

---

**CONSIDERATION OF SMART CARDS AS THE  
DOD PKI AUTHENTICATION DEVICE CARRIER**

---

**Special Report to Congress**

**10 January 2000**

**Table of Contents**

Executive Summary ..... iv

1. Introduction..... 1

    1.1 Purpose..... 2

    1.2 Background ..... 2

    1.3 Approach..... 3

    1.4 Overview of Report Structure ..... 3

2. Minimum Mandatory Requirements ..... 4

    2.1 FIPS 140-1 Level 2 Validation ..... 4

    2.2 Signature Algorithms ..... 4

    2.3 Key Sizes..... 4

    2.4 Quality of Algorithm Parameters ..... 5

    2.5 Private Key Protection..... 5

    2.6 Private Key Generation..... 5

    2.7 Private Key Activation..... 5

    2.8 Private Key Deactivation..... 6

    2.9 Private Key Destruction..... 6

3. Description of Cryptographic Token Technologies..... 7

    3.1 Smart Cards..... 7

    3.2 USB Tokens ..... 8

    3.3 PCMCIA Cards ..... 9

    3.4 Diskettes..... 10

    3.5 Other Token Technologies..... 10

4. Compliance with Minimum Mandatory Requirements ..... 11

    4.1 FIPS 140-1 Level 2 Validation ..... 11

    4.2 Signature Algorithms ..... 11

    4.3 Key Sizes..... 12

    4.4 Quality of Algorithm Parameters ..... 12

    4.5 Private Key Protection..... 12

    4.6 Private Key Generation..... 12

    4.7 Private Key Activation..... 12

    4.8 Private Key Deactivation..... 13

    4.9 Private Key Destruction..... 13

5. Assessment Against Additional Factors ..... 14

    5.1 Cost of the Token..... 14

    5.2 Cost of the Reader..... 15

    5.3 Initial Cost of Ownership ..... 15

    5.4 Support for Photo ID..... 16

    5.5 Support for Other Technologies..... 16

    5.6 Support for Multiple Applications ..... 17

    5.7 COTS Availability ..... 17

    5.8 DoD Infrastructure—Development..... 18

    5.9 Interoperability..... 18

    5.10 Convergence with Telecommunications Industry ..... 18

---

5.11 Form Factor—Convenience .....	19
5.12 Portability.....	19
5.13 Durability .....	19
5.14 Onboard Memory Capacity.....	20
5.15 Technology Maturity.....	20
6. Summary of Findings.....	21
Appendix A: References .....	A-1
Appendix B: Description of DoD PKI.....	B-1
Appendix C: Synopsis of FIPS Publication 140-1 .....	C-1
Appendix D: Acronym List and Glossary of Terms .....	D-1

## **Executive Summary**

As the Department of Defense (DoD) strives to achieve knowledge superiority and to provide critical information to the warfighter, it recognizes the need for robust information assurance capabilities to protect the confidentiality, integrity, and authenticity of this information. To this end, the DoD is implementing a public key infrastructure (PKI), a key and certificate management infrastructure designed to support confidentiality, integrity, availability, authentication, and access control in computer networks. This PKI will require authentication device carriers (i.e., tokens) to store and carry cryptographic keys and certificates supporting user identity authentication.

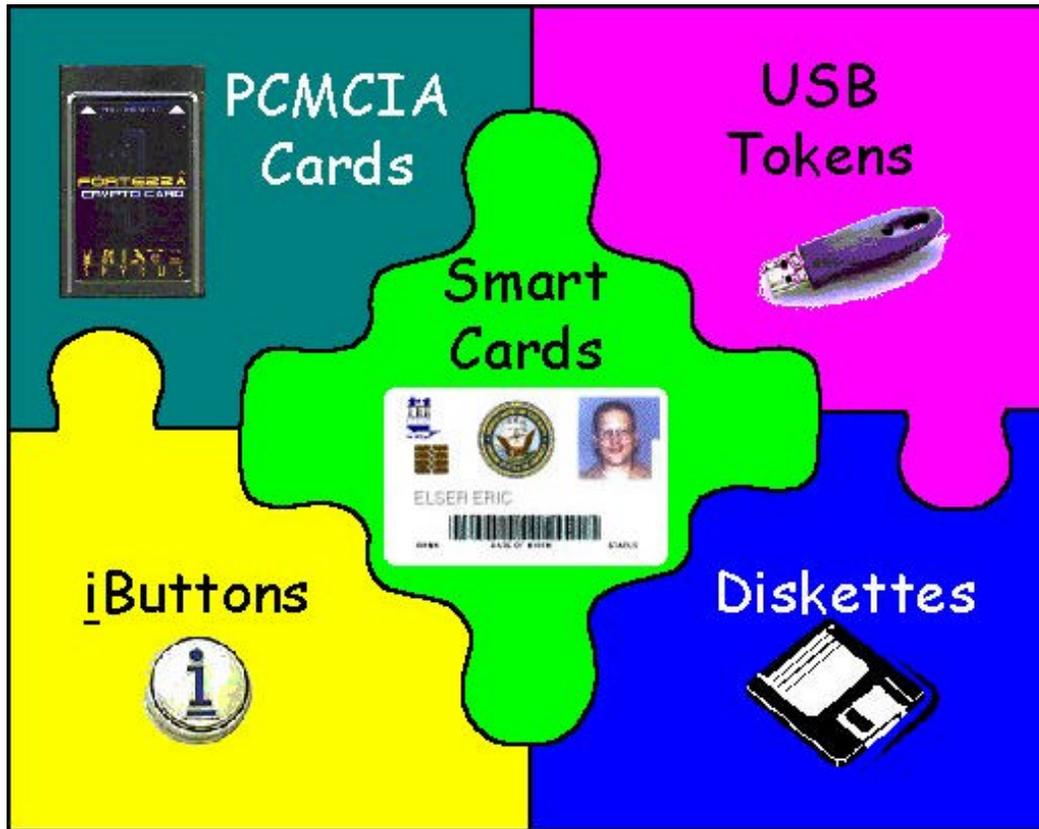
DoD has also embarked on an aggressive plan to implement smart card technology throughout the Department. The smart card combines multiple technologies on a single plastic card, including a microcomputer based on an embedded integrated circuit computer chip. Smart card technology is already being used at a number of DoD activities and operating units to reinvent business processes, enhance missions, reduce costs, and improve quality of life. On 10 November 1999, the Deputy Secretary of Defense (DEPSECDEF) directed that smart cards be used as the Common Access Card (CAC) for active duty personnel (to include the selected reserve), DoD civilian employees, and eligible contractor personnel. It will be the principal card used to enable physical access to DoD buildings, and as the DoD's primary platform for the PKI authentication token.

This report responds to the reporting requirement in Section 374 of the fiscal year (FY) 2000 Defense Authorization Act (Public Law 106-65), which required the evaluation of the option of using the smart card as the DoD's authentication token. This study also addresses other devices that could be used as this token, and compares the costs and benefits of using the smart card versus other token technologies. As discussed below and in detail in this report, results of this study show that the smart card is the most feasible, cost effective technology for the DoD PKI authentication token. Smart cards also provide numerous additional advantages over other token technologies by virtue of the multiple other technologies included on the card.

The evaluation approach for this effort began with the identification and description of the minimum mandatory requirements for the DoD cryptographic token. The foundation for these requirements is the DoD X.509 Certificate Policy (CP), which is the governing policy document outlining requirements for the DoD cryptographic token. These requirements address National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 140-1 Level 2 certification; signature algorithms; minimum key lengths; quality of key parameters; and private cryptographic key protection, generation, activation, deactivation, and destruction.

Various cryptographic token technologies, including smart cards, universal serial bus (USB) tokens, Personal Computer Memory Card International Association (PCMCIA) cards, diskettes, and Dallas Semiconductor's iButton were researched and analyzed. The cryptographic token technologies were then mapped against the minimum mandatory requirements to discover which met those requirements. This analysis revealed that smart cards, USB tokens, PCMCIA cards,

and iButtons either currently meet these requirements or are expected to meet them in the very near future. Only the diskettes failed to meet the minimum mandatory requirements.



Technologies that met the minimum mandatory requirements were then compared against a range of other criteria, including relative cost of implementation, added benefits, and relative advantages and disadvantages. These additional criteria proved to be the key discriminators in supporting the recommendation for the smart card as the primary DoD token. As detailed in this report, the smart card has the lowest cost of all readily available tokens; has the most cost-effective readers; has the lowest total cost of ownership; supports increased interoperability; is available from multiple vendors in large quantities; supports multiple technologies and multiple applications; can leverage existing infrastructure within DoD; is portable and convenient to use; and can provide sufficient memory capacity for additional applications and multiple certificates. Additionally, smart cards will serve as the official DoD identification card and will support future biometric technologies.

Based on the evaluation, this report concludes that smart card technology offers the most feasible, cost effective authentication mechanism to support the DoD PKI and to protect its critical information.

# **Consideration of Smart Cards as the DoD PKI Authentication Device Carrier**

## **Special Report to Congress**

10 January 2000

### **1. Introduction**

Public Key Infrastructure. As the Department of Defense (DoD) strives to achieve knowledge superiority and to provide critical information to the warfighter, it recognizes the need for robust information assurance capabilities to protect the confidentiality, integrity, and authenticity of this information. To this end, the Department is implementing a public key infrastructure (PKI), a key and certificate management infrastructure designed to support confidentiality, integrity, availability, authentication, and access control in computer networks. This PKI will require authentication device carriers (i.e., tokens<sup>1</sup>) to store and carry cryptographic keys supporting user identity authentication. The International Standards Organization (ISO) 7816 series Integrated Circuit (IC) card, more commonly known as the smart card, is one such token technology that the DoD is considering for its PKI. This report provides a thoughtful evaluation of the appropriateness of the smart card as the PKI token supporting user identity authentication, and compares the relative costs and benefits of token technologies in this context.

