Smartcards, security, and biometrics

How biometrics-augmented authentication can make today's smartcards more secure

By Thomas Suwald, NXP Semiconductors

ABSTRACT

The increased use of smartcards has led to increased concerns over smartcard security. Adding biometrics (the analysis of a physical or behavioral characteristic unique to each person) can add a new level of security to smartcard authentication. This white paper looks at the biometric techniques best suited for use with smartcards, presents the options for implementing biometrics in a smartcard system, and provides examples of real-world biometric smartcards that are either already in use or nearing deployment.

TABLE OF CONTENTS

I. THE PRESENT CHALLENGE: BETTER SMARTCARD SECURITY

Since their introduction nearly 30 years ago, smartcards have become a worldwide phenomenon. Originally designed as a replacement for cards with magnetic strips or barcodes, these now-familiar plastic cards, each equipped with a microcontroller chip, support everything from mass transit and building access to banking, commerce, entertainment, healthcare, civilian identification, and more. Market analysts have defined more than 40 application categories for smartcards, and billions of smartcards are in use every day around the world.

With this increased use, though, comes increased concerns over security. Smartcards are typically protected by a two-factor authentication process that involves showing the card and then entering a password or PIN code, but this may not be enough to prevent fraud or misuse. Adding biometrics – that is, the analysis of a physical or behavioral characteristic unique to each person – can add a new level of security to smartcard authentication.

Biometrics, which include things like fingerprints and facial structures or handwritten PINs and signatures, can either replace traditional methods of authentication, such as tokens and passwords, or can be used in conjunction with these traditional methods, for an added level of security.

The advantage that biometrics have over other methods of authentication is that they're unique to an individual and they're something that is always with a person. They can't be forgotten and they're extremely difficult to share, lose, or steal. The person has to be physically present to supply a biometric sample, at the time of authentication, and this reduces the likelihood of fraud even further. All these things make biometrics a compelling option for smartcard authentication.

There are several biometrics suitable for use with smartcards, and there are various ways to implement biometrics in smartcard systems. Some of these methods are already in use, while others are still in the early stages of development.

This white paper looks at the ways smartcards are used, explains the two methods for integrating biometrics into a smartcard system (with off- or on-card scanning), and reviews the biometrics best suited for use with smartcards.

A first assumption: identification versus verification

Technically speaking, biometric authentication can be used for one of two purposes: identification or verification.

- Identification involves comparing a biometric sample to samples stored in a database. This is referred to as a one-to-many comparison. For example, the DNA of an unknown person might be compared to samples in a DNA database. Matching the donor's DNA to a database sample serves to identify the unknown person.

- Verification involves a one-to-one comparison, where a biometric sample is compared to a single sample stored in a reference template. For instance, the scan of a person's fingerprint can be stored in a reference template on a smartcard. Matching a person's live fingerprint scan with the scan in the smartcard's reference template serves to verify that the live scan belongs to the same person who scanned the fingerprint in the reference template.

With smartcards, authentication is more typically used for verification. As a result, the biometric methods described in this white paper use verification as their basis.

II. WHAT'S POSSIBLE WITH BIOMETRICS: SMARTCARD USE CASES

A good place to start, when discussing the implementation of biometric-augmented authentication, is to look at use cases that might benefit from the effort.

Security is the key issue, so biometrics are best suited for use in applications that require a certain level of security. There are a few contactless applications, such as transport ticketing and highway tolling, where transaction speed is in many ways more important than secure authentication, and biometrics may not be a suitable addition to the process. But these are the exceptions.

The great majority of smartcard applications support transactions that benefit from the added security that biometrics can bring. Any time someone wants to use a smartcard to, for example, pay for something, enter a secure area, submit private information, apply for a government service, or cross a national border, biometric authentication can add a much-needed level of assurance and safety.

There are essentially two ways that a smartcard can be equipped to support biometrics, with off-card scanning or on-card scanning. The difference lies in how the system collects biometric data from the person requesting authentication. In off-card scenarios, the smartcard terminal is used to collect the data, and in on-card scenarios, the smartcard itself can be used to collect the data. The subject of off- and on-card scanning is covered in more detail later, but understanding the basic concept of where biometric data is collected can make it easier to envision specific use cases.

The following are smartcard applications that are particularly good candidates for the use of biometric-augmented authentication. Biometrics are either being piloted or are already in widespread use in many of these areas:

- **Border crossings**
  Electronic passports (ePPs) have been in use since 2000, and many of today's ePP schemes support the storage of biometric templates for authentication. Off-card scanning remains the implementation of choice. Fingerprint scanning and iris scanning have both been deployed in border-crossing applications, but, due to its advantages in usability and speed, facial recognition has become the standard.

- **Physical-access control**
  In research facilities, government offices, military installations, and other security-sensitive environments, adding biometrics to the physical-access process can help ensure that only the right people gain entry to restricted areas. A fingerprint reader, for example, can be installed at the access point, and the sampled fingerprint can be sent to the smartcard for secure processing.

- **Banking and payment**
  Bank cards that comply with the Home Banking Computer Interface (HBCI) represent a significant increase in user security, but there can still be problems if a thief gains access to both the card and the PIN code. In this situation, biometrics such as fingerprints and handwriting samples can address the threat by applying unique physical or behavioral characteristics as an additional authentication factor. Biometrics can also help address issues associated with Card Not Present (CNP) scenarios, where stolen credit-card credentials may be presented to an online store.

A dedicated reader can be equipped with biometric capabilities, or, for the most portable and most convenient setup, the smartcard itself can be used to collect and process biometric data. Figure 1 gives an example. A contactless smartcard has been equipped with a capacitive-touchpad interface so it can accept a PIN of six digits, entered in normal handwriting. In this case, the number "5" is part of the PIN code and has been traced by hand on the card. The handwritten number is used with the card's embedded algorithm for handwriting recognition. The contactless smartcard is, by nature, already compatible with the existing reader infrastructure, so there's no need to develop a specialized reader that supports biometrics, and this lowers cost.

