Maturity of Smart Card Chip Technology and Its Application to Web Security

Cathy Medich, Sree Swaminathan, Kelly Urban, Siva Narendra
Smart Card Alliance

1. Abstract

This position paper provides an overview of smart card secure element chip technology, the markets and applications that use smart card chip technology, the security provided by smart card technology, and the standards that are used to support smart card applications. Contrary to some beliefs, smart card silicon is a highly standardized piece of security hardware that is widely available in the market, and is already in use globally in payments, identity (e.g., e-passports, government employee ID) and access control applications. The scale and standardization of secure smart card technology bring the most obvious core security component that should be integrated into the next generation of unified web security standards.

2. Smart Card Chip Technology Overview

A smart card chip is an integrated circuit that includes an embedded secure microcontroller and supports the ISO/IEC 7816 standard for direct physical contact and/or the ISO/IEC 14443 standard for a remote contactless radio frequency interface. With a secure microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and mutual authentication) and interact intelligently with computers, mobile phones, and other readers. Smart card technology conforms to international standards and industry specifications also govern the use of smart card technology for various applications.

The term, "smart card," is something of misnomer. While the plastic card was the initial smart card form factor, smart card technology is now available in a wide variety of form factors, including plastic cards, key fobs, subscriber identification modules (SIMs) used in mobile phones, watches, electronic passports and USB-based tokens.

3. Smart Card Technology Market Scale

Smart card technology is used globally in applications and systems requiring smart secure devices. According to Eurosmart's annual market study on global smart card shipments, 7.7 billion smart cards are forecasted to ship globally in 2014.

Prominent applications for smart card technology that are currently deployed include:

- Identity applications including employee ID badges for physical access to buildings and secure computer and network access; citizen ID documents; electronic passports; driver's licenses; and online authentication devices. Today, smart card technology is used by all U.S. federal employees and contractors with Personal Identity Verification (PIV) credentials to secure access to government systems and buildings; in U.S. citizens' passports to secure identity information; and in federal programs like the Transportation Security Administration (TSA) Transportation Worker Identification Credential (TWIC) and the Department of Defense Common Access Card (CAC).
- Healthcare applications including citizen health ID cards; health provider ID cards; and portable medical records cards. Smart card technology is now being recommended in legislation to create a pilot for a proposed Medicare Common Access Card (H.R. 3024).

- Mobile applications including billions of mobile phone subscriber identity modules (SIMs) in use today, plus in Near Field Communication (NFC)-enabled phones to secure mobile payments.
- Transit fare payment applications, with virtually all major transit fare payment systems using contactless smart cards as the primary ticket medium.
- Global payment standard EMV chip cards, now used in more than 80 countries worldwide with 2.3 billion EMV chip cards issued to date.

4. Smart Card Technology/Application Standards and Specifications

To support global interoperability requirements, smart card technology uses proven global standards, and applications using smart card technology are based on both global standards and industry-specific specifications. Key standards and specifications include the following:

- ISO/IEC 7816 – Identification Cards – Integrated Circuit Cards defines the various aspects of the card and its interfaces, including the card's physical dimensions, the electrical interface, the communications protocols, the data elements and commands.
- ISO/IEC 14443 - Identification Cards - Contactless Integrated Circuit(s) Cards - Proximity Cards defines the interfaces to a "proximity" contactless smart card, including the radio frequency (RF) interface, the electrical interface, and the communications and anti-collision protocols.
- ISO/IEC 18092 - Information technology - Telecommunications and Information Exchange between Systems - Near Field Communication - Interface and Protocol defines communication modes for the NFC interface and protocol (NFCIP-1) using inductive coupled devices operating at the center frequency of 13.56 MHz for interconnection of computer peripherals.
- The Personal Computer/Smart Card (PC/SC) specification allows smart card readers to be integrated easily with middleware or other applications, regardless of manufacturer or command set. Although this standard was developed for use in a Microsoft environment, it is now considered the de facto standard for many other platforms as well.
- The Advanced Security Secure Digital (ASSD) standards defined by the SD Association enable memory card devices to support ISO/IEC 7816 functions. The smartSD standards defined by the SD Association enable memory card devices to support ISO/IEC 14443 functions.
- The Chip Card Interface Device (CCID) specification was developed for Universal Serial Bus (USB) smart card readers. The specification was defined by the USB Implementer's Forum (USB-IF) in conjunction with the smart card industry. CCID defines a command set and transport protocol over the USB so that a host system can communicate with a smart card reader. A specific USB class is now defined for smart card readers.
- GlobalPlatform specifications are used to enable an open and interoperable infrastructure for smart cards, devices and systems.
- Java Card provides a smart card operating system for running multiple applications.

Since smart card technology provides a general purpose computing platform, applications can use a wide range of standards and specifications that are appropriate to their specific functions. Examples include:

- "Federal Information Processing Standard (FIPS) 201 Personal Identity Verification (PIV) of Federal Employees and Contractors," which uses symmetric and public key cryptography depending on use.

