United States Government Accountability Office

GAO

Report to Congressional Requesters

January 2010

BORDER SECURITY

Better Usage of Electronic Passport Security Features Could Improve Fraud Detection

GAO-10-96

January 2010

BORDER SECURITY

Better Usage of Electronic Passport Security Features Could Improve Fraud Detection

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-96, a report to congressional requesters

Why GAO Did This Study

In 2005, the Department of State (State) began issuing electronic passports (e-passports) with embedded computer chips that store information identical to that printed in the passport. By agreement with State, the U.S. Government Printing Office (GPO) produces blank e-passport books. Two foreign companies are used by GPO to produce e-passport covers, including the computer chips embedded in them. At U.S. ports of entry, the Department of Homeland Security (DHS) inspects passports. GAO was asked to examine potential risks to national security posed by using foreign suppliers for U.S. e-passport computer chips. This report specifically examines the following two risks: (1) Can the computer chips used in U.S. e-passports be altered or forged to fraudulently enter the United States? (2) What risk could malicious code on the U.S. e-passport computer chip pose to national security? To conduct this work, GAO reviewed documents and interviewed officials at State, GPO, and DHS relating to the U.S. e-passport design and manufacturing and e-passport inspection systems and procedures.

What GAO Recommends

GAO recommends that DHS implement the systems needed to fully verify e-passport digital signatures at U.S. ports of entry, and in coordination with State, implement an approach to obtain the necessary data to validate the digital signatures on U.S. and other nations' e-passports. DHS agreed with our recommendations.

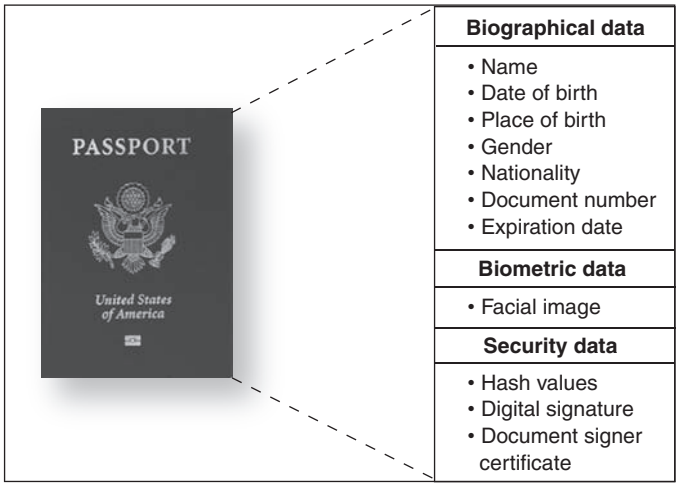
View GAO-10-96 or key components.
For more information, contact Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

What GAO Found

State has developed a comprehensive set of controls to govern the operation and management of a system to generate and write a security feature called a digital signature on the chip of each e-passport it issues. When verified, digital signatures can help provide reasonable assurance that data placed on the chip by State have not been altered or forged. However, DHS does not have the capability to fully verify the digital signatures because it has not deployed e-passport readers to all of its ports of entry and it has not implemented the system functionality necessary to perform the verification. Because the value of security features depends not only on their solid design, but also on an inspection process that uses them, the additional security against forgery and counterfeiting that could be provided by the inclusion of computer chips on e-passports issued by the United States and foreign countries, including those participating in the visa waiver program, is not fully realized.

Protections designed into the U.S. e-passport computer chip limit the risks of malicious code being resident on the chip, a necessary precondition for a malicious code attack to occur from the chip against computer systems that read them. GPO and State have taken additional actions to decrease the likelihood that malicious code could be introduced onto the chip. While these steps do not provide complete assurance that the chips are free from malicious code, the limited communications between the e-passport chip and agency computers significantly lowers the risk that malicious code—if resident on an e-passport chip—could pose to agency computers. Finally, given that no protection can be considered foolproof, DHS still needs to address deficiencies noted in our previous work on its computer systems to mitigate the impact of any malicious code that may be read from e-passport computer chips and infect those systems.

Contents of the U.S. E-passport Computer Chip



Source: GAO analysis based on State Department information.

Contents

Abbreviations

ANSI	American National Standards Institute
CBP	U.S. Customs and Border Protection
DHS	Department of Homeland Security
GPO	Government Printing Office
IC	integrated circuit
ICAO	International Civil Aviation Organization
IT	information technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PKI	public key infrastructure
RF	radio frequency
RFID	radio frequency identification
US-VISIT	United States Visitor and Immigrant Status Indicator Technology

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

January 22, 2010

The Honorable Henry Waxman
Chairman
The Honorable John Dingell
Chairman Emeritus
Committee on Energy and Commerce
House of Representatives

The Honorable Bart Stupak
Chairman
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
House of Representatives

In 2005, the Department of State (State) began producing and issuing electronic passports (e-passports). These new e-passports have an embedded computer chip that stores information identical to that printed in the passport, including the traveler's name, date of birth, photo, passport number, and passport expiration date. By comparing the information contained on the chip with the information printed in the passport, inspecting officials can more readily identify whether the photo or the biographical information has been altered or counterfeited, which provides greater assurance of the integrity of the passport.

State's Bureau of Consular Affairs is responsible for the design and issuance of passports, and U.S. Customs and Border Protection (CBP) in the Department of Homeland Security (DHS) inspects the documents at ports of entry to the United States. By agreement with State, the U.S. Government Printing Office (GPO) produces blank e-passport booklets. Among the many components that are used to make e-passport booklets, GPO has contracts with two European companies to produce the e-passport covers, including the manufacturing and inlaying of the computer chips into the e-passport covers. Both European companies use subcontractors in Asia for parts of the work. Concerns have been raised that the use of foreign-produced computer chips introduces risks to the integrity of the U.S. e-passport.

In response to your request, this report focuses on potential risks to national security posed by the use of foreign suppliers for U.S. electronic passports. Specifically, it examines the following two risks: (1) Can the computer chips used in U.S. e-passports be altered or forged to fraudulently enter the United States? (2) What risk could malicious code on the U.S. e-passport computer chip pose to national security?

To determine whether e-passport chips can be altered or forged so that a traveler could fraudulently enter the United States, we interviewed officials from State's Bureau of Consular Affairs and reviewed State Department policies, procedures, and guidance documents regarding the public key infrastructure (PKI) used to protect the data on the e-passport computer chip and assessed them against relevant International Civil Aviation Organization (ICAO) and National Institute of Standards and Technology (NIST) standards and guidelines. We interviewed officials at one passport agency and reviewed systems documentation to understand how U.S. e-passports are personalized. We determined the extent to which information stored on U.S. e-passport computer chips is inspected at U.S. ports of entry by interviewing DHS and CBP officials and reviewing documentation regarding the systems and procedures used to inspect e-passports at the ports of entry.

To determine whether malicious code on the e-passport chips poses a risk to national security, we determined how U.S. e-passport computer chips are manufactured and incorporated into the production of blank U.S. e-passport booklets based on interviews with GPO and manufacturer officials and reviews of GPO documentation. We met with officials from NIST and the National Counterterrorism Center to determine the level of threat that exists to U.S. e-passports. We interviewed GPO and State officials and reviewed documentation that describes the U.S. e-passport computer chip architecture and operations. We reviewed documents governing the manufacturing of the blank e-passport covers. We identified protections that have been designed into the e-passport computer chip as well as controls that are in place to reduce the possibility of malicious code on the e-passport computer chip.

Additional details on our scope and methodology can be found in appendix I. We conducted this performance audit from June 2008 to January 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe

that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

U.S. passports are official documents that are used to demonstrate the bearer's identity and citizenship for international travel and reentry into the United States. Under U.S. law, the Secretary of State has the authority to issue passports, which may be valid for up to 10 years.[1] Only U.S. nationals may obtain a U.S. passport, and evidence of citizenship or nationality is required with every passport application. Federal regulations list disqualifying situations under which U.S. citizens are not eligible for a passport, such as those who are subjects of a federal felony arrest warrant.

The security of passports and the ability to prevent and detect their fraudulent use are dependent upon a combination of well-designed security features, solid issuance procedures for the acceptance and adjudication of the application and the production of the document, and inspection procedures that utilize the available security features of the document. A well-designed document has limited utility if it is not well produced or if inspectors do not utilize the security features to verify the authenticity of the document.

In 2005, State began issuing e-passports, which introduced an enhanced design and physical security features. GPO manufactures blank e-passport booklets for State using a variety of materials from different suppliers. Currently, GPO has two suppliers—Infineon and Gemalto—under contract for the covers of the e-passports.[2] These covers include the computer chip embedded in the back cover that can communicate using contactless ID technology. Security-minded versions of this technology are employed in contactless smart cards used in applications such as automatic banking and identification. As of February 1, 2009, the State Department had issued over 30 million e-passports.

[1]A tourist passport, for individuals 16 years or older, is valid for 10 years from the date of issuance; it is valid for 5 years for younger travelers. An official passport, for federal employees traveling on official government business, and a diplomatic passport, for government officials with diplomatic status, are each valid for 5 years from the date of issuance.

[2]One contract was originally awarded to Axalto, which later merged with GemPlus to create Gemalto.

Document Security Features

To combat document fraud, security features are used in a wide variety of documents, including currency, identification documents, and bank checks. Security features are used to prevent or deter fraudulent alteration or counterfeiting of such documents. In some cases, an altered or counterfeit document can be detected because it does not have the look and feel of a genuine document. For instance, in U.S. passports, detailed designs and figures are used with specific fonts and colors. While these features are not specifically designed to prevent the use of altered or counterfeit documents, inspectors can often use them to identify nongenuine documents.[3]

Security features of travel documents are assessed by their capacity to secure a travel document against the following threats:

- counterfeiting—unauthorized construction or reproduction of a travel document,
- forgery—fraudulent alteration of a travel document, and
- impostors—use of a legitimate travel document by people falsely representing themselves as legitimate document holders

While security features can be assessed by their individual ability to help prevent the fraudulent use of the document, it is more useful to consider the entire document design and how all of the security features help to accomplish this task. Layered security features tend to provide improved security by minimizing the risk that the compromise of any individual feature of the document will allow for unfettered fraudulent use of the document. While most security features in the U.S. e-passport are physical features, the introduction of the computer chip also allows for the use of electronic security features.

Inspection of Travel Documents to Enter the United States

In general, at ports of entry, travelers seeking admission to the United States must present themselves and a valid travel document, such as a passport, for inspection to a CBP officer. The immigration-related portion of the inspections process requires the officer to confirm the identity and

[3]We previously reported on security features of State-issued travel documents, including e-passports, in GAO, *Border Security: Security of New Passports and Visas Enhanced, but More Needs to Be Done to Prevent Their Fraudulent Use*, GAO-07-1006 (Washington, D.C.: July 31, 2007).

determine the admissibility of the traveler by questioning the individual and inspecting the presented travel documents. In the first part of the inspection process—primary inspection—CBP officers inspect travelers and their travel documents to determine whether they should be admitted or referred for further questioning and document examination. If additional review is necessary, the traveler is referred to secondary inspection—in an area away from the primary inspection area—where another officer makes a final determination to admit the traveler or deny admission for reasons such as the presentation of a fraudulent or counterfeit passport.

E-passport Computer Chip Construction and Communication

The chips used in the U.S. e-passports are integrated circuits (IC) that are essentially complete computers that contain a central processing unit, various types of memory, and other components that perform specialized functions such as random number generation and advanced cryptographic processing. The chips contain both hardware and software. The hardware circuitry and the operating system are implanted into the various layers of the chip in a process called photolithography, which employs a technique called masking wherein the chip's circuitry is defined on a series of glass plates called the photomask. The photomask is used as a template to transfer the pattern of the chip's electronic components into the various layers of the physical chip. Once implanted, the circuitry is considered permanent and not changeable except through physical attack.

While the chip's operating system is implanted into the chip through the photomask at chip creation time, other software needed on the chip—for example, the traveler data—are written to the chip later, during personalization of the chip.

The e-passports are designed as contactless proximity cards, and communication with the embedded chip is only via a radio frequency (RF) link established according to standard methods with a device generally called a reader. To support global acceptance and interoperability of e-passports, ICAO issued standards that define how data are to be stored on and read from e-passports, including the RF communications.[4] According to the ICAO standards, contactless communication with the

[4]ICAO, *Machine Readable Travel Documents, Part 1 Machine Readable Passports, Volume 2 Specifications for Electronically Enabled Passports with Biometric Identification Capability*, ICAO 9303 Part 1, Sixth Edition (2006).

e-passport is governed by ISO/IEC 14443, an international standard that defines the transmission protocol used to transfer data between the reader and the chip.[5] Higher-level reading from and writing to the chip is implemented through the ISO/IEC 7816-4 command set.[6] ISO 7816-4 is an international standard set of commands used to communicate with the chip and to control all reading from and writing to the chip based on a strict command/ response scheme. The reader initiates all commands to the chip and the chip provides the expected response. The chip itself cannot initiate any communications with the reader. ISO 7816-4 includes controls to limit read and write access to the chip to authorized parties.

The United States issues e-passports with both ISO/IEC type A and type B interface connections. Both types use the same transmission protocol, but vary in how communications are established between the chip and the reader and in how information is encoded for transmission.

The chip has no onboard power, but instead pulls the energy it needs from the electromagnetic field emitted by the reader. The e-passport antenna receives the electromagnetic energy from the reader and converts it to electric current to power the chip. The chip can be powered and communicate only when it is in close proximity—up to about 10 centimeters—to an appropriate reader.[7] With both types of chips, the antenna is a component external to the chip and separately attached to it as part of the overall book cover manufacturing process.

The Software Contents of the Chip

While the communication protocols and command set are standardized, the operating system and other software used on the chips are vendor-specific. As is typical with smart card ICs, the software on the e-passport chips is partitioned into three general areas: the IC dedicated software, the basic embedded software, and the application embedded software. The IC dedicated software contains software used for testing purposes and software to provide other services to facilitate usage of the hardware on

[5]The ISO/IEC 14443 standard is composed of four parts, covering physical characteristics, radio frequency power and signal interface, initialization and anticollision procedures, and transmission protocols.

[6]ISO/IEC, *Identification cards—Integrated circuit cards, Part 4: Organization, security and commands for interchange*, ISO/IEC 7816-4, Second Edition (Jan. 15, 2005).

[7]With special equipment and under certain circumstances, the read distance can be increased somewhat.

the IC. The IC dedicated software is developed by the IC manufacturer and it is part of the photomasks of the chips.

The basic embedded software is typically not provided by the chip manufacturer, but is usually developed by a third party and delivered to the chip manufacturer for incorporation into the chip's photomask. An important component of the basic embedded software is the operating system for the chip. The operating system implements the ISO 7816-4 command set and controls all communication between the chip and the outside world.

The third major partition of software on the chip is the application embedded software, which is also typically provided by a third party and provides functionality specific to the particular application for which the chip is intended to be used. In the case of the U.S. e-passports, the application software is data contained in a file layout using an open, ICAO-specified logical data structure used for machine-readable travel documents.

The E-passport Production Process

In producing e-passport booklets for State, GPO has tapped into the existing global smart card industry, resulting in a wide number of different companies involved in the e-passport chip production and inlay process. Two separate companies were awarded contracts to supply chips for the U.S. e-passports. Infineon, a German company, fabricates its own chips and embeds a commercial operating system from a third-party company on them. Gemalto, a Dutch company, obtains chips from NXP, a Dutch semiconductor manufacturer. Gemalto provides NXP with its own operating system, which NXP embeds within the chip prior to shipping the chip to Gemalto.

Although each of these contractors takes a different path to create and provide e-passport covers to GPO, both use a common subcontractor for attachment of the antenna to the chip and the inlaying of the chip into the back cover of the e-passport booklet. GPO itself finishes production of the e-passport booklet by inserting the paper pages into the covers, installing a metal strip down the inside spine for RF shielding, and, in a process termed pre-personalization, preparing the chip for use by the State Department. State personalizes the e-passport by printing bearer data onto the data page and writing digital data onto the chip as part of its issuance procedures.

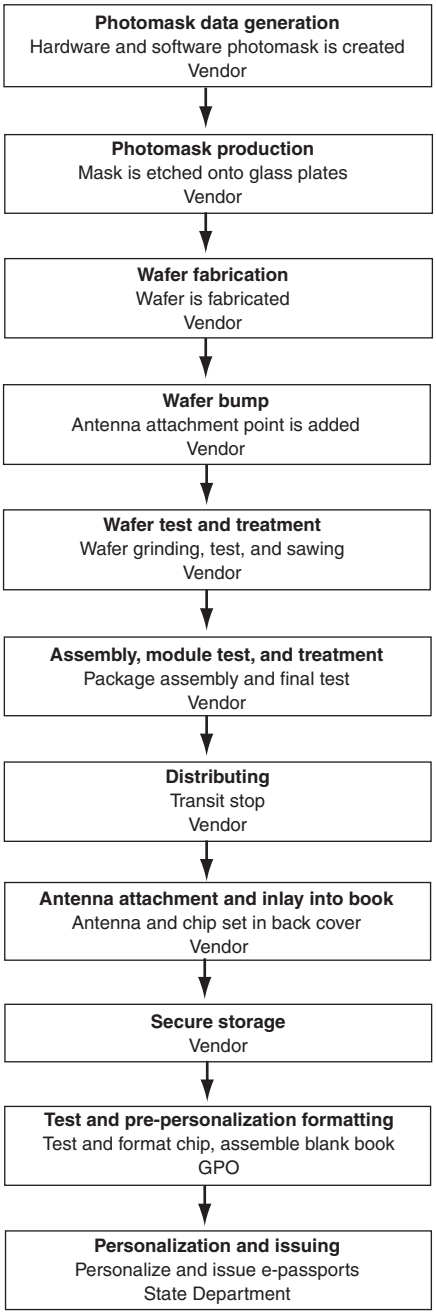
Gemalto E-passport Chip and Booklet Production Process

As seen in figure 1, several steps are involved in the production of an e-passport using Gemalto's e-passport booklet. Gemalto involves several subcontractors to produce the cover before it is delivered to GPO. For instance, while the operating system software is created by Gemalto, it is implanted on the chip when it is fabricated by NXP. Companies overseas are also involved in the production of the chip and its incorporation into the e-passport cover.

In pre-personalization, GPO tests and formats the chips, preparing them for personalization by State, and finishes overall construction of the e-passport booklet. GPO then ships the finished, blank e-passport books to the 21 State Department passport issuing offices around the country that then personalize and issue them to U.S. citizens, as needed.[8]

[8]State has 19 domestic passport agencies and centers that accept, examine, adjudicate, and process passport applications; they issue passports to those determined to be citizens or nationals of the United States. State also has two domestic passport personalization facilities that produce and issue the passports once one of the passport centers or agencies has approved the passport application.

Figure 1: Gemalto E-passport Chip and Book Production Process

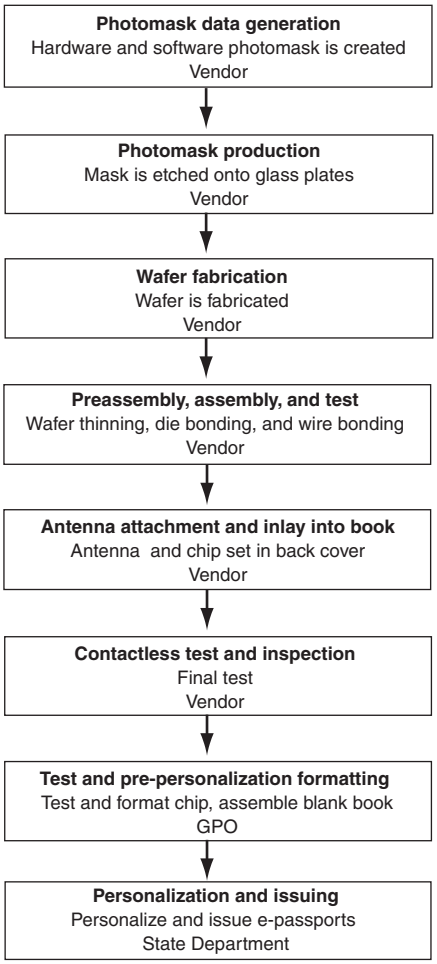


Source: GAO analysis based on GPO and Gemalto information.

Infineon E-passport Chip and Book Production Process

Similar to Gemalto's production process, the production process at Infineon also involves several subcontractors to produce the booklet cover before it is delivered to GPO (see fig. 2). The operating system and other embedded software used on the Infineon chips are developed by a third-party company, and shipped to Infineon for incorporation into the photomask pattern. As with the Gemalto production process, GPO tests and pre-personalizes each chip, finishes the books, and distributes the finished, blank e-passport books to the 21 passport-issuing offices.

