SECURE TECHNOLOGY ALLIANCE

**A SECURE TECHNOLOGY ALLIANCE PAYMENTS COUNCIL WHITE PAPER**

# Biometric Payment Cards

**Version 1.0**

March 2019

**Secure Technology Alliance**
191 Clarksville Road
Princeton Junction, NJ 08550

**www.securetechnologyalliance.org**

# About the Secure Technology Alliance

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions, including smart cards, embedded chip technology, and related hardware and software across a variety of markets including authentication, commerce and Internet of Things (IoT).

The Secure Technology Alliance, formerly known as the Smart Card Alliance, invests heavily in education on the appropriate uses of secure technologies to enable privacy and data protection. The Secure Technology Alliance delivers on its mission through training, research, publications, industry outreach and open forums for end users and industry stakeholders in payments, mobile, healthcare, identity and access, transportation, and the IoT in the U.S. and Latin America.

For additional information, please visit www.securetechalliance.org.

# Table of Contents

# 1 Introduction

The payment industry continues to push for payment authentication methods that improve on traditional methods while minimizing disruption to the card manufacturing process. With this in mind, some card vendors, technology suppliers, and solution providers are redefining what could become the next standard for payment technologies with cards—biometric authentication. Biometrics has always provided a way to address multifactor authentication, fulfilling the "who you are" factor requirement and working in conjunction with "what you have" (a card) and "what you know" (a PIN).

This white paper focuses on fingerprint matching as a biometric authentication solution for payment cards. While solutions involving other biometric factors (e.g., iris recognition, facial recognition, biorhythm) could be implemented in the future, the current inclusion of fingerprint sensors in multiple devices makes fingerprint matching the most viable solution at this time.

While fingerprint capture on an external device can be supported, this white paper looks solely at incorporating fingerprint capture, template storage, and matching on the payment card itself. Although the implementation models differ slightly, new technologies that enable template matching and storage in the secure element, battery-free operation, and fast transactions are being showcased in pilots and proof-of-concept launches around the world.

It is important to mention that product availability is still in the early stages and standards are still evolving, with specifications being written by industry standards bodies and the payment networks. Therefore, this white paper should be considered as a primer and an introduction to biometric payment cards. For further details, contact the payment networks and the individual solution providers.

# 2 Overview

New developments are opening the door to a new type of payment card, a biometric card that relies on the prevalent user-to-mobile authentication technology—fingerprints—for authentication. Such a card can change the way cardholders authenticate themselves for a payment transaction.[1]

## 2.1 Biometric Payment Card Components

Figure 1 shows the main components of a dual-interface biometric card.

