Mobile Devices and Identity Applications

A Smart Card Alliance Identity Council Publication

Publication Date: September 2012
Publication Number: IC-12002

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 use of mobile devices for secure identity applications is an emerging market that leverages the functionality and security built into mobile devices. This white paper was developed by the Smart Card Alliance Identity Council to describe the secure use of mobile devices for identity applications. The white paper describes the global trend toward using digital identity credentials and the role that smart card technology plays in securing those credentials and protecting digital identity transactions. The white paper concludes with descriptions of different scenarios illustrating how mobile devices can be used for identity authentication.

2 Mobile Devices and Identity

2.1 Mobile Device Trends

Mobile devices impact people's lives every day. The mobile phone has evolved into a powerful, location-aware mobile computer that can not only make calls but also send text messages, e-mail messages, and access the Internet and media. Incorporated image sensors can take pictures and capture video. The phone can act as a mobile entertainment center that is able to play music, videos, and games. For many individuals, the phone has become the default device with which to search the Internet, access mobile banking services, make reservations, send and receive text messages, provide social network updates, and more. With more than 100 million smartphones currently shipping every quarter, it can be argued that mobile devices are the most influential technology and business driver in the world today.

These dramatic changes are due in part to advances in low power computing and embedded operating systems, application (apps) development support, and cloud-based services (for laptops, tablets, and mobile phones) that leverage always-on connectivity and the capabilities of smart mobile devices. Both platform providers and developers have made significant investments in mobile application development platforms. App development has also been enabled by continued investment in and upgrade of the telecommunication and other communications networks. Consumer demand and the easy distribution and promotion of mobile device applications in online application stores (such as Apple's iPhone App Store and Google Play) are further reasons for the explosive growth.

Smart card technology is present in almost all mobile devices, in the form of a subscriber identity module (SIM) or other secure element form factor,[1] such as a smart secure digital card (e.g., microSD). This technology is essential to ensuring the security of the many different interactions and transactions performed using the phone. Most importantly, however, smart card technology in the mobile device can also be used to protect consumer privacy in a convenient, cost-effective, and easy-to-use way.

2.2 Digital Identity Trends

In addition to advances in technology, the tragedy of 9/11 contributed to broad adoption of secure smart card technology in passports and identity cards. Smart card technology can help prevent identity theft and assist countries in verifying citizen and non-citizen identities.

The first wave of electronic passport implementation in 2005–2008 illustrated the advantages of integrating a smart card chip into government documents. More than 96 countries have implemented electronic passports, and the third generation of the electronic passport is currently being defined.

Digital identity technology is also being used in national identification cards, healthcare cards, enterprise and government employee credentials, and electronic driver's licenses, where it delivers the following benefits:

- Provides better, faster, more efficient access to e-services
- Safeguards privacy and prevents fraud by using secure technologies to protect personal data
- Improves mobility by implementing widely accepted and interoperable identity credentials
- Enables a wide range of use cases across logical and physical domains, including use for authentication, digital signatures, and encryption
- Establishes trust for the issuer as well as the credential holder

At present, it is common for individuals to carry multiple ID cards, such as a driver's license, healthcare card, and employer or student identification card. The construction, data models, and designs of identity cards vary, from plain plastic "flash pass" cards to microprocessor-based smart cards with robust on-card computing capabilities. However, more and more governments, organizations, and individuals are adopting identity credentials that incorporate smart card technology.

[1] Form factors include: microSD secure element; embedded secure element; removable Universal Integrated Circuit Card (UICC) secure element.

2.3 The Mobile Device–Digital Identity Intersection

The identification credentials that people currently carry can be securely integrated into mobile devices in a variety of digital formats. Depending on the application, mobile devices can store a variety of credentials:

- Very simple software tokens
- One-time passwords
- Personal identification numbers (PINs) and passwords
- Public key infrastructure (PKI) certificates
- Biometric data
- Security Assertion Markup Language (SAML) tokens
- Java Web tokens, which are used by evolving standards such as OAuth and OpenID Connect

These credentials can be used to enable a wide range of functions and services from anywhere and at any time:

- Benefits and entitlements (e.g., healthcare services)
- Access to physical resources (e.g., building entry)
- Access to logical resources (e.g., network logon)
- Electronic signatures for online transactions
- Loyalty applications
- Access to other computing terminals (e.g., laptop logon)
- Protection of data on the device (e.g., data encryption)
- Protection of work domains (e.g., bring-your-own-device (BYOD) scenarios where work applications are protected by work-related credentials)
- Access to cloud services and applications
- Financial services such as electronic banking, mobile payments, and online payments

2.4 Mobile Devices as Identity Platforms

Mobile devices make an ideal platform for carrying identity credentials and using them to authenticate the device holder. For one thing, it is more convenient for people to carry a single mobile device than numerous plastic ID cards. A number of companies have recently promoted mobile device-based wallets, and the use of near field communication (NFC) technology enables consumers to make payments and complete other transactions using these wallets. The presence of an electronic ID credential on a mobile device can also allow the device holder to access secure Web services (potentially in addition to a username and password or other authentication information). A digital identity credential in a phone could be used to both access a building and digitally sign e-mail messages being sent from the phone.

Further, the processing and memory capabilities of a smartphone can provide extended capabilities. A number of mobile device features can enhance or extend the functionality of identity credentials. For example, key codes delivered through simple text messages can be used for further authentication, or location-based services can add more security to the transaction by confirming the location of the person.

2.5 Mobile Devices and the Role of Smart Card Technology

The SIM or universal integrated circuit card (UICC) in a mobile device is a smart card that provides a high level of security for mobile communications. Its use in a mobile device to carry identity credentials can both protect the credentials and enhance the security of an identity authentication transaction. In most mobile networks, the SIM and UICC perform the following functions:

- Store subscriber identity data securely
- Store mobile operator data securely
- Store subscriber phone books securely
- Authenticate subscribers to the mobile network
- Encrypt information communicated over the mobile network
- Support conditional access systems and digital rights management that enable mobile operators to deliver content to consumers securely

According to Eurosmart, over 5.2 billion smart cards will be shipped in 2012 for telecommunications applications.[2]

Mobile devices also employ smart card technology in the secure element (SE). The SE is a secure microprocessor that includes a cryptographic processor to facilitate transaction authentication and security, and provide secure memory for storing applications and data. SEs are used to support any secure transaction, such as payment, transit ticketing, building access, or secure identification. The UICC can include the SE or the SE can be a separate chip that is embedded in the mobile phone, in a removable microSD card, or in a different mobile phone accessory.

User ID credentials should be stored in the SE, to guarantee that they are protected against attacks and to achieve the highest level of security for user credentials. Such attacks can include:

- Internal attacks from malicious software running on the device
- External attacks over a network or other external interface
- Brute force attacks (people trying to physically extract the information stored in specific hardware)

In leveraging the secure element in a mobile device for identity authentication, mobile device users can supply additional authentication factors, including:

- A PIN or password
- Biometric data (fingerprints, facial images, gesture recognition, voice recognition)

Recent events and data compromises have shown that software security measures have not been sufficient to ensure the security and privacy of data and transactions. A hardware solution (e.g., using a smart card) is one way to address these security issues. Hardware and software security should be complemented by thorough security policies and processes.

The smart card industry has significant experience in implementing hardware-based security, with multiple solutions available that meet industry standards for security implementations (e.g., FIPS 140, Common Criteria). Smart card industry standards and solutions are being used to achieve the highest level of security in mobile form factors. The existing rigorous certification processes can validate the ability of the credential container (i.e., the secure element) to address a series of identified threats and attacks.

[2] http://www.eurosmart.com/

3 Mobile Identity Use Cases

To illustrate how mobile devices can be used to support identity-related transactions, this section presents several use cases that present different approaches for storing and using identity credentials on mobile devices.

