain a Routing Service licence. To this end the Routing Service is issued a unique e-ID Routing Service ID for use in the network.

The Routing Service offers routing products to E-service Providers. The Routing Service can design the Routing Service products as required, providing that they comply with all the conditions specified in the scheme documentation.

The Routing Service can assign the performance of specific tasks to external parties (for example, an Acquiring processor[7]).

The Routing Service can use terms and conditions that are centrally specified (by the Scheme Management Organisation) to reach commercial and bilateral agreements with all Authentication Providers of the scheme. Alternatively, depending on the business model specified for the e-ID General scheme, this can also be done bilaterally between all Routing Services and Authentication Providers.

5.5 Authentication Provider

An Authentication Provider wishing to join the scheme and develop and offer e-ID authentication products for End Users will need to register with the Scheme Management Organisation and obtain an Authentication Provider's licence. To this end the Authentication Provider receives a unique e-ID Authentication Provider ID for use in the network.

Authentication Providers offer products to the End Users, in this example a means of authentication. The Authentication Provider can design the products as required, providing that they comply with all the conditions specified in the scheme documentation.

The Authentication Providers can use terms and conditions that are centrally specified (by the Scheme Management Organisation) to reach commercial and bilateral agree¬ments with all Routing Services of the scheme. Alternatively, depending on the business model specified for the e-ID scheme, this can also be done bilaterally between all Authentication Providers and Routing Services.

7 An explanation of 'Acquiring processor' is given in the Annex.

Conclusion and Opportunities

In the previous two chapters we have explained the basic principles of how e-ID as a scheme could work. We described the benefits of the 4-party model approach and how this solution could work for a user. In this final chapter the most important findings are reiterated. Finally, some interesting opportunities that arise once a sound e-ID infrastructure is implemented are discussed.

6.1 Conclusion

The importance and urgency of sound e-ID solutions in Europe is undisputed. Many solutions already exist but unfortunately as of yet none of these solutions provide cross-border interoperability. The fictitious 'e-ID General scheme' as currently developed into a business-to-government version in The Netherlands, addresses this challenge as a network problem. Its main difference from current e-ID models is the separation of the party issuing the means of authentication and the party routing e-ID transactions. This leads to a 4-party model that allows for endless scalability. All roles of the parties are described in a set of agreements, referred to as a scheme. All parties that adhere to the scheme can join the e-ID network. This model has a proven track record in global payment networks and could bring e-ID several benefits. The agreements assure the interoperability of the network and stimulate cooperation. E-service providers and End Users will have the freedom to choose their way to access the e-ID network: this will stimulate market competition leading to enhanced and innovative value added services. From the successful payments systems that apply this 4-party model we learned that the re-use of existing solutions provides a high user friendliness and low acceptance barriers. Altogether this new approach to the e-ID challenge could be an interesting approach for pan-European interoperable e-ID solutions.

6.2 Opportunities

6.2.1 Application in adjacent spheres

In this document, the e-ID solution is only regarded to be used by governmental E-service Providers. However, the need for reliable online authentication and identification stretches out to the fields of business-to-business and business-to-consumer. An e-ID scheme can be broadened and used in business-to-business and business-to-consumer settings as well. The widening of the scope of an e-ID scheme exerts its influence on various other network issues:

- An excessively broad scope results in additional complexity of the network. The number and complexity of the rules required for the appropriate management of the network will increase with the range of users and areas of application. This can have an impact on both the network and the level playing field.
- An excessively narrow scope will impede the network effects. The gains available to the participants in the network will be limited and the network will not grow. This will exert an influence on the business case.

Choosing the right scope for the application of the e-ID scheme will have a positive effect on the usage and growth of the network. While the scheme can initially be developed for e-government purposes, keeping in mind the broader application of the network is essential to reap its full potential.

6.2.2 Value added services

So far we have regarded e-ID as an abstract service. In reality, there can be various different services derived from secure authentication. In many European countries, there is a basic need for secure login to governmental websites and applications that hold valuable and privacy sensitive information. In addition to secure login, one could think of the following additional features for the e-ID network:

- **Single sign-on:** this can help to facilitate transactions that involve multiple E-service Providers, where otherwise the End User would have to login multiple times.
- **Digital signing:** the secure authentication means can be used to create electronic signatures, for example to enable document signing.
- **Attribute collection:** the End User can authorise the collection of additional information about the person or entity, e.g. address, nationality.
- **Attribute verification:** it is not always necessary to obtain personal information, but verification of a claimed (sub-)identity can be sufficient. A good example is age verification (e.g. is this person over 18?).
- **Mandate management:** within companies, employees act on behalf of their company when using specific electronic services. A company may want to delegate authorisations for the use of these services so that access to these services by can be managed efficiently.