Smart Cards. DoD has embarked on an aggressive plan to implement smart card technology throughout the Department. The smart card combines multiple technologies on a single plastic card, including:

- A microcomputer based on an embedded integrated circuit computer chip. This microprocessor can store both programs and data in its memory and run programs when connected, via a standard card reader, to a card operating system (on a network, PC, laptop, or communications device)
- A magnetic stripe with three standard tracks which can be used for various applications
- A barcode which can store permanent information
- A photograph and basic identifying information.

Smart card technology is already being used at a number of activities and operating units throughout DoD. Using the card as an enabling device for multiple applications, the Department is reinventing business processes, enhancing missions, reducing costs, and improving quality of life. Section 373 of the fiscal year (FY) 2000 National Defense Authorization Act (Public Law 106-65) requires expanded use of smart card technology within DoD. On 10 November 1999, the DEPSECDEF directed that smart cards be used as the standard identification card for active duty and civilian personnel, the principal card used to enable physical access to DoD buildings, and as the DoD's primary platform for the PKI authentication token.

---

<sup>1</sup> For this report, the term "token" is synonymous with "authentication device carrier." While the term "token" sometimes refers to the cryptographic module that supports additional security functions beyond user identity authentication (e.g., confidentiality, integrity, and access control), the scope of this report is limited to evaluating the feasibility of token technologies as authentication device carriers.

## 1.1 Purpose

Per Section 374 of the FY 2000 National Defense Authorization Act (Public Law 106-65) (see Exhibit 1), this report evaluates the feasibility of using smart cards as the DoD's authentication device carrier, or token. This feasibility study also addresses other devices that could be used as a PKI token, and compares the costs and benefits of using the smart card versus those devices.

### Exhibit 1. Report Requirement From FY 2000 National Defense Authorization Act

**SEC. 374. REPORT ON DEFENSE USE OF SMART CARD  
AS PKI AUTHENTICATION DEVICE CARRIER.**

- (a) Report Required: Not later than February 1, 2000, the Secretary of Defense shall submit to Congress a report evaluating the option of the Department of Defense using the Smart Card as a Public-Private Key Infrastructure authentication device carrier. The report shall include the following:
- (1) An evaluation of the advantages and disadvantages of using the Smart Card as a PKI authentication device carrier for the Department of Defense.
  - (2) A description of other available devices that could be readily used as a PKI authentication device carrier.
  - (3) A comparison of the cost of using the Smart Card and other available devices as the PKI authentication device carrier.

## 1.2 Background

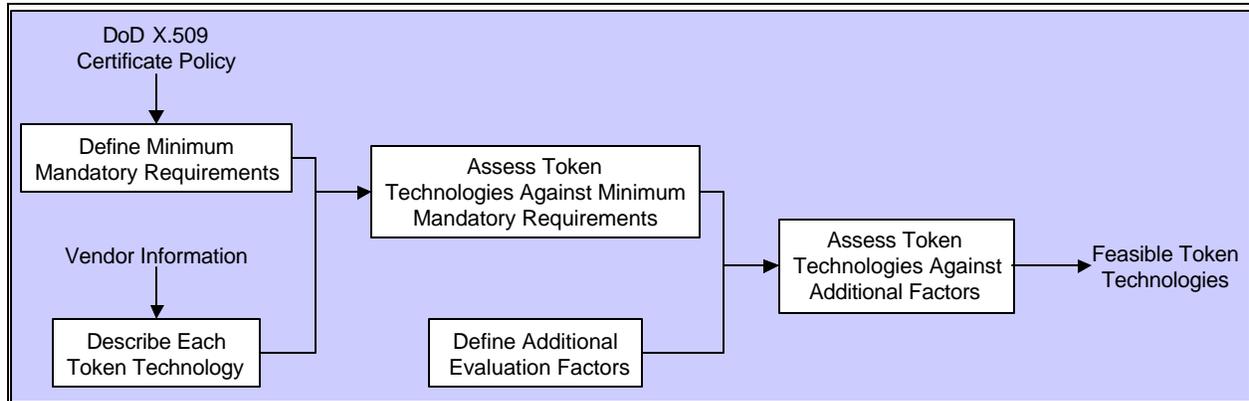
Because of the criticality of the DoD's mission and the information it leverages in support of this mission, it is vital that the Department get the right information to the right people at the right time. Therefore, ensuring the value and integrity of that information is essential, and is dependent on the DoD's ability to protect that information and to limit access to the appropriate users. To this end, the DoD is implementing a Department-wide PKI. In a 6 May 1999 memorandum, the Deputy Secretary of Defense (DEPSECDEF) stressed the need for a DoD PKI to enhance information security and mandated that all DoD organizations begin to issue hardware-based PKI tokens by January 2002. On 10 November 1999, the DEPSECDEF directed that smart cards become the Common Access Card (CAC) for all DoD personnel. The CAC will replace the existing military identification card, become a civilian personnel identification card, and be used as the DoD's authentication token. The CAC will be issued through the Defense Enrollment Eligibility Reporting Systems/Real-Time Automated Personnel Identification System (DEERS/RAPIDS) system.

The DoD recognizes the importance of this token for the PKI and the capabilities that a smart card can offer. For several years, the DoD and the Military Departments have been pilot testing smart card technology for applications such as personal identification, access control, asset tracking, deployment, training and medical records, and stored value. Despite the prevalence of these efforts, however, very limited testing of smart cards as a PKI token has occurred within the DoD. To determine the effectiveness of smart cards as the PKI token, Congress mandated in Section 374 of the FY 2000 National Defense Authorization Act (Public Law 106-65) (see Exhibit 1) that the Secretary of Defense submit to Congress a report addressing the smart card as the PKI authentication device carrier.

### 1.3 Approach

The evaluation approach for this effort (see Exhibit 2) began with identification and description of the minimum mandatory requirements for the DoD cryptographic token. Foremost among the documents used to define these requirements was the DoD X.509 Certificate Policy (CP), which is the governing policy document outlining requirements for the DoD cryptographic token. The various cryptographic token technologies, including smart cards, universal serial bus (USB) tokens, Personal Computer Memory Card International Association (PCMCIA) tokens, diskettes,

**Exhibit 2. Token Feasibility Evaluation Approach**



and other alternative token technologies, were analyzed, then mapped against the minimum mandatory requirements to reveal which complied with those requirements. Technologies meeting the minimum requirements were then compared against a range of other criteria, including relative cost of implementation, added benefits, and advantages and disadvantages, to determine which technology was the most effective for use as the DoD PKI authentication token.

### 1.4 Overview of Report Structure

The structure of this report follows the evaluation approach identified in Section 1.3 and illustrated in Exhibit 2. Section 2 defines the minimum mandatory requirements for the DoD cryptographic token. Section 3 describes the various available cryptographic token technologies, giving a brief description of each token technology and the current and near-term projected vendor offerings and industry trends. Referencing the requirements and technology capabilities, the report then provides a comparative analysis of those various technologies, including an assessment of their compliance with the minimum mandatory requirements (Section 4) and a comparison of additional advantages and disadvantages, relative costs, and other factors (Section 5). Finally, Section 6 provides summary thoughts on the effectiveness of the smart card as the DoD cryptographic token for identity authentication.

This report also includes several appendices. Appendix A lists the primary references used in preparing this report. Appendix B provides supplemental background information about the DoD PKI program. Appendix C provides supplemental background information about the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) Publication 140-1. Appendix D provides an acronym list and glossary of terms.

## 2. Minimum Mandatory Requirements

The DoD X.509 CP is the primary policy document governing the technical and procedural controls and mechanisms required to be implemented by the DoD PKI. (For readers unfamiliar with the DoD PKI program, Appendix B provides supplemental background information.) The requirements described below, obtained from the latest version of the CP, are the current minimum mandatory requirements for the DoD PKI cryptographic token.

In a related effort, DoD is presently developing a target token strategy for the Department's long-term PKI deployment. As this strategy is developed and implemented, requirements for future tokens may be more stringent than those that currently exist and may impact the cost of existing token technologies. However, it is expected that any cost increase will be within the cost ranges described in this report.

### 2.1 FIPS 140-1 Level 2 Validation

The DoD X.509 CP requires that the DoD PKI end user, Certificate Authority (CA), and Registration Authority (RA) tokens be validated at FIPS Pub 140-1 Level 2 and that the tokens be hardware based. [§6.2.1]<sup>2</sup>

FIPS Pub 140-1, *Security Requirements for Cryptographic Modules*, is the relevant security standard for cryptographic tokens. FIPS Pub 140-1 specifies the security requirements that must be satisfied by a token utilized in a security system that protects unclassified information in computer and telecommunication systems. The standard provides four increasing, qualitative levels of security—Level 1 through Level 4—intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. Appendix C provides supplemental information about FIPS Pub 140-1.

