Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

More Than a Pretty Face, Biometrics and SmartCard Tokens

In the modern world, there is an ever-growing need to authenticate and identify individuals automatically. The current technologies of using a personal identification number (PIN) or password for these purposes are inadequate because they are disclosable, transferable and hard to remember. Biometric-based authentication and identification methods are emerging as the most reliable. With rapid progress in electronic and Internet commerce, there is also a growing need to authenticate the identity of a person for secure tr...

Copyright SANS Institute
Author Retains Full Rights

AD

More than a pretty face, Biometrics and SmartCard Tokens

Gregory Williams
GSEC
Gregory018
12/24/01

1.0 Introduction

In the modern world, there is an ever-growing need to authenticate and identify individuals automatically. The current technologies of using a personal identification number (PIN) or password for these purposes are inadequate because they are disclosable, transferable and hard to remember. Biometric-based authentication and identification methods are emerging as the most reliable. With rapid progress in electronic and Internet commerce, there is also a growing need to authenticate the identity of a person for secure transaction processing.

The goal of biometric authentication is to determine if the user is the authentic enrolled user or an impostor. Assuming the user has previously enrolled, positive verification or identification consists of quality input, processing and successful outcome of the matching process.

When designing a system to handle large population identification, accuracy and reliability of authentication are significant challenges. The biometric systems need to handle variations, distortions and noise in inputs from the real world This paper will address many of the types of Biometrics available as well as the use of smart card technology.

2.0 Biometrics Technology

The word biometrics comes from the Greek words bio and metric, meaning "life measurement". By measuring something unique about an individual and using that to identify them, we can achieve a dramatic improvement in security of the key store. Biometrics involves using the different parts of the body, such as the fingerprint or the eye, as a password or form of identification. Practically all-biometric systems work in the same manner. First, a person is enrolled into a database using the specified method. Information about a certain characteristic of the human is captured. This information is usually placed through an algorithm that turns the information into a code that the database stores. When the person needs to be identified, the system will take the information about the person again, translates this new information with the algorithm, and then compare the new code with the ones in the database to discover a match and hence, identification.[10]

This method of identification is preferred over traditional methods involving passwords and PIN numbers for various reasons:

- The person to be identified is required to be physically present at the point-of-identification
- Identification based on biometric techniques, gets rid of the need to remember a password or carry a token

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

With the increased use of computers as vehicles of information technology, it is necessary to restrict access to sensitive/personal data. By replacing PINs, biometric techniques can potentially prevent unauthorized access to or fraudulent use of automatic teller machines (ATMs), cellular phones, smart cards, desktop PCs, workstations, and computer networks. PINs and passwords may be forgotten, and token based methods of identification like passports and driver's licenses may be forged, stolen, or lost. Various types of biometric systems are being used for real-time identification, the most popular are based on face recognition and fingerprint matching. However, there are other biometric systems that utilize iris and retinal scan, speech, facial thermograms, and hand geometry. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user.

2.1 Biometric authentication consists of the following steps:

- Capture human input
- Filter out unwanted input such as noise
- Generate a statistical representation of the biometric input (template)
- Perform a match against biometric information previously gathered and stored during an enrollment procedure

2.2 Two methods of biometric authentication are defined below:

- Verification is the process of verifying the user is who they claim to be
- Identification is the process of identifying the user from a set of known users [12]

The goal of biometric authentication is to determine if the user is an authentic enrolled user or an impostor. Assuming the user has previously enrolled, positive verification or identification consists of quality input, processing and successful outcome of the matching process.[12]

2.3 Procedure for authenticating yourself to a computer application:

1. Insert your smart card into a reader. The smart card contains your cryptographic keys and biometric fingerprint data.
2. Enter your shared-secret PIN (or password), in order to unlock the digital representation of your fingerprint.
3. Place your finger on the scanner. The scanned fingerprint is compared to the fingerprint data on the smart card.
4. If the data matches, the smart-card fingerprint data is converted into a number and combined with the smart-card secret PIN (retrieved in Step 2) and used as a symmetric cryptographic key to decrypt the private key.
5. A nonce (**random number**) is passed from the computer application to the smart card.
6. The private key on the smart card is used to encrypt the nonce and pass it back to the application.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

