



BIOCENTRIC

SOLUTIONS

I N C O R P O R A T E D

**WHITE PAPER:
Why use a biometric and a
card in the same device?**

8417 Excelsior Drive, Madison, WI 53717-1901
Tel: 608-821-0821 Fax: 608-821-0822

www.biocentralsolutions.com

Introduction

Once we consider the question, the advantages of using a biometric for identification are obvious. Each of us has forgotten our password and, in an effort not to forget it the next time, written it down, or chosen one that was easy to remember. In essence we have undermined security for the sake of convenience. The use of biometrics changes all of this. Instead of using what we know to prove who we are, we use some unique feature of ourselves such as a fingerprint, handprint or the sound of our voice. A world that replaces a memory test with a fingerprint scanner is quiet attractive, and there are numerous devices available today that provide secure access based solely on a biometric. Although this is a step in the right direction, this paper makes the argument that more needs to be done.

To get an understanding of the problem let us start with how a biometric, such as a fingerprint, is used to prove our identity. The process begins by making a copy, or template, of our fingerprint. This template must be stored somewhere and kept available for comparison with a live scan of our fingerprint. Where this template is stored is a pivotal question. It could be stored in each individual fingerprint scanner, but for most applications this is highly impractical. A better solution is to store the template in some central database. Now matching a live fingerprint against all the templates in the database can identify an individual, or, if the individual's name is provided with the live fingerprint, the identity can be verified by looking up the template associated with that individual and doing the comparison. As nice as this solution is, it suffers from several disadvantages. Large databases can be very costly to produce and maintain, and when they go down our biometric devices are useless. There is also the question of an individual's right to control personal biometric information. Few of us would like our biometric templates stored in various unknown locations beyond our control. The potential disclosure of this information to unauthorized individuals not only raises questions of individual privacy, but also presents a serious security threat. Without going into the details, we think it is reasonably clear that the more difficulty a potential adversary has in obtaining a legitimate biometric template, the more secure the identification process.

Our solution to this problem is to store the biometric template on a token, which is read by the same device that gathers the live biometric. Webster defines a token as "something serving as a sign of authority, identity, [or] genuineness..." Here the token is used to tie a physical attribute (our biometric) with our identity. We will consider three different types of tokens: a read only token represented by a plastic card with a PDF417 patch which we will call an optical card, a read and write token represented by a memory card, and a smart token represented by a smart card. By using one of these tokens our biometric/token reader can compare a person's template and live biometric without ever having to communicate with some external device. The comparison can be done within the reader. The purpose of this paper is to show how these tokens can provide a convenient, secure identification process that protects the individual's privacy. To do this we first need to review a few critical facts about some modern cryptographic methods.

Public key cryptography

Imagine that you are in command of a submarine hiding somewhere in the middle of the Atlantic Ocean. You are running out of supplies and need to meet your supply ship soon. To set up a rendezvous you send a message to the supply ship asking it to meet you at a certain latitude and longitude at a particular time. There is an enemy destroyer sitting nearby that is listening intently for any signal from your submarine, and if it is able to read that signal then you are in a great deal of trouble. To prevent this you encrypt the message. If this scenario was unfolding during W.W.II you would have several good encryption algorithms available. Today we call them symmetric encryption algorithms, meaning that both the encryption and decryption keys are the same. As long as you and the supply ship shared the same special secret key then you could both communicate securely. Unfortunately, if the destroyer had also obtained this key, maybe from another submarine it recently captured, it could also read your encrypted communications. Even if you knew this you could do little. Setting up a new secret key would require a meeting with your supply ship - a cryptographic Catch-22 with some serious consequences.

Today you would be in a far better situation. You could use a public key algorithm to communicate securely. These algorithms are called asymmetric, because the key used to encrypt a message is different from the key needed to decrypt a message. More importantly, given the encryption key it is very difficult to determine the decryption key. This allows us to publicly distribute the encryption key while keeping the decryption key secret; thus the name public key cryptography. Now every submarine in the fleet can generate its own public/private key pair and publicly distribute the encryption key. Even if a private key is compromised, a new pair can be generated. There is a problem with the slowness of public key algorithms, but this can be overcome by using them to transmit a random number. The random number is then used as the secret key for some faster symmetric algorithm, which in turn is used to encrypt the message.

The development of RSA and Diffie-Hellman in the 1970's provided the tools needed to do public key cryptography. But these tools solve more than just the problem described above. They also provide a way to produce digital signatures. There exist things called hashing algorithms that are very good at taking long messages and converting them to fixed length numbers or hash values. "Good" means that changing one letter in the message will result in changing about half of the bits in the hash value. Since these hash values are very large, the odds that two messages will give the same hash value is very small. Thus, for all practical purposes, hash values can be used as an almost unique representation of the original message. To take advantage of this, use the public key algorithm again, but this time call the private value the signing key and the public value the verification key. If we encrypt the hash value with the signing key then everyone can decrypt with the verification key. By also making the hashing algorithm public, anyone can verify that the hash value encrypted by the signing key actually matches the hash value produced by the hashing algorithm. In other words, we have a way to produce a digital signature that anyone can verify.

As long as we can be sure of the identity of the person holding the private signing key, digital signatures provide the perfect mechanism for authentication, integrity and nonrepudiation. Unfortunately, guaranteeing a person's identity under certain circumstances is not easy. The establishment of a Public Key Infrastructure, or PKI, is aimed at solving this problem. Some have suggested that one strong component of this PKI should be biometrics. In the discussion that follows it will become clear how public key and biometrics provide the strongest security when used together.

Combining the biometric and card reader

Before discussing the three types of tokens mentioned in the introduction it is important to consider the device or reader that will be reading the token and handling the biometric measurements. We have already discussed the simplest situation where a biometric reader sends information directly to another device, such as a computer, for comparison with a previously stored template. It is possible to have a second reader handle the token and send information stored on it to the computer. There are several products on the market today that have both a token reader and a biometric reader send information to a computer where the information on the token is compared with the information coming from the biometric reader. Some of these products combine the two readers into one module while others keep the two readers separate. In our opinion this is not much of an improvement over the use of a biometric reader alone; sensitive biometric and other information is being removed from the token and thus being put at risk of exposure.

Often these products encrypt the information being sent from the token reader to the computer and may even encrypt the live biometric being sent. Of course, this is the correct thing to do under the circumstances, but sensitive biometric information is still being exposed to the less secure environment of the computer. We feel that it is far more desirable to keep the biometric template from ever leaving the reader, and at all other times to keep the template within the token. In the same way that it is easier to secure information on a stand-alone computer than on a computer connected to a network, especially the Internet, it is easier to secure information on a special purpose biometric/token reader than on a multi-purpose computational device. During the discussions that follow we will assume such a biometric/token reader where the comparison of the biometric template with the live biometric always occurs within the reader.

The optical card

The first token we will consider is one with read-only capability: specifically, a credit card piece of plastic with a two-dimensional bar code such as a PDF417 patch. Our goal will be to see how we can use this simplest of tokens to provide convenient security while preserving individual privacy. At a minimum the token needs to contain the biometric template and the token holder's name. If we like, it can hold other information such as what the holder has access to and when to allow access. All of this information should be stored in the two-dimensional bar code. Other information can also be on the card, such as a photograph and name allowing the card to double as a standard form of identification.

Take a look at how this token interacts with the biometric/token reader. As before we will assume that the biometric is a fingerprint. When an individual wants to gain access the card is inserted into the reader. The reader verifies that the card is legitimate. Once this has happened the token holder places a finger on the fingerprint scanner. The reader then compares the live fingerprint with the template obtained from the token. If they match the individual is allowed access to whatever the reader is guarding.

To make this procedure secure several things need to be done. We first consider how the biometric/token reader verifies that the token and the information it holds are legitimate. Fortunately, a digital signature of the information in the two-dimensional bar code solves this problem nicely. Here is how it works: during enrollment when the information is stored on the token, the organization issuing the token uses its private signing key to digitally sign the two-dimensional bar code. This allows the public verification key to be stored in all of the readers without fear of giving a potential adversary the ability to forge the digital signature. Unfortunately, a digital signature does not protect the data from disclosure, so the information in the two-dimensional bar code, to include the digital signature, should also be encrypted.

Next we have to consider how the biometric/token reader tells the device it is guarding whether the individual trying to gain access should be admitted. If the target device is a lock on a door then it is possible to protect this signal by physical means such as bolting the biometric/token reader to the wall and then setting up the lock to freeze shut if an unauthorized party removes the reader. Unfortunately, physical means of guarding the connection may not be practical in all situations, such as in the case of computer access; and it isn't good enough just to send a message that says, "OK, let John Doe sign on." Any predictable message like this can be copied by an adversary and used to gain unauthorized entrance. One way to avoid this problem is to use public key cryptography to encrypt the information going between the biometric/token reader and the device it is guarding. Those interested in the sophisticated protocols used today to secure this type of communication may wish to refer to the sources listed below.

