



Global Business Dialogue on Electronic Commerce

# Securing Electronic Transactions

## Recommendations

November 30, 2004

*Leading Chair (Europe/Africa)* Hermann-Josef Lamberti  
COO and Member of the Board  
Deutsche Bank AG

### INTRODUCTION

For e-commerce, as well as e-Government, it is important to be able to use electronic channels for legally binding transactions such as closing a deal or filing a petition. The recipient of electronic data must be able to prove that data is integer and authentic.

As long as integrity and authentication of data is not achieved, application owners have the choice to either:

- accept the potential risk that they might not be able to prove that the customer initiated a transaction (e.g. closed a deal or authorized a payment), or
- not allow transactions on the Internet and ask customers to use other channels (for example, a paper-based document).

As a consequence, the lack of authentication might become a limiting factor for e-commerce and e-Government. Hence, there is a need for an infrastructure of trust.

In 2003, the GBDe contacted payment service providers and content providers from various regions and business sectors and asked about challenges in e-payments. Among the answering parties, the implementation of a widely available infrastructure of

trust was top priority. Furthermore, examinations like those of Prof. Jeffrey Cole, which were presented at the 2003 GBDe Summit, show that consumers are sensitive to the problem of identity theft, even when they do not take a financial risk.

Today, there is still no widely accepted trust infrastructure in most countries. In this paper, we want to analyze the current situation, identify reasons for the current stalemate and discuss ways to overcome the problems.

## **Existing trust infrastructures**

### **Digital passports issued by government**

Some countries run a public key infrastructure (PKI) and have already started to issue digital passports that may be used for electronic signatures. These digital passports are smart-card based and can be used for e-Government as well as private purposes. For example:

- **Belgium:** The Belgian Government started to introduce digital passports in 2003 that are mandatory for all citizens. In order to have a stable workload at the local authorities, all citizens will obtain a digital passport by 2009. Each digital passport will be valid for 5 years.
- **Estonia:** Estonia is the only EU member state that has a digital passport that is mandatory for all citizens. As of January 2004, 368,000 cards, in total, were issued.
- **Finland:** Finland was the first EU member state to introduce a (not mandatory) digital passport. At the end of 2003, about 15,000 cards had been issued.
- **Brunei:** Brunei made a full roll-out of a digital passport to all its citizens. At the end of 2003, about 350,000 cards had been issued.
- **Malaysia:** Malaysia issued more than 4 million digital passports (as of April 2003).
- **Macao:** Macao issued about 15,000 cards (as of April 2003).
- **Hong Kong:** Hong Kong started issuing digital passports in July 2003.

- **Oman:** Oman started to roll-out digital passports in October 2003.
- **Taiwan:** The Taiwan government launched a smart-card based digital passport for all citizens in April 2003, which can be used for e-Government as well as private purposes. The digital passport is not mandatory, but free of charge until the end of 2004 (500,000 passports have been issued as of September 2004).

There are pilot projects or feasibility studies in many countries, for example:

- Local authorities in France, Ireland, Italy, Spain, UK and Israel participate in the pilot project eEpoch<sup>1</sup> for local e-government. As a first step, they want to reach a proof of concept and run interoperability tests.
- Austria, Belgium, Bahrain, Japan, Saudi Arabia, Switzerland, Thailand and United Arab Emirates have completed pilot projects or feasibility studies.
- The German government started the private-public-partnership initiative “German Signature Alliance” in 2003. Details are described below.

## **Existing systems in the banking sector**

Many banks run systems that allow their customers to check their accounts, transfer money or do online-brokerage. Below are some infrastructures used in order to secure these transactions:

- **Password-based systems:** The customer and bank agree on some password that allows login to the bank’s server. In order to close a transaction, sometimes one-time passwords are used. The PIN/TAN-system works that way: The personal identification number (PIN) is used for login, a list of transaction numbers (TAN) serve as one-time passwords.
- **Token-based systems:** A security token generates passwords (transaction numbers) on demand. These passwords are valid for a short time (only minutes) and are used in order to authenticate transactions.

---

<sup>1</sup> eEpoch is a demonstration project funded by the European Communities conceived as proof of concept of the eEurope Smart Card Charter.

- **Signature Cards:** Some banks have already issued signature cards that can be used for login and financial transactions. However, the number of signature cards is still small.