7. The application verifies that a certified public key obtained from the network-based directory service or from the card does decrypt the encrypted message from the card and reveal the same nonce that was originally passed to the card. [21]

2.4 Primary biometrics disciplines include:

- Finger-scan (optical, silicon, ultrasound, touchless)
- Facial-scan (optical and thermal)
- Voice-scan (not to be confused with speech recognition)
- Iris-scan
- Retina-scan
- Hand-scan
- Signature-scan
- Keystroke-scan
- Palm-scan

2.5 Disciplines with reduced commercial viability or in exploratory stages include:

- DNA
- Ear shape
- Odor (human scent)
- Vein-scan (in back of hand or beneath palm)
- Finger geometry (shape and structure of finger or fingers)
- Nailbed identification (ridges in fingernails)
- Gait recognition (manner of walking) [20]

2.6 Benefits and Problems

There are three basic levels or stages of security. The lowest level involves something the user knows, such as a password or PIN . The next level is something the user has--an ID card, for example.. Combining these makes for tighter security and is the technique used with most automatic teller machines9 ATMs). However, these levels fall short of conclusively identifying an individual. In contrast, biometric systems base authentication on physical characteristics (what the user is) that cannot be shared or easily compromised. Combining a biometric with a PIN or password is stronger still.

The ICSA 1999 Biometrics Survey (www.icsa. net/) notes that for all the potential of biometric-based security, it still hasn't caught on with most industries. One reason is that biometric devices have been expensive, though lately prices have come down--some start as low as $100 per seat. Also, biometric systems usually require additional equipment on the PC. And integrating biometric user verification with existing applications has been difficult. This, however, is not because of a lack of standards.

3.0 How they work

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

3.1 Fingerprint Recognition

A fingerprint recognition system analyzes and compares a finger's unique set of ridge patterns and minutiae (the places where the finger's ridges stop, fork, break, for example). [11]

This system consists of a hardware scanner and recognition software which records specific fingerprint characteristics, saves each user's data in a template, and then refers to the templates when the user next tries to gain access. Fingerprint systems are accurate, but they can be affected by changes in the fingerprint (burns, scars, and so on) and by dirt and other factors that distort the image. [11]

> Fingerprint identification begins with the ridge, the raised surface of skin on a finger. Fingerprint recognition systems record these patterns of ridges in a database, then compare subsequent readings against this database to make an identification. Current fingerprint systems for the PC record several fingerprints per person.
>
> Each fingerprint has one of three basic patterns: loop, whorl, or arch. In a loop pattern, the ridges start from one side of the finger, then reach the core point (approximately the center) of the finger and "loop" back to the same side. In a whorl pattern, some ridges form more or less concentric circles around the center of the finger, and the remainder shape themselves around these circles. The ridges in the arch pattern begin at one side of the finger and end at the other, forming a kind of arch over the center. Some fingerprints combine two or more of these basic patterns.
>
> Just as important as the type of pattern are a print's minutiae, the points where the ridges stop, fork, break, or change in other ways. Minutiae can include any of the following:
>
> **Bifurcation**: The point where a ridge splits into multiple ridges, called branches.
>
> **Divergence**: The point that marks where a set of nearly parallel ridges spread apart or come together.
>
> **Enclosure**: Where a ridge splits into two branches and then reunites a short distance later.
>
> **Ending**: Where a ridge terminates.
>
> **Valley**: The space on either side of a ridge.
>
> Each minutia is classified according to criteria such as its position on an x,y coordinate system, the space between the ridges at that point, the curvature of the ridges, and so forth. The entire fingerprint is the total of all its characteristics, including the pattern and all the minutiae.[11]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Fingerprint Recognition Technology

Recognition systems capture fingerprints and record their characteristics. The images themselves are not stored. The two primary hardware technologies used in finger-imaging systems are optical and capacitive. In an optical system, the finger is placed on a glass surface, and an internal light source highlights the ridges. The capturing device typically uses a sensor based on a CCD (charge-coupled device) like those used in scanners and digital cameras.

