WHITE PAPER

Smart Card Alliance

A SMART CARD ALLIANCE HEALTH AND HUMAN SERVICES COUNCIL WHITE PAPER

Healthcare Identity Authentication and Payments Convergence: A Vision for the Healthcare Industry

Publication Date: February 2016
Publication Number: HHSC-16001

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

Table of Contents

1 Introduction

The overall goal of a convergence vision for the healthcare industry is to leverage available technology components to add healthcare identity authentication applications to the existing payments infrastructure. The Smart Card Alliance Health and Human Services Council developed this white paper to outline a vision for healthcare identity authentication and payments convergence and to provide insight into the opportunities and challenges afforded to the healthcare community as the U.S. migrates to EMV.

The United States is currently in the process of adopting EMV[1], a global standard used by payment applications residing on chip cards[2], point-of-sale (POS) systems, and payment terminals. The U.S. move to EMV chip payments is driven by the payments industry's desire to reduce card fraud, provide global interoperability, and enable safer payment transactions. Meanwhile, healthcare-related fraud is at an all-time high, with billions of dollars lost annually. Clearly, there is an immediate need to increase security for healthcare identity authentication and payments as well.

The pace of U.S. EMV migration is accelerating. Merchant and consumer education campaigns are increasing public awareness of EMV. According to the EMV Migration Forum, over 400 million EMV chip cards have been issued in the U.S. as of the end of 2015, with over 60% of consumers having at least one EMV chip card in their wallets.[3] Most major retailers have converted legacy POS systems to systems that include smart card readers that can accept EMV-compliant chip cards; many have also included support for Near Field Communication (NFC) and contactless payments as part of the conversion. U.S. retailers are making strong progress in migrating their legacy infrastructure to support EMV chip payments, with over 750,000 merchant locations enabled as of January 2016.[4]

Smart card technology and applications are supported by global standards that are used by application and device developers to meet interoperability and other requirements. EMV, managed by EMVCo[5], is the globally adopted payment standard used to implement EMV chip payment applications. Other smart card technology standards are developed by the international community[6] and incorporated into the EMV specifications or used in EMV implementations. For example, ISO/IEC 7816 is a multi-part international standard used in smart card development that has been adopted by EMVCo. Each part of ISO/IEC 7816 defines interoperable specifications relevant to various aspects of smart card technology and its interfaces. This ISO standard and others like it provide for global interoperability by standardizing features such as how to communicate with the card, where the chip is located, and where antennas are placed on contactless cards. The resulting global framework of standards provides a foundation for developing and managing smart card applications that are interoperable with the EMV payment acceptance hardware infrastructure.

The emergence of the EMV-enabled POS infrastructure enables the convergence of healthcare identity authentication and payment; that is, for the healthcare industry to use available smart card and EMV technology to add healthcare identity authentication to the payments acceptance infrastructure. By leveraging the EMV migration and consequent shift in POS technology, healthcare smart cards and the hardware infrastructure to support them are becoming a reality.

---

1 For more information on EMV, see the Smart Card Alliance white paper, "EMV 101 for the Healthcare Industry," at http://www.smartcardalliance.org/publications-emv-101-for-the-healthcare-industry/.

2 In this white paper, the terms "chip card" and "smart card" are used interchangeably. Both refer to a device or card that includes an embedded integrated circuit (IC) chip. Smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and digital signatures) and interact intelligently with a smart card reader.

3 EMV Migration Forum, http://www.emv-connection.com/consumers/

4 "The EMV-Accepting U.S. Merchant Base Hits 750,000, Visa Reports," Digital Transactions, January 28, 2016.

5 http://www.emvco.com

6 Examples of organizations developing smart card standards are ISO/IEC, GlobalPlatform and NFC Forum.

2 Scenarios for Convergence

Healthcare identity authentication and payment convergence can be realized through a variety of technological options, with either front- or back-end integration. Back-end integration requires agreement on a platform definition (including API functionality) across a network of payment and healthcare provider systems. In addition, having a financial processor's system perform transactions directly with a healthcare provider's system requires significant security oversight and compliance. In contrast, front-end integration at a POS terminal or on a smart card can be managed without cross-industry involvement; both smart cards and POS terminals are designed to support multiple applications (e.g., an EMV payment application and a healthcare identity application). Front-end integration using multiple applications on a smart card could be accomplished by leveraging the GlobalPlatform card management standard[7], running in the Java Card runtime environment, or using the MULTOS product platform.

To illustrate the ease of front-end integration to support convergence, this white paper presents four example scenarios, described below. Each scenario discusses integration requirements and benefits and risks of the approach.