## **Existing private sector initiatives – an example of a bridge-CA**

In order to connect existing company PKIs and make them useable for secure e-mail transfer, bridge-CA initiatives like the European Bridge-CA (EB-CA) were founded. The heart of a bridge-CA is a collection of root-certificates of the participants that commit to a set of basic rules. In particular, these rules ensure technical e-mail interoperability. Employee's certificates can be checked using the associated root-certificates stored in the bridge.

A bridge-CA is a non-hierarchical approach that allows secure communication without expensive exchange of certificates.

### **Applications**

Following are PKI-usage examples from different regions of the world.

#### **Example form Asia: Japan**

There are four different certification infrastructures in Japan: The Government PKI (GPKI) used for online applications between citizens and the government; the Local Government PKI (LGPKI) used for the interaction among local governments, the Public Certification Service for Individuals, JPki, to issue electronic certificates for residents, and the Certificate Service Providers (CSPs) built for corporate entities. The cross-certification between LGPKI, JPki, CSPs and GPKI enables to make online applications for the government.

Enterprises, trying to make online applications to the government, may be registered by private CSPs (as of November 2004 there were 20 such CSPs in Japan). These CSPs have to run through an accreditation process, which means that they have to pass a test (including an investigation)

The Public Certification Service for Individuals, JPKI, started on January 2004, and electronic certificates have been issued for residents by Prefectural Governors at the offices of municipalities. Electronic certificates are valid for three years with issuance commissions of five hundred yen. With electronic certificates, residents can make electronic applications such as tax declarations, pension matters, passport, transfer via the Internet from anywhere and anytime.

#### **Example from Asia: Taiwan**

In Taiwan, a government PKI was established in 1995. Certificates are issued for enterprises, organizations and individuals. The infrastructure is in particular used for the official inter-government document exchange (G2G), e-procurement service (G2B) and e-tax service (G2C), making use of the PKI infrastructure.

Today, the PKI is rarely used in e-commerce. However, it is likely that the government PKI will influence e-commerce in the long run.

The Government Root Certification Authority (GRCA) is the highest certification authority in the hierarchical structure of government PKI. The GRCA also acts as the interface between CAs within and without the government PKI. Under GRCA, the certificates issued by “Government CA” are used for all government agencies, the certificates issued by “Ministry of the Interior CA” are used for all citizens, and the certificates issued by “Ministry of Economic Affairs CA” are used for business groups. In order to encourage government departments and private companies to develop PKI applications, the “Government Test CA” provides testing certificates as well as developing kits.

#### **Example from Latin America: Brazil**

In Brazil, a public key infrastructure called ICP-Brasil was implemented by the Federal Government. The infrastructure is mainly used for public services (e.g. in the Department of Justice). Today, there are token-, Smartcard- and computer-based solutions in place. There are trials on the local level to integrate all public related services (e.g. health care, social insurance issues, IDs and driver’s license) in a Smartcard-based infrastructure. The most

popular application is the ReceitaNet-system, which allows all citizens to process their personal tax declaration electronically. Currently, this system is used by more than 90% of Brazilian taxpayers.

In business, trust infrastructures are used in the financial sector. More than 90% of Brazilian Internet banking services are based on a PKI. Some banks issue smartcards in order to secure financial transactions.

### **Example from Europe: Belgium**

In Belgium, a national PKI called CERTICOM was introduced in 2003. It is based on the national electronic ID card that can be used for authentication and (qualified) electronic signature. Starting with specific user groups like notaries, all citizens will obtain their (mandatory) electronic ID until the end of 2008.

The infrastructure is run by the Government and is used in both e-Government and private sector applications. Status information on certificates is provided free of charge.

## **The legal framework**

### **Europe**

Following the European Electronic Signature Directive, most EU member states have regulations in place that define electronic signatures and clarify the obligations of the CSP.

The signature directive defines qualified signatures. Such signatures are mostly smartcard-based and require a secure identification of the card-holder by the CSP. These qualified signatures are an electronic equivalent to hand-written signatures.

Electronic signature laws slightly differ in each of the EU member states, particularly for the underlying identification processes that are required for CSPs that issue qualified certificates. Each member state has its own supervisory system. Furthermore, some member states allow (qualified) company signatures, others do not. The EU directive ensures that certificates, which are qualified in one member state, are qualified in all.

