Who We Are

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
... 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 Payments Security Q&A
- Dynamic Security Code Cards: A Primer
- Electric Vehicle Charging Open Payment Framework with ISO 15118
- 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
Webinar Topics and Speakers

1. Introduction
2. Benefits of Dynamic Security Code Cards
3. Issuer perspective
4. Stakeholder implementation considerations
Introduction
Francine Dubois, IDEMIA
The Shift to Digital Commerce Is Here to Stay

Share of consumers who have shifted to digital¹

12.3% Mar 2020

45% Nov 2020

79% of consumers plan to continue the digital shopping practices they adopted during the pandemic¹

+42% North America digital transactions from June 2019 to June 2020²

2020 CNP fraud x2³

References:
1. PYMTS.com, Online security and the DEBIT-CREDIT divide, January 2021
2. CNP Newsletter, February 11, 2021
3. Robert Tharle, Fraud Prevention, November 21, 2020
CNP Fraud and COVID

• **Opportunistic fraud tied to Pandemic**
  - Fraudulent e-commerce shops set up to steal card data with CVV
  - Bot and “carding” attacks increasing. Fraudsters deploy bots to make small purchases to identify valid cards, followed by more frequent higher value transactions. Target = vulnerable merchants with less robust fraud systems like small to medium eCom businesses, QSRs or charitable websites
  - Huge increase in click and collect or Buy Online, Pickup In-Store (BOPIS) which helps fraudsters evade robust in-store EMV defenses and gain access to goods the same day with compromised credentials

• **40 million cards exposed in 2020** (50% issued in the US) and a corresponding 20% YoY increase from 2019. Similarly, demand for CNP records rose in 2020 with a 20% YoY increase

---

1. FIS, *Early indicators of fraud trends emerging from COVID-19*, July 13, 2020
False Positives/Declines

Legitimate purchase made with a valid payment card that is incorrectly rejected by the card issuer

- **Prevalence**
  - New shoppers 2x greater than pre-Covid and 5-7x more likely to get declined

- **Impact on eMerchants**
  - 40% of declined users never come back to that site
  - Millions in lost revenue

- **Impact on Issuers**
  - Loss of market share to competitor
  - 68% Reduction in cardholder spend
  - Cost of customer support call, etc...

- **Impact on Consumers**
  - Frustration

---

25% of cardholders move a declined card to the back of their wallet

39% of cardholders change their payment method after a decline

68% average spend reduction per order after a decline

---

1. Forter “New User Missed opportunity”
4. Radial, False Positives White Paper, The monster that’s really killing you and how to survive, 2018
The Need for New Solutions

- Increase in security
- Lower CNP fraud rate
- Lower fraud management costs
- Less card reissuance
- Increase in revenue
- Less false positives & missed opportunities

The right balance between security & transaction approval
What Are Dynamic Security Code Cards?
Cyril Lalo, Ellipse
The Natural Evolution of Payment Cards

Extending the security enhancements of EMV to eCommerce

- Card & transaction data
- Contact EMV
  - Contactless
  - DCVx2
- Authorization
- Authentication & synchronization
  - Speed & convenience
  - Dynamic Card Security Code for more secure CNP transactions
What Are Dynamic Security Code Cards?

Regular EMV Dual Interface payment card with embedded mini-screen

- Electronic paper display
- Security code refreshes automatically
  - Using a timer or
  - During every EMV transaction
- Identical characteristics of regular payment card
Dynamic Security Code cards – Overview

**Time-based** solution

- Code changes automatically, at set intervals
- Utilizes an internal real-time clock (RTC)
- Battery powered

**EMV integrated** solution

- New code generated natively by the EMV App during every EMV transaction
- Powered by terminal (POS, ATM, contact or contactless)
Dynamic Security Code Cards
Benefits of Dynamic Security Code Cards

Oliver Manahan, Infineon Technologies
Increase in Security

Additional layer to other CNP fraud solutions

**Combats fraud at the source**
- Provides protection at the **card level**
- Deters card information theft

**Addresses false positives**
- Brings **issuer-controlled** dynamic data point to verification process
- Enables more accurate and reliable authorizations

**Disrupts points of collection**
- Provides date, time and place of origin for each DCVx2 (EMV integrated)
- Benefits all cards, including those with static security codes
Familiar & easy to use

- Used exactly the same way as regular static security codes
- Works on any channel
- Does not require additional apps or plugins
- Provides peace of mind
Transparent to Merchants

- No additional action required to process dynamic security codes
- No impact on infrastructure, checkout page, and ordering systems
- Works on existing card not present channels
Issuer Advantages

Stronger card security
- Reduction of CNP fraud
- Lower fraud management cost
- Less card reissuance

Market differentiation
- Brings real consumer appeal
- Improve brand image

Revenue increase
- New customer acquisition
- Value add service

Improve cardholder trust and confidence
Top of wallet for in-person transactions, eCommerce, and eWallets
Stakeholder Implementation Considerations

Gerry Glindro, IDEMIA
Tom Rapkoch, Visa
Implementation: Issuer

**Time-based solution**
- Dynamic Security Code refresh frequency
- Decisions on validation server
  - In-house development/Off-the-shelf software
  - Payment network service
- Proper Card/battery disposal