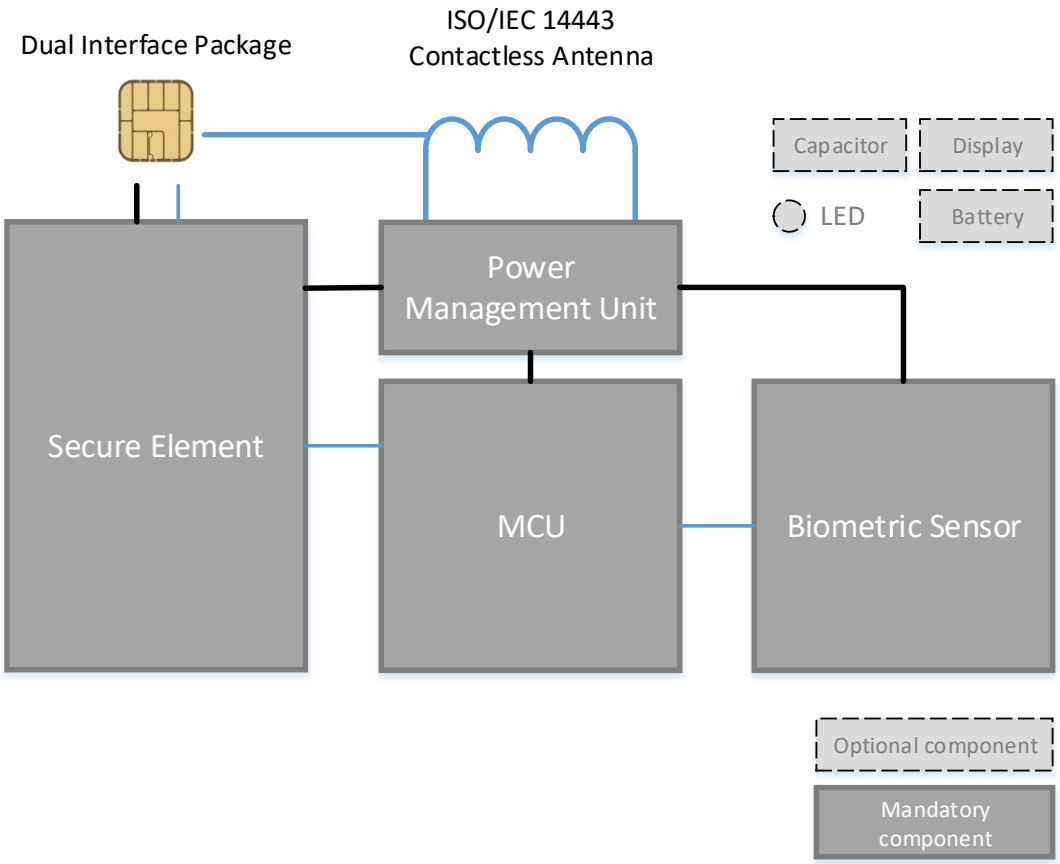


**Figure 1. Components of a Biometric Card**

As in a traditional card, the secure element (SE) contains the EMV-compliant payment applications and is EMVCo certified. Unlike a traditional card, cardholder verification is performed directly on the card. The microcontroller unit (MCU) performs the biometric functions, such as extraction and, in some cases, matching, although in most biometric cards, matching and template storage are handled by the SE for security reasons. Storing templates and performing matching in the SE reduces the chance that templates or authentication communications will be compromised. The biometric system relies on the

[1] Biometric cards can also support other authentication requirements, such as authentication for access; however, this white paper focuses on payments.

technology (hardware and software) that is used in smartphones, adapted to the specific requirements of a smart card (e.g., size, thickness).

Biometric cards can be powered by a magnetic field, which is provided by the payment terminal, so that the card may not require a battery. The power management unit extracts power from the magnetic field and provides it to all components of the card. Usually one contactless antenna powers the power management unit and communicates with the SE. Most solutions support both contact-based and contactless interfaces for the biometric function, using a dual-interface package.

In cases where the solution supports it, LEDs can provide visual feedback to the cardholder. Otherwise, feedback is provided by standard approval messages from the point-of-sale (POS) terminal.

## 2.2 Fingerprint Enrollment Methods

To ensure fingerprint matching, a card can store multiple biometric templates created from different orientations. Solution providers currently offer three different approaches to template capture and enrollment:

- On-card enrollment
- Enrollment at a payment terminal
- Enrollment at a bank

### 2.2.1 On-Card Enrollment

On-card enrollment is managed entirely by the card components and could be done at any location. Templates are captured in the card's fingerprint reader and stored directly in the SE. A sleeve or NFC-enabled device provides power to the card for initial enrollment. Visual feedback is provided by the card, sleeve or NFC-enabled device, and the template is never captured by, stored on, or transmitted to a third-party device, reducing potential security risks.

### 2.2.2 Enrollment at a Payment Terminal

When enrollment takes place at a payment terminal, the first payment transaction requires the cardholder to enter a PIN on the terminal while touching the fingerprint sensor. Once enough information for the templates has been collected, the templates can be used for payment authentication. The user interface is provided by LEDs on the card.

### 2.2.3 Enrollment at a Bank

Enrollment at a bank requires that the bank provide a specific enrollment terminal or tablet at the bank. An intermediate app transfers the fingerprint to the SE using secure messaging. The interface with the terminal or tablet can be contact or contactless.

## 2.3 How Biometric Payment Cards Work

A biometric card is used for payment as follows:

1. The payment terminal requests communication.
2. The card SE starts up and replies to the terminal.
3. The MCU is activated, communicating with the biometric sensor to perform image extraction.

4. The image is evaluated, either in the SE or in the MCU, by comparing the saved fingerprint templates with the cardholder's fingerprint. Comparison in the SE is more secure than comparison in the MCU.
    - If there is a match, cardholder verification passes (for example, an LED on the fingerprint sensor may glow green[2]) and the SE performs the transaction.
    - If there is no match, cardholder verification fails (for example, an LED on the fingerprint sensor may glow red[2]). Either the transaction is rejected or an alternative cardholder verification method (CVM) is required, such as a PIN.
5. If the transaction is a contactless transaction and the match succeeds, the consumer device cardholder verification method (CDCVM) or other network-defined indicator is sent to the terminal. The terminal may now accept a larger transaction value.

## 2.4 Issuer Considerations

Issuers need to understand the differences between launching a fingerprint card and launching a traditional card. Fingerprint solutions are being designed so that disruptions to the traditional card manufacturing and personalization processes are minimal.

Issuers should anticipate the need for new profiles and scripting to accommodate new versions of payment applications. Also, because a fingerprint transaction is most similar to an offline PIN transaction, issuers need to understand the implications of introducing fingerprint transactions into markets where online PIN and signature are the de facto standard for financial transactions.

The payment networks can provide issuers with additional information about supporting biometrics.

## 2.5 Use and Life Cycle Management Considerations

After a card is issued, the biggest impact is on the user enrollment process. Issuers and vendors will need to define rules for one-time template enrollment and communicate specific disposal procedures to cardholders.

## 2.6 User Experience

Biometric payment cards can be used with current POS terminals. Once a template is successfully enrolled, the user experience during a biometrically authenticated transaction should not differ from the user experience during any other transaction. The cardholder either taps the card on or inserts the card into the POS terminal while holding a finger on the fingerprint sensor. If the fingerprint matches the template, authentication is successful and the transaction is approved with an indicator sent to the issuer indicating the result of the biometric match.[3] If there is no match, the requirement for authentication defaults to the next CVM on the list.

In situations where the card has to be handed to the vendor (such as at a restaurant), the card behaves like any non-biometric card.

[2] How pass/fail information is communicated is implementation specific.

[3] The method for indicating the biometric match result to the issuer for contactless and contact transactions varies by payment network. Some payment networks consider an on-card biometric CVM as the CDCVM. Please contact the payment networks for additional information.

# 3 Benefits of Biometric Payment Cards

Biometric payment cards offer the most benefits when the card is being used for a contactless transaction. When a transaction is contactless, the addition of fingerprint authentication results in improved consumer experience and strengthened risk management. Regardless of transaction type, however, implementing fingerprint authentication on a payment card requires no changes to the current terminal infrastructure.

## 3.1 Transaction Advantages

The addition of fingerprint authentication to a contactless card offers several major advantages.

First, fingerprint authentication increases convenience for the cardholder.[4] For the issuer, fingerprint authentication can strengthen risk management evaluations. And last, the biometric function can be integrated into the current POS infrastructure and pass an indicator of the result of the biometric match; this may permit higher value contactless transactions (in some markets) or serve as the CVM for transactions above a certain amount (e.g., instead of PIN).

### 3.1.1 Cardholder Convenience

Fingerprints as a mode of authentication offer several benefits to cardholders. Transactions can be significantly faster, as there is no need to enter a PIN. (PIN-based authentication and other CVMs can still be options if authentication fails.) Cardholders therefore no longer have to remember a PIN.

Traditional payment cards need approximately 300 milliseconds[5] for one transaction, plus additional time may be required for entering a PIN. For biometric cards, the estimated required transaction time, including authentication, is about 1 second, which is less than the time required by a traditional payment card transaction using a PIN.

Fingerprints also provide cardholder assurance that card misuse will be prevented, and provide a supplementary authentication factor, as described in the EU Revised Payment Services Directive (PSD2) Regulatory Technical Standards (RTS) on strong customer authentication: "The authentication shall be based on two or more elements which are categorized as knowledge, possession and inherence (Biometrics) and shall result in the generation of an authentication code."

### 3.1.2 Risk Management

A payment transaction always involves risk management evaluation, performed either by the issuer host or by the chip card payment application. The EMV risk management process evaluates such things as cryptogram validation results, transaction specifics (amount, country, currency), card authentication and cardholder verification results (offline data authentication (ODA), PIN), and the state of the financial account being used in the transaction (credit limit or balance).