### 2.2 Signature Algorithms

A signature algorithm defines the cryptographic process used to generate digital signatures. Per the 8 August 1997 DEPSECDEF memorandum, the DoD PKI must support both the Digital Signature Standard (DSS) and commercial signature algorithms (e.g., the Rivest, Shamir, and Adleman [RSA] signature algorithm). To achieve FIPS Pub 140-1 certification, the token must be capable of being operated such that only FIPS approved algorithms are used. Current FIPS-approved signature algorithms, as specified in the DSS, FIPS Pub 186-1, include the Digital Signature Algorithm (DSA) and the American National Standards Institute (ANSI) X9.31 version of the RSA signature algorithm.

### 2.3 Key Sizes

Cryptographic key size determines the relative strength of a cryptographic algorithm. Generally, the longer the key, the more secure the algorithm. The DoD X.509 CP stipulates that for the DSA, the cryptographic module must support a 160-bit or longer private key and a 1024-bit or

---

<sup>2</sup> For this report, references to specific sections from the DoD X.509 CP are identified in brackets (e.g., [§...])

longer prime modulus. For the RSA algorithm, the cryptographic module must support a 1024-bit or longer public key size. [§6.1.3]

These minimum key length requirements translate to storage capacity requirements for the DoD cryptographic token. For DSA, the algorithm parameters that the token needs to store include the 1024-bit or longer prime modulus, the 160-bit or longer private key, and two additional 160-bit or longer DSA parameters (i.e., the DSA  $q$  and  $g$  parameters). Additionally, the token must provide additional memory capacity to store the associated public-key certificate, estimated to be about 1.5 kilobytes (KB) in size. The total minimum storage capacity requirement for DSA, therefore, is about 1.7 KB (i.e.,  $128 + 20 + 20 + 20 + 1,536$  bytes =  $1,724$  bytes  $\approx 1.7$  KB).

For RSA, the algorithm parameters that the token needs to store include the 1024-bit or longer public value and the variable-length encryption parameter (i.e., the RSA  $n$  and  $e$  parameters, respectively), which together are nominally about 768 bytes. As with DSA, the associated public-key certificate for RSA is about 1.5 KB. The total minimum storage capacity requirement to support RSA, therefore, is about 2.3 KB (i.e.,  $768 + 1,536$  bytes =  $2,304$  bytes  $\approx 2.3$  KB).

Combining these two storage capacity values, the total minimum storage capacity requirement for the DoD token is 4 KB.

## 2.4 Quality of Algorithm Parameters

The CP requires that the DSA public key parameters be generated, tested, and checked as specified in the DSS. [§6.1.4, 6.1.5]

## 2.5 Private Key Protection

The security of public/private key encryption hinges on the protection of the private key. As such, and in accordance with DoD X.509 CP, all tokens must be operated such that the private asymmetric cryptographic keys are never output in plaintext. Furthermore, the CP requires that only the subject of the corresponding certificate have access to a private signing key. [§6.2.1]

## 2.6 Private Key Generation

The minimum requirement is for the signature private key to be generated in and by the token. [§6.2.6]

## 2.7 Private Key Activation

The CP requires that a pass-phrase, personal identification number (PIN), biometrics data, or other mechanism of equivalent authentication robustness be used to activate the private key in a token. Entry of activation data must be protected from disclosure, that is, the data must not be displayed while it is entered. [§6.2.7, 6.4.1]

## **2.8 Private Key Deactivation**

The CP requires that the token support deactivation via a manual logout procedure or by passive timeout. [§6.2.8]

## **2.9 Private Key Destruction**

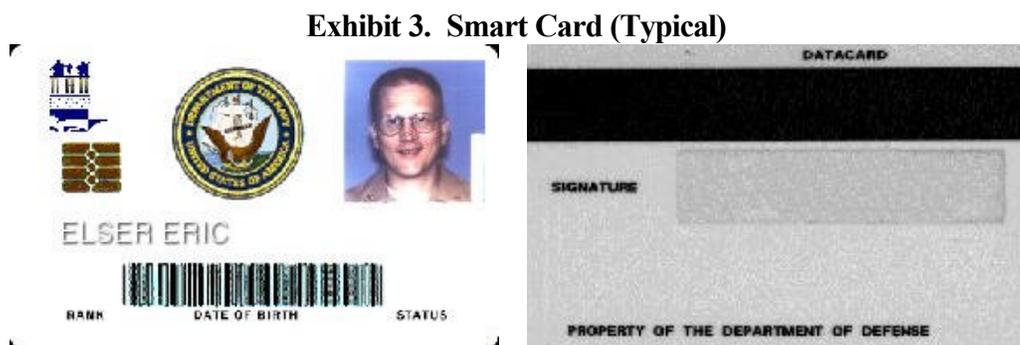
The CP requires that the token support zeroization (i.e., erasure) of private keys when they are no longer needed, or when the certificates to which they correspond expire or are revoked. Physical destruction of the token must not be required to meet this requirement. [§6.2.9]

### 3. Description of Cryptographic Token Technologies

This section briefly describes the various available cryptographic token technologies and the current and near-term projected vendor offerings and industry trends.

#### 3.1 Smart Cards

ISO 7816 IC cards, more commonly known as smart cards, are credit card-size tokens with embedded memory and/or microprocessor IC chips. Smart cards are categorized as either memory cards or microprocessor-based cards. Memory cards are not suitable for cryptographic applications because they lack a microprocessor and cannot perform cryptographic processes on the card. Therefore, for the purposes of this report, a smart card is a microprocessor-based IC card. The smart card communicates with the outside world via a reader connected to a standard (e.g., serial, USB, PCMCIA) interface in a contact environment, or via radio frequency (RF) electromagnetic waves in a contactless environment. Exhibit 3 illustrates the front and back sides of a typical smart card.



Inherent to a microprocessor-based smart card are security features that allow it to hold multiple applications in separate protected areas on a single card. The processor on the card follows programmed logic and incorporates algorithms that provide security features. Cryptographic smart cards can perform complex asymmetric public key algorithm-based functions, such as generation of digital signatures. Key pairs for public key cryptography can be generated by the microprocessor on the card, so that private keys need never be exposed outside the card in unencrypted format.

The credit card-size form factor<sup>3</sup> of the smart card allows printing on the card and hybridization of other technologies such as magnetic stripe, bar code, optical stripe, security features, digital engraving of a picture, and hologram. Because its form factor is identical to today's typical personal identification card, the smart card is ideally suited for serving as a photo identification card supporting physical access control to buildings and facilities. Additionally, the smart card is highly versatile since it can interface to a PC via several possible interfaces, including the traditional serial port, USB, PCMCIA, or contactless interfaces.

<sup>3</sup> The term "form factor" refers to the physical shape and dimensions of a particular token technology. The smart card is similar in shape and size to the common credit card; the form factors of the other token technologies considered in this report are very different.

In the past 2 years, significant progress has been achieved in memory capacity, processor speed, and IC security. Additionally, cryptographic co-processors have been incorporated into ICs to meet industry demands for more sophisticated applications such as PKI. Companies in the private sector have taken steps to move the technology towards standardization and interoperability by providing products such as JavaCard and Smart Card for Windows. Vendors have also developed other products that combine PKI and smart cards. While many organizations are beginning to look at combining smart cards and PKI, there have not been any major large-scale distributed implementations to demonstrate the feasibility of this technology combination within the U.S.

The public and private sectors are becoming increasingly involved in promoting the movement towards electronic business, electronic commerce, and security solutions through smart card technology implementations. In 1999, worldwide manufacturers shipped 1.5 billion smart cards, and the number is projected to increase by 24 percent annually, up to 4 billion by 2004. The government sector's share of the market was 4 percent in 1999 and is expected to grow to 11.2 percent by 2004.<sup>4</sup> Numerous government, commercial, and financial institutions, both domestic and foreign, are turning to smart card technology to ensure secure electronic transactions. In the private sector, one company has begun issuing PKI-enabled smart cards that enable customers to perform financial transactions over the Internet. Internationally, the Finnish and German governments are currently adapting their national identification cards to incorporate smart card technologies which will permit all citizens of both countries to interact electronically with their respective governments. The Spanish Mint's Ceres Project involves the storage of PKI digital certificates on smart cards to enable secure networked communications between government and public sector organizations, as well as securing private sector interaction with government web sites. These cards will be issued to millions of Spanish citizens. In the commercial telecommunications sector, smart cards are a key component for mobile subscribers in the Global System for Mobile (GSM) communications system, the most widely deployed wireless phone system in Europe and Asia. Increasingly, business and government communities are implementing the use of cryptographic keys and algorithms on smart cards to create a secure, more robust environment in which electronic commerce and point-to-point electronic transactions can thrive.

### **3.2 USB Tokens**

USB refers to an interface incorporating the high-speed external bus standard for PCs that was introduced in 1996. The USB interface can be used to support a variety of tokens to include smart cards and other unique security devices described herein. The USB token refers to a device containing an embedded microprocessor chip that interfaces directly with a PC's USB port without any additional hardware, such as a card reader. In terms of processing power, the microprocessors used in USB tokens are identical to those used in smart cards. Like the smart card, the USB token can generate asymmetric keys and perform cryptographic functions directly on the token. Additionally, it can provide an encryption engine within the token and is able to store private keys, passwords, and electronic certificates. Exhibit 4 illustrates two examples of typical USB tokens.

---

<sup>4</sup> *Smart Card Directory 2000*, pp. 13-14.

