ITIF

The Information Technology
& Innovation Foundation

Electronic Identification

Daniel Castro ▮ September 2011

Explaining International Leadership: Electronic Identification Systems

BY DANIEL CASTRO

SEPTEMBER 2011

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Identification is routinely used to help facilitate commercial and government transactions, such as taking out a loan or applying for government benefits. While individuals can use traditional forms of identification in face-to-face transactions, these forms of identification are less useful for conducting business on the Internet. To address this challenge, many governments are creating national electronic identification (e-ID) systems—a collection of technologies and policies that enable individuals to electronically prove their identity or an attribute about their identity to an information system. This report reviews the programs and practices of some of the countries with the most advanced and widely deployed national e-ID systems. It highlights the successes and failures of different approaches and focuses on the lessons that policymakers, particularly in the United States, can learn from nations that have begun adopting and using e-ID systems.

National e-ID systems offer a variety of benefits for individuals, businesses and governments. These systems can help reduce identity theft and enable individuals to use online applications more securely in a variety of industries such as health care and banking. Individuals can use an e-ID to authenticate to online services, securely communicate online, purchase goods and services, and create legally-binding electronic signatures, such as to sign a contract. Businesses can use identity management functions to better interact with their customers on the Internet, such as to authenticate users to online applications or to verify the ages of their customers. Finally, government can use e-IDs to streamline e-government services, allow individuals to sign and submit forms online, and offer innovative services.

Many European countries have been investing in national e-ID systems, as have countries in the Middle East and Asia. While no country has achieved universal deployment and use of a national e-ID system, some countries have made more progress than others. At present the clear leader is Estonia, which has issued approximately 1.2 million e-ID smartcards to an eligible population of 1.3 million citizens (i.e. individuals age fifteen and older). Since inception, cardholders in Estonia have used their e-ID to create more than 52 million electronic signatures and authenticate more than 88 million electronic transactions. Estonia has even used its e-ID system to allow citizens to vote online.

In contrast, as of 2011, the United States does not have a national e-ID system. Most individuals still use a collection of poorly secured usernames and passwords to access online

services and, more than a decade after Congress passed the Electronic Signatures in Global and National Commerce Act (ESIGN), most individuals never use secure electronic signatures to sign documents. However, the federal government recently launched the National Strategy for Trusted Identities in Cyberspace (NSTIC), a new initiative to develop an online identity ecosystem. Policymakers have many opportunities to learn from the countries furthest along in deploying e-ID systems as they shape the technology, institutions and policies that will guide e-ID development in the United States.

Countries have many options for building an e-ID system, and each country can design a system to address its unique needs. While demographic, cultural and historical factors may influence a country's national e-ID strategy, and existing ID infrastructure such as national registries may make deployment easier, all countries appear able to take advantage of this technology. Although the United States is late in creating a national e-ID strategy, if it heeds the lessons from early adopters it can capitalize on an enormous opportunity to create an e-ID system that can leapfrog those of other countries and help invigorate our information economy.

Therefore, to promote e-ID adoption and use in the United States, policymakers should do the following:

- *Create an e-ID implementation plan with broad input from all stakeholders, including the private sector.* The government cannot build a successful national e-ID system without support from all stakeholders. The countries with the most widespread use generally have both public and private-sector applications utilizing the e-ID system and virtually every country uses the private sector to operate a portion of the e-ID infrastructure. Moreover, the private sector has many resources that can be built on and is the current supplier of much of the identity infrastructure, such as certificate authorities, that will be used.

- *Build an e-ID framework that supports both current and emerging technologies.* The government should not specify any particular technology for e-IDs but rather establish a technology-neutral e-ID framework that allows both public and private-sector identity providers to issue e-IDs using the technology of their choice. Countries such as Austria that have not created a single national token, such as a smartcard, but rather have established a flexible framework for e-IDs, offer citizens more options for obtaining an e-ID.

- *Use government to increase both supply and demand for e-IDs.* Technologies like e-ID systems exhibit strong network effects whereby the value of the technology grows as the number of users increases. A critical mass is needed to create the right value proposition for private-sector service providers to rely on the technology; without that critical mass, systems that accept e-IDs will not develop. Government, at the federal, state and local level, should invest in the identity ecosystem to overcome this "chicken-or-egg" problem inherent in its creation. The countries that are further ahead in e-ID adoption and use have aggressively invested in e-ID technology in advance of market demand for the technology; the most successful countries have also coupled these investments with demand-side programs to spur

use of the technology.

- *Design an e-ID solution that maximizes utility for both users and service providers.* One of the reasons that e-ID solutions have had slow adoption in many countries is that many of the security benefits of using e-IDs, compared to using one-off solutions, have been one-sided: service providers use e-IDs to verify the identity of users, but users do not have the opportunity to verify the identity of the service providers. The United States should follow the lead of Germany, one of the few countries to implement an e-ID system that uses mutual authentication. Using mutual authentication confers the security benefits of e-IDs to both service providers and users, thereby giving users more incentive to adopt e-IDs.

- *Ensure that privacy does not come at the expense of eliminating useful information from the information economy.* Although privacy is often cited as a concern for the development of national ID systems, an e-ID system can enhance user privacy by reducing the amount of information revealed during a transaction. For example, individuals can prove that they are over the age of twenty-one without revealing their exact date of birth or name. While this is a potential benefit for individuals, there is a risk that data sets that might otherwise be generated and that are useful for society will no longer be created. The solution to such a risk is to ensure that policymakers understand the value of data sets and take into account the need to enable beneficial types of data sharing when legislating or rulemaking. Given the importance of information to the information economy, the government agency leading the development of the e-ID system should ensure that enabling beneficial forms of data sharing is one of the metrics by which potential solutions are evaluated.

- *Strive for disruptive innovation, not just incremental innovation.* Technological progress is often evolutionary rather than revolutionary. This is often the case in government where technology is used only to make existing processes more efficient, rather than to find new ways to redesign or reengineer processes to take advantage of new technology. Implementing an e-ID system gives government the opportunity not only to implement incremental innovation, but also to use the technology for disruptive innovation. Some steps are straightforward. For example, government agencies can be better integrated by allowing single-sign-on and reducing the number of login prompts as users navigate from one agency to another. Government can also find opportunities for more radical change in how it delivers services to citizens. For example, the government can follow Belgium's lead and use e-IDs to implement an "ask once" policy, eliminating the need for users to provide information to government more than once.

- *Ensure that e-ID solutions are accessible and available to all individuals.* As e-IDs become more common, they will likely become a prerequisite to participation in certain aspects of digital society and commerce. Thus it will be necessary to ensure that a digital divide does not emerge whereby certain populations are unable to participate because the technology is either not accessible or not available for their use. The development of the e-ID should therefore specifically take into account the needs of different groups, including non-U.S. citizens, low-income populations, and people with disabilities. Providing all individuals access to an e-

ID will help ensure that organizations can phase out legacy systems for electronic authentication and signatures, and will not need to run additional programs for those unable to obtain an e-ID.

- *Design an e-ID system for the global digital economy.* Systems designed for today's digital economy should reflect its global nature. Ideally, an e-ID issued in one country should be accepted in another. Unfortunately, every nation with an e-ID system today faces significant challenges to making its system interoperable outside of its borders. To this end, the U.S. should more actively lead the development of international standards for federated identity-management systems. In addition, it should work to develop an interoperability framework that would allow e-IDs created in one nation to be accepted in another for online authentication and electronic signing. Properly managed, the growth of e-ID technology should help reduce barriers to the free flow of information by allowing secure transactions between individuals and organizations across national borders.

A national e-ID system will provide a platform for the public and private sectors to develop a wide array of innovative and productivity-enhancing products and services online that require one's identity, or an aspect of one's identity to be confirmed. Policymakers should embrace the opportunity to create an innovation-driven approach to a national e-ID system that balances competing interests, improves privacy and security for users, and combines the strengths of both the public and private sector.

INTRODUCTION

As a famous cartoon in *The New Yorker* once noted, "On the Internet, nobody knows you are a dog." The ability to hide one's identity on the Internet has certain advantages; however, the inability to positively prove one's identity to others online poses an obstacle to the development of many applications. While individuals increasingly use the Internet to perform tasks that once required them to interact with someone in person, they often cannot complete transactions online that require showing identification, such as applying for government benefits or refinancing a mortgage. The lack of a trusted, interoperable and easy-to-use form of electronic identification poses a serious obstacle to completing these types of transactions securely and efficiently. Creating a widely-accepted form of electronic identification will not only enable individuals to use online applications more securely, it will also allow the public and private sectors to offer a wide array of innovative and productivity-enhancing products and services online that require one's identity, or an aspect of one's identity to be confirmed.

Although the United States is late in creating a national e-ID strategy, if it heeds the lessons from early adopters it can capitalize on an enormous opportunity to create an e-ID system that can leapfrog those of other countries and help invigorate our information economy.

Many governments are tackling this challenge, some with more success than others. Others have not yet taken action and do not currently have a plan in place to solve this problem. This report reviews the programs and practices of some of the countries with the most advanced and widely deployed national electronic identification systems. It highlights the successes and failures of different approaches and focuses on the lessons that policymakers, particularly in the United States, can learn from nations that have begun adopting and using electronic identification systems.

Background

Most identity systems have arisen out of necessity. Historically, in small enough communities, individuals did not require proof of identity as they were either recognized by others or could find someone who could vouch for their identity. However, as communities became large and mobile this was no longer possible. Instead, a trusted third party provided individuals proof of identity. Governments and religious authorities typically fulfilled this role. Today, government is the primary provider of identification documents such as passports or birth certificates in the offline environment.

Identification documents provide two basic services: verification of a person's identity (e.g., "This is Joe Smith") and verification of an attribute (e.g., "This person is a U.S. citizen").

Government is often both an identity provider and an attribute provider. For example, a U.S. driver's license serves both as proof of identity for commercial and government transactions and as a credential to show that an individual is approved to operate a motorized vehicle. The private sector may also be an identity provider or an attribute provider. For example, a company may issue photo IDs to all of its employees asserting both the individuals' identities and permission for those individuals to enter the employer's place of business. Similarly, many businesses offer membership cards or loyalty cards to their customers. While these cards may show an individual's identity, they typically are not legally accepted forms of identification. Furthermore, not all attribute providers are identity providers. A university, for example, may issue a diploma conferring a degree on an individual, but a diploma is not proof of identity.

Government uses various controls to ensure the integrity of identification documents, both to prevent individuals from obtaining documents under false pretenses and to prevent forgeries. First, the government employs countermeasures in the identity proofing process to prevent individuals from obtaining identification containing false information. For example, a government agency may require that minors applying for an ID card bring a parent or guardian who can attest to their identity. Second, the government can employ various mechanisms to ensure the security of an actual identity document. For example, a passport may contain a watermark or other physical property to make forgeries more difficult.

Recently, many governments have begun investing in digital technology to improve the security of these credentials. For example, instead of issuing a paper ID card, a government may issue a smartcard with certain cryptographic properties that decrease the likelihood of forgeries. In addition, some governments are making identity documents machine-readable to gain administrative efficiency, such as faster processing times at border crossings. China, for example, has launched an ambitious plan to create a machine-readable national ID, and India is creating a unique ID number for every citizen linked to biometric information such as fingerprints and iris scans. Mexico plans to issue a national ID smartcard to all of its citizens by 2012. The card will contain biometric data including a photograph, signature, fingerprints and iris scans. The Mexican government expects that the ID will help increase transparency in government aid programs and combat organized crime by reducing the ability of drug traffickers to use fraudulent identification.[1] Since 2007, the U.S. government has issued electronic passports (e-passports) with an embedded computer chip containing the personal information displayed on the data page of the passport, a digital photograph, and a digital signature. The digital signature provides assurance that data on the e-passport has not been altered or forged.[2] Although these types of documents are sometimes referred to as electronic IDs, these types of ID systems are not the subject of this report.

In this report, an electronic identification (e-ID) system refers to a system of technologies and policies that enable individuals to electronically prove their identity or an attribute about their identity to an information system. Paper-based forms of identification, such as national identity cards, help facilitate transactions among citizens, businesses and government. While these forms of identification are effective in the physical world, proving

identity remotely on the Internet is more difficult than in face-to-face transactions. For this reason, many countries have begun to introduce e-IDs for their citizens to use with third parties, such as government agencies or businesses. With close to two billion Internet users worldwide, the ability to easily establish one's identity and credentials online will be increasingly necessary to conduct secure transactions on the Internet.[3]

BOX 1: ELECTRONIC PASSPORTS

While passports are a form of national identification, the use of passports for purposes other than border control is somewhat limited. However, electronic passports (e-passports) are quickly becoming one of the most common forms of electronic identification. In recent years, many countries have introduced e-passports with biometric information to prevent unauthorized entry and to facilitate legitimate trade and travel. An e-passport typically contains a radio frequency identification (RFID) chip, which stores not only the standard passport data but additional digital biometric information such as a photograph, iris pattern, or fingerprint. E-passports help governments better authenticate passport holders and reduce the risk of document tampering. The information stored electronically in the e-passport is digitally signed and encrypted to prevent counterfeiting and manipulation. The widespread implementation of e-passports is the result of the United Nation's International Civil Aviation Organization (ICAO) Document 9303, which specified an international standard for machine-readable travel documents.[4] However, while most countries use a standard biometric file format defined by ICAO, the exact implementation of e-passports varies by country. The only biometric data stored on U.K. e-passports, for example, is a photograph.[5] German e-passports, in addition to including photographs and personal information, contain two fingerprints.[6]

Using biometric-enhanced passports, government officials can more quickly and accurately process travelers through customs and immigrations. The Australian government has established SmartGate kiosks at its international airports to allow travelers with Australian or New Zealand e-passports to self-process through the passport control area.[7] The SmartGate system uses data in the e-passport and facial recognition technology to perform the customs and immigration checks that are usually conducted by a Customs Officer. SmartGate will be gradually opened to other nationalities that have ICAO-compliant e-passports.

Terminology and Technology

A brief overview of the terminology and the technology used in e-ID systems will help some readers better understand the ideas put forth in this report.

Electronic Signatures, Digital Signatures and Digital Certificates

The term "electronic signature" is often used imprecisely. For the purpose of this report, an electronic signature refers to a signature that is processed, stored or transmitted electronically. This includes, but is not limited to, electronically transmitted documents bearing handwritten signatures, such as a PDF document with a handwritten signature, and digital documents that have been encoded with an electronic signature. This report

will focus primarily on more advanced uses of electronic signatures that involve the use of digital signatures to securely sign an electronic document.

Digital signatures are an important subset of electronic signatures. Digital signatures use a technique known as asymmetric cryptography requiring two components: a private key for the sender to use to sign a document and a public key for the receiver to use to verify the signature. The keys are generated by a certificate authority, a trusted third party such as a private company or the government. Certificate authorities issue digital certificates that contain these public keys, along with information about owners and the cryptographic protocols used. The certificate is signed by the issuing certificate authority and is valid only for a specified date range. The public key of a certificate authority is typically distributed in software packages, such as web browsers. A public key infrastructure (PKI) defines the set of certificate authorities for digital signatures and the trust relationships between the various certificate authorities.

Digital signatures can provide three critical cryptographic functions. First, digital signatures can be used for authentication. The receiver of a message that has been digitally signed can verify the signature to authenticate the identity of the signer of a message. Second, digital signatures can provide integrity. Using a digital signature, the receiver of a message can verify not only the source of the signature, but also that the message has not been modified. Third, digital signatures can be used to provide non-repudiation—the property of being able to prove to a third party that the signature was provided by the signatory. Digital signatures occur frequently in electronic transactions, not only between individuals, but also to securely pass information between electronic devices or applications.

Identification, Authentication and Signing

Identification, authentication and signing technologies are some of the fundamental building blocks of online services. Each of these terms represents a different function, as explained below.

Identification refers to the process of answering the question "Who is there?" Identification can occur through self-identification or third-party identification. An example of self-identification is when a user enters a username on a website. An example of third-party identification is when a website recognizes a returning user by, for example, a cookie or small file with data set in the user's browser.

Authentication refers to the process of answering the question "Is that person who he says he is?" Authentication occurs by verifying the credentials offered by an individual. For example, this might mean checking a user's password or verifying the validity of a digital certificate. In the offline world, an example of this would be a bartender verifying that a driver's license photo matches the physical appearance of the individual presenting the license, that the license is valid, and that the individual is of legal drinking age.

Signing refers to process of attributing an identity to a specific transaction. An example of this would be a user appending his or her name to the end of an email agreeing to a transaction with another user. An example from the offline world is when an individual signs a receipt to confirm delivery of a package.

Benefits of e-ID Systems

Electronic ID systems generate a variety of benefits for individuals, businesses, and government, including facilitating commerce in the digital economy, enabling e-government services, and improving security for online transactions.

Many types of e-commerce transactions become more efficient with an e-ID system. These systems enable individuals to authenticate to online services, securely communicate online, and create legally-binding electronic signatures, such as to sign a contract or enroll in a service. Businesses can use identity management functions to interact with their customers, such as to authenticate users to online applications. Citizens benefit from electronic ID systems that enable single-sign on (SSO). SSO gives individuals a more seamless online experience by allowing them to use one credential to sign in to multiple sites rather than have to log in multiple times using different credentials. Users of e-IDs can also better protect their privacy online by limiting the amount of information they share with others. The use of e-IDs also enables many private-sector services that depend on knowing the identity of the individual or something about the individual, such as his or her age, that is otherwise difficult to verify remotely. Some e-IDs can also be used as a digital wallet to make purchases both in person and online.

The use of e-IDs can also facilitate many types of e-government services. Government can streamline many services, such as providing government benefits, which depend on knowing an individual's identity. Government can also better offer innovative services, such as online voting, that require remote authentication. Citizens may complete and sign government forms electronically from anywhere with an Internet connection, thus eliminating time-consuming trips to government offices or public notaries. Similarly, businesses can securely interact with government online for activities such as paying taxes or requesting permits. Using secure electronic communication also eliminates the need to transcribe data from paper forms, helping to reduce errors and processing time. Government receives many of the benefits from increased efficiency, for example by eliminating duplicate data entry, and reducing the costs associated with unnecessary paperwork including printing costs, storage, transportation and disposal.[8]

Finally, the use of e-ID systems can improve the security of online transactions and help prevent fraud and identity theft. First, e-IDs can create more trust and accountability in the identity ecosystem. For example, by creating sufficient audit logs, it may be possible to create chains of trust that allow a source of fraudulent e-IDs to be identified much more easily than with analog IDs. Second, e-IDs can make it more secure for users to login to information systems by enabling multi-factor authentication. An example of multi-factor authentication is requiring the user both to know a PIN and have an e-ID token to login to a website. Much like an ATM card, if an e-ID is lost or stolen, it cannot be used without the PIN or password. Most information systems today do not use multi-factor authentication for user login. Instead, most users track and maintain multiple usernames and passwords. Although the best practice is to use a unique password for different accounts, individuals commonly reuse the same password on multiple sites. This means that if a user's password is compromised on one website, it is compromised on every other site that uses the same password. Further, if a user's password is compromised, the user

must locate and track every account that reuses this password. In contrast, with an e-ID, the user only has to change the password once. In addition, since users must remember multiple passwords today, they often use a weaker, but easier-to-remember, password rather than a stronger, but more complex, password. If users only have a single e-ID to manage, they will have more of an incentive to use strong passwords.

ELECTRONIC IDENTIFICATION SYSTEMS: DEPLOYMENT AND USE

This report looks at countries that have widely deployed electronic identification (e-ID) systems at the national level that allow individuals electronically to provide identification and sign digital transactions to entities in both the public and private sector. It will primarily focus on nationwide initiatives and avoid analyzing regional projects or those limited to addressing a single application or sector. This report identifies countries leading in electronic identity systems based on three factors: the level of adoption of the technology, the maturity of the digital infrastructure, and the level of use of the technology in the public and private sector.