The four example scenarios are:

- Scenario 1: two chip cards and one multi-application POS terminal

  Two chip cards perform independent transactions on the same POS terminal, which runs two separate applications to route transaction information to the appropriate back-end system.

- Scenario 2: one multi-application chip card and one multi-application POS terminal

  A single chip card hosts two applications that use the same POS terminal. One chip card application manages financial payment transactions; the second application manages healthcare identity authentication. The POS terminal runs two separate applications to route transaction information to the appropriate back-end system.

- Scenario 3: one chip card with a "special" payment application

  In a variation of Scenario 2, a special payment application on the chip card provides non-payment transactional support.

- Scenario 4: mobile healthcare transactions

  Mobile transactions can use NFC with a POS terminal that supports contactless payment transactions. The mobile application could use a derived credential from any of the above scenarios to facilitate a mobile transaction for healthcare identity authentication or payment.

2.1 Scenario 1: Two Chip Cards and One Multi-application POS Terminal

In the simplest scenario, two chip cards use the same POS terminal for the financial transaction and for identity authentication. The terminal is the convergence point for all healthcare identity and payment transactions.

In this scenario, the POS terminal has one application that reads an EMV-compliant chip card to implement payment transactions and a second healthcare identity authentication application to read the healthcare card.

[7] http://www.globalplatform.org

The transaction would begin with the terminal performing either a financial transaction (EMV) or a healthcare identity authentication transaction. An external application or the POS menu would prompt the healthcare provider attendant to indicate which transaction to perform. If the transaction is an EMV payment transaction, the basic EMV chip data flow would not change. If it is a healthcare transaction, the terminal would query the card to discover an application for identity authentication. The identity authentication application could be a specific healthcare authentication application or use another existing application (such as a government-issued Personal Identity Verification (PIV)[8] card or an electronic driver's license (EDL)[9]).

This scenario offers the following benefits:

- The EMV chip card issuer does not have to be involved with the healthcare identity card issuer, making secure card provisioning much easier and eliminating the need for commercial agreements to be in place.
- Integration costs are minimal, since the healthcare application is a standalone application within the POS terminal and healthcare provider network.
- The requirement for a single multi-application POS terminal minimizes deployment and support costs and saves on valuable counter real estate.

This scenario incurs the following risks:

- Having the POS terminal support multiple services—EMV payment and healthcare identity authentication—requires coordination with the POS device and healthcare identity authentication solution providers.
- This solution could be costly for larger healthcare organizations, which may have complex, embedded POS terminals within a registration or front desk system.

2.2 Scenario 2: One Multi-application Chip Card and One Multi-application POS terminal

Smart cards can store multiple applications securely on a single chip. However, using a single multi-application card at a single multi-application POS terminal requires application integration both on the card and on the POS.

Application integration is not so much a technology challenge as it is a commercial challenge; for both the card and the terminal, one party is the owner (the issuer for EMV chip card) and one party is the co-branded partner (the healthcare entity providing the identity authentication application). A smart card operating system, such as Java Card OpenPlatform (JCOP), can support multiple applications securely using a combination of data encryption and security domains. The owner of the card (for example, a financial issuer) creates a secure domain that can only be accessed using a set of keys that is shared with the co-branded

[8] A Personal Identity Verification card is a U.S. Federal government smart card that provides logical and physical access to Federal facilities.

[9] An electronic driver's license is a state-specific smart card that contains current biographic data for the driver.

partner (the healthcare application provider). The healthcare application provider rotates the keys out to a new key set known only to the provider.[10]

This approach has several advantages:

- EMV chip card issuer data is securely managed and invisible to the healthcare application provider.
- Healthcare application provider data is securely managed and invisible to the EMV chip card issuer.
- Both the healthcare application and EMV chip application reside on the same card. The EMV chip card issuer is the brand owner and the healthcare application provider is the co-brand partner.

This scenario offers the following benefits:

- The relationship between the financial issuer and the healthcare provider is a business relationship.
- The patient has one less card to carry.
- A private security domain is associated with the healthcare provider for the healthcare provider application.

This scenario incurs the following risks:

- The card issuance process is more complex.
- The scenario creates dependencies that have to be recreated or refreshed whenever a patient changes healthcare providers or a financial card is reissued.

2.3 Scenario 3: One Chip Card with "Special" Payment Application

In this scenario, a single chip card would have a "special" payment application that supports EMV chip payment and also allows non-payment data to be stored on the card. Visa and MasterCard have developed payment applications that support on-card data storage.[11] These applications allow an EMV-compliant payment application to store "extra" data that can be used for a non-payment transaction or for identity authentication. The data can be write-protected and validated by the terminal application with a message authentication code (MAC) to insure data integrity.