The EU directive also mentions non-qualified signatures like advanced signatures (based on a PKI, but they might be software certificates). Such signatures might be used in a legal claim in order to brought forward evidence. The usage of advanced signatures is sufficient for most business purposes. However, only qualified signatures come along with a formal shift in the burden of proof.

### **Japan**

In Japan, “Legislation on electronic signatures and certification system” is in place. If, by construction of the PKI, no one but the principal is able to sign, then an electronic signature is equivalent to the principal’s seal or the hand written signature. Certificates originally issued to enterprises for G2B purposes might also be used in private communication (i.e. B2B or B2C). The certification is provided through 20 CSPs, which are accredited by the Government.

Furthermore, the Japanese Government (Ministry of Justice) has adjusted the business register law in order to allow special electronic seals. The corresponding certificates (business entity name and name of representatives) are issued by a designated specific registry, which operates under government responsibility.

Prefectural Governors have issued electronic certificates for the Public Certification Service for Individuals, JPKI, based on Law concerning Digital Signature Certification of Local Public Entity

### **The current situation**

Today, in most countries, there exists no widely available trust infrastructure which allows authentic transactions over electronic channels. One reason is that such an infrastructure comes with a high initiation effort:

- All participants have to be registered.
- Certificates, and often hardware-tokens, have to be distributed.
- Private PCs have to be fitted with appropriate software readers for additional hardware (e.g. smartcard reader).

- The certificate service providers (CSP) have to run servers that guarantee (real-time) validation of certificates.
- Application providers must integrate the trust infrastructure into their processes.

Significant shares of the total running costs are fixed costs. Hence, the costs per user depend crucially on their total number. In the same way, the benefit for customers and application owners is related to the number of participants: For customers, the number of applications is crucial, for application providers it is important to have a large number of customers that are able to use the system.

If there is a large number of customers and applications, then the total benefit for the participants will exceed the total costs, and one may get a positive business case for the infrastructure.

If, however, the number of customers and applications is too small, then the total benefit will be below the total costs, and a positive business case cannot be achieved. Critical mass problems are typical for infrastructures in which the benefit depends on the number of participants. In case of trust infrastructures, we have to reach critical masses for both customers and applications. This situation is sometimes called the chicken and the egg problem.

So far, most infrastructures cannot reach the critical mass. Most success-stories known are infrastructures for closed user groups like enterprise implementations, for which the CSP is the application provider at the same time.

### **Barriers that prohibit building infrastructures of trust**

The costs of building and running the trust infrastructure play a crucial role: The higher these costs are, the more participants are needed in order to reach the break-even point. This means that any measure that increases the costs of the infrastructure is an economical barrier and decreases the likelihood that the critical mass can be reached.

Such barriers can be regulations that:

- do not allow the usage of standard software with the consequence that customers or application owners have to implement new software, or
- define processes that differ from existing, well-established ones.

Furthermore, if the infrastructure may only be used for a certain purpose or by special user groups, then this will limit the benefit for all participants. For example, non-harmonized regulations or a lack of technical interoperability might prohibit cross-border transactions and create such a limitation.

## **A pragmatic approach**

### **Technical issues**

In order to minimize the initiation effort for all parties, an infrastructure of trust should be based on well established technical standards. In particular, it must be possible to use standard software.

### **Business case**

There must be a clear business case for all stakeholders, private customers, application owners and infrastructure providers (CSPs).

Private customers usually have to pay for the convenience of taking part in the infrastructure. However, application owners usually have the largest benefit. Hence, it is more likely that customers will participate in the infrastructure if they do not have to pay the total cost. There are business models in which application owners pay some fee to the CSP or provide incentives for customers. Such approaches look promising.

If application owners have to pay for usage of the infrastructure, the fee must be smaller than the estimated benefit to the application owner.

Models, in which fixed costs of running the infrastructure are allocated to a small group of early users, come with high fees for

customers and application owners. It is unlikely that such models will be successful. It is a general observation that a large number of transactions are needed to reach the break-even.

### **Legal issues**

National laws should set a legal framework for trust infrastructures, in general and electronic signatures, in particular, that:

- guarantee legal certainty – since this is the fundamental benefit for all infrastructure users,
- allow usage of international technological standards – otherwise solutions become proprietary and non-interoperable,
- do not hinder usage of existing infrastructures – minimizing the initiation effort,
- allow realization of a viable business case for all stakeholders.

