SECURE TECHNOLOGY ALLIANCE

A SECURE TECHNOLOGY ALLIANCE PAYMENTS COUNCIL WHITE PAPER

Dynamic Security Code Cards: A Primer

Version 1.0

July 2020

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).

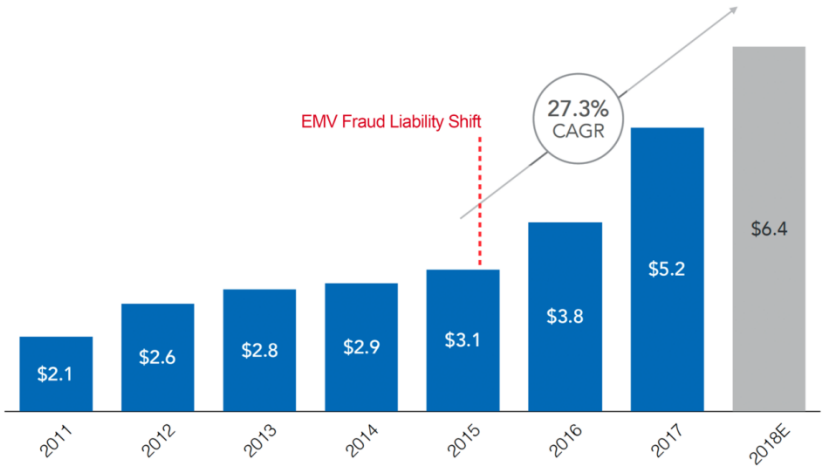
The Secure Technology Alliance, formerly known as the Smart Card Alliance, invests heavily in education on the appropriate uses of secure technologies to enable privacy and data protection. The Secure Technology Alliance delivers on its mission through training, research, publications, industry outreach 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 implementation of EMV in the United States has resulted in numerous changes affecting all stakeholders—merchants, issuers, processors, and consumers. One of the more notable results of EMV implementation, however, is that fraudsters have shifted their focus to card-not-present (CNP) transactions (Figure 1 and Figure 2) to avoid the enhanced security of EMV.



Source: FT Partners 2018

Figure 1. CNP Fraud in the United States

Card payment type	Remote card payments fraud ($ billions)	
	2015	2016
Total cards	**3.40**	**4.57**
Credit cards	2.37	3.15
Debit cards[1]	1.03	1.42

Source: https://www.federalreserve.gov/publications/2018-payment-systems-fraud.htm

Figure 2. Remote Card Payments Fraud According to Federal Reserve

CNP fraud incidents have far-reaching consequences that affect all payments stakeholders. It is therefore critical to manage this increased threat while minimizing friction for consumers.

The next sections discuss the impact of CNP fraud on merchants and issuers.

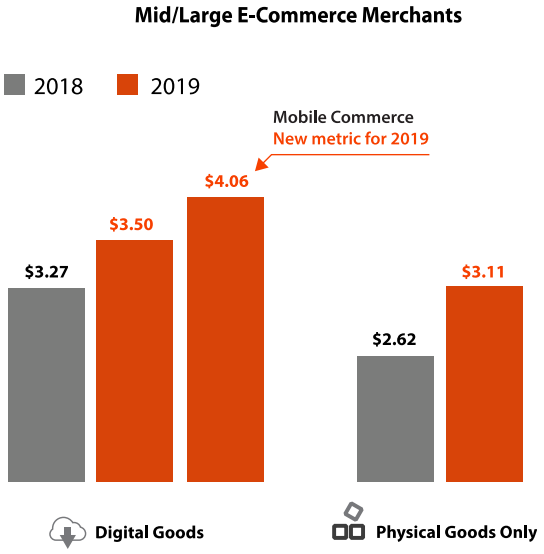
1.1 CNP Fraud: Impact on Merchants

CNP fraud has a serious impact on e-merchants, who not only lose goods (and the associated revenue) but who are also subject to chargebacks. To counter this, e-merchants must invest in more anti-fraud tools, which raises the overall cost of goods (and may eventually be passed on to the consumer).

As Figure 3 shows, in 2019, the cost of fraud[1] rose for CNP transactions for both digital and physical goods. For mobile commerce fraud, costs were $4.06 per $1 (a new metric for 2019).

In addition to chargebacks and fees, these higher costs included:

- The cost of redistributing merchandise
- Labor/investigation costs
- Legal prosecutions resulting from fraud
- IT/software security costs
- Device assessment[2] (m-commerce)
- Individual assessment[3] (m-commerce)



Source: Lexis Nexis, True cost of fraud report 2019

Figure 3. Cost of Fraud for Digital and Physical Goods for Mid/Large E-Commerce Merchants with $10 Million+ in E-Commerce Sales

1.2 CNP Fraud: Impact on Issuers

Issuers are also being seriously impacted by CNP fraud, often needing to reissue cards. Issuers also can be liable for the following costs, which far exceed the cost of replacing a card:

- Customer service support
- Fraud teams and investigations
- Loss in revenue from false declines of transactions deemed by the issuer as being too risky

---

[1] Fraud definitions: Unauthorized transactions, misuse of stolen payment methods, fraudulent requests for refund/return, redistribution costs associated with redelivering purchased items. Does not include insider fraud or employee fraud.