Many countries have launched national electronic ID systems and are at various stages of deploying this technology. As shown in Table 2, there are over 600 million individuals in OECD countries that have created e-ID systems. Since many nations have only recently begun their rollouts, adoption levels are expanding daily as more citizens receive e-IDs and government agencies and businesses launch new services that make use of this technology. While no country has achieved universal adoption and use, some countries have made more progress than others.

Much of the investment in e-IDs has been seen in Europe. The European Union has driven the development of interoperable national ID cards with the creation of the European Citizen Card (ECC) standard. At the Manchester Ministerial Conference in 2005, European nations unanimously endorsed a plan to create an electronic ID program in member countries. As shown in Table 2, many European countries, including Belgium, Finland, Sweden, and Portugal (among others), have created national e-ID programs. Many of these programs are fairly recent. For example, Lithuania began a national roll-out of a biometric national e-ID in January 2009. While the primary purpose of the Lithuanian smartcard is to provide a more secure ID card and facilitate efficient border control, the ID card also contains a digital certificate that can be used by individuals on a computer with a card reader for more secure online transactions, such as authenticating to an online service or electronically signing a document.[9]

Countries outside of Europe are also pursuing national e-ID initiatives, including Bahrain, Qatar, Malaysia, Oman, Saudi Arabia and the United Arab Emirates (UAE). Saudi Arabia, for example, has created an e-ID program that will replace its mandatory national ID card. The e-ID will contain biometric information, serve as an official travel document and offer a digital signature function through a public-key infrastructure application.[10] Other Middle Eastern countries have also made substantial investments in these types of programs—as of April 2009, 98 percent of UAE citizens had completed their registration for the new e-ID and over a million cards had been issued out of a population of approximately 4.6 million.[11]

As shown in Table 1, countries can be divided into five categories: high-deployment/high-usage, high-deployment/low-usage, low- deployment/high-usage, low-deployment/low-usage, and no deployment/no usage.

	High deployment	Low deployment	No deployment
High use	Estonia	Denmark, Sweden, Italy, Spain	n/a
Low use	Austria, Belgium, Malaysia, Slovenia	Finland, Germany, Iceland, Lithuania, Portugal	n/a
No use	n/a	n/a	United States

Table 1: Levels of deployment and use of e-ID systems, select countries

The clear leader in deployment and usage of a national e-ID system is Estonia. As of early 2011, Estonia had issued approximately 1.2 million cards out of an eligible population of 1.3 million citizens (i.e. individuals age fifteen and older). In addition, since inception cardholders have used their card to create more than 52 million electronic signatures and used their e-ID for 88 million electronic authentication transactions.

A second group of countries, including Austria, Belgium, Malaysia and Slovenia all have high levels of adoption of e-IDs, but have yet to show high levels of use. For example, Austria, Malaysia and Slovenia all have near universal roll-out of e-ID cards, but the data shows little use of digital certificates for signing digital documents or authenticating citizens to electronic services. Belgium also has a high level of deployment, having fully rolled out the e-ID system to its 10.7 million citizens, and is already using its second generation of e-IDs. However, Belgium also reports a relatively low rate of use, with 14.2 percent of citizens using an e-ID to electronically file their income tax.[12]

A third group of countries have low levels of deployment, but higher rates of use among the population. These nations include Denmark, Sweden, Italy and Spain.

A fourth group of countries have begun to deploy e-ID systems but still are in a nascent stage, lacking both high levels of deployment and use. These nations include Finland, Germany, Iceland, Lithuania, and Portugal.

Finally many nations, including the United States, have not begun to deployment a national e-ID system and consequently have no use.

Country	Population	e-ID	Name	Website
Australia	21,766,711	No	n/a	n/a
Austria	8,217,280	Yes	Bürgerkarte	www.buergerkarte.at

Belgium	10,431,477	Yes	BelPIC	eid.belgium.be
Canada	34,030,589	No	n/a	n/a
Chile	16,888,760	No	n/a	n/a
Czech Republic	10,190,213	No	n/a	n/a
Denmark	5,529,888	Yes	OCES	www.signatursekretariatet.dk
Estonia	1,282,963	Yes	ID-kaart	www.id.ee
Finland	5,259,250	Yes	FINEID	www.fineid.fi
France	65,312,249	Yes	Vitale	www.sesam-vitale.fr
Germany	81,471,834	Yes	ePA	www.personalausweisportal.de
Greece	10,760,136	No	n/a	n/a
Hungary	9,976,062	Yes	Client Gate	ugyfelkapu.magyarorszag.hu
Iceland	311,058	Yes	Rafræn skilríki	skilriki.is
Ireland	4,670,976	No	n/a	n/a
Israel	7,473,052	No	n/a	n/a
Italy	61,016,804	Yes	CIE and CNS	www.progettocns.it
Japan	126,475,664	Yes	Juki Card	www.juki-card.com
Luxembourg	503,302	No	n/a	n/a
Mexico	113,724,226	No	n/a	n/a
Netherlands	16,847,007	Yes	DigiD	www.digid.nl
New Zealand	4,290,347	No	n/a	n/a
Norway	4,691,849	Yes	MyID, BankID, BuyPass	Various
Poland	38,441,588	No	n/a	n/a
Portugal	10,760,305	Yes	Cartão de Cidadão	www.cartaodecidadao.pt
Slovak Republic	5,477,038	No	n/a	n/a
Slovenia	2,000,092	Yes	Various	Various
South Korea	48,754,657	Yes	i-PIN	i-pin.kisa.or.kr
Spain	46,754,784	Yes	DNIe	www.dnielectronico.es
Sweden	9,088,728	Yes	Various (BankID, Nordea, TeliaSonera)	Various
Switzerland	7,639,961	Yes	Suisse-ID	www.suisseid.ch

Turkey	78,785,548	Yes	Various	Various	
United Kingdom	62,698,362	No	n/a	n/a	
United States	313,232,044	No	n/a	n/a	

Table 2: Summary of national e-ID systems in OECD countries

COUNTRY PROFILES

The following section provides an overview of select countries and their e-ID systems.

Austria

Austria has a rather unique system for electronic IDs (e-IDs). The Austrian government launched its e-ID initiative in November 2000 with the mission of using e-IDs to facilitate access to public services, such as health insurance. The Austrian citizen card enables e-government applications by allowing citizens to electronically identify themselves to public authorities and to sign documents, such as contracts or government forms. In contrast to a single type of e-ID, such as a national ID smartcard, the Austrian Bürgerkarte (citizen card) can take many forms. The initial plan included providing smartcards to citizens, but the government committed from the outset to allowing alternative tokens to be used for electronic identification.

Austria allows citizens to enable the e-ID feature on a number of physical tokens from both the public and private sector including government ID cards, bank cards, health insurance cards, and mobile phones. For example, since March 2005, all bank (ATM) cards issued by Austrian banks have also been required to be official, secure signature-creation devices (SSCD), meaning they are capable of generating an electronic signature as defined by Austrian law. In addition, Austria began to distribute health insurance cards in May 2005 and completed its roll-out by November 2005.[13] Beginning in 2004, individuals could also use their mobile phones as citizen cards using the "A1Signature" service provided by an Austrian telecom provider. Other types of citizen cards include public service cards used by various federal ministries, student service cards provided by some universities, and membership cards from the Austrian Computer Society.[14] As of 2008, Austria had distributed approximately nine million e-IDs or virtually one for every citizen.[15]

All citizen cards store basic personal information, including the individual's name and date of birth. In addition, every person is assigned a unique identifier, known as the sourcePIN. The sourcePIN is derived from data in the Central Register of Residents and is stored on the citizen card. The purpose of the number is to help eliminate ambiguity about a person's identity that may arise when relying solely on data such as name and date of birth. Citizen cards also contain a digital certificate for digital signatures, which individuals can opt to link to a specific email address. Finally, the citizen card can also contain an electronic mandate that authorizes the cardholder to act on behalf of another person or legal entity.[16] Depending on the type of card used, additional data may be stored on the card, such as bank account information on the ATM card or a student ID number on a student ID card.

In general, the minimum amount of information necessary to identify an individual is stored on the card.[17]

Austria has emphasized technology neutrality in its support of e-ID. While the government has developed standards for the citizen card, the requirements are minimal and provide much flexibility for implementation. For example, the standard states that the e-ID must be capable of generating and verifying an electronic signature, but it does not mandate a specific cryptographic algorithm. The standard does define a basic security layer XML interface to ensure interoperability between different implementations. The security layer abstraction allows developers to create Internet applications without concern for the specific implementation on each different type of citizen card.

The Austrian e-ID system also emphasizes interoperability with foreign e-IDs, a characteristic unique to Austria. To date, efforts have been made to allow the use of Belgian, Estonian, Finnish and Italian e-IDs in the Austrian system. Non-Austrians not listed with the Central Register of Residents are added to the Supplementary Register and assigned a sourcePIN based on the unique identifier in their own country's e-ID, such as the tax ID number used with Italian ID cards. While the framework is in place to accept foreign e-IDs, applications have not yet been designed with this functionality, so use by foreigners is limited.[18]

The Austrian government has actively promoted the use of e-IDs, and has procured and made freely available the software needed by citizens to use their e-IDs on their personal computers. The government similarly purchased and made freely available the software modules needed by developers to implement server-side applications such as authenticating a user, verifying a signature and creating a signature. By providing the basic building blocks for creating secure online applications, the Austrian government has made it easier for the private sector to take advantage of the widespread availability of e-IDs.

Belgium

Belgium has worked diligently to provide e-IDs to its population of 10.7 million. Conceived in 2001, e-ID cards were officially launched in 2004; as of 2009, 90 percent of Belgian citizens had one.[19] With over nine million e-IDs in circulation, the Belgian personal identity card (BelPIC) is the largest national e-ID system in Europe.[20] The card is compulsory for citizens from the age of twelve. In 2007, Belgium also began issuing foreign permanent residents an e-ID. The e-ID for foreign residents comes in two varieties: one for foreign residents from within the EU and one for foreign residents from outside the EU. In addition, in 2009, Belgium introduced e-IDs for children under the age of twelve. The card is optional for children living domestically, but required for those traveling abroad.[21]

Figure 1: Example of a Belgium e-ID card

As shown in Figure 1, the BelPIC card contains visual printed data including name, place of birth, nationality, gender, card number and expiration date, signature, photograph, national registration number (RRN), place of issue and issuer. The design purposefully omits an address from the card to avoid the need to replace the card when individuals move. The card also contains this personal data on an embedded chip. In addition, the card contains two digital certificates: one for authenticating and one for signing. All cards have the authentication and signature capabilities enabled by default; however, users can choose to opt out of these features.[22] The e-ID for children does not contain a digital certificate for signing since children cannot enter into legally binding contracts in Belgium.

Since 2004, early adopters of the Belgium electronic ID card could use the card to authenticate to e-government applications using a digital certificate stored on the card. Today citizens can use the card for a variety of applications, such as digitally signing their electronic tax filings. The Belgian government now offers over six hundred services online for its citizens, including applications such as "Police on the Web" that allows citizens to interact with local police to report stolen items or graffiti.[23] The e-ID can also be used to purchase tickets, as for sporting events—cardholders who do so then use their ID card as their ticket to enter the stadium. However, actual reported usage of e-IDs remains relatively low in both the public and private sector and the availability of services in the private sector are minimal.[24]

One of the most popular e-government services is the "Tax-On-Web" service, which allows individuals to declare their taxes online. Although e-declarations are popular, most are not done with the e-ID. Users also have the option of using a Federal Token, a one-time password (OTP). Federal Tokens are a set of twenty-four unique OTPs used to access government services online. As shown in Figure 2, in 2009, approximately 240,000 individuals used the Federal Token to submit their online tax declarations compared to approximately 61,000 who used the e-ID.
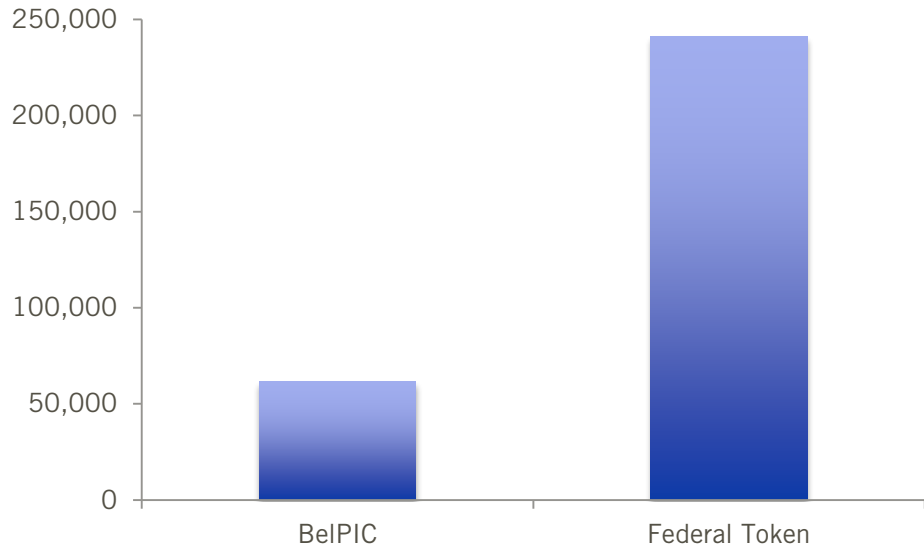
Figure 2: Technology used for e-declaration in Belgium, 2009[25]

Use is particularly low for the signing function of the e-ID due to a variety of factors including low awareness among citizens, low perceived value among businesses and government agencies, and challenges with using the card-based signature functionality on a PC.[26]

Denmark

Unlike many European countries, Denmark has not implemented a card-based national e-ID system. The Danish government does not issue national ID cards. Instead, individuals can obtain identity documents such as passports and drivers licenses. In addition, Denmark maintains a national population register. Originally established in 1924 and maintained at the local level, the population register was centralized in 1968. Each citizen has a central population register (CPR) number, a unique personal ID number that is used in many public and private-sector transactions.

As early as 1992, Denmark had an e-government strategy calling for an e-ID; however, it took more than ten years to launch the first national e-ID solution. The first project was OCES, a software-based digital signature certificate installed on a user's PC.[27] It was launched in 2003 by the Ministry of Science, Technology and Innovation. Users enrolled in OCES by visiting a government website and entering their CPR number and email address. Two separate passcodes were then sent to the user: one at the email address and one to the mailing address on file for their CPR record. Both codes were needed to install and activate the software certificate on the user's PC.

In July 2010, the government began issuing NemID, a new e-ID solution intended to replace OCES.[28] The government ceased issuing OCES digital certificates in June 2011. OCES certificates expire after two years, so they will be completely phased out and replaced with NemID by mid-2013.[29] NemID is intended to provide a single sign-on solution for e-government applications, online banking and other services. In addition, it can be used to sign electronic transactions. NemID provides two-factor authentication and

consists of a username, password, and a key card with a set of one-time passcodes (OTP). The key card is a small credit-card sized document printed with 148 OTPs. After these OTPs are used up, the user is sent by mail a new key card with new passcodes.

The process to obtain a NemID is similar to OCES. The advantages of the NemID are that, unlike OCES, it provides two-factor authentication and it can be used on any PC. Adoption of NemID has been rapid. On October 13, 2010 the Danish IT and Telecom agency announced that it had issued more than a million NemIDs since it was first launched in July. The agency also noted that the e-IDs had been used more than 17 million times since adoption. In comparison, since OCES was launched in 2003, only 1.5 million of these digital signatures have been issued.[30] Adoption has been driven in part by online banking—as banks convert to NemID they upgrade their customers.

Various other sector-specific e-ID systems are in place including for taxes, banking, and health care. For example, the Danish tax authority (SKAT) provides two electronic signature methods for individuals and businesses: a one-time password and a software-based digital certificate installed on a PC. Banks also issue netID, an e-ID solution, to their customers. Banks establish a netID for their customers using the information in the CPR. In health care, the government provides citizens with health insurance cards, which can contain digital certificates. There are two health insurance cards: a National Health Insurance Card (yellow card) and a European Health Insurance Card (blue card). The yellow card provides access to medical services in Denmark; the blue card provides access to health care to citizens traveling abroad in EU member states. Health care providers use the cards to retrieve medical records and file insurance claims. The cards can also be used to access other services, such as borrowing books from the library. The cards can contain a digital certificate used for health care applications.[31]

Estonia

Estonia launched its electronic ID card program in February 1999 when the Estonian Parliament passed the Identity Documents Act. The Act became effective January 1, 2000 and established national guidelines for the creation of a mandatory national identity card. Before this, Estonia did not have a national personal identification document. The ID card was created to function both as a physical ID and an electronic ID. The Act states that the national identity card will contain digital data allowing citizens to perform electronic transactions—specifically, a certificate enabling digital identification and digital signing.[32] Estonia issued its first electronic ID cards in 2002, some 130,000 cards in that first year.[33] As of 2011, over 90 percent of the population in Estonia had an e-ID.[34] With a population of approximately 1.3 million, this means that the Estonian government has now distributed identity cards to over a million citizens. Foreign residents can also obtain a card for their use.

Estonia's national ID contains the following information on the front of the card: name, photograph, signature, personal ID number, date of birth, gender, citizenship status, card number, and card expiration date. The back of the card contains the following information: place of birth, card issue date and residence permit information if available. The card also contains the non-graphical information (i.e. data not including the

photograph or signature) in machine-readable format. The chip on the ID card contains two certificates, one for electronic authentication and one for electronic signatures. Estonia is one of the few European countries where the electronic signature functionality is not optional.[35] The certificates contain the cardholder's name and personal ID number, and the authentication certificate also contains an official e-mail address unique to each cardholder. The card is compulsory for citizens age fifteen or older.

Figure 3: Example of an Estonian e-ID card

Estonia provides an official e-mail address to each citizen. The e-mail address is used for official government communications, but it can also be used for private communications. A citizen's email address is in the format "firstname.lastname_NNNN@eesti.ee" where NNNN represents four random digits. Every card holder can also receive email at the address "ID_CODE@eesti.ee" where ID_CODE represents the personal ID number of the citizen. Estonia does not provide an email service to its citizens; instead, the e-mail address acts as a relay and citizens specify an email account where the messages are delivered. All email addresses are publicly listed on Estonia's National Registry of Certification Service Providers' certificate directory.[36]

The Estonian e-ID project includes both public and private-sector partners. The national ID card is officially administered by the Estonian Citizenship and Migration Board, a government agency. The electronic infrastructure is maintained by the Certification Center, AS Sertifitseerimiskeskus (SK), a partnership between two banks, Hansapank and Eesti Ühispank, and two telecom companies, Eesti Telefon and EMT. SK is the certification authority for electronic IDs in Estonia and operates the associated certificate-related information services. SK also operates the distribution of ID cards—citizens can go to the retail branches of these banks to get their cards. Finally, the company TRÜB Baltic AS, a subsidiary of Swiss TRÜB AG, is responsible for personalizing the cards—both physically and electronically.[37]

SK has created various systems to encourage the use of electronic IDs. One important implementation is DigiDoc, a technical framework that allows individuals to create and verify digital signatures for electronic documents. DigiDoc consists of multiple components to create, share and verify digital signatures, including a client application for use on a desktop PC, a web-based online application, and a portal to verify and share documents with multiple signatures. DigiDoc also includes various programming libraries

that allow developers to easily implement digital signature capabilities into commercial applications. DigiDoc is based on XML Advanced Electronic Signatures (XadES), a technical standard published by the European Telecommunication Standards Institute (ETSI) that defines a structured format for storing signed data, digital signatures, and security attributes.[38] DigiDoc uses a standardized format to promote interoperability.

The government has not placed any restrictions on the use of the e-ID in the private sector and the authentication mechanism is available to any outside developer. Thus, any organization can build an application that uses the e-ID for identification and authentication. Currently, applications exist for using the e-ID to authorize online bank transactions, to sign contracts and tax declarations, to authenticate to wireless networks, to access government databases, and for automated building access.