The addition of a biometric sensor to a payment card adds information concerning the transaction that can be used in to enhance the risk management process. This enhanced process can be implemented either at the host or on the card, depending on the biometric system and the payment application.

---

[4] The orientation of the payment terminal could limit cardholder access to a fingerprint sensor for a contact transaction.

[5] Depending on the key length used, or if offline data authentication is used, a transaction could take longer than 300 milliseconds. A contactless tap may not provide enough time.

The enhanced risk management enabled by biometric cards can help issuers improve authorization rates and decrease the fraud resulting from lost or stolen cards.

### 3.1.3 Processing Infrastructure

The processing infrastructure has been standardized for mobile devices using a biometric and is supported to a certain extent by payment terminals. Biometric indicators can be used for both contactless and contact transactions.[6]

In some countries, contactless payment without a CVM can be limited by a ceiling transaction amount. Adding a biometric match, such as fingerprint authentication, can allow transactions above this ceiling.

In the U.S., however, there may be CVM amount limitations for contactless transactions; the cardholder may be prompted for a CVM for transactions exceeding certain amounts.

## 3.2 Impact on Terminal Infrastructure

The ability to add a biometric sensor to a standard ID-1 card body and power this sensor with a standard contact or contactless card reader has made biometric authentication of EMV-compliant or contactless transactions much more practical for issuers and acquirers. It is no longer necessary to add an external biometric sensor to the POS terminal or to manage the biometric authentication process at the terminal. The authentication process handled by the card is completely transparent to the terminal.

A biometric payment card will work without requiring either hardware or firmware changes to EMV chip-enabled terminals. This compatibility makes integration much easier.

In addition, the current guidelines from the different payment networks for biometric cards assume that the terminal will not be sending any additional elements in an authorization request message or be performing any additional processing. All biometric information that needs to be conveyed to the issuer host (for enhanced risk management) has already been added to the data elements currently being returned from the card to the terminal. The terminal handles these data elements in the usual manner, and the authorization host is able to interpret any new information conveyed in specific bits of these modified data items. There is no impact to acquirer systems or software.

Issuers wishing to leverage biometric cards to enable more offline authorizations or provide different card risk-management parameters (for example, offline limits) do so through different card personalization parameters. The terminal infrastructure follows standard processing rules dictated by EMV specifications (for contact transactions) and by the payment networks (for contactless transactions).

Everything works the same way, as far as the cardholder-to-merchant front end is concerned. However, the back-end system now has access to additional CVM-related information, and the issuer can use biometric authentication results to fine-tune both card risk management and host risk management decisions.

[6] Note that the method for indicating the biometric match result to the issuer for contactless and contact transactions varies by payment network. Some payment networks consider an on-card biometric CVM as the CDCVM. Please contact the payment networks for additional information.

# 4 Additional Implementation Considerations

This section discusses additional biometric payment card considerations for issuers in North America.

## 4.1 Processing

When biometric capture and match are done entirely on the card, the cardholder's biometric data never leaves the card. In this scenario, there is no processing impact on terminals, merchants, or acquirers.

In payment transactions at an ATM or when the cardholder does not retain control of the card (e.g., at a restaurant), a biometric payment card acts like a non-biometric chip card.

Issuers will need to look for new information in current data elements to check the result of the biometric verification process. Issuers may also have to support new post-issuance issuer scripts that change the biometric data on the card when necessary.

## 4.2 Standards, Specifications, and Security

Standards for biometric payment cards are still under development. For current specifications, contact the payment networks.

The payment networks may require additional security evaluations to ensure that biometric data is handled securely.

## 4.3 Product Considerations

In determining whether to implement biometrics, issuers should consider their specific product needs. The addition of biometrics can increase confidence that the correct cardholder is using the card. This may be useful for cards supporting specific CVMs or cards supporting offline transactions.

Issuers should also consider costs in identifying which products or cardholder segments are appropriate for biometric card implementation. Biometric cards currently cost more than EMV chip cards, due to increased card complexity and components.

Issuers should contact their payment network for further information.

## 4.4 Cardholder Education

Cardholders will need to be educated on how to use biometric payment cards. Such education should include at least the following information:

- How the enrollment process works.
- How the cardholder's security and privacy are protected during fingerprint capture and storage.
- How to use the card at the POS (e.g., the location of the fingerprint sensor, orientation of the finger on the sensor, expected transaction time, feedback on correct or incorrect biometric read or comparison).

## 4.5 Impact on Terminals

At this time, the payment networks do not require recertification of EMV terminals to use payment cards with biometric sensors if the CVM used for the biometric match is supported.

As discussed in Section 3.2, no changes to EMV terminals are needed for transactions to use biometric payment cards.

## 4.6 Risk Management

An authentication session involving a card that includes a biometric sensor can have three potential outcomes:

1. Biometric authentication is not performed.

   This may be because the cardholder refused to present a finger or because the terminal does not accommodate finger placement during the transaction (for example, at an ATM).

2. Biometric authentication succeeded.

   The cardholder presented a finger, and the biometric authentication process concluded that the fingerprint matched the fingerprint template stored on the card.

3. Biometric authentication failed.

   The cardholder presented a finger, but biometric authentication failed.

The result of a biometric authentication session is important information, which should be conveyed to the issuer in an authorization request (or clearing record), to be used in an enhanced risk management process. In addition, part of the issuer risk management process can be delegated to the card application, with the issuer defining card behavior specific to each of the three potential authentication outcomes. This could involve a number of behaviors, including: using different CVM methods; using different offline counters and limits; using different offline data authentication mechanisms; using a different file structure; and/or using other profile specifics.

In anything but the most primitive biometric-sensor-on-card implementations, the issuer host will receive an indication of whether biometric authentication was performed in a particular transaction, and whether authentication succeeded or failed.

Typically, the Card Verification Results (CVR), or other card-originating data element, will convey the results of a biometric authentication attempt to the host in the authorization request or clearing record. These card elements are already sent by the acquirer (no changes are required to the acquiring software). It is just the specific content of the bitmap sent that will vary in a biometric implementation.

To obtain the maximum benefit from biometric cards, the issuer host should be upgraded to include these indicators in the issuer host risk management process, just as issuers currently consider the results of offline PIN presentation or offline data authentication in determining whether an online transaction should be approved.

# 5 Biometric Payment Card Real-world Examples

Multiple global payment networks have launched biometric payment card pilots and initiatives.

## 5.1 Visa Examples

Visa is piloting a new dual-interface (chip and contactless) biometric payment card with Mountain America Credit Union and Bank of Cyprus—the first pilot in the U.S. to test an on-card biometric sensor for use with contactless payments.[7] Visa is also participating in a pilot with Unilux Cards and Areeba in Dubai.[8] Visa has reported that consumers continue to have strong interest in biometrics, with recent survey results including:

- A total of 86% of consumers are interested in using biometrics to verify identity or to make payments, and more than 65% of consumers are already familiar with biometrics.
- Consumers were most familiar with fingerprint recognition, with 30% having used it once or twice and another 35% using it regularly.
- Of all the biometric authentication techniques queried, fingerprint recognition ranked the highest (50%) in terms of the desired payment authentication method for in-store usage.[9]

## 5.2 Mastercard Examples

Mastercard piloted biometric payment cards in South Africa and Bulgaria in 2017. South Africa was the first market to test the biometric card technology. Two separate trials were concluded: one with Pick n Pay, a leading supermarket retailer, and one with Absa Bank, a subsidiary of Barclays Africa.[10] In 2018, Mastercard has announced biometric card pilots with the National Bank of Kuwait,[11] Fransa Bank (Lebanon),[12] and Intesa Sanpaolo (Italy).[13]

Mastercard has also published the results of their European trial with UniCredit Bulbank in Bulgaria; participants in the trial reported the following results:[14]

---

[7] "Press Here! Visa Begins Pilots of New Biometric Payment Card," Visa press release, Jan. 14, 2018, https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.15401.html.

[8] "Areeba to pilot fingerprint payment card," Finextra, April 16, 2018, https://www.finextra.com/pressarticle/73468/areeba-to-pilot-fingerprint-payment-cards.

[9] "Press Here! Visa Begins Pilots of New Biometric Payment Card," https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.15401.html.

[10] "Thumbs Up: Mastercard Unveils Next Generation Biometric Card," https://newsroom.mastercard.com/press-releases/thumbs-up-mastercard-unveils-next-generation-biometric-card/, April 20, 2017.