The problem is that oil and dirt from fingers can collect on the sensing area, leaving a kind of ghost impression called a latent image. Over time, latent images can degrade the device's ability to capture a print accurately. Hardware makers have developed several means of dealing with this problem. One method includes keeping the most recently noted latent image in memory, then erasing the image from the scan itself so only the new print remains.

Capacitive systems use a sensor chip, an array of circuits that creates an image of the fingerprint by measuring the electrical field surrounding it. This type of system is very precise, but direct contact from users' fingers could damage the device in the long run. It is possible to combine optical and capacitive systems. One product uses an opaque electro-optical polymer film sensor to read the finger's electrical field and convert it into an optical image; the device then digitizes that image into data.

Fingerprint Recognition Products

American Biometric BioMouse Plus
Compaq Fingerprint Identification Technology
Digital Persona U.are.U Deluxe
Identicator BioLogon
Identix TouchSafe Personal
Saflink SAF/nt 2.0
Sony Fingerprint Identification Unit

3.2 Face Recognition

Sophisticated image-processing software identifies patterns and spatial relationship in faces. Some products use thermal imaging to create maps of subcutaneous blood vessels.[11]

Recognizing the shapes and positioning of the features of a person's face is a complex task, and face recognition software has only recently begun to accomplish it. First a camera captures the image of a face, and then the software extracts pattern information it can compare with user templates. [11]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The face recognition process has two major parts: detection, locating a human face in an image and isolating it from other objects in the frame, and recognition, comparing the face being captured with a database of faces to find a match.

During detection, the hardware/software combination isolates the facial elements of an image and eliminates extraneous information. The software examines the image for typical facial structures (such as eyes and nose), and once it has found them, it calculates the remainder of the face. It then cuts away background details, leaving a close-up of a face inside a rectangular frame called a binary mask.

Recognition operates according to principles such as eigenfaces or eigenfeatures. (The German eigen refers in this case to the recursive mathematics used to analyze unique facial characteristics.) An eigenface-based system sees each facial image as a two-dimensional set of light and dark areas (eigenfaces) arranged in a particular pattern. The recognition algorithm stores each image as a combination of eigenfaces and then compares the eigenface characteristics of the current face with those in the database.

An eigenfeature-based system focuses on specific features such as the nose, eyes, mouth, eyebrows, and bone curvatures, and the relative distances between them. The system analyzes the currently scanned face and extracts particular eigenfeatures, then compares these with other analyses in the database. Eigenfeature systems typically work in conjunction with eigenface systems to produce the most accurate identification possible. In general, eigenfeature systems are more accurate in identifying faces despite substantial variations such as beards and glasses.

A major difficulty for face recognition systems is that a person's face changes over time. The system must take these changes into account--not only for the face being captured but all other faces in the database as well--to make the correct identification.

All face recognition products store multiple images for each user, and they depend on a set of rules to determine identity from all the relevant data. Some products use artificial intelligence neural-network technology, in which a system effectively learns from experience. In a face recognition system, this learning process allows the system to narrow the range of facial types in the database to which it compares the current face.

Face recognition systems can and do work with only frontal facial images, but some systems offer increased security by storing both front and side views. This produces a 3-D map of the face, eliminating the security problem of imposters showing photographs of legitimate users to the camera. If the recognition system does not detect three-dimensionality, it refuses access.

Another approach uses thermal imaging. These systems use infrared cameras to capture the pattern of blood vessels under the facial skin. These systems offer the advantage of being less susceptible to changes in the skin's surface or to the positioning of the head and can operate in darkness.[12]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Face Recognition Products
FaceIt NT
TrueFace Network

3.3 Iris Recognition

An eye recognition system uses a video camera to capture complex patterns of tissues in the iris or or blood vessels in the retina. This is considered the most secure method.