The government is using e-IDs to eliminate waste and improve services: for example, citizens can access health care services using their e-IDs rather than needing a separate health care card. The Estonian police board is integrating the ID card with a driver database so that they can verify the status of drivers, eliminating the need for citizens to carry a separate driver's license. In the Estonian cities of Tallinn, Tartu, and Harjumaa, the government implemented a paperless ticket system with e-IDs to replace physical tickets for public transportation. Passengers can purchase fares at kiosks, on the Internet, or by mobile phone and then use their national ID card as their ticket. Passengers who qualify for reduced or no-cost fares can also use their ID card as their ticket. Over 120,000 individuals use the ID ticket system regularly in these cities and twenty months after implementation accounted for 60 percent of municipal ticket income.[39]
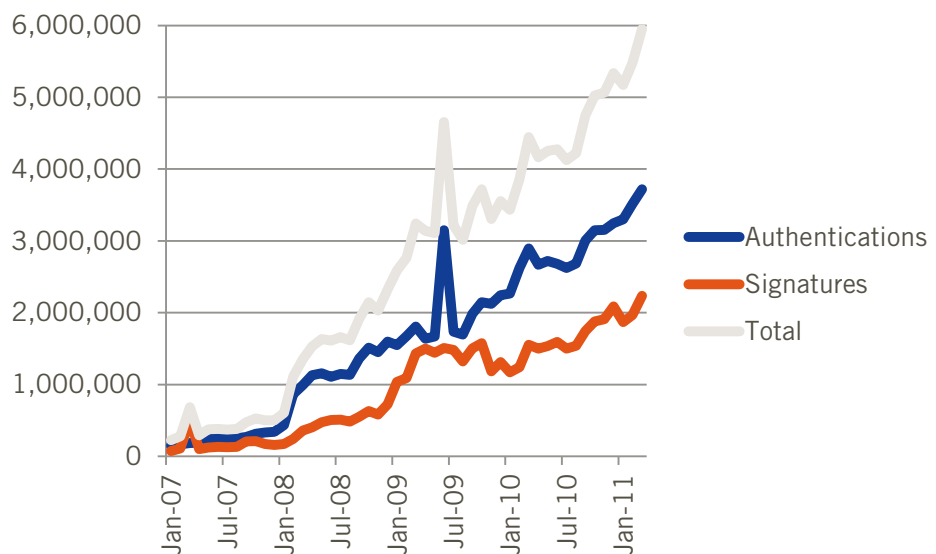

Figure 4: Number of signature and authentication transactions in Estonia, 2007-2011

The success of e-IDs in Estonia can be seen in the numbers. As shown in Figure 4, the use of e-IDs for electronic signing and authentication continues to grow steadily. In addition, one of the most innovative applications of the e-ID in Estonia, introduced in 2005, has

enabled citizens to vote over the Internet. Almost one quarter of Estonian voters in the parliamentary elections in March 2011 cast their vote online using their e-ID.[40] Furthermore, 15 percent of cardholders in Estonia use the e-ID for public transportation and 10 percent of cardholders use the e-ID for electronic signatures.[41] However, even with widespread deployment of e-IDs, 65 percent of taxpayers filed their taxes online using a PKI sponsored by banks rather than with their e-ID.[42] One reason for this is that the secure online infrastructure created by the banks existed before the national ID cards were launched.

Estonia has also launched "Mobiil-ID" an electronic ID for mobile telephones. Like the electronic ID card, the Mobiil-ID contains certificates that allow individuals to identify themselves and sign documents digitally. The Mobiil-ID certificates are stored on a subscriber identity module (SIM) card used in mobile phones. Many digital services allow individuals to use the Mobiil-ID instead of the ID card.

Malaysia

Malaysia has long sought to be a global leader in the information technology industry. Beginning in 1996, the Malaysian government created the Multimedia Super Corridor, now known as MSC Malaysia, as a government initiative to transform the nation into a knowledge-based society. As part of this overall plan, in 1999 Malaysia began developing MyKad, one of the world's first national e-ID cards. Since its inception, the goal has been for MyKad to be a multi-purpose smartcard to use in both the public and private sector. The government had rolled out the MyKad to all Malaysian citizens and permanent residents over the age of twelve by 2005.[43] By 2006, the government had issued 19 million smartcards.[44] Today, deployment is near universal within the country and the card must be carried at all times.

MyKad is the size of a standard credit card and the latest version is embedded with 64 kilobytes (KB) of non-volatile memory that stores personal information, a thumbprint and digital certificates for different services. The card includes security measures intended to prevent tampering and fraud, such as a standard challenge-and-response mechanism to prevent unauthorized access to the card. This security measure helps to prevent unauthorized users from reading private data or changing data on the card. MyKad includes a public key infrastructure (PKI)—the card can store a digital certificate issued by a Malaysian certification authority.[45]

Figure 5: Example of a Malaysian MyKad card

To take advantage of the MyKAD PKI, known as "MyKey," card holders must acquire a digital certificate from a certification authority such as Trustgate or Digicert. These certification authorities provide digital certificates that can be loaded on an ID card, smartcard or USB token. The price for a digital certificate is approximately ten dollars a year. The digital certificate can be used to make online transactions more secure. For example, a website can require a user to provide a digital certificate (and thus prove her identity) before granting access to the online application. Using the digital certificate, a user can also digitally sign an online transaction.[46]

Developed by several agencies, including the Malaysian Road Transport Department, the Royal Malaysian Police, the Immigration Department, and the Ministry of Health, Malaysia's compulsory national ID card is designed to be a single authentication token for use in transactions with both government entities and private businesses.[47] The card works as a debit card, an ATM card and a driver's license. MyKad can also be used at Malaysian immigration checkpoints for more efficient exit and re-entry of the country. Each e-ID card contains encrypted information about its owner, including e-cash balance, health information, driver's license information, passport information, and biometric data including fingerprints and a photograph. Malaysian citizens and permanent residents can use their e-ID card for over thirty different applications, including e-commerce transactions, e-banking, health care, and the use of public transportation.[48] For example, the "Touch 'n Go" functionality on MyKad allows card holders to quickly pay for charges such as tolls, parking and bus fares.

Businesses and government are successfully developing a diverse set of applications that use MyKad to implement new solutions. For example, the Malaysian government provides a generous fuel subsidy for citizens to make driving more affordable. As a result of the artificially low prices, thousands of Thais and Singaporeans cross the border every day to buy fuel at a steep discount—a costly consequence of the Malaysian policy. To address this issue the company ePetrol has developed a new application to have gas station kiosks sell fuel at two prices: an unsubsidized price to any customer and then a subsidized price to customers who can prove their citizenship with their MyKad. In theory, this application could be extended if the government wanted to further target its subsidy program, such as

only providing the subsidy to certain low-income drivers or to individuals with fuel-efficient vehicles registered in their name.[49]

Another company has developed a mobile device "AXIA" that incorporates built-in card reader technology to allow mobile access to e-ID cards. With the AXIA smart phone, for example, a sales person can capture a customer's MyKad information and allow a customer to easily purchase a product or sign up for a service. Customers use their MyKad with the mobile device to quickly identify themselves and then complete the transaction electronically. Any data collected on the smart phone can then be uploaded using a mobile data service.[50]

Children are issued a similar identification card called "MyKid." ("My" refers to Malaysia and "Kid" refers to the acronym "Kad Identiti Diri" meaning "Personal identification card.") Unlike MyKad, MyKid does not contain biometric data such as fingerprints and a photograph. The main purpose of MyKid is to be the official government-issued identification for interacting with the public and private sector. The primary applications of the card are with hospitals, clinics and schools. These organizations can use MyKid to access personal health and education information.[51]

Norway

Norway has three principle e-ID systems, one sponsored by the government and two by the private sector. These systems are not interoperable.

The government provides MinID ("MyID"), a voluntary e-ID system that can be used to access a variety of online government services. It is available to citizens over the age of thirteen. Individuals register for a MinID online using their national ID number. The Tax Authority then sends out a set of one-time passwords in the mail to the address on file with the national register. Individuals can then use these codes to authenticate to online services. Alternatively, individuals can register a mobile phone and receive one-time passwords via SMS. MinID provides users single-sign-on capabilities across approximately fifty e-government services including at the Directorate of Taxes, the Ministry of Labor and Welfare Services, and the State Education Loan Fund. As of April 2010, two million Norwegians had registered for MinID accounts.[52] Many of these individuals have registered for MinID to file their taxes online.[53]

The private sector offers two e-ID solutions: BankID and Buypass. Both of these e-ID systems provide a greater level of assurance than MyID. The Norwegian government recognizes four different levels of assurance for online authentication and electronic signatures. MinID does not meet the highest level of assurance in Norway; however, BankID and Buypass meet this standard.

Provided by a consortium of banks, BankID gives citizens the ability to authenticate to various online services and electronically sign documents, both in the public and private sector. An e-ID can come in different forms depending on the bank and include one-time passwords, an electronic code calculator, and a smartcard.[54] Individuals obtain an e-ID by presenting identification, such as a passport, at the bank. Notably, BankID can be issued to both individuals and legal entities (i.e. an organization). In addition, BankID is available

both as a remotely stored certificate accessed with a password and unlocked with a PIN, and as a certificate stored on the SIM card of a mobile phone. BankID has had swift adoption. As of 2006, some 600,000 BankID certificates had been issued.[55] As of June 2011, BankID users totaled more than 2.5 million out of a population of 4.7 million and these individuals were completing thousands of transactions per day using their e-ID. In addition, 328 organizations accepted BankID. The majority of these service providers are banks, with the remainder in the private sector and government.[56]

BuyPass is another e-ID solution offered by the private sector and available as both a smartcard and on a mobile device. The Norway Post and Norwegian Lottery run this e-ID system, which was conceived in 1997 and first piloted in 1999. As of 2008, BuyPass had two million users generating over 13 million transactions per month. The BuyPass e-ID card is available for approximately seventy dollars.[57] BuyPass is being used in both the public and private sector.

Sweden

Sweden established its electronic signature legislation in 2000 and issued its first e-IDs in 2003.[58] The Swedish e-ID system provides an interesting contrast to those of many European countries. Rather than create a single government-issued e-ID card, Sweden has created an e-ID system in partnership with the private sector. In Sweden, both the government and the private sector issue e-IDs and, depending on the e-ID chosen, Swedish users have the option of obtaining an e-ID on a card, on a mobile device, or on a file that can be downloaded to a PC. All e-IDs include two certificates: one for authentication and one for signing. They also contain the name and personal ID of the individual. Electronic IDs are available to individuals for both personal and professional use. Professional e-IDs are linked to a specific organization's ID number rather than to an individual's ID number.[59]

Currently there are four private-sector providers of e-IDs in Sweden: BankID (a consortium of banks), Nordea (bank), Telia (telecom) and Steria (IT security). File-based and mobile e-IDs are restricted to people over the age of eighteen; card-based e-IDs provided by the private sector are available to adults and children age thirteen and older with parental consent.[60]

The government also issues two types of ID cards: the National ID card prepared for E-Legitimation (NIDEL) issued by the police and an ID card issued by the Tax Authority. Sweden began offering the NIDEL card in October 2005. This card serves as a proof of identity and citizenship. It contains a digital photo of the cardholder, meets ICAO standards, and is a valid travel document within the Schengen area. The NIDEL card is available to all citizens, but is not compulsory and does not replace previously-issued paper ID cards. The card contains a contact chip, and may be used in the future to access government services.[61] The Tax Authority card is available to individuals age thirteen and older (and with parental consent to those under age eighteen). While the NIDEL card contains a chip and could provide e-ID functionality, this is currently not offered. The Tax Authority ID card can serve as an e-ID. As of 2009, approximately 300,000 NIDEL cards and 30,000 Tax Agency cards had been issued.[62]

The BankID is the most used e-ID in Sweden with over two million active users in 2010. In 2010, Swedbank began issuing the first Mobile BankID to allow people to use an e-ID on their mobile phone.[63] The file-based e-IDs are the primary use of e-ID in Sweden for e-government services, accounting for approximately 92 percent of e-IDs used. Card-based e-IDs are used more in the private sector (10 percent) than the public sector (1.3 percent).[64] The cost of e-IDs varies by implementation. The file-based e-IDs are available at no cost to users; however, card-based implementations can cost between forty and eighty euros. Each relying party (e.g., business or government agency) pays by the transaction.

Use of e-IDs in Sweden is fairly evenly split between the public and private sector. Various government services allow individuals to use electronic IDs including for filing taxes, obtaining services from the Swedish Social Insurance Agency, applying for and renewing a driver's license, and registering vehicles.[65] Most of the services in use are at the national level rather than the local level. In the private sector, the dominant use of e-IDs is for online banking. In addition, approximately five hundred e-commerce sites accept the BankID card or mobile BankID.[66] In addition, the availability of e-IDs has led to the development of some new businesses and services in Sweden. For example, the company Egreement AB has an e-contracts service that allows individuals with e-IDs to quickly create, sign, store and manage electronic contracts completely online without ever needing a face-to-face meeting.

The Swedish e-ID is most widely used for annual income declaration. People can use one of five e-declaration services to sign their declaration: an e-ID, a security code (over the Internet), a telephone, SMS, or smart phone. As shown in Figure 6, the percent of users of e-IDs for declaring annual income electronically has grown slowly, from around 20 percent of e-filers in 2005 to almost 30 percent in 2011. Notably, there has also been an increase in the total number of e-ID users during this period, from approximately 400,000 in 2005 to 1.3 million in 2011.
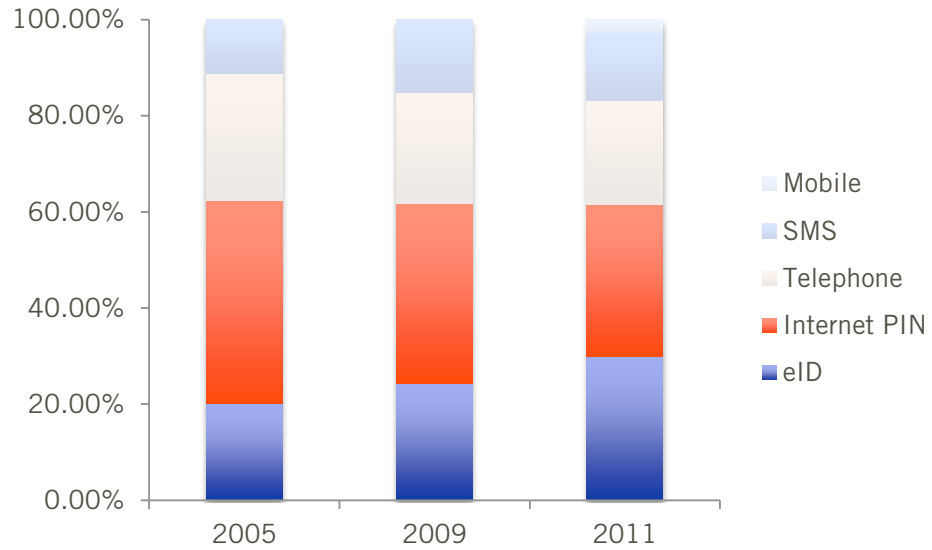

Figure 6: Percent users signing e-declaration in Sweden by technology, 2005-2011[67]

Turkey

At present Turkey does not have a nationwide e-ID system, although the government is currently planning to begin issuing Turkish e-ID cards (T.C. Kimlik Karti) in 2012. Turkey completed a three-phase pilot in 2010 for a national e-ID system.[68] Approximately 220,000 cards were issued to residents in Bolu.[69] The card allowed citizens to access government and bank web sites and could be used in hospitals and pharmacies. As of 2009, there were ten systems using the pilot e-ID cards for authentication.[70]

Turkey's new smartcard implementation will replace the current paper ID card. The front of the card will contain the individual's photograph, name, gender, date of birth, nationality, card number and expiration date, and a Turkish Republic Identity Number (TRIN), a unique personal ID number used by all government agencies and frequently in private-sector transactions (as it is printed on the national ID card). The back of the card will contain the card owner's parents' names, last name at birth, place of birth, issuing authority, blood group, marital status and religion.[71] The chip will additionally contain biometric data (fingerprint and finger vein) and digital certificates. A citizen's biometric information is stored only on the e-ID card.

Turkey has made a number of investments to create the organizational, technological, and policy-related infrastructure necessary to deploy a national e-ID system. Over the past ten years, Turkey established a central civil registration system (MERNIS), administered by the Ministry of Interior, and the TRIN. In addition, four service providers offer digital certificates for software-based electronic signatures and two mobile phone operators provide mobile e-signatures using the SIM cards.[72] In 2008, Turkey began operating e-Government Gateway, a national identity management system to provide single-sign-on for government applications.[73] Users can authenticate to the system using an e-ID (for those participating in the pilot), or a combination of their TRIN and password (obtained by mail or in person for a fee), a digital signature, or a mobile signature.[74]

United States

As of 2011, the United States does not have a national e-ID system. Although the United States passed federal electronic signature legislation in 2000, creating the legal framework for such a system, this was a necessary, but not sufficient step for creating a robust electronic identity ecosystem. Currently, neither the government nor the private sector provides a widely used electronic ID in the United States. Experts widely agree on the need for better identity management in the United States. For example, the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency recommends, "The United States should allow consumers to use government-issued credentials (or commercially issued credentials based on them) for online activities, consistent with protecting privacy and civil liberties."[75] Similarly, the National Broadband Plan recognized that for government to be able to deliver services online requires the ability to securely identify and authenticate individuals online. The Plan also noted that college students could more easily apply for financial aid if agencies could share information that they already have about individuals. To that end, it recommended that "OMB and the Federal CIO Council should develop a single, secure enterprise-wide authentication protocol that enables online service delivery." In addition, the Plan suggested that

"Congress should consider helping spur development of trusted 'identity providers' to assist consumers in managing their data in a manner that maximizes the privacy and security of the information."[76] Unfortunately, federal efforts to improve identity standards at the national level have routinely been met with opposition from a broad range of activists. For example, opposition to REAL ID, legislation which was passed by Congress in 2005 to create federal standards for state-issued identity cards, has prevented states from implementing the proposed reforms to date.

BOX 2: U.S. FEDERAL GOVERNMENT ELECTRONIC IDENTITY MANAGEMENT EFFORTS

The federal government has taken some steps over the past decade to bring the United States closer to adoption of a national-level action plan for the creation of electronic identification of its citizens or residents. To date, most of the activities by the federal government have focused on improving the quality and security of identification used to gain access to federal information systems. These government-wide efforts to standardize identity management began at the behest of guidance issued by Joshua Bolten, then director of the Office of Management and Budget, in December 2003 in response to the E-Government Act. The memorandum "E-Authentication Guidance for Federal Agencies" directed all agencies to conduct e-authentication risk assessments using specific criteria for all systems.[77] It also defined four identity authentication assurance levels ranging from "Level 1: Little or no confidence in the asserted identity's validity" to "Level 4: Very high confidence in the asserted identity's validity." The guidance outlined a risk framework for agencies to use to classify the identity assurance level of each system based on potential impact for authentication errors. The impact errors include inconvenience, distress or damage to reputation, financial loss or agency liability, harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, and civil or criminal violations.[78]

In August 2004, President Bush issued Homeland Security Presidential Directive 12 (HSPD 12), which called for "establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees)."[79] This directive specifically included a requirement to create an identification standard that could be authenticated electronically and used to control both physical access to facilities and logical access to information systems. This directive did not apply this standard to national security systems. Before HSPD 12, agencies independently created ID management systems to meet their organizational needs and objectives.