- **Online transactions**
  Using today's methods, providing a credit-card number to an online service or retailer is inherently risky, because there are so many opportunities for the card number and its security code to be stolen, hacked, or misused. Adding biometrics to the authentication process can help reduce these risks. Figure 2 gives a sample scenario, with online access from a laptop computer. A USB-type contactless reader connects to a smartcard that supports handwritten PIN entry. Only after the PIN has been entered and verified is any sensitive user information forwarded from the card's secure element to the online application. Any key loggers or other malware will only be able to intercept encrypted communications.

- **Government services**
  From vehicle registration and tax declaration to social programs like welfare and healthcare, more and more government services can be accessed online. With smartcards that can store biometric data, such as one or two fingerprint samples, online government services can be more secure. In the case of vehicle registration, an off-card fingerprint reader, installed at the car dealership, can let car buyers register their new vehicles on the day of purchase, without having to wait in line at a government office. Similarly, an on-card scheme that supports direct PIN entry with handwriting analysis can provide secure access to various services.

- **Legal documents**
  Contracts, rental agreements, real-estate purchases, and other legal documents typically require a verified signature to be legally binding. Off- or on-card fingerprint scanners can be used to confirm the identities of everyone involved and, when people aren't able to appear in person to sign a document, an electronic document combined with a biometric can serve as a verified signature.

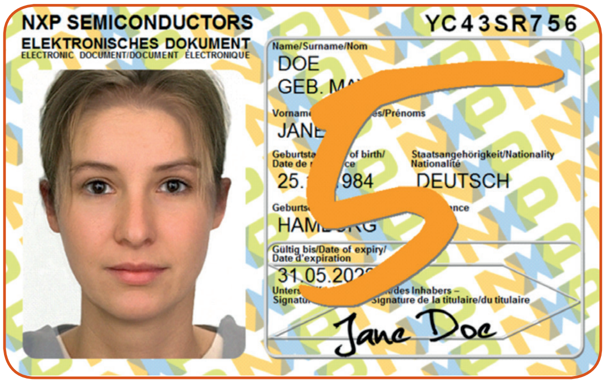
NXP SEMICONDUCTORS
ELEKTRONISCHES DOKUMENT
ELECTRONIC DOCUMENT/DOCUMENT ÉLECTRONIQUE
YC43SR756
Name/Surname/Nom
DOE
GEB. M
Vorname es/Prénoms
JANE
Geburtsta of birth/ Date de ce
25. 984
Staatsangehörigkeit/Nationality Nationalité
DEUTSCH
Geburts nce
HAM RG
Gültig bis/Date of expiry/ Date d'expiration
31.05.202
Unters des Inhabers – Signatu Signature de la titulaire/du titulaire
Jane Doe
5

Figure 1 Biometric-augmented smartcard with handwriting recognition (Source: NXP Semiconductors)

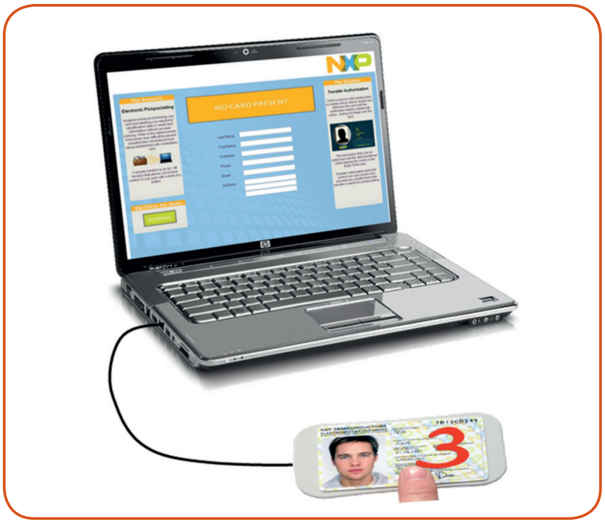

Figure 2 Securing online applications (Source: NXP Semiconductors)

III. HOW IT WORKS: THE BASICS OF BIOMETRIC AUTHENTICATION

From the user's standpoint, adding biometric authentication to the smartcard process requires a bit of upfront work, because the user has to register the biometric before using the smartcard. But once the upfront work is done, the authentication process can be quick and easy. There are three steps in total:

Step 1: Enrollment
This step prepares the smartcard for use and pairs the person with the card. A reference sample, such as a fingerprint or a sample of writing, is taken. The reference sample, called a template, is stored either in a database, managed by the authenticating authority, or on the card itself.

If the template is stored in a central database, then there is the added issue of keeping the database secure, so it's protected from misuse. If the template is stored on the card, it is typically saved in an encrypted format or as an encrypted hash code, so it is safe from tampering. A hash code is a numerical value tied to a fixed input. It is essentially a one-way encryption of a given file and is extremely difficult to decode. Only the hash code, and not the file itself, is stored on the card.

It's important to note that, with any biometric system, variations need to be taken into account. This is true even with biometric traits that are relatively stable and typically change very little over time, such as fingerprints. This is because the scanning procedure itself can introduce variations. There can be slight variations in the way the person interacts with the scanning sensor, and environmental conditions, such as temperature and humidity, can change readings. The sensors themselves can introduce variations, too, due to sample and signal-conditioning effects, or the sensor's linearity and resolution. The impact of variations can be minimized by taking more than one sample of the same biometric, a process called oversampling.