During the development of the e-ID scheme the value added services could be kept in mind. Decisions have to be made about features that are part of the core functionality (collaborative) and the services that could possibly be added to the proposition (competitive). Leaving room for additional services could stimulate innovation and further growth of the network.

Terminology

The use of the terms with the notes listed in the following table is applicable to this document.

TERM	NOTES
Account	The account maintained with an Issuer and Acquirer used for processing the transactions.
Acquiring processor	A party that, within the scope of the e-ID scheme, can assume the responsibility for carrying out part or all of the transaction-processing duties of the Routing Service, under the overall responsibility of the Routing Service.
Authentication (End User)	Authentication is the term used for the verification of a claimed identity with the objective of recognising the user (such as a person or company). Authentication is based on the use of what are referred to as 'means of authentication'. Examples of means of authentication in the real world include passports and driving licences. Other means of authentication are used in the electronic world, since the person involved has to be recognised by a computer system. Examples of means of authentication in the electronic domain include usernames and passwords, tokens, cards with PIN codes, as well as more complex forms such as 'PKI cards', which improve the reliability of the correct recognition of the user.
Authentication Provider	A party that offers End User authentication means, which can be used online to prove a claimed identity. The Authentication Provider is also responsible for the enrolment of End Users.
Competitive domain	Part of the market where market parties compete, typically with their own service offerings enabled through a common infrastructure in a cooperative domain.
Cooperative domain	Part of the market where market parties cooperate, typically to create a common infrastructure to enable competitive service offerings.

TERM	NOTES
Digital signature	When properly implemented the digital signature gives the receiver reason to believe the message was sent by the claimed sender. The legal consequences of the digital signature are implemented on a national level according to the European Signature Directive. Within this context, the Qualified Electronic Signature (QES) is legally equivalent to the handwritten signature.
End User	A person or entity (e.g. enterprise, government) that wants to use electronic services, and has to authenticate itself in order to do so.
E-recognition	The process of electronically verifying whether a person acting on behalf of an organisation is granted by the organisation to do so in the context of a specific transaction, in combination with identifying the organisation itself.
E-service Provider	An institution (e.g. government) that offers online electronic services to End Users. Access to these services requires some form of electronic authentication.
Identification	Identification entails linking a set of specific data to a person (the user) to distinguish that person from other persons. These persons can be both natural and legal entities. The set of specific data required for the unique identification of a person depends on the context: when, for example, an individual is to be distinguished than the citizen's service number can be used. Enterprises can be distinguished by their unique Chamber of Commerce registration number.

TERM	NOTES
Public Key Infrastructure (PKI)	An establishment of architecture, technology, organisation, procedures and rules based on public key cryptography, aimed at enabling reliable and secure electronic communication and electronic services.
PKIoverheid	The Public Key Infrastructure (PKI) developed by the Dutch government: an infrastructure using qualified certificates to ensure secure identification of users, for example used to digitally sign documents.
Qualified Certificate	A certificate that is issued according to official national or European regulations by an official certificate service provider.
Qualified Electronic Signature	An advanced electronic signature based on a qualified certificate and created by a secure signature creation device.
Routing Service	A party that offers E-service Providers access to the e-ID network. To do so, the Routing Service is connected to all participating Authentication Providers.
Scheme	The whole of regulations governing the development and marketing of the defined product or services within the scheme. This also defines rules for market entry, as well as maintenance of the regulations itself.
Secure Signature Creation Device (SSCD)	Device that can be used to place a digital signature in a secured way, meeting the criteria as outlined in the Directive 1999/93/EC of the European Parliament on a Community framework for electronic signatures.

Publisher's imprint

Published on request of the Ministry of Economic Affairs.

Authors

Innopay:
Leendert Bottelberghs
Cassandra Hensen
Chiel Liezenberg

With special thanks to Bart Giesbers for reviewing this document.

Design and layout
www.**myriad**design.nl