Figure 2: Infineon E-passport Chip and Book Production Process



Source: GAO analysis based on GPO and Infineon information.

Threats to E-passport Computer Chips

Since 1997, GAO has identified federal information security as a high-risk area.[9] Malicious code is one of the primary threats to federal information security. NIST defines malicious code—sometimes called malware—as "a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim."[10] Malicious code can be used for many purposes and come in many forms. For example, malicious code might be designed to delete files on a system or repeatedly attempt access to a system service and thus effectively shut it down. The effects of malicious code can range from performance degradation to compromise of mission-critical applications. Some common forms of malicious code include viruses, worms, and Trojan horses. Viruses infect a system by attaching themselves to host programs or data files. Worms are self-contained programs that can self-replicate and do not require human interaction to spread through a system or network. Trojan horses are nonreplicating programs that appear benign but are designed with a malicious purpose.

Malicious code often takes advantage of vulnerabilities in a system's software to either spread or execute. For example, a common vulnerability, known as a buffer overflow, redirects system control to a malicious program through badly designed software. Inadequate controls on a network's connections or services are another common vulnerability that allows malicious code to spread. Common protections against malicious code include input checking at the boundaries of a system, such as at external interfaces to a system; network controls to lower the possibility that malicious code could spread within a system; and patch management to address vulnerabilities in the system's software that malicious code can exploit.

In general, a successful malicious code attack first requires that the malicious code get into a system. This can occur, for example, by inserting infected media into the computer or through incomplete controls on the system's network connections. Second, the malicious code needs to spread to those areas of a system to which it wants to cause damage. Malicious code can spread in many ways, including various network protocols and services and also in simple file transfers. Finally, malicious

[9]GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: January 2009).

[10]NIST, *Guide to Malware Incident Prevention and Handling*, SP800-83 (Gaithersburg, Md.: November 2005).

code needs to be executed, often by taking advantage of vulnerabilities in a system's software.

Therefore, in the case of e-passports, a successful malicious code attack from the chip would first require that malicious code get on the chip. Second, that it get transferred from the chip onto agency computers during the e-passport inspection process and then spread to vulnerable areas within those systems. And, finally, the malicious code would have to be executed.

Although communication with the chips is designed to be via the contactless ID interface that complies with the ISO 7816-4 standard, which includes an authentication procedure to limit read and write access to the chip to authorized parties, an alternate, illicit way data can be attempted to be read from or written to the chip is through physical tampering techniques. In general, the aim of such an attack is to discover confidential data stored on the chip—such as cryptographic keys—which can be used to open access to the chip via the contactless interface.

Common Criteria

Common Criteria is an international standard method for evaluating security features of information technology (IT) components. The U.S. portion of this effort is coordinated through a partnership of NIST and the National Security Agency (NSA) called the National Information Assurance Partnership (NIAP). It provides a framework for evaluating security features of IT components. The Common Criteria program evaluates commercial-off-the-shelf information assurance and information assurance-enabled products. These products can be items of hardware, software, or firmware. Evaluations are performed by accredited Common Criteria testing laboratories whose results are then certified by a validation body. A product is considered Common Criteria certified only after it is both evaluated by an accredited laboratory and validated by the validation body.

Common Criteria certifications are expressed in a seven-step assurance scale called Evaluation Assurance Levels. The seven ordered levels provide an increasing measure of confidence in a product's security functions. All evaluated products that receive a Common Criteria certificate appear on a validated products list, which is available on the Common Criteria Web site.

To facilitate the efficient use of testing resources, an international agreement was developed under which one country's Common Criteria

certifications would be recognized by the other participating countries.[11] This is intended to eliminate unnecessary duplication of testing efforts.

Common Criteria certifications need to be carefully considered. We have reported previously that the fact that a product appears on the validated products list does not by itself mean that it is secure.[12] A product's listing on any Common Criteria validated products list means that the product was evaluated against its security claims and that it has met those claims. The extent to which vendor-certified claims provide sufficient security for a given application is another question.

E-passports Have Reasonable Safeguards to Assure That Computer Chip Data Cannot Be Altered or Forged, but Ports of Entry Lack the Capabilities to Use Them

A complex environment has been established to provide reasonable assurance that the data contained on electronic passports can be used to help determine whether an individual should be admitted to the United States. The overall control environment depends on each party effectively implementing the controls that have been established to govern its operation and utilize the controls implemented by the other agencies. State uses a technology commonly referred to as public key cryptography to generate digital signatures on the data it writes to the computer chips on the e-passport. These digital signatures, when effectively implemented, can help provide reasonable assurance that integrity has been maintained over the data placed on the chip by State. Our review found that DHS has not implemented the capabilities needed to completely validate the digital signatures generated by State before relying on the data, which adversely affects its ability to obtain reasonable assurance that the electronic data provided in a chip were the same data that State wrote in the e-passport. While DHS has some controls that somewhat mitigate this weakness, it does little to ensure that altered or forged electronic data can be detected. Accordingly, until DHS implements this functionality, it will continue to lack reasonable assurance that data found on e-passport computer chips have not been fraudulently altered or counterfeited.

[11]Thirteen countries are recognized as certificate producers under the Arrangement on the Mutual Recognition of Common Criteria Certificates in the Field of IT Security: the United States, Australia, Canada, France, Germany, Japan, the Netherlands, New Zealand, Norway, Spain, South Korea, Sweden, and the United Kingdom.

[12]GAO, *Information Assurance: National Partnership Offers Benefits, but Faces Considerable Challenges*, GAO-06-392 (Washington, D.C.: Mar. 24, 2006).

State Generates Digital Signatures That Can Be Used to Provide Needed Assurance

ICAO has issued e-passport standards that have been adopted by the United States and other countries.[13] As part of its specifications for e-passports, ICAO requires the use of digital signatures and a public key infrastructure to establish that the data contents of the computer chip are authentic and have not been changed since being written. A PKI—a system of hardware, software, policies, and people—is based on a sophisticated cryptographic technique known as public key cryptography. The use of a PKI for e-passports primarily serves to provide (1) data integrity (the electronic data placed on the passport have not been changed), and (2) authentication (the country issuing the e-passport was the source of the data). In its standards, ICAO specifies only the use of well-known cryptographic algorithms for use in e-passports.

As discussed in appendix II, public key cryptography is used to generate and validate digital signatures. In particular, the "public key" is used to validate the digital signature that is used to authenticate the data being signed. However, a means is necessary for the user to reliably associate a particular public key with a document signer. The binding of a public key to a document signer is achieved using a digital certificate, which is an electronic credential that guarantees the association between a public key and a specific entity.[14]

In agreement with ICAO standards for e-passports, State generates and writes a digital signature on the chip of each e-passport during the personalization process. As illustrated in figure 3, State stores the following information on the e-passport computer chip: biographical information about the traveler, the traveler's facial image, and security data. The biographical data and facial image are organized into data groups for storage on the e-passport. Each data group is condensed using a hashing algorithm and the resulting hash values are stored in the security data.[15] A digital signature is generated on these hash values, which represent the data stored on the e-passport computer chip. Hence, the security data on an e-passport consist of three key elements: the data

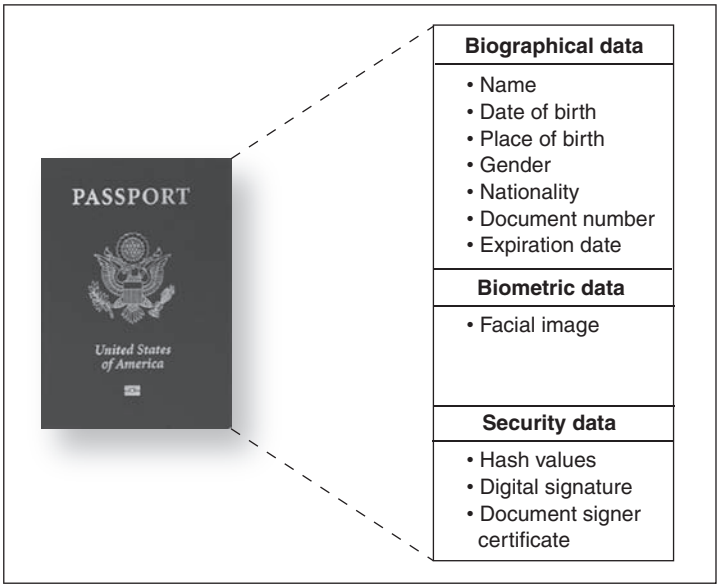
[13]ICAO 9303, Part 1, Volume 2.

[14]A digital certificate is created by placing the entity's name, the entity's public key, and certain other identifying information in a small electronic document that is stored in a directory or other database. Directories may be publicly available repositories kept on servers that act like telephone books for users to look up others' public keys.

[15]A hash is created using a special one-way cryptographic algorithm that is designed to process an input file to produce a unique condensed fixed-length message digest.

group hash values, the digital signature, and the certificate needed to validate the digital signature. This certificate—known as the document signer certificate—is associated with a digital signature on a U.S. e-passport's data and is used to validate that the signed data contained in that passport were actually generated by State. The keys and certificates associated with U.S. e-passports are established in a hierarchical manner to establish a "chain of trust" that a third party, such as DHS, can use to obtain reasonable assurance that the data contained in the passport are the data that were actually written on to the e-passport by State.

Figure 3: Contents of the U.S. E-passport Computer Chip



Source: GAO analysis based on State Department information.

State has developed a comprehensive set of controls to govern the operation and management of the PKI that generates the digital signatures used to help assure the integrity of the passport data written to the chip. These controls include the development of policies and practices that are consistent with best practices described in federal guidelines. For example, State's policies and procedures for generating and storing digital signatures and certificates from cryptographic modules minimize the risk of compromise or unauthorized disclosure. Further, State's procedures require the use of cryptographic modules validated against the level 3

criteria of FIPS 140-2, which is consistent with federal best practices and requirements.[16]

If properly validated, the digital signatures on State's e-passports should provide those reading the chip data, including DHS, reasonable assurance that the data stored on the chip were written by State and have not been altered. Proper validation includes verifying that the document signer certificate was issued by the State Department.