Iris recognition The pattern of the iris (the band of tissue that surrounds the pupil of the eye) is complex, with a variety of characteristics unique in each person. An iris recognition system uses a video camera to capture the sample and software to compare the resulting data against stored templates.

Retina recognition. Probably the single most secure of all, these biometric systems work with the retina, the layer of blood vessels located at the back of the eye. The retinal image is difficult to capture, and during enrollment the user must focus on a point while holding very still so the camera can perform the capture properly. The only thing that is actually determined is the pattern of the blood vessels, but since this pattern is unique in each person, identification can be precise.

The two eye-based systems, iris and retina, are generally considered to offer the best security, because of the distinctiveness of the patterns and the quality of the capture devices.[11]

3.4 Hand Recognition

These systems create a three-dimensional image of hands (or fingers) and analyze the relative shapes, lengths, areas, and positions of fingers, knuckles, and so on.

Hand geometry. With this system, the user aligns a hand according to guide marks on the hand reader hardware, and the reader captures a three-dimensional image of the fingers and knuckles and stores the data in a template. Hand geometry has been around for several years, and it was used for a security system at the 1996 Olympic games.

Finger geometry. These devices are similar to hand geometry systems. The user places one or two fingers beneath a camera that captures the shapes and lengths of the areas of the finger and the knuckles. The system captures a three-dimensional image and matches the data against the stored templates to determine identity.

Palm recognition. Similar to fingerprint recognition, palm biometrics focuses on the various textures, such as ridges and other minutiae, found on the palm.[11]

3.5 Voice recognition

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Voice systems record speech and analyze the speaker's tone and inflection. Accuracy can be affected by normal variations caused by illness, fatigue, and mood changes.

This method captures the sound of the speaker's voice as well as the linguistic behaviors. Its primary use is in telephone-based security applications, but its accuracy can be affected by such things as extraneous noises and the effects of illness or fatigue on the voice. One obvious problem with voice recognition is fraud: The system can be fooled by a tape of someone's voice. For this reason, advanced voice systems can extend the verification process by giving the user longer and more difficult phrases to read aloud, or requesting a different phrase to be read each time. This does increase the time needed for verification, however, and thus cuts into the system's overall usability.[11]

Voice Authentication Product Reviews
Citadel GateKeeper
voicecrypt 2.01

3.6 Signature recognition

Signature recognition systems note not only shape but also pen pressure, speed, and the points where the pen leaves the paper. Normal variations make multiple samples necessary.

Signature verification systems have one major thing going for them: public acceptance. On everything from the Declaration of Independence to a credit card slip, people tend to accept a person's signature as proof of identity. Actually, signature recognition systems, also called dynamic signature verification systems, go far beyond simply looking at the shape of a signature: They measure both the distinguishing features of the signature and the distinguishing features of the process of signing. These features include pen pressure, speed, and the points at which the pen is lifted from the paper. These behavioral patterns are captured through a specially designed pen or tablet (or both) and compared with a template of process patterns. The problem is that our signatures vary significantly over time and from one instance to another. [11]

3.7 Comparison 0f Biometric Techniques

ID Type	Strengths	Weaknesses	Cultural Concerns
Fingerprint	Accurate Widely available Cheap Small reader	3 to 7 percent of population does not have usable print	Some countries Prohibit fingerprint Images for uses Other than criminal Justice.
Iris	Very accurate Image never changes	Perceived as intrusive. Camera experience.	Unacceptable in some cultures.
Retina	Highest accuracy	Perceived as intrusive. Head	Unacceptable in some cultures.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

		must be still during scan.	
Facial Image	Not considered intrusive Cheap	Less accurate. Image changes.	Unacceptable where photos are prohibited.
Facial Thermogram	Very accurate	Not yet commercially available	May be unacceptable where photos are prohibited.
Voice	Not considered intrusive. Only biometric for telephone use	Less accurate	None
Hand Geometry	Not considered intrusive.Fast. Low data storage	Less accurate. Large reader. May change	None
Signature Dynamics	Not considered intrusive. Convenient for financial transactions.	Less accurate. Multiple samples required	None