Such a data storage application could be used to support a profile that authenticates the cardholder to healthcare applications and also identifies any entitlements specific to the cardholder. As an example, multiple back-end healthcare identity management systems could require a specific network IP address to route the identity validation request. That address can be loaded on the chip card. The terminal application reads the stored data to initiate identity authentication and validates the data with a MAC. Optionally, the back-end identity management application could update the data on the card, similar to how a one-time password works.

This scenario offers the following benefits:

[10] This process can be simplified by designating a trusted service manager to manage key rotation.

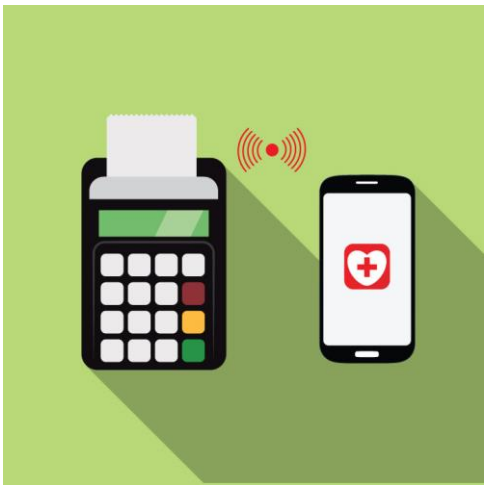
[11] The MasterCard product is MasterCard M/Chip Advance, and the Visa product is Integrated Data Storage.

- Two separate transactions are combined into a single transaction. Accessing the stored data is part of the EMV transaction.
- Although certification is required for the "special" payment application profile, the payment applications themselves are already available, tested, and available in the market.
- Financial issuers can provide this service as a service offering to managed healthcare identity partners.

This scenario incurs the following risks:

- The terminal application is more complex.
- The scenario creates dependencies that have to be recreated or refreshed whenever a patient changes healthcare providers or a financial card is reissued.

2.4 Scenario 4: Mobile Healthcare Transactions



The transactions in any of the scenarios described above could also be contactless, assuming that both the cards and the POS terminals operate in contactless mode.

An NFC-enabled mobile device could be provisioned with the applications described in these scenarios. The payment or healthcare identity authentication transaction is done by tapping the mobile device on the POS contactless terminal. The mobile device can also support a biometric factor or a password, for extra security. Transactions could be linked to a GPS mobile coordinate for post-processing activities.

A mobile device can also support secure card-not-present transactions. Because the keys necessary for a financial or healthcare identity authentication application reside securely on the mobile device, a derivation of the keys could be used to sign a transaction that is completed in the cloud or on a networked server. This capability would offer significant benefits for enabling patient portal access and remotely managing patient continuity across multiple platforms.

3 Implementation Considerations

The healthcare industry faces challenges in implementing both EMV chip payment and healthcare identity authentication applications. Considerations include the cost of implementation, the speed that adoption occurs, the complexity associated with issuing multiple applications, new mobile requirements, and support for interoperable standards.

3.1 Cost of Implementation

U.S. industries are already moving toward an infrastructure that supports EMV chip payments with the healthcare industry moving as well. Because payment terminals are generally controlled by an acquiring network and not the healthcare provider, this migration will be subject to third party coordination which will include how the terminal migration is funded. Generally for smaller providers, the POS terminal can be a standalone platform which will reduce the financial burden. For larger healthcare providers, an integration effort may be necessary with some of the cost needing to come from the healthcare provider. Once an EMV chip payment terminal is implemented, that terminal can be leveraged for healthcare identity authentication as well.

3.2 Speed of Adoption

The healthcare industry is slowly adopting EMV chip payment. Because healthcare is a heavily regulated industry, healthcare personnel are required to focus on meeting mandatory government initiatives and deadlines (such as meaningful use, the Affordable Care Act, HIPAA, and HITECH). Healthcare organizations therefore might not see an immediate need for EMV adoption nor be knowledgeable about the benefits that can be derived from additional payment security and the use of the EMV infrastructure to enable healthcare identity authentication. Education is key to increasing the speed of adoption.

3.3 Multiple Application Issuance

Scenarios in which multiple applications are loaded onto a single smart card require security controls and coordination between multiple issuers. For example, during the data generation and card personalization process, the identity application issuer may need to be securely linked to the payment application issuer. While most authorized card personalization bureaus have these capabilities, this process is not business as usual for either payment card issuers or healthcare providers. Commercial agreements for this process will need to be developed and executed.