DHS Has Not Implemented the Capability to Fully Verify E-passport Digital Signatures

In July 2007, we reported that DHS was not fully using a key security feature of the U.S. e-passport—namely the data stored on the chip.[17] At that time, DHS had not fully deployed e-passport readers to all primary inspection lanes at all ports of entry and did not have a schedule to do so. We also reported that the implemented e-passport reader solution was not capable of validating e-passport digital signatures, which would help to ensure that the data written to the e-passport chips have not been altered. Since that time, while DHS has begun planning an acquisition for new e-passport readers, DHS has made no further deployments of e-passport readers, nor has it implemented a solution that would allow for the full verification of the digital signatures on e-passport computer chips.

DHS Has Not Fully Deployed E-passport Readers to the Ports of Entry

In 2006, as a part of the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) system, DHS deployed 237 e-passport readers at 33 air ports of entry—212 are installed in primary inspection lanes and 25 are installed in training areas.[18] No e-passport readers are deployed in secondary inspection areas. While these 33 air ports of entry were chosen because they process the largest volume of travelers—about 97 percent—from Visa Waiver Program countries, the majority of lanes at these airports do not have e-passport readers.[19] Even though the same

[16]NIST, *Security Requirements for Cryptographic Modules*, FIPS 140-2 (Gaithersburg, Md.: May 25, 2001).

[17]GAO-07-1006.

[18]US-VISIT is a program designed to use biometric and biographic information to control and monitor the pre-entry, entry, status, and exit of foreign visitors. US-VISIT's goals are to (1) enhance the security of U.S. citizens and visitors, (2) facilitate legitimate travel and trade, (3) ensure the integrity of the U.S. immigration system, and (4) protect the privacy of visitors.

[19]Citizens of Visa Waiver Program countries are not required to obtain a U.S. visa to enter the United States for business or tourism purposes for 90 days or less.

e-passport readers may be used to read U.S. e-passports, U.S. citizens are primarily processed through lanes at these air ports of entry that are not equipped with e-passport readers.

At equipped primary inspection lanes, CBP officers can use e-passport readers to access the biographical information and digitized photograph stored on the e-passport chip. To read e-passports, officers place the biographical page of the e-passport on the reader's glass plate. The reader then electronically scans the biographical information printed on the page and uses it to access the information stored in the e-passport's chip. Once the biographical data and photograph from the chip are displayed on the primary inspection computer screen, the officer is to compare the information displayed with the information on the biographical page of the passport and verify that they match. The results of any validation activities conducted on the data by the system are also presented to the officer. Any mismatches could indicate fraud.

While a total of 500 e-passport readers were purchased by the US-VISIT program. DHS has made no further deployments of e-passport readers since 2006. Those not deployed are in storage, used for training, or used to support system development activities. Following the deployment at the 33 air ports of entry in 2006, responsibility for deploying the e-passport readers was shifted from the US-VISIT program to CBP. CBP officials partially attributed the lack of progress in deploying e-passport readers to its failure to allocate funding for the activity since it assumed the responsibility from US-VISIT. According to DHS officials, the slower than expected times to read data from e-passport chips also influenced its decisions to not further the deployment of the e-passport readers.

In 2008, DHS transferred $11.4 million of no-year funds from US-VISIT to CBP for planning, purchasing, and deploying e-passport readers at all CBP primary processing lanes and secondary inspection areas at the ports of entry. According to CBP officials, it is currently planning an acquisition for new e-passport readers. As a part of the acquisition planning, CBP also expects to determine whether it will replace the 500 currently deployed or stored e-passport readers with new readers that will likely have better performance than the current readers. According to DHS, CBP is planning an e-passport reader procurement that will allow for the full deployment of e-passport readers in fiscal year 2011.

In our prior work, we recommended that DHS develop a deployment schedule for providing sufficient e-passport readers to U.S. ports of entry.[20] With the identification of funding for the effort, CBP has initiated planning for further deployment of e-passport readers, but has not yet developed a deployment schedule. Until DHS installs e-passport readers in all inspection lanes, CBP officers will not be able to take advantage of the data stored on e-passport chips. For instance, without e-passport readers, CBP officers are unable to read the photograph and biographic information stored on the e-passport chip, information that would better enable officers to detect many forms of passport fraud, including impostors and the alteration or substitution of the photos and information printed in the passports, and help to determine the traveler's identity and admissibility into the United States.

DHS Has Not Implemented the Public Key Infrastructure Needed to Verify E-passport Digital Signatures

While DHS's systems conduct some validation activities to ensure the integrity of the data on the e-passport chip, it does not have adequate assurance that the data stored on the chip have not been changed since they were authored by a legitimate issuing authority—in the case of U.S. e-passports, the State Department.

In primary inspection lanes that are equipped with e-passport readers, CBP's workstations conduct a series of checks using data read from the e-passport computer chip, including the biographical data, the facial image, and the security data. First, the CBP workstation verifies that the biographical data read from the computer chip match that read from the printed biographical page. Second, the CBP workstation calculates the hash values of the data groups read from the computer chip and compares them with the hash values stored in the security data. If available, the CBP workstation will also use the digital certificate to verify the digital signature. The expiration date of the e-passport and the digital certificate are also checked. Finally, if the e-passport has been previously read by CBP, the hash value of the facial image is compared with the value stored by CBP. If this is the first time the e-passport has been encountered, the hash value is stored for future comparisons. Any mismatches are to result in an error being displayed to the CBP officer.

Further, in October 2008, DHS began to make U.S. passport data available to CBP officers in primary inspection. DHS is now receiving U.S.-issued passport data through a datashare initiative with the Department of State.

[20] GAO-07-1006.

CBP has modified its workstations to retrieve this additional information when U.S. passports, including e-passports, are processed. When CBP officers enter U.S. passport data into appropriately configured CBP workstations, the photograph of the traveler, as issued by the State Department, will be displayed to the officer.[21] As e-passports are issued by State, the corresponding information is made available to DHS through the datashare. State worked with DHS to transfer data on all valid historical U.S. passports. As more historical U.S. passport information becomes available, more photographs will be displayed to primary officers upon processing a U.S. citizen through primary inspection.

However, the key step that is missing is that the CBP workstation does not validate the legitimacy of the public key used to verify the digital signature. Such a validation would provide assurance that the public key in the document signer certificate was generated by the State Department. Without this verification, CBP does not have reasonable assurance that the e-passport data being protected by the digital signature were written by the State Department because forgers or counterfeiters could simply generate the keys necessary to digitally sign the forged data and include their own certificate in the e-passport for verification purposes. Checking the legitimacy of the certificate containing the public key that is used in the digital signature validation process would effectively mitigate this risk.

When generated, the document signer certificates are themselves digitally signed. However, CBP does not have access to the public keys necessary to validate these digital signatures. While DHS tested the functionality of storing and using this information to verify the certificates included by State and other nations on e-passports using the CBP workstation, the functionality was not implemented for operations because the infrastructure to collect and maintain the international certificate database did not exist. According to DHS officials, this function was a US-VISIT requirement, but did not get implemented, in part, because a DHS component that would be responsible for operating the public key database was never identified. DHS officials also stated that the slow performance of reading e-passports diminished the importance of implementing this function.

[21]According to CBP, it has updated its workstation software to display the additional information when conducting primary inspections at airports and at pedestrian and vehicle lanes at land ports of entry.

Not being able to check the legitimacy of the document signer certificates affects not only CBP's ability to verify the integrity and authenticity of the data written to U.S. e-passport computer chips, but also its ability to verify the integrity and authenticity of computer chip data on any country's e-passport. The United States requires all 35 participants in the Visa Waiver Program to issue e-passports, and ICAO has estimated that over 50 countries issue e-passports. Because CBP does not have the necessary information to fully validate the digital signatures that these countries generate, it does not have reasonable assurance that data signed by those countries were actually generated by the authorized passport issuance agency for that country. Hence, it cannot ensure that the integrity of the data stored on the e-passport's computer chip has been maintained.

Two key issues need to be resolved for CBP to be able to rely on data stored on e-passport computer chips. First, a database needs to be established and populated with the digital certificates needed to fully validate the digital signatures that can be accessed by CBP inspection workstations at the ports of entry. An approach needs to be developed and implemented to populate the database with the needed information, including State Department data for U.S. e-passports, that can be used to fully validate the digital signatures. According to ICAO, this information should be distributed only through secure diplomatic channels.[22] Second, CBP needs to develop and implement functionality on its inspection workstations to access the database when e-passport data are read to verify that the legitimate passport-issuing authority signed the data being relied upon. Until these two key issues are addressed, CBP will continue to lack reasonable assurance that data found on e-passport computer chips have the necessary integrity; hence, the security enhancements that could be provided by e-passport computer chip data against counterfeiting and forgery are not completely realized.

[22]One source of certificate data could be the ICAO Public Key Directory. ICAO's directory is to include only document signer certificates that have been validated by ICAO. However, there is not universal use of the ICAO Public Key Directory by e-passport-issuing countries.

Malicious Code Does Not Pose a Significant Risk to U.S. E-passport Computer Chips or Federal Computer Systems That Read Them

Protections designed into the U.S. e-passport computer chip limit the risks of malicious code being resident on the chip, a necessary precondition for a malicious code attack to occur from the chip against computer systems that read them. GPO and State have taken additional actions to decrease the likelihood that malicious code could be introduced onto the chip. While these steps do not provide complete assurance that the chips are free from malicious code, the limited communications between the e-passport chip and agency computers significantly lowers the risk that malicious code—if resident on an e-passport chip—could pose to agency computers. As we previously discussed, the e-passport's digital signature can provide reasonable identification of unauthorized modification of the user data areas—including modifications resulting from the introduction of malicious code. Finally, given that no protection can be considered foolproof, DHS still needs to address deficiencies noted in our previous work on the US-VISIT computer systems to mitigate the impact of malicious code, should it infect those systems.

U.S. E-passport Chip Designs and Manufacturing Processes Limit Exposure to Malicious Code

Security features designed into the e-passport computer chips, including the digital signature, provide protections against the introduction of malicious code onto the chip during the e-passport booklet production process. For example, among other features, the chips include physical tamper protections that aid in sensing or thwarting physical attacks, a cryptographic authentication procedure to lock the contactless interface against unauthorized access, and incorporation of a digital signature that can be used to identify any unauthorized modification of the user data areas.

Physical Tamper Protections Help Ensure against Physical Attacks on the Chip

As of 2007, NIST had not been able to identify any known cases of a malicious code attack against a computer network from a contactless chip.[23] Nevertheless, both NIST and DHS agree that it is possible and have generally identified physical tamper attacks as threats to embedded electronic chips in contactless applications such as e-passports.