Many approaches can be used to secure the identity transaction; these use cases are presented as illustrative examples and are not intended to include all possible approaches. It is also important to note that the use cases are intended to present a vision for how mobile devices may be used for identity authentication; not all mobile devices can support the capabilities described in these use cases at this time. The use cases presented include:

- Mobile-assisted authentication for employees: using the mobile device to receive, store and present identity credentials for logical access or using the mobile device as a reader with existing contactless employee ID credentials to enable secure logical access
- Identity credential validation in the field using NFC-enabled devices as readers
- Authentication with an NFC-enabled laptop
- NFC-enabled physical access control

3.1 Mobile Assisted Authentication

Both small and large companies deal with the challenge of issuing and maintaining employee identity credentials for physical access to company facilities. In addition, some companies use these same identity credentials for logical access and web-based authentication. Companies incur significant costs to maintain the infrastructure that supports employee identity credentials and to equip facilities, computers and employees with the readers that enable their use.

Mobile devices represent both a better way for companies to manage physical access and a cost-effective and convenient way for employees to access company information (network or enterprise access).

The use cases in this section illustrate three different approaches for using mobile devices to authenticate an employee to a network:

1. Using the mobile device as an “out-of-band” solution to determine whether an employee is the “right” employee.
2. Leveraging the NFC capabilities of a mobile device to read and transmit the details of a company ID credential
3. Using the mobile device as the ID credential, leveraging the SE to securely store credentials and authenticate the employee.

3.1.1 Using the Phone as an Out-of-Band Authentication Device

Using the phone as an out-of-band authentication device requires that an employee’s mobile phone be provisioned with an application that, when requested, either produces a one-time password (OTP) or prompts the person for confirmation. In addition, the phone must be correlated with the person’s identity. Once a preregistered user ID–password combination is entered, the phone can be used as an additional factor to authenticate the employee.

For example, when an employee tries to gain access to the company network, the network initiates a dialogue with the phone. The application on the phone is activated either through a short message service (SMS) message or an Internet-based request or push. The phone then displays a company Web site or prompt (Figure 1) and asks the employee to confirm the access attempt. The accepted or rejected response from the employee determines whether access is granted. Alternatively, the phone may display an OTP, which the employee enters on the Web site to gain access to the network.

Figure 1. Mobile Device as an Out-of-Band Authentication Solution

This approach can have several benefits. Using the phone as an out-of-band authentication device provides an additional authentication factor (something you have) and also protects against certain forms of attack—specifically phishing attacks to capture identity credentials for fraudulent use. To achieve access, someone must now intercept the user ID–password combination as well as the OTP from the mobile device. In addition, since virtually all phones are capable of supporting OTP applications, this solution is the most generally available to organizations and is relatively easy to use.

3.1.2 Leveraging NFC and the Employee ID Badge

The emergence in the market of NFC-enabled mobile devices creates opportunities to further improve security and authentication for remote applications. An employee with an NFC-enabled phone may be able to tap a contactless smart ID credential against the phone and use the information on the card to confirm the employee's identity.

In this use case example, the phone would be associated with the person's employee ID. Once a preregistered user ID–password combination is entered, the phone could be used to capture data from the contactless smart ID card.

Also in this use case, the company Web site initiates a dialogue with the phone. The application on the phone is activated either through an SMS message or an Internet-based request or push. The phone would then display the company Web site and prompt the employee to tap the company-issued ID card against the phone (Figure 2).

The data from the ID card would be securely transferred through the phone to the issuer of the card, where it is validated. Assuming that the card is valid and matches the user ID–password information provided earlier, the employee would be granted access to the Web site or network.

It is important to note that the application on the phone would store the appropriate permissions, or keys, to access the card details. If the card is a smart card, the data generated is dynamic, and only the company can correlate the data to a specific employee.

Figure 2. NFC-Enabled Mobile Device and the Employee Badge

This approach would have several benefits. In addition to protecting against phishing (as described in the previous section), leveraging the card and the NFC capabilities of the phone could avoid man-in-the-middle and man-in-the-browser attacks, assuming that the data from the card is sent directly to the card issuer for validation and not sent first through the browser. In essence, the card and phone act as two "what you have" factors for authentication.

As NFC-enabled phones penetrate the market, this authentication method may become a popular initial authentication method, as there would be no need for card issuers to provision phones with employee identity credentials (i.e., in an SE or on a SIM). That said, the penetration of NFC-enabled phones in the market is still very small and the phone must be able to be configured as an NFC-enabled reader to implement this use case.