[11] "National Bank of Kuwait and Mastercard make GCC debut of pioneering biometric solutions," Zawya, May 14, 2018, https://www.zawya.com/mena/en/story/National_Bank_of_Kuwait_and_Mastercard_make_GCC_debut_of_pioneering_biometric_solutions-ZAWYA20180514123958/.

[12] "Fransabank and Mastercard Launch the First Biometric Card in Lebanon," Fransabank press release, July 25,2018, https://www.fransabank.com/English/MediaCenter/GroupNews/Pages/Fransabank-and-Mastercard-Launch-the-First-Biometric-Card-in-Lebanon.aspx.

[13] "PAYMENTS INNOVATION Italian Bank Intesa Sanpaolo, Mastercard To Test Biometric Contactless Payment Cards," PYMNTS.com, Dec. 19, 2018, https://www.pymnts.com/news/payments-innovation/2018/intesa-sanpaolo-mastercard-biometric-contactless/.

[14] "Mastercard makes biometric cards a reality in Europe: New Trial in Bulgaria," Mastercard press release, July 27, 2017, https://newsroom.mastercard.com/eu/press-releases/mastercard-makes-biometric-cards-a-reality-in-europe-new-trial-in-bulgaria/.

- A total of 93% of the participants found the biometric card more convenient to use than entering a PIN during the transaction.
- A total of 95% of the participants found the biometric card more secure than a regular chip card.
- More than 90% of the participants would upgrade or probably upgrade their favorite card with the biometric feature if it were available.

## 5.3 American Express Examples

American Express has previously conducted small internal pilots of fingerprint cards to validate the enrollment and payment experience, and analyze performance under different technical set-ups.

## 5.4 JCB Example

JCB launched a pilot trial of the JCB Biometrics Card with fingerprint authentication in April 2018, involving JCB employees. Once card users record their fingerprints using a smartphone or tablet app, they can make purchases using fingerprint authentication at merchants accepting JCB Contactless payments.[15]

## 5.5 Other Examples

Additional biometric payment card pilots have been announced globally, including:

- AirPlus (Germany)[16]
- Societe Generale (France)[17]
- Carte Bancaire (France)[18]

[15] "JCB Pilot of Japan's First Fingerprint Authentication Chip Card from IDEMIA," April 18, 2018, https://www.acnnewswire.com/press-release/english/42883/jcb-pilot-of-japan's-first-fingerprint-authentication-chip-card-from-idemia.

[16] "AirPlus announces the first ever successful deployment of contactless biometric payment cards," Sept. 27, 2017, https://www.airplus.com/corporate/en/media-relations/press/studies-and-white-papers/2017/airplus-announces-the-first-ever-successful-deployment-of-contactless-biometric-payment-cards.html.

[17] "Societe Generale to issue biometric cards for unlimited contactless payments," Banking Technology Magazine, Oct. 22, 2018, https://www.bankingtech.com/2018/10/societe-generale-to-issue-biometric-cards-for-unlimited-contactless-payments/.

[18] "Societe Generale, the first bank in France to experiment with the biometric card," Societe General press release, October 18, 2018, https://www.societegenerale.com/en/newsroom/societe-generale-first-bank-in-France-to-experiment-with-the-biometric-card.

# 6 Conclusions

The concept of using biometric authentication in a payment transaction has been around for several years, but until recently, was less commercially feasible because the addition of biometric authentication mechanisms required an expensive update to the terminal infrastructure (i.e., the addition of a biometric sensor device and the software to run the device in the context of an EMV or payment transaction). This biometric upgrade was unlikely to occur given that the majority of the associated cost would be borne by stakeholders that had less to gain from the addition of biometric authentication (i.e., merchants and acquirers).

However, recent improvements in the fields of microcircuitry, power harvesting, and miniaturization have made it possible to add a biometric sensor (and microprocessor) to an EMV chip card, without requiring any internal power source. The biometric unit is able to 'harvest' enough energy from a standard EMV or contactless reader to perform biometric authentication; and this authentication session is fast enough to be performed during a standard EMV payment transaction.