1998 Unisys Corporation [13]

Choosing a biometric system often involves balancing the sensitivity of the data against the cost of protecting it and the likelihood the technology will be accepted.[13]

4.0 What is a Smart Card?

Smart Cards are a tamper-resistant and portable way to provide security solutions for tasks such as client authentication, logging on to a Windows 2000 domain, code signing and securing e-mail.

Smart cards provide:

- Tamper-resistant storage for protecting private keys and other forms of personal information.
- Isolation of security-critical computations involving authentication, digital signatures, and key exchange from other parts of the organization that do not have a "need to know".
- Portability of credentials and other private information between computers at work, home, or on the road. [1]

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

A smart card is a card that is embedded with either a microprocessor and a memory chip or only a memory chip with non-programmable logic. The microprocessor card can add, delete, and otherwise manipulate information on the card, while a memory-chip card (for example, pre-paid phone cards) can only undertake a pre-defined operation.

Smart cards, unlike magnetic stripe cards, can carry all necessary functions and information on the card. Therefore, they do not require access to remote databases at the time of the transaction.

4.1 Today, there are three categories of smart cards:

Integrated Circuit (IC) Microprocessor Cards. Microprocessor cards offer greater memory storage and security of data than a traditional mag stripe card. Chip cards also can process data on the card.

. Some examples of these cards are:

- Cards that hold money ("stored value cards")
- Card that hold money equivalents (for example, "affinity cards)
- Cards that provide secure access to a network
- Cards that secure cellular phones from fraud
- Cards that allow set-top boxes on televisions to remain secure from piracy

Integrated Circuit (IC) Memory Cards. IC memory cards can hold up to 1-4 KB of data, but have no processor on the card with which to manipulate that data. Their memory can be rewritten.

Optical Memory Cards. Optical memory cards can store up to 4 MB of data. But once written, the data cannot be changed or removed. Thus, this type of card is ideal for record keeping - for example medical files, driving records, or travel histories. Today, these cards have no processor in them [2]

4.2 Understanding smart cards

Logging on to a network with a smart card provides a strong form of authentication because it uses cryptography-based identification and proof of possession when authenticating a user to a domain.

For example, if a malicious person obtains a user's password, that person can assume the user's identity on the network simply through use of the password. Many people choose passwords they can remember easily, which makes passwords inherently weak and open to attack.

In the case of smart cards, that same malicious person would have to obtain both the user's smart card and the personal identification number (PIN) to impersonate the user. This combination is obviously more difficult to attack because an additional layer of information is needed to impersonate a user. An additional benefit is that, after a small number of

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

unsuccessful PIN inputs occur consecutively, a smart card is locked, making a dictionary attack against a smart card extremely difficult

4.3 Using Smart Card Authentication on Windows 2000. A How To.

The following simplified how to, was taken from Microsoft 2000 documentation, installing Smart Cards on Windows 2000 Server. This is includes for reference and to demonstrate how easy it is to install and use Smart Card Authentication in a Windows 2000 environment. See Microsoft Documentation for further assistance. http://www.microsoft.com/windows2000/en/server/help/ ©2000 Microsoft Corporation. All rights reserved. Terms of Use.

4.3.1 To install a smart card reader on a computer

1. Shut down and turn off the computer.
2. Depending on the type of reader you have purchased, attach your reader to an available serial port or insert the PC card reader into an available PCMCIA Type II slot.
3. Restart your computer and log on as an administrator.
4. Install the drivers for your particular smart card reader. Windows 2000 comes with drivers for a variety of readers. If yours is not included with Windows 2000, follow the manufacturers instructions included with your smart card reader.

