SECURE
TECHNOLOGY
ALLIANCE

The webinar will begin shortly

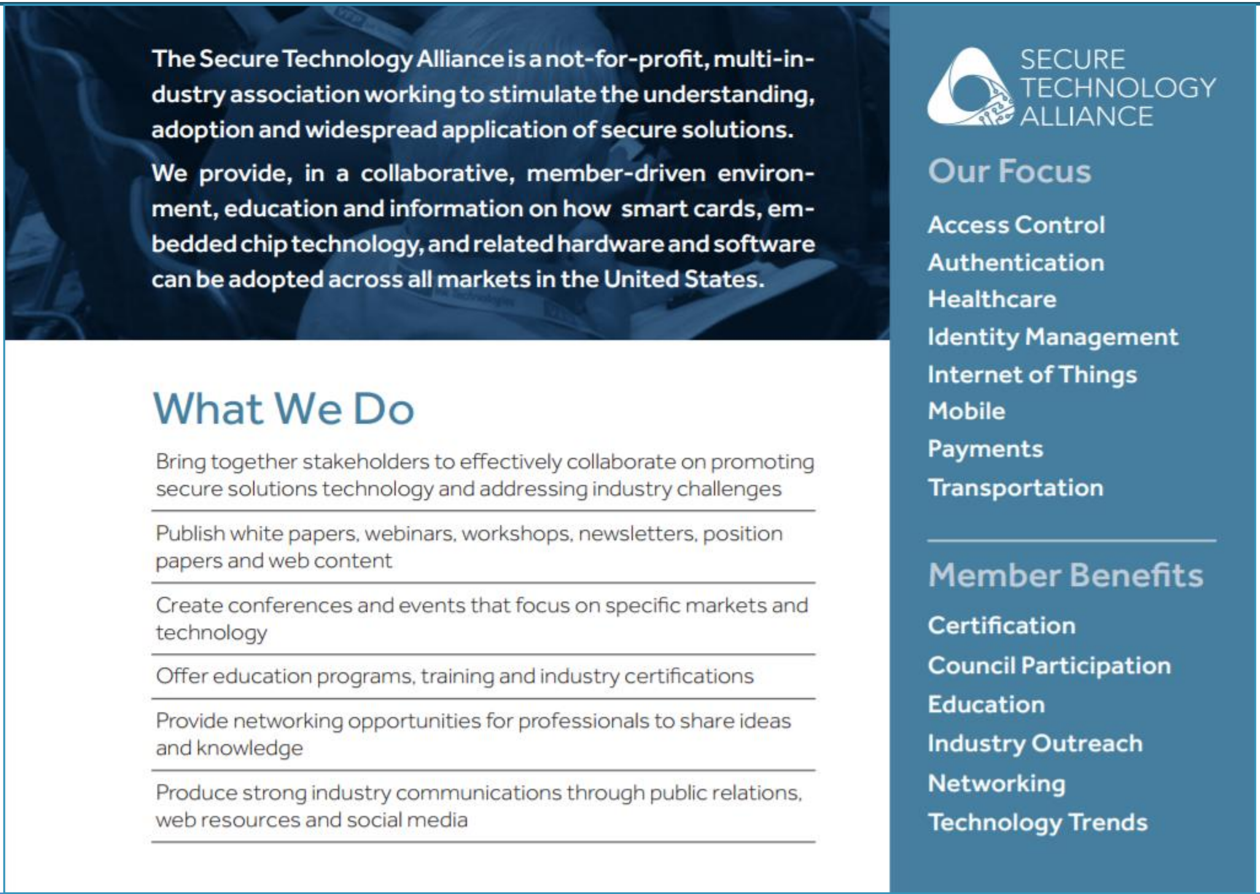
SECURE TECHNOLOGY ALLIANCE

# Biometric Payment Cards

Secure Technology Alliance Payments Council

July 25, 2019

# Who We Are



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.

We provide, in a collaborative, member-driven environment, education and information on how smart cards, embedded chip technology, and related hardware and software can be adopted across all markets in the United States.

