



Secure use of the eID



Contents

eGovernment and electronic identification	4
Challenges	5
Standardisation.....	5
Legislation	5
Member states' initiatives	6
The Austrian sectoral model.....	6
The Belgian model	6
Trust is key	8
eID for eGovernment	8
eID for e-Inclusion	8
eID and the Belgian knowledge region	9
The eID card reader label.....	9
Joint efforts.....	9
The DIS institute initiative	10
Policies, Design, Technology, Legislation.....	10
Policies.....	10
Design	11
Technology.....	13
Legislation.....	13
eID for maximising user convenience: three cases.....	16
eID and the Kruispuntbank voor Sociale Zekerheid.....	16
eID and the Vlaamse Maatschappij voor Watervoorziening.....	17
eID and Acerta.....	18
Conclusion.....	19



This paper is based on the information presented during the L-SEC eID event, March 14, 2006.

The following topics were presented:

De eID op kruissnelheid

Peter Vanvelthoven – Minister van Werk en Informatisering

Electronic identity in an information security framework: A regulatory approach

Dr. Andreas Mitrakas, Legal Adviser, European Network and Information Security Agency

eID - The future in Europe

Reinhard Posch - CIO of the Federal Government of Austria

Europese procedure eID kaartlezers en behoeften op niveau van toepassingen

Jan Deprest – Voorzitter Fedict

Gebruik van de elektronisch identiteitskaart in de sociale sector: concrete toepassingen en toekomstige visie

Frank Robben – General Manager Kruispuntbank Sociale Zekerheid

eID richtlijnen en label: de kaart, de toepassingen en de gebruikers op één lijn

Jurgen Truyen - Manager L-SEC

Policy Guidelines: Structural change in your security management?

Gilbert Van Fraeyenhoven – Partner Ernst & Young Technology, Security and Risk Services

Case Study: Implementing eID at Acerta

Nils Meulemans - CTO SecurIT

No quality without control: Technological guidelines

Kim Van Esbroeck – Marketing Manager Integri

Application Design Guidelines when implementing eID based Electronic Signature, Authentication and/or Data Capture

Olivier Delos – Partner Sealed

Case Study: eID als trigger: het verhuisproces online

Jan Hammenecker - Vlaamse Maatschappij voor Watervoorziening

Juridische aandachtspunten bij eID-toepassingen

Professor Jos Dumortier - Professor ICRI K.U.Leuven

Geert Somers - Associate Researcher, ICRI K.U.Leuven

Questions and answers

Ronny Bjonas – Security Strategist Microsoft

Hugues Dorchy – eID Program Manager Fedict

Jos Dumortier - Professor ICRI Leuven

Sylvie Lacroix – Partner Sealed

Carlo Schüpp – Director Deloitte ERS

Jurgen Truyen – Manager L-SEC

Kim Van Esbroeck – Marketing Manager Integri

Gilbert Van Fraeyenhoven – Partner Ernst & Young Technology, Security and Risk Services

This paper is offered for information purposes only. L-SEC makes no representation or warranty, express or implied, of its accuracy or completeness. L-SEC assumes no liability for the use of or reliance on this information in this paper, or any of the referenced materials.

eGovernment and electronic identification

In June 2005, the European Commission adopted the initiative “i2010: European Information Society 2010”, to encourage the development of the digital economy and an inclusive information society. The ambitious goals set out in this initiative were at the core of the 2005 Ministerial eGovernment Conference in Manchester. During this conference, the third in a series that started in 2001 under the Belgian Presidency of the European Council, the stress was on accessible, citizen-centric eGovernment services. Electronic identification is a major facilitator for these services, as the 2005 Ministerial Declaration states:

“By 2010 European citizens and businesses shall be able to benefit from secure means of electronic identification that maximise user convenience while respecting data protection regulations. Such means shall be made available under the responsibility of the Member States but recognised across the EU.”¹

eGovernment leads to modernized public administrations, that offer citizens improved, efficient and personalised services. For businesses, eGovernment can lead to more efficient cooperation between the public and private sectors. Identity management, in this respect, is about ensuring that digital identities can help legitimate users access eGovernment services.

Identity tokens like the eID can be used for traditional as well as online interactions between citizens and government services, and in contexts of law enforcement and public security. But digital identities also play a role in the interactions between public administration databases. The digital identity is what links a citizen's data in one repository to the same individual's information in another. Information about citizens is distributed among several systems, and is at the heart of various transactions, and processes, completed via a wide variety of devices and applications. Moreover, citizens can act as private persons, but also as mandatory, as representatives of organisations, or of a certain profession. Solid identity management systems and practices are a basic requirement for the development of interactive e-commerce and eGovernment applications.