3.1.3 Using an Identity Credential Stored in the Mobile Phone's Secure Element

A company-issued credential can also be stored in the SE of a phone. Storage of the credential in the SE requires the company to work with the SE owner (for example, the phone manufacturer or mobile network operator) to pay for memory space on the SE and provision the credential to the chip. In addition, the phone is associated with the employee ID. Once the employee uses preregistered logon credentials, the company can communicate with the credential on the phone.

In this use case, when an employee tries to gain access to the company network, the network initiates a dialogue with the phone. The application on the phone is activated either through an SMS message or an Internet-based request or push. The phone then displays a company Web site (Figure 3) and prompts the employee to confirm the access attempt. The company can also collect another password.

The ID credential stored on the SE is securely transferred to the issuer of the card, where it is validated. Assuming that the credential is valid and matches the user ID–password information provided earlier, the employee would be granted access to the network.

As described in the previous section, leveraging the dynamic data generated from an out-of-band device significantly reduces the risk of several forms of malicious attack. The added benefit of this approach is that it is easier to use than an approach requiring the employee to tap a card on the phone. To the employee, it is a relatively convenient process, similar to the process described in Section 3.1.1, but with the security enhancements offered by smart card technology.

Figure 3. Identity Authentication Using the Secure Element

3.2 PIV on a Phone

In 2004, Homeland Security Presidential Directive 12 (HSPD-12) mandated a standard for a secure and reliable form of identification to be used by all Federal employees and contractors. This eventually led to the PIV (Personal Identity Verification) program.[3] The goals of this program are to improve the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems and to create the infrastructure necessary to deploy and support an identity credential that can be used and trusted across all Federal agencies for physical and logical access. Currently, government agencies and commercial enterprises are issuing PIV or PIV-interoperable credentials and cards.

Mobile devices provide an opportunity to complement the PIV card or the PIV reader or both. The Federal government is currently defining its policy and strategy for using PIV credentials with mobile phones. It is anticipated that FIPS 201-2 will recognize mobile devices as an additional computing environment for accessing PIV-enabled applications, with a new NIST Special Publication (SP 800-157) to be developed to define how PIV credentials will be used with mobile devices.[4]

3.3 Card Validation in the Field

NFC-enabled phones can provide additional opportunities for in-person security and authentication of people carrying contactless ID cards. One possible solution is for security personnel (for example, security guards or first responders) to confirm a person's identity by having that person tap an ID card against the guard's NFC-enabled phone. The security guard would start an application on the phone, which prompts for a card to be tapped. The data on the card would be communicated to the phone using NFC and then transferred to the SE. The ID credential would then be securely transferred to the issuer of the card, where it is validated. Assuming the card is valid, the phone would display a digital image and other relevant information to the security guard (Figure 4) to assist in confirming the person's identity.

---

[3] Additional information on the PIV program can be found on the Smart Card Alliance web site at http://www.smartcardalliance.org/pages/publications-government-id-resources.

[4] "Updates on the Personal Identity Verification Standards," Hildegard Ferraiolo, NIST, presentation, Interagency Advisory Board (IAB) Meeting, May 23, 2012, http://www.fips201.com/resources/audio/iab_0512/iab_052312_ferraiolo.pdf

Figure 4. NFC-Enabled Mobile Phone Used as a Reader

One requirement critical to this solution is that the application on the phone must have access to the appropriate permissions, or keys, to access the details on the card. Smart card and smart card-reading solutions are based on the theory that the phone has the correct keys to open the secure identity verification application. Also, the data generated is dynamic, and only the correct issuer's systems can interpret and correlate this data to a specific user.

Leveraging the reading capabilities of NFC-enabled phones can offer a few key benefits to organizations and individuals. First, the number of cards used fraudulently in the market can be greatly reduced. Instead of relying on the image on a card, security guards would be able to access a digital image of the cardholder and electronically verify an individual's identity.

Second, phones can represent a low cost and convenient terminal for deployment to security guards or first responders. Traditionally, hardware costs have been the impediment to reading cards in the field. Now, card-reading capability can exist in a low-cost, mobile communication device.