[2] Uniquely identify a remote computing device or user (Solution examples: device ID/fingerprint; geolocation).

[3] Analyzes human device interactions and behavioral patterns, to discern between a real user and an impostor by recognizing normal user and fraudster behavior (Solution examples: authentication by biometrics; email/phone risk assessment; browser/malware tracking).

- Loss in revenue while the cardholder is waiting for a replacement card
- Loss in revenue when the card on file loses "top of wallet" status and is replaced with a competitor's card
- Loss in revenue due to lost consumer confidence, which translates into less spending
- Damage to the brand, including deterioration in cardholder confidence and degradation in cardholder loyalty
- Disintermediation if cardholder chooses an alternate payment method not associated with the issuing bank

1.3 Dynamic Security Codes

One of the tools used by many e-merchants to validate that the cardholder has possession of the card is the card security code, a three- or four-digit number printed on the card. This is a weakness in itself since that security code is static.

The cardholder gives the card security code to the merchant, who transmits it to the card issuer for verification, together with PAN and expiration date. While the Payment Card Industry Data Security Standard (PCI DSS) prohibits storing card security codes by a merchant (or any stakeholder in the payment chain), a fraudster can obtain the security code if, for example, a merchant stores the data contrary to PCI requirements, or if someone at a brick-and-mortar retail location copies and sells or uses the data. The stolen code can then be reused in combination with the PAN and other card data to commit fraudulent CNP transactions.

This white paper explores one way to address this particular weakness—using cards with dynamic security codes. Security professionals often recommend a layered approach to security,[4] and dynamic security codes are one possible defense against CNP fraud. Other, non-card-based solutions, such as sending the dynamic code to the cardholder via mobile, SMS, or email, employ a similar concept to replace the static code on the card. However, these solutions are considered out of scope for this white paper. This paper focuses on card-based solutions as one of the tools to be considered.

[4] For more information, see U.S. Payments Forum, *Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud*, July 2016, https://www.emv-connection.com/near-term-solutions-to-address-the-growing-threat-of-card-not-present-fraud/.

2 Benefits of Dynamic Security Codes

Dynamic security code cards represent an entirely new mode of authentication, one that is transparent to both consumers and merchants (many of which ask for the security code for CNP transactions) and that also offers numerous benefits to issuers (Section 5.1).

2.1 New Mode of Authentication

Today's payment cards carry vital information, embossed or printed on the card, such as the PAN, the cardholder's name, an expiration date, and a security code. If that data is obtained illegally (for example, by a corrupt employee or a data breach), it can be used to make fraudulent online payments.

One of the methods used to reduce CNP fraud has been to tokenize the PAN; that is, to replace it with a PAN-like number, or token.[5] Dynamic security codes add an additional layer of security to tokenization: rather than being static, the security code changes on the card and is displayed on a mini-screen built into the card (Figure 4).

Figure 4. Example Dynamic Security Code

The security code can be set to change automatically, either at particular intervals (i.e., time-based) or after a specific event occurs (e.g., the event can be a specific action taken by the cardholder or a terminal interaction). Dynamic security codes have a much shorter lifespan than static ones, making them less useful for fraudulent online payments.

2.2 Consumer Benefits

For a security solution to be successful, consumer ease of use is key. Indeed, the more friction there is for cardholders, the higher the risk that they will either abandon the purchase altogether or go somewhere else. The dynamic security code is totally transparent to the cardholder—the cardholder simply enters the security code displayed on the card in the appropriate field on the e-merchant's site; the code is located in the same place on the card as a static code is today.

[5] U.S. Payments Forum, *EMV Tokenization Primer & Lessons Learned*, June 2019, https://www.uspaymentsforum.org/emv-payment-tokenization-primer-and-lessons-learned/.

2.3 Merchant Benefits

Whether a security code is static or dynamic makes no difference to a merchant who requests that code. There are no changes to the customer experience on a merchant's site, and no changes necessary to the site to accept dynamic security codes. Merchants pass this information to the acquirer with the rest of the payment data, in the field currently used for a static security code. Merchants are not responsible for validating the security code.

However, use of dynamic security codes has ancillary benefits even for merchants, as the eradication of fraud vectors leads to better approval rates and reduction in disputes, among other benefits.