Step 2: Live sample
With the template in place, the smartcard is now ready for use. Each time the card is put to work, the user provides a live version of the reference sample as part of the authentication process. For example, if the template is a fingerprint, the user provides a new fingerprint, at the time of authentication, for verification. In a setup that uses off-card scanning, the live sample is taken by the smartcard terminal by means of a separate piece of equipment, such as a dedicated fingerprint reader. In a setup that uses on-card scanning, the sample is taken by the card itself. Either way, the next step, comparison, is usually performed on the card.

Step 3: Comparison
To complete authentication, the live sample, from step 2, is compared to the reference sample in the template. If the live sample is verified to be a match with the template, then the smartcard is authenticated and the transaction can proceed.

Biometrics are typically used in what's called three-factor authentication. This approach uses three things for verification: something you know (a PIN code), something you have (a smartcard), and something you are (an individual biometric property). Figure 3 gives an example of three-factor authentication.

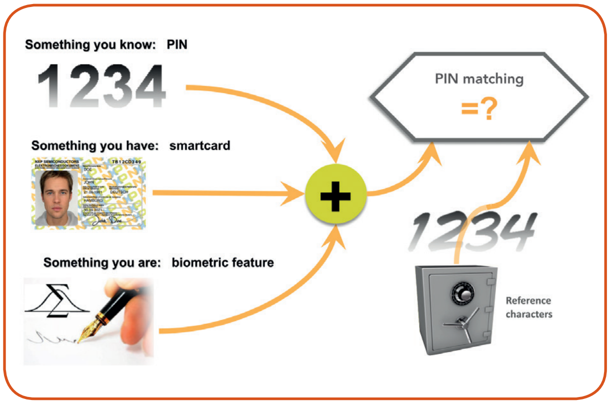

Figure 3 Three-factor authentication with biometrics
(Source: NXP Semiconductors)

In some cases, two of these factors can be combined. For example, with a handwriting biometric, you might be asked to use your finger to write the numbers of your PIN code. The handwriting sample is the "something you are," while the PIN code is the "something you know."

Biometric verification relies on a multi-step processing model illustrated in Figure 4 and described in Table 1. The details of the biometrics process change depending on where the scanning takes place. With off-card scanning, the smartcard terminal or an external device performs the steps of live data capture, signal pre-processing, feature extraction, compression, and optional hash code generation. The live sample or its hash code is sent to the smartcard for matching with a template or the template's hash code. Restrictions like power consumption and physical size don't normally apply, so off-card scanning can often deliver better capture performance.

With on-card scanning, the biometric sensor is embedded in the smartcard. Form factor is, obviously, a limiting factor here, since smartcards are, by definition, small and thin. Power consumption plays a role, too, since on-card scanning can require additional processing, which uses more power. In early trials, manufacturers have already been successful integrating fingerprint sensors and handwriting sensors into standard-sized cards.

With the sensor embedded in the smartcard, the card can perform all the functions needed for authentication: live data capture, signal processing, template matching. One drawback is that the integration of on-card sensors may increase cost. With a fingerprint sensor, for example, the critical cost contributors are the sensor itself, along with the need for a more powerful smartcard controller and a far greater card-integration effort. The higher implementation cost may, however, be offset in the long run because it eliminates the need for specialized smartcard terminals that support biometrics. Also, with on-card scanning, biometrics can be added without extensive updates to the network or processing infrastructure, and this can offset the cost of implementation. In the long run, on-card scanning can be less expensive to implement than off-card scanning.

Table 1 Components of the biometric processing model

Process block	Definition
Sensor	Acts as the interface between the real world and the authentication system and acquires the live sample. Format varies according to the sample being collected (image acquisition, capacitive sensor, etc.).
Pre-processing	Prepares the biometric input data, collected during live sampling, for use by the biometric system. Tasks include removing artifacts, enhancing input through noise filtering or rotation, or applying some kind of normalization, such as scaling.
Feature extraction	Selects the relevant data for use in the reference sample, called a template. Data that won't be used by the matching process is discarded, to reduce the volume of data.
Template generator	Synthesizes the relevant characteristics, produced by feature extraction, to create a template. The template is a vector of numbers or an image with particular properties.
Reference templates	Created during the enrollment process, reference templates are later used for comparison with live samples during the authentication process. Reference templates can be stored on the smartcard itself or in a database managed by the authenticating authority.
Template matching	Analyzes the live input by comparing it with the reference template. The result of this process confirms or denies authenticity. Template matching often involves a detection threshold: if the probability for authenticity is above a certain threshold, then authenticity is confirmed. Setting the detection threshold higher or lower can help balance the tradeoff between security and usability.

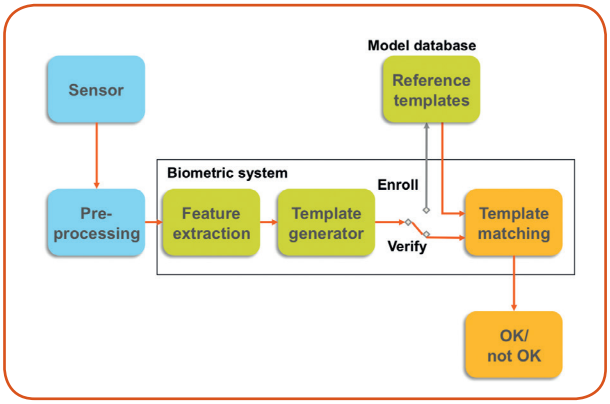

Figure 4 Biometric processing model (Source: NXP Semiconductors)

IV. MAKING A CHOICE: THE BEST BIOMETRICS FOR SMARTCARDS

Biometrics come in a variety of forms. These generally fall into one of two categories: physical characteristics and behavioral characteristics. Some examples of physical characteristics are fingerprints, the network of veins in a hand, the physical geometry of a hand, the specific arrangement of features on a person's face, and certain components of the human eye, including the retina and the iris. Examples of behavioral characteristics are how a person types on a keypad, the way a person writes a particular phrase or a sequence of numbers, or how they sign their name. Voice recognition is a hybrid biometric, involving a combination of physical and behavioral characteristics.

