

Secure Access Control with Government Contactless Cards

David Engberg
CoreStreet, Ltd.
One Alewife Center, Suite 200
Cambridge, MA
dengberg@corestreet.com

Abstract—Government agencies have begun widespread usage of public key technology for information security applications such as secure email, document signing, and secure login. These deployments use PKI tokens in the form of contact smart cards with private keys protected through a match-on-card second factor such as a PIN. More recently, the government has begun to standardize card technology for contactless physical access. These contactless cards will be capable of symmetric key usage, but will not be able to perform private key operations. They will also typically be limited to 1-4kB of read/write data storage.

This paper discusses ways to use digitally signed messages to perform strong authentication and authorization using the current generation of contactless smart cards. This will compare different strategies under consideration and discuss the security and usability considerations of each. Particular emphasis is placed on techniques to support the use of these cards in inter-agency and offline settings.

Keywords—*contactless, smart cards, biometrics, access control*

1 OVERVIEW

There are two questions that must be answered by an access control system before permitting access. The first question is: “*Who are you?*” The answer to this question is your **identity**, which is permanent throughout your life. The process of answering this question, **authentication**, must rely on one or more factors to uniquely determine your identity. These factors are typically divided into three categories:

Something you have: E.g. a badge, a metal key or a smart card

Something you know: E.g. a PIN or a password

Something you are: E.g. your fingerprint, your iris or your voice

An access control system authenticates these factors to identify each user. Since your identity never changes, the process of authentication should always yield the same result, even if the factors used may change.

Once your identity is determined, the system must answer a second question: “*Are you currently allowed to access this resource?*” This question is answered through a process called **authorization** or **validation**. Unlike authentication, which should always yield the same identity for each person, the result of authorization may change frequently. This change may be the result of a change in user privileges (e.g. a promotion), a change in policies, or a change in the environment (e.g. time of day, etc.).

This document describes techniques and technologies that can be used to perform secure access control using the