2.4 Issuer Benefits

Card issuers are seriously affected by the epidemic of CNP fraud and have a vested interested in fighting it. The dynamic security code card, although more expensive than a standard chip card, offers benefits in addition to fraud reduction. Benefits may include lower overall cost based on the potential for not needing to replace cards, higher customer satisfaction, reduced involvement of fraud teams, the potential for additional revenue (from reduced declines, higher customer confidence/spend and top of wallet status), acquisition of new cardholders, and the perception that the issuer is an innovator.

Another benefit to issuers is that using dynamic security codes supports traceability. Issuers know when a code was valid. If a code is used when it is no longer valid, issuers can better determine where the code was compromised by reviewing card-present transactions that took place when the code was displayed.

These benefits are described in more detail in Section 5.1.

3 Dynamic Security Code Technical Approaches

All payment cards include a security code, although different payment schemes use different names for the code:

- CID or Card IDentification number: Discover, American Express
- CSC or Card Security Code: American Express
- CVC2 or Card Validation Code 2: MasterCard
- CVD or Card Verification Data: Discover
- CVN2 or Card Validation Number 2: China Union Pay
- CVV2 or Card Verification Value 2: Visa

3.1 Overview

Dynamic security codes were developed to counter the increasing incidence of CNP transaction fraud resulting from the theft of static security codes. When the security code is dynamic, it is pointless for potential fraudsters to memorize or store a stolen code.

This white paper focuses on two approaches to changing dynamic codes:

- At issuer-defined time intervals
- During a card-present EMV transaction, such as at a point of sale (POS) or ATM

CNP transactions using the dynamic security code are formatted exactly the same way as CNP transactions that use a static code, using the same fields and field parameters (i.e., length). Cardholders and merchants can maintain their current payment habits and processes, with no need for change.

3.2 Time-Based Solution

One solution for providing dynamic security codes is to change the code on a schedule. Cards that use the time-based solution rely on an internal real-time clock (RTC) to change the code automatically, at set intervals (Figure 5). The issuer can customize the interval at which the code is changed, which can range from minutes to hours.

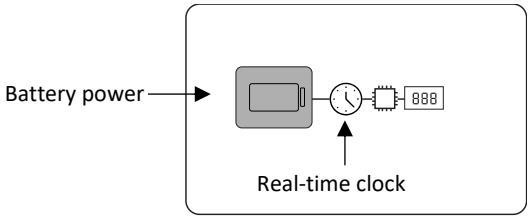


Figure 5. Time-Based Solution

Code validity requires synchronization of each card's internal clock and the back-end server record. Cards using this solution need an internal battery to power the clock and software to manage the processes required to change the code. The codes are typically derived using time-based algorithms (e.g., OATH) or proprietary algorithms such as those devised by Visa and other providers.

3.3 EMV-Integrated Solution

A second solution for providing dynamic security codes is to change the code when a particular event occurs. Standard EMV transaction mechanisms and data elements are used to generate dynamic security codes each time the contact or contactless EMV card is inserted or tapped at a POS or ATM.

Cards using the EMV-integrated solution do not need an internal battery. The display electronics are connected to the EMV chip, and the POS or ATM terminal infrastructure is leveraged to harvest the power required to change the code on the card (Figure 6). The standard EMV elements are used to validate the dynamic security code during a CNP transaction.