Notice that our read-only token was little help in solving the problem in the last paragraph; using the computational power of the reader solved it. Unfortunately, the reader is not as effective at protecting the information contained on the two-dimensional bar code. The reason for this is subtle. Remember that we said this sensitive information needed to be encrypted. This certainly protects information from just being read right off of the card, but the encryption requires that every biometric/card reader contain the decryption key for every token that might be used in it. In practical terms, this will usually mean that every biometric/token reader an organization has will contain the same decryption key. Thus, if even one reader is compromised then an adversary will be able to read sensitive information on anyone's card. This is not to say that the adversary will now have the ability to circumvent our biometric/token reader. The private signing key is necessary for that, and the private signing key can be kept much more secure since it is only used to make the cards. Still, it would be nice if it were a bit harder for someone to intrude on our token holder's privacy. Fortunately, there is a token that can do this for us. It is a "smart" token, or smart card. We will get to this token later, but first let us see what can be done using a memory card as a token.

The memory card

A memory card is a piece of plastic about the size of a credit card with an embedded memory chip. This token can do all the things our previous read-only token can do, but has the additional advantage of allowing information to be written on it by the biometric/token reader. Storage of this type can be very useful and even add to security. As an example, whenever a holder of a token tries to gain unauthorized entry to a place or device, that failed attempt can be recorded on the token. If the holder tries this once too often, the token can be disabled. Another example would involve a site protected by a number of stand-alone biometric/token readers. The fact that these readers are not networked together would make the collection of time and attendance information difficult using a read-only token, but a memory card could collect this information for later download to some central database where the information can be used to verify an employee's attendance.

There are many more examples of how useful the additional functionality of the memory card can be. One that might not be so apparent is the similarity of the memory card to the smart card. Any biometric/token reader that is configured to read a memory card is already in the correct physical form to read a smart card. Though a great deal of software will need to be added, the necessity to build or design another reader is unlikely. Thus, the memory card makes a nice stepping-stone to the ultimate token, the smart card.

The smart card

Most of us have heard about smart cards, those little computers that we carry around in our pockets disguised as credit cards. We may have wondered what makes them so appealing. In this section we will get a chance to see how the computational power of the smart card can give us some striking improvements in both security and functionality. As they have become more popular, smart card applications have been written for health care, financial services, travel and even loyalty programs. All of these can be

available for use by an institution that decides to use smart cards as their tokens; however, it must be pointed out that multiple applications on a smart card might give rise to some security concerns. Still, the versatility of a smart card is a big plus.

For us, though, the really big advantage of using a smart card is the marked improvement in security that it provides over the other two types of tokens already discussed. Recall that the encryption protecting the biometric template (and other sensitive information on the token) was weakened by the fact that the decryption key had to be held on every reader that accepted that token. The biometric/token reader was capable of decrypting and verifying that the data contained within the token was authentic, but the token had no way of verifying that the reader asking for this information was legitimate. This point is worth repeating; the biometric/token reader can protect itself by only accepting data from legitimate tokens, but optical and memory cards have no way of determining if the reader requesting information from them is legitimate. Smart cards are not as disadvantaged. They have the computational power to authenticate the biometric/token reader before giving up valuable information. This authentication uses all of the public key tools we discussed above and if done correctly protects the sensitive information from disclosure to any unauthorized device.

One final question needs to be addressed before leaving the topic of smart cards: Why not do the comparison of the live and biometric template on the smart card itself? The reason is quite simple. If a single smart card were to be compromised by an adversary then it could be used to gain unauthorized access to every reader originally authorized to take it. By contrast, if a biometric/token reader is compromised then our adversary will gain access only to whatever that reader was guarding. In short, it is best to leave the comparison of the live and biometric template on the reader.

A summary and comparison of the three cards

	Standard Biometric Product Using Token	Optical Card with Biometric/Token Reader	Memory Card with Biometric/Token Reader	Smart Card with Biometric/Token Reader
Biometric template	Sometimes stored on the token	Always stored on the token	Always stored on the token	Always stored on the token
Live biometric and template are compared	On some other device	Within the reader	Within the reader	Within the reader
Biometric template	Leaves the token and the reader	Leaves the token but not the reader	Leaves the token but not the reader	Leaves the token after the token authenticates the reader
Location of secret keys	Varies	In the reader	In the reader	In the card and the reader
Storage of transactional data	Possibly	No	Yes	Yes
Additional applications	Possibly	None	Some	Many
Cost	Varies	Low	Medium	High

Now that we have taken a detailed look at each of the three tokens we can take some time and compare their various advantages. It will be instructive to include in this comparison the typical biometric product using a token on the market today. As mentioned above, these products either use separate biometric and card readers or, when the two are combined in the same unit, simply use the readers to gather information which is then passed to a computer. The table below gives a summary of this comparison.