## What We Do

- Bring together stakeholders to effectively collaborate on promoting secure solutions technology and addressing industry challenges
- Publish white papers, webinars, workshops, newsletters, position papers and web content
- Create conferences and events that focus on specific markets and technology
- Offer education programs, training and industry certifications
- Provide networking opportunities for professionals to share ideas and knowledge
- Produce strong industry communications through public relations, web resources and social media

## Our Focus

- Access Control
- Authentication
- Healthcare
- Identity Management
- Internet of Things
- Mobile
- Payments
- Transportation

## Member Benefits

- Certification
- Council Participation
- Education
- Industry Outreach
- Networking
- Technology Trends

# 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 about the means of improving the security of the payments infrastructure and enhancing the payments experience

## SELECTED COUNCIL RESOURCES

- Biometric Payment Card
- Contactless Payments: Proposed Implementation Recommendations
- Contactless EMV Payments: Benefits for Consumers, Merchants and Issuers
- Contactless Payments in the U.S.: Guides for Merchants and Issuers
- Contactless Payments Security Q&A
- EMVCo Payment Account Reference (PAR): A Primer
- Implementation Considerations for Contactless Payment-Enabled Wearables
- IoT and Payments: Current Market Landscape
- Blockchain and Smart Card Technology

SECURE TECHNOLOGY ALLIANCE

# Introductions & Agenda

- Randy Vanderhoof, Secure Technology Alliance

- Oliver Manahan, Infineon Technologies

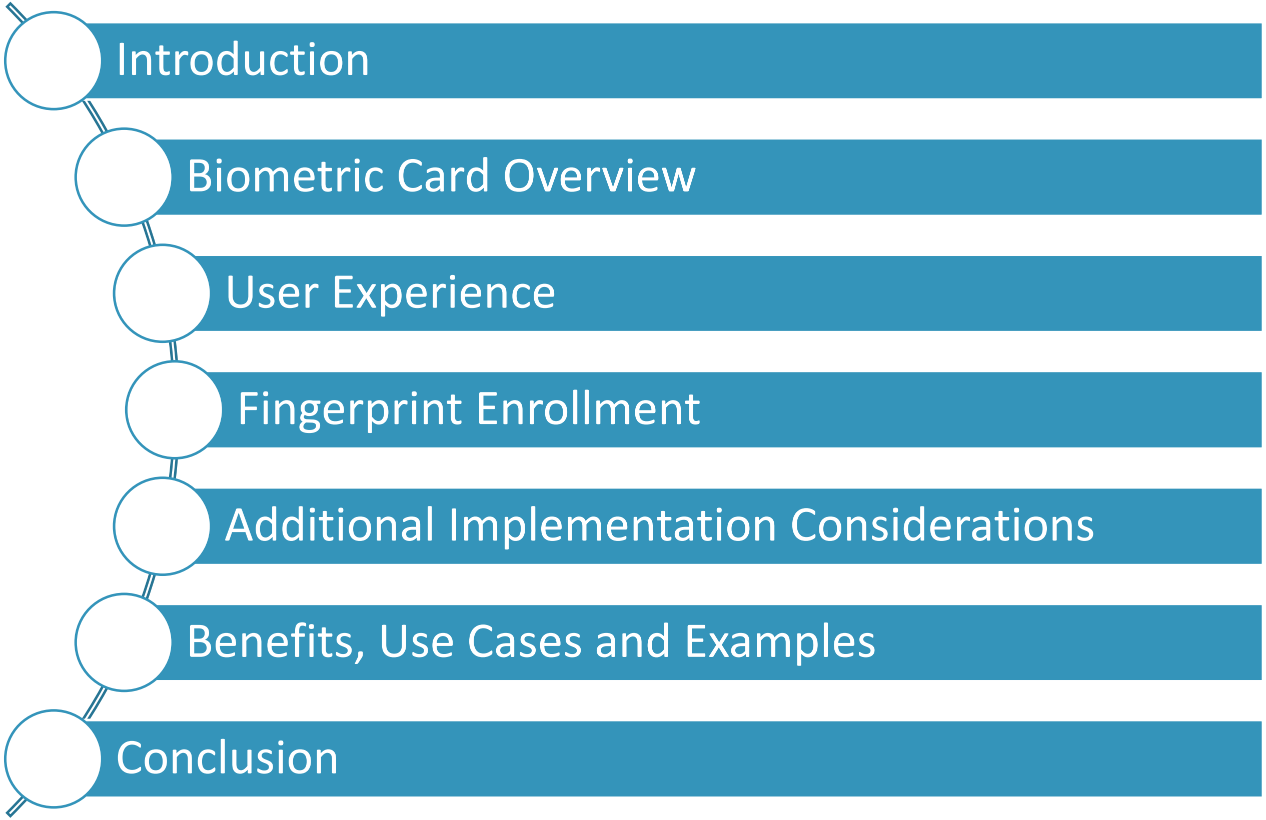
- Jose Correa, NXP Semiconductors

- Tom Rapkoch, Visa

- Gerry Glindro, IDEMIA

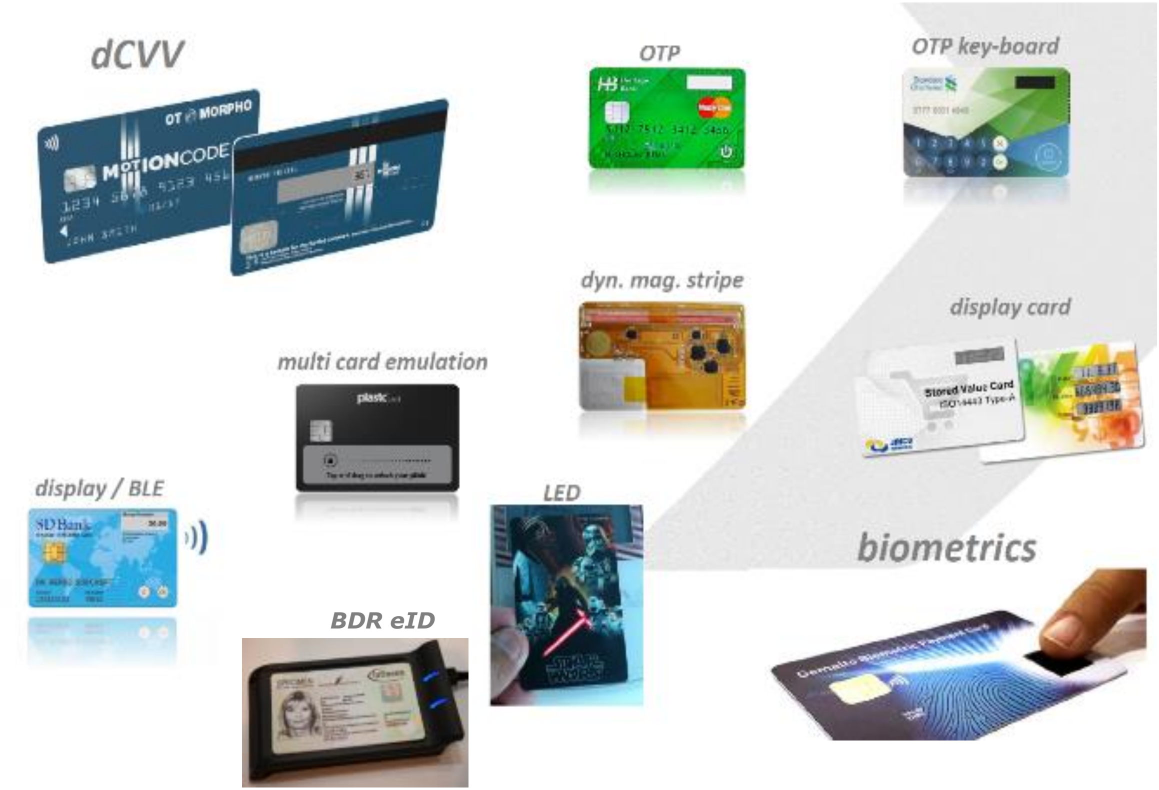
SECURE TECHNOLOGY ALLIANCE

# Agenda



- Introduction
- Biometric Card Overview
- User Experience
- Fingerprint Enrollment
- Additional Implementation Considerations
- Benefits, Use Cases and Examples
- Conclusion

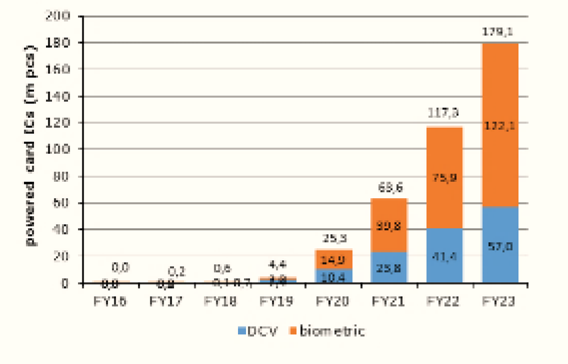
# Different Types of Cards



Source: *LINXENS*

# Enhanced Card ICs Market

Enhanced card ICs [m pcs*]



**ABI - Next generation Powered Payment ABI report, Oct 2017 (pieces)**

Segments for biometric cards:

- Payment DIF cards
- ID cards
- Financial inclusion
- Access

## Biometric Card Verification

- "Standard smart card market" needs to **show innovation**
- Major **payment networks push** and standardization getting concrete…
  - VISA: Released the Visa Biometric Sensor-on-card Specification (VBSS) v. 0.9 in March 2019
  - MC: available spec. since **end 2017**
- **Additional convenience and security,** 2nd factor authentication (applicable also to FIDO)
- Biometric technology has become **widely accepted by mobile telephony**
- Use cases…
  - **Premium security** for high-end customer base
  - In some **regions** (Africa + LATAM) to **mitigate** payment & social/welfare **fraud**
  - **Convergence** with other use cases as access, ID as **personal** data **not to be central stored**

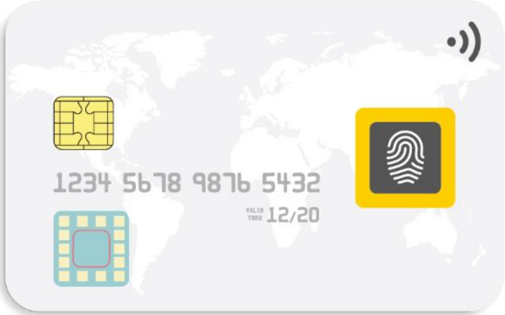
## Dynamic Card Verification

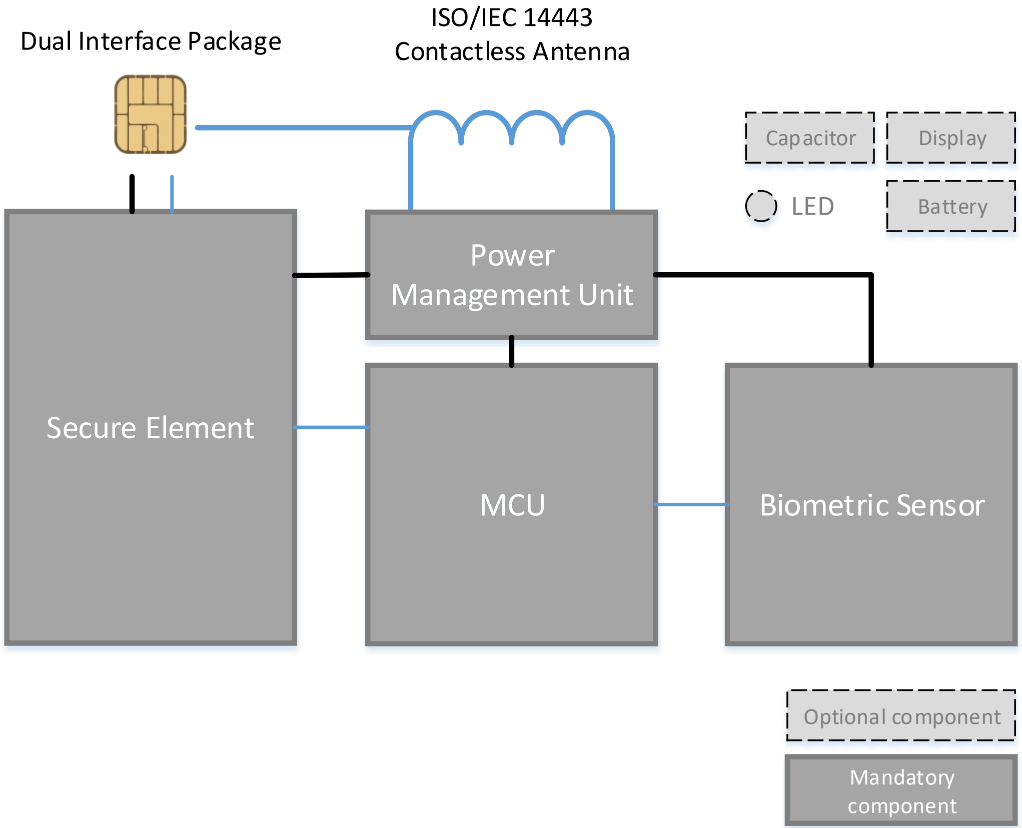
- **Additional security layer** against rates of CNP fraud
- Usually a 3-digit display mounted on the rear of cards

# Agenda

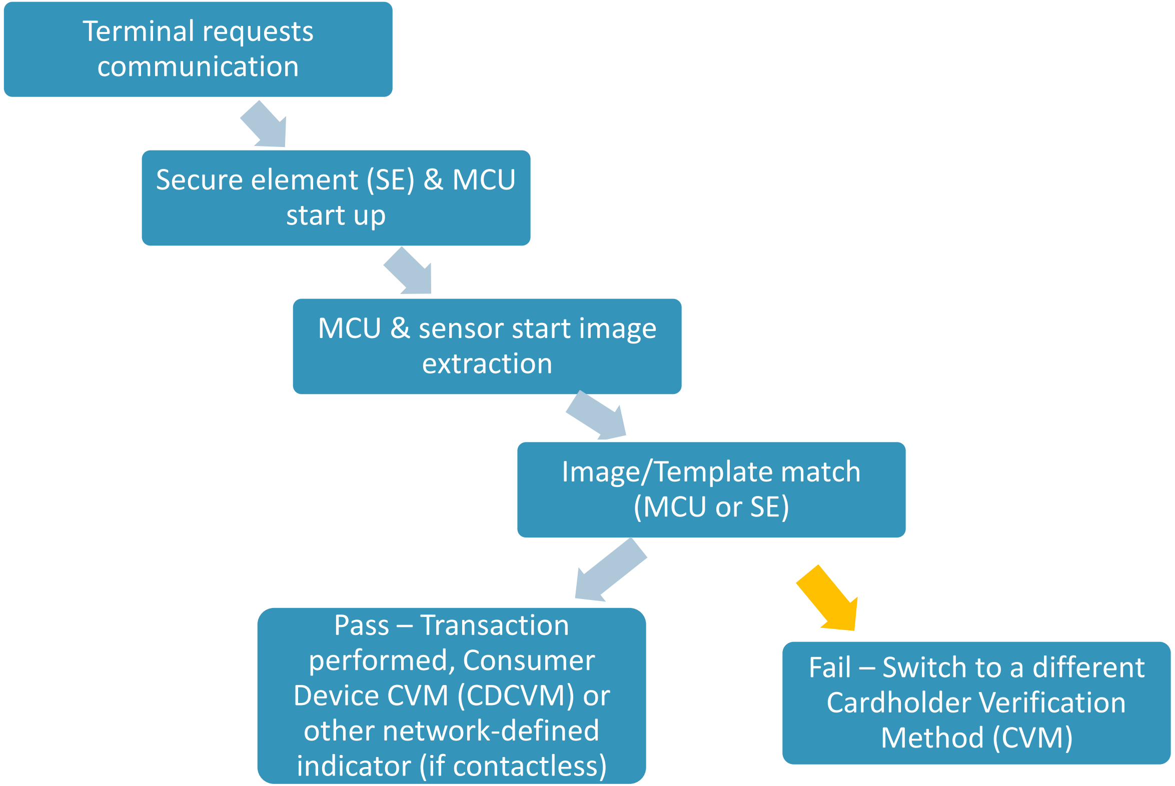
- Introduction
- **Biometric Card Overview**
- User Experience
- Fingerprint Enrollment
- Additional Implementation Considerations
- Benefits, Use Cases and Examples
- Conclusion

# Architecture





# How Biometric Cards Work



Terminal requests communication

Secure element (SE) & MCU start up

MCU & sensor start image extraction

Image/Template match (MCU or SE)

Pass – Transaction performed, Consumer Device CVM (CDCVM) or other network-defined indicator (if contactless)

Fail – Switch to a different Cardholder Verification Method (CVM)

# Agenda

- Introduction
- Biometric Card Overview
- **User Experience**
- Fingerprint Enrollment
- Additional Implementation Considerations
- Benefits, Use Cases and Examples
- Conclusion

# User Experience

- Contact & contactless capable
- Primarily a PIN replacement
- Maintain acceptable speed of transaction (1 second or less)

SECURE TECHNOLOGY ALLIANCE

# Agenda

- Introduction
- Biometric Card Overview
- User Experience
- **Fingerprint Enrollment**
- Additional Implementation Considerations
- Benefits, Use Cases and Examples
- Conclusion

# Fingerprint Enrollment Options

## On Card Enrollment

## On Terminal

## On Bank

# Agenda

- Introduction
- Biometric Card Overview
- User Experience
- Fingerprint Enrollment
- **Additional Implementation Considerations**
- Benefits, Use Cases and Examples
- Conclusion

# Additional Implementation Considerations

- **Issuer Considerations**
  - Manufacturing requirements: differences vs. traditional card construction, power (battery) requirements
  - Personalization considerations: profile updates, equipment requirements

- **Use and Lifecycle Considerations**
  - Activation, enrollment, expiration, disposal

- **Security Considerations**
  - Template capture & storage best practices

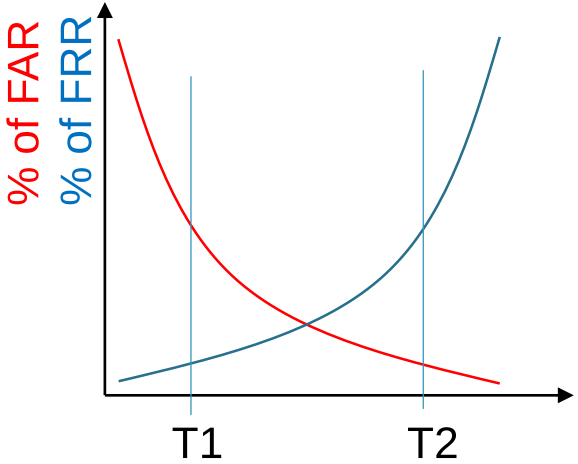
SECURE
TECHNOLOGY
ALLIANCE

# Additional Implementation Considerations

- **False Acceptance Rate (FAR) and False Reject Rate (FRR)**

FRR: % of failed authentication trials of cardholder

FAR: % of successful authentication trials by fraudster



- Operation threshold needs to be defined based on
  - T1: convenient usage (low False Reject Rate) but risky (high % of False Accepts)
  - T2: lower convenience (high False Reject Rate) but secure (low % of False Accepts)

# Agenda

- Introduction
- Biometric Card Overview
- User Experience
- Fingerprint Enrollment
- Additional Implementation Considerations
- **Benefits, Use Cases and Examples**
- Conclusion

# Biometric Pilots (2018) Details

MOUNTAIN AMERICA CREDIT UNION

Bank of Cyprus

| | | |
|---|---|---|
| **Participants** | 130 participants (75 Visa, 50 MACU, 5 FPC) | 50 participants (Bank employees) |
| **Duration** | 6 week trial (Feb – Mar) | 3 month trial (Feb - Mar) |
| **Technology** | Dual interface debit - Kona-I / FPC | Dual interface - Gemalto / Zwipe / FPC |
| **Enrollment** | Enrollment via mobile POS using fingerprint sensor embedded on card | Enrollment via tablet using fingerprint sensor integrated into tablet |

# Potential Benefits

- Speed of transaction – can be faster than PIN
- Use of CDCVM may allow for exceeding contactless thresholds
  - Qualifies as a factor for PSD2
- Enhanced risk management
- No change to terminal required*
- Participant feedback
  - Willingness to pay for the card
  - Fraud protections
  - “Cool” factor

* Note: some exceptions have been identified and are being addressed

# Challenges, and How to Resolve Them

- Peace of mind
  - Many participants emphasized need to solve for swipe and card not present use cases for fear of fraud
    - Resolution: introduction of ability to use other CVMs on the card should biometric validation fail
- Card mechanics were not intuitive and caused confusion
  - Adjusting to the new elements of a biometric card, such as the red and green lights
    - Resolution: cardholder training on functionality
- Biometric methods were inconsistent
  - Unsuccessful usage attempts
    - Resolution: improvements in performance of biometric application – faster, better matching capabilities
- Enrollment procedures need fine-tuning
  - Pilot enrollments required dedicated POS devices or tablets
    - Resolution: new in-home enrollment procedures (sleeves, etc.) being developed to ease adoption
- Limitations of certain card readers
  - Mechanized ATM card readers and dip readers that may not allow user to keep sensor engaged may pose problems
    - Resolution: focus on contactless

# Current Pilots

Source: Nilson Report #1156

| | NatWest | CRÉDIT AGRICOLE |
|---|---|---|
| **Participants** | 200 participants (Bank employees) | 200 participants |
| **Duration** | Open-ended | TBD |
| **Technology** | Dual interface - Gemalto / FPC | Dual interface debit – G&D / NXP / FPC |
| **Enrollment** | Enrollment at Branch and self-enrollments kits provided | Enrollment at Branch and self-enrollments kits to be provided |

# Agenda

- Introduction
- Biometric Card Overview
- User Experience
- Fingerprint Enrollment
- Additional Implementation Considerations
- Benefits, Use Cases and Examples
- **Conclusion**

# What’s Been Done and What’s More to Come

- Advancements in manufacturing (microcircuitry, power harvesting, miniaturization) has made on-card biometric verification commercially feasible.

- Cost shifted to issuer and/or cardholder for on-card biometric sensor. No longer an expense for terminal manufacturers, merchants, and acquirers.

- Still more work to be done that may take some time
    - Payment networks’ modifications on application specifications to integrate biometric verification
    - Relaying authentication results to issuer host/processor

# Drivers for Biometric Payment Cards

- Work continues driven by advantages in biometric card verification
  - Enhanced cardholder experience (no PIN required).
  - Biometrics are seen as a strong authentication mechanism
  - Additional risk management information available to issuer host/processor
  - Reduce risk of a fraudulent transaction
  - Higher pre-authorized transaction amounts
  - Less help desk support related to blocked/forgotten, or stolen PIN
  - Proof-of-life indicator

# For Additional Information: Contact the Payment Networks

- Discover – Kenny Lage, kennylage@discover.com
- Mastercard – biometric.card@mastercard.com
- Visa – Tom Rapkoch, trapkoch@visa.com
- American Express – contact not available

SECURE
TECHNOLOGY
ALLIANCE

# Q&A

# Payments Resources

- Secure Technology Alliance Knowledge Center - https://www.securetechalliance.org/knowledge-center/
  - Biometric Payment Cards
  - Contactless Payments:  Proposed Implementation Recommendations
  - Contactless Payments in the U.S.: Guides for Merchants and Issuers
  - Implementation Considerations for Contactless Payment-Enabled Wearables
  - IoT and Payments: Current Market Landscape
- U.S. Payments Forum – https://www.uspaymentsforum.org

# Speaker Contact Information

- Randy Vanderhoof, Secure Technology Alliance - rvanderhoof@securetechalliance.org
- Oliver Manahan, Infineon Technologies - manahan.external@infineon.com
- Jose Correa, NXP Semiconductors - jose.correa@nxp.com
- Tom Rapkoch, Visa - trapkoch@visa.com
- Gerry Glindro, IDEMIA - gerry.glindro@idemia.com

SECURE
TECHNOLOGY
ALLIANCE

191 Clarksville Road
Princeton Junction, NJ 08550