With all these biometrics to choose from, how can we select the best options for use with smartcards? First, we can evaluate a given biometric to gauge its viability as a tool for authentication. In 1999, the academics Jain et al[1] defined seven factors for assessing the suitability of a trait for use as a biometric in authentication. Table 2 provides our version of these factors.

Table 2 The seven characteristics of a suitable biometric for authentication

Factor	Definition
Universal	Every person using the system should possess the trait
Unique	The trait should be sufficiently different for each person using the system that it can be used to distinguish one person from another
Permanent	The trait should change very little over time, so the matching algorithm can have longevity
Measurable	The trait should be easy to collect, and the collected data should be in a form that permits effective analysis
Performance	The technology used to collect and analyze the trait should be accurate, robust, and fast
Circumvention	It should be difficult to work around or trick the system using an artifact or substitute
Acceptability	The people who use the system should be comfortable enough with the technology that they will be willing to have their trait captured and assessed

It's important to point out that there is no single human characteristic that meets all these criteria to their fullest extent. The perfect biometric for authentication simply doesn't exist. But there are several human traits that can be considered good enough. When it comes to smartcard authentication, though, there are a few more factors to consider. Any biometric that will be used in conjunction with a smartcard has to be practical to implement, and has to be compatible with the smartcard format. It has to work within the expected operating environment, and, perhaps most important of all, it has to be cost-effective. This immediately rules out certain biometric formats, such as DNA, which is too expensive, the way a person walks, which requires too much space to measure, and a person's odor profile, which requires too much complex analysis.

In applications that require the highest levels of security, it may make sense to use biometrics that would otherwise be too expensive or cumbersome for use with smartcards. These include hand geometry, hand-vein structure, iris and retina scans, voice recognition, and keyboard entry. For the more typical smartcard application, however, the reality is that there are only a few suitable biometrics. Future development may make more formats and methods feasible but, for now, there are basically three biometrics that best meet the key requirements of reliability, usability, form factor, and cost: fingerprints, face recognition, and handwriting analysis.

A more detailed discussion of these three biometrics is provided in the body of this paper. Appendix II covers biometrics that may, due to improvements in technology, be more suitable for use with smartcards in future. These include the physical biometrics of hand geometry, hand-vein pattern, iris pattern, and retina pattern, the behavioral biometric of keystroke pattern, and the hybrid biometric of voice recognition.

Before we take a closer look at the three most feasible biometrics, though, it makes sense to consider the different environments where smartcards are used. Having an understanding of these environments can make it easier to select an appropriate biometric.

[1] Jain, A.K.; Bolle, R.; Pankanti, S., eds. (1999). "Biometrics: Personal Identification in Networked Society." Kluwer Academic Publications. ISBN 978-0-7923-8345-1

V. SMARTCARD OPERATING ENVIRONMENTS: THEIR EFFECT ON BIOMETRICS

Smartcards are typically used in what are called closed or open environments.

In a closed environment, the scanning device is operated by the authenticating authority and the equipment is constantly supervised. Border crossings and corporate offices are examples of closed environments. Closed environments can use either method of biometric scanning (on-card or off-card), but off-card scanning is the method used more widely today. This is mostly because closed environments typically provide enough space to accommodate the relatively bulky equipment, such as fingerprint scanners and image-capture devices, used to collect live samples. The scanning equipment is closely monitored, so this reduces the chances of equipment tampering.

In an open environment, the scanning device is not always under the control of the authenticating authority. These are typically environments where the user requests authentication through the use of a personal computer, a tablet, a smartphone, or some other system not owned and operated by the authenticating authority. Taken on a global level, the open environment is staggeringly large, involving billions of devices.

In open environments, cost and usability, as well as efficiency, are the primary concerns. Off- and on-card scanning can both be used in open environments. For off-card scanning, where a separate device is needed to take the live sample, fingerprint scans are usually the best choice. For on-card scanning, which requires the most compact footprint, fingerprint scans and handwritten PIN entry are the most practical.

On-card scanning, which involves equipping the smartcard itself with the ability to store a template, take a live sample, and perform a comparison, is a particularly attractive idea for open environments. Having a secure element integrated onto the smartcard ensures security during the processing step, because it enables data encryption, and can reduce the chances of tampering, even in an open environment.

A smartcard with on-card scanning and verification may even be able to provide a pseudo-closed environment. This is true if the smartcard sends the results of its biometric matching process to the host in an encrypted manner. This essentially creates a firewall between the smartcard and the host.

In general, on-card scanning is the better choice where installation of external biometric sensors is impractical. Also, having an easy-to-use, one-piece solution can increase the adoption rate, since consumers don't have to invest in or install complex equipment for use at home or on the road.

VI. MANAGING TRADEOFFS: SECURITY AND USABILITY

With most biometric authentication systems, the designers typically have to make a tradeoff between security and usability. A system that takes very precise readings of a fingerprint, for example, may take a long time to scan each fingerprint. The high level of precision makes the system more secure, but the slowness make it less usable. In general, higher security typically leads to lower usability, and vice versa.

The tradeoff between security and usability can be evaluated using two concepts, the False Acceptance Rate (FAR) and the False Rejection Rate (FRR).

Measuring security: FAR
FAR is a measure of security. It indicates how frequently an intruder successfully bypasses the biometric authentication method. The higher the FAR, the less secure the system. The FAR is calculated as follows:

$$\text{FAR} = \frac{\text{Number of false acceptances}}{\text{Number of intruder attempts}} \times 100$$

Using this formula, a FAR of 0.1 percent indicates that the chances of fooling the system are 1 in 1000. Depending on the number of authentication requests, this may or may not be an acceptable FAR. In a border-control application, where many thousands of people are being checked every day, a FAR as low as 0.01 percent may still be unacceptable.

Measuring usability: FRR
FRR is a measure of usability. It indicates how frequently a user is rejected by the system and forced to retry the authentication. The higher the FRR, the less usable the system. The FRR is calculated as follows:

$$\text{FRR} = \frac{\text{Number of false rejections}}{\text{Number of enrollee attempts}} \times 100$$

Having a high FRR means more retries. This can lead to frustration and can damage the reputation of the authentication system. Such was the case with a certain retina-scanning system, used for a time in London’s Heathrow Airport, which required users to stay absolutely still for more than 12 seconds. This proved difficult for many people to do, so the scans frequently failed. Passengers reported they spent more time being scanned by the machines than when they went through traditional passport control. The high FRR, combined with high rates of user dissatisfaction, spelled the end of the system. After several years of trial use, the iris-scanning system was retired and replaced by a facial-recognition system that has, thus far, experienced a lower FRR and a higher rate of user satisfaction.

Finding the right balance: EER
The point at which the FAR and the FRR are equal is referred to as the Crossover Rate or the Equal Error Rate (EER). The EER can be used to measure quality, because a low EER indicates a system that more effectively balances the tradeoff between security and usability.

VII. THE THREE BEST OPTIONS: FINGERPRINTS, FACES, AND HANDWRITING

In this section, we take a closer look at the three biometrics best suited for use with smartcards: fingerprint scans, facial recognition, and handwriting analysis.

Fingerprint scans

The unique patterns formed by the ridges on the tips of human fingers have, for more than a century, been used to identify people, and fingerprints are still one of the best biometrics available. Despite the need to come into contact with human skin, a substance that can introduce variations in the sample, scanning fingerprints is a method that can be relied on to deliver a high level of security with electronic IDs.

Fingerprints are cost-effective, relatively simple to obtain, easy to use, and small. However, fingerprints can be affected by cuts, dirt, and age, and require a certain amount of power and computational resources to capture and manage. Obtaining high-quality images of distinctive fingerprint ridges and minutiae can be a fairly complex task, and partial prints can be a limiting factor.

There are several methods for scanning a fingerprint:

- **Ultrasound fingerprint sensor**
  These systems are quite new and, as a result, not yet in widespread use. The finger is placed against a piece of glass and an ultrasonic sensor reads the whole fingerprint in one pass. The process takes one or two seconds to complete.

- **Optical fingerprint reader**
  These are the fingerprint readers most commonly found today. They use the reflections created by pressing a finger against the reader surface to create an image of the fingerprint. Optical readers are somewhat bulky, so they can’t be integrated onto a smartcard. They are small enough, however, to be suitable for home use, and can be used in closed or open environments.

- **Capacitive array sensor**
  The fingerprint sensor is composed of an array of capacitors, integrated on a silicon chip. The variation in electrical capacitances is used to produce a sample. When a finger is placed against the surface of the sensor chip, the ridges of the fingerprint are closer to the nearby pixels and have a higher capacitance. The valleys of the fingerprint are farther away, and have lower capacitance. Capacitive sensors are small enough to be integrated into a smartcard, but at present the integration process is relatively expensive. Another consideration is that the sensor surface needs to be exposed, so the user can access it, and this leaves the sensor unprotected. Also, the sensor needs to be properly grounded to ensure reliable operation, and this can be difficult to achieve with a contactless smartcard.

- **Capacitive line sensor**
  A more economical variation of the capacitive sensor, called a capacitive line sensor, has the user swipe their finger over the sensor, creating stripes of the fingerprint image. A stitching process is then used to combine the stripes into a complete image. The added processing and power requirements for image stitching make capacitive line sensors a less-than-ideal choice for integration in smartcards. In addition, the issues associated with sensor exposure and improper grounding also apply.

In smartcard systems, off-card scanning is, at present, the most cost-effective approach for using fingerprints as a biometric. This is because sensor cost and power consumption are not critical, and sensor performance is easier to ensure. The small size of the sensor makes it a good choice for in-home use. As described earlier, even if the live sample is taken by an off-card sensor, the matching process can happen on the card itself.

Facial recognition

The exact positioning and shape of the eyes, nose, and mouth, along with the contours of the cheek bones and jaw, make each human face unique. Still images and video are used to document facial features and create a template for comparison. Facial recognition is becoming a standard in the authentication of international travelers, mainly due to its good usability, speed and user acceptance.

Upon enrollment, several pictures are taken of the subject from different angles and with different facial expressions. At the time of verification, the subject stands in front of a camera for a few seconds, and then the image is verified against the stored template. The subject may be asked to blink, smile, or nod while the live sample is being taken. This helps prevent fraud, by ensuring that the subject is not wearing a mask or simply presenting a photo to the scanner. Use of facial thermography, which records the heat of the face, can prevent fraud, too.

The need for a high-resolution image sensor, combined with a thermo sensor and reproducible illumination, currently restrict usage to off-card scanning. That is, face recognition requires the presence of a smartcard terminal or other type of host interface. The environmental conditions need to remain constant, and the lighting needs to be right, so facial recognition is better suited to use in closed environments, where these factors can be monitored and controlled. The smartcard terminal can house the sensor, process the image, and extract the necessary data, while the card can store the template and compare it to the live sample.

Handwriting recognition

How someone writes a series of characters or how they sign their name can be a useful biometric for authentication. Unfortunately, how people sign their name or write a word can change over time, and signatures can vary depending on certain external factors, such as sickness, injury, or mood. These variations reduce the reliability of handwriting and signatures as a method of authentication, but because the technology for analyzing handwriting and signatures is well suited for use with smartcards, signature analysis and, in particular, handwriting analysis are worth considering for smartcard applications.

A signature-recognition system evaluates a signature by examining how it was written, or verifies the signature by estimating how it was created. Verification of a complete signature is a somewhat complex processing task and is currently restricted to use with position- and pressure-sensitive touchpads. These touchpads can be used in open and closed environments, but are not suitable for integration into the smartcard itself.

What makes handwriting analysis an attractive biometric for smartcards is that the interface for entering the code can be made an integral part of the card. The subject, using their finger as the writing mechanism, traces a series of letters or numbers, one at a time, onto the card. The card is equipped with a two-dimensional touch sensor, a pressure sensor, or a combination of the two. Each character is a separate live sample that is verified against its own template, stored on the card.

Entering a handwritten PIN code requires less-intensive processing than other biometrics, including fingerprints, and the processing can be performed by the smartcard's on-chip circuitry. Using a capacitive touchpad to capture the handwriting can be a good choice in terms of manufacturability, since the touchpad's sensor can be placed in the antenna substrate.

VIII. ON-CARD SCANNING: TWO REAL-WORLD EXAMPLES

At present, two methods for adding biometric scanning to a smartcard, to support on-card scanning, have reached the industrialization stage. The first, developed by the Italian company PinKey, integrates a fingerprint sensor, while the second, developed by NXP Semiconductors, integrates a capacitive touchpad.

The PinKey Biometric Card (with fingerprint sensor)

This card, illustrated in Figure 5, has an embedded capacitive fingerprint sensor provided by IDEX. It features a biometric algorithm, running on a separate microcontroller, capable of real-time image processing and template matching with the user's fingerprint. This particular approach makes it possible to keep the biometric user data private and secure inside the smartcard. The smartcard comes in a standard ID1 format, and complies with the ISO 7816 standard. Due to the high power requirements of the processing system, the card requires an embedded flexible battery, which limits the lifespan of the card. Also, the card cannot be operated in full contactless mode, and this may limit the number of applications it supports. Details on the PinKey biometric card are available on the company's website (www.PinKey.it).

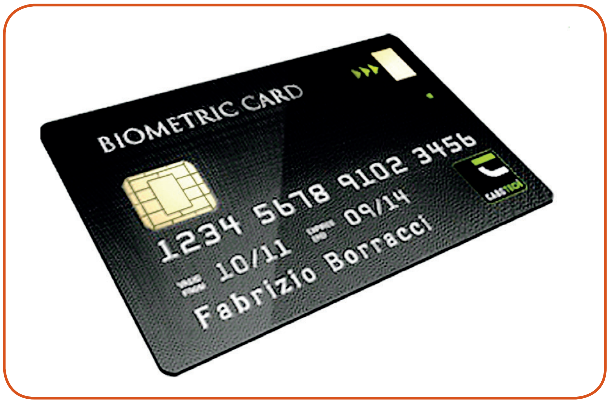

Figure 5 The PinKey Biometric Card (Source: PinKey)

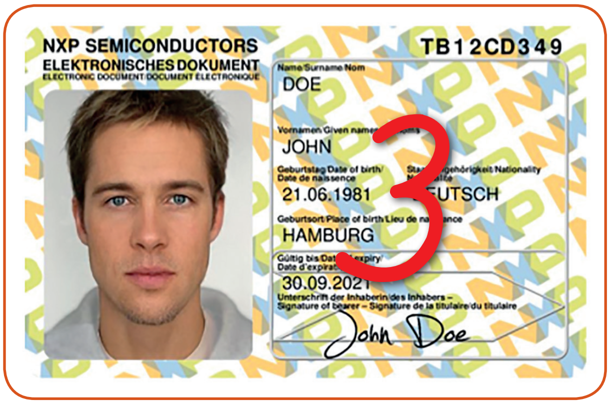

Figure 6 The NXP smartcard with capacitive touchpad (Source: NXP Semiconductors)

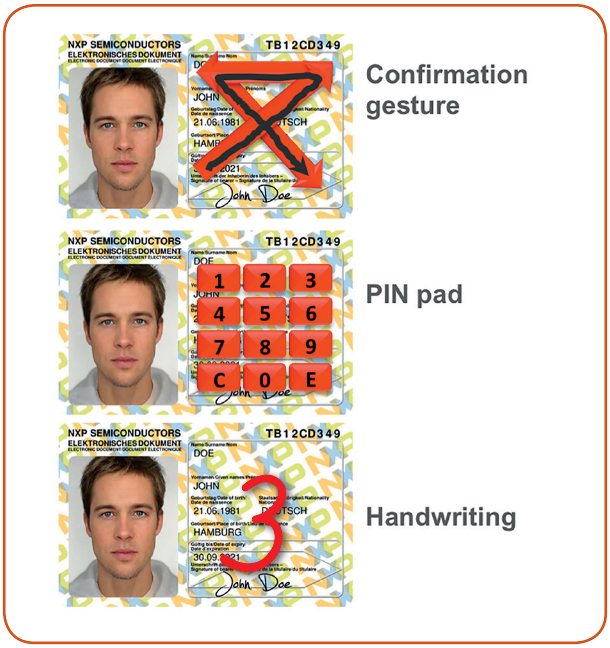

Figure 7 Three touchpad configurations (Source: NXP Semiconductors)

The NXP biometric smartcard (with capacitive touchpad)

This card, illustrated In Figure 6, supports direct PIN entry on a contactless smartcard. It uses the cardholder's handwriting as a biometric feature. The PIN, which can be up to six digits or more, is entered by hand. The individual numbers of the PIN code are captured in the writer's unique way of writing through the use of an integrated capacitive touchpad.

The embedded biometric system verifies the input data against a set of character templates. The achievable alphabets, including Chinese, Japanese, and Cyrillic, and the keypad positions, give the card a high degree of flexibility in terms of how it's configured and where it's used. As shown in Figure 7, the touchpad can be configured to recognize handwriting, confirm a gesture, or present a PIN pad.