- Global EMV chip card payment specifications, managed by EMVCo, which use both Triple DES (TDES) symmetric key technology and public key cryptography to support different security functions.

5. Smart Card Chip Technology Security

The most comprehensive chip security is multi-dimensional. No single security mechanism protects completely against the broad spectrum of possible attacks. Therefore, the design of a secure chip and its use in a system must incorporate hardware, software, and system countermeasures to protect data and transactions.

Security should be an integral part of every smart card solution deployed. It is important to consider the security strength of the chip platform selected for any smart card application. Overall system security would also be enhanced by other measures implemented at the system level.

Secure smart card microcontrollers are commercially available that are designed to function in hostile environments. These chips are fortified with mechanisms that are designed to withstand attempts to extract the confidential data the chip is protecting.

5.1 Secure Microcontroller Architecture

To defend against attacks, a secure chip should have an architecture that allows the chip to withstand all known attack types. Each chip manufacturer incorporates its own features and security modules into its chip architecture. The manufacturer may utilize its own nomenclature for the modules, but the modules perform similarly or identically while providing varying levels of protection.

Independent third party test laboratories can verify that each specific secure chip platform adequately protects itself from known/defined threats. Many chip manufacturers use feedback from these third party labs to improve and invent new countermeasures that they would never willingly share with their competition. Therefore, it is better to specify which threats the chip must be capable of resisting (and to what degree) than to specify the countermeasure.

Figure 1 is a block diagram of the components of a typical secure smart card microcontroller.

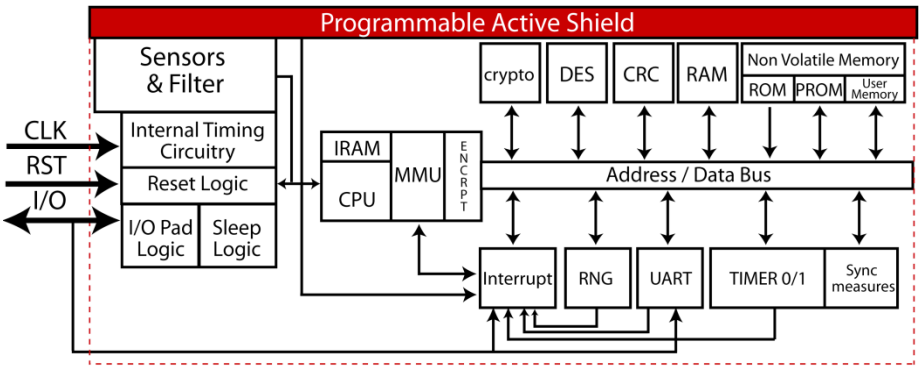

Figure 1. Components of a Typical Secure Smart Card Microcontroller

6. Industry Certifications and Evaluations

The government and financial payments industries have led the way in establishing security evaluation and certification programs for the various layers of smart card security. This section describes two security evaluations that are used by the industry.

These standardized evaluations and certifications use a very few trusted third party labs to empirically verify that specific threats (that are state-of-the-art at the time) are prevented to a defined level of effectiveness. Measures of effectiveness encompassed in these standards include expertise, time, and cost of equipment required to achieve the specific attack. Equally important to the verification function, such standardized evaluations and certifications provide a framework to publish results of testing without disclosing details of the countermeasures that are used and verified. The resulting confidentiality allows smart cards to have their most effective security countermeasures tested without attackers knowing specifically what these countermeasures are. Best of all, those applying or specifying smart cards need not consider the specific hardware countermeasures (such as those described in this paper), but need only require that their card meet the required level of certification. Smart cards are also subject to rigorous functional and interoperability testing, which is outside the scope of this position paper.

6.1 ISO/IEC 15408 – Common Criteria

Common Criteria (CC) is an internationally approved security evaluation framework providing a clear and reliable evaluation of the security capabilities of IT products, including secure chips, smart card operating systems, and application software. CC provides an independent assessment of a product's ability to meet security standards, with the goal of giving customers confidence in the security of IT products and leading to better decisions about security. Security-conscious customers, such as national governments, are increasingly requiring CC certification in making purchasing decisions. Since the requirements for certification are clearly established, vendors can target very specific security needs while providing broad product offerings.

CC has been adopted and is recognized by 14 countries, which allows customers in any of these countries to purchase products with the same level of confidence. Evaluating a product with respect to security requires identification of the customer's security needs and an assessment of the capabilities of the product. CC helps customers complete both of these processes using two key tools: protection profiles and evaluation assurance levels.

6.1.1 Protection Profiles

A protection profile defines a standard set of security requirements for a specific type of product. Protection profiles are the basis for the CC evaluation. By listing required security features for specific product families, CC enables products to achieve conformity to a relevant protection profile. During CC evaluation, each product is tested against a specific protection profile, providing reliable verification of the security capabilities of the product. For smart cards, the protection profile covers secure chips, smart card operating systems, and application software. These components can be evaluated as separate entities or combined into a secure smart card. More than 25 protection profiles for secure chips, smart card operating systems, application software, and other smart card related devices and systems are listed on the CC portal.