#### Exhibit 4. USB Tokens (Typical)



Although USB ports have become more prevalent in new PCs, USB tokens have not found a strong commercial market. No industry standardization exists beyond the USB port interface. Multiple supply sources producing high quantities do not exist; as a result, pricing is moderately high. Unlike smart cards, integration of USB tokens in the commercial telecommunications industry has not occurred. In addition, as with most of these tokens, the form factor does not allow for any added functionality (e.g., magnetic stripe, bar code, and photo for identification purposes).

### 3.3 PCMCIA Cards

The PCMCIA card is a hardware device that supports specific dedicated functions (i.e., different PCMCIA cards support different functions). Examples of PCMCIA card functions include memory devices, input/output devices (e.g., modems and fax modems), and portable diskette drives. PCMCIA cards are most commonly used to provide additional computing features for portable computers such as laptops. There is no widespread commercial acceptance for this hardware device in desktop computers. The majority of PCMCIA authentication token vendor offerings are compliant with NSA's FORTEZZA Crypto Card standards. Exhibit 5 illustrates two typical PCMCIA cards that provide cryptographic functionality.

#### Exhibit 5. PCMCIA Cards (Typical)



Although PCMCIA cards clearly provide the strongest security and largest memory storage capacity, the high cost of the tokens is likely to endure for some time (as well as the added cost for the reader and computer interface, which are typically not integral to the majority of desktop PCs). PCMCIA cards as authentication tokens have seen limited acceptance in the commercial marketplace, and like USB tokens, integration of PCMCIA cards in the commercial telecommunications industry has not occurred. The PCMCIA card also does not allow for any added functionality (e.g., magnetic stripe, bar code, and photo for identification purposes). Additionally, the larger form factor can be inconvenient.

### 3.4 Diskettes

The diskette has the advantage of being the lowest priced and most commoditized of the token alternatives. However, diskettes provide the poorest security and portability. There is no hardware present in the diskette to protect data stored on the diskette, and it provides no processing capability. If used for PKI, DoD keys would have to be generated in the software or at the server and transferred to the diskettes for storage. Additionally, this form factor does not allow for any added functionality (e.g., magnetic stripe, bar code, and photo for identification purposes).

### 3.5 Other Token Technologies

For this report, the only other token technology considered is Dallas Semiconductor Corporation's iButton (see Exhibit 6). The iButton is a computer chip encased in a 16-mm stainless steel case. The iButton can be attached to articles of clothing, wallets, and the like. Also, a cryptographic Java iButton exists that can securely store data and Java applets to the chip, as can a "Java Ring" with a cryptographic iButton attached to a ring.

#### Exhibit 6. Other Token Technologies



**iButton**



**Java Ring**

To use, the iButton is touched momentarily to an appropriate receptor. Most cryptographic tokens used in information technology applications such as secure web access or secure email require a constant presence in a reader. Because the iButton is a momentary device, its application in this type of environment is impractical. A \$15 Type DS1402 Blue Dot Receptor product interfaces with the iButton. It, in turn, connects to a PC's parallel, serial, or small computer systems interface (SCSI) port. The cryptographic version of the iButton uses the DS1954 chip, which is FIPS 140-1 Levels 1 and 2 validated.

One example of an iButton implementation is the U.S. Postal Service's PC Postage program. E-Stamp Corporation, a PC Postage service provider company, provides an electronic postage solution that utilizes the iButton and serves a user base of more than 13,000 people. However, there is not widespread commercial acceptance for iButton technology, the iButton has seen little integration with the commercial telecommunications industry, and the form factor does not allow for any added functionality (e.g., magnetic stripe, bar code, and picture).

#### 4. Compliance with Minimum Mandatory Requirements

From a technological standpoint, all of the token technologies described in Section 3, except for the diskette, are either currently capable of meeting the minimum mandatory requirements for authentication tokens as defined in Section 2 or are expected to meet those requirements soon. Exhibit 7 summarizes the extent of requirements compliance for each token technology type, and the subsections that follow provide amplifying information. (Note: The rows in the table, and the subsections that follow, correspond to the requirements subsections in Section 2.)

**Exhibit 7. Capability to Comply with Minimum Mandatory Requirements**

	Smart Card	USB Token	PCMCIA Card	Diskette	iButton
<b>FIPS 140-1 Level 2 Validation</b>	Pending *	Pending *	Yes	No	Yes
<b>Signature Algorithms</b>	Yes	Yes	Yes	Yes	Yes
<b>Key Sizes</b>	Yes	Yes	Yes	Yes	Yes
<b>Quality of Algorithm Parameters</b>	Yes	Yes	Yes	No	Yes
<b>Private Key Protection</b>	Yes	Yes	Yes	No	Yes
<b>Private Key Generation</b>	Yes	Yes	Yes	No	Yes
<b>Private Key Activation</b>	Yes	Yes	Yes	No	Yes
<b>Private Key Deactivation</b>	Yes	Yes	Yes	No	Yes
<b>Private Key Destruction</b>	Yes	Yes	Yes	No	Yes
Legend: <span style="background-color: green; color: black; padding: 2px;">Green</span> <span style="background-color: yellow; color: black; padding: 2px;">Yellow</span> <span style="background-color: red; color: black; padding: 2px;">Red</span>					
* Smart cards and USB tokens are expected to achieve FIPS 140-1 Level 2 validation soon.					

##### 4.1 FIPS 140-1 Level 2 Validation

Through its Cryptographic Module Validation Program, NIST periodically publishes a list of FIPS 140-1 validated and certified cryptographic modules. To date, some PCMCIA cards and the iButton have received FIPS 140-1 Level 2 (or higher) validation/certification from NIST. Various smart card and USB token vendors are seeking FIPS 140-1 Level 2 certification for their current and/or future product offerings, and it is anticipated that many will achieve this certification in the next 3 to 6 months. The diskette, due to limitations in its design, will never achieve Level 2 certification.

##### 4.2 Signature Algorithms

All of the token technologies can support either the DSA or the FIPS-approved version of the RSA signature algorithm (i.e., ANSI X9.31 RSA), and there are cryptographic token products available today that actually implement both signature algorithms. Also, there are products available that implement the RSA signature algorithm, but it is unclear whether these implementations are based on the ANSI X9.31 standard or the competing Public-Key Cryptography Standard (PKCS) #1 standard. (Informally, NIST has indicated that it may consider approval of the PKCS#1-based RSA algorithm.) It is anticipated that vendors will begin offering hardware token products that support both the DSA and ANSI X9.31 RSA signature algorithms in the next 3 to 6 months, particularly as their awareness of this requirement increases.

### **4.3 Key Sizes**

All of the token technologies support the 4 KB minimum memory capacity requirement to store the asymmetric cryptographic keys and associated public-key certificates as described in section 2.3.

### **4.4 Quality of Algorithm Parameters**

All of the hardware token technologies (i.e., all token technologies except diskette) can meet the algorithm parameter quality requirements. Proper implementation of these requirements is validated by NIST in conjunction with its Cryptographic Module Validation Program.

### **4.5 Private Key Protection**

All of the hardware token technologies can be designed to ensure that the private key remains in the token and never exists outside the token in unencrypted form. They can all perform the asymmetric algorithm processing onboard the token so that the private key never appears in the host platform, where it could be intercepted. Additionally, all hardware token technologies provide access control mechanisms for protecting private signing keys and can be configured to support multiple PINs supporting different purposes.

### **4.6 Private Key Generation**

All of the hardware token technologies can support private key generation on the token. Each is capable of using its onboard microprocessor resources to perform random number and private key generation calculations.

Achieving shorter key generation times has been a challenge for the cryptographic token vendors. Key generation using the token's primary microprocessor requires several seconds or sometimes minutes. To improve the speed and quality of the key generation process, vendors have added math co-processors and/or separate random number generators to their tokens. One vendor has claimed that its product has achieved a key generation time of under 100 milliseconds. Most of the hardware token vendors have implemented pseudo (i.e., discrete) random number generators in their token products, while others (i.e., selected smart card and PCMCIA card vendors) offer true (i.e., continuous) random number generators. True random number generators have the advantage of producing "stronger" random numbers which are significantly more resistant to brute force cracking attempts.

### **4.7 Private Key Activation**

All of the hardware tokens can be configured to require a password for private key activation and protection. Security is enhanced because the passwords are encrypted and stored on the token. Additionally, tokens can be configured to be automatically "locked" after a predetermined number of unsuccessful user password attempts, to prevent discovery of the password through "brute force" or guessing.

#### **4.8 Private Key Deactivation**

All of the hardware tokens support deactivation, both via a manual logout procedure and as a default action whenever the token is removed from its reader or slot.

#### **4.9 Private Key Destruction**

All of the hardware tokens support zeroization (i.e., erasure) of private keys when they are no longer needed.

## 5. Assessment Against Additional Factors

Beyond meeting the minimum mandatory requirements, other factors that could influence the effectiveness of a token must be considered. In that light, this section explores additional factors that would make a difference in selecting a target token. Exhibit 8 shows how other factors can affect the feasibility of using these tokens. The subsections following Exhibit 8 define these factors and justify the remarks denoted in the table.