**EMV integrated solution**
- Educate users on regular POS transactions to refresh
### Implementation: Personalization Bureau

<table>
<thead>
<tr>
<th></th>
<th>Time-Based Solution</th>
<th>EMV-Integrated Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personalization Timeframe</strong></td>
<td>Some battery drain while in vault storage.</td>
<td>No change</td>
</tr>
<tr>
<td><strong>Hardware</strong></td>
<td>2(^{nd}) contactless module required (ISO 154693)</td>
<td>No change</td>
</tr>
<tr>
<td><strong>Personalization</strong></td>
<td>EMV chip and display personalization</td>
<td>Regular EMV personalization</td>
</tr>
<tr>
<td><strong>Certification</strong></td>
<td>Payment network certification</td>
<td>Payment network certification</td>
</tr>
<tr>
<td><strong>Time server</strong></td>
<td>Synchronization with UTC time used with Verification Server</td>
<td>Not applicable</td>
</tr>
<tr>
<td><strong>Perso Scrap</strong></td>
<td>Proper removal of battery from scrapped cards</td>
<td>Not applicable</td>
</tr>
<tr>
<td><strong>Fulfilment/packaging</strong></td>
<td>Special fulfilment and special mailing packaging</td>
<td>Regular fulfilment and mailing</td>
</tr>
<tr>
<td><strong>Visual inspection</strong></td>
<td>Visual check – sufficient sampling size to ensure DSC refreshes tied to refresh period</td>
<td>Automated inline camera inspection during EMV personalization or visual check with card reader</td>
</tr>
</tbody>
</table>

**Dynamic Security Code Cards**

22
### Implementation: Issuer Processor

<table>
<thead>
<tr>
<th></th>
<th>Time-Based Solution</th>
<th>EMV-Integrated Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Change mechanism</strong></td>
<td>Time based. Automatically updated at configured intervals.</td>
<td>Updated during a card-present EMV transaction.</td>
</tr>
<tr>
<td><strong>Change frequency</strong></td>
<td>The change interval is based on the issuer’s risk policy and can range from 15 min. to 24 hrs.</td>
<td>The change interval is based on the frequency of card-present EMV transactions.</td>
</tr>
<tr>
<td><strong>Clock management</strong></td>
<td>Yes</td>
<td>Not Applicable</td>
</tr>
<tr>
<td><strong>Infrastructure integration</strong></td>
<td>Requires light integration</td>
<td>Leverages existing EMV infrastructure</td>
</tr>
<tr>
<td><strong>Algorithms</strong></td>
<td>OATH, Visa, others</td>
<td>Leverage algorithms available in current authorization platforms (i.e., algorithms used to generate static CVV or contactless magnetic stripe CVV)</td>
</tr>
<tr>
<td><strong>Verification server</strong></td>
<td>• Proprietary server software</td>
<td>Leverages existing Issuer processor HSM</td>
</tr>
<tr>
<td></td>
<td>• Visa solutions</td>
<td></td>
</tr>
</tbody>
</table>
Implementation: Processor – Time Based

1. Card data (PAN, expiry date and DCVV Value) sent "normally" via Payment Service Provider up to the issuer’s authorization server, just as a transaction with a "normal" card.

2. Card is recognized as a Dynamic CVV by its PAN or BIN: as a result, DCVV check is routed for validation towards the DCVV server.

3. The DCVV server compares the DCVV Value submitted with the one it calculates.

4. Result (Valid / Invalid) is routed back to the issuer’s server.

5. Transaction is approved/rejected.
**Implementation: Processor – EMV Integrated**

DCVx2 verification request replacing CVx2 verification request

*BIN/PAN range or product ID

*CVx2 = CVV2 (Visa) or CVC2 (Mastercard)
## Implementation: Network

<table>
<thead>
<tr>
<th><strong>Time-based solution</strong></th>
<th><strong>EMV integrated solution</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable static security code checking</td>
<td>Disable static security code checking</td>
</tr>
</tbody>
</table>
| Network and card must be in sync  
  • Time Window Unit |  |
| Key designation |  |
| In-flight transactions, deferred authentication | Transparent, no change |
Conclusions
Cyril Lalo, Ellipse
Conclusions

Dynamic Card Security Codes are more secure than static data.

Card level security addresses fraud at the source.

An issuer-centric solution.

Transparent for cardholders.

Robust addition to analytical/behavioral-based security layers.
Payments Resources

• Secure Technology Alliance Knowledge Center - https://www.securetechalliance.org/knowledge-center/
• Dynamic Security Code Cards: A Primer white paper
• EMV Connection web site
• mDL Connection web site
• U.S. Payments Forum – https://www.uspaymentsforum.org
Speaker Contact Information

- Jason Bohrer, Secure Technology Alliance - jbohrer@securetechalliance.org
- Francine Dubois, IDEMIA – francine.dubois@idemia.com
- Cyril Lalo, Ellipse – clalo@ellipse.la
- Oliver Manahan, Infineon Technologies – manahan.external@infineon.com
- Gerry Glindro, IDEMIA – gerry.glindro@idemia.com
- Tom Rapkoch, Visa – trapkoch@visa.com