USE OF ELECTRONIC IDENTITY CARDS IN THE PRIVATE SECTOR

Lionel Khalil
LIPN, Institut Galilée, Université Paris 13
99 av. J-B. Clément, 93430 Villetaneuse, France
lionel.khalil@lipn.univ-paris13.fr

Abstract Based on the evaluation of real-life application experiences, we have proposed a definition of Trust- and Quality-based Risk analysis to better understand the user's judgement; we have emphasized that the e-government should be driving the development of the use of ID-cards in the private sector. We have tried to propose basic concepts to urbanise the development of ID-cards: people may accept the constraints of in-depth authentication only in relation to trusted Institutions. Applications of this technology must be limited and separated into categories of equal risk and frequency of use.

Keywords: risk analysis, identity cards, trust

1. Introduction

Banks and other Institutions are currently using paper-based ID-Cards and signatures in their services; so, banks are involved in the development of Electronic Identity Card (ID-card) models. In the past, numerous online payment methods have been devised and their implementation has constituted very instructive but fruitless attempts to transpose and make less visible traditional banking techniques, originally developed with the use of practical media [Bou04]. Whatever their benefits and performance may be like, their deployment has appeared prohibitive faced with competition from less secure systems constituted by the transmission "in mid air" of a bank card number.

Let's define trust as a perception of security and a presupposition of the quality of the Institution. When people talk about authentication in e-technology, they talk as if their only concern is risk management, regardless of the client's perception of trust. The existence of the transaction is based on trust through the authentication of both sides. On the application side, the validation of the commitment of the client's side is rationally based on risk analysis and risk management with regard to the security of the system. On the client side, the

E. Nardelli et al. (eds.), *Certification and Security in Inter-Organizational E-Service*

validation of the commitment of the application's side is based on trust. Thus, the issue of trust is fundamental to the success of e-commerce.

Based on the real-life application experiences of bank and governmental projects, we want to express methodological proposals for organizational issues in implementing ID-cards' urbanisation in a multilateral context regarding the protection and social implications of ID-Cards, such as users' security responsibilities and protection of users' privacy.

In this paper we consider that private sector needs in many cases to identify their clients. Before, they were using the paper based Identity Card. Because of the evolution of the e-government, the private sector should remain involved in the creation of Electronic Identity Card (ID-card) models [Kha03a]. We present two main points to this approach. We consider that the e-government has to lead the development of Electronic Identity Cards or e-ID card, not only for the access to e-government services, but also to be used for business transactions in the private sector. This approach points out that applications of this technology must be separated into categories of equal risk and frequency of use. This makes this approach a good strategy for the implementation of Electronic Identity Cards.

Overview. The rest of this paper is structured as follows: In section 2 we will present a definition of Quality-based Risk analysis. Section 3 motivates the work by showing examples in Europe of the kind of system we would like to model: in some projects the ID-card is only used for access to e-government services. The France case study gives an alternative view, where the private and public sectors share the use of ID-card. Then we would like to argue two points with regard to this subject. In section 4 we formalise the idea that the e-government should be leading the development of the use of ID-cards in the private sector. Section 5 describes why applications of this technology must be limited and separated into categories of equal risk and frequency of use. Finally, we conclude the paper in section 6.

2. Definition of Quality-based Risk Analysis

We remind you of the definition of Risk Management approved by A.N.S.I. [ATIS01]: "The process concerned with identification, measurement, control and minimisation of security risks in information systems to a level commensurate with the value of the assets protected". On the Institution side, the risk assessment is based on a process of analyzing exposure to risk and determining how to best handle such exposure.

Banking experts are using classical risk analysis: the market needs an in-depth authentication payment system with physical use of the card. In the past, there have been fruitless attempts to impose in-depth authentication in e-commerce. The judgement of the market was severe: no added value for high

security payment systems. We think that the risk analysis from the user's view point is different from the bank's view point.

Regardless of the interest of the transaction between a client and an Institution, the evaluation of the risk of the transaction is different for each side because the environments of each side are different. On the Institution side, the risk is evaluated by a process of risk management analysis, and on the client side, the risk is mainly an evaluation based on a quality-based risk analysis.

To define a quality-based risk analysis, we need to define the notion of trust.

In [Men01], Mendez et al. propose the definition of trust developed by Lorentz in [Lor82, Lor01], which provides the following definition: trust is a bounded rational analysis which evaluates an expectation of goodwill and benign intent. This analysis is an anticipation of the behavior for a specific task based on a generalization of normalized behavior for a similar task.

There are 4 segmentations of this analysis :

- assurance - incentive structure,
- commitment (long term relationship),
- familiarity,
- and representation.

Trust is re-evaluated in real-time with new information. A similar definition was expressed in [Kar96] by Karpik. Trust is composed of inductive, calculated, and normative judgements based on an interaction process between respectively emotional, intellectual, and social commitments (see also [Noo01]):

- inductive judgements based on emotional commitments,
- calculated judgements based on intellectual commitments,
- and normative judgements based on social commitments.

Classical risk analysis: a rational analysis is to minimise the exposure to risk based on the evaluation of the damaged and trust is analyzed as a weakness.

without trust, risk is infinite - social judgement is embedded in the risk analysis and trust is a necessary asset to evaluate the risk analysis.

Remark: there is a difference between integrating organizational issues in an evaluation scheme as an asset (for example Human Machine Interaction and social engineering evaluation) and the fact that the system itself is based on trust.

For example, a CA in a PKI is trusted because the Institution that owns the CA is trusted. This trust is mainly outside the scope of the evaluation of the classical risk analysis of the organisation of the PKI.

With this definition, we can precisely define the commitment of both sides in a transaction: on the application's side, commitment is rationally based on classical risk analysis and risk management, and the commitment on the user's side remains how to best handle the risk's exposure, based on a quality-based risk analysis.

On the client's side, the Institution's risk analysis remains both a perception of security and a presupposition of the quality of the Institution. We refer to [Men01, Kar98, Wil93] for a detailed demonstration that Concludes that a transaction is based on an evaluation of "why we conclude a transaction"; and trust and risk management are based on "how we conclude a transaction".

The perception of ID-cards issued by Institutions (such as the government, notaries, banks, the post) is based on a quality-based risk analysis. The evaluation of trust changes with time: in the short term perception, Trust is linked to the Institution; in the medium- term the user re-evaluates the risk through the everyday use of the e-card. The risk management evaluation has to reinforce the trust [Kha03b].

3. Overview in Europe and case study in France

Many member states of the EU (European Union) are currently evaluating the introduction of e-ID cards or have already started deployment. The Electronic Identity Card supports different names: Electronic Identity Card in Italy for example [AFNT04, ACFN+04], ID-Card in Finland, Electronic Identity Card for Belgian Citizens or e-ID for Maltese citizens. These cards are the electronic version of the current National identity card that enables secure access to and use of the e-government services. Two main projects are supported by the European Community: EUCLID and eEpoch [eEpoch01]. EUCLID (European initiative for a Citizen digital ID solution) is a project funded by the European Community under the Information Society Technology programme. It responded to the identified needs of the citizens and the business community by improving the security of transactions and interoperability of the cards. eEpoch is a Demonstration Project of the Information Society Technologies Programme of the European Union and it is organized according to the framework defined by the European Commission. The aim of eEpoch is to demonstrate interoperable and secure smart card based digital identification systems, which provide the levels of trust and confidence necessary for citizens to interact digitally with their national and local authorities and other European institutions [San04].

In some countries the e-government has decided to lead the development of Electronic Identity Cards or e-ID card, not only for access to e-government services, but also to be used for business transactions in the private sector. The Italian project goes further in interoperability between private and public ser-

vices: the Electronic Identity Card includes a National Multiservice Card. In the UK, the NERSC (North East Regional Smartcard Consortium) is a region-wide multi-application citizen smartcard that can be used for travel throughout the North East Region to support local authority public services as well as other commercial applications [NERSC03]. In [Eng02], Engel recalls that the legal issues in relation to the use of public ID in the private sector have already been addressed by the EU.

The French experience is an example of the privatisation of ID-card issuing. For 4 years, the French banks were working on two parallel projects: the Identrus network and Ministry of Finance Certificates (MINEFI). The first one was a worldwide project. But French banks did not find an ideal application for an Identrus Certificate. Therefore the Banks decided not to implement the Identrus infrastructure, but to buy on demand Identrus Certificates (from other Identrus Banks) and brand and resell these certificates to end-users. This position is a defensive position with regard to the development of Identrus Certificates: the major expected benefits of this solution are the short time-to-market and low initial investments. The main concern of the Banks was to control the customer's commercial relationship. Meanwhile, there was cooperation between the financial industry and the Ministry of Finance to agree on common standards for electronic signatures in the e-government and e-banking (except that Identrus certificates are not compliant with MINEFI certificates), with one target being that bank signatures will be used for the e-government, hence enabling government to save on costs [Kha02]. The Ministry of Finance pushed for soft certificates for the e-government three years ago, and banks issued around 30,000 to companies for VAT and social taxes; each year extra services have been added. These may also be used for corporate on-line banking. Although the Ministry of Finance has been pressing banks to issue its certificates, the Ministry of the Interior wants now to issue its own certificates. Even though this cooperation was a success, the privatisation of ID-cards issued for corporations was not accepted in all branches of government, mainly because the project was held by the Ministry of Finance while the Ministry of the Interior was historically in charge of Electronic Identity Cards. Today, the Ministry of the Interior is trying to take over the project from the Ministry of Finance. One of the main subjects of disagreement lies in the privatisation of Electronic Identity Card issuing. But the new project to reissue Electronic Identity Cards for corporations and small and medium enterprizes will face two problems: the disagreement of banks who have already invested in the project of their supervisory Ministry, and the current lack of budget from the government. Unfortunately, this situation sends unclear messages to the market and reduces trust in e-government policy. The weaknesses of the project were clear: no interoperability between ID-Cards for corporate on-line banking. Banks remain in competition and those certificates are rejected by other

Ministries. Nevertheless, the e-government should be leading the development of Electronic Identity Cards and sending clear messages to the market.

4. The e-government should be leading the development of ID-technology.

In real life, business partners and customers do not need an in-depth authentication of their partners. There are two exceptions: bill payments and credit services for Banks, and government taxes and official documents. The law admits the validity of contracts even when partners do not know each other well (see [Kha02]). After the Internet Revolution, each government decided to offer on-line services. But the problem with in-depth authentication remains the same as in real life. The whole economy, meanwhile, has been working on-line without in-depth authentication. ID-cards are a concern for banks and the government and one of them has to create the market. If Electronic Identity Cards are privatized the following problems may arise: banks remain in competition, as, even though they are taking a State role, they will prefer to promote their own branded Electronic Identity Card which is linked with their own products and services, even in an interoperable model. The privatisation of ID-cards is too sensitive an issue. The e-government has to mandate the interoperability of private Electronic Identity Cards in order to fulfil the needs of the Corporations and Small and Medium Enterprizes market. The main question is: under what conditions will the whole market accept an all-in-one card? Some elements of the answer lie in the notions of protection of the right to privacy and liberty, added value, and risk management. If banks have to develop an e-card project, the banks should follow the lead of government policy and priorities. One of the reasons is that the market needs a clear separation of powers.

5. The market needs a clear separation of powers.

People accept to transfer some of their power in their ID-tokens. People do not make the distinction between authentication and authorization; so while a token can give access to its holder to many services, the risk to the holder is the sum of the risk of each service. The perception of the token is both positive and negative: positive because it opens up many services and negative because the holder has to protect it. For example, in the US, with a Social Security Number and a birth certificate one can get a passport, a driving licence and a bank account. In this section, we propose basic concepts to urbanise the development of ID-cards to respect users' needs, users' protection and a multilateral context.

Urbanisation constraints of users' needs are a direct relationship between facility of use, frequency of use and risk. The holder's protectiveness towards the token is higher when the power given is higher, and is higher when acti-

vation of the card is easier. "People don't want to pull out their passport each time they need to buy groceries." Different kinds of services require different levels of power transferred. The perception of the added values and risks of carrying an ID-card depend on the level of power which is transferred in this ID-Card. Thus, only ID-Cards with the same value and the same frequency of use can be merged.

Urbanisation constraints to respect users' protection become stronger. Due to people's desire to defend a strong sense of liberty, they prefer to separate different aspects of their lives. People are sensitive to the protection of their right to privacy. Even though the service might say that it is only accessing a specific aspect or part of a multi-application, people won't trust it. People do not want to use their private ID-Cards in a professional situation. Their cautiousness reflects their reluctance to mix different aspects of their lives. The protection of privacy pushes towards separate identifiers for different activities in life: professional badges, personal Security Social Number, personal ID-card and personal driving licence.

In addition, if people lose an all-in-one ID, they have no other ID to fall back on. All services would be blocked. More than one card would avoid access to public services being denied.

Urbanisation constraints will manage organizational security in a multilateral context. Current risks will be amplified. Urbanisation has to manage the order to obtain different cards: no opportunity for a procedure allowing the creation from scratch of a false ID. In a multilateral context, do not create an all-in-one pass card which will attract criminal interest.

A potential solution would be to have more than one card: one for everyday life and one for more sensitive information. The characteristic of the everyday life card would be to benefit from quick issuing, and services with a high frequency of use and low risk in the transaction, such as some administrative services, transport services, public leisure services, student ID, library access, canteen pass, or electronic purse. On the other hand, for the second more classic ID-card, we can imagine in-depth control upon issuing. All the e-government services including a full recognized electronic signature like a traditional paper-based ID-card. Depending on the country the driving licence and the Social Security Card could be separated or merged with one of these two cards.

Thus the development of private ID-Cards has no hope outside the policy of an ID-Card launched by the government. The private sector will take advantage of remaining close to the e-government standards. We will leave the case study of the difficulty of embedded applications between banks and government for future work.