In response to HSPD 12, the National Institute of Standard and Technology (NIST) Computer Security Division created the Federal Information Processing Standards Publication 201 (FIPS-201) on Personal Identify Verification (PIV) of Federal Employees and Contractors in March 2006. The goal of FIPS-201 was to create a standard to support HSPD-12 and create interoperability between different government systems. FIPS-201 specified the technical requirements of

the identification standard for federal employees and contractors. The standard described both the administrative requirements, such as identity proofing, registration and issuance, and the architectural requirements, such as the physical card characteristics, system interfaces and security controls. NIST separately issued additional standards for using smartcards and biometric information in Special Publication 800-73 and Special Publication 800-76 respectively. Separate standards for accreditation for PIV card issuers and certification of related IT systems are also not covered within this NIST standard. As of December 2010, 79 percent of the federal employee and contractor workforce requiring ID cards (4,562,288 individuals) had received PIV cards.[80] An example of an HSPD-12 compliant card is the common access card (CAC) issued by the Department of Defense (DoD) for access to DoD systems and facilities.[81]

In 2008, the Federal CIO Council created the Information Security and Identity Management Committee (ISIMC) which created the Identity, Credential and Access Management (ICAM) subcommittee. The purpose of the subcommittee is to foster "government-wide identity and access management, enabling trust in online transactions through common identity and access management policies and approaches, aligning federal agencies around common identity and access management practices, reducing the identity and access management burden for individual agencies by fostering common interoperable approaches, ensuring alignment across all identity and access management activities that cross individual agency boundaries, and collaborating with external identity management activities through inter-federation to enhance interoperability."[82] The ICAM subcommittee is run by GSA and DOD.

In addition to developing technical requirements (see Box 2), in recent years the government has tried to development a holistic vision for ID management throughout the federal government. The National Science and Technology Council (NSTC), a Cabinet-level council formed in 1993, created a subcommittee on Biometrics and Identity Management in 2003. This eventually led to the creation of the NSTC Task Force on Identity Management, which undertook a systematic review in 2008 of the state of identity management in federal government. The Task Force found over 3,000 independently operated federal IT systems that used PII with little coordination and significant overlap. The task force recommended creating a more organized framework that would maintain the existing federated approach to data while increasing security, eliminating duplication, and improving privacy.[83]

In February 2009, President Obama initiated a sixty-day cyberspace policy review, which generated a number of short, medium and long-term recommendations for improving the nation's digital infrastructure. Chief among these recommendations for near-term action was the following: "Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests, leveraging privacy-enhancing technologies for the Nation."[84] The report recognized that building secure and trusted systems, especially for critical infrastructure, requires creating a trusted identity architecture. Moreover, it recommended laying out not just a technical foundation, but also a policy foundation for trust. The report states, "The Federal government should work with

international partners to develop policies that encourage the development of a global, trusted eco-system that protects privacy rights and civil liberties and governs appropriate use of law enforcement activities to protect citizens and infrastructures."[85]

In response to these recommendation, Howard Schmidt, the White House Cyber Security Coordinator, released the draft "National Strategy for Trusted Identities in Cyberspace" (NSTIC) in June 2010.[86] The draft report laid out the first national strategy for creating an "identity ecosystem." The report did not delve into technical or policy mechanisms, but instead outlined a broad vision for online identity and presented four broad goals:

- Develop a comprehensive identity ecosystem framework

- Build and implement an interoperable identity infrastructure aligned with the identity ecosystem framework

- Enhance confidence and willingness to participate in the identity ecosystem

- Ensure the long-term success of the identity ecosystem

The report also included nine action items including designating a federal agency to lead this effort, expanding existing federal efforts, working with the private sector, and collaborating with international efforts.[87] Importantly, the strategy does not limit itself to e-ID for individuals, but instead seeks to address the broader issues of identity and trust between all online transactions, including machine-to-machine (M2M) transactions.

In April 2011, the White House released a final version of the NSTIC that updated the draft strategy.[88] The new document outlined four guiding principles for the development of a national e-ID strategy including that the solution be privacy-enhancing and voluntary; secure and resilient; interoperable; and cost-effective and easy to use. The government also committed to developing a roadmap for further federal activity to build the identity ecosystem with the private sector. Following its release, various technology companies and non-profit organizations endorsed the new strategy.[89]

Outside of government, various private-sector initiatives to create identity management solutions have so far failed to achieve widespread adoption and use in the United States, especially for applications requiring high levels of identity assurance. The most success has been found in providing digital identities to access web services that require little identity information, often limited only to an email address. The most notable private-sector effort in this area came from Microsoft, which created Passport (which today has evolved into Windows Live ID). Originally conceived as an online identity service for all Microsoft Network (MSN) service, it has evolved into an identity system for both Microsoft and third-party sites and a digital wallet to store credit card and address information for e-commerce. As an early promoter of an online identity system, Microsoft faced fierce criticism for its Passport product from groups like the Electronic Privacy Information Center (EPIC) because of potential privacy risks.[90] Despite these setbacks, Windows Live ID had over five hundred million users worldwide as of August 2009.[91]

In terms of adoption and use, the most successful initiatives have come from the private sector, such as Facebook Connect and OpenID. Facebook Connect, launched in 2008, enables users to login to third-party websites using their Facebook accounts. Adoption of Facebook Connect has been swift and over 2.5 million websites have integrated with Facebook.[92] Similarly, OpenID, a distributed identity system framework created in 2005 by an industry-sponsored coalition, now claims over a billion user accounts accepted at over fifty thousand websites.[93] The decentralized OpenID framework allows anyone to use or become an OpenID provider and does not specify the means by which users must be authenticated. As a result, users can find many different websites that either issue or accept OpenIDs, including many popular websites, such as Google, Facebook, Microsoft, Yahoo, AOL and MySpace.

Since OpenID does not specify an authentication mechanism, identity service providers can offer additional layers of security to users based on their needs. For example, Symantec offers the Personal Identity Portal which provides an OpenID implementation for users that can be extended to provide two-factor authentication, such as requiring a browser certificate or using a security token. Google offers two-factor authentication using a security code sent to the user's mobile phone. These types of mechanisms can increase the security of online authentication and protect users in case their usernames and passwords are compromised, such as in the 2011 Sony hacking case.

Developers use identity platforms like Facebook Connect and OpenID to provide their users a single sign-on (SSO) capability with a trusted identity provider (i.e. Google or Facebook) rather than require users to register and maintain a separate username and password on their site. This gives users a more seamless experience as they navigate across different sites because their identity provider can validate their login credentials once and then assert the user's identity to other websites without the user having to login again. The transactions between the website and the identity provider occur automatically in the web browser and are transparent to the user. SSO is made possible by the use of identity standards like Security Assertion Markup Language (SAML), OAuth protocols and WS-Federation.

The federal government has begun to pilot some private-sector SSO implementations. The National Institutes of Health (NIH) Open Identity for Open Government pilot project allows private-sector companies to serve as identity providers for individuals to access NIH applications and data sources. Previously, individuals had to either create separate accounts for each of these resources or belong to an authorized partner, such as another federal agency or educational institute with a federal identity agreement in place. Now individuals can access resources using an OpenID or Information Card. When the project launched in September 2009, ten companies, including Yahoo!, PayPal, Google, Equifax, AOL, VeriSign, Acxiom, Citi, Privo, and Wave Systems, announced that they would support the pilot program.[94]

LESSONS FROM EARLY ADOPTERS

Policymakers have many opportunities to learn from the countries furthest along in deploying electronic identity systems. There is no single reason why a county like Estonia is

the leader, although there are various factor at play that have led to its relative success. The following section reviews the impact of certain decisions on the development of e-ID systems in various countries, focusing primarily on the countries that have shown the greatest progress, but also drawing on lessons from other early adopters. It also shows that countries have many options for building an e-ID system, and can design a system to address their unique needs.

Legal Framework for Electronic Signatures

Signatures have always served an important role in identifying individuals and allowing them to signify acceptance of an agreement. Various types of legal agreements, including business contracts, credit card transactions, personal checks, government documents, and wills, require signatures. With the dawn of the information age, an increasing number of individuals and businesses communicate electronically, and thus need an electronic means to sign agreements and messages when a face-to-face meeting is unnecessary or impractical. Many nations, including the United States, have responded by updating laws and regulations to recognize the electronic signature as a valid legal instrument much like a handwritten signature on paper. However, acceptance in the eyes of the law is a necessary, but not sufficient, step towards ubiquitous use of electronic signatures.

Various technologies, including passwords, access tokens (e.g., smartcards) and biometrics, can be used to implement electronic signatures with varying degrees of security. Systems often use one or more of these technologies to establish your identity based on something you know (e.g., password), something you have (e.g., access token) or something unique to you (e.g., biometrics). Passwords use a shared key, usually an alphanumeric combination of text, to establish the identity of the user. A personal identification number (PIN) is a common example of a password. Access tokens include a variety of electronic devices that can identify a user to a system, such as RSA tokens, which generate new electronic PIN codes at fixed time intervals, and smartcards, a plastic card with an embedded microprocessor programmed to activate only after the user enters a password. Examples of biometrics include fingerprints, iris scans, voice recognition, or even a digitized image of a handwritten signature.

A legal framework is a prerequisite for widespread use of e-IDs to create legally-binding signatures. Such a framework is necessary as the use of electronic signatures can only prosper if they are recognized as valid legal mechanisms. Legislation creating the legal regime for electronic signatures must balance both security and efficiency. As policymakers increase the strictness of technical standards, they may improve the security of electronic signatures, but decrease technology neutrality and discourage innovation. They try to find a balance with laws that remove ambiguity and uncertainty from the use of electronic signatures but still provide enough flexibility to allow efficient online transactions. While many nations have passed electronic signature legislation, few have invested in large-scale implementation of the digital infrastructure needed to make electronic signatures accessible and available to most citizens.

Much of the legislation on electronic signatures passed in individual countries has been based on legislation created elsewhere, which has helped create some degree of uniformity

internationally. For example, many countries have based their electronic signature legislation on the Utah Digital Signature Act (the "Utah Act"). Passed by the state legislature in 1995, the Utah Act was the first state legislation to address many of the specific needs for users to authenticate online transactions. The Utah Act allows for the establishment of licensed certification authorities or "cybernotaries." The purpose of the certification authority is to certify that a given "digital signature affixed by means of the private key corresponding to the public key listed in the certificate is a legally valid signature of the subscriber."[95] This effectively limits the use of electronic signatures to digital signatures using only state-licensed certification authorities. However, by creating technology-specific legislation for electronic signatures, legislators were able to include specific provisions about when a digital signature would be considered valid (e.g., if the certificate authority had not been revoked the certificate). If these conditions were met, then the law states that a "digitally signed document is as valid as if it had been written on paper."[96]

Electronic signature legislation has also been based on the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (the "Model Law"). The Model Law was created in 1996 to provide a template for countries to harmonize and unify international trade law with respect to the use of electronic commerce. The Model Law recommends a number of provisions for the treatment of non-paper-based communication and storage of information, including the use of electronic signatures. Specifically, with regards to electronic signatures, the Model Law provides technology-neutral language that allows for much flexibility in its interpretation. As defined by the Model Law, an electronic signature is considered valid when two conditions are met: 1) the method to electronically sign a message can be used to identify the signer and indicate that the signer approved the information in the message; and 2) the method used "is as reliable as was appropriate for the purpose for which the data message was generated or communicated."[97] Such flexibility allows businesses to use the electronic signature technology most appropriate to their particular business needs and the security level appropriate for any given transaction.

Provisions of the Model Law were adopted in many countries, although a smaller subset adopted the provisions relating to electronic signatures. These countries include Australia, China, France, Mexico, New Zealand, Singapore, Slovenia and South Korea. The principles outlined in the Model Law are also reflected in U.S. law as well as the Uniform Electronic Commerce Act adopted in 1999 by Canada.[98]

In the United States, two legal acts provide the legal framework for electronic signatures: the Electronic Signatures in Global and National Commerce (ESIGN) Act and the Uniform Electronic Transactions Act (UETA). The U.S. Congress passed ESIGN in 2000 to facilitate the use of electronic records and electronic signatures in interstate and foreign commerce. The National Conference of Commissioners on Uniform State Laws created UETA as model legal framework for states to support the use of electronic signatures. It has since been adopted by forty-seven states, the District of Columbia, Puerto Rico, and the Virgin Islands. Three states, Illinois, New York and Washington, have not adopted UETA but have adopted other legislation relating to electronic signatures.[99]

Neither EISGN nor UETA mandated the use of electronic signatures; instead they eliminated potential restrictions on the use of electronic contracts, records or agreements, such as requirements that a document have a stamp, seal or be embossed to be valid if an equivalent assurance could be provided by electronic means. For example, ESIGN states that "a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation."[100] In addition, neither act mandates a specific technology; both give parties the freedom to determine the most appropriate technology for their transactions.

European countries have worked to standardize legislation on e-signatures. In 1997, the European Commission released a forward-looking document, "A European Initiative in Electronic Commerce," calling for a regulatory framework that would engender trust and confidence in electronic commerce, including the use of digital signatures and digital certificates for signing messages and authenticating users to services.[101] The report noted that the current mix of laws was creating barriers to cross-border transactions among European nations. As the report stated, "A number of Member States' rules governing the formation and the performance of contracts are not appropriate for an electronic commerce environment and are generating uncertainties relating to the validity and enforceability of electronic contracts."[102] To remedy this, the EC recommended creating a standard framework for digital signatures. The report set a goal of "ensuring a common legal framework encompassing the legal recognition of digital signatures in the Single Market and the setting up of minimum criteria for certification authorities. Worldwide agreements on digital signatures will also be needed."[103]

In response, in December 13, 1999, the European Parliament and Council adopted Directive 1999/93/EC on a Community framework for electronic signatures.[104] The Directive set out to harmonize definitions and rules for electronic signatures, digital certificates, and related technology in member countries. The guidelines specified a special class of electronic signatures termed "advanced electronic signatures" that would receive the same legal recognition in relation to electronic data that handwritten signatures have in relation to data on paper. In addition, the Directive specified rules governing the creation of digital certificates and certificate authorities to ensure consistent treatment across EU countries. Finally, the Directive specified that certificate authorities are liable for damages caused to an entity that reasonably relies on the accuracy of the data.

A European Commission report on the status of the Directive in 2006 found that "all 25 EU Member States have now implemented the general principles of the Directive."[105] The report noted that uses of advanced electronic signatures has had "a very slow take up," but that simpler types of e-signatures, such as one-time passwords and tokens, used by e-banking and e-government services, are much more prevalent.[106] The report identified a number of factors for the low rate of adoption of advanced e-signatures, including liability issues for service providers. Because of liability concerns, service providers show little interest in providing digital certificates to be used for other services. In addition, the use of PKI technology has created some interoperability obstacles limiting the use of a single technology across borders or by different applications.

More recently, the European Commission has launched an "Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market."[107] This plan implements a number of recommendations from the Cross-Border Interoperability of eSignatures (CROBIES) study initiated by the European Commission. These recommendations included creating a trusted list of certificate service providers (i.e. certificate authorities), creating an e-signature validation service at the EU level, and having the European Committee for Standardization (CEN) update standards for e-signatures to create a framework.[108] Moreover, it noted that "the means of e-identification have been deployed without coordination between Member States" and the need to address interoperability to avoid building technical, legal and organizational barriers between solutions in different countries.[109]

In March 2010, the European Commission launched the Europe 2020 Strategy, a ten-year economic plan for the EU economy. Among seven principle initiatives in the Europe 2020 Strategy is the Digital Agenda for Europe (DAE). DAE proposes specific actions to reduce barriers to cross-border online services, including revising the eSignature Directive and adopting a Directive on e-IDs.[110]

Outside of Europe, many countries have passed similar legislation. Malaysia passed the Digital Signature Act (DSA) in 1997 as part of a broader set of legislative initiatives created to make Malaysia an attractive destination for investment by information technology companies.[111] The DSA is modeled after the Utah Act and provides a framework for the licensing of certification authorities to provide digital signatures. Specifically, the DSA outlines the steps to become a licensed certification authority, the duties and responsibilities of certification authorities, and the requirements for users of digital signatures. Also included in the legislation is clarification on issues such as the legal recognition of digital signatures, the liability of certification authorities, and the use of time stamps. Although the legislation confers the legal status of handwritten signatures to electronic signatures, absent from the DSA is any requirement that electronic records or contracts be treated the same as paper records or contracts. This means that some legal requirements, such as record keeping requirements, may not be satisfied using electronic records.

Singapore enacted the Electronic Transaction Act (ETA) in 1998. In contrast to the Malaysia DSA, the Singapore ETA more closely follows the UNCITRAL Model Law. In addition to provisions to facilitate the use of electronic signatures, the ETA establishes uniform rules and standards to facilitate electronic commerce and the exchange of electronic records. For example, the ETA clarifies that electronic communication can be used to create contracts and establishes various rules to define legally to whom an electronic message should be attributed and how receipt of electronic messages should be confirmed.

Although many countries have e-signature laws now, better standardization between nations is still necessary to achieve seamless cross-border interoperability.

Cultural and Historical Factors

Various cultural and historical elements play a role in the evolution of e-ID systems in countries. For example, in countries with a history of national ID cards and the use of central population registers, the population may be more accepting of e-ID systems that extend on existing functionality. Moreover, the organizational structure may also be in place to deploy an e-ID system, which may make deployment easier. For example, prior to the rollout of its e-ID system, Belgium had developed a robust identity infrastructure including a national register, personal identifiers, and a national ID card. Belgium already had a compulsory national ID system in place before its e-ID was developed, and had issued ID cards since 1919.[112] All individuals age twelve and older must carry their ID cards at all times. Thus, cultural attitudes about a national e-ID, as a replacement to the existing compulsory national ID card, were not fraught with the same political angst found in other countries.

In other countries the political hostilities to a national ID system have been a barrier to creating more secure ID systems. For example, many individuals in the United States have resisted improvements in the ID system even at the state level. The resistance to the REAL ID Act in the United States is emblematic of these difficulties. Similarly, other countries, including Australia, Canada, New Zealand, and the United Kingdom, have all flirted with national ID and electronic ID systems but none of these have come to fruition.

However, other countries where citizens harbor distrust of national ID policies have begun implementing e-ID systems. For example, in the Netherlands, resistance to centralized government databases and government collection of personal information was so great that a decennial census was cancelled in 1980 due to opposition.[113] Similarly, in France, internal resistance to ID efforts is tied, at least in part, to historical factors such as the use of ID systems to control the population during the Vichy regime, including the use of national identifiers, central databases to track internal movement, and the collection of personal information such as religion.[114] Germans also have a strong reluctance to the creation of national ID databases because of past abuses; however, most carry an ID card.[115] In contrast, Spain has introduced an e-ID system without much resistance even though Spanish ID cards were first introduced in 1944 by General Franco to monitor the population, maintain civil obedience, and repress political dissidents.[116] Similarly, Italians have been generally accepting of ID cards, even though they were introduced under Mussolini. However, some citizens have objected to certain elements of ID cards, such as the use of fingerprints, because of the perception that this is used for criminals.[117]

Country Demographics

Judging from the list of successfully deployed e-ID systems, it is evident that the leaders are predominantly countries like Estonia with smaller populations. In addition, these countries generally embrace information technology, have above-average broadband rankings, and have forward-thinking e-government strategies. Arguably, a small country may be more nimble in its policymaking. For example, a small country with a homogenous population may not face the same political resistance when proposing new technology projects that would be found in a more politically divided nation. However, small countries are not necessarily at an advantage. Their IT systems generally have higher fixed costs and lower

marginal costs. Thus, large countries like the United States should expect to be able to build an e-ID system at a lower average cost per user than smaller countries. Indeed, as noted earlier, the world's two most populous countries—China and India—are both investing in IT for their respective ID projects. The countries in the lead generally also score high on having a digitally literate population. Digitally illiterate populations could pose a barrier to high levels of use of an e-ID.

National Registries

As shown in Table 3, many countries use national population registers to maintain citizen information. Population registers may be maintained centrally or at the local level, as in Germany and Japan. Many European countries use central population registers. For example, Sweden has used a national population register since the seventeenth century. Originally managed by the Church of Sweden, the National Tax Agency took over in 1991. The population register contains various information about residents including: name, personal ID number, address of residence, marital status, partner, children, parents, guardian, place of birth, residence at birth, adoption, citizenship, and status change due to emigration or death.