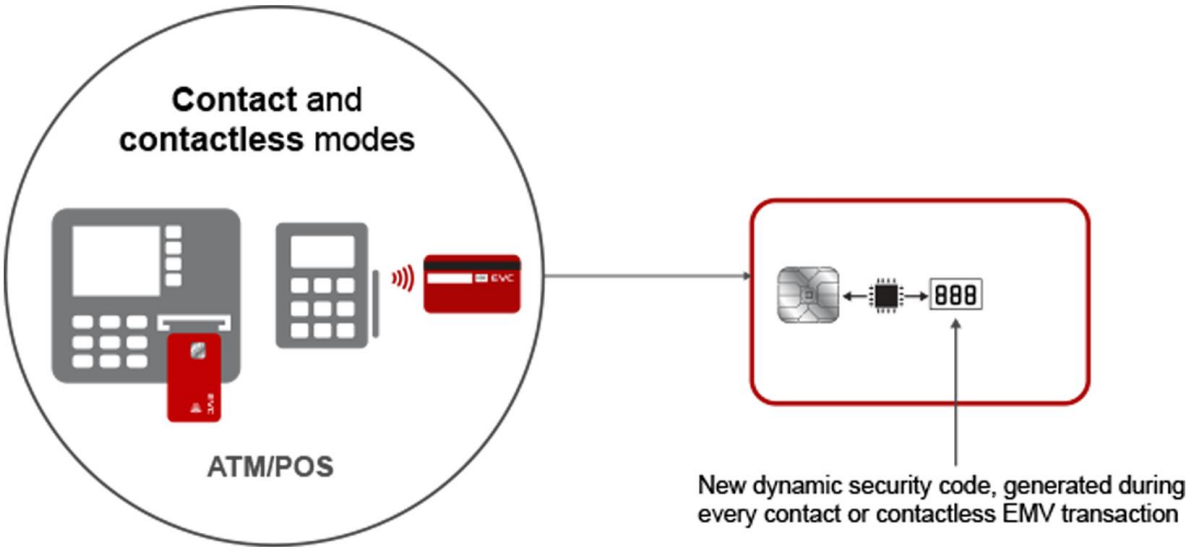


Figure 6. EMV-Integrated Solution

4 Code Verification Server Technical Approaches

Like static codes, dynamic security codes must be verified to complete a transaction.

4.1 Time-Based Solution

Cards that use the time-based solution generate dynamic security codes using an algorithm shared by the card (e.g., Visa, OATH, others) and the back-end server. Verification can be performed by either a proprietary dedicated server or a commercially hosted solution (e.g., Visa dCVV2 Authenticate Service).

The time-based solution requires time synchronization between the card and the server or service and incorporates a time-based validity window (meaning, a code is valid for only a certain amount of time).

4.2 EMV-Integrated Solution

Cards that use the EMV-integrated solution generate dynamic security codes using the algorithms available in existing authorization platforms, such as hardware security modules (HSMs) that are currently used to generate either static security codes or contactless magnetic stripe security codes. Current software implementations can easily be reused for this purpose. Code synchronization between the card and server is handled automatically, using standard EMV protocols and mechanisms.

Other algorithms can be supported with custom development.

Code verification can be integrated into standard payment HSMs or performed by a managed service hosted on the cloud or on site (Figure 7).

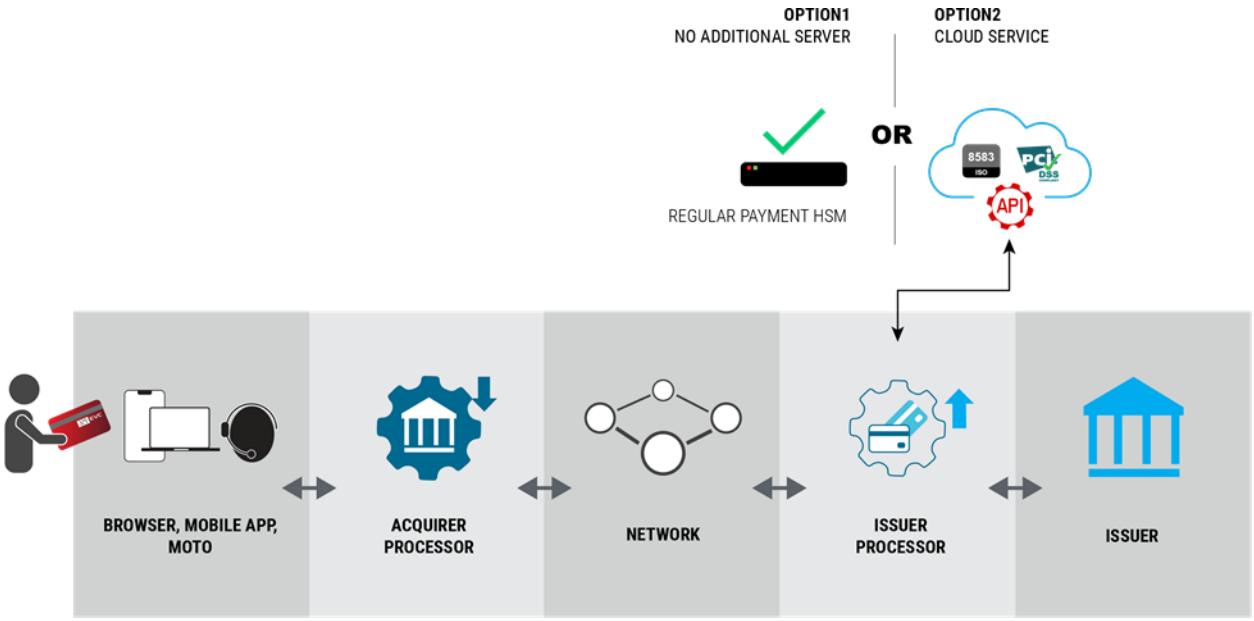


Figure 7. Code Verification Service Options

4.3 Dynamic Security Code Method Comparison

Table 1 compares the two methods for implementing dynamic security code cards.