6.1.2 Evaluation Assurance Levels

An evaluation assurance level (EAL) measures the depth of engineering review and evaluation of the product lifecycle. Unlike a protection profile, the EAL does not indicate the actual security capabilities of the product but independently stipulates the level of evidence reviewed and tested against the vendor's

claims. Figure 2 shows the seven CC EALs (EAL1–EAL7) and the level of testing required to achieve the different levels. Vendors can choose an EAL.

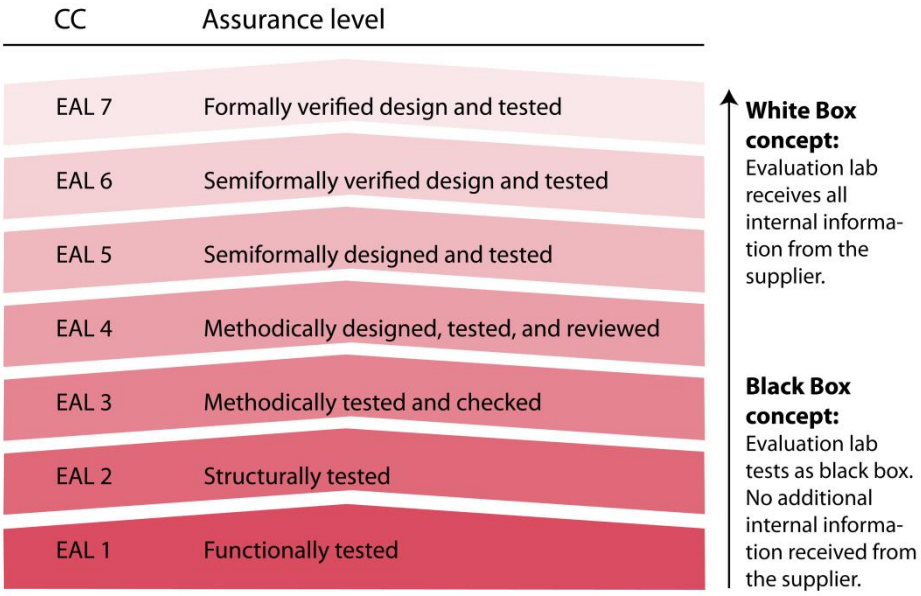

Figure 2. Common Criteria Evaluation Assurance Levels

6.2 FIPS 140 for Cryptographic Modules

"FIPS 140 Security Requirements for Cryptographic Modules" is the U.S. government security standard for cryptographic modules. It applies to the entire smart card, including the secure chip, the operating system, and the application software. This standard is the benchmark for implementing cryptographic software and hardware and specifies best practices for implementing cryptographic algorithms, handling key material and data buffers, and securely working with the operating system. In the late 1990s, smart card manufacturers began submitting smart cards for FIPS 140-1 certification. In 2001, FIPS 140-1 was replaced by FIPS 140-2, and FIPS 140-3 will soon replace FIPS 140-2.

FIPS 140 specifies the requirements for cryptographic modules in the areas of secure design and implementation, including module specification, ports and interfaces, roles, services, and authentication, finite state model, physical security, operational environment, cryptographic key management, electromagnetic interference/electromagnetic compatibility (EMI/EMC), self-tests, design assurance, and mitigation of other attacks.

7. Web Security and Smart Card Chip Technology

The maturity of smart card chip technology – from market size and breadth, standards, and certification – implies that billions of dollars have been already been spent enabling this hardware-based security infrastructure. Several solutions are already available in the market that integrate smart card-based solutions to web browsers including solutions from companies that have submitted position papers.

Applications enabled by such solutions include strong authentication, including mutually authenticated Transport Layer Security (TLS) connection, digital signatures, data encryption including data-at-rest/virtual private network (VPN)/Voice over Internet Protocol (VoIP), key protection, remote provisioning, and WebRTC (Web Real-Time Communication).

Existing hardware token standards and specifications such as ASSD, smartSD, PC/SC, Global Platform, Java Card, and CCID already support smart card chip technology. New hardware token specifications such as the Fast IDentity Online (FIDO) Alliance Universal 2nd Factor (U2F) specification could likely use smart card technology as its core for security. We recommend that W3C consider supporting a wide array of possible smart card-based technologies, rather than supporting one particular standard.

We recommend that the Web Crypto API working group collaborate with smart-card-centric companies to define how to standardize access to existing and new hardware tokens that use smart card chip technology as the core security component. The Smart Card Alliance can assist in facilitating this collaboration.

8. 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.

9. Contact Information

Cathy Medich, cmedich@smartcardalliance.org
Sree Swaminathan, sridher.swaminathan@firstdata.com
Kelly Urban, kelly.urban@firstdata.com
Siva Narendra, siva@tyfone.com