Country	Type of Population Register
Austria	Central
Belgium	Central
Denmark	Central
Estonia	Central
Finland	Central
Germany	Local
Japan	Local
Luxembourg	Central
Norway	Central
Poland	Central
Slovak Republic	Central
Spain	Central
Sweden	Central
Turkey	Central
United Kingdom	Central

Table 3: Type of population register, select countries

National Identification Card

Many countries have some form of a national identification card. Even in those countries without national ID cards, the government still provides documentation such as birth certificates to help establish an individual's identity. In countries with a national ID card, obtaining the card may be compulsory. Some nations with compulsory national ID cards also require citizens to carry the card at all times. For example in Greece, not only are ID cards mandatory, carrying them is also compulsory.[118] Not all nations with national ID cards have this requirement. For example, Germany has a mandatory ID card; however, carrying the card is not compulsory.[119] ID cards may also be compulsory for foreigners, such as in Spain.[120]

The absence or presence of a compulsory national identification card is an important policy factor influencing the diffusion of e-IDs. For many countries, a compulsory national ID card has been a standard practice for many years and poses few political or philosophical objections among politicians and citizens. In other nations, such as the United States and the United Kingdom, the idea of a national ID system may be anathema to ideas of privacy for some civil libertarians. Where the use of a national ID is already commonplace, the transition to an e-ID has met less resistance, as an e-ID is generally more resistant to forgery and implements additional functionality.

Compulsory use of a national ID that serves as an e-ID also means that the take-up rate of an e-ID can be much higher. Faster take-up means that government can more quickly begin to start reaping the benefits of an e-ID system, such as more efficient citizen-government interactions. This faster return on investment means that these governments have more of an incentive to invest in an e-ID program. Many of the benefits from e-IDs come from positive network effects and thus the benefits grow as the number of users increases. To illustrate the network effect, consider email, where the value of email service to each user increases with the number of users. The same is true for applications like secure email, which require digital certificates; again, the value of the application increases as more users gain access.

Many nations have made their national e-ID card mandatory, including Belgium and Estonia. Belgium's e-ID replaced the existing national ID card, and is likewise compulsory for individuals age twelve and older. As a result, the organizational capacity to issue and deliver e-ID cards already existed.[121] In addition, since 1996 all citizens, regardless of age, have had a social security card (SIS-card) to access social security services. The use of the SIS-card also helped facilitate the eventual deployment of the e-ID system since it meant that individuals and institutions were familiar with card technology.[122]

Some countries where the card is not obligatory have still turned to government mandates to help speed adoption. In UAE, for example, the government passed a resolution that prohibited recruiting or hiring any UAE national or resident that did not possess an e-ID card.[123] While such programs have been criticized by some scholars as introducing another dimension to the digital divide by creating an "ID divide" the effectiveness of such an approach in encouraging e-ID use is evident.[124]

The lack of a national ID card can also be seen as a factor in the development of an e-ID solution. For example Denmark, which has struggled to develop an e-ID solution for almost 20 years, is one of four countries in the European Union that does not have a national ID card system. The other three countries are Ireland, Latvia and Lithuania.[125] While some countries have rejected national ID cards in the past, they should recognize that technology is changing the cost/benefit equation. Forgoing the creation of a national e-ID, and related systems like national registries, imposes a not inconsequential cost on countries by limiting the type and quantity of applications and services available to citizens.

Organizational Issues

The Degree of Centralization or Decentralization

Various aspects of e-ID systems are implemented at either the national or local level. Some components may be more efficient to implement and manage at the national level, while others may be better left to local government. Various countries approach this issue differently. For example, Denmark's e-government strategy is to allow implementation of solutions at the local level while using common standards and frameworks where necessary to simplify legal, organizational and technical issues.[126] In Germany, the Federal Data Protection Law, which is designed to protect privacy, does not allow the government to create a centralized database of biometric information. Instead, biometric information is stored only on identity cards and passports.[127] In addition, German e-ID cards are issued by local government authorities.[128]

In some countries, such as France and the United States, citizens resist the idea of centralized government databases of personal information and instead use decentralized databases for different sectors or regions. Decentralization can sometimes have a negative impact. For example, although the e-ID system in Belgium is managed at the national level, many of the government services that would be most likely to take advantage of e-IDs are at the local level. As a result of this disconnect, development of e-government services that use the e-IDs has been somewhat sporadic and uncoordinated. For example, some services will be available to only certain regions or to individuals speaking a certain language.

Entity Leading the Design and Implementation

The design and implement of an e-ID system is shaped by the government entity leading the development. The mission and objective of the agency can influence the outcome. This can be seen in Sweden, which has multiple identity providers and identity documents. The Swedish e-ID strategy was motivated by a desire to create secure e-government services. In contrast, the NIDEL identity card issued by the police in Sweden was created to provide an identity document for the Schengen Treaty and does not contain an e-ID certificate.[129]

The government entity leading the development of the Swedish e-ID system has changed over the years. Currently, the Swedish Tax Authority, also responsible for the national population register, centrally manages the e-ID system. The Ministry of Finance is the principal policymaking organization.[130] Notably, the Tax Agency and the Social Insurance Agency—the two principal entities utilizing e-IDs for government services—have been

actively shaping e-ID governance.[131] Strong buy in from the principal government agencies that would utilize the e-ID system has likely contributed to its relative success.

Similarly, the population that is served by the e-ID system may be influenced by the leading agency. The Swedish Tax Authority e-ID card is available not only to Swedish citizens, but also to people under the age of eighteen and non-Swedish citizens.[132]

Policy Issues
Replacement of Existing ID Cards
Some countries have created a new and distinct e-ID system; others have added electronic identification and authentication functionality to an existing ID card. For example, in Sweden, Belgium and Estonia e-ID cards replaced previously-issued paper ID cards. In Belgium, although the e-ID card did replace the national ID card, the e-ID card did not replace the social security card (SIS-card) or the driver's licenses for political reasons.[133] When e-IDs are replacing existing ID cards, the length of time that the older ID cards were valid can influence the adoption time table. For example, in Germany the existing ID card is valid for ten years so it will take up to a decade before all citizens who are required to have a national ID obtain the new e-ID.[134] Other countries have created an entirely new ID system. For example, the Austrian e-ID did not replace any existing identification.

Government Programs to Spur Demand and Increase Use
Issuing e-IDs to citizens and residents is only one step towards creating a robust national system for electronic identity management. Many nations have also adopted demand-side policies to spur faster adoption and more use of e-IDs. For the most part this has meant investment in e-government initiatives that use e-IDs to make interacting with government more citizen-friendly and efficient as in filing taxes, obtaining government benefits, signing government documents, making payments, and paying for public transportation. Estonia has perhaps been the most innovative and has used the e-ID to allow citizens to vote online. For those countries that also use the e-ID as a travel document, it can involve creating new services, such as automated "e-Gates" at border crossings and at airports, offering citizens more convenience as an enticement to adopt e-IDs. In some European countries such as Estonia and Finland, the e-ID also serves as a valid identity document for travel within the Schengen Area.

Many countries also have programs to broadly increase adoption and use of digital technology. For example, between 2002 and 2006, the European Commission had the eTEN Programme to implement electronic services across various domains including government, health, and education.[135] The European Commission Directive on e-signatures was not intended to directly create demand for e-IDs, but rather to create a platform to build digital services. However, other regulations have had a more direct impact on demand. The Directive 2001/115/EC specified that invoices could be sent and stored electronically, rather than on paper, if qualified electronic signatures were used. Similarly, the Directive 2004/18/EC established a framework for using e-signatures for public procurement. The Directive states that the "use of electronic signatures, in particular advanced electronic signatures, should, as far as possible, be encouraged."[136] Likewise the

Commission Decision 2004/563 on electronic and digitized documents establishes that e-signatures, when necessary, will be used to determine the validity of documents.[137]

The lack of services in some countries can help explain lower than desired adoption rates. Sweden, for example, has fewer e-government services at the local level allowing the use of e-IDs. Of course, some government opportunities to utilize e-IDs have not come to fruition because of technical, legal or organizational barriers. For example, in Belgium plans to combine the e-ID card with other credentials such as the driver's license or the social security card have failed because of concerns about privacy or legal barriers.[138] Although proposals were made to use the Belgian e-ID for services like electronic voting and registering a child's birth, these were ultimately not pursued because of political objections.[139]

In the absence of a national electronic ID system, businesses and government have created a wide range of solutions that provide various levels of identification and authentication. Alternative systems that provide similar functionality to e-ID systems may reduce the adoption and use rate of e-IDs. For example, in Belgium many users still opt to use a one-time password provided as an alternative to the e-ID to file their taxes.[140] In the United States the Internal Revenue Service (IRS) allows taxpayers to create a PIN to sign their tax returns when filing electronically and verify their identity using information from the previous year's tax return.[141] In the commercial space, many different service providers in the United States have sought to provide users various types of online identity solutions; however, no solution provides users a seamless online experience. Companies have introduced products that provide some of the features of a robust online identity solution, yet without widespread interoperability, none of these products has achieved widespread adoption by the average consumer.

In countries that lack an e-ID system, various means are used to authenticate the identity of individuals. For example, passcodes may be sent to the mailing address of an individual or businesses may ask individuals to verify personal information known about them by a third-party, such as a credit bureau. However, these types of systems can be inefficient, expensive and error-prone. Some countries have even created specific mechanisms to remotely verify the identity of a person. For example, in Germany the German postal service offers the Postident service to businesses that want in-person verification of an individual's identity. Individuals can have their identity verified in person either by presenting ID to a mail carrier or by presenting it to an agent at a post office.[142]

Public or Private Solution
When implementing a national electronic identity solution, whether it is a national electronic ID card or a PKI system, policymakers must choose the degree to which the solution is provided by the public sector or the private sector. Most e-ID systems have both public and private-sector elements. For example, in Austria both public and private organizations can be identity providers. The development of the card standard, however, was led by both federal government staff responsible for implementing a national e-government strategy and by the Secure Information Technology Center – Austria ("A-

SIT"), a non-profit organization consisting of public institutions focused on developing information security competencies.[143]

On one end of the spectrum you can have a solution mostly run by the private sector. For example, in Norway many citizens use the Norwegian BankID Scheme delivered by the Banking and Business Solutions (BBS), a coalition of private-sector banks. The banks manage the overall e-ID system, develop the technical standards, manage all operations, including verifying an individual's identity and issuing credentials, and provide the digital certificates. An over reliance on the private sector can have drawbacks if solutions are not properly implemented. For example, critics of BankID note that its security protocols are opaque, thus preventing public review.[144] In addition, liability rules need to be established to deal with misuse. In Norway, for example, individuals generally have primary liability for fraud or abuse of their e-IDs.[145] However, banks also share some financial responsibility for misuse unless the individual acted negligently.

In comparison, the Swedish e-ID system has largely been led by the government, but implemented by the private sector. Costs were a factor in this decision. The Swedish government pursued a market-based approach for the e-ID system both to use competition to lower total costs and to shift the implementation foundation costs from the government to the private sector.[146] Policymakers also wanted to leverage the private-sector identity infrastructure that was already in place at the banks.

The public sector is typically involved in e-ID governance, such as developing and implementing the legal, organizational and technical framework and standards. All e-ID systems have private-sector involvement because the contracts to run key elements of the project typically go to private-sector companies. Examples include production of e-ID tokens (if applicable) and development of technical infrastructure. The private sector may also be involved in running the certificate authority and issuing the credentials, although the public sector may take on this role. The German national e-ID card, for example, allows citizens the option of activating the signature function on the e-ID for a fee. To activate this function, the citizen must use a private-sector certification authority.[147] In some countries, private-sector certificate authorities may be able to set their own fee schedule. Digital certificates are valid for a fixed length of time (e.g., three years) unless revoked by the certificate authority (e.g., because the private key to the certificate is compromised).

The private sector is also an important stakeholder because it will produce many of the electronic services that will make the e-ID either a success or failure. Many private-sector industries, including banking, utilities, telecommunications, health care and retail, can use e-IDs to better offer services to their customers online. The difference between Estonia and Belgium provides a good example of how private-sector engagement can help promote use of e-IDs. In Belgium, the private sector has been slow to develop services that take advantage of the e-ID. This is at least partially because of strict privacy rules and the slow deployment of the cards, which only recently became universal. In contrast, the private sector's active role in creating services that use e-IDs has been instrumental to the success of

the e-ID system in Estonia. In particular, the banks and telecom operators have heavily promoted the use of e-IDs to improve security and offer new services.[148]

In addition to being an identity provider by issuing e-IDs, the private sector also can be an attribute provider. An attribute provider links certain assertions to an individual's identity. In Spain before the deployment of the current e-ID card, various private-sector entities served as attribute providers by issuing software-based digital certificates containing both identity information and an assertion about the individual. For example, a Chamber of Commerce would issue a digital certificate certifying that an individual works for a particular firm, or a professional association would issue a digital certificate certifying that an individual is a licensed doctor.[149]

Technology Issues
Form of e-ID
As shown in the case studies, nations have used various technologies to deliver e-IDs. In general, countries choose among the following technologies: smartcards, mobile phones, one-time passwords, and software-based certificates on a PC. Smartcards are either contact or contactless cards. Contact cards are most prevalent in many European countries including Belgium, Estonia, Italy, Portugal and Spain. At least one country, the Netherlands, provides a contactless card, i.e. a card that uses radio frequency identification (RFID). Contactless cards are commonly used in the United States in credit cards, such as the Visa PayWave or MasterCard PayPass, to pay fares on some public transit systems, and for electronic toll-collection on toll roads, bridges and tunnels.

Policymakers should be aware of usability issues relating to different e-ID technologies. To use a smartcard for online transactions, such as logging in to a website or signing an electronic document, individuals would insert their e-ID card into a card reader connected to a computer and then enter a PIN or password to authorize the transaction. To use a smartcard at home, users need to have card readers on their PCs and the correct software installed on their PCs. To meet the needs of all users, the software must also be available for multiple operating systems. The cost of card readers can vary: in the United States, a typical USB card reader costs less than fifty dollars as of 2011. One reason for the slower adoption in Belgium is due to the complexity involved in using the e-ID cards. Many users did not have card readers, and those that did found that the necessary software was difficult to install and use. For example, the software initially lacked a one-click software installation or even an installation wizard. While this has been improved, using the signing capabilities on the card still requires some additional software configuration.[150]

Some countries provide only one type of e-ID whereas others offer multiple forms. Policymakers must decide whether to implement technology-neutral policies for e-ID systems. Policymakers typically must balance more flexible policies with a need for standardization for both the form and the technical requirements of each token or certificate. Austria exhibits perhaps one of the more technology neutral e-ID systems. Rather than limit e-IDs to a single government-issued form of identification, Austrians can use the e-ID functionality on the smartcard or device of their choosing (e.g., mobile phone

or PC). In Estonia as well an individual can use a mobile phone or a smartcard as an e-ID. Similarly, Sweden offers both a software certificate and a smartcard implementation.

Open Platform

Open platforms allow third parties to build on an existing solution. Some countries have built an e-ID for a specific purpose, such as to be used as a travel document for border control or to access e-government services. Other countries have built the e-ID system with the intent to create an identity service that can be used for multiple purposes in both the government and the private sector. Providing extensibility allows the e-ID to be used for more than one purpose and to evolve over time. Creating an e-ID with an open platform, i.e. a set of open standards others can build upon, allows developers to independently innovate and create new applications for users and to integrate e-IDs into various systems. This is particularly necessary to allow other entities to become attribute providers and provide data or credentials that e-ID users can share with other service providers.

Part of achieving an open platform involves creating a fully documented application programming interface (API) that developers can use to interact with the e-ID. This gives developers the technical information they need to design products and services that use an e-ID. In addition, some e-ID tokens, such as smartcards, have memory that can store application-specific data. Some countries that use cards for the e-ID, including Austria, Belgium, Finland, Italy and Portugal, allow application-specific data to be written to the e-ID. In contrast, the e-ID card specifications in other countries, including Estonia, Denmark, and the Netherlands do not have this functionality.[151] Allowing data to be written to the e-ID cards allows different applications to be created and used with the e-ID. For example Oman, which was one of the first Middle Eastern countries to launch an e-ID card, has used an open platform so that new applications and data can be developed for the card after it is issued to citizens.[152]

Use of Biometrics

Multi-factor authentication relies on the use of different types of information to authenticate a user. This includes what you have (e.g., a token), what you know (e.g., a password) and who you are (e.g., an iris scan). The use of biometric data can help increase the security of some transactions. Many ID systems, such as national IDs, passports, and driver's licenses, use biometric information such as fingerprints or photographs, to prevent an ID from being used by someone other than the owner. Not surprisingly, some e-ID systems have also begun to incorporate biometric data. Requiring the use of biometric data to complete a transaction adds an additional layer of security by linking the use of an e-ID to a specific individual. Examples of biometric data include fingerprints, palm prints, hand geometry, finger vein recognition, facial recognition and iris recognition. Adding biometrics to an e-ID requires both organizational and technological infrastructure for capturing the biometric data when enrolling users in the system. In addition, using biometrics with e-IDs can require additional technology, such as finger print readers.

One common objection to the use of biometric information is that an individual's biometric information, unlike a password, cannot be changed if it is ever compromised (e.g., a person cannot get new fingerprints). This is true. However, unlike a password, the

security from using biometric data does not come from its secrecy but rather from its uniqueness. This means that biometrics can help prevent someone from using another person's e-ID. For example, a person can share a PIN but cannot share a fingerprint. Biometric information is particularly useful when collected using secure hardware in a controlled environment to prevent attackers from spoofing (i.e., sending false) biometric data. Although masquerading attacks are plausible under many different conditions, biometrics can add another layer of security to e-ID systems.

Another objection is that biometric data may be used for purposes beyond the original intent, such as for governments or businesses to track individuals. As described in the section below on privacy, various technical and legal protections can mitigate these potential risks. While the privacy issues surrounding the use of biometric data can be overcome through a well-designed ID system, the potential objections from users about the inclusion of biometric data can serve as a barrier to their use. Belgium, for example, chose not to implement biometrics on the e-ID because of the costs and potential user backlash.[153]

Interoperability

Most of the efforts at establishing interoperable e-ID systems have occurred between EU member states. For example, the European Citizen Card sets a physical and technical standard for European ID cards. The European Commission also established the twenty million euro "Secure idenTity acrOss boRders linKed" (STORK) project in May 2008 to allow citizens in different countries to use their e-ID cards across borders. These efforts require that nations establish both technical and legal measures to ensure cross-border interoperability.[154]

Still, technical interoperability between various e-ID solutions is fairly minimal and users face interoperability challenges. Some countries face interoperability problems even within the country. For example, although Swedish e-IDs have a common technical structure, the exact implementation and interface for each type of e-ID varies. Interoperability problems increase the cost of adoption for service providers and decrease the value of adoption for users. When there are multiple standards, each relying party, such as a business or government agency, must make its systems work with each issuer or may choose not to accept all forms of e-IDs. Government standards can help eliminate these problems. To fix this issue in Sweden, the government is proposing to create a federated system with a common interface for both end users and relying parties.

Affordability of e-ID Card

Affordability is an important factor in achieving widespread adoption of e-IDs. Affordability is influenced by both the cost of the e-ID and the relative wealth of the population. Larger countries should benefit from economies of scale and see a lower average cost per person for e-IDs. Wealthier countries should also be more likely to create e-ID initiatives as the programs would be more affordable.