Table 1. Time-Based Versus EMV-Integrated Dynamic Security Code Methods

Parameter	Time-Based Solution	EMV-Integrated Solution
Change mechanism	Time based. Automatically updated at configured intervals.	Event based. Updated during a card-present EMV transaction.
Change frequency	The change interval is based on the issuer's risk policy and can range from 15 min. to 24 hrs.	The change interval is based on the frequency of card-present EMV transactions.
Power source	Internal battery	Power harvesting
Clock management	Yes	No
Shelf life (time in vault before personalization)	6 months	Based on lifetime of the card
Product lifetime	Based on code refresh rate	Based on lifetime of the card
Infrastructure integration	Requires light integration	Leverages EMV infrastructure
Algorithms	OATH, Visa, others	Various algorithms available in current authorization platforms (i.e., algorithms used to generate static CVV or contactless magnetic stripe CVV)
Verification server	• Proprietary server software • Visa solutions	• Cloud API • Issuer processor HSM in-house
Commercial availability	• Certified products available • Commercially deployed	• New technology • Products available for pilots
End of life/recycling considerations (i.e., battery disposal)	Yes	No

5 Issuer Considerations

This section examines the use of dynamic security codes from the issuer's perspective, including the advantages, impact on the user experience, and the considerations inherent in choosing an appropriate implementation technology.

5.1 Advantages

Issuers can realize multiple benefits from the use of dynamic security codes:

- Reduced costs
- Strengthened security
- Increased revenues
- Opportunity for differentiation
- Ease of implementation
- Ease of deployment

5.1.1 Cost Reduction

Issuers may realize a major reduction in cost if they don't reissue cards after a breach of CNP data. Most fraud occurs 10–30 days after card data has been stolen[6] (to prevent identification of the point of compromise). When a card uses the time-based solution to generate new codes, by the time the compromised dynamic security code is used, it will be obsolete. When a card uses the EMV-integrated solution, the cardholder can update the security code on demand. If a code is compromised, the issuer can contact the cardholder and instruct the cardholder to insert or tap the card at a POS or ATM and generate a new code immediately, thus preventing further use of the stolen code and obviating the need to reissue the card.

Issuers may also experience a reduction in the cost of managing fraud. Because cards generate new codes at known intervals, issuers can easily identify transactions that take place while the code is compromised. A logged history of code changes identifies the period between when a code that was later compromised was generated and when the next code was generated. The data logged during this period, in conjunction with all other transaction history data related to the card, are valuable in identifying suspected points of compromise.

In addition, the possible window for fraudulent transactions is drastically minimized. The frequency of code change is optimally set to 24 hours or less when cards use the time-based solution. When cards use the EMV-integrated solution, the cardholder can be notified to change the code immediately.

Finally, issuers will enjoy a reduction in lost opportunity costs. Use of dynamic security codes means that cardholders no longer have to wait for a replacement card, therefore eliminating the risk to issuers that cardholders will substitute a card from a competing issuer for the compromised card.

5.1.2 Stronger Card Security

Dynamic security codes strengthen the security of all transactions, but especially CNP transactions, in a number of ways. To start, the code is protected "at the source"—that is, on the card itself.

[6] Source: IDEMIA interviews.

Additionally, because the issuer is aware of the dynamic security code being used with a specific PAN, when that account is enrolled into a mobile wallet (e.g., Apple Pay, Google Pay), a dynamic security value will be utilized in the token provisioning, enhancing the security of the wallet enrollment.

When cards use the EMV-integrated solution, security is strengthened by each cardholder's unique use patterns (i.e., code changes only when user performs card-present transactions). Because code validity is unpredictable, there is no preset validity window and the cardholder can control the security code update on demand. Another advantage of EMV integration is that it enables geolocation data. A security code can be associated with the POS or ATM where it was generated. If unauthorized CNP transactions using these codes take place, it is possible to locate the points of compromise. Stolen-card data collection rings are disrupted, thereby reducing overall CNP fraud for both cards with dynamic security codes and cards with static security codes.

Dynamic security codes may improve security even when merchants do not require the security code during transactions. These merchants typically request the code when the customer creates an account with the merchant or changes their online profile (such as to change a postal or email address).

Overall, dynamic security codes provide an additional, frictionless layer of security with no impact on transactions.

5.1.3 Revenue Increase

The use of dynamic security codes can not only cut costs for issuers, it may increase CNP revenue (by up to 20% according to some issuers who have deployed such cards[7]). Several use cases have shown that cards that incorporate these codes experience increased cardholder approval rates (Section 10 lists a few use cases). Cardholders are more confident that transactions involving the cards are secure.

In addition, the dynamic security code capability can allow issuers to increase market share, recruiting new customers (+ 5% for some issuers[8]) by emphasizing the safety of CNP transactions performed using the card. Cardholders for whom the card becomes top of wallet represent increased interchange revenue.

5.1.4 Market Differentiation

Cards that incorporate dynamic security codes can provide issuers with a means of market differentiation, leading to greater card adoption and use. The card is perceived as a more advanced payment card that provides a solution to CNP fraud. Cardholders can actually see the code change and realize that it is not the same as the static code on the back of a card.