The integrated touchpad is based on a 3x3 capacitor matrix, as shown in Figure 8. The touchpad can be integrated into existing smartcards (hidden underneath the plastic), so the basic design of the card can stay the same and there's no need for a redesign. This can save costs in development and manufacturing.

The NXP biometric smartcard is designed with flexibility in mind. It uses the ISO/IEC 14443A contactless communication standard, so it is compatible with the millions of MIFARE chip card terminals already in place throughout the world. Seamless compatibility with the existing MIFARE-based smartcard infrastructure makes it possible to use the new biometric smartcard in a wide range of well-established smartcard applications, including identification, banking, home shopping, and physical access.

Using ISO/IEC 14443A also creates an authentication solution that is compatible with the rapidly growing number of smartphones equipped with an interface for Near Field Communication (NFC). Compatibility with NFC-enabled smartphones provides a convenient, cost-effective way to use biometric authentication in an open environment, and that can help address some of the security concerns associated with activities like home banking and online shopping.

NXP's biometric smartcard uses a battery-free concept that gives it a lifespan of up to 10 years. The smartcard is powered by a contactless reader, a contactless smartcard terminal, or an NFC-enabled smartphone.

In preparation for its release on the open market, the NXP biometric smartcard has been tested by potential customers in identification and banking applications. These initial tests have yielded very positive feedback, with high rankings for ease of use.

To support the full release of its biometric smartcard solution, NXP will combine the necessary components, including the biometric subsystem, the user interface, and the required cryptographic functions, into a single tiny module that will be easy to integrate into a smartcard.

For more information about the biometric smartcard, contact NXP at www.nxp.com.

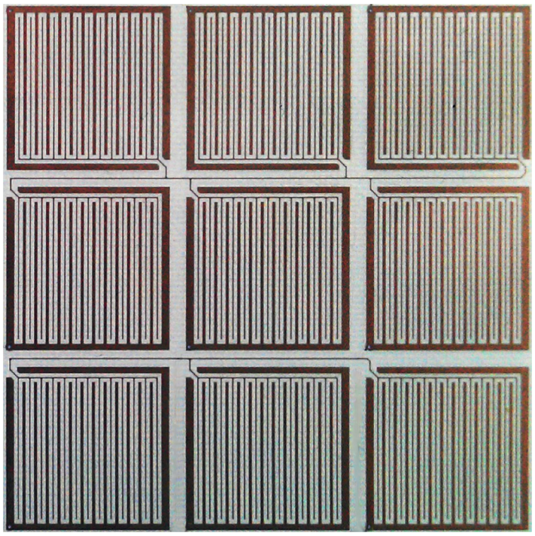

Figure 8 The 3x3 touch-sensor matrix (Source: NXP Semiconductors)

SUMMARY

Biometrics offer a compelling way to increase security in smartcards. The functions for scanning and verifying biometric data can be designed into an external device, used in conjunction with the smartcard or, better yet, can be integrated onto the smartcard itself. At present, the best approach – in terms of power efficiency, longevity, and flexibility – is to use an integrated capacitive touchpad on the smartcard. NXP has already developed a proof-of-concept version of this kind of smartcard and is working toward its introduction on the open market. For more information, contact NXP at www.nxp.com.

SOURCES FOR FURTHER READING

The following scholarly publications provide additional information on the topic of biometrics and how they can be applied to smartcard authentication schemes.

Hong and Jain, “Integrating faces and fingerprints for personal identification,” IEEE Trans. Pattern Anal. Mach. Intell., Volume 20, No. 12, Dec. 1998, pp. 1295–1307.

Jain, Hong, and Bolle, “On-line fingerprint verification,” IEEE Transactions on Pattern Recognition and Machine Intelligence, Volume 19, No. 4, Aug. 1996, pp. 302–314.

Mali and Bhattacharya, “Comparitive Study of Different Biometric Features,” International Journal of Advanced Research in Computing and Communication Engineering, Vol. 2, Issue 7, July 2013.

Sahoo, Soyuj Kumar; Mahadeva Prasanna, SR, Choubisa, Tarun (1 January 2012). "Multimodal Biometric Person Authentication: A Review," IETE Technical Review 29 (1): 54. doi:10.4103/0256-4602.93139.

IX. APPENDIX I: EVALUATION MATRIXES

Table 3 lists commonly used physical and behavioral biometrics and rates how well they meet the criteria for each characteristic. The biometrics marked with an asterisk (*) are the ones currently best suited for use with smartcards.

Table 4 lists commonly used biometrics and rates their suitability for use with smartcards. The first consideration is compatibility, the second is cost. Those marked with an asterisk (*) are today's best options.

Table 3 Profiles of various authentication biometrics in use today

	Universal	Unique	Permanent	Measurable	Performance	Circumvention	Acceptability
Physical biometrics							
Fingerprint*	Medium	High	High	Med	High	Medium	Medium
Hand geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Hand vein	Medium	Medium	Medium	Medium	Medium	Medium	Low
Face*	High	Low	Medium	High	Low	High	High
Iris	High	High	High	Medium	High	Low	Low
Retina	High	High	Medium	Low	High	Low	Low
Behavioral biometrics							
Voice	Medium	Low	Low	Medium	Low	High	High
Keystroke	Low	Low	Low	Medium	Low	Medium	Medium
Handwriting*	High	Medium	Low	High	High	Medium	High
Signature*	Low	Low	Low	High	Low	High	High

* Best suited for use with smartcards

Table 4 Current authentication biometrics and their suitability for use with smartcards

	Compatibility		Cost	
	On-card	Off-card	On-card	Off-card
Physical biometrics				
Fingerprint*	Medium	High	High	Low
Hand geometry	N/A	High	N/A	Medium
Hand vein	N/A	High	N/A	High
Face*	N/A	High	N/A	Medium
Iris	N/A	High	N/A	High
Retina	N/A	High	N/A	High
Behavioral biometrics				
Voice	N/A	High	N/A	Low
Keystroke	N/A	N/A	N/A	N/A
Handwriting*	High	High	Low	Low
Signature*	Low	High	High	Low

* Best suited for use with smartcards

X. APPENDIX II: OTHER POSSIBLE BIOMETRICS

The biometrics described in this section are currently used for authentication but are not, at present, suitable for use with smartcards, due to their size, processing requirements, usability, and/or cost. For now, they are reserved for use in only the highest-security applications in tightly controlled environments. They may, in future, be viable options for use with everyday smartcard applications, so they're included here.