This concept may be applicable to other use cases, with the benefit of immediate information exchange when (for example) a health card is tapped on a doctor's NFC phone in a hospital or a driver's license is tapped on a police officer's phone (or on a bar owner's phone to verify the cardholder's age without providing any other personal information).

3.4 Authentication with a Contactless Smart ID Card or NFC-Enabled Mobile Device and NFC-Capable Laptop

The ability to use smart cards for authenticating identity in remote transactions is not limited to mobile devices. In January 2012, Intel announced plans to embed contactless card-reading capabilities in the Ultrabook product suite, with other product lines to follow. The implication is that soon all communication devices—phones, tablets, laptops—will be able to read contactless smart ID cards or NFC-enabled mobile devices and use the credentials from the card or the mobile device to authenticate users for access to online services and transactions.

Strong online authentication not only benefits consumers but has tremendous benefit for e-commerce merchants, online banking providers, and governments at the federal, state, and local level. In addition, employees would be able to tap their badges directly on their laptops to access their enterprise network.

In the case of the Intel laptop, when the laptop recognizes that there is an authentication requirement for access to a particular Web site, the Intel Protection Technology (IPT) platform prompts the user to tap the

appropriate contactless smart card or NFC-enabled mobile device on the appropriate location on the laptop. The data is read through the NFC capabilities built into the laptop (Figure 5) and transferred to the Manageability Engine (ME) on the computer motherboard, where it is encrypted. The ME is a controlled area of the chip set; it is tamper-proof and operates in isolation from the operating system for added security. The encrypted data is then sent to the issuer of the card, where it is decrypted and read. Assuming the identity credentials from the card or mobile device are valid, the user would be granted access to the network.

Figure 5. NFC-Enabled Laptop and Contactless Smart Card

3.5 Physical Access Control in an NFC-Enabled World

The most simplistic mobile access control model is to replicate existing card-based physical access control principles using smartphones with NFC technology. The smartphone would be equipped with a digital key which, when presented to a reader, passes the identity information to an access control system. Based on a pre-defined set of access rights, the access control system would make the decision to unlock the door (Figure 6).

NFC-enabled mobile access control has some basic requirements, including the following:

- First, NFC-enabled handsets are required. This can be achieved via handsets with an embedded secure element, a SIM or UICC-based secure element, or an add-on device (such as a microSD card) that incorporates a secure element.
- Second, there must be an ecosystem of devices (i.e., readers, locks, and other hardware) that can read and respond to the digital keys stored in NFC-enabled handsets.
- Third, there must be a way to manage digital keys. All identity provisioning/de-provisioning and sharing must occur within a trusted boundary, to ensure a secure channel for communicating identity data objects between validated endpoints so that all transactions between phones, readers and locks can be trusted. A common access control trusted service manager (TSM) would interface seamlessly to the mobile network operator (MNO), its TSM, and the NFC smartphones that will receive the encrypted keys for storage in the secure element, the SIM, or the microSD. Provisioning and de-provisioning would be executed over-the-air via a managed services portal, much like today's plastic cards, with one-time or batch uploads and drop-and-drag simplicity.

Figure 6. NFC Phone and Physical Access Control

It is believed that NFC-enabled mobile access will be used in three primary environments: residential, hospitality (hotels), and commercial. With the NFC ecosystem in place, a home's family members will be able to receive digital house keys over-the-air to their smartphones. When the homeowner wants to give a repair person temporary access, it will be possible to send a temporary key and then revoke it when the project is finished. Similarly, business travelers will be able to receive hotel room keys on their smartphones that enable them to bypass the front desk when checking in. In a commercial application such as a hospital, users will be able to receive digital keys on their smartphones that are configured to operate with all of the access control infrastructure's various readers and locks and to support a variety of security levels and associated access rules.

Moving beyond the simple card emulation model described thus far, the mobile access control model can also leverage the smartphone's on-board intelligence to perform most of the tasks that are currently performed by the access control system. Instead of having a wired physical access control system, a mobile device with its wireless connection could be both the key and the processor. Instead of a reader going to a panel and a panel going to a computer, the phone can become the rules engine to make the access control decision.