6. Conclusion

We have shown that several interesting projects have been launched within a precise framework. Based on the evaluation of real-life application experiences, we have proposed a definition of Trust and Quality-based Risk analysis to better understand users' judgement; we have emphasized that the e-government should be driving the development of the use of ID-cards in the private sector. We have tried to propose basic concepts to urbanise the development of ID-cards: people may accept the constraints of in-depth authentication only in relation to trusted Institutions. Due to people's desire to defend a strong sense of liberty, they prefer to separate different aspects of their lives.

We emphasize specifically the role of applications with the same level of risk and use. E-society could not propose today a unique card for all services: to protect privacy, to avoid denied access for people who lose the card, and not to attract the interest of criminals.

The all-in-one Card can only be developed by Institutions which have the same interests, which are not in competition, or which are their clients' only providers, Institutions which have their clients' trust, such as governmental institutions, schools, public transport companies, and, in many cases, banks. People may accept the constraints of in-depth authentication only in relation to these Institutions.

A pragmatic solution would be to develop at least two ID-cards, one for everyday life and one to replace the paper-based National Identity Card. The private sector needs to integrate the use of these ID-cards into its e-commerce strategy.

References

[AFNT04] Franco Arcieri, Fabio Fioravanti, Enrico Nardelli, Maurizio Talamo. Reliable peer-to-peer access for Italian citizens to digital government services on the Internet. 3rd International Conference on Electronic Government (EGOV-04) Zaragoza, Spain, Aug.2004. In *Lecture Notes in Computer Science*, vol.3183

[ACFN+04] Franco Arcieri, Mario Ciclosi, Fabio Fioravanti, Enrico Nardelli, Maurizio Talamo. The Italian Electronic Identity Card: a short introduction. 5th U.S. National Conference on Digital Government (DGO-04) Seattle, Wa., USA, May.04. http://www.diggov.org/library/library/dgo2004/

[ATIS01] Alliance for Telecommunications Industry Solutions. Telecom Glossary 2000. approved by American National Standards Institute, Inc. T1.523-2001, February 28, 2001.

[Bou04] D. Bounie and P. Gazé. Payment and Internet: Analysis, Stakes and Research Perspectives in Economics of Banking, May 2004.

[eEpoch01] eEpoch. e-ID and the Information Society in Europe. White Paper, september 2001.

[Eng02] S. Engel-Flechsig. Study on legal issues in relation to the use of public ID (Electronic Identity) Radicchio Ltd. UK, October 2002.

[Kar96] L. Karpik. Dispositifs de confiance et engagements crédibles. *Sociol. Trav.* num 4, 527-550, 1996.

[Kar98] L. Karpik. La confiance: réalité ou illusion? Examen critique d'une thèse de Williamson. *Rev. Eco.* vol. 49, num 4, 1043-1056, 1998.

[Kha03a] L. Khalil. Signature électronique: certificats qualifiés "publics" ou certificats qualifiés "privés". In *Communication et commerce électronique*, num 4, page 11, avril 2003.

[Kha03b] L. Khalil. Enjeux de l'acte authentique électronique. In *Colloque sur l'Acte authentique du 17-18 octobre 2003 - Université de La Rochelle*, Droit In Situ éd., 2003.

[Kha02] L. Khalil. *Signature électronique: le cadre juridique d'une autorité de certification bancaire.* Thèse, ANRT ed., 2002.

[Lor01] E. Lorentz. Inter-organizational trust, boundary spanners and communities of practice. In *Réseaux*, num 108, 65-85, FT R&D Hermès Science Publication, 2001.

[Lor82] E. Lorentz. Confiance, contrats et coopération économique. *Sociol. Trav.* num 4, 487-508, 1982.

[Men01] A. Mendez, N.Richez-Battesti. Pour une vision dynamique de la confiance: quelques réflexions à partir d'une banque mutualiste. In *Confiance et rationalité*, Dijon, 5-6 May 1999. In Les colloques, num 97, Ed INRA, Paris, 2001.

[Noo01] B. Nooteboom. How to combine calculative and non-calculative trust. In *Trust and Trouble in organizations*. Symposium , Erasmus University, Rotterdam, May, 2001.

[NERSC03] North East Regional Smartcard Consortium. *The North East A Community of Communitie*, 2003.

[San04] R. Sanchez-Reillo. *Pan-European interoperability solutions: Experiences from eEpoch Pilot Sites. 2004, e-ID Workshop on e-Go for reliable e-services: Electronic Identity from theory to practice*, 2004.

[Wil93] O.E. Williamson. Calculativeness, Trust and Economic Organization. *J. Law Econ.*, volume XXXVI, April, 453-487, 1993.