**Exhibit 8. Comparison Against Additional Factors**

	Smart Card	USB Token	PCMCIA Card	iButton
<b>Cost of Token</b>	\$5-\$20	\$12-\$35*	\$50-\$500*	\$20-\$35*
<b>Cost of Reader</b>	\$0-\$50	\$0-\$30	\$75-\$150	\$15
<b>Initial Cost of Ownership</b>	Medium	High	High	High
<b>Support for Photo ID</b>	Yes	No	No	No
<b>Support for Other Technologies</b>	Yes	No	Limited	No
<b>Support for Multiple Applications</b>	Yes	No	No	No
<b>COTS Availability</b>	Available	Planning	Available	Planning
<b>DoD Infrastructure—Development</b>	Pilots	None	None	None
<b>Interoperability</b>	Evolving	Infancy	None	Infancy
<b>Convergence with Telecomm Industry</b>	Yes	No	No	No
<b>Form Factor—Convenience</b>	More	Less	Less	Less
<b>Portability</b>	Yes	Limited	Limited	Yes
<b>Durability</b>	Medium	Medium	Medium	High
<b>Onboard Memory Storage Capacity</b>	Adequate	Adequate	Adequate	Inadequate
<b>Technology Maturity</b>	Matured	Infancy	Matured	Infancy

Legend: Green Yellow Red

\* Includes cost of interface adapters.

### 5.1 Cost of the Token

The cost of the token varies depending on the level of information security provided by the technology. The cost of the technology increases as higher standards of security are incorporated into the token. Processing speed, memory capacity, market demand, and competition also influence costs.

In assessing costs associated with security standards, DoD requires that the Target PKI token be FIPS Pub 140-1 Level 2 compliant. Because current smart card technology is not Level 2 compliant, we have estimated the cost for a smart card that would meet this standard. Currently, a triple-Data Encryption Standard (DES)-enabled, 8-bit processor, electronic purse, 8 KB Electrically Erasable Programmable Read-Only Memory (EEPROM) card costs about \$3.50 when purchased in bulk quantities. A cryptographic co-processor card<sup>5</sup> having functional capabilities similar to the EEPROM card will cost approximately \$5 to \$20 per card, when

<sup>5</sup> Smart card technology can be used to carry out many different functions, so there are different types of cards ranging from memory cards to microprocessor cards to crypto co-processor cards. This report focuses on the crypto co-processor card because its performance is best suited to meeting the security requirements of the DoD PKI token and commercial industry.

purchased in bulk quantities (e.g., 100,000 or more cards). The trend in the smart card industry has been toward improving processing speeds and memory capacity while decreasing production costs.

PCMCIA cards provide the required security and have the largest memory storage capacity; however, the costs of these tokens can reach \$310 per token and are likely to cost this much for the foreseeable future. USB token and iButton costs, on the other hand, range from \$12 to \$35, but are relatively new technologies and prices will fluctuate based on market demand.

## **5.2 Cost of the Reader**

The cost of purchasing a token reader, excluding costs associated with its installation and maintenance, varies depending on the type of token technology implemented. Currently, smart card readers configured with PCMCIA interfaces can cost as high as \$130 per unit, readers configured as serial devices cost about \$50 per unit, and smart card readers integrated directly into PCs cost only about \$2-\$3 per unit. Recent gains in smart card popularity and use will likely lead to new PCs coming equipped with smart card readers, thus eliminating the need to purchase a separate reader.

Use of a USB token requires a USB token reader, which in turn connects to the PC via a USB interface port. USB token readers can cost up to \$35 per unit. Total cost of the token, reader, and adapter board averages \$65 per implementation. Newer model desktop and laptop PCs come equipped with USB interface ports, effectively eliminating the cost of the reader. However, older model PCs do not have these ports, so either the PC has to be replaced or a USB port interface adapter card has to be installed in the PC to use USB tokens.

PCMCIA slots are common on laptop PCs but not on desktop PCs. Therefore, purchase of a PCMCIA interface and associated adapters would likely be necessary for most desktop PCs. Costs associated with PCMCIA slots and interface adapter cards for desktop PCs range from \$75 to \$150 per unit.

The cost for an iButton reader using the Blue Dot Receptor is approximately \$15 per unit. Although this reader is relatively inexpensive, there are no plans for commercial industry to integrate this reader into the production of future model PCs.

## **5.3 Initial Cost of Ownership**

Ownership is another factor associated with cost. This factor addresses the cost of setting up an infrastructure to support the operation and maintenance of the token throughout its life cycle. The operation and maintenance of the token would be similar regardless if the token selected.

Start up costs of software development and system integration vary among the different token technologies. Even though these costs are not easily quantifiable, one can observe that the smart card industry is much further along in lowering these up-front costs. Organizations and leading companies in the private sector have been working on standardizing interfaces between the PC, the smart card reader, and the smart card. Two major bank card organizations have developed and published specifications for their payment systems, thereby reducing system and application

development times and costs. Yet another private company is actively developing its JavaCard specifications to support the development of reusable software modules for smart cards. The smart card industry as a whole is moving towards agreement on a set of common standards and specifications. Several industry workgroups are addressing smart card issues such as interoperability. The most notable workgroup, the Personal Computer Smart Card (PC/SC) workgroup, is defining a standard smart card-to-PC interface such that applications can interoperate with different vendors' readers and smart cards. This interoperability will speed application development time and reduce costs. Two major-name client web browser products are "out of the box" capable of communicating with smart cards.

By contrast, start up costs for USB, PCMCIA, and iButton token-based solutions are higher. Currently there are only a handful of vendors using these technologies. Therefore, system and application developers must develop customized software for each of their unique customer bases.

In terms of the cost of migration to upgraded technology, additional factors that must be considered include competition among the vendors and the durability or projected longevity of each vendor as a company. For example, since there are currently only two USB token vendors and one iButton vendor, today's USB token and iButton customers incur the risk of higher token prices or possibly even product non-availability at some point in the future. The proliferation of smart card vendors, however, indicates that smart cards, as a technology, will prevail for many years to come.

#### **5.4 Support for Photo ID**

In addition to providing a vehicle for gaining access to computer networks and systems, the PKI token of greatest benefit to the DoD will also serve as the means of photo identification for active duty personnel (to include the selected reserve), DoD civilian employees, and eligible contractor personnel. The smart card's form factor is identical to today's typical personal identification card, thus it is ideally suited for serving as a photo identification card supporting physical access control to buildings and facilities.

#### **5.5 Support for Other Technologies**

Of the PKI token technologies evaluated, the smart card is best suited to housing other technologies, including:

- Hologram
- Microprinting
- Bar code (including two-dimensional bar code)
- Magnetic stripe
- Signature panel
- The words "Property of the Department of Defense" to delineate ownership.

The other PKI token technologies are not suited for these other technologies.

## 5.6 Support for Multiple Applications

Multiple applications refer to the core token platform's ability to support several applications on the same micro controller (e.g., PKI, building access, electronic payment, mobile phone subscriber data, etc.). Multiapplication smart cards have the intelligence built into the operating system to facilitate features that enable different applications to coexist on the same token. Furthermore, with the growth of interpretive card platforms (e.g., JavaCard, MULTOS, Smart Card for Windows), many of the multiapplication support features are becoming standardized.

PCMCIA cards also store multiple application information because the technology is based on chip sets. Currently, no strong standards initiatives call for them to become multiapplication-ready. USB and iButton tokens present similar issues in that they also have the potential to allow multiapplication support, but no widely used standards exist because they are still in the early stages of development.

## 5.7 COTS Availability

The DoD PKI token must be commercially available to permit outsourcing of elements, as appropriate. Of the existing token technologies on the market today, smart cards are by far the most extensively produced. The plastic card manufacturing industry produces billions of cards each year, of which hundreds of millions are smart cards. Multiple vendors have well-established production capacities to meet requirements for banking, telephony (e.g., pay phones and mobile phones), set-top boxes, transit, and access control customers. These cards are available from multiple sources in large quantities.

Additionally, various vendors are increasingly targeting their smart card development and production efforts to address PKI requirements. For example, one vendor provides a complete secure web access solution that includes smart cards. Another vendor has integrated its smart card with its virtual private network (VPN) products to enhance the security of its VPN solutions. Still another vendor is testing and piloting their JavaCard specification-based secure web server application. Thus, smart card-based, PKI-enabled identification and authentication products for network security, certified email exchange, web browsing, and the like are becoming more readily available.

Although USB interface ports are becoming more prevalent in new PCs, USB tokens have not developed a strong commercial market. Limited market demand means limited supply and consequently very few USB token-based applications and pilot implementations currently exist. Currently available iKey-based applications include a boot protection application developed and integrated by an operating system protection application, and a secure web access and identification application. Future iKey-based applications include FORTEZZA interoperability and building access. USB token implementations exist primarily in the academic sector.

PCMCIA cards are available in abundance; however, only one PCMCIA card can currently meet specific DoD requirements—FORTEZZA. FORTEZZA cards are used primarily in the Defense Messaging System (DMS) environment.

## 5.8 DoD Infrastructure—Development

The DoD PKI token can prove more cost-effective if it is able to leverage the existing infrastructure within the Department. Within the DoD, significant investments have been made in infrastructure that utilizes plastic card-based technology. For example, the world-wide DEERS/RAPIDS is issuing smart card-based civilian and military ID cards to all members of DoD. The Department will be able to leverage this investment by integrating a smart card-based authentication token into a card-ready culture and its accompanying DoD-wide infrastructure.

## 5.9 Interoperability

The DoD PKI token will provide for secure interoperability with the DoD and its federal, allied, and commercial entities. Existing commercial and government standards, including Public Key Cryptology Standard (PKCS), Microsoft Cryptographic Application Programming Interface (MS CAPI), and X.509, are being used to establish a framework for using PKI within DoD. If these standards are closely followed during planning and implementation of a PKI token solution, then DoD can ensure maximum use of commercial-off-the-shelf (COTS) products.