In Malaysia, the government issues citizens an e-ID card at no charge. Non-citizens who apply for the card can receive one for a payment of RM 40 (approximately 11 USD). Replacement cards are on a sliding scale based on the number of replacements, ranging

from RM 100 to a maximum of RM 300 (approximately 28 USD to 84 USD).[155] Some countries make the e-ID available at a price below cost. In Spain, for example, the government priced the e-ID card at approximately 6.80 euros in 2008, approximately a fourth of the cost of the card to the government.[156]

Other factors influence the lifetime cost of an e-ID to an individual. For example, some e-ID cards require an additional fee to install the digital certificates used for electronic authentication and signing. This fee may be paid to the government or a private-sector certificate authority. The total cost of the e-ID also depends on how frequently the e-ID must be renewed and the associated renewal fee. The length of validity of the e-ID may differ from the length of validity of the digital certificates. For example, in Spain the e-ID card is valid for five years for individuals under the age of thirty, ten years for those between age thirty and seventy, and does not expire for those above seventy. The digital certificate, however, is only valid for thirty months.[157]

Country	Cost (€)
Austria	57
Belgium	15
Estonia	10
Finland	40
Germany	8
Italy	20
Portugal	5
Slovenia	12
Spain	10
Turkey	2

Table 4: Approximate cost of e-ID, select countries[158]

In Sweden, the cost of an e-ID varies based on the implementation, with file-based e-IDs available at no cost to the user, and card-based e-IDs costing up to eighty euros. Similarly, in Spain software-based digital certificates for online authentication to e-government applications are issued for free by the Spanish Mint whereas the e-ID card is available for a fee.[159] Not surprisingly the level of adoption and use of software-based e-IDs in these two countries have been significantly greater than the use of card-based e-IDs. The affordability of the e-ID solution also depends on any required extras, such as card readers. One reason for the slower adoption of the Belgian e-ID is that the card readers were initially priced high. But they have come down in recent years. For example, at the early stages of deployment the cost of readers was approximately seventy euros compared to approximately ten euros in 2010. In contrast, Estonia has promoted the availability of

affordable card readers. Early on the government sold a card reader "starter package" for twenty euros and required government computers to have a card reader.[160]

Privacy

Privacy concerns are common with many applications of technology, especially those that involve personally identifiable information. Some privacy advocacy groups will oppose all efforts to build an e-ID system regardless of how well the system is designed. These groups fundamentally object to the government collecting and processing personal information and view this as an unjust intrusion of government into an individual's right to privacy.[161] The merits and demerits of this rather extreme view, which would oppose most mainstream government functions that depend on the use of personal information such as collecting income taxes, paying Social Security benefits, and providing Medicare, are beyond the scope of this report. Instead, this report will focus on privacy objections to the use of e-ID technology specifically.

Privacy advocates raise objections to the use of enhanced identification cards or national identification cards, citing potential threats to civil liberties, including increased monitoring and surveillance and a decrease in anonymous free speech. Certainly some of these objections are valid: totalitarian governments can and have used this type of technology to decrease personal freedom. However, technology does not dictate the values of a society. While totalitarian governments may have created national IDs, national IDs did not create totalitarian governments. As the experience of many countries has shown, free and democratic societies use national ID cards to make government more efficient and productive. Taken as a whole, the benefits of using technology to improve ID systems vastly outweigh the risks.

While many concerns are overblown, there are also many legitimate privacy threats that should be taken into account when designing a national e-ID system. For example, while handwritten signatures do not reveal much information about an individual, e-signatures often contain additional data other than just first and last name. This data, such as an address and date of birth, are often necessary to ensure that one "John Smith" cannot sign for another "John Smith." A well-designed e-ID system should enhance an individual's privacy and protect against known threats, including security attacks against the confidentiality, integrity or availability of the e-ID system. This also means that e-ID systems need strong security controls, such as ensuring robust e-ID registration procedures. Electronic ID systems can be designed to minimize the amount of data that is made available to a third party, but technologies and policies must support this goal.

Germany, for example, has a number of policies to protect individual privacy, particularly from abuses by government. Some of these policies limit the technology, for example, by prohibiting centralized databases of biometric information or allowing the use of pseudonyms for electronic transactions. Other policies limit the use of the data. For example, biometric information is allowed to be used only for identification and cannot be used to determine other information, such as race.[162] Other privacy risks can also be reduced with e-IDs. For example, the risk of privacy violations are significantly higher if an individual loses a username/password combination than if he or she loses an electronic ID

that cannot be used without a PIN number. Moreover, using a single e-ID can reduce the difficulty of maintaining multiple usernames and passwords for different services and improve security.

Other privacy activists object to e-IDs out of concern for identity theft. Using e-IDs can actually provide users more privacy than using traditional identification. The reason for this is that e-IDs can be programmed to provide yes or no responses to queries that reveal no more information than what was requested. For example, consider the amount of information divulged when a typical person goes into a liquor store to buy a bottle of wine. In the United States, many retailers would ask the customer for proof of age to determine if the customer is of the legal age to purchase alcohol. Typically, the customer would then provide a driver's license. The store owner would then be able to see a substantial amount of personal information about the customer including their name, date of birth, address, and maybe even whether or not that person is an organ donor. At a minimum, the store clerk would review the customer's date of birth. With an e-ID, the card could be programmed to return a simple yes or no response to the more precise question "Is this cardholder legally allowed to purchase alcohol?" For example, the German e-ID card is able to restrict data transfers to certain personal attributes, such as "over eighteen", to service providers depending on what information they are authorized to receive.[163] This avoids releasing unnecessary information and creates a more private transaction.

Still privacy concerns have derailed some efforts at deploying e-ID solutions. For example, in Denmark the Ministry of Finance, Ministry of Interior and the Local Government Denmark (an association of Danish municipalities) tried to create a single, multi-purpose e-ID card in the 1992 to replace the existing array of ID solutions (such as the driver's license and SIS-card), but their efforts were stalled by privacy concerns raised by policymakers in Parliament.[164] Eventually the ID functionality was postponed, and the OCES digital signature solution was developed instead. The current system avoided some of the more serious privacy objections by integrating civil society organizations into the development process.[165]

Privacy-Enhancing Policies
Many countries implement specific rules or policies that are aimed at reducing privacy threats, although these restrictions can impose other problems. These include policies such as data minimization, which requires organizations to limit the amount of data they collect, and data breach notification, which requires organizations to notify individuals if personally-identifiable information is compromised. Some countries have data handling policies that specifically prohibit linking various government databases that contain personally-identifiable information. For example in France, one government leader notes that because of specific restrictions on interconnected government records, France cannot create a universal identity card or use this card for health insurance purposes.[166] In contrast, Belgium adheres to an "ask once" principle for e-government, which seeks to eliminate requiring individuals to submit information multiple times to government agencies. Instead, a single agency becomes the primary source of data. For this method to work effectively, data on individuals in government databases must be accessible by a common identifier. In Belgium, the personal ID number (RRN) is principally used for this purpose.

A different mechanism is used in Austria. Here each citizen card contains a unique identifier associated with the individual's identity in the Central Register of Residents. To eliminate linkages between personal data stored in different databases, this number is not used in transactions. Instead, a derivation of this number is created, known as the sector-specific personal identifier (ssPIN), to help protect personal information.[167]

Broadly speaking, Belgium has a relatively strict privacy framework for personal data. The Belgian Privacy Commission maintains strict control over the use of personal information in both the public and private sector. For example, any use of the personal ID number (RRN) must be approved by the Privacy Commission. In part, this is because the RRN reveals personal information (age and gender). Since the e-ID contains the RRN automatically, all uses of the e-ID must be approved by the Privacy Commission. The impact of these strict privacy controls has been, in the words of one study on the Belgian e-ID system, that the "necessary effort is considered too high compared to the return on investment."[168]

The technical configuration of an e-ID system can also determine what entities have access to sensitive transactional information. For example, Swedish e-ID providers currently use their own certificate authority, rather than a national certificate authority. Having a central, government-run CA can provide standardized security across all providers, although standardized security requirements could effectively achieve the same outcome. One policy lever that government can use to require stronger privacy policies is to make CA accreditation dependent on meeting certain privacy requirements.

Privacy-Enhancing Technologies

A variety of technologies can be used to reduce the risk of privacy of threats to users of e-IDs including encryption, access control, unique identifiers, and "verify-only" modes for credentials and biometric information.[169]

Encryption

Encryption can be used to secure the data stored on an e-ID token, data in transit, and data stored by a third party, such as a central government database. Countries can encrypt personal information stored on an e-ID token to protect the data from misuse; however, many countries leave data stored on e-IDs unencrypted (much the same way that data printed on ID cards are unencrypted). The data on an e-ID card, for example, might only be decrypted if the user supplies a PIN code or the data may only be decrypted by entities with a valid key from government authorities. Many countries, as shown in Table 5, encrypt data in transmission.

Country	Encrypt Stored Data on Cards	Encrypt Transmitted Data
Austria	No	Yes
Belgium	No	Yes
Estonia	No	Yes

Finland	No	Yes
Germany	No	Yes
Italy	No	Yes
Netherlands	No	Yes
Portugal	No	Yes
Spain	No	Yes
Sweden	No	Yes

Table 5: Privacy-enhancing encryption features, select countries[170]

Access Control

One way to control the release of information is to require that individuals enter a PIN to authorize any data transfer from an e-ID card. Access-control technology can also limit who can access data in an e-ID. Access control can be used to limit access to both encrypted data and non-encrypted data (i.e., plaintext). For example, data may be stored on an e-ID card in plaintext, but only authorized users can access the card either with permission from the e-ID governing entity, the user, or both. Other data may be available to anyone who has possession of the card. Currently many European countries, including Austria, Belgium, Estonia, Finland, Germany, Italy, Portugal and Spain all provide PIN-based access control to aspects of the e-ID card.[171] Many countries, however, make access to basic personal information (e.g., name and address) available to anyone with possession of the e-ID.

Many countries combine different access-control restrictions for different types of data. For example, the Turkish e-ID technical specification allows basic personal information to be read from the card without authorization. An individual's JPEG photograph, however, can only be accessed with a PIN. Finally, a secure card access device, which requires the card and card reader to mutually authenticate each other, is required to read biometric fingerprint information.[172] For example, some data on the Spanish e-ID card can be accessed only from special e-ID readers located in police stations that can match a person's fingerprints to the e-ID card.[173]

Combining encryption with access control can ensure, for example, that both a user and a service mutually authenticate identities before allowing the exchange of personal information. To improve the security of a two-party online transaction, both parties should have confidence about the identity of the other entity. As noted by Herbert Kubicek and Torsten Noack, two scholars who have studied e-ID systems, many of the European e-ID systems have primarily benefited the government or private sector by increasing the security of the identity of the consumer.[174] However, consumers do not gain additional information unless the identity of the government or private-sector party is similarly enhanced. Germany is an exception to this rule. German law requires that before an individual transmits information from his or her e-ID card, the service provider must first transmit a valid authorization certificate with information about the service provider. This "double-

sided, mutual authentication" is a unique innovation to the German e-ID. This certificate both provides proof of identity for the service provider and is evidence that the service provider has met data privacy and security requirements set out by the government which, for example, prevents using the data for illegitimate business purposes.[175] Authorization certificates are revoked if personal data is misused.

Unique Identifiers

Unique identifiers are used in various contexts to distinguish between like-items, including cards, devices, services, and individuals. Currently individuals use government-issued unique identifiers in various contexts. For example, in the United States individuals may use a Social Security Number, passport number or driver's license number as a unique identifier. Problems can arise, however, when these unique identifiers are misused or reused for purposes beyond their initial design. For example, in the United States a Social Security Number is often used outside of its original purpose for linking individuals to their tax records and government benefits. Additionally, it is used to authenticate the identity of an individual. Misuse of Social Security Numbers is one of the major causes of identity theft.[176] This type of use is a problem when the Social Security Number is also routinely shared and used as a unique identifier in non-government databases. Similarly, Sweden has issued personal ID numbers for use in both public and private records since 1974.[177] In contrast, the Belgian Privacy Commissions promotes a data minimization principle such that all uses of personal data must be justified. In practice this means that few private-sector organizations use the Belgian personal ID number (RRN).[178]

A unique identifier can protect user privacy. In Austria, citizens have resisted the idea of using a single unique identifier in government databases. Instead, citizens use multiple, sector-specific unique identifiers generated from the unique identifier on their ID card. For example, the identifier used for tax purposes is different than the one used for health services. Use of different sector-specific identifiers prevents information in one government agency from being linked to information in another.[179]

Some unique identifiers reveal personal information. For example, a unique identifier may include a person's date of birth. This is the case in Sweden where the personal identification number used widely by government and the private sector consists of digits representing an individual's date of birth, geographic region, and sex.[180] Similarly, in Denmark, the personal identity number (CPR) contains ten digits: six to represent date of birth, three random digits, and one digit for gender.[181]

In Estonia and Sweden, the e-IDs use the national register number as a unique identifier; in Finland, the e-ID uses a unique identifier derived from the Social Security Number. Users of the German e-ID card can also create a pseudonym for each unique service that allows the individual to avoid transferring certain personal data. Unique identifiers used with e-IDs can be designed to be unique to a specific application (e.g., a website) or a specific industry or sector (e.g., a health care identifier). To preserve the privacy of the user, different unique identifiers used in different contexts or systems for the same person can be designed so that they cannot be linked together even by colluding third parties or so that they can be linked together only by a trusted authority. Policies and practices surrounding

the use of unique identifiers can also contribute to privacy for individuals. For example, the data minimization privacy principle would suggest that unique identifiers should be used only when required, and not when other information is sufficient.

Verification of Credentials and Biometrics

One way that e-ID systems can protect user privacy is by providing verification of information for service providers rather than providing the actual information. The most common example of this is verification that an individual meets certain criteria, such as being over a certain age. Rather than provide a specific age or date of birth, the e-ID system just provides a true or false response. Similar features can be provided for other data or credentials. In particular, a form of verification can be used for biometric information to reduce the collection and distribution of this sensitive personal data. For example, rather than storing a scanned image of a digital finger print, an e-ID card might just save certain key elements of the finger print that allow the system to positively identify an individual.[182] In addition, this information may be stored only on the e-ID, rather than in a government or private-sector database. Various policies, some enforceable through technology, can also reduce the misuse of biometric data. Within the e-ID system, for example, software controls can restrict access to biometric data to those service providers with government authorization who have obtained user consent. More broadly, privacy legislation can prohibit government and businesses from collecting or using biometric data without an individual's consent.

Authentication Protocol

Authentication is used to determine the identity of a user. Many European e-ID systems use a digital signature application to provide authentication. While using digital signatures provides an effective means of authentication, doing so generates digital evidence of the authentication event that can be verified by a third party. As explained by the European Network and Information Security Agency, this is like the difference in the physical world between "*leaving* a witness-signed *copy* of a photograph as opposed to simply *showing* it to someone to identify oneself without that person recording any data from the photograph with signature" (emphasis in original text).[183]

RECOMMENDATIONS FOR THE UNITED STATES

As shown in this report, the policies and technologies used to create an e-ID system in a country can have a dramatic impact on outcomes. While demographic, cultural and historical factors may influence a country's national e-ID strategy, and existing ID infrastructure such as national registries may make deployment easier, all countries appear able to take advantage of this technology. Although the United States is late in creating a national e-ID strategy, if it heeds the lessons from early adopters it can capitalize on an enormous opportunity to create an e-ID system that can leapfrog those of other countries and help invigorate our information economy.

As detailed below, policymakers should do the following:

- Create an e-ID implementation plan with broad input from all stakeholders, including the private sector

- Build an e-ID framework that supports both current and emerging technologies

- Use government to increase both supply and demand for e-IDs

- Design an e-ID solution that maximizes utility for both users and service providers

- Ensure that privacy does not come at the expense of eliminating useful information from the information economy

- Strive for disruptive innovation, not just incremental innovation

- Ensure that e-ID solutions are accessible and available to all individuals

- Design an e-ID system for the global digital economy

Achieving this will require a forward-thinking approach to e-ID systems that balances competing interests and addresses privacy concerns, while also embracing an innovation-driven framework that combines the strengths of both the public and private sector.

Create an e-ID implementation plan with broad input from all stakeholders, including the private sector

The NSTIC rightly describes the U.S. government's goal as creating not just an e-ID system, but an entire identity ecosystem involving a variety of legal, organizational and technological factors. The identity ecosystem consists of multiple stakeholders including users, identity providers and service providers from both the public and private sector. The NSTIC provides a high-level description of the policy goal, but the U.S. government has not yet created an implementation plan to achieve rapid adoption and use. Creating an implementation plan for e-IDs in the United States should be a top priority and all stakeholders should be involved in the discussion.

The government cannot build a successful national e-ID system without broad support from the private sector. As described above, most countries involve the private sector to varying degrees. The countries with the most widespread use generally have both public and private-sector applications utilizing the e-ID system and virtually every country uses the private sector to operate a portion of the e-ID infrastructure. The private sector can serve both as an identity provider and as an attribute provider. In addition, the private sector has many resources that can be built on and is the current supplier of much of the identity infrastructure, such as certificate authorities, that will be used. For example, companies like Facebook, Google, and Microsoft already provide single-sign-on capabilities for their users and provide a platform so that third parties can use this online authentication service too. In addition, some businesses, such as financial institutions, telecommunication service providers, and utilities, already have existing mechanisms in place to verify an individual's identity online or in person. Experian, to take one example, provides online identity verification services to facilitate customer interaction on the Internet. Leveraging existing elements in our current identity ecosystem, such as the large number of individuals who use online banking, may help speed deployment. These tools

and experiences should be integrated into a common set of best practices as we build the future identity ecosystem.

The government agency leading the development of the e-ID should also include other government stakeholders, at the federal, state and local levels. For example, although the NSTIC is appropriately placed within the Department of Commerce, as explained earlier, building better electronic identity systems has been identified as a key priority for improving cybersecurity domestically and building better e-government services. This will involve coordination with the Department of Homeland Security as well as with other agencies that interface frequently with citizens such as the Social Security Administration and the Internal Revenue Service. It may also require the involvement of other government entities such as the U.S. Postal Service or state-run Department of Motor Vehicles for the secure delivery of e-ID tokens and identity proofing. Various stakeholders will have competing interests and while no one agency's narrow interests should trump greater societal goals, the needs of different stakeholders should be accounted for.

Build an e-ID framework that supports both current and emerging technologies

The government should not specify any particular technology for e-IDs but rather establish a technology-neutral e-ID framework that allows both public and private-sector identity providers to issue e-IDs using the technology of their choice. This means that the government should not require that e-IDs be implemented, for example, on smartcards, but instead should define broad functional requirements for the e-IDs. The private sector can then propose various solutions that meet these requirements. For example, providers of existing smartcard systems, including those used for financial services, health care services, corporate and government networks and facilities, and mass transit, can potentially offer an e-ID using these smartcards. In addition, if policymakers create a flexible framework that supports multiple technologies, then identity providers will also be able to provide citizens with e-ID using other technology, such as mobile e-IDs. Countries such as Austria that have not created a single national token, such as a smartcard, but rather have established a framework for e-IDs, offer citizens more options for obtaining an e-ID.

This does not mean that the government should leave all implementation details to the private sector. The government should maintain sufficient oversight of private-sector implementations to promote competition, choice and innovation in the identity ecosystem. For example, the government should ensure that private-sector identity providers use open protocols and interoperable standards to avoid vendor lock-in. Using open protocols will also ensure transparency for technical standards, thereby helping to promote trust by users and relying parties. Government should also establish identity proofing standards that certified identify providers will use to issue e-IDs. Finally, government should remember that the identity ecosystem extends beyond individuals and should encompass a variety of entities including organizations, systems, and devices.

Use government to increase both supply and demand for e-IDs

While there are clear potential benefits from an e-ID system, in the absence of a killer app, the benefits may not be immediately available to users or service providers. A key reason is because technologies like e-ID systems exhibit strong network effects whereby the value of

the technology grows as the number of users increase. A critical mass is needed to create the right value proposition for private-sector service providers to rely on the technology; without that critical mass, systems that accept e-IDs will not develop. Government, at the federal, state and local level, should invest in the identity ecosystem to overcome this "chicken-or-egg" problem inherent in its creation. The countries that are further ahead in e-ID adoption and use have aggressively invested in e-ID technology in advance of market demand for the technology; the most successful countries have also coupled these investments with demand-side programs to spur use of the technology. Therefore, the U.S. government needs to not only act as a convener and facilitator for private-sector development of e-ID systems, but also take specific actions to boost both supply and demand.