The biometrics are organized as follows:

Physical biometrics	▸ Hand geometry ▸ Hand-vein pattern ▸ Iris pattern ▸ Retina pattern
Behavioral biometric	▸ Keystroke pattern
Hybrid biometric	▸ Voice recognition

Hand geometry

The length of the fingers, their width, thickness, curvature, and relative location of these features make each human hand unique. Hand-geometry scanners use a method called orthographic scanning. The user places their palm against a beaded projector screen. The scanner then uses infrared LEDs with mirrors, reflectors, and a camera to record a black-and-white silhouette of the hand. The physical shape of the hand is what matters. The scanner doesn't record surface details, which means it ignores things like fingerprints, lines, scars, and skin color.

Hand-vein pattern

This is a relatively recent approach that uses the network of blood vessels underneath the skin. The patterns are seen as unique and do not change over time except in size. Since veins are below the skin, and have a number of differentiating features, they are very difficult to copy or forge. Infrared sensors are used to capture the vein patterns.

Iris pattern

The iris is the colored part of the eye. There are more than 250 qualities that can be measured in the iris, including rings, furrows, freckles, and the corona (the refractive surface of the eye), and this makes the iris a highly accurate biometric. False acceptance rates are typically very, very low with iris scans. The accuracy of an iris scan is influenced by the hardware's ability to accommodate all individual heights, and the ability to compensate for the surrounding physical environment (such as fluorescent lights). The subject is usually asked to blink or move their eye to prove it's an actual eye, and not a photograph of an eye, that's being scanned.

The biggest drawback of present-day iris scanning, though, is that the subject has to stay absolutely still for more than 12 seconds for a full reading. This is not always easy for people to manage, and can lead to a high rate of false rejections. Despite being a highly secure method for identification, the long reading times and high number of false readings has, in real-world implementations, caused significant user frustration. As mentioned in the main body of this paper, the iris-scanning setup in London's Heathrow Airport was eventually retired for this reason.

Retina pattern

The retina is a light-sensitive layer of tissue at the back of the eye. The complex network of blood vessels in the retina form a pattern that is unique to each person. Even identical twins do not share the same pattern. The retina pattern generally remains unchanged from birth until death. This makes retina patterns one of the most precise and reliable biometrics for authentication, ranked almost as high as DNA in terms of accuracy.

There are certain medical conditions, including diabetes, glaucoma, and retina degenerative disorders that can change the retina pattern, but overall accuracy remains high. Error rates of less than 1 in 10 million have been reported. Retina scanning has been used by several US government agencies, including the FBI, the CIA, and NASA.

With a retina scan, the subject looks through an eyepiece and the scanner casts a beam of low-energy infrared light, undetectable to the eye, onto the retina. The beam traces a standardized path on the retina and the amount of light reflected in each region creates an image of the blood vessels. As with iris scans, retina scans need consistent environmental conditions and the hardware needs to be configured such that it can accommodate people of differing heights. Also, the subject may be asked to blink or move their eye in order to demonstrate that the retina being scanned is, in fact, from the subject's actual eye, and not a photograph.

Keystroke pattern

Using keystroke patterns as a biometric involves measuring how long a person holds down a key (dwell time) and how long it takes for a person's fingers to move from one key to another (flight time). Various algorithms differentiate between absolute and relative timing. The captured data is analyzed to determine aggregate factors, such as cadence, content, spatial corrections, and consistency. A signature-processing routine identifies patterns for later verification.

The accuracy of keystroke patterning for authentication depends, in large part, on the number of keystrokes entered. Tracking a larger number of keystrokes increases accuracy. This makes keystroke patterning a problematic method for smartcard authentication, since the cards themselves are too small to provide an adequately sized keyboard. Even if an external, off-card keyboard is used to support the smartcard, users may be reluctant to type in the necessary number of keystrokes for effective authentication.

Voice recognition

As a hybrid biometric, voice recognition involves a combination of physical and behavioral characteristics. The physical components of a person's voice are referred to as the voice tract and include the size and shape of the mouth, the lips, the vocal cords, the passages at the top of the throat, along the larynx, and the nasal cavities. The behavioral component of voice recognition includes several variables, such as accent, emotion, sickness, and age.

The human voice is not constant, and this poses a problem when relying on voice recognition for secure authentication, because the false acceptance rate can be unacceptably high. At present, the processing algorithms used for voice recognition are more complex than those for handwriting recognition. Also, voice-recognition algorithms can sometimes be fooled by pre-recorded voice samples.

The size of the hardware, the processing power required, and the need for constant environmental conditions currently limits the use of voice recognition to fixed installations in closed environments. Nevertheless, voice recognition can be used in combination with fingerprint and/or handwriting recognition to strengthen the authentication process. A limiting factor for integration into the smartcard itself is the size of the microphone – today's microphones are, for the most part, too big to be a workable addition to a smartcard.

Notes

www.nxp.com

Date of release: October 2014
Document order number: 9397 750 17548
Printed in the Netherlands