eID cards: Improving trust and reducing the cost of e-government transactions

Eliminating Costly, Time-Consuming, and Fraud-Prone Paper Processes
As governments around the world move from paper to online transactions with eID cards, they recognize numerous benefits, such as:

- Saving institutions and citizens time and money by reducing:
  - –Branch and office visits
  - –Printing
  - –Mailing
  - –Data entry
  - –Storage
- Increasing privacy and transaction security because eID cards:
  - –Are uniquely programmed
  - –Bind an electronic transaction to a card and PIN
  - –Are difficult to fraudulently modify or duplicate
  - –Utilize sophisticated encryption technology
  - –PersistentlyAuthenticate each transaction
- Enabling governments to conduct more secure transactions because eID cards:
  - –Identify all participants in round-trip transactions
  - –Reduce potential fraud in benefit payments

Governments around the world are embracing electronic ID (eID) cards—smart card-based identification credentials that support digital signature technology. Electronic ID cards can address many of the challenges faced by citizens, governments, and businesses today, such as expensive and time-consuming paper processes, privacy protection, and identity fraud. By supporting digital signature technology, eID solutions provide a fast, inexpensive, and secure approach to online transactions.

What is a smart card?

A smart card is a credit-card form factor device that securely stores a digital ID/certificate within a specially designed microprocessor on the card. There are two kinds of smart cards: contact smart cards, which must be inserted into a card reader when used and contactless smart cards, which use wireless communication and can be read from a short distance. Contact smart cards generally provide greater security than contactless smart cards because they must be physically inserted into a card reader and PIN-based authentication must be provided for access, authentication, and digital signing. Smart cards can also include the traditional features of physical ID cards such as images, pertinent personal data, and even magnetic stripes and barcodes.

Taking it a step further with digital signatures

Conducting business using paper processes and traditional ID cards is no longer realistic. Not only are paper processes expensive and time-consuming, but handwritten signatures on paper are easily reproduced and forged.

Digital signatures, on the other hand, are much more difficult to imitate or forge because the technology authenticates the identity of the sender or signer of an electronic document. Digital signatures also add assurances that the content of an electronically delivered message or document hasn't been altered since its creation.

Digital signature technology works by binding a cardholder's identity (digital ID) to a particular document. This cannot be transferred to subsequent transactions because the card uniquely signs each transaction instance. This capability restricts signatures from being reused on other documents. And, with eID and digital signature solutions, it is much more difficult to complete a fraudulent transaction without the cardholder's knowledge because both the physical card and the card's protective PIN (personal identification number) are required for each transaction.

System design best practices

- Store all personal information in encrypted form in the ID card and in all databases.
- Transmit only encrypted information.
- Enable cardholders to authorize card content extraction with a password, PIN, and/or biometric verification for all transactions.
- Construct applications so that transaction records cannot be used as surveillance tools.

As represented by the above best practices, the onus of privacy protection is on the institution. When implementing eID solutions, governments and organizations must define practices like those above and then educate citizens and customers to help them understand why eIDs are beneficial to them and how governments will work to safeguard their privacy.

eID solutions are catching on

Around the globe, smart card-based government IDs are taking off. The following is a sampling of projects as reported in *Card Technology* magazine in October 2006:

- Belgium: 4.5million cards; 8million are projected
- China: 102million cards issued; 800million projected
- Germany: 80,million projected
- Italy: 2million cards issued; 40million projected
- Japan: 1million cards issued
- South Africa: 30million issued
- Spain: 35million issued
- UK: 50million projected

Leading the way in the U.S.

The United States Department of Defense has been one of the early adopters of eID cards and has had much success with its Common Access Card (CAC). The CAC is a smart card issued as standard identification for active duty military personnel, reserve personnel, civilian employees, and eligible contractor personnel.

An accessible solution today

The client-side technology required to support eID solutions is currently available, and the software required for application support is already widespread: Adobe® Reader® software, popular web browsers, e-mail programs, and most operating systems now natively support smart card technology and thus eID cards. In terms of hardware, smart card readers are available as add-on USB and PCMCIA devices, and computer manufacturers are building them directly into new laptops and desktop PC keyboards. This means that eID solutions are becoming highly accessible for government, business, and consumer processes.

What about privacy?

Violation of privacy has been raised as one objection to eID solutions, especially when it comes to government ID cards. In reality, it's not eID technology that has the potential to compromise privacy, but the processes employed by the governments and organizations that issue and conduct business transactions with eIDs. With this in mind, governments and organizations need to adopt robust privacy protection policies for the issuance of eID cards, and enforce rigid privacy protection practices for all the systems and processes surrounding eID transactions.

In fact, when it comes to privacy, smart cards stand apart. Smart cards are built with significant inherent security protection, so users can be confident their personal information is safe. Moreover, private data can be sectioned off from public data so that unauthorized requestors cannot access it. Cardholders may also be required to authenticate to the card to permit export of this data. Adopting and enforcing best practices for privacy protection and then educating users about the benefits of eID cards and the measures being taken to protect cardholders' privacy are the key actions governments can take to promote these technologies.

A cost-effective solution

Electronic ID cards deliver a solid return on investment by enabling governments and businesses to cut the costs associated with traditional transactions. While the costs of eID implementation and rollout may be significant, the cost-savings and efficiency benefits are greater.

The client-side user technology required to support eID cards is largely in place, and card provisioning and enablement processes have been streamlined, making it easier and more cost effective for governments to implement solutions. In addition, digital ID vendors are offering a wide variety of deployment models to make it more feasible for organization to embrace eID cards.

In March 2005, for example, Germany defined a federal eCard strategy requiring all smart-card-based projects to support digital signatures. With over 80 million citizen smart cards expected to be in use by 2008, Germany and the institutions participating in the program are expecting to realize significant cost-cutting and efficiency benefits. A large pharma company has also reported savings of up to $100 per signature vs. managing signed paper documents.

Comparing security

When it comes to card soutions, one of the clear advantages of smart cards is the security they offer to data stored. Some institutions have considered placing barcodes on ID cards as a means to maintain unique IDs and prevent fraud. Barcodes, however, can be scanned without the individual's knowledge and therefore have the potential to violate an individual's privacy. In addition, barcodes cannot be used to create digital signatures, introducing opportunities for fraud and security breaches. Unlike data printed on a card or stored in a barcode on the back of the card, a smart card provides the capability to store public data in an open format and private data in an encrypted format, based on the needs of the government.

In summary

Smart cards and digital signature technology, combined to create eID cards, enable governments to more easily communicate and transact with citizens.

With eID solutions:

- Participants receive a high level of protection over how their electronic identities can be used and therefore a high level of privacy protection.
- The security of online transactions is increased because smart card and digital signature technologies provide more assurances of the participant's identities.
- Governments can streamline processes and cut costs associated with existing manual practices utilized in numerous government applications, such as those used for social services, taxes, health, retiree benefits, and driver's licensing.

Today, eID solutions, combined with robust application support for digital signatures provide a compelling foundation for continuous process improvement and cost savings. Forward-looking countries and government institutions that decide to capitalize on these new technologies will reap the benefits.

Adobe®

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

Adobe, the Adobe logo, Acrobat, and Better by Adobe are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2007 Adobe Systems Incorporated. All rights reserved. Printed in the USA.

05/07