While this innovation has made biometric cards more commercially feasible, there is still work to be done. Payment networks must make modifications to their application specifications in order to integrate the new cardholder verification method(s) into a standard transaction, and to convey authentication results to the issuer host/processor. This will essentially be a new product with all the associated requirements, including testing and letters of approval.

None of these changes are major, but the sum of these minor modifications will take some time to implement; and the situation is still in flux, because specifications have not all been finalized.

The industry expects a fully-certified biometric card to be available before the end of 2019, but this may be an optimistic prediction. Work is proceeding; and a number of pilot projects have shown the feasibility and advantages of the new biometric-enabled smart payment card. However, it may take some time for all components of the authorization system to be fully enhanced. Other challenges remain as well, such as a simple way for the user's biometric to be registered on the card.

The main advantages of a biometric authentication system on a payment card are:

- Enhanced cardholder experience (no PIN required).
- Increased cardholder confidence in the security of the payment transaction. (Biometrics are seen as a strong authentication mechanism).
- Additional risk management information now available to the issuer host/processor.
- Reduced risk of a fraudulent transaction and of transaction repudiation when biometric authentication is performed.
- Higher pre-authorized transaction amounts when biometric authentication is performed due to enhanced issuer risk mitigation strategies (particularly over the contactless interface, where cardholder authentication is often not performed during the payment transaction).
- Less help desk support related to blocked, forgotten, or stolen PINs.
- 'Proof of life' indicator for remote access to services. (It is easier to borrow/steal/guess a PIN, than to borrow a fingerprint.)

It is worth noting that biometric authentication no longer requires major work and expense from terminal manufacturers, merchants, and acquirers. Currently none of these stakeholders are affected by new biometric-sensor-on-card specifications; and the cost of implementation has now shifted to the Issuer and/or cardholder.

# 7 Publication Acknowledgements

This white paper was developed by the Secure Technology Alliance Payments Council to provide a primer on biometric payment cards for issuers, issuer processors, payment networks and merchants.

Publication of this document by the Secure Technology Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Secure Technology Alliance wishes to thank Council members for their contributions. Participants involved in the development and review of this white paper included: American Express; CPI Card Group; Discover Financial Services; Entrust Datacard; First Data; G+D Mobile Security; Gemalto; IDEMIA; Infineon Technologies; Ingenico; Mastercard; MULTOS International; NXP Semiconductors; Rambus; Verifone; Visa.

The Secure Technology Alliance thanks the Council members who participated in the project to write and review the document, including:

- **Andreas Aabye**, Visa
- **Reena Abraham**, Gemalto
- **Bruce Coleman**, American Express
- **Jose Correa**, NXP Semiconductors
- **Jack DeLangavant**, MULTOS International
- **Allen Friedman**, Ingenico
- **Gerry Glindro**, IDEMIA
- **Melanie Gluck**, Mastercard
- **Jack Jania**, CPI Card Group
- **Kenny Lage**, Discover Financial Services
- **Oliver Manahan**, Infineon Technologies
- **Ken Mealey**, American Express
- **Cathy Medich**, Secure Technology Alliance
- **Jean-Louis Meyer**, Entrust Datacard
- **Markus Moesenbacher**, Infineon Technologies
- **Sreenivasan Parameshwara**, American Express
- **Nick Pisarev**, G+D Mobile Security
- **Brian Russell**, Verifone
- **Sridher Swaminathan**, First Data
- **Christopher Tomczak**, Discover Financial Services
- **Bernard Wong**, Mastercard
- **David Worthington**, Rambus

## Trademark Notice



## About the Secure Technology Alliance Payments Council

The Secure Technology Alliance Payments Council focuses on securing payments and payment applications in the U.S. through industry dialogue, commentary on standards and specifications, technical guidance and educational programs, for consumers, merchants, issuers, acquirers, processors, payment networks, government regulators, mobile providers, industry suppliers and other industry stakeholders.

The Council's primary goal is to inform and educate the market about the means of improving the security of the payments infrastructure and enhancing the payments experience. The group brings together payments industry stakeholders to work on projects related to implementing secured payments across all payment channels and payment technologies. The Payments Council's projects include research projects, white papers, industry commentary, case studies, web seminars, workshops and other educational resources.

Additional information on the Payments Council can be found at https://www.securetechalliance.org/activities-councils-payments/.