A comparison of biometric identification devices-Notice the inclusion of cost on the last row. From our previous discussion it might appear that we should always use a smart card, but smart cards can be very expensive when compared with the other options we have discussed. It is important to keep in mind, when considering how much to spend on security, that there is no way to provide perfect security. All we can hope is to control our risks and that usually means comparing the cost of a security breach with the cost of installing a security system. An optical card with a PDF patch will cost around 50 cents, but most organizations looking to move to a biometric identification system will probably already be issuing cards to their members. A PDF patch can be put on just about any piece of plastic so, for all practical purposes, we can assume no additional cost for the optical cards.

Memory cards vary in price from roughly \$1.50 to \$2.00 if they are bought in large enough quantity (as high as ten thousand cards). Smart cards are even more expensive and run between \$5.00 to \$15.00 in bulk. Given the requirement that our cards handle the sophisticated cryptographic processing that public key algorithms impose we can assume a price closer to \$15.00. Notice that we have not mentioned the cost of the readers or the supporting enrollment stations. This is because the cost of the cards usually dominates the decision, as the following example will show. Say that a certain State would like to put standalone biometric/token readers in a thousand State Patrol cars. The State also plans to put a PDF patch on the back of every driver's license issued in the State. If the State has five million drivers then it would cost on average \$5,000,000 more to issue memory cards, and \$50,000,000 more to issue smart cards, than to issue the standard driver's license. The cost of putting a PDF patch on the back of drivers' licenses would be the cost of installing enrollment stations at each State institution that issues the licenses. The same cost would be incurred for the memory and smart cards so the only real difference in cost among the three options is for the cards themselves.

As can be seen, price can play a big role in deciding what token to use, but so should the level of security desired. Let us review what level of security each token can give. The table above provides a nice guide by pointing out what we should look for:

Where is the biometric template stored? Where are the live biometric and template compared? How is the transfer of data to this location accomplished? What is the location of the secret keys? Can transactional data be stored? And what additional applications can live on the token?

The optical card allows storage of the biometric template in encrypted form on the card. In conjunction with an integrated biometric/token reader the template and live biometric can be compared on the reader with the template never leaving the reader. Unfortunately, because of the read-only nature of the optical storage, all keys have to be kept on the reader and no transactional information can be gathered and recorded on the card. The memory card does provide for the storage of transactional information and some additional related applications, but all the keys still need to live on the reader. Finally, the smart card gives all the functionality of the other two tokens with the additional ability to authenticate the biometric/token reader before releasing any sensitive information. This makes it much more difficult for an adversary to gain access to the biometric template, protected as it is with the smart card's own secret encryption and signing keys, and adds another level of security to the identification process as well as strongly protecting every card holder's privacy.

In comparison, most other biometric identification products using a token do not take full advantage of the token. The biometric template is stored on the token, but it is moved around a great deal. The best that any of these devices could do (and there is no evidence that any of them do this) would be to use the separate biometric scanner to gather the live biometric and transmit it to the smart card reader for comparison with the stored template. To do this securely, the live biometric information being transmitted would have to be protected using the same sophisticated public key protocol that was used to protect messages coming from our integrated biometric/token reader. This in turn, would require a "smart" biometric reader. In other words, the biometric reader would have to have the computational capability of our integrated biometric/token reader. If this is the case, then we might as well integrate the biometric scanner with the token reader and gain the additional tamper protection of a single unit; just another argument demonstrating the advantage of an integrated biometric/token reader.

In summary, modern technology has provided us with a convenient, secure method of identifying individuals and providing secure access while simultaneously protecting an individual's privacy. Whether your organization needs increased security of its physical access, or better control access to computers and networks, a variety of cost-effective solutions now exists.

References

Document prepared for the GSA Government Smart Card Group, "Guidelines for Placing Biometrics in Smartcards", September 22, 1998. A. J. MENEZES, P. C. VAN OORSHCOT, S. A. VANSTONE, Handbook of Applied Cryptography, CRC Press, New York, 2nd addition, 1997. B. SCHNEIER, Applied Cryptography: Protocols, Algorithms, and Source

Code in C, John Wiley & Sons, New York, 2nd edition, 1996.