### **Role of Governments**

There are different actions governments can take in order to foster the development of trust infrastructures:

- Governments may run their own trust infrastructure, which can be combined with a digital passport. In this case, governments should use open standards and allow private sector to make use of the infrastructure.
- Governments may encourage private sector to build up privately owned trust infrastructures, and link these infrastructures up with their e-Government projects. In this case, e-Government projects may be important in order to achieve the critical mass of users.

### **Examples of initiatives**

#### **German Signature Alliance**

In spring 2003, the German Signature Alliance was founded as a private-public-partnership between Federal German Government and private sector representatives. After the first year of its existence, the alliance has more than 30 members, including all major German banks and technology partners.

The alliance brings together private and public sector parties in order to promote the use of electronic signatures and establish a

standard for interoperable applications. The members also want to define basic economic rules that allow a return on investment for the infrastructure provider. Furthermore, the participants agreed to adjust regulations so that well established business processes, like existing processes in the financial service industry (for bank cards), may be used to issue signature cards. In April 2004 Germany's Federal Government initiated a revision of the German Signature Law.

e-Government applications should be launched on a large scale in order to generate demand for usage of the new infrastructure. The German Government plans to replace a paper based social security ID and related annual notifications with an electronic system where the information is stored in a large database. In this case, a personal signature card issued by any private company might serve as a key to this information (and make the social security ID obsolete). Such an application has the potential to generate demand for signature cards, which would help to reach the critical mass.

## **Recommendations**

It is a fundamental decision whether governments issue digital passports and run a trust infrastructure for their citizens or whether such infrastructure operates under private responsibility. The GBDe does not favor one alternative over the other. A chosen alternative may be related to the legal situation and the cultural background in each country.

We note that it is unlikely that both systems can co-exist in one country. In particular, when governments issue mandatory digital passports, there would be no need for privately issued citizen-IDs. Therefore, it is important that governments make a clear statement which path the country will follow. Otherwise, one may end up in a stalemate, in which companies only create small-scale infrastructures for their employees or customers.

Depending on the decision, there are different implications to all stakeholders – leading to different recommendations.

## **1. Governments or publicly owned institutions run the infrastructure.**

In this case the GBDe recommends that:

- The infrastructure should use international industry standards. Furthermore, it should be possible to use standard software in order to process digitally signed documents. Proprietary technical solutions should be avoided.
- If the infrastructure is based on smartcards, then these cards should only be used for identification (like a passport) and PKI issues. All further data should be stored in the application rather than on the smartcard.
- The regulatory framework should provide legal certainty for all users of the trust infrastructure. If electronic signatures are used, they should serve as a pendant to handwritten signatures.
- Experience shows that it can be hard to sell digital IDs to citizens. If the cards are not mandatory, they must be low priced and provide a significant benefit for each citizen.
- Private sector companies should be allowed to use the infrastructure, i.e. accept digitally signed documents and integrate them in their workflow.
- Private companies should make use of the infrastructure in their applications.
- Governments should implement attractive e-Government applications based on the infrastructure.
- Existing private sector knowledge should be included when the infrastructure is built up. Governments may also make use of private companies for maintenance.

## **2. Governments or publicly owned institutions will not run the infrastructure.**

In this case the GBDe recommends that:

- Governments should clearly communicate the decision and encourage private companies to build-up an infrastructure of trust.

- The number of private infrastructures should not be limited. Therefore, the infrastructures should be based upon the principle of interoperability.
- In order to lower initiation effort, it should be possible to build up infrastructures of trust based on existing infrastructures (e.g. smartcards issued by banks or telcos). Regulations should ensure that digital signatures based upon such infrastructures may be used for all purpose – without a need for significant changes in the existing processes.
- A viable business case is crucial for a privately run infrastructure. If e-Government applications make use of a private infrastructure and thereby save costs, then governments should be willing to pay for the usage. It is unlikely that a private infrastructure will be successful if the citizens pay all the costs and application owners receive most of the benefits. In particular, national law should not prohibit such business cases.
- Cooperation in the private sector is more likely to reach the critical mass of users and applications. Therefore, the GBDe encourages companies to work together in order to build up and run infrastructures of trust.