4.3.2 Supported smart cards

When you install Windows 2000, support for the Gemplus GemSAFE and Schlumberger Cryptoflex smart cards is included in the default installation. You do not need to configure anything on the client or server to use either of these cards. Cryptographic smart cards can only be obtained directly from the respective companies and not from Microsoft Corporation.

While support for these cards is included in Windows 2000, other RSA-based cryptographic smart cards will also work with Windows 2000, provided the card vendor has developed acryptographic service provider(CSP) for the card using CryptoAPI and the Smart Card Software Developer's Kit, which is available through Microsoft Developer's Network (MSDN).

Smart card personal identification numbers (PINs) can be changed anytime the CSP displays the private key PIN dialog box. PIN management is the responsibility of the card CSP and the user. Windows 2000 does not manage PINs.[1]

4.3.3 To set up a smart card for user logon

1. Log on as an enrollment agent for the domain where the user's account is located.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

2. Open Internet Explorer

3. From Internet Explorer, in **Address**, type the address of the certification authority that issues smart card logon certificates , and then press ENTER.

4. Click **Request a certificate**, and then click **Next**. Click **Advanced request**, and then click **Next**.

5. Click **Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station**, and then click **Next**. If you are prompted to accept the smart card signing certificate, click **Yes**.

6. On the **Smart Card Enrollment Station** Web page, in **Certificate Template**, do one of the following:

   - Click **Smart card Logon** if you want to use the smart card for logging on to windows only.

   - Click **Smart card User** if you want to use the smart card for secure e-mail as well as logging on to Windows.

7. In **Certification Authority**, click the name of the CA you want to issue the smart card certificate.

8. In **Cryptographic Service Provider**, select the cryptographic service provider of the smart card's manufacturer.

9. In **Administrator Signing Certificate**, click the Enrollment Agent certificate that will sign the enrollment request.

10. In **Enter User Name**, click the appropriate user account, and then click **Submit Certificate Request**.

11. When prompted by the system, insert the smart card into the smart card reader on your computer, click **OK**, and then, when prompted by the system, enter the personal identification number (PIN) for the smart card.

12. (Optional) If the smart card you are setting up has a previously installed certificate on it, a message appears, asking whether you want to replace the existing credentials on the card. Click **Yes**.

13. After the certificate is installed on the smart card, the CA Web page will give you the option of viewing the certificate you just installed or beginning a new smart card certificate request.

    For step 1, anyone in the domain who has an Enrollment Agent certificate and has security permissions to issue smart card certificates is considered an "enrollment agent".

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

4.3.4 To log on to a computer with a smart card

1. At the Windows logon screen, insert your smart card in the reader.
2. Type the personal identification number (PIN) for the smart card when prompted by your computer
   - If the PIN you enter is recognized as legitimate, this logs you on to the computer and to the Windows domain, based on the permissions assigned to your user account by the domain administrator
   - If you enter the incorrect PIN for a smart card several times in a row, you will be unable to log on to the computer using that smart card. The number of allowable invalid log on attempts before lock out occurs varies according to the smart card manufacturer. Contact your administrator for a replacement

4.3.5 To prepare a certification authority to issue smart card certificates

1. Confirm that the proper security permissions are set on the Smart Card Logon, Smart Card User, and Enrollment Agent certificate templates. For more information, see Related Topics.
2. Log on with administrator rights to the certification authority you will be using to issue smart card certificates .
3. Open Certification Authority
4. If you want to issue certificates that are only for Windows logon via smart cards:
   - In the console tree, click **Policy Settings**.
   - On the **Action** menu, point to **New**, and then click **Certificate to Issue**.
   - Click the **Smart Card Logon** certificate template , and then click **OK**.
5. If you want to issue certificates that can be used for secure e-mail as well as Windows logon via smart cards:
   - In the console tree, click **Policy Settings**.
   - On the **Action** menu, point to **New**, and then click **Certificate to Issue**.
   - Click the **Smart Card User** certificate template, and then click **OK**.
6. In the console tree, click **Policy Settings**.
7. On the **Action** menu, point to **New**, and then click **Certificate to Issue**.
8. Click the **Enrollment Agent** certificate template, and then click **OK**.
   - To open **Certification Authority**, click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Certification Authority**