Over the past few years, the character of typical eGovernment transactions has evolved. The first eGovernment applications were informative transactions, whereby citizens could access information online. In a second phase, they evolved to become one-way performative transactions. Citizens would typically download a form, print it, manually complete it and sign it, then send it on by regular mail. With e-payments and e-signatures, a next phase started, introducing two-way performative transactions. Today's processing environments have called for fully-fledged eGovernment transactions, like e-Invoicing and e-Procurement. In the global economy, these transactions are essentially international. For eGovernment to take shape in, cross-border operability is an absolute necessity.

¹ All information concerning the 2005 Ministerial eGovernment Conference is available from <http://www.egov2005conference.gov.uk/>, and from http://europa.eu.int/information_society/activities/egovernment_research/minconf2005/index_en.htm

Challenges

In January 2006, the European Commission report, “Your Voice on eGovernment 2010”, was released. It included the input of more than 400 respondents, including citizens, representatives of public administrations and businesses, who answered questions concerning eGovernment. The survey revealed that the mutual recognition of the electronic identities of different member states ranked highest among the priorities for achieving the objectives and benefits of electronic identification and authentication for public services. A potential lack of interoperability was considered the biggest barrier.

Next to interoperability of the electronic identities, identity management in an international context introduces other challenges, like the mutual recognition of electronic signatures, and of the end user registration processes, which form the basis of reliable electronic identities. Other areas that require recognition between member states are authorisation management and the use of attributes, to name just a few. In view of applications that are used in the global economy, and that are subject to specific legislation, like digital tachographs, and e-Invoicing applications, the link between identity management and application is another area of concern. Member states also need to cooperate to tackle the growing threat of identity theft, and to safeguard the overall security of the identity management systems they deploy.

Standardisation

Standardisation is a first step in overcoming interoperability challenges. The ICT Standardisation Board (ICTSC) was set up in 1998 on the initiative of the European standards organisations CEN (European Committee for Standardisation), CENELEC (Electrotechnical Standardisation) and ETSI (European Telecommunications and Standards Institute). ICTSB created EESSI, the European Electronic Signature Standardisation Initiative in 1999, to coordinate standardisation activities related to the implementation of the European Directive on electronic signatures (Directive 1999/93/EC). In July 2003, the results of the EESSI initiative were published in the Official Journal.

Within ETSI, the technical committee ESI (Electronic Signature Infrastructure) works on standardisation efforts in the area of electronic signatures, with certificates for eAccounting as one particular area of interest.

Within CEN, the efforts in the area of ICT are centralised in ISSS, the Information Society Standardization System. Here, e-Invoicing is one of the areas of interest. The CEN/ISSS eInvoicing Workshop will present its deliverables to the public in April 2006.

Standards drawn up by these standardisation bodies are leveraged by the member states. ETSI TS 101 456, for instance, is a landmark for qualified signatures, listing the policy requirements for certification authorities that issue the certificates to be used for generating these qualified signatures. Compliance with the standard, which covers diverse aspects ranging from issuing, validation and revocation to format and policy management, ensures that qualified signatures can be recognized across domains and member states.

Legislation

ENISA, the European Network and Information Security Agency, is involved in security related legislation that addresses deficiencies and interoperability in the European internal market. Cases like Enron and Parmalat caused the enactment of new corporate governance regulations, in the United States as well as in Europe. Currently, directives concerning the content and publication of financial statements and annual reports are being reviewed. Accounting directives, like 83/349/EEC and 78/660/EEC will be modernised, to enhance corporate governance in Europe. Reports are will be made available in electronic form, and electronic signatures will play an important role in this respect.

Advanced electronic signatures, as described in Article 2(2) of Council Directive 1999/93/EC are required, to guarantee the authenticity and integrity of the electronic documents.

Several member states have taken local initiatives to facilitate the use of electronic identities, like the distribution of electronic identity cards in Belgium, and the introduction of a biometric passport in the UK last March, to be issued to UK applicants gradually from August 2006 onwards.

Member states' initiatives

The 2005 Ministerial Conference Declaration specifies that it is each member state's responsibility to provide citizens and businesses with secure means of identification to be recognized across the EU. Member states are currently introducing local eID schemes that are based on a variety of models. Each model represents a specific answer to the challenge of balancing efficiency and users privacy. Within a European context, each model has to accommodate interaction with foreign eIDs.

The separated model, as it is used in France, allows for a separate eID per application. In the flat model, adopted in some of the Scandinavian countries, one eID is used to access several applications. The sectoral model provides a core eID that is linked to several application-specific eIDs. This model is the foundation for the Austrian eID.

The Austrian sectoral model

Austria's electronic identification scheme involves secure, so-called sector specific digital certificates. The scheme promotes interoperability, and facilitates incorporating eIDs of other member states into the local eGovernment processes.

All Austrian citizens have an identifier that is stored in the public resident register. For each citizen, a source PIN is generated from this identifier. The source PIN is owned and controlled by the citizen, and cannot be stored in any database. In Austria, passports are not legally required, so citizens can also store their PIN on other media than the traditional smart card. They can opt for a mobile phone, an affinity card or a banking card. Several entities can issue eIDs: public institutions, but also private organisations, like banks.

Each company or institution is identified as a sector. Austria uses sector-specific PINs for identification and authentication against separate applications. Sector-specific PINs are generated based on the combination of the citizen's source PIN and the code that has been assigned to each separate sector. The sector code is generated using a one-way hash, so the source pin cannot be calculated from the sector-specific PINs. As a result, identities cannot be linked across services, and privacy is protected.

Authentication is completed via an electronic signature, for which the digital certificates have been stored on the eID. For interoperability with other member states, the Austrian system creates substitutional source PINs based on other member state's eIDs. As a result, foreign eIDs can be used to access Austrian applications. The Austrian eID system has been proven to be interoperable with the Belgian, Italian, Finnish and Estonian national eID cards.

The Belgian model

The Belgian eID is an essential part of the local e-government policy. It is a lever for the development of e-government services, for the growth of the e-society and for promoting Flanders as a knowledge region. The Belgian eID is a smart card containing 2 certificates: one for authentication, and one for generating digital signatures. The Belgian eID also contains identity data, more specifically the identity data that are also visible in printed form on the card, except for the address of the cardholder, which is only stored in electronic form. Frequent requests to include other details, including vital health information like the citizen's blood group or whether he or she suffers from diabetes, have so far always been rejected. The rationale behind the limitation of data on the card is that there should be a clear distinction between public and private data, and that any private data should receive the highest possible



protection. The card can, however, be used as a key to access centrally stored information. This principle will be applied when the functionality of the current social security information card (SIS card) will be integrated in the eID.

10.000 cards are produced every day, and by the end of March 2006, over 2,4 million eIDs will have been distributed among the Belgian population². 15.000 twelve year olds have been offered a card reader when collecting their eID. The readers are also being distributed via stores nationwide.

Some changes have been made to the first Belgian eID specifications. In the first version, the certificate used for signing, which is disabled for minors, could not be activated once they reach the age of 18. This has now been changed.

² Exact data and graphs are available from <http://godot.be/eIDgraphs>.

Trust is key

Citizens clearly agree that the eID is a valuable tool for enhancing public trust in electronic public services. Half of the respondents participating in a survey by Fed-e-View confirmed that the eID would heighten the security of interactions on the internet. As the eID can provide a uniform, unambiguous way of authenticating against several applications, it will increase usability for all user groups, both for civil servants and for citizens. The card is not a contact less card, and does not include RFID technology, nor are there any other data on the chip than the identification data that have always been available on the traditional ID cards. Moreover, to activate the keys stored on the chip, users always have to enter their PIN. These measures have been taken based on the view that maximal user confidence is required to ensure the full deployment of the eID.

eID for eGovernment

Within the Flemish government, Tax-on-Web is one of the applications offered. In the past three years, the number of users has multiplied from 58.000 to 580.000. In the field of social security, nearly all notifications can be completed electronically, using the eID. The eID also allows citizens to access their personal national registry file via <https://mijndossier.rn.fgov.be>. They can verify their data and check who has been granted access to these data.

In a number of art academies throughout Flanders, enrolment procedures at the start of the academic year are sped up as student identity data are captured automatically from the eID, rather than filled in manually. The Flemish Housing Society (Vlaamse Huisvestingsmaatschappij) uses the eID to accelerate the application procedure for social rental properties. An internet application ensures that all data required to complete the application file are requested and collected electronically.

The “eRegeren” project of the Flemish government simplifies the process of putting topics on the agenda of the Flemish Government. As part of the process, files are exchanged and followed up electronically.

Some municipalities have opened e-counters, offering electronic services based on the eID, like the retrieval of official documents. In some towns, access to the local libraries is based on the eID, while in others, access to local waste recycling parks is granted on the basis of the address information stored on the eID card.

More applications are being developed at the moment. “BeHealth”, for instance, will become the portal of the Belgian health sector, where all parties involved in healthcare to the general public can exchange information. “Phenix” is the new information system in the Belgian judiciary system, based on electronic files. Selor, the recruitment agency of the federal government, allows applicants to track their personal application using their eID.

eID for e-Inclusion

The eID is part of the government’s eSociety strategy, which has led to initiatives like the “Internet for all / Internet voor iedereen” offering, and the distribution of card readers among twelve year olds. E-Inclusion also applies to children under the age of twelve. They will receive a secure means of identification and authentication so that they too can be part of the information society, and register, for instance, electronically at the local library. The “Safer Chat” initiative invites youngsters to use their eID to access a secured chat room; secured in the sense that the age data on the card are used to ensure the chat room can only be accessed by minors, not by ill-meaning adults. Another initiative is the ethical ID programme developed by CIBG (Centrum voor Informatica van het Brussels Gewest), a card reader programme that masks the data that are not relevant to a certain action, and only outputs the result of the relevant check on the eID data. When, for instance, only senior citizens can apply for a reduced fee entry ticket, age is the only relevant part of information that has to be shown to the operator.

eID and the Belgian knowledge region

The eID is an important tool in the promotion of the knowledge region. Belgian universities are putting the Lisbon objectives into practice, putting Belgium on the map as a European knowledge region, and generating economic growth. Belgium plays a pioneering role in this respect, with foreign delegations visiting governmental organisations and universities for knowledge sharing. At the same time, multinationals, like Microsoft and Adobe consider Belgium as an excellent breeding ground for eID application projects, which brings foreign investment into the region. The Belgian eID expertise also opens business opportunities abroad.

The eID card reader label

To exploit the full potential of the eID, home users and businesses need reliable, trustworthy eID readers. Several types of card readers are available, from basic readers for home use, to those with screens and secure pin pads, as used in shops and banks. Fedict identified the trustworthiness of card readers as one of the important requirements for the success of eID applications. Card reader manufacturers produced a wide range of products, often including extra features, which made it difficult for consumers to select the product that suited their needs. Fedict decided to establish an eID reader label to could help consumers select a reliable reader, would guarantee compatibility and raise overall consumer trust.

In cooperation with sector organisation Agoria, Fedict provided a series of test script that could be used by the manufactures to determine if their readers were eID compliant. The card reader label is based on a set of well-defined procedures and test tools. The requesting party can download the Fedict software, executes the scripts, and submit the test results to Fedict. After approval of these results, Fedict issues a registry number and publishes the information on its eID website (www.eid.belgium.be). Today, more than 25 readers have been proven compatible. The full list is available from <http://www.cardreader.be>.

The eID card reader label was set up to contribute to the overall trust that is required for eID applications to take off. For eID applications as such, the Belgian government decided not to initiate actions from government services, but to support initiatives based on best practices and expertise from the industry. The DIS initiative is an important milestone in this respect.

Joint efforts

The introduction of digital IDs for citizens is the result of the work of three main groups of actors. The government can provide the platform, and ensure that the legal framework is in place. The government acts as the trustworthy issuer of the cards. As part of its social responsibility, in providing digital IDs, the government has to ensure it promotes e-inclusion, closing the digital cap. The government also has to create awareness, showing the public which advantages the eID can bring, like secured access to internet resources, faster and error-free data capture, or convenient digital signing.

The industry, a second group of stakeholders, has to create and provide applications that can inspire governments and individuals to make the most of the technology at hand. To make this happen, companies should think beyond their own borders, looking for possibilities to include new functionalities that will benefit customers and, therefore, generate new business. Even though the eID is unexplored territory to many, companies should embrace innovation and include eID functionalities in their applications.

Promoting the eID involves an open view, and willingness to evolve, both from the government and from the industry players. A specific mind set is also required from the citizen, who has to be willing to use the new functionalities offered.



What binds the three actors, government, industry, and citizens, is a relationship of trust: trust that efficient and reliable applications will be provided, that the eID protects citizens' rights, and that the legal framework is established.

The DIS institute initiative

As an information and networking platform for all parties involved in information security, L-SEC wants to contribute to the required trust establishment. During its annual eID events, L-SEC brings together representatives of government organisations, of the industry and academic world, to discuss and present eID topics.

L-SEC is also initiator for projects, like ADAPID, (advanced applications for electronic Identity cards), the IWT project that aims at developing a framework for secure and privacy-preserving eID applications. This project involves both technical and legal aspects. As part of this project, an extensive list of requirements has been drawn up, ranging from privacy and accountability to usability and social-acceptance related requirements. The L-SEC consortium is also involved in tender procedures, bringing together the technological, business and legal expertise of its members, about forty in total, to submit bids together.

In March 2006, a new initiative was launched to promote trust and to help the industry develop powerful eID applications. DIS institute, an initiative of L-SEC members, was officially launched. DIS institute's mission is to provide structured help to organisations that are building eID-enabled applications, and to increase user trust.

The institute will control, maintain and safeguard the DIS eID standards, and will promote the standard in the market. The DIS eID standard, which is currently being drafted and will be launched this autumn, covers four areas: policies, design, technology and legislation.

The institute will also appoint accreditation partners, to audit companies and verify if they comply with the eID standard. DIS institute will grant certificates after successful audits, and will control the certification process. In the pre-implementation stage, the DIS partners provide companies with advice and training on all aspects of the DIS standard. Once companies have implemented the recommendations, the accreditation partners conduct their audit.

Companies can choose one of two levels, depending on the stakes involved. An application granting access to a recycling park based on the eID, for instance, will be less critical than an e-banking application with eID-based signatures. Once the company has demonstrated it complies with the requirements in the four areas, technology, design, policies and legislation, it will be granted a certificate, a clear sign of reliability, which will increase consumer trust.

Policies, Design, Technology, Legislation

The DIS eID standard is not just another IT security standard. It is in line with other standards in the field of IT security, and as such, it incorporates basic information systems security management principles. The DIS standard, however, is eID specific and has been developed to respond to the industry's particular needs in the development of eID applications. To ensure that all aspects involved are covered, four areas are distinguished: policies, front-end and back-end design, front-end and back-end technology, and finally, legislation.

Policies

The eID security policy touches upon several processes and functions. The information systems that interact with the eID must be developed or acquired as defined in the eID standard. This means they should incorporate security measures as outlined in the technology and design requirements. Counter to what often happens with less sensitive data, eID production data must not be used in a test environment. Segregation of duties is another focal point. All people dealing with eID data need to be fully aware of the importance of security.

They must understand the sensitive nature of the data involved and they have to know which actions to undertake in case irregularities or abnormal behaviour is detected.

Logical access to information systems must be authorised on a need-to-know basis, and the organisational requirements concerning the segregation of duties must be respected at all times. Identity management, authentication and access management should be well considered and should ensure that data are accessed in accordance with the policies.

As far as IT operations are concerned, they should be carried out regularly, to ensure the continued integrity and confidentiality of the data, and the availability of the systems. Special attention should be paid to media handling and back-up practices. Monitoring should ensure that intrusion attempts do not go unnoticed, that vulnerabilities are identified and tackled and that the quality of the systems is ensured.

Physical access management is a basic requirement too. The facilities must provide the suitable environment that protects the vital components of the information systems and the data stored. Physical access management is related to facility entry controls, employee and visitor access management, and media access management.

Organisations should also be prepared for possible eID related incidents. To this aim, incident response procedures should be set up, defining the required escalation processes, and establishing contacts with legal and regulatory authorities. The organisation has to decide on a communication strategy that fits in with the legal requirements in this respect, and it has to identify which disciplinary actions will be taken in the aftermath of an incident.

It is clear that the eID policy requirements fit in with overall security management requirements. Companies should comply with general security management principles that have not been defined in the eID standard as such. This includes, among others, third party management, sound human resources policies and procedures and solid change management practices.

When the policy requirements have been met, this means that the adequate environment has been created for compliance in other areas, like technology and design, or legislation. For the organisation, this means that the necessary controls are in place. For the citizen, it shows that the prerequisites for the secure use of his personal eID data have been fulfilled.

Design

The eID can be used for data capture, for strong authentication, and for placing digital signatures. The design section of the standard lists requirements for front-end and back-end design aspects for the implementation of each of these functions.

The requirements provide an overview of critical issues to be taken into account when implementing these functions. The list of requirements can be used as a checklist. It ensures the propagation of best practices, and results in trustworthy and reliable applications.

When electronic signatures are concerned, it is important to consider the exact business context and the types of signatures that are required in a certain context. The 1999/93/EC directive defines the electronic signature as “data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication”. The advanced electronic signature is defined as “an electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable”. Qualified electronic signatures are advanced electronic signatures based on a qualified certificate. The qualified electronic signature is the only type of signature that automatically has the same legal value as a handwritten signature.

The context also determines the meaning of the signature. The signature added to an e-mail message is different from the signature added to an e-invoice. In fact, when signing an invoice, on paper or electronically, the issuer confirms that the payment has been settled. Companies could, however, rely on the signature to guarantee the data origin and integrity. A signature validation policy is required to ensure that all parties involved are clear about the agreed function of the signatures added. The policy lists the requirements for signature validation, with respect to particular business needs.

Design is also concerned with the development methods and the security measures taken in the process. The Capability Maturity Model methodology can be adopted to avoid undocumented development, development with unclear behaviour and unclear security levels. Secure development also involves that there are auditable logging facilities, and that; in general, state of the art security measures are taken to ensure secure processes. This involves the use of updated or certified cryptographic libraries, the most recent managed software environments, and adequate protection against malicious software, to name just a few requirements.

The signature creation process imposes its own requirements. One focal point is the appearance of the document to be signed. The signer needs to know exactly what he or she is going to sign. WYSIWIG secure viewers can provide maximum reassurance, and protect against hidden information and code.

To provide the parties involved with information on the signature, an explicit policy signature can be used, which identifies which policy applies when validating the signature. Other additions possible are a time stamp token or time mark (ES-T), or an ES-T with complete validation information (ES-C), or with extended validation information (ES-X). For long-term archiving, the ES-C or ES-X signature may be extended with an extra time stamp or time mark (ES-A).

Signature attributes can identify the signer's certificate identifier, the signature policy, the data content type, the commitment type, and other elements, like the signer's role, the place and time of signing. There are specific requirements for the interface as well. The interface has to be consistent and appropriate, and correspond to the signer's expectations, while error messages and status information should be adequate. An inactivity time-out should be set, and the signer should always be in control of the process. In general, the signing process itself should be protected against threats, like insecure communications, incorrect or invalid certificates, or hidden elements in the signer's documents.

The signature verification process consists of three stages, and for each stage, requirements have been listed. First, the information for verification has to be collected: the signer's document, the signature format and lifetime information, the signature attribute and the certificate path information. Then, the information can be verified. The certificate policy and qualified statement are checked, and the certificate path is constructed and validated. The revocation status of the entire path is checked, time stamps and time marks are verified, as are the signer's attributes. Once the validation is completed, the signature verification output is presented. A final set of requirements lists the recommendations and information presented to the signer: the legal requirements that have been met, information related to rights and duties involved in using the eID, and information concerning the secure viewer.

Just like for signing, specific requirements are stipulated for authentication and for data capture. Here too, several angles are taken into account: the development process itself, the security of the system, the process and the related policies, the information presented to the user, the verification process, and the trusted paths underlying the completed actions.

When applications meet the requirements listed for each of the eID functionalities they offer, this increases their value. When business, legal and policy requirements are fulfilled, and

best practices in technology and security are applied, these results in the level of trust required for the successful introduction of any eID application.

Technology

The technology requirements listed allow application developers to determine whether their solutions contain the correct implementations. This means that the valid use of the eID is supported and that invalid use is handled correctly.

In order to verify if the requirements are met, the applications must be tested. While actual eID cards can easily be used to this end, and are readily available, they will not cover invalid scenarios, which should also be part of thorough testing. This can be solved through the use of test eIDs, but an even more efficient solution is the use of an eID card simulator.

The simulator software runs on a PC, and a probe attached to this PC will replace the actual eID in the testing process. The advantages are clear. One software package contains all test scenarios that are outlined in the standard, both the ones for valid and for invalid attempts. Any type of behaviour can be programmed, and new or changed test scenarios can easily be added. Though the initial investment may be larger, using a software solution rather than actual cards is cost-efficient in the long run.

The DIS eID standard includes several test scenarios that should be run in order to check the technology underlying the eID application. A first set of scenarios is aimed at checking the compliance with different card versions, to ensure that new versions of the card's operating system are supported too.

Another set checks the compliance with different card conditions. When a card has been revoked, for instance, access to the application should be denied, and a valid message should be displayed to help the user rectify the issue. When a user exhausts the allowed number of PIN trials, or the eID has been blocked. Again, the card owner should not be granted access to the application. The system also has to accommodate different card personalisation. It should, for instance, always correctly identify which part of an individual's full name represents the surname, and which part the first name. Card access is another area that needs checking. When a wrong PIN is introduced, the user should be invited to try again, until the set number of PIN trials is exhausted. As long as the correct PIN has not been introduced, access should not be granted.

The application should also comply with the requirements concerning card behaviour. When the card returns an error as a response to a read command, for instance, access should not be granted, and an appropriate recovery process should be initiated. The same applies in case of problems with the verify command.

Sound test practices will ensure that applications meet all the technological requirements to provide businesses and consumers with efficient and reliable solutions.

Legislation

For eID applications to be successful, they must function in accordance with the governing legislation governing the use of the eID, and the personal data it contains, or gives access to. One of the most important regulations in this area is the Privacy Protection law that implements the European directive 95/46/EC. The use of the national registry number, the unique identifier for each Belgian citizen, is also subject to strict regulations. When using the eID in business contexts, there are other aspects to take into account, like the electronic signature legislation, regulations concerning contract conclusion, fair trade practices and consumer protection. In addition, there are laws related to cyber crime, and stipulations on liabilities and continuity.

If applications fail to respect its users' privacy, this has dramatic repercussions. Privacy legislation is of public order. The privacy commission controls the application of the privacy

legislation, and criminal sanctions are imposed in case of non-compliance. Organisations that fail to protect user data will be subject to liability. Moreover, they will cause a dramatic fall in consumer trust.

The DIS standard provides companies developing eID applications with an extensive list of requirements to be met. When organisations comply with legislative requirements, they are also better prepared to respond to potential attacks, or abuse of their applications or systems. And finally, legal compliance is important in view of general corporate and IT governance.

eID applications operate in several contexts: business-to-business and business to consumer, but also in government to business and government to consumer encounters. A breach of trust in one of these contexts will undoubtedly impact the other contexts as well. eID legislation concerns both authentication using the eID and generating digital signatures using the eID.

The DIS standard lists a number of requirements that have to be met when the eID is used for authentication.

The first parts of the requirements are related to the front-end. The collection of data has to be limited to relevant and necessary data only, while the purpose of data collection has to be acceptable and in line with reasonable expectations.

The user, on the other hand, must receive adequate identification and contact information concerning the provider of the service. When data are stored, users must be given a chance to correct and update their information. Any commercial communication has to be sufficiently identifiable. When publicity is made, this should be done in accordance with legal requirements, and all information offered to the consumer should be in the appropriate language.

Other regulations are related to price indications, which must be clear, and the possibility to report illegal activities to the authorities. There are rules that relate to the presence of a code of conduct and its availability to users, and to password creation, which should be sufficiently randomised. The user should also be informed about proper password use.

The second part focuses on the back-end. Personal data should only be stored as long as they are required, while all user data stored should be adequately protected. European and Belgian legislation is very strict about the transfer of user data outside the EU, where different privacy legislation applies. Access to the stored data has to be limited within the organisation, and third party access has to be controlled. The national registry number must not be used.

Specific requirements have been listed for the use of the eID to generate digital signatures for contracts or for submitting documents to governmental authorities.

A first set is related to the question whether it is legally correct to sign a certain transaction. What should be taken into consideration is the fulfilment of formal legal requirements, which are comparable to those governing the use of traditional signatures. There are some exceptions, i.e. the signing of creation or transfer of rights in real estate, or contracts requiring the involvement of courts, public authorities and professions exercising public authority.

Before asking the signatory to sign, specific information has to be provided. This information includes general terms and conditions, as well as pricing information, information on technical steps to be carried out, the subsequent filing of the concluded contract, and the languages offered for conclusion of the contract. In B2B contexts, the contract between the parties may define other arrangements concerning the information that must be provided.

Once the signatory has completed the signing process, he or she has to be informed about the terms of the contract, and receive an acknowledgement of the receipt of the order, as well as a summary. Again, in B2B contexts, contracts may stipulate other arrangements concerning acknowledgement and summary of the order. When the order has been received, the legal requirements concerning the storage of information need to be met, and data should be stored



as stipulated in the legal limitations, in accordance, for instance, with the proportionality principle.

The DIS standard helps application providers incorporate legal compliance from the initial development stages onwards. This way, companies can be sure to provide applications that meet legal requirements, and contribute to the required user confidence and trust.

—

eID for maximising user convenience: three cases

eID and the Kruispuntbank voor Sociale Zekerheid

The Belgian social sector involves more than 2000 public and private actors. To cooperate, they use a secured connection that also links them to other governmental networks, to the internet and to Isabel, the electronic banking solution. In 2005, nearly 16 million electronic transactions were completed between the social sector on the one hand, and enterprises and citizens on the other.

These transactions involve structured electronic messages, 185 types in total, or are completed via the integrated portal. The portal is also used to provide companies with tailor-made information, via their individual e-box. The same environment includes an integrated e-workspace that allows e-teams to cooperate online, and a data warehouse fed by all social security institutions. The data stored can be used as a basis for policy support, evaluation and research.

The unique identifiers for citizens (national registry numbers) and for organisations play a central part in the transactions. Between the actors involved, agreements have been made concerning the management and electronic storage of authentic data.

As a result of efforts to streamline processes and to manage and exchange electronic data efficiently, the administrative cost for enterprises, due to social sector-related requirements, has decreased with 1.7 billion Euros between 2002 and 2004. The eID can lead to an even higher level of efficiency. Some challenges, however, still need to be addressed. The current eID covers the identification and authentication needs of users over twelve years of age, who have been registered as Belgian citizens. The eID also allows adult users to place digital signatures. For people younger than twelve, or those not listed in the population registers, another solution is required. In some cases, authentication or a digital signature will need to be accompanied by information about the signer's profession, or about the mandates he or she has been given. These mandates or professional states will be linked with specific user rights or privileges.

The Kruispuntbank uses a Policy Enforcement Model that has been established as a joint effort between several public services. Users authenticate against a PEP, a policy enforcement point. Here, the user request is passed on to a PDP, a policy decision point. At this policy decision point, the relevant authorisation policy is retrieved from the PAPs, the policy administration points. In these PAPs, policies are stored and maintained. If required, information is retrieved from the policy information points, which contain information on mandates and attributes. Then, the authorisation decision is passed on to the policy enforcement point, and the user.

With their eID, users can access resources and complete transactions on the portal site www.socialsecurity.be. For employers, this portal allows several functionalities, like the immediate notification of the commencement and finishing of an employment relationship, or several notifications related to social risks, like unemployment, illness, occupational accidents, and more. For citizens, three applications are operational today. One of these is E-LO, which allows employees that have taken a career break to consult their personal time credit information ('tijdskrediet'). Other applications cater for professionals involved in social security operations, like representatives of municipalities, who can apply for allowances for handicapped persons online.

Once the eID has been distributed to all Belgian citizens older than twelve, it can replace the current social security card (SIS card). The eID will then be used as an entry key to the social security data that are securely stored centrally.

eID and the Vlaamse Maatschappij voor Watervoorziening

The Vlaamse Maatschappij voor Watervoorziening (VMW) provides drinking and industrial water, and processes waste water. The company also offers a range of related services. VMW manages 1.060.000 contracts and services approximately 2.600.000 users. The company has always been a pioneer in providing online services. In 2002, VMW introduced the electronic invoice, and since 2003, consumers can enter their water meter readings on the VMW site. Based on their entry, the invoice can be generated within 24 hours, which is much faster than after the traditional on-site readings by VMW representatives.

VMW will now start using the eID to streamline the administrative processing of consumer moves and address changes. Each year, 15% of all VMW users move into a new property. This amounts to a total of 150 000 address changes to be managed by the company. As such, it is one of the most important customer processes, and any cost savings in this area have a considerable impact on the company's expenses.

The priorities identified were clear: there should be a clear business drive, and any changes to existing processes should benefit the customer as well as the business. In order to be successful, processes and applications should be perfect from day one, as consumer trust is key to the success of the investment. When users notice that the system does not work as expected, consumer trust plummets and the success of the application is impacted.

The business drive behind the automation of the customer relocation process was clear: when users change their address, this used to involve paper forms filled out and signed by customers. The same form had to be signed by the persons leaving the property, as well as the new inhabitants, who both had to agree that the filled out meter readings were correct. Once completed, the form was sent to VMW by regular mail. On receipt, the new customer addresses were entered manually into the databases, a final invoice was made for the person leaving the property, and a first invoice for the person moving in. Each step in the process was time-consuming, implied potential delays, while the processing of forms was labour-intensive and error-prone.

Especially in case of errors, the costs were considerable. The return on investment in this case, will clearly be due to a reduced amount of errors. Introducing an automated process, based on the eID ensures correct user data, correct invoices, which lead to more satisfied customers and partners. Moreover, the security offered by the eID, for authentication and e-signatures provides an added plus.

For customers, the automated process implies that they do not need to take a day off to sort out their address change, or to spend any time trying to rectify incorrect invoices.

In order to limit the risks involved in changing a high-impact customer process, VMW opted for a phased approach. The chosen customer process required little re-engineering, and a limited investment. Moreover, the process could be completely integrated into other services, like the e-invoicing and the web index, and back-office processes like the online checks of water use, the use of GPRS for field work and the back-office invoice handling. In a next phase, the eID will also be used as a centrepiece of other customer processes, like the water supply for newly built homes, or for online payments.



eID and Acerta

The Acerta social security fund provides an online service to accountants and internal payroll officers. The so-called “unique counter” gives them access to information on legislation, administrative and financial issues, and allows them to register new companies with the Kruispuntbank voor Belgische Ondernemingen (KBO), where all Belgian enterprises need to register in order to receive an official enterprise identification number.

Before, limited access was granted to users authenticating with a user password combination. They could, for instance, access information on legal issues.

In order to interact with the KBO via the Acerta counter, users had to go through a lengthy registration process, which involved physically visiting the Acerta desk to complete the registration there and then.

The eID dramatically simplified registration and ensured a higher level of security than the former user password schemes. Within the underlying architecture, the SecurIT TrustBuilder, a plug-in for the IBM Tivoli web access management solution, is used for implementing the authentication policy. For checking the certificate status, SecurIT partnered with Intesi. The Intesi PKBox checked the certificate status via OCSP or via the CRLs supplied by Certipost, who provided the certificates used.

The application, open to a limited user group at first, provides a useful test bed for eID applications.

Conclusion

User identification is fundamental to electronic services, both in the private sector and in government services. In e-commerce today, online services are usually only delivered after the payment has been received by the service provider, as there is no real guarantee of the user identity. For e-commerce applications to take off, and for eGovernment to reach its goals of providing user-centric, modern and efficient services to individuals and businesses, the distribution of a secure and trusted identification tool is a vital component.

As several applications in operation today show, the Belgian eID meets the needs of both business and government organisations, and fits in with initiatives and objectives that have been set in a European context. To ensure that the eID is used to its full potential, powerful, secure and efficient applications should be brought to the public.

The launch of the DIS institute and the introduction of the DIS eID standard will help and stimulate companies and organisations to supply these applications, and establish the level of trust that is required for successful eGovernment and e-commerce. As such, the institute contributes to the objectives listed in the Manchester 2005 Ministerial eGovernment Declaration, ensuring that the secure electronic identification tools provided are used to maximise convenience while respecting privacy.