In a mobile-enabled physical access control use case, when an employee goes to a door, several things can happen. The phone can confirm the location, make sure the employee has the proper authorization to access the area, and ensure that they are allowed access at that specific time. All of this data can be checked against data stored in the cloud; the handset can then send an encrypted signal to the door for it to open. Physical access control systems would no longer need to be hardwired allowing electronic access control to be used on interior doors, filing cabinets, and storage units where it previously would have been cost-prohibitive to install a traditional wired access control infrastructure.

4 Conclusions

Mobile devices are a critical element in most people's lives, not only providing a communications platform but also supporting an ever-increasing array of applications. The use of mobile devices as a platform for secure transactions—payment, identity authentication, ticketing, access control, and many others—is an emerging market globally. The convergence of the move to digital identity credentials stored on smart ID cards with the new technologies being built into mobile devices offers opportunities for individuals to use a mobile device to authenticate identity in a wide variety of ways:

- Generating and receiving one-time passwords to log on to secure sites or access secure services.
- Storing digital identity credentials on a mobile device's secure element and using them to log on, digitally sign, and encrypt documents.
- Storing digital identity credentials on the secure element in an NFC-enabled mobile device and using the credentials for physical access or secure logon.
- Using an NFC-enabled mobile device as a low cost reader, to read identity credentials presented with a contactless smart ID card securely.

While identity authentication is a new use for mobile devices, identity applications can leverage smart card technology and the standards developed for mobile and payment applications to ensure security, and to enable innovative approaches for identity authentication.

5 Publication Acknowledgements

This document was developed by the Smart Card Alliance Identity Council to present the vision of the secure use of mobile devices for identity applications and to describe different use cases for current and NFC-enabled mobile devices.

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 thanks the Council members for their contributions. Participants involved in the development of this document included: Accenture LLP; Booz Allen Hamilton; Consult Hyperion; Deloitte & Touche LLP; Gemalto; HID Global Corporation; Hirsch-Identive; HP Enterprise Services; Identification Technology Partners; Identive; IDmachines; INSIDE Secure; Intellisoft; NXP Semiconductors; SecureKey Technologies; XTec, Incorporated.

The Smart Card Alliance thanks the following Council members who wrote content and participated in the project team for this document:

- **Stefan Barbu**, NXP Semiconductors
- **Sal D'Agostino**, IDmachines
- **Frazier Evans**, Booz Allen Hamilton
- **Chris Gardner**, SecureKey Technologies
- **Walter Hamilton**, ID Technology Partners
- **Harold Kocken**, Deloitte & Touche LLP
- **Deb Spitler**, HID Global
- **Brian Stein**, Accenture LLP
- **Lars Suneborn**, Hirsch-Identive
- **Abel Sussman**, Booz Allen Hamilton
- **Mike Zercher**, NXP Semiconductors

Identity Council members who participated in the review of the white paper included:

- **Brent Bowen**, INSIDE Secure
- **Kevin Doty**, HP Enterprise Services
- **Margaret Ford**, Consult Hyperion
- **Philip Hoyer**, HID Global
- **Imran Khan**, HP Enterprise Services
- **Neville Pattinson**, Gemalto
- **Rick Pratt**, XTec, Incorporated
- **Steve Rogers**, Intellisoft
- **Dan Schleifer**, IDmachines
- **Joe Tassone**, Identive

The Smart Card Alliance thanks **SecureKey** and **HID Global** for providing graphics that were used in developing the Section 3 figures.

About the Smart Card Alliance Identity Council

The Identity Council is focused on promoting best policies and practices concerning person and machine identity, including strong authentication and the appropriate authorization across different use cases. Through its activities the Council encourages the use of digital identities that provide strong authentication across assurance environments through smart credentials – e.g., smart ID cards, mobile devices, enhanced driver's licenses, and other tokens. The Council furthermore encourages the use of smart credentials, secure network protocols and cryptographic standards in support of digital identities and strong authentication on the Internet.

The Council addresses the challenges of securing identity and develops guidance for organizations so that they can realize the benefits that secure identity delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to bear on addressing the challenges of securing identity information for proper use.

Additional information on the use of smart card technology for identity applications can be found on the Smart Card Alliance web site at http://www.smartcardalliance.org.