3.4 Mobile Considerations

Healthcare organizations are just beginning to adopt sophisticated information technology systems and mobile applications. Mobile applications must be secure and compliant with applicable laws and regulations.

Achieving an appropriate level of support and security on a mobile device is challenging due to the variety of available handsets and operating systems. Another consideration has to do with scaling. Not every individual that has access to healthcare services will carry a mobile device. Elderly Americans and individuals enrolled in Medicaid programs may use their Medicare or Medicaid ID card, and individuals who are considered underserved often may not have access to mobile devices. The types of devices and diversity of people who require medical care make it challenging for organizations to create mobile policies, follow all standards, and protect against data losses.

Notwithstanding the above challenges, the use of mobile applications in healthcare provides significant opportunities for increased administrative efficiencies, scalability of subscriber base, and enhanced security.

3.5 Interoperability and Standards

The Smart Card Alliance strongly encourages all suppliers, practitioners, and providers to collectively collaborate to examine, adopt and execute strong standards and protocols. This will help to achieve industry wide interoperability so that the full range of the benefits from using smart card technology can be realized. It is critical that solution adoption be strongly aligned with interoperable standards to prevent industry fragmentation.

4 Conclusion

Several significant trends are affecting the U.S. payments and healthcare industries: the growth in healthcare-related fraud; patient and record mismatch; and payments fraud, as fraudsters target the U.S. rather than countries that have already implemented EMV. Smart card technology provides solutions to help reverse these trends.

Healthcare industry requirements can only be met by using secure technologies that do not sacrifice the quality of patient care. Smart card solutions consistently meet all security standards and can address the types of fraud that are perpetrated in the healthcare industry today. Smart card technology can provide security, interoperability, and strong authentication and exceeds the standards required to safeguard

medical records and payments. With the U.S. moving quickly to EMV chip technology for credit and debit card payments, the healthcare industry has the opportunity to leverage this new infrastructure to reduce fraud significantly and improve patient identity authentication.

The Smart Card Alliance recommends that healthcare organizations leverage proven smart card-based technology, including the proven EMV payments infrastructure. These standards-based solutions will contribute to a new paradigm of workflow automation for the healthcare industry that facilitates real-time payment authorization, increases patient health record security, improves patient identity management, and provides new auditing capabilities. While issues of ownership responsibility and implementation cost have, to date, stalled smart card technology adoption for identity authentication within the U.S. healthcare industry, EMV payment migration is expected to stimulate interest in smart card solutions. Payment terminals and systems are being converted to accept EMV-compliant chip cards. As this interoperable infrastructure expands, the costs associated with healthcare provider implementation and adoption of a smart card infrastructure decrease.

All organizations that upgrade to EMV will benefit from enhanced payments security and reduced fraud. The healthcare industry would experience maximum benefit if adoption is uniform and if the EMV chip infrastructure is leveraged for healthcare identity authentication as well. While certain standards may still need to be developed, uniform healthcare organization adoption of EMV and smart card technology-based identity authentication solutions will increase security, decrease payment vulnerability, reduce fraud and improve workflow for healthcare entities.

5 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Health and Human Services Council to outline a vision for healthcare identity authentication and payments convergence and to provide insight into the opportunities and challenges afforded to the healthcare community as the U.S. migrates to EMV.

Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank Health and Human Services Council members for their contributions. Participants involved in the development of this white paper included: ABnote; Ingenico; LifeMed ID Inc.; MasterCard; Verifone; Visa Inc.; and XTec, Inc.

The Smart Card Alliance thanks the Council members who participated in the project team to write the document, including:

- **David Batchelor**, LifeMed ID Inc.
- **John Ekers**, ABnote
- **Cathy Medich**, Smart Card Alliance
- **Morgan Richard**, XTec, Inc.
- **Bryan Russell**, XTec, Inc.
- **Mike Strock**, Smart Card Alliance

The Smart Card Alliance also thanks Council members who participated in the review of the white paper including:

- **Andreas Aabye**, Visa Inc.
- **Ramin Aghdaee**, MasterCard
- **Aron Clark**, Visa Inc.
- **Allen Friedman**, Ingenico
- **Simon Hurry**, Visa Inc.
- **JC Raynon**, Verifone

Trademark Notice

About the Health and Human Services Council

The Smart Card Alliance Health and Human Services Council brings together human services organizations, payers, healthcare providers, and technologists to promote the adoption of smart cards in U.S. health and human services organizations and within the national health IT infrastructure. The Health and Human Services Council provides a forum where all stakeholders can collaborate to educate the market on how smart cards can be used and to work on issues inhibiting the industry.