Most smart cards implement the basic standards defined by ISO 7816 dictating the dimensions and placement of the chip on the card and its interface (method of communication) with the outside world. Additionally, these standards define uniform file structures for the smart card, but providers of card operating systems can implement these standards in different ways. The result is that many commercially developed operating systems are available on the market. To ensure that computers can read a smart card with a certificate, most technology providers deliver two software packages to provide Application Programming Interface (API) level interoperability—one implementing either PKCS-11 and/or MS CAPI and another serving as the driver for the card, which is specific to the vendor's operating system. This allows for a transparency of the card when using the application. As a result, vendors have created an environment similar to that for printers, wherein any printer can work with any PC if the appropriate driver is installed on that PC.

Although a ubiquitous standard exists for the USB bus, the USB token itself has no standard. Also, no standards exist for the iButton; therefore, USB and iButton tokens developed to date are non-standards based. Moreover, application providers such as Netscape or Microsoft Explorer have not integrated these tokens into their browsers. PCMCIA cards are currently used only in the DMS environment and are not integrated into commercial applications.

## 5.10 Convergence with Telecommunications Industry

In terms of convergence with and integration into the commercial telecommunications industry, smart cards are at the forefront. For example, smart cards are a key component for mobile subscribers in the GSM communications system, the most widely deployed wireless phone system in Europe and Asia. The other token technologies have not converged with the commercial telecommunications industry.

### 5.11 Form Factor—Convenience

The form factor of the token can also play a significant role with respect to token use in the DoD environment. The smart card token is easiest to carry because it is thin and lightweight and can be placed in a wallet or attached to an ID badge lanyard. On the other hand, the PCMCIA card form factor is larger and less convenient, and the USB token and iButton have to be carefully inserted into their respective interface devices during use. The relative inconvenience of using the other tokens makes smart cards the easiest to use.

### 5.12 Portability

Portability addresses how the token will interface with workstations within the system so that the user is not restricted to working on a single designated computer.

Assessment of the current technologies reveals that all of the tokens evaluated exhibit some level of portability. Smart cards exhibit the greatest portability, and just like a diskette can be moved from PC to PC without loss of functionality. Once PCs become USB port-equipped, the USB token will become highly portable as well. In terms of portability across applications, the USB, PCMCIA, and iButton tokens are at a distinct disadvantage; currently only the smart card can be used in different devices supporting diverse applications, such as PCs, point of sale (POS) terminals, automated teller machines (ATM), mobile phones, or set-top boxes.

### 5.13 Durability

Durability refers to the expected physical life of a token technology. It is critical that any token technology DoD adopts be durable enough to withstand the unique and often harsh conditions that characterize token use and storage by military personnel, particularly those operating in combat or otherwise harsh environments. The majority of token vendors state that their products will last 10 or more years. However, the vendors' durability tests generally address the number of read/write cycles possible after subjecting the tokens to adverse conditions such as washing machines or extreme temperatures, which are generally not entirely representative of military operational and environmental conditions.

Because the USB token and iButton token technologies are relatively new, there is insufficient empirical data available to support an accurate quantitative comparison of the relative durability of the different token technologies considered in this report. From a qualitative standpoint, however, the iButtons appears to be the most durable token technology because of its stainless steel construction. Durability of the other token technologies varies depending on the token fabrication technology employed, quality of the electrical contacts used, and product line quality (i.e., token vendors typically offer low-cost, basic-quality token products targeted for certain customers as well as higher-cost, higher-quality products targeted for customers with more stringent requirements).

Smart card insertion lifetime varies depending on the quality of the electrical contacts used, which are typically rated between 10,000 and 100,000 insertions. Another factor affecting smart card lifetime is the expected physical lifetime of the plastic, which is nominally 2 to 3 years, possibly longer if the card plastic is not embossed.

USB devices were not originally designed to support frequent insertion into USB ports. Similarly, the least durable component for PCMCIA cards is the relatively fragile electrical connector. Like USB tokens, exact durability figures for the PCMCIA electrical connectors are not known.

#### **5.14 Onboard Memory Capacity**

To serve effectively as a multi-application token, the token technology selected must provide sufficient memory to support the storage of additional application data, including cryptographic keys and certificates. Currently, iButtons provide a memory capacity of 6 KB and the current generation of smart cards and USB tokens provide 16 KB of memory. Of the token technologies, PCMCIA cards provide the most memory capacity—about 1,000 KB. Thus, all of the token technologies except iButton provide adequate memory to support multiple applications. An important observation, however, is that all of the token technology vendors' product lines are continually evolving to offer higher memory capacity products. The iButton vendor, for example, is expected to introduce a new product very soon that will provide a substantially larger memory capacity (i.e., greater than 100 KB).

#### **5.15 Technology Maturity**

It is important to select a token technology that is mature enough to ensure the best return on investment. A mature technology can be easily upgraded and supported by different vendors if necessary. Another benefit of a mature technology is that it allows for more competition among manufacturers and vendors, lowering the cost. The development stage of a particular token technology can be discerned by studying the following factors:

- Number of applications and size of user base
- Current market domination
- Current infrastructure
- Existing standards and initiatives
- Price normalization
- Date of introduction.

Of the token technologies considered in this report, smart cards and PCMCIA cards are the most mature. USB and iButton token technologies are considered to be in their infancy stages.

## 6. Summary of Findings

This report, as mandated by Section 374 of the FY2000 National Defense Authorization Act (Public Law 106-65), evaluates the effectiveness of the smart card as the DoD's PKI authentication device carrier, or token. This report also describes other available devices that could readily be used as a PKI token, and compares the costs and benefits of using the smart card versus other devices. Findings based on this evaluation support the recommendation to use the smart card as the DoD's PKI authentication device carrier. A summary of these findings follows.

As part of this evaluation, current token technologies and their capability to meet the minimum mandatory requirements of the DoD PKI, as defined in the DoD X.509 CP, were analyzed. These requirements address the following areas: FIPS 140-1 certification, signature algorithms, minimum key lengths, quality of key parameters, private asymmetric cryptographic key protection, private key generation, private key activation, private key deactivation, and private key destruction. Analysis revealed that smart cards, USB tokens, PCMCIA cards, and iButtons currently meet the minimum mandatory requirements or are expected to meet them in the near future. Although smart cards and USB tokens have not yet achieved FIPS 140-1 Level 2 validation status, they are expected to do so in the near term. Only diskettes failed to meet these minimum mandatory requirements.

Additional critical factors influencing the effectiveness of specific token implementation were then assessed. Results of this assessment proved to be the key discriminator in supporting the recommendation to choose the smart card as the primary DoD PKI token. Justification supporting smart card implementation based on these additional factors follows.

- **Cost of the Token:** The smart card, even when accounting for its upgrade to FIPS 140-1 Level 2 certification, has the lowest cost of all readily available tokens, with the least susceptibility to wide price fluctuations based on market demand.
- **Cost of the Reader:** Although readers for smart cards, USB tokens, and iButtons currently are comparably priced, smart cards were determined to prove the most cost-effective over the long term due to recent gains in smart card popularity and use. A case in point is that the new PCs are coming equipped with smart card readers, thus eliminating the need to purchase separate readers. Additionally, some commercial smart card initiatives are providing thousands of card readers to the public free of charge. Further, reader costs can be reduced if shared among different agencies using smart cards for multiple applications.
- **Initial Cost of Ownership:** Smart card costs can be significantly reduced by leveraging production capabilities and processes developed, utilized, and monitored by both commercial industry leaders and customers.
- **Support for Photo ID:** Only the smart card supports inclusion of a digitized photograph for personnel identification purposes.
- **Support for Other Technologies:** Only the smart card has a form factor that effectively supports the addition of other technologies, such as hologram, bar code, magnetic stripe, and microprinting.

- **Support for Multiple Applications:** Multiapplication smart cards have the greatest capability among the tokens evaluated to support multiple applications.
- **COTS Availability:** Of the available token technologies, only smart cards are being implemented within DoD on a large scale and are currently available from multiple vendors in large quantities.
- **DoD Infrastructure:** Smart card use can leverage the existing DoD infrastructure provided by DEERS/RAPIDS for token issuance, cost sharing, and token and configuration management. Separate infrastructures would have to be developed to support all of the other token technologies. Additionally, choosing a token technology other than smart cards for use as the PKI authentication token would not alleviate the cost to the Department of using smart cards for multiple applications including the DoD CAC.
- **Interoperability:** Major commercial technology providers have developed operating systems compliant with defined universal standards to ensure that most computers can read a smart card storing a certificate. USB and iButton tokens do not have defined universal standards, and PCMCIA cards are not integrated into commercial applications.
- **Convergence with Telecommunications Industry:** Smart cards are at the forefront in terms of convergence with the commercial telecommunications sector, particularly the mobile phone market.
- **Form Factor—Convenience:** The size and location of card readers make the smart card the easiest token to use. Additionally, throughout DoD, numerous personnel are using smart card technologies. This factor will reduce the level of necessary training and change management efforts that must be implemented to introduce smart cards as the PKI token.
- **Portability:** Although all tokens are portable, smart cards were assessed as having the greatest portability based on the likely ubiquity of smart card readers and their accessible location on desktop computers.