5.1.5 Easy Implementation

Implementation of dynamic security codes is not complicated for issuers. The process involves issuers only; there is no necessity to coordinate with cardholders, merchants, or other stakeholders. The infrastructure changes required are minimal: issuers will need only to institute code validation, either in the form of a verification server or third-party service (Section 6).

[7] Source: IDEMIA.
[8] Source: IDEMIA.

5.1.6 Easy Deployment

Issuers will find that cards using dynamic security codes are easy to deploy. The new card simply replaces the cardholder's current card making it frictionless and transparent to cardholders. Issuers may see significant adoption rates – all cardholders may adopt the new card. Cards that use dynamic security codes work on any device and any channel, requiring neither hardware changes nor plugins.

5.2 Impact on Merchants and Users

Dynamic security code cards are used the same way as current static security code cards, without requiring additional action from the merchant who already request security codes. Cardholders use these cards just like a regular payment card during both card-present and CNP transactions. The only potential inconvenience is that cardholders will no longer be able to memorize their security codes. It will always be necessary to provide the current code by looking at the card. Cardholders will need to be instructed on how to use the dynamic security code card, as many may have memorized the static value and the card may need to be used for a card-present transaction to change the security code (depending on the technology).

Merchants can be reassured that use of these cards will not affect their current procedures. Merchants who require the security code for transactions will submit the dynamic code instead of the static code, again without requiring additional action. In actuality, the merchant won't even be aware if the code entered by the cardholder is static or dynamic – and they won't need to know. It is entirely transparent to the merchant.

5.3 Technology Choices

Selecting the appropriate technology to implement dynamic security codes requires a number of considerations.

5.3.1 Time-Based Solution Considerations

One major advantage of the time-based solution is that it does not depend on the EMV chip technology used on the card. Basing the code change on a time interval rather than a particular event that can only be triggered by an EMV-compliant card makes this solution flexible.

However, because cards that rely on the time-based solution include a battery, these cards are subject to shelf life limitations, which also affects the amount of time they can be kept in inventory. It is currently recommended that for optimal operational lifetime, time in storage should not exceed six months. The inclusion of a battery also introduces special packaging and mailing considerations (for example, using a sturdier envelope to protect the card while in transit through the postal system who uses automated sorting equipment).

In addition, issuers who adopt the time-based solution will have to comply with environmental regulations governing both battery usage in consumer products and restrictions on battery recycling. The cards may require special markings and additional accompanying documentation to inform cardholders that they cannot simply cut up an outdated card but must dispose of it properly. Issuers themselves will also need to plan for supplemental waste management and card recycling.

The time-based solution imposes potential limitations on what materials can be used in the form factor. For example, issuers will want to avoid using foil on the card because of the internal battery. In addition, the requirement for an internal battery imposes thermal and planarity limitations for instant

issuance applications (for example, the surface of the card might no longer be totally flat which would impact thermal printing).

5.3.2 EMV-Integrated Solution Considerations

The EMV-integrated solution is EMV chip agnostic (i.e., not dependent on the chip selected for the card). Dynamic codes can be implemented on any EMV-compliant card. Because power is supplied by the terminal, there are no limitations on card materials, shelf life, or card disposal methods.

The new security code is generated during a card-present EMV transaction (i.e., at a POS or ATM). This opens an avenue for issuers to reach out to their cardholders to promote use of the card in both card-present and CNP scenarios.

5.3.3 Impact on Security

The time-based solution changes card security codes automatically, at programmed intervals. Because a code may change in the middle of a CNP transaction, multiple security codes need to be valid simultaneously. Multiple codes must also be valid to allow for time drifts between the card and the verification server. Time drifts occur because the RTC quartz crystal embedded in the card is sensitive to factors such as pressure and mechanical vibrations.

The EMV-integrated solution does not require multiple valid codes. Only one security code needs to be valid at any one time. However, the code can only change when the cardholder performs a card-present transaction. Security may be jeopardized by cardholders who avoid card-present transactions for any length of time.

6 Verification Server Considerations

How to verify dynamic security codes is a consideration for both issuers and processors.

Verification can be performed locally on hardware that has a standard HSM. As an alternative, an external service can provide the verification service.

6.1.1 Time-Based Solution

Codes generated using the time-based solution can be verified by a local verification server, either on site or hosted externally. Verification software provided by a solution vendor or developed in house is installed on hardware with a standard HSM, and verification is implemented as a standard supplemental process. The server requires the dynamic security code key and access to an accurate time server that is synchronized with UTC time.

Local verification allows processors to retain control and manage costs. In addition, this solution allows processors to implement a variety of verification algorithms, such as OATH and Visa. According to Worldpay, who implemented this solution in 2018, no fraud was seen on transactions processed this way.[9]

Issuers may prefer to take advantage of an external hosted service, such as the one provided by Visa. The service provides dynamic code validation when transactions routed through VisaNet are identified as originating on a dynamic-code-capable cards. The Visa service utilizes the dynamic CVV key that the issuer personalized on the card chip. After successful validation, Visa may optionally compute the static code if the static code key is exchanged with Visa. The transaction is then forwarded to the issuer and appears as a standard transaction with the proper static security code.

Using this external service requires that a unique key be shared between the issuer and Visa. The security code is processed accordingly based on whether the PAN is configured to support the dynamic code. The conversion to a static code is optional; the conversion is intended simply to ease implementation.

6.1.2 EMV-Integrated Solution

Verification of a dynamic code generated using the EMV-integrated solution is transparent to issuers, unless they are performing CNP security code verification.

The verification process can be performed on site, as a supplemental process for any standard HSM running verification software that has the dynamic security code key. The verification software can be developed and deployed in house by an issuer, a processor, or a third-party service provider. Onsite deployment supports control over the service and allows for customization.

Verification can also be implemented as a managed service hosted in a PCI-DSS-compliant cloud. This choice offers several advantages over verification performed on site, such as low initial deployment costs, near-infinite scalability, and provisioning flexibility. Using a cloud service has relatively little impact on current processes. CNP transaction security codes are routed to the verification server based on the BIN or PAN. Additional requirements are a call to the verification program API and a key ceremony service to generate appropriate keys.

[9] Source: IDEMIA interview with Worldpay.

7 Card Manufacturer Considerations

The two different approaches to dynamic security code implementation involve different considerations for card manufacturers.

7.1 Time-Based Solution

Cards that implement dynamic security codes using the time-based solution require battery-powered electronics which are sensitive to assembly timing. This type of card must be produced using a cold-lamination manufacturing process, requiring curing time under a press; manufacturers will have to consider storage logistics during the curing period.

Other considerations include the following:

- Electronics need to be ordered and assembled in a timely manner. The battery starts draining as soon as it is attached to the electronics.
- The manufacturing process must be closely synchronized with the electronics assembly process to minimize delays between electronics assembly and encapsulation.
- Manufacturers will need to plan for longer production lead times.
- Manufacturing has limitations with survey finishes that require a high temperature process (e.g., metallic foils, hot stamp).
- Artwork must be designed to provide a transparent window in which to display the security code.
- The presence of the battery means that manufacturing scrap will have to be disposed of according to local law.

7.2 EMV-Integrated Solution

Using the EMV-integrated solution raises fewer issues for manufacturers.

Manufacturers can produce EMV-integrated dynamic security code cards using current hot-lamination, dual-interface manufacturing processes and equipment. This type of card can accommodate the same types of surface finishes and materials as any standard EMV card. The electronics that support the dynamic security codes can be sourced as standard inlays.

The only considerations for manufacturers concern the display and the card material:

- Artwork must be designed to provide a transparent window in which to display the security code.
- Metal cards may require special considerations.

8 Personalization Bureau Considerations

Most considerations for personalization bureaus depend on the choice of implementation technology. Regardless of the technology chosen, however, display functionality quality control needs to be performed during or after personalization (or both).

8.1 Time-Based Solution

Cards that implement the time-based solution introduce hardware, timing, design, and disposal considerations for personalization bureaus.

In cards that generate dynamic security codes using the time-based solution, the chip that runs the EMV application is separate from the chip that runs the dynamic security code application. The EMV application is personalized through the contact interface; the dynamic security code application is personalized through the contactless interface. Therefore, to perform this operation, a personalization bureau will need to add an ISO/IEC 15693 contactless module to the personalization machine.

The dynamic code is calculated based on the chip's internal clock value and a key that is loaded during personalization. In addition, the UTC time server must be calibrated carefully to check the accuracy of the chip's internal clock value.

As is true for any battery-powered device, slow battery drain can be expected while the card is not in use. The refresh rate of the display is set during personalization, and expected battery life should be taken into consideration when setting the refresh rate. The longer the refresh rate, the longer the battery will last. It is recommended that personalization be completed within six months of card manufacture, and it is important to set the card's expiration date before the end of the expected battery life.

Personalization bureaus should also consider the packaging used for the shipment method used to deliver the cards to cardholders. While the card body meets industry standards, material that enhances the rigidity of packaging will protect the card from damage with different mail sorting equipment.

To avoid damaging the card's electronics, thermal printing and embossing need to remain in designated areas.

Finally, certain federal, state, or local laws may require additional information that tells the cardholder how to dispose of the card properly once it has expired. In addition, environmental laws regarding battery recycling may make it necessary to procure a battery punching tool to remove the batteries from scrap cards before they are processed for recycling.

8.2 EMV-Integrated Solution

The EMV-integrated solution introduces fewer considerations for personalization.