Physical tamper attacks involve stripping away the chip's outer coverings, exposing the electronic circuitry on the wafer, and analyzing or monitoring chip activity by inserting electronic probes onto components etched into the wafer. In general, the aim of such an attack is to discover confidential

[23]NIST, *Guidelines for Securing Radio Frequency Identification (RFID) Systems*, SP800-98 (Gaithersburg, Md.: April 2007), 4-7.

data stored on the chip—such as cryptographic keys—which can be used to open access to the chip via the contactless interface. In terms of a malicious code threat, the purpose then would be to write malicious code onto the chip via the RF interface.

In its guide to chip-level security for contactless ICs, DHS identifies common methods used in physical tamper attacks on contactless ICs.[24] For example, after removing top layers of plastic or other coverings and uncovering the electrical surfaces of the chip, attackers could probe into the various chip layers in an attempt to understand its processing. Common methods of physical attack are those related to (1) fault introduction, (2) IC monitoring, and (3) reverse engineering. The purpose of each of these attacks is ultimately to uncover secret information—such as cryptographic keys or passwords—that would allow an attacker to open the chip for read/write access via the contactless interface. In fault introduction, attackers attempt to introduce faults randomly, at specific times during the processing, or in specific locations on the IC circuitry, to gain additional information about the chip processing during such faults, which could provide clues to the memory location of secret keys. Similarly, such clues can be uncovered using IC monitoring, where readers or probes placed on the chip's internal circuitry are used to monitor calculations or flows of data on the chip. Finally, attackers could attempt to reverse engineer the computer chip to decipher its hardware architecture and read the secret information.

In its guide, DHS identifies countermeasures for each of these types of attack. For example, protections against fault introduction include implementing sensors that detect when parameters, such as light or temperature, vary outside of expected values. If such variations are sensed, the chip may automatically reset or even disable itself. Protections against IC monitoring might include encrypting the traffic flowing along the internal circuitry so that interpretation would be difficult. Protections against physical analysis include encrypting information stored in memory and scrambling the design of the logic contained in the operating system when laid down in memory during IC creation. Well-designed security microcontrollers, with numerous security features and support for mutual authentication and sophisticated cryptographic functions, can be designed

[24]DHS Science and Technology Directorate, *Chip-Level Security for RFID Smart Cards and Tags*.

to make it extremely difficult, costly, and time-consuming for attackers to compromise.

In its solicitation for the e-passport covers, which included the computer chips, GPO specified several hardware and software requirements to protect against physical attack, including specific features to assist in protection against power and timing attacks. It also included requirements for sensors to monitor, for example, temperature and voltage variations, which might be indicative of a physical tamper attack. The chips used in the U.S. e-passports are considered security microcontrollers designed for applications where security is an important consideration, such as payment, identity, and secure access and, as such, they incorporate several features against physical tamper attacks. Both types of chips used in the e-passports have incorporated some recommended countermeasures for all of the common categories of attack identified by DHS. For example, the chips incorporate temperature and light sensors to monitor when those operating conditions vary from expected values and employ memory encryption against reverse engineering of the chip .

While it is not possible to provide complete protection against the more invasive physical attacks, the goal is to make the cost of mounting such an attack prohibitive. While the threat of physical attack to the embedded chips in the e-passport cannot be completely discounted, the security features incorporated into the microcontrollers in U.S. e-passports make a physical tamper attack impractical.

Cryptographic-Based Authentication Procedures Control Contactless Access to the Chip during Booklet Production

During production of the e-passport covers, the manufacturers, their subcontractors, and at GPO and State—or anywhere en route between these sites—the chips are protected from unauthorized access through the contactless interface by authentication procedures based on cryptography.

The manufacturing and personalization process for the e-passport booklet is complex and involves many handoffs between different sites, companies, and sometimes different countries. For example, while both e-passport cover contractors originate chip manufacturing in Europe, they also send the chips to various third-party companies in Asia for additional manufacturing steps. The overall process can take almost 2 years from the time the chip leaves the fabrication plant until it is finally issued by the State Department to a bearer as part of an e-passport.

During the production life cycle of the e-passport book—from chip creation at the chip manufacturers through to personalization by State—contactless access to the chip is controlled by a symmetric cryptography

authentication procedure. Cryptographic algorithms provide different measures of strength, depending on the algorithm and the overall length of the keys involved. According to NIST estimates, the version used on the e-passports can, at best, provide protection from a brute force attack until 2030.[25]

This locking mechanism not only controls access to the chip, but differentially allows only certain functions to be performed.

Other Design and Manufacturing Steps Help Mitigate the Risk from Malicious Code

Several other design features limit the chance that malicious code could be placed on the chip. For example, according to GPO, an additional step used to protect the e-passport chips from unauthorized access during the manufacturing process takes advantage of standard industry practice to not include customer identification with chips during production runs. During the chip-manufacturing process, an anonymous cataloging scheme is employed that makes it difficult to associate bulk lots of chips with their destined applications. Therefore, on the production floor, it cannot be determined which chips are to be used in U.S. e-passports.

In addition, after the chips are manufactured and incorporated into the e-passport cover, steps are taken by GPO and State to protect the user data areas of the chip from tampering. First, as part of its formatting procedures to prepare the chips for personalization, GPO ensures that the user data area is free from any data—including malicious code. During the formatting of the user data area, if any memory cell is found to be defective, then GPO discards the e-passport booklet. Therefore, any malicious code successfully implanted within the user data area after manufacture and through any of the chip's travels through its production cycle up until it arrived at GPO would be erased from the chip.

As we previously discussed, during the e-passport personalization process, a digital signature is applied to the data to help assure the integrity and authenticity of the data written to the chip. One of the benefits of the digital signature is that any insertion of malicious code into, for example, the bearer's digital image would be caught, provided the digital signature is fully and properly verified. Such a successful check would provide reasonable assurance that malicious code has not been inserted into the user data areas of the chip memory since it was personalized by State.

[25]See NIST, *Recommendation for Key Management—Part 1: General*, SP 800-57 (Gaithersburg, Md.: March 2007).

Limited Communications between the E-passport Chip and Agency Computers and Security Certifications and Reviews Mitigate Risks Posed by Malicious Code

GPO and State have taken steps to gain confidence that their e-passport computer chips are secure. While these steps do not provide complete assurance that the chips are free from malicious code, the limited communications between the e-passport chip and agency computers significantly lowers the risk that malicious code that could be resident on an e-passport chip could pose to agency computers. The chips have been tested for both interoperability and conformance to ICAO specifications and exercised by GPO as part of their formatting process. The chips have undergone a formal, independent process to validate some aspects of their security. GPO and State also periodically conduct security reviews of the chip manufacturer sites.

Controls on the Interface between the E-passport Computer Chip and Agency Computers Limit the Opportunities for Transfer of Malicious Code

One key feature that mitigates the risk that malicious code on the chip could pose to agency computers is the highly restricted nature of the data exchange between the chip and agency computers during the reading of the e-passport. The e-passport computer chip adheres to ISO 14443 and ISO 7816-4 for communications through the contactless interface. The standards restrict the computer chip to a slave role whereby it responds only to a specific set of commands with known and limited response data. Because the chip cannot independently initiate communication with a reader, the flow of data from the chip to the reader and host computer can be precisely controlled and limited to only what is expected by the host computer.

The result is that opportunities for the covert embedding of malicious code within data transferred from the chip to agency computers are correspondingly limited. For example, the passport number, bearer's name, and date of birth are data sets restricted to a well-defined set of characters and are of fixed length. Consequently, if a reader accepts inputs only within these bounds, it will limit the risk posed by malicious code. The digital image of the bearer is the only data set transferred that is of enough size to provide for opportunities to hide malicious code. The image is formatted according to a standard graphics format that facilitates integrity checking of its contents. According to DHS officials, when e-passports are read, the data from the chip are verified both by the e-passport reader as well as by the agency host computer before the data are processed.

Testing Helps to Verify Proper Functioning of E-passport Chip Communications

Prior to contract award, and at various points thereafter, the U.S. e-passport chips have undergone testing for a variety of purposes.

According to GPO officials, the solicitation for the e-passport covers was based on State Department requirements for specific functionality, security, performance, and availability. For example, it included requirements for the chip to meet ISO 14443 communications and ISO 7816-4 command set standards and other standard specifications. As part of the award selection process, GPO, State, NIST, and NSA conducted testing of sample books from each bidder to determine whether they would meet requirements as specified in the request for proposal.

During pre-award testing, for example, GPO ran initial tests to ensure basic functionality as specified by ISO 7816-4, including the ability to initialize, read, write, and lock the chip. GPO also ensured that each e-passport cover was of the correct form and thickness so that it could mechanically pass through its production equipment suite. The sample booklets then went to State, which conducted tests to ensure the books could work with its personalization systems.

According to NIST officials, they performed electronic testing that looked at the potential for eavesdropping, jamming, and remote activation (skimming). For eavesdropping, the test was conducted to determine whether the legitimate communication could be intercepted, but no attempt was made to see if the encrypted communication could be understood. For jamming, the purpose was to determine whether legitimate communications with the chip could be prevented. For remote activation, the purpose was to determine the distance from which a reader could elicit a response from the chip, but no attempt was made to test the basic access control or to read the data on the chip. NIST also conducted different types of durability tests including static bend, dynamic bend, climate, chemical resistance, physical protection of the integrated circuit chip, and electromagnetic testing. None of NIST's tests were designed to test for the presence of malicious code on the chip. While the tests exercised some portions of ISO 14443 and ISO 7816-4, NIST did not conduct any tests to ensure full conformance with these standards.

NSA officials stated that they conducted electronic testing of the booklet, but this was confined to radio frequency testing and shielding testing specifically tasked by GPO to evaluate the susceptibility of the booklet to skimming by looking at the distance over which the booklet's chip could become energized. NSA performed no substantive tests of communication with the chip and no testing at all with regard to malicious code.