On the supply side, government should be both an identity provider and an attribute provider. Identity providers issue e-IDs to users. As a first and easy step, government agencies should make changes so that future personal identity verification (PIV) cards issued to government employees and contractors, such as the common access card (CAC) issued by the Department of Defense, include digital certificates for online authentication and electronic signatures that can be used in the private sector. Equipping the more than 2 million federal employees and 8.2 million state and local government employees will help bootstrap use of e-ID technology throughout the nation.[184]

Second, to ensure that any individual in the United States who wants an e-ID can obtain one, at least one federal government agency should commit to begin offering e-IDs within one year of the approval of a standard. This e-ID should be available to any U.S. resident upon request for a reasonable fee. The agency issuing the e-ID could build on existing systems and processes already in place to issue physical IDs. For example, both the Department of State and the Department of Homeland Security already have identity proofing processes in place for issuing identification documents (e.g., passports and frequent traveler cards). The e-ID would not need to use an existing token, such as a passport, but could instead be offered as a new token, such as a smartcard or software certificate for a PC or mobile phone. The issuing agency could use a variety of methods to securely deliver the physical token or activation code to the user, including face-to-face at a local government office, such as a U.S. Post Office, Social Security office or Department of Motor Vehicles (DMV), or via U.S. mail using restricted delivery requiring an adult signature (i.e., requiring the mail carrier to verify the identity of the person to whom the mail is addressed). State and local governments could also issue e-IDs. For example, state government could offer an e-ID through the DMV.

Many government agencies can also be attribute providers. Attribute providers make a claim about an individual. For example, the Social Security Administration can provide an assertion as to whether an individual has qualified for disability benefits, which in turn may be used by other agencies, for example to provide discounts for local public transportation. Various agencies, including the Department of State, DMVs and state vital statistics offices can provide assertions of age, date of birth and sex.

While the public sector should invest in e-ID systems, experiences in other countries that have high deployment but low use have shown that the government cannot simply take an "if we build it, they will come" approach to this technology. Government should build an e-ID infrastructure, but it needs to do more. On the demand side, the government should promote the use of e-IDs for electronic authentication and signing. First, the U.S. Chief Information Officer (CIO) should make e-IDs the default technology used for authentication to all federal agency websites. Second, the U.S. CIO should require that all federal agencies, within six months, identify high-value and high-volume e-government services that require user authentication, and establish a timeline for accepting e-IDs for online authentication. In addition, all agencies should identify current processes requiring ink signatures, such as certain tax forms, and evaluate whether these processes can be made more efficient using e-IDs. The private sector can help identify areas where the use of an e-ID can be most productive. For example, in May 2011 the Mortgage Bankers Association sent a letter to the Federal Housing Administration (FHA) at the U.S. Department of Housing and Urban Development (HUD) to permit the use of e-signatures for all mortgage origination forms.[185] FHA had previously announced that it would begin accepting electronic signatures for third-party documents from mortgagees, but not documents from the lenders.[186] Finally, the government should use incentives to spur faster adoption among users, such as offering e-IDs at a discount for early adopters.

Many countries have deployed e-ID systems but have failed to take full advantage of them, even within government. In particular, when the technology is being led by the national-level government, the state and local governments may not adopt the technology. To address this issue, the U.S. government should use strong incentive programs to encourage state and local e-government services to utilize e-ID technology, such as tying grants or other funding mechanisms to state and local efforts to utilize e-ID technology. The use of e-IDs should be a key feature of e-government at the federal, state and local level.

Design an e-ID solution that maximizes utility for both users and service providers

The use of e-IDs can benefit both users and service providers by making online transactions more efficient and secure. However, as noted earlier, all e-ID systems suffer from a chicken-or-egg problem that delays adoption. Maximizing the benefits for both parties will help speed adoption by incentivizing users to obtain an e-ID and service providers to invest in e-ID systems.

The agency controlling the development of an e-ID often shapes its outcome. It would be reasonable, for example, to expect an e-ID system developed by the Social Security Administration to emphasize access to e-government services, or an e-ID system developed by the Department of Homeland Security to focus on border control and public safety. While the NSTIC is appropriately situated in the Department of Commerce, which will hopefully lead to an emphasis on commerce, other government stakeholders should be actively involved in its development so that opportunities to achieve other important goals are not missed. In particular, improving information security should be a key priority of the e-ID strategy in the United States. Identity theft cost thirty-seven billion dollars in the United States in 2010 and affected 8.1 million adults.[187] As the President's Identity Theft

Task Force reported, improving consumer authentication processes should be a primary strategy for preventing identity theft and misuse of consumer data.[188]

One of the reasons that e-ID solutions have had slow adoption in many countries is that many of the security benefits of using e-IDs, compared to using one-off solutions, have been one-sided: service providers use e-IDs to verify the identity of users, but users do not have the opportunity to verify the identity of the service providers. The United States should follow the lead of Germany, one of the few countries to implement an e-ID system that uses mutual authentication. Using mutual authentication confers the security benefits of e-IDs to both service providers and users, thereby giving users more incentive to adopt e-IDs.

The e-ID system should be built with security in mind and use security controls, such as audit trails, to create accountability in the identity ecosystem. This would ensure that law enforcement could trace back any fraudulent e-IDs created by identity providers to their source. Policymakers will also need to ensure that any necessary improvements are made to the existing processes used to guarantee the integrity of birth certificates, Social Security Numbers and other identification documents issued by the government. For example, the state government agencies responsible for maintaining vital statistics may need to invest in systems to automate and improve the security of the identity proofing process. We do not want simply to digitize existing flaws in our identity ecosystem that would allow individuals to obtain false identification documents. Strong security protections will also incentivize use by the private sector. Banks, for example, are more likely to replace existing authentication mechanisms, such as a username and password, with an e-ID if it offers more security for the bank and customers.

Government will also need to address the issue of liability to both establish a clear framework and avoid a patchwork of conflicting state laws. The question of liability arises when private-sector entities issue identity credentials. For example, most certificate authorities currently transfer the liability of web certificates to website operators.[189] If a third party relies on an identity credential that turns out to be either stolen or fake, is the issuer liable? Typically, government identity providers are not liable for fraud or misuse of identity documents; the liability rests on the user and the service provider making use of the credential. Similarly, private-sector identity providers, unless they are negligent in their practices, should not be liable if an individual obtains an e-ID fraudulently or uses a stolen e-ID. Federal legislation will likely be needed to prevent states from creating conflicting liability standards. For example, the Virginia legislature is considering legislation that would limit liability for identity providers.[190] A federal standard would help create regulatory certainty and eliminate a potential disincentive for the private sector to offer e-IDs.

In addition, government should protect both consumers and service providers from fraud and misuse by providing public insurance for transactions completed with an e-ID. By offering insurance to reduce their risk, similar to what is offered by the FDIC to consumers for deposit accounts, the government can encourage users and relying parties to adopt e-IDs for transactions. This does not necessarily need to be a one-size-fits-all solution. One

way to build flexibility into the system is to offer different levels of liability protection for different types of e-IDs. Those e-IDs that provide higher levels of trust, such as by requiring more thorough identity proofing standards, can offer higher levels of liability insurance. By protecting consumers and service providers who use an e-ID for transactions, the government will make the use of e-IDs more valuable and thus encourage the use of electronic signatures over ink-based signatures.

Ensure that privacy does not come at the expense of eliminating useful information from the information economy

Although privacy is often cited as a concern for the development of national ID systems, as discussed above, an e-ID system can enhance user privacy by reducing the amount of information revealed during a transaction. For example, individuals can prove that they are over the age of twenty-one without revealing their exact date of birth or name. While this is a potential benefit for individuals, there is a risk that data sets that might otherwise be generated and that are useful for society will no longer be created. For example, an e-ID could be used to allow individuals to purchase prescription medication without revealing the name of the physician who wrote the prescription or demographic information such as age and gender. This data, however, may have beneficial uses, such as combating prescription drug abuse or studying drug effectiveness in a given population. The McKinsey Global Institute estimates that the value of data to health care in the United States exceeds $300 billion annually.[191]

The solution to such a risk is to ensure that policymakers understand the value of data sets and take into account the need to enable beneficial types of data sharing when legislating or rulemaking. ITIF has noted earlier the need for the Department of Commerce to create a Data Policy Office to encourage data policies that foster economic activity, such as increasing data sharing, reducing barriers to global information flows, and protecting consumer privacy.[192] For example, the Data Policy Office could evaluate the impact of data regulations on competition and innovation, fund research on important issues like data de-identification, and work with other nations to improve international frameworks for sharing data across borders. The Data Policy Office would help ensure that beneficial uses of data are not curtailed by overly-restrictive data privacy policies. Given the importance of information to the information economy, the government agency leading the development of the e-ID system should ensure that enabling beneficial forms of data sharing is one of the metrics by which potential solutions are evaluated.

Strive for disruptive innovation, not just incremental innovation

Technological progress is often evolutionary rather than revolutionary. This is often the case in government where technology is used only to make existing processes more efficient, rather than to find new ways to redesign or reengineer processes to take advantage of new technology. Implementing an e-ID system gives government the opportunity not only to implement incremental innovation, but also to use the technology for disruptive innovation. Some steps are straightforward. For example, government agencies can be better integrated by allowing single-sign-on and reducing the number of login prompts as users navigate from one agency to another. Government can also find opportunities for more radical change in how it delivers services to citizens. For example, the government can

use e-IDs to implement an "ask once" policy that eliminates the need for users to provide information to government more than once. Instead, each data point is stored with a single authoritative government agency responsible for maintaining that data and then information is shared across government agencies.

The use of e-IDs also has the potential to be a major driver of innovation if it is an open platform that others in the private sector and public sector can build on. For example, as the health care sector continues to invest in health IT such as electronic health records, more needs to be done to securely authenticate patients and providers to online health care systems and authorize prescriptions, orders, and payments. The use of e-IDs can help make health care more secure and efficient. Another important step in this direction is for the e-ID to be an open platform for attribute providers. Attribute providers can be in the public or private sector. An open platform gives flexibility to both users and service providers. Professional licensing organizations, including state bar associations and medical licensing boards, can be attribute providers. A medical licensing board, for example, could provide a credential so that pharmacies could verify that a doctor submitting an e-prescription is currently licensed to practice. Universities can be attribute providers as well. For example, online stores can use a credential to ensure that student discount programs are used only by students currently enrolled full-time. One especially important attribute provider will likely be financial institutions. Conceptually, a credit card account or cash balance is just another type of attribute that can be associated with an individual's e-ID. Financial institutions can use e-IDs to enable e-payment solutions, including cash, debit and credit transactions. Individuals will be able to use their e-IDs as a virtual wallet to make purchases and send and receive money. Relying parties would make their decision of whether or not to trust a credential based on the trust they have in the attribute provider. The potential for innovation here is limitless.

Ensure that e-ID solutions are accessible and available to all individuals

As e-IDs become more common, they will likely become a prerequisite to participation in certain aspects of digital society and commerce. Thus it will be necessary to ensure that a digital divide does not emerge whereby certain populations are unable to participate because the technology is either not accessible or not available for their use. The development of the e-ID should therefore specifically take into account the needs of different groups, including non-U.S. citizens, low-income populations, and people with disabilities. Providing all individuals access to an e-ID will help ensure that organizations can phase out legacy systems for electronic authentication and signatures and will not need to run additional programs for those unable to obtain an e-ID.

First, policies should permit the issuance of e-IDs to non-U.S. citizens. The e-IDs should be issued without regard to immigration status to ensure that this segment of the population, including foreign tourists, permanent residents, foreign students, and temporary workers, are not excluded from digital society and commerce. Immigration status should not be a factor because an e-ID is not a proof of citizenship or residency. Instead, immigration status is an attribute that can be included on an e-ID by request. The federal government, state and local governments, and the private sector should be free to

issue or not issue e-IDs to undocumented individuals that satisfy identity proofing standards (much as they are with today's ID cards).

Second, various programs can help ensure that e-ID solutions are available to all individuals. To address the affordability issue, federal subsidies could be used to make e-IDs available to low-income populations. Another potential way to extend e-IDs to low-income populations is to add e-ID functionality to electronic benefits transfer (EBT) cards used in various social services programs such as Temporary Aid for Needy Families (TANF), Supplemental Nutrition Assistance Program (SNAP), and Special Supplemental Nutrition Program for Women, Infants and Children (WIC). Such a change would require upgrading from magnetic stripe cards to smartcards where necessary.

Finally, the U.S. should design an e-ID strategy that allows people with disabilities to fully participate in digital society. Other countries have embraced accessibility requirements for e-ID systems. For example, Denmark, which uses printed key cards with one-time passwords for online authentication and signing, provides both a large-text key card and a phone-based solution that automatically calls the user's phone and reads the one-time passcode aloud.[193] Ideally, e-ID solutions should be created with a universal design in mind that allows the technology to be used by individuals with varying levels of physical abilities. This means that both inaccessible technology requirements should be avoided and that multiple forms should be considered so that individuals can find alternative solutions based on their needs. Designing e-ID solutions for all users will help prevent barriers to their widespread adoption and use.

Design an e-ID system for the global digital economy

Systems designed for today's digital economy should reflect its global nature. Ideally, an e-ID issued in one country should be accepted in another. Unfortunately, every nation with an e-ID system today faces significant challenges to making its system interoperable outside of its borders. Currently, for example, many countries are participating in the EU STORK project for cross-border interoperability in Europe. However, more needs to be done to create an international e-ID framework. To this end, the U.S. should more actively lead the development of international standards for federated identity management systems. In addition, it should work to develop an interoperability framework that would allow e-IDs created in one nation to be accepted in another for online authentication and electronic signing. Properly managed, the growth of e-ID technology should help reduce barriers to the free flow of information by allowing secure transactions between individuals and organizations across national borders. However, if the deployment of these systems is mismanaged there is a risk that some citizens will be cut off from certain online services and will be unable to participate in some online communities.

ENDNOTES

1.   "Mexico to Issue Citizens National Identity Card," *The Associated Press*, July 29, 2009, http://abcnews.go.com/International/wireStory?id=8197948.

2   "The U.S. Electronic Passport Frequently Asked Questions," U.S. Department of State, n.d., http://travel.state.gov/passport/passport_2788.html (accessed August 2, 2011).

3.   Internet World Stats. "Internet Users in the World, Distribution By World Regions – 2011," March 31, 2011, http://www.internetworldstats.com/stats.htm (accessed August 2, 2011).

4.   "Machine Readable Travel Documents: Part 1" International Civil Aviation Organization (2006), http://www.icaeo.int.

5.   U.K. Home Office, "Biometric Passports," London, n.d., http://www.ips.gov.uk/passport/about-biometric-chip.asp (accessed May 16, 2008).

6.   Federal Ministry of the Interior, Federal Republic of Germany, "The e-Passport: Basics," Berlin, Germany, n.d., http://www.bmi.bund.de (accessed May 16, 2008).

7.   Australian Customs Service, "SmartGate—Frequently Asked Questions," n.d., http://www.customs.gov.au/ site/page.cfm?u=5555 (accessed August 8, 2008).

8.   "Citizen Card: FAQ" Buergerkarte.at, n.d., http://www.buergerkarte.at/en/hilfe/faq.html.

9.   "Gemalto provides e-identity cards in Lithuania," CBR Security (April 17, 2009), http://security.cbronline.com/news/gemalto_provides_e_identity_cards_in_lithuania_170409.

10.   "Gemalto provides national e-ID cards in Saudi Arabia" CBR Security (April 1, 2009), http://security.cbronline.com/news/gemalto_provides_e_id_cards_in_saudi_arabia_010409.

11.   "UAE Population Register and ID card program" Gemalto (May 2009), http://www.gemalto.com/brochures/download/uae_casestudy.pdf.

12.   Herbert Kubicek and Torsten Noack, "Different countries-different paths extended comparison of the introduction of eIDs in eight European countries," IDIS 3 (2010), 235-245.

13.   Herbet Leitold and Reinhard Posch, "Common Criteria in Austria – Overview of Experiences," 6th ICCC 2005 Tokio (September 28, 2005), http://www.a-site.at/pdfs/20050928_CC-in-Austria-Web.pdf.

14.   "The Status of Identity Management in European eGovernment Initiatives," DG Information Society and Media, European Commission (February 28, 2007), 10, http://ec.europa.eu/information_society/activities/ict_psp/documents/identity_management_eu_02_07.pdf.

15.   Geoff Llewellyn, "The Smart Route to Identity Assurance and Public Service Improvement," Gemalto (February 2009), 13.

16.   "Citizen Cards – Overview" Buergerkarte.at. n.d. http://www.buergerkarte.at/en/ueberblick/index.html.

17.   "Citizen Cards – Data Protection and Security" Buergerkarte.at. n.d. http://www.buergerkarte.at/sicherheit-datenschutz.de.php.

18.   Siddhartha Arora, "National e-ID card schemes: A European overview," *Information Security Technical Report* 13 (2008) 50.

19.   Geoff Llewellyn, "The Smart Route to Identity Assurance and Public Service Improvement."

20.   Frank Maes, "Belgium Country Update," Presentation at Porvoo Group 16 (March 2010).

21.   Ilse Mariën and Leo Audenhove, "The Belgian e-ID and its complex path to implementation and innovational change," *Identity in the Information Society* 3 (2010) 27-41.

22.   Ibid.

23.   Geoff Llewellyn, "The Smart Route to Identity Assurance and Public Service Improvement."

24.   Mariën and Audenhove, "The Belgian e-ID and its complex path to implementation and innovational change."

25.   Mariën and Audenhove, "The Belgian e-ID and its complex path to implementation and innovational change," 38-39.

26.   Ibid.

27.   National IT and Telecom Agency, "Ofte stillede spørgsmå" [Frequently Asked Questions], n.d. https://www.nemid.nu/support/ofte_stillede_spoergsmaal/.

28. National IT and Telecom Agency, "I dag er der NemID til alle," (July 1, 2010), https://www.nemid.nu/om_nemid/aktuelt/20100701_i_dag_er_der_nemid_til_alle.html.

29. National IT and Telecom Agency, "Ofte stillede spørgsmå."

30. National IT and Telecom Agency, "NemID runder 1 million aktive brugere," (October 20, 2010), https://www.nemid.nu/om_nemid/aktuelt/20101020_nemid_har_rundet_en_million_aktive_bruger e.html.

31. Jens Villiam Hoff and Frederik Villiam Hoff, "The Danish eID case: twenty years of delay," *Identity in the Information Society* 3 (2010).

32. Identity Documents Act [Estonia], 1 January 2000, available at: http://www.unhcr.org/refworld/docid/4728ab1b2.html (accessed 26 April 2010)

33. "eID in action: Estonia," *IDABC, European Commission*, July 2005, http://ec.europa.eu/idabc/en/document/4487/5584.

34. "e-Estonia," Estonia.eu, n.d., http://estonia.eu/about-estonia/economy-a-it/e-estonia.html (accessed August 15, 2011).

35. European Network and Information Security Agency, "Privacy Features of European eID Card Specifications," (2009), http://www.enisa.europa.eu/act/it/eid/eid-cards-en/at_download/fullReport.

36. Ibid.

37. DG Information Society and Media, European Commission "eID in Estonia," (October 17, 2006), http://www.epractice.eu/files/documents/cases/191-1170255573.pdf.

38. "What is DigiDoc?" SK.ee, n.d., http://www.sk.ee/pages.php/02030510101 (accessed April 27, 2010).

39. "Ticket and payment solutions," SK.ee, n.d., http://www.sk.ee/pages.php/020306,1099 (accessed April 27, 2010).

40. "Statistics about Internet Voting in Estonia," Vabariigi Valimiskomisjon, n.d., http://www.vvk.ee/voting-methods-in-estonia/engindex/staitistics/ (accessed August 15, 2011).

41. Ibid.

42. Arora, "National e-ID card schemes: A European overview," 4.

43. All population estimates in this report from the Population Reference Bureau at http://www.prb.org (accessed May 2011).

44. "MyKad Malaysia leverages Unisys expertise to roll out smartcards to 24 million citizens," *SecureIDNews* (May 5, 2006) http://www.secureidnews.com/2006/05/05/mykad-malaysia-leverages-unisys-expertise-to-roll-out-smart-cards-to-24-million-citizens.