DoD requires a robust information assurance capability to protect adequately mission-critical information for the warfighter and has identified PKI as a way to provide this capability. Of the PKI authentication token technologies evaluated in this report, smart card technology offers an effective mechanism to support the DoD PKI and to protect the Department's critical information. As a technology, smart cards are capable of meeting both the minimum and additional DoD PKI authentication device requirements. While there are currently no smart card products available that meet all of the FIPS security requirements, it is anticipated that vendors will make such product offerings available in the coming months, particularly if the DoD publishes a requirements specification for a large-scale purchase. Implementation of smart card technology will provide the benefit of supporting multiple applications and promoting more efficient electronic business practices.

## Appendix A

### References

The following primary sources provided information that was used in preparing this report:

1. *National Defense Authorization Act for Fiscal Year 2000*, Public Law 106-65, 106th Congress, 5 October 1999.
2. *X.509 Certificate Policy for the United States Department of Defense*, Version 5.0, 13 December 1999.
3. *Department of Defense (DoD) Public Key Infrastructure (PKI)*, Deputy Secretary of Defense memorandum, 6 May 1999.
4. *Smart Card Adoption and Implementation*, Deputy Secretary of Defense memorandum, 10 November 1999
5. *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards Publication (FIPS Pub) 140-1, National Institute of Standards and Technology, 11 January 1994.
6. *Security Requirements for Cryptographic Modules*, Draft for Comment, Federal Information Processing Standards Publication (FIPS Pub) 140-2, National Institute of Standards and Technology, 17 November 1999.
7. *United States Department of Defense Public Key Infrastructure Target Class 4 Token Security Requirements*, Draft Version 0.006, 8 December 1999.
8. *Management Reform Memorandum #16—Identifying Requirements for the Design, Development and Implementation of a DoD Public Key Infrastructure*, Deputy Secretary of Defense memorandum, 8 August 1997.
9. *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication (FIPS Pub) 186-1, National Institute of Standards and Technology, 15 December 1998.
10. *FIPS 140-1 Cryptographic Modules Validation List*, National Institute of Standards and Technology, 10 January 2000. (Note: The *FIPS 140-1 Cryptographic Modules Validation List* is updated frequently; the latest version is available online at <http://csrc.nist.gov/cryptval/140-1/1401val.htm>.)
11. *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*, American National Standards Institute (ANSI) X9.31-1998, May 1998.
12. *PKCS #1 v2.0: RSA Cryptography Standard*, RSA Laboratories, 1 October 1998.
13. *Smart Card Directory 2000*, Elizabeth Hildreth, Ed., Faulkner and Gray, New York, 1999.

## **Appendix B**

### **Description of DoD PKI**

The Department of Defense (DoD) must ensure the availability, integrity, confidentiality, nonrepudiation, and authentication of its information to successfully accomplish its critical mission. To achieve this goal, the Deputy Secretary of Defense (DEPSECDEF) issued the 6 May 1999 memo entitled "DOD PKI," which presented the DoD's vision and strategy for implementing general-purpose PKI services to a broad range of applications, at levels of assurance consistent with operational mission requirements. In his memo, the DEPSECDEF emphasized that the Department "must take an aggressive approach in acquiring and using a PKI that meets the requirements of all Information Assurance (IA) services." On 10 November 1999, the DEPSECDEF directed that smart cards be used as the standard identification card for both active duty and civilian personnel; the principle card used to ensure physical access to DoD buildings, and as the DoD's primary platform for the PKI authentication token. Further, in today's highly interconnected, shared-risk environment, DoD IA capabilities must address the pervasiveness of information as a vital aspect of warfighting and business operations.

Public Key Infrastructure (PKI) is the keystone for the protection of DoD information and is one element of the Defense-In-Depth strategy in which layers of defense are used to achieve the Department's IA and security objectives. A common, integrated DoD PKI will support multiple assurance levels, thus enabling users to cost effectively and efficiently select appropriate security solutions based on sensitivity or value of the data and the level of risk.

Public key cryptography using digital certificates offers the best available technology for secure transmission of data across public and private wide area networks. It provides a high degree of assurance of data confidentiality, data integrity, access control, and user identification among users of networked applications, including electronic mail (e-mail), web-based information services and transactions, and electronic commerce. As an enabling technology, PKI provides the framework and services for the generation, production, distribution, control, and accounting of public key certificates.

#### **Target DoD PKI Objectives**

The DEPSECDEF memo encouraged widespread use of public key-enabled applications and provided specific guidelines for applying PKI services throughout the Department. The Target DoD PKI will have the following attributes:

- Adopt industry standards, wherever possible
- Support multiple applications and products
- Provide secure interoperability throughout DoD, and with other partners such as federal government agencies, allies, industry, and academia
- Support digital signature and key exchange applications
- Support key/data recovery
- Be commercially based, allowing for outsourcing of elements as appropriate

- Support Federal Information Processing Standards (FIPS) – compliance requirements.

The Target DoD PKI will be developed in accordance with the Department's Defense in Depth, layered information assurance specifications. It will support two assurance levels, defined as Classes 3 and 4 for the protection of unclassified/sensitive information. Each assurance level has its own set of requirements for technical implementation and process controls, which becomes more rigorous as the level increases. The DoD Certificate Policy defines the applicability of these assurance levels for the protection of information based on its value or sensitivity, the risk and the consequences of loss, disclosure, or modification.

### **Public Key Enabled System Elements**

A public key enabled system is composed of three elements—certificate management, registration, and public key enabled applications—which must work together to achieve secure functionality. The Target DoD PKI will use centralized certificate management and decentralized registration. It will be achieved by applying layered security (e.g., operating the PKI as appropriate on protected networks), which will enable the DoD to minimize government off-the-shelf developments and leverage existing commercial PKI technology, standards, and services.

Certificate management provides for the generation, production, distribution, control, accounting, and destruction for public keys and public key certificates. It is composed of the Certification Authority (CA) and Directory Services. Certificate management relies on a trusted third party, the CA, to certify the identity of the possessor of a private key used for digital signature or key exchange. The CAs provide digitally signed certificates for users and components.

The Local Registration Authorities (LRA) use software tools recognized by the infrastructure to handle the registration process. The LRAs are responsible for authenticating the identity and attributes of the user (end entity) for the CA. It is also the responsibility of the LRA to verify the accuracy of information on the certificates.

The PKI supports the employment of cryptographic security services by providing valid public key information, certificates, and Certificate Revocation Lists to cryptographic-enabled applications. The user's cryptographic-enabled applications perform the data encryption and decryption and/or sign and verify signatures. Encryption and digital signature can provide confidentiality, integrity, non-repudiation, and authentication of the information.

### **PKI Implementation Strategy**

The strategy for implementing the DoD Target PKI is outlined in the 6 May 1999 DEPSECDEF memo. Implementation timelines will be driven by both the current state of commercial technologies and the technical risk of adopting solutions that may become obsolete or fail to meet future requirements. Consistent with the DoD IA Strategy, the DoD PKI Strategy will immediately begin to leverage the existing capabilities and services afforded by the commercial PKI industry. While using the FORTEZZA and Class 3 initiatives as sources of lessons learned,

the strategy for the target DoD PKI is not limited to building on either of these efforts to achieve the target DoD PKI. The DoD Target PKI will apply the best commercially available technologies unless they fail to meet the most stringent military requirements. Government developed technologies will only be used when no suitable commercial capability is available.

## **Appendix C**

### **Synopsis of FIPS Publication 140-1**

This appendix provides a synopsis of the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) Publication 140-1.

FIPS Publication 140-1 is currently undergoing revision by NIST, and a draft of the successor publication (i.e., FIPS Publication 140-2) was recently distributed for industry review and comment. FIPS Publication 140-2 is expected to be approved in late 2000 or early 2001.

#### **Applicability**

Per the Computer Security Act of 1987, NIST has the responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems. In accordance with Section 2315 of Title 10, U.S. Code, or Section 3502(2) of Title 44, U.S. Code, the FIPS 140-1 standard is applicable for unclassified use only in automatic data processing or telecommunications equipment used for routine administrative and business applications such as payroll, finance, logistics, and personnel management. It is not applicable to any data processing or telecommunications system or equipment, the function, operation, or use of which:

- (A) involves intelligence activities;
- (B) involves cryptologic activities related to national security;
- (C) involves the direct command and control of military forces;
- (D) involves equipment which is an integral part of a weapon or weapons system; or
- (E) is critical to the direct fulfillment of military or intelligence missions, provided that this exclusion shall not include automatic data processing or telecommunications equipment used for routine administrative and business applications such as payroll, finance, logistics, and personnel management;

#### **Overview**

The FIPS 140-1 standard specifies requirements for four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g., low value administrative data, million dollar funds transfers, and life protecting data), and a diversity of application environments (e.g., a guarded facility, an office, or a completely unprotected location). Each security level offers an increase in security over the preceding level. These four increasing levels of security will allow cost-effective solutions that are appropriate for different degrees of data sensitivity and different application environments.

On July 17, 1995, NIST's Computer Systems Laboratory (CSL) and the Communications Security Establishment (CSE) of the Government of Canada announced the establishment of the Cryptographic Module Validation Program (CMVP). The CMVP validates commercial products for conformance to FIPS 140-1 based on independent, third party testing by accredited laboratories. Products validated by this program will be accepted for use in both Canada and the

United States for the protection of sensitive, unclassified information. Federal agencies are encouraged by NIST and CSE to specify FIPS 140-1 validated products in their procurements.

## **Security Levels**

Security Level 1 is considered the lowest level of security and does not require physical security mechanisms. Security Level 4 is the highest level of security and includes requirements for protection of the device against a compromise of its security due to environment conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature. Each of the security levels is briefly described below.

### **Security Level 1**

Level 1 is considered the lowest level of security and requires no physical security mechanisms in the cryptographic module beyond the requirement for production-grade equipment. Level 1 allows software cryptographic functions to be performed in a general-purpose personal computer (PC), and NIST believes that such implementations are often appropriate in low-level security applications. Examples include Integrated Circuit (IC) cards and add-on security products.

### **Security Level 2**

Security Level 2 improves the physical security of a Level 1 cryptographic module by adding the requirement for tamper-evident coatings or seals, or for pick-resistant locks. Tamper-evident coatings or seals are affixed to a cryptographic module so that the coating or seal will have to be broken to gain physical access to the plaintext cryptographic keys and other critical security parameters within the module.

Level 2 provides role-based authentication in which a module must authenticate that an operator is authorized to assume a specific role and perform a corresponding set of services either directly or indirectly via a computer process acting on his or her behalf. Additionally, Level 2 allows software cryptography in multi-user timeshared systems when used in conjunction with a C2 or equivalent trusted operating system.

### **Security Level 3**

Security Level 3 requires enhanced physical security, which unlike Level 2, employs locks to protect against tampering with a cryptographic module, or employs coatings or seals to detect when tampering has occurred in order to prevent an intruder from gaining access to critical security parameters held within the module.

Level 3 provides for identity-based authentication in which a module must authenticate the identity of an operator and verify that the identified operator is authorized to assume a specific role and perform a corresponding set of services. This may be done either directly or indirectly via a computer process acting on his or her behalf.

### Security Level 4

Security Level 4, which provides the highest level of security, requires an envelope of protection around the cryptographic module that detects penetration of the device from any direction. For example, if an attempt is made to cut through the enclosure of the cryptographic module, the attempt should be detected and all critical security parameters should be zeroized. Level 4 also protects a module against compromise due to environmental conditions or fluctuations outside of the module’s normal operating ranges for voltage and temperature.

### Summary of Security Requirements

Table C-1 summarizes the FIPS Publication 140-1 requirements for Security Levels 1 through 4. (Table C-1 is the same as Table 1 from Section 4 of the FIPS Pub.)

**Table C-1: Summary of Security Requirements**

	Security Level 1	Security Level 2	Security Level 3	Security Level 4
<b>Crypto Module</b>	Specification of cryptographic module and cryptographic boundary. Description of cryptographic module including all hardware, software, and firmware components. Statement of module security policy.			
<b>Module Interfaces</b>	Required and optional interfaces. Specification of all interfaces and of all internal data paths.		Data ports for critical security parameters physically separated from other data ports.	
<b>Roles &amp; Services</b>	Logical separation of required and optional roles and services.	Role-based operator authentication.	Identity-based operator authentication.	
<b>Finite State Machine</b>	Specification of finite state machine model. Required states and optional states. State transition diagram and specification of state transitions.			
<b>Physical Security</b>	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope.
<b>EEP/EFT</b>	No requirements.			Temperature and voltage.
<b>Software Security</b>	Specification of software design. Relate software to finite state machine model.		High-level language implementation.	Formal model. Pre- and post-conditions.
<b>Operating System Security</b>	Executable code. Authenticated. Single user, single process.	Controlled access protection (C2 or equivalent)	Labeled protection (B1 or equivalent). Trusted communications path.	Structured protection (B2 or equivalent).
<b>Key Management</b>	FIPS approved generation/distribution techniques.		Entry/exit of keys in encrypted form or direct entry/exit with split knowledge procedures.	
<b>Cryptographic Algorithms</b>	FIPS approved cryptographic algorithms for protecting unclassified information.			
<b>EMI/EMC</b>	FCC Part 15, Subpart J, Class A (business use). Applicable FCC requirements (for voice).		FCC Part 15, Subpart J, Class B (Home use).	
<b>Self-Tests</b>	Power-up tests and conditional tests.			

### Summary of Physical Security Requirements

Table C-2 summarizes the physical security requirements for Security Levels 1 through 4. Note that only the column labeled “Single Chip Modules” is applicable to the types of token technologies addressed in this report. (Table C-2 is the same as Table 2 from Section 4.5 of FIPS Publication 140-1.)

**Table C-2: Summary of Physical Security Requirements**

	<b>Single Chip Modules</b>	<b>Multi-Chip Embedded Modules</b>	<b>Multi-Chip Standalone Modules</b>
<i>Security Level 1</i>	Production-grade chip (with standard passivation).	Production-grade chip and production-grade multi-chip embodiment.	Production-grade chips, production-grade multi-chip embodiment, and production-grade enclosure.
<i>Security Level 2</i>	Level 1 requirements. Opaque tamper-evident coating.	Level 1 requirements. Opaque tamper evident coating.	Level 1 requirements. Opaque enclosure with mechanical locks or tamper-evident seals for covers and doors.
<i>Security Level 3</i>	Levels 1 and 2 requirements. Hard, opaque tamper-evident coating.	Levels 1 and 2 requirements. Hard opaque potting material, strong non-removable enclosure, or strong removable cover with removal detection and zeroization circuitry. Protected vents.	Levels 1 and 2 requirements. Hard, opaque potting material, or strong enclosure with tamper response and zeroization circuitry for covers and doors. Protected vents.
<i>Security Level 4</i>	Levels 1, 2, and 3 requirements. Hard, opaque removal-resistant coating. EFP/EFT for temperature and voltage.	Levels 1, 2, and 3 requirements. Tamper detection envelope with tamper response and zeroization circuitry. EFP/EFT for temperature and voltage.	Levels 1, 2, and 3 requirements. Tamper detection/response envelope with zeroization circuitry. EFP/EFT for temperature and voltage.

## Appendix D

### Acronyms and Glossary of Terms

#### Acronyms

ANSI	American National Standards Institute
API	Application Programming Interface
ATM	Automated Teller Machine
CA	Certificate Authority
CAC	Common Access Card
COTS	Commercial Off the Shelf
CP	Certificate Policy
DEERS	Defense Enrollment Eligibility Reporting System
DEPSECDEF	Deputy Secretary of Defense
DES	Data Encryption Standard
DMS	Defense Messaging System
DoD	Department of Defense
DON	Department of the Navy
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EEPROM	Electrically Erasable Programmable Read-Only Memory
FIPS	Federal Information Processing Standard
FY	Fiscal Year
GSM	Global System for Mobile
IC	Integrated Circuit
ISO	International Standards Organization
KB	Kilobyte
KEA	Key Exchange Algorithm
LRA	Local Registration Authority
MS CAPI	Microsoft Cryptographic Application Programming Interface
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PC/SC	Personal Computer Smart Card
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
POS	Point of Sale
RA	Registration Authority
RAPIDS	Real-time Automated Personnel Identification System
RF	Radio Frequency
RSA	Rivest, Shamir, Adleman (encryption algorithm)
SCSI	Small Computer Systems Interface
USB	Universal Serial Bus

## Glossary of Terms

access	Ability to make use of any information system (IS) resource.
access control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
biometric	A physical or behavioral characteristic of a person.
byte	8 bits
certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.
confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
cryptographic key (key)	A parameter used in conjunction with a cryptographic algorithm that determines: <ul style="list-style-type: none"><li>• the transformation of plaintext data into ciphertext data,</li><li>• the transformation of ciphertext data into plaintext data,</li><li>• a digital signature computed from data,</li><li>• the verification of a digital signature computed from data, or</li><li>• a data authentication code (DAC) computed from data.</li></ul>
cryptographic module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
digital signature	A non-forgeable transformation of data that allows the proof of the source (with non-repudiation) and the verification of the integrity of that data.
form factor	The physical size and shape of a component.
hardware	The physical equipment used to process programs and data in a cryptographic module.
initialization vector (IV)	A vector used in defining the starting point of an encryption process within a cryptographic algorithm (e.g., the DES Cipher Block Chaining [CBC] mode of operation).

---

input data	Information that is entered into a cryptographic module for the purposes of transformation or computation.
integrity	Protection against unauthorized modification or destruction of information.
interface	A logical section of a cryptographic module that defines a set of entry or exit points that provide access to the module, including information flow or physical access.
key exchange	The process of exchanging public keys in order to establish secure communication.
kilobyte	1,024 bytes
password	A string of characters used to authenticate an identity or to verify access authorization.
personal identification number (PIN)	A 4- to 12-character alphanumeric code or password used to authenticate an identity, commonly used in banking applications.
plaintext key	An unencrypted cryptographic key that is used in its current form.
port	A functional unit of a cryptographic module through which data or signals can enter or exit the module. Physically separate ports do not share the same physical pin or wire.
privacy	State in which data and system access is restricted to the intended user community and target recipient(s).
private key	A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity and not made public.
public key	A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and which may be made public.
public key (asymmetric) cryptographic algorithm	A cryptographic algorithm that uses two related keys, a public key and a private key; the two keys have the property that, given the public key, it is computationally infeasible to derive the private key.
public key infrastructure (PKI)	Framework established to issue, maintain, and revoke public key certificates.
registration authority (RA)	Entity responsible for identification and authentication of certificate subjects that has automated equipment for the communication of applicant data to Certification Authorities and does not sign or directly revoke certificates.
zeroization	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data.