As part of GPO's normal pre-personalization processing, GPO exercises and tests each chip's functionality to verify, among other things, the

correct reading and writing of every chip. GPO's processing does not systematically exercise every chip function or the full ISO 7816-4 command set and associated error handling. GPO officials said that while they test the basic functionality of the chip as they proceed through the pre-personalization processing, full ISO 14443 communications and ISO 7816-4 command set processing—including ensuring that all error handling is performed correctly—is done as part of the international ICAO interoperability and conformance tests held approximately every 2 years. The State Department is the official U.S. representative to these tests, although GPO frequently participates, by request, in support of State. According to ICAO, the interoperability and conformance tests are intended to accomplish two things. First, they ensure that e-passports from different countries can be read by readers provided by multiple vendors. Second, they ensure compliance with various aspects of the ISO 14443 communication and ISO 7816-4 command set standards. The U.S e-passport chips have been part of some of the interoperability and conformance tests that have been run in the last several years.[26]

All these tests provide important assurances for their stated purposes by exercising functionality, in particular the limited e-passport chip communications, that helps to protect against the risk of malicious code. In general though, such testing is limited to verifying functionality and cannot provide absolute assurance that malicious code has not been implanted onto the e-passport computer chip.

Security Certifications and Security Reviews Provide Some Assurance That Computer Chips Are Free from Malicious Code

The creation of the computer chip used in U.S. e-passports is a complex process that involves many components created by different entities. Because the U.S. government does not control the entire supply chain for all the components on the chip, it relies on security features provided by the chip component suppliers, the extent to which these suppliers test and

[26]According to GPO officials, because of competitive pressures within the smart card industry, the chip manufacturers will often modify their chips to enhance their processing. These changes may involve chip circuitry changes, for example, to increase the speed of the chip's processing. Sometimes the chip operating system needs to be modified as well to mesh with the circuitry changes. GPO officials stated that State generally likes to take advantage of these enhanced chips and use them if it can. Therefore, sometimes the chip manufacturer will deliver samples of enhanced chips that GPO will evaluate separately from the production line. If agreed to by the Configuration Change Board—on which both State and GPO sit—the enhanced version of the chip may be folded into production. In those cases where a chip change is significant, it may trigger the need to participate in the full ICAO interoperability and conformance testing. Revalidation with NIST and others could also be needed.

certify their products, and the extent to which these suppliers develop and produce the chips in a secure manner.

Some Aspects of the Security of the Chips Were Certified Using Common Criteria

NIST guidelines state that federal agencies should give substantial consideration in IT procurements to products that have been evaluated and tested by accredited laboratories against appropriate security specifications and requirements.[27] One established mechanism for providing security evaluation and testing services for commercial-off-the-shelf hardware, software, or firmware is Common Criteria. Common Criteria certifications are a well-known international standard mechanism for validating and documenting various security aspects of IT products. Evaluations are performed by accredited Common Criteria testing laboratories whose results are then certified by a validation body. In the case of the chips used in the U.S. e-passports, selected security features of their hardware components were evaluated using Common Criteria by a recognized European laboratory and certified by Germany's Common Criteria certification body.

In its solicitation for the e-passport covers, including the computer chips, GPO specified that preference will be given to computer chips that are certified at Common Criteria EAL 4+ against a Common Criteria-compliant Protection Profile.[28] According to Common Criteria definitions, an EAL 4 rating is intended to provide a moderate to high level of independently assured security. To achieve this rating, the testing lab must conduct a variety of structured activities, including an analysis of the security functions of the product using a complete interface specification and both the high-level and low-level design of the specific features of the product being tested, review and confirmation of any vendor testing that was conducted, and conduct of an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

[27]NIST, *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, SP800-23 (Gaithersburg, Md.: August 2000).

[28]According to Common Criteria, a Protection Profile is an implementation-independent statement of security needs for an IT product. A "+" designation on an EAL rating indicates that security requirements beyond those specified in the Common Criteria standard were included in the target of evaluation and also satisfied.

The computer chips selected for use in the e-passports each had received an EAL 5+ rating against a compliant Protection Profile. According to Common Criteria, an EAL 5 rating incorporates all of the EAL 4 requirements and, in addition, requires, among other things, semiformal design descriptions, a more structured architecture, covert channel analysis, and improved mechanisms that provide confidence that the particular implementation of the product being evaluated has not been tampered with during development. Specific security features evaluated to achieve the EAL 5 rating include many useful in helping to prevent the introduction of malicious code. Examples of these include support for cryptographic functions, protections against physical manipulation, and features to ensure correct operating conditions for the chip.

However, a key software component of the chip—the operating system—was excluded from the evaluation. The operating system on the chip implements and controls, among other functions, the ISO 7816-4 command set that is the primary means of communication between the chip and the outside world—including agency computers.

Under Common Criteria, it is not uncommon for critical components of a product to be excluded for particular evaluations. In particular, the exclusion of important software components, such as the operating system, from the Common Criteria evaluation of hardware features is not unusual because the higher-level software embedded on chips is often a third-party product and not designed by the chip manufacturer itself. The chip manufacturer is typically not responsible for undertaking a Common Criteria evaluation of third-party embedded software used on its chips. Typically, it would be up to the software provider to get its product certified using Common Criteria. However, this is an expensive and time-consuming process. Hence, care needs to be taken with Common Criteria certifications that can be meaningfully understood only within the context of the specific subset of security functions included in the evaluation.

We have previously noted that one of the challenges in using the National Information Assurance Partnership is the difficulty in matching agencies' needs with the availability of NIAP-evaluated products.[29] According to Infineon and Gemalto officials, back in 2006 when the request for proposal for the e-passport covers was issued, there was no Protection Profile available that covered the operating systems of such chips. Since that

[29]GAO-06-392.

time, however, Common Criteria operating systems suitable for use on smart cards have become available. According to GPO officials, Infineon provides such chips today, and GPO is in the process of transitioning them into production so that, at least for the Infineon line, the e-passports will include a Common Criteria-certified operating system.

The user operating system contains arguably most of the software functioning on the chip. Therefore, obtaining assurance as to its secure functioning and freedom from malicious code is an important activity. However, given the highly restricted nature of the current communications between the chip and agency computers, we do not see the lack of Common Criteria certification of the chip operating system as significantly increasing the risk to agency computers from malicious code.[30]

While Common Criteria certification confers some assurance regarding the specific security functions included in the evaluation, care must be taken in extending that assurance into confidence in the overall security of the product for its intended use. GAO has previously reported that within its limitations, the Common Criteria process provides benefits. However, the lack of performance measures leaves questions unanswered as to its true effectiveness.[31] The use of commercial products that have been independently tested and evaluated is only a part of a security solution that contributes to the overall information assurance of a product.

GPO Has Conducted Reviews of the E-passport Computer Chip Manufacturing Sites

Prior to contract award, and periodically thereafter, GPO—sometimes accompanied by the State Department—conducted on-site security reviews of the companies that manufacture the e-passport chips and the covers, and of some of their subcontractors. According to GPO officials, its reviews are concerned with not just security risks, but also with other risks—for example, the extent to which a site performs continuity of operations planning or the risk that a single source of supply for one of the components might pose a risk to the delivery of the components. In

[30]If the communications between the chip and agency computers were extended beyond their current limited scope, the risk from malicious code on the chip would need to be reevaluated. For future use, the ICAO specification does allow for additional data sets to be passed across this interface, for example, fingerprint data and other biometrics.

[31]GAO-06-392.

conducting the security reviews, GPO officials stated that they make an attempt to visit every vendor involved in the production of the e-passport booklet, including, for example, the security ink suppliers, paper providers, thread providers, and the chip providers. The sites are spread across several countries, and within some countries there may be multiple sites. For example, for both Infineon and Gemalto, production of the chips involves several sites within Europe.

These reviews employ an American National Standards Institute (ANSI) standard for security product manufacturing that covers a variety of risk areas, including information, IT, material, supply chain, physical intrusion, personnel, and disaster recovery.[32] For example, the standard addresses such concerns as proper controlled access to restricted areas within a facility. During the security review, GPO generally gets a high-level briefing from the company and talks with staff at the site. According to GPO officials, they have reviewed almost every site twice since March 2006. In recent security reviews of the chip manufacturing sites, both Infineon and NXP were found to be in compliance with their own stated security policies and meeting the Class 1 level of the ANSI standard.

From the security reviews, GPO can get some sense of some of the protections in place at the development sites—for example, access control to development areas and security awareness training. GPO learned through its reviews, for example, that Gemalto has an access control policy wherein development premises are divided into secure and nonsecure zones, and the operating system development is in the secured zone. This provides some assurance that since physical access to the software destined for the chips is controlled, opportunities for the inclusion of malicious code can be limited.

[32]ANSI/NASPO, *Security Assurance Standards for the Document and Product Security Industry*, ANSI/NASPO-SA-v3.0P-2005 (Washington, D.C.: March 2007).

To Further Mitigate the Effect of a Malicious Code Attack, DHS Needs to Address Previously Noted Weaknesses in US-VISIT Computer Systems

Given that there can be no guarantees against a malicious code attack originating from the e-passport computer chip, agency systems need to have a strong security posture, in accordance with federal government standards. We have previously reported on weaknesses in DHS's US-VISIT computer systems, which could increase the ability of malicious code to infect and propagate through agency computers.[33] Weaknesses, such as unpatched software vulnerabilities, can invite a malicious code attack and enhance the ability of the attack to spread across the network by leaving important linkages within the network unprotected. DHS needs to address these deficiencies to ensure that any malicious code resident on the e-passport chip and read onto DHS computers can be contained and its effect minimized.

One of the strong recommendations from NIST is that computer systems run antivirus software, which scans systems' files and memory spaces for known malware. NIST strongly recommends the use of antivirus software to identify and protect against malicious code. Detecting such code prior to its further spread can limit a malicious code infection and protect downstream systems. According to DHS officials, workstations that control the interface with the chip are protected by antivirus software, which includes access protections, buffer overflow protections, and scanning of files as they are accessed.

One of the key weaknesses in US-VISIT that we found in 2007—patch management—is of particular concern with respect to malicious code that could be read from an e-passport. Malicious code often attacks systems by exploiting vulnerabilities in operating systems, services, and applications. When software vulnerabilities are discovered, the software vendor may develop and distribute a patch or workaround to mitigate the vulnerability. Patch management is, therefore, an important element in mitigating the risks associated with malicious code and the vulnerabilities they depend on. NIST's, NSA's, and DHS's own policies stress the importance of keeping computer systems up to date with security patches. Outdated and unsupported software is more vulnerable to attacks and exploitation. NIST guidelines state that applying patches is one of the most effective ways of reducing the risk of malware incidents.[34]

[33]GAO, *Information Security: Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program*, GAO-07-870 (Washington, D.C.: July 13, 2007).

[34]NIST SP800-83.

In our prior report, we noted that while DHS has taken steps to ensure that patches for the workstations' operating system were kept up to date, some workstations at the ports of entry did not consistently maintain secure configurations. As a result, vulnerabilities left unpatched on those systems increase the chance of malicious code being executed should it get ingested.[35] According to DHS officials, they are in the midst of upgrading workstations to a version of Microsoft Windows that contains features to help prevent the execution of malicious code—for example, special services to detect and prevent the execution of code from the data areas. DHS needs to ensure that it completes the upgrade of the workstations and that such services are enabled on workstations reading data from the e-passport computer chips.

Conclusions

Ensuring the integrity of passports requires continual vigilance so that they can continue to be used to support the critical border security mission—facilitating the travel of those who are entitled to enter the United States while preventing the entry of those who are not. A well-designed passport has limited utility if it is not well produced or border officers do not utilize the available security features to detect attempts to fraudulently enter the United States. While U.S. e-passport covers, including the embedded computer chip, are manufactured by foreign companies, State's public key infrastructure, which is used to generate digital signatures during the personalization process for each issued passport, can provide reasonable assurance that the data written onto the chip were authored by State and have not been altered. However, DHS has not implemented the capabilities needed for CBP officers to fully utilize this security feature. Without e-passport readers at the ports of entry or a system that allows for the full validation of digital signatures on e-passports, CBP officers' inspection of not only U.S. e-passports, but also of e-passports issued by foreign countries, including those participating in the visa waiver program, is affected. Without these capabilities, the additional security against forgery and counterfeiting that could be provided by the inclusion of computer chips on e-passports issued by the United States and foreign countries, including those participating in the visa waiver program, is not fully realized.

[35]DHS has provided evidence to us that it has addressed some of the weaknesses noted in patch management of its systems. However, others remain unresolved.

While the use of e-passports and radio frequency communications represents another potential attack vector to federal computer systems, the risk posed by the transmission of malicious code on U.S. e-passports is not significant. The U.S. e-passport chips have security features that minimize the threat of tampering during the manufacturing and production process. GPO and State have also taken steps to assure the security of the embedded computer chips in U.S. e-passports. Because the communications between e-passport computer chips and federal computer systems have been designed to be limited, the opportunities for transfer of malicious code are correspondingly limited. Combined, these measures significantly reduce the risks from someone using e-passport computer chips as a conveyance for malicious code to federal computer systems.

Recommendations for Executive Action

To ensure that border officers can more fully utilize the security features of electronic passports, we recommend that the Secretary of Homeland Security take the following two actions to provide greater assurance that electronic passport data were written by the issuing nation and have not been altered or forged:

- Design and implement the systems functionality and databases needed to fully verify electronic passport digital signatures at U.S. ports of entry.
- In coordination with the Secretary of State, develop and implement an approach to obtain the digital certificates necessary to validate the digital signatures on U.S. and other nations' electronic passports.

Agency Comments and Our Evaluation

We provided draft copies of this report to the Secretaries of State and Homeland Security and to the Public Printer at the Government Printing Office for review and comment. We received formal written comments from the Department of Homeland Security, which are reprinted in appendix III. In its comments, DHS concurred with our recommendations. However, DHS believes that the report incorrectly portrays CBP's ability to detect the fraudulent use of U.S. passports. DHS cites the ability of CBP's officers to access U.S. passport application data from State and use it to detect impostors and altered data in U.S. passports. We agree that providing State passport data to CBP officers during the inspection process enhances their ability to detect the fraudulent use of U.S. e-passports. Nevertheless, while State has expended significant resources to produce an e-passport that includes contactless chip technology and public key cryptography to help prevent counterfeiting and forgery, DHS

has not implemented the capabilities to fully utilize these security features and is not fully realizing the security benefits of the inclusion of electronic technology on e-passports.

We received informal comments from the State Department. State believes that the draft report presents a comprehensive and balanced assessment of the security of the e-passport design. We also received technical comments from State, GPO, and DHS, which we incorporated in the report, as appropriate.

As we agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the report date. At that time, we will send copies of this report to the Secretaries of State and Homeland Security and the Public Printer. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-4499 or barkakatin@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix IV.

Dr. Nabajyoti Barkakati
Chief Technologist
Director, Center for Technology and Engineering

Appendix I: Scope and Methodology

To determine whether e-passport chips can be altered or forged so that a traveler could fraudulently enter the United States, we interviewed officials from State's Bureau of Consular Affairs and reviewed State Department policies, procedures, and guidance documents regarding the public key infrastructure (PKI) used to protect the data on the e-passport computer chip and assessed them against relevant International Civil Aviation Organization (ICAO) and National Institute of Standards and Technology (NIST) standards and guidelines. We interviewed officials at one passport issuance agency and reviewed systems documentation to understand how U.S. e-passports are personalized. We determined the extent to which U.S. e-passport computer chips are inspected at U.S. ports of entry by interviewing Department of Homeland Security (DHS) officials and reviewing documentation regarding the systems and procedures used to inspect e-passports at the ports of entry. Within DHS, we met with officials from the U.S Customs and Border Protection (CBP), the Screening Coordination Office, and the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program office.

To determine whether malicious code on the e-passport chips poses a risk to national security, we determined how U.S. e-passport computer chips are manufactured and incorporated into the production of blank U.S. e-passport booklets based on interviews with the Government Printing Office (GPO) and manufacturer officials and our reviews of GPO documentation. We met with officials from NIST and the National Counterterrorism Center to determine the level of threat that exists to U.S. e-passports. We interviewed GPO and State officials and reviewed documentation that describes the U.S. e-passport computer chip architecture and operations. We reviewed documents governing the manufacturing of the blank e-passport covers, including GPO contracts with the manufacturers and the memorandum of understanding between GPO and State. We determined that for malicious code on the e-passport computer chip to be a risk to agency computers, it must first get on the chip, then get transferred off the chip and onto agency computers, and then subsequently get executed. Therefore, we identified and evaluated protections that have been designed into the e-passport computer chip to reduce the possibility of malicious code being introduced onto the chip, controls in place to limit the transfer of malicious code off of the chip and onto agency computers, and the security posture of the agency computer systems interfacing with the e-passport chip. We also reviewed the results of testing conducted on the e-passport computer chips by GPO, NIST, the National Security Agency, and ICAO, and through the Common Criteria program. We discussed and reviewed the results of security reviews conducted by GPO. We met with GPO, State, and CBP officials to

understand how each agency interacts with the e-passport computer chips and the potential risk that malicious code could pose to these agencies.

We conducted this performance audit from June 2008 to January 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

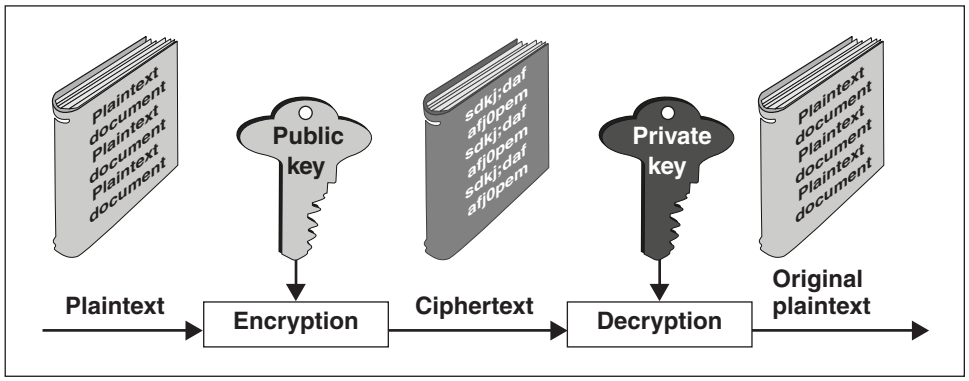
Appendix II: Digital Signatures and Public Key Cryptography

Cryptography is the transformation of ordinary data (commonly referred to as plaintext) into a code form (ciphertext) and back into plaintext using a special value known as a key and a mathematical process called an algorithm. Cryptography can be used on data to (1) hide their information content, (2) prevent their undetected modification, and/or (3) prevent their unauthorized use. A basic premise in cryptography is that good systems depend only on the secrecy of the key used to perform the operations rather than on any attempt to keep the algorithm secret. The algorithms used to perform most cryptographic operations over the Internet are well known; however, because the keys used by these algorithms are kept secret, the process is considered secure.

The basis of PKI's security assurances is a sophisticated cryptographic technique known as public key cryptography, which employs algorithms designed so that the key that is used to encrypt plaintext cannot be calculated from the key that is used to decrypt the ciphertext.[1] These two keys complement each other in such a way that when one key is used for encryption, only the other key can decrypt the ciphertext. One of these keys is kept private and is known as the private key, while the other key is widely published and is referred to as the public key. When used as shown in figure 4, public key cryptography can help to assure data confidentiality because only the private key can be used to decrypt the information encrypted using the public key. When used as shown in figure 5, public key cryptography can help provide authentication, nonrepudiation, and data integrity because the public key will only work to decrypt the information if it was encrypted using the private key. In both cases, ensuring the security of the private key is vital to providing the necessary security protections. If the private key is compromised, there can be little assurance that data confidentiality, authentication, and data integrity can be provided by the PKI.

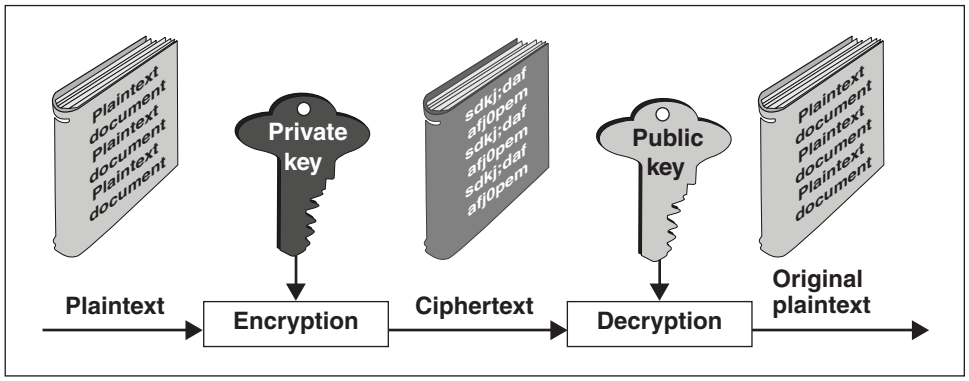
[1]A more comprehensive discussion of public key infrastructure technology can be found in GAO, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, GAO-01-277 (Washington, D.C.: Feb. 26, 2001), and NIST, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, SP 800-32 (Feb. 26, 2001).

Figure 4: Using Public Key Cryptography to Provide Data Confidentiality



Source: GAO analysis and Corel Galley (images).

Figure 5: Using Public Key Cryptography to Provide Data Integrity and Authentication



Source: GAO analysis and Corel Galley (images).

Cryptographic techniques are used to generate and manage the key pairs (a public key and private key), which are in turn used to create electronic "certificates," which link an individual or entity, such as State, to its public key. These certificates are then used to verify digital signatures (providing authentication and data integrity).

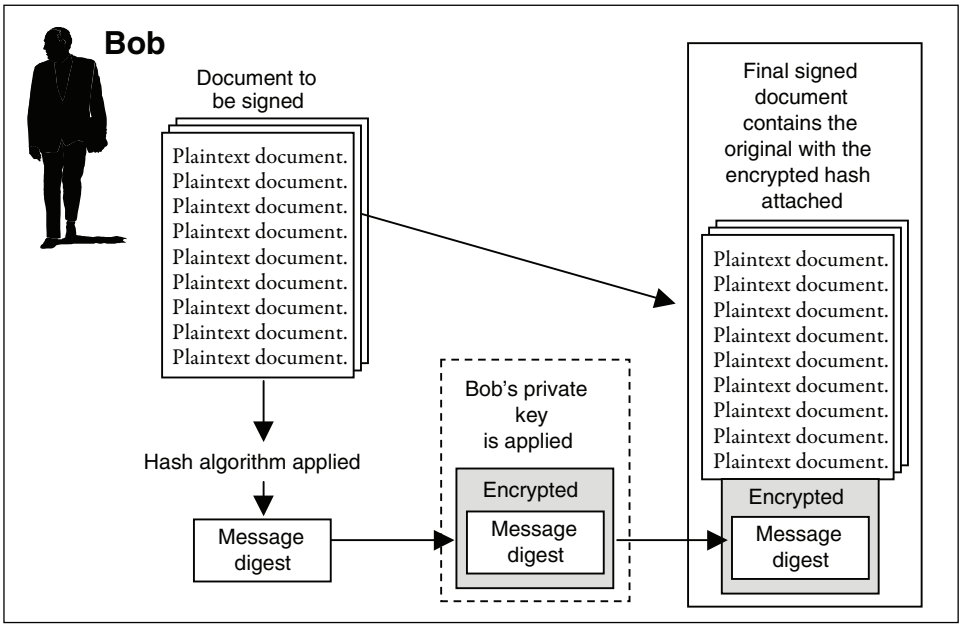
Creating and Using Digital Signatures

Public key cryptography can be used to create a digital signature for a message or transaction, thereby providing authentication, data integrity, and nonrepudiation. For example, if Bob wishes to digitally sign an electronic document, he can use his private key to encrypt it. His public key is freely available, so anyone with access to his public key can decrypt

the document. Although this seems backward because anyone can read what is encrypted, the fact that Bob's private key is held only by Bob provides the basis for Bob's digital signature. If Alice can successfully decrypt the document using Bob's public key, then she knows that the message came from Bob because only he has access to the corresponding private key. Of course, this assumes that (1) Bob has sole control over his private signing key and (2) Alice is sure that the public key used to validate Bob's messages really belongs to Bob.

Digital signature systems use a two-step process, as shown in figure 6. First, a hash algorithm is used to condense the data into a message digest. Second, the message digest is encrypted using Bob's private signing key to create a digital signature. Because the message digest will be different for each signature, each signature will also be unique, and using a good hash algorithm, it is computationally infeasible to find another message that will generate the same message digest.

Figure 6: Creating a Digital Signature

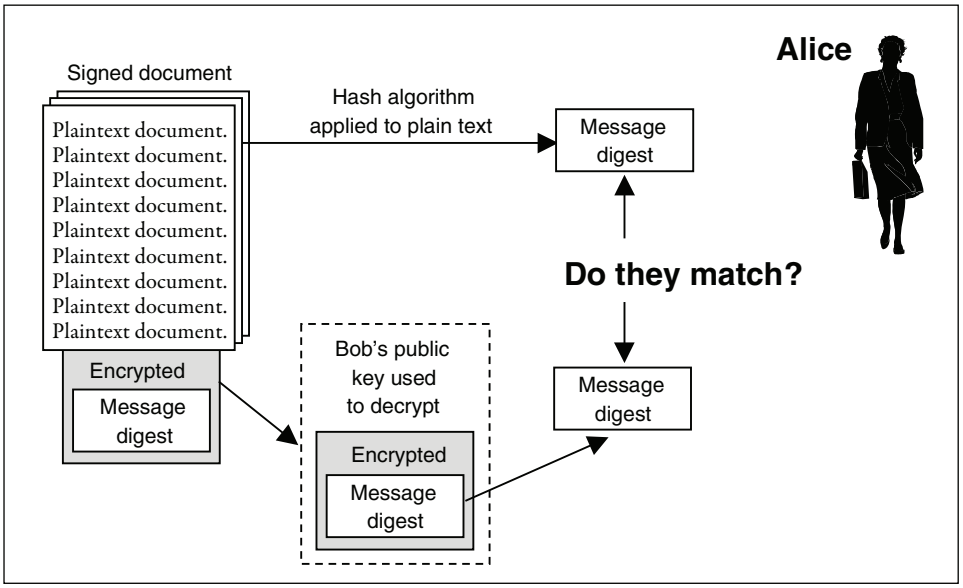


Source: National Institute of Standards and Technology.

Alice (or anyone wishing to verify the document) can compute the message digest of the document and decrypt the signature using Bob's public key, as shown in figure 7. Assuming that the message digests match, Alice then has three kinds of security assurance. First, that Bob actually

signed the document (authentication). Second, the digital signature ensures that Bob in fact sent the message (nonrepudiation). And third, because the message digest would have changed if anything in the message had been modified, Alice knows that no one tampered with the contents of the document after Bob signed it (data integrity). Again, this assumes that (1) Bob has sole control over his private signing key and (2) Alice is sure that the public key used to validate Bob's messages really belongs to Bob.

Figure 7: Verifying a Digital Signature



Source: National Institute of Standards and Technology.

Digital Certificates and Certification Authorities Link Public Keys with Specific Users to Convey Trust

A digital certificate is an electronic credential that guarantees the association between a public key and a specific entity. It is created by placing the entity's name, the entity's public key, and certain other identifying information in a small electronic document that is stored in a directory or other database.

Directories may be publicly available repositories kept on servers that act like telephone books for users to look up others' public keys. The digital certificate itself is created by a trusted third party called a certification authority, which digitally signs the certificate, thus providing assurance that the public key contained in the certificate does indeed belong to the individual or organization named in the certificate. A certification

authority is responsible for managing digital certificates. The purpose of the certification authority is to oversee the generation, distribution, renewal, revocation, and suspension of digital certificates. The certification authority may set restrictions on a certificate, such as the starting date for which the certificate is valid as well as its expiration date. It is at times necessary to revoke digital certificates before their established expiration dates, for example, when the private key is compromised. Therefore, the certification authority is also responsible for providing certificate status information and may publish a certificate revocation list in a directory or maintain an online status-checking mechanism. The PKI software in the user's computer can verify that the certificate is valid by first verifying that the certificate has not expired and then by assuring that it has not been revoked or suspended.

Appendix III: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

December 10, 2009

Dr. Nabajyoti Barkakati
Director
Center for Technology and Engineering
Applied Research and Methods
Government Accountability Office
Washington, DC 20548

Dear Dr. Barkakati:

Thank you for providing us with a copy of the Government Accountability Office's (GAO) draft report entitled, "BORDER SECURITY: Better Usage of Electronic Passport Security Features Could Improve Fraud Detection" (GAO-10-96).

DHS and U.S. Customs and Border Protection (CBP) concur with the GAO's findings and recommendations; however a key aspect to resolving the issues relates to work outside of CBP's control. In an effort to satisfy the intent of the GAO's recommendations, CBP agrees to work with the Department of State (State) on a plan to validate electronic signatures and to work with them to establish a directory of digital certifications for U.S passports. In addition, CBP in coordination with the Department of Homeland Security (DHS) and State agrees to cost out the projects, request necessary funding, and determine feasibility and costs to obtain similar signatures for non-USA e-passports.

We wish to point out the report leaves a seriously false impression with regard to CBP's ability to detect fraudulent use of ***U.S. passports***. While it might be true that the inability to read the chip in ***foreign*** passports limits the ability of CBP officers to ***quickly*** detect ***foreign*** passport fraud, the fact that CBP officers verify ***with the application data from the State Department*** - each and every U.S. passport presented – means that imposters and data altered documents are actually caught on a very regular basis now. It is also important to note that our ability to verify with the U.S. passport application data from State means that the CBP officer ***sees the exact same information*** they would see if they opened the chip on the U.S. passport. CBP has had complete historical passport application data for several months now.

Although there is an acknowledgement of this verification of U.S. passports in the report – it is but one mention against multiple references throughout the report which leaves the seriously false impression that CBP officers are unable to detect fraudulent use of U.S. passports if they don't read the chip.

The following is our response to the recommendations.

Recommendation 1: Design and implement the systems functionality and databases needed to fully verify electronic passport digital signatures at U.S. ports of entry

Response: Concur. CBP will work with the State Department on a plan to validate the digital signatures of U.S. passports at Ports of Entry. This plan will serve as a basis to cost out the project to request funding. In addition, CBP will work with DHS and State to determine the feasibility and costs to obtain the digital signatures of other nations' electronic passports and utilize them accordingly.

Recommendation 2: In coordination with the Secretary of State, develop and implement an approach to obtain the digital certificates necessary to validate the digital signatures on U.S. and other nations' electronic passports.

Response: Concur. CBP will work with the Department of State on a plan to establish a directory of digital certificates for U.S. passports in such a way that CBP can utilize it for validating the electronic US passport digital signatures. This plan will serve as a basis to cost out the project to request funding. In addition, CBP will work with DHS and State to determine the feasibility and costs to obtain the digital signatures of other nations' electronic passports.

Thank you for the opportunity to provide comments to the draft report.

Sincerely,

Jerald E. Levine
Director
Departmental GAO/OIG Liaison Office

Appendix IV: Contact and Staff Acknowledgments

GAO Contact

Dr. Nabajyoti Barkakati, (202) 512-4499 or barkakatin@gao.gov

Staff Acknowledgments

In addition to the contact named above, William Carrigg, Richard Hung, and John C. Martin made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548