Because the code displayed in an EMV-integrated solution is driven by the chip that runs the EMV application, no additional hardware is required for personalization. The chip is personalized through the same interface, writing personalization data to both the EMV application and the dynamic security code application. The personalization script must include the key needed to calculate the code, unless dynamic security code computation is integrated into the payment applet. Fully personalized EMV integrated cards refresh the dynamic security code every time an EMV transaction is conducted at a POS terminal or an ATM. The initial code can be displayed either upon personalization or after the first EMV transaction.

9 Payment Network Perspectives

Payment networks have indicated interest in implementations of dynamic security code cards.

According to Visa: “With the implementation of EMV chip transactions, the largest fraud vector – counterfeit fraud – has been significantly reduced. However, fraudsters are diligent, and have attacked the next easiest fraud channel: online CNP transactions. This has spurred the payment industry to develop robust tools to address this vulnerability, such as Secure Remote Commerce (SRC) and 3-D Secure (3DS). While comprehensive, these solutions also require significant development on multiple vectors in the payment ecosystem – issuers, acquirers, merchants, and networks. Dynamic security codes, as described in this paper, are a comparatively easy solution that may not be as comprehensive, but can be implemented with fairly minimal development required. It can also be implemented unilaterally by issuers and issuer processors, since the solution requires no changes at the acquirer or merchant level. Introducing dynamic data into the transaction message is always preferable to static data, and use of dynamic security codes increases security for CNP transactions significantly.”

Other payment networks have not offered perspectives for this white paper at the time of publication.

10 Use Cases

The following are use cases from a sample of issuers who have experience with cards capable of generating a dynamic security code. The statistics for each case cover the period beginning in July 2019. There are no publicly announced use cases in the U.S. and Latin America as of the date of this white paper publication.

10.1 Société Générale Bank, France

This bank issued Visa, Mastercard, and Cartes Bancaires products to all customers (Black, Gold, Classic). The cards were marketed through different media (Internet banners, the press, metro, bus shelters, and TV spots). The bank offered dynamic security code option for 1€ per month. A total of 30% of DSC cardholders are affluent customers. A total of 10% of all cards issued daily include dynamic security codes. Dynamic-security-code cardholders shop online 20% more of often than non-dynamic-security-code cardholders.

For more information, see https://www.societegenerale.com/en/tech-culture-it/cybersecurity/dynamic-crypto-card.

10.2 Orange Bank, France

Orange Bank issued Visa cards only to their affluent cardholders at 7.99€ per month. They advertised through bank branches, including mobile branches, and their website. A total of 15% of all Orange cards include dynamic security codes. They offered additional perks such as no ATM fees, no international fees and free travel insurance.

For more information, see https://www.orangebank.fr/offre/carte-visa-premium. Note that the information is in French.

10.3 China Minsheng Banking Corp

This Chinese bank issued cards to their Visa Signature customers only for a one-time fee of $15. They used the local national social networks (such as WeChat) to advertise. All cards issued use dynamic security codes daily. All customers are affluent.

11 Conclusions

Cards that incorporate dynamic security codes are an effective solution to combat CNP fraud, regardless of the technology used to implement the codes. Dynamic data is by definition more secure than static data, and when it is layered with other security solutions, such as EMV 3DS or SRC, fraud mitigation is greatly improved.

Furthermore, unlike other CNP fraud prevention tools, dynamic security code cards combat fraud at the source—that is, on the physical card—and are an issuer-centric solution that requires no implementation on the part of a merchant and no behavior modification on the part of the cardholder.

The gold standard in security is to use a layered approach. Dynamic security code cards are an easy layer that any issuer can incorporate into their security strategy.

12 Publication Acknowledgements

This white paper was developed by the Secure Technology Alliance Payments Council to provide a primer on dynamic security code cards, their benefits for issuers, merchants and cardholders, and implementation impact on payments stakeholders.

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: ABCorp; Ellipse; IDEMIA; Infineon Technologies; MULTOS International; Thales; Visa; Worldpay.

The Secure Technology Alliance thanks **Francine Dubois**, IDEMIA, for leading this project, and Council members for their contributions. Participants involved in the development and review of this white paper included:

- **Reena Abraham**, Thales
- **William Bondar**, PNC Bank
- **Jack De Langavant**, MULTOS International
- **Francine Dubois**, IDEMIA
- **Gerry Glindro**, IDEMIA
- **Cyril Lalo**, Ellipse
- **Laval Law**, Ellipse
- **Michelle Lehouck**, ABCorp
- **Christine Lopez**, Worldpay
- **Oliver Manahan**, Infineon Technologies
- **Cathy Medich**, Secure Technology Alliance
- **Sebastian Pochic**, Ellipse
- **Tom Rapkoch**, Visa

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/.