45. Ibid.

46. "DIGISIGN ID Basic / Enhance" Digicert, n.d., http://www.digitcert.com.my.

47. National Registration Department, Ministry of Home Affairs, Malaysia, "MyKad: The Government Multipurpose Card," n.d., http://www.jpn.gov.my/kppk1/Index2.htm (accessed August 8, 2008).

48. National Registration Department, Malaysia, n.d.

49. Paul Tan, ePetrol: Possible fuel subsidy control mechanism," Blog of Paul Tan, (May 2008) http://paultan.org/archives/2008/05/21/epetrol-possible-fuel-subsidy-control-mechanism/.

50. "Read your MyKad with this" *The Star Online* (July 2, 2009) http://star-techcentral.com/tech/story.asp?file=/2009/7/2/prodit/20090702110851.

51. "MyKid – Identity card of Malaysia for children below 12 years old" MalaysiaCentral.com (December 2006) http://www.malaysiacentral.com/information-directory/government-rules-and-politics/identification-documents/mykid-identity-card-of-malaysia-for-children-below-12-years-old/.

52. Agency for Public Management and eGovernment (DIFI) "MinID" n.d., http://minid.difi.no/minid/minid.php?lang=en.

53. IDABC, European eGovernment Services, "eID Interoperability for PEGS: Update of Country Profile study: Norway country profile," (July 2009), 12.

54. BankID, "Ofte stilte spørsmål" (Frequently Asked Questions), n.d., https://www.bankid.no/Hjelp-og-nyttige-verktoy/Ofte-stilte-sporsmal-FAQ/.

55. Roger Dean and Juliet Hoskins, "Issues of identity" The European Association for e-identity and Security (October 2006) <www.eema.org/index.cfm?fuseaction=focus.content&cmid=330>.

56. Jon Sederqvist, "BankID," MACAW Card Bulletin, 16 (2009), https://www.bankid.no/Global/MACAW%20Card%20Bulletin%2016-2009%20-%20BankID.pdf.

57. Listed at 379.00 NOK on "Prisliste: BuyPass SmartKork" (Price List: BuyPass SmartCard), Buypass.no, (February 2011), http://www.buypass.no.
58. Åke Grönlund, "Electronic identity management in Sweden: governance of a market approach," *Identity in the Information Society* 3 (2010).
59. Grönlund, "Electronic identity management in Sweden: governance of a market approach."
60. Swedbank, "BankID/e-legitimation," n.d., http://www.swedbank.se/privat/internet-och-telefontjanster/bankid-(e-legitimation)/index.htm.
61. ePractice.eu, "eGovernment Factsheet - Sweden - National Infrastructure," September 16, 2009, http://www.epractice.eu/en/document/288382.
62. Grönlund, "Electronic identity management in Sweden: governance of a market approach."
63. BankID, "Mobile BankID – electronic identification launched in mobile phones," n.d. http://www.bankid.com/en/Mobile-BankID/.
64. Grönlund, "Electronic identity management in Sweden: governance of a market approach."
65. Ibid.
66. Swedbank, "BankID/e-legitimation."
67. "Antal personer som deklarerat elektroniskt per 2 maj 2011 - sista dag för deklaratio" (Number of people who declared electronically as of May 2 2011), Skatteverket (May 2011), http://www.skatteverket.se and Grönlund, "Electronic identity management in Sweden: governance of a market approach."
68. TUBITAK UEKAE, "Elektronik Kimlik Doğrulama Sistemi," n.d., http://www.ekimlik.gov.tr/.
69. Mücahit Mutlugün, email message to author, May 11, 2011.
70. Mücahit Mutlugün and Oktay Adalier, "Turkish National Electronic Identity Card," *SIN '09 Proceedings of the 2nd international conference on security of information and networks* (2009).
71. Mutlugün, "Turkish National Electronic Identity Card."
72. IDABC European eGovernment Services, "eID Interoperability for PEGS: Update of Country Profiles study: Turkish country profile," (August 2009).
73. Ibid.
74. "Türkiye Cumhuriyeti Vatandaş Kimlik Doğrulama Sistemi" [Turkey Identity Verification System], e-Devlet Kapısı, n.d., https://giris.turkiye.gov.tr/Giris3/.
75. James A. Lewis, "Securing Cyberspace for the 44th Presidency," CSIS Commission on Cybersecurity for the 44th Presidency, 2008, http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf.
76. "National Broadband Plan: Connecting America," Federal Communications Commission, 2010, http://www.broadband.gov/plan/.
77. Joshua B. Bolten, "E-Authentication Guidance for Federal Agencies," M-04-04, Executive Office of the President, Office of Management and Budget, December 16, 2003, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf.
78. Ibid.
79. Department of Homeland Security, "Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004, http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm.
80. "Current Status – HSPD-12," IDManagement.gov, December 2010, http://www.idmanagement.gov/presentations/HSPD12_Current_Status.pdf.
81. "DoD Common Access Card," CAC.mil, n.d., http://www.cac.mil/CardInfo.html.
82. "Identity, Credential and Access Management (ICAM)," IDManagement.gov, May 26, 2011, http://www.idmanagement.gov/drilldown.cfm?action=icam.
83. The President's Identity Theft Task Force, "Combating Identity Theft: A Strategic Plan," (September 2008), http://www.idtheft.gov/reports/IDTReport2008.pdf.
84. "Cyberspace Policy Review," White House, 2009, 6, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
85. Ibid.
86. "National Strategy for Trusted Identities in Cyberspace: Creating Options for Enhanced Online Security and Privacy," White House (June 25, 2010), http://www.dhs.gov/xlibrary/assets/ns_tic.pdf.
87. Ibid.

88. "National Strategy for Trusted Identities in Cyberspace," White House (April 2011), http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

89. "What Others are Saying About NSTIC," National Institute of Standards and Technology, n.d., http://www.nist.gov/nstic/what-others-are-saying.html.

90. "Microsoft Passport Investigation Docket," EPIC (February 27, 201), http://epic.org/privacy/consumer/microsoft/passport.html.

91. "Windows Live ID OpenID CTP Status Update," Microsoft, August 27, 2009, http://winliveid.spaces.live.com.

92. "Statistics," Facebook, n.d., http://www.facebook.com/press/info.php?statistics (accessed August 22, 2011).

93. "What is OpenID," OpenID, February 26, 2011, http://openid.net/get-an-openid/what-is-openid/.

94. "Open Identity for Open Government at NIH," *Interface* Center for Information Technology, National Institutes of Health (2009), http://datacenter.cit.nih.gov/interface/interface245/open_gov.html.

95. Utah Digital Signature Act, Utah Code Ann. §46-3-102 *et seq.*

96. See section 46-3-403. Ibid.

97. "Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law" *United Nations Commission on International Trade Law* (January 30, 1997): 5 http://daccessdds.un.org/doc/UNDOC/GEN/N97/763/57/PDF/N9776357.pdf?OpenElement.

98. "Status: 1996 - UNCITRAL Model Law on Electronic Commerce" *United Nations Commission on International Trade Law* http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html (accessed June 30, 2009).

99. National Conference of State Legislatures, "Uniform Electronic Transactions Act," n.d., http://www.ncsl.org/default.aspx?tabid=13484 (accessed August 1, 2011).

100. Electronic Signatures in Global and National Commerce Act, S. 761, 106th Cong. (2000).

101. European Commission, "European Initiative in Electronic Commerce, Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee on the Regions," April 15, 1997, http://cordis.europa.eu/esprit/src/ecomcom.htm.

102. European Commission, "European Initiative in Electronic Commerce."

103. European Commission, "A European Initiative in Electronic Commerce," and Ingrid Havemann, "Electronic Signature Legislation in European Law, Its Use and Efficacy," International Portal of the University of Allcante on Intellectual Property & Information Society, January 26, 2004, http://www.uaipit.com/files/publicaciones/0000002034_electrsignih-Ingrid.pdf

104. European Parliament, "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures," December 13, 1999, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:NOT

105. European Commission, "Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures," March 15, 2006, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0120:EN:NOT.

106. European Commission, "Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures."

107. European Commission, "Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market," November 28, 2008, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52008DC0798:en:NOT.

108. European Commission Information Society, "Main undertakings under the Action Plan," European Action Plan on e-signatures and e-identification, February 23, 2011, http://ec.europa.eu/information_society/policy/esignature/action_plan/undertakings/index_en.htm#Commission's_Electronic_Signature_Service_Infrastructure_(ESSI).

109. European Commission, "Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions -

Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market."

110.   European Commission Information Society, "Action 8: Revision of the eSignature Directive, Pillar: Digital Single Market," Digital Agenda for Europe: 2010-2020, n.d., http://ec.europa.eu/information_society/digital-agenda/index_en.htm.

111.   "Digital Signature Act 1997" Act 562, Laws of Malaysia, http://www.kpkk.gov.my/akta_kpkk/Digital%20Signature.pdf.

112.   Edgar A. Whitley and Ian Hosein, *Global Challenges for Identity Policies* (Palgrave Macmillan, 2010), 25.

113.   Whitley and Hosein, *Global Challenges for Identity Policies*, 39.

114.   Whitley and Hosein, *Global Challenges for Identity Policies*, 27.

115.   Whitley and Hosein, *Global Challenges for Identity Policies*, 32.

116.   Pablo Ouziel, "The Spanish Identity Card: Historical Legacies and Contemporary Surveillance," University of Victoria (2009) http://www.pabloouziel.com/Academic%20Essay/The%20Spanish%20Identity%20Card%20(final).pdf.

117.   Whitley and Hosein, *Global Challenges for Identity Policies*, 38.

118.   Whitley and Hosein, *Global Challenges for Identity Policies*, 34.

119.   Gornung and Roßnagel note that German authorities only impose penalties for providing false information. Gerrit Hornung and Alexander Roßnagel, "An ID card for the Internet – The new German ID card with 'electronic proof of identity,'" Computer Law & Security Report, Vol. 26, No. 2, 2010, pg. 151-157.

120.   Alexander Heichlinger and Patricia Gallego, "A new e-ID card and online authentication in Spain," IDIS (2010), 44.

121.   Mariën and Audenhove, "The Belgian e-ID and its complex path to implementation and innovational change."

122.   Mariën and Audenhove, "The Belgian e-ID and its complex path to implementation and innovational change."

123.   "UAE Population Register and ID card program" Gemalto (May 2009), http://www.gemalto.com/brochures/download/uae_casestudy.pdf.

124.   Peter Swire and Cassandra Butts, "The ID Divide" *Center for American Progress* (June 2, 2008) http://www.americanprogress.org/issues/2008/06/id_divide.html.

125.   Whitley and Hosein, *Global Challenges for Identity Policies*, 24.

126.   Hoff and Hoff, "The Danish eID case: twenty years of delay."

127.   Whitley and Hosein, *Global Challenges for Identity Policies*, 33.

128.   Gornung and Roßnagel note that German authorities only impose penalties for providing false information. Gerrit Hornung and Alexander Roßnagel, "An ID card for the Internet – The new German ID card with 'electronic proof of identity,'" Computer Law & Security Report, Vol. 26, No. 2, 2010, pg. 151-157.

129.   Grönlund, "Electronic identity management in Sweden: governance of a market approach."

130.   Ibid.

131.   Ibid.

132.   Ibid.

133.   Mariën and Audenhove, "The Belgian e-ID and its complex path to implementation and innovational change."

134.   Gornung and Roßnagel note that German authorities only impose penalties for providing false information. Gerrit Hornung and Alexander Roßnagel, "An ID card for the Internet – The new German ID card with 'electronic proof of identity,'" Computer Law & Security Report, Vol. 26, No. 2, 2010, pg. 151-157.

135.   European Commission Information Society, "About eTEN," n.d., http://ec.europa.eu/information_society/activities/eten/library/about/intro/index_en.htm

136.   European Parliament, "Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public

supply contracts and public service contracts," March 31, 2004, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0018:en:NOT.

137. European Commission, "Report on the operation of Directive 1999/93/EC on a Community framework for electronic signatures."

138. Mariën and Audenhove, "The Belgian e-ID and its complex path to implementation and innovational change."

139. Ibid.

140. Ibid.

141. FAQ's for Preparing and e-Filing Your Own Tax Return," IRS, n.d., http://www.irs.gov/efile/article/0,,id=217432,00.html (accessed February 9, 2011).

142. "Postident, Questions and Answers," Deutsche Post DHL, n.d. http://www.deutschepost.de/dpag?tab=1&skin=lo&check=yes&lang=de_EN&xmlFile=link1017202_1009859 (accessed May 11, 2011).

143. "About A-SIT," Secure Information Technology Center Austria, n.d., http://www.a-sit.at/de/allgemein/asit_en.php.

144. Yngve Espelid et al., "Robbing Banks with Their Own Software—an Exploit Against Norwegian Online Banks," *Proceedings of the IFIP 23rd International Information Security Conference* 278 (2008).

145. Ibid.

146. Grönlund, "Electronic identity management in Sweden: governance of a market approach."

147. Hornung and Roßnagel note that German authorities only impose penalties for providing false information. Gerrit Hornung and Alexander Roßnagel, "An ID card for the Internet – The new German ID card with 'electronic proof of identity,'" Computer Law & Security Report, Vol. 26, No. 2, 2010, 151-157.

148. Tarvi Martens, "Electronic identity management in Estonia between market and state governance," *IDIS* 3 (2010), 226-230.

149. Heichlinger and Gallego, "A new e-ID card and online authentication in Spain," 57.

150. Mariën and Audenhove, "The Belgian e-ID and its complex path to implementation and innovational change," 37.

151. European Network and Information Security Agency, "Privacy Features of European eID Card Specifications."

152. "National ID Programme A First in the Region," Digital Oman (2005), http://www.digitaloman.com/indexbf54.html?issue=1&lang=en&id=28_1 (accessed August 3, 2011).

153. Mariën and Audenhove, "The Belgian e-ID and its complex path to implementation and innovational change."

154. "STORK: What is it?" n.d., https://www.eid-stork.eu/index.php?option=com_content&task=view&id=37&Itemid=61.

155. "FAQ: Identity Card" National Registration Department of Malaysia (2008), http://www.jpn.gov.my/BI/4_5_kadpengenalan.php.

156. Heichlinger and Gallego, "A new e-ID card and online authentication in Spain," 54.

157. Heichlinger and Gallego, "A new e-ID card and online authentication in Spain," 55.

158. Note that the cost may vary based on implementation. Whitley and Hosein, *Global Challenges for Identity Policies*, 25.

159. Heichlinger and Gallego, "A new e-ID card and online authentication in Spain," 56.

160. Fabrice Mattatia, "An Overview of Some Electronic Identification Use Cases in Europe," in *Practical Studies in E-Government;* eds. Saïd Assar and Imed Boughzala, (Springer Science: 2011), 79.

161. Shane Ham and Robert D. Atkinson, "Frequently Asked Questions about Smart ID Cards," Progressive Policy Institute (January 18, 2002), http://www.dlc.org/print.cfm?contentid=250075.

162. Whitley and Hosein, *Global Challenges for Identity Policies*, 33.

163. Gornung and Roßnagel note that German authorities only impose penalties for providing false information. Gerrit Hornung and Alexander Roßnagel, "An ID card for the Internet – The new German ID card with 'electronic proof of identity,'" Computer Law & Security Report, Vol. 26, No. 2, 2010, pg. 151-157.

164. Hoff and Hoff, "The Danish eID case: twenty years of delay."

165. Ibid.
166. Mattatia, "An Overview of Some Electronic Identification Use Cases in Europe," 75.
167. "Citizen Cards – Overview" Buergerkarte.at. n.d., http://www.buergerkarte.at/en/ueberblick/index.html.
168. Mariën and Audenhove, "The Belgian e-ID and its complex path to implementation and innovational change," 32.
169. European Network and Information Security Agency, "Privacy Features of European eID Card Specifications."
170. Ibid.
171. Ibid.
172. "Turkish national electronic identity card"
173. Heichlinger and Gallego, "A new e-ID card and online authentication in Spain," 52.
174. Herbert Kubicek and Torsten Noack, "Different countries-different paths extended comparison of the introduction of eIDs in eight European countries," *Identity in the Information Society*, 3, May 2010, 235-245.
175. Gerrit Hornung and Alexander Roßnagel, "An ID card for the Internet – The new German ID card with 'electronic proof of identity,'" *Computer Law & Security Report*, Vol. 26, (2010), 151-157.
176. The President's Identity Theft Task Force, "Combating Identity Theft: A Strategic Plan."
177. Grönlund, "Electronic identity management in Sweden: governance of a market approach."
178. Mariën and Audenhove, "The Belgian e-ID and its complex path to implementation and innovational change."
179. Whitley and Hosein, *Global Challenges for Identity Policies*, 24-25.
180. Grönlund, "Electronic identity management in Sweden: governance of a market approach."
181. Hoff and Hoff, "The Danish eID case: twenty years of delay."
182. European Network and Information Security Agency, "Privacy Features of European eID Card Specifications."
183. Ibid.
184. State and local government employee estimate excludes education and hospitals. Bureau of Labor Statistics, U.S. Department of Labor, Career Guide to Industries, 2010-11 Edition, State and Local Government, Except Education and Health, on the Internet at http://www.bls.gov/oco/cg/cgs042.htm (accessed July 26, 2011).
185. Letter from Stephen A. O'Connor, Senior Vice President, Mortgage Bankers Association to Robert C. Ryan, Acting Assistant Secretary for Housing – Federal Housing Commissioner, U.S. Department of Housing and Urban Development, May 31, 2011, http://www.mbaa.org/files/News/InternalResource/76814_FullLetter.pdf.
186. "Electronic Signatures on Third Party Documents," Letter from David H. Stevens, Assistant Secretary for Housing – Federal Housing Commissioner, U.S. Department of Housing and Urban Development, (April 8, 2010), http://www.hud.gov/offices/adm/hudclips/letters/mortgagee/files/10-14ml.pdf.
187. "2011 Identity Fraud Survey Report" Javelin Strategy & Research (2011), http://www.idsafety.net/report.php.
188. The President's Identity Theft Task Force, "Combating Identity Theft: A Strategic Plan."
189. Nevena Vratonkic et al. "The Inconvenient Truth about Web Certificates," *The Workshop on Economics of Information Security (WEIS)*, Fairfax, Virginia (June 2011), http://infoscience.epfl.ch/record/165676/files/WEIS11-Vratonjic_1.pdf.
190. House Bill No. 2259, Virginia General Assembly, (2011). http://lis.virginia.gov.
191. James Manyika et al., "Big data: The next frontier for innovation, competition and productivity," McKinsey Global Institute, May 2011, http://www.mckinsey.com/mgi/publications/big_data/pdfs/MGI_big_data_full_report.pdf, 2.
192. Daniel Castro, "Create a Data Policy Office Not a Privacy Policy Office," Innovation Policy Blog, February 7, 2011, http://www.innovationpolicy.org/create-a-data-policy-office-not-a-privacy-pol.
193. NEM ID, "Rigtigt og forkert om NemID," n.d., https://www.nemid.nu/support/ofte_stillede_spoergsmaal/rigtigt_og_forkert_om_nemid/.

ABOUT THE AUTHOR

Daniel Castro is a Senior Analyst with the Information Technology and Innovation Foundation. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security and accessibility. Before joining ITIF, Mr. Castro worked as an IT analyst at the Government Accountability Office (GAO) where he audited IT security and management controls at various government agencies. He has a B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a Washington, D.C.-based think tank at the cutting edge of designing innovation strategies and technology policies to create economic opportunities and improve quality of life in the United States and around the world. Founded in 2006, ITIF is a 501(c) 3 nonprofit, non-partisan organization that documents the beneficial role technology plays in our lives and provides pragmatic ideas for improving technology-driven productivity, boosting competitiveness, and meeting today's global challenges through innovation.

FOR MORE INFORMATION, CONTACT ITIF BY PHONE AT 202.449.1351, BY EMAIL AT MAIL@ITIF.ORG, OR ONLINE AT WWW.ITIF.ORG.