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- The security permission setting of a certificate template indicates who is allowed to request a certificate of that type.
- The Enrollment Agent certificate does not have to be issued from the same CA that will issue certificates for smart cards (as illustrated in this procedure). The issuing CA for the Enrollment Agent certificate just needs to be a trusted enterprise CA in the domain. In that case, you need to make sure that there is an enterprise CA in your domain capable of issuing Enrollment Agent certificates by following steps 1, 2 and 5-7 on that CA
- This procedure only applies to enterprise CAs [1]

5.0 Summary

SINCE SEPT. 11, previously obscure security concepts such as biometrics have become front-page headlines. Cries for tighter security in all aspects of our daily lives are everywhere. Clearly, businesses must implement basic security measures as part of their basic responsibilities. Even in small and privately held companies, Information Technology (IT) security is recognized as a responsibility that, although it doesn't look anything like the traditional physical security measures, is increasingly important today.

Much of the threat of cyber terrorism stems from a perception that computer systems are not secure. This perception is usually true to some degree because the very act of networking computer systems implies that security has been compromised. The increasing pervasiveness of Internet technology has only made matters worse; universally accessible technology means that it is available to the bad guys as well as the good ones. Biometrics offers at least in part a way to defend against cyber terrorism and provide increased network security.

6.0 References

1. Smart Cards, Microsoft white pages, Windows 2000 Server Documentation
   URL: **http://www.microsoft.com/windows2000/en/server/help/**

2. What is a Smart Card?
   URL: http://java.sun.com/products/javacard/smartcards.html

3. An overview of Smart Card Security
   URL: http://home.hkstar.com/~alanchan/papers/smartCardSecurity/

4. Smart Card Basics .Com
   URL: http://www.smartcardbasics.com/

5. SCIA Smartcard Overview
   URL: http://www.scia.org/

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

6. Network Security by Eric Maiwald, Osborne/McGraw-Hill copyright 2001
Smart Cards, Biometrics P10-11 and P179.

7. Magazine Article, Biometric Security, Dr, Dobb's Journal, Computer Security.
P 93-96.

8. Overview of a SmartCard
URL: http://home.hkstar.com/~alanchan/papers/smartCardSecurity/

9. The Basics of Biometrics
URL: http://library.thinkquest.org/28062/?tqskip=1

10. An Overview of Biometrics
URL: http://biometrics.cse.msu.edu/info.html

11. Biometric Security: How it works
URL: http://www.zdnet.com/pcmag/features/biometrics/

12. Biometric Digest
URL: http://www.biodigest.com/index.asp

13. Biometric Basics
URL: http://www.unisys.com/execmag/1998-12/journal/sidebar1.htm

14. Buyer's Guide: Biometrically speaking
URL: http://www.networkcomputing.com/1017/1017buyers2.html

15. Tests of Biometrics "Six Biometric Devices Point the Finger at Network Security"
URL: http://www.networkcomputing.com/910/910r1.html

16. ICSA 1999 Biometrics Survey
URL: http://www.icsa.net/

17. Biometric Basics 4/6/99 issue of PC Magazine
URL: http://www1.zdnet.com/pcmag/pctech/content/18/07/tu1807.001.html

18. Are you ready for biometrics
URL: http://www1.zdnet.com/pcmag/features/biometrics/

19. Biometric Security
URL: http://www1.zdnet.com/pcmag/features/biometrics/how.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

20. Biometrics Explained
URL: http://www.biometricgroup.com/

21. Smart Cards and Biometrics: Your Key to PKI *The cool way to make secure transactions*.
by David Corcoran, David Sims and Bob Hillhouse

22. Biometric Overview
URL: http://www.infosyssec.com/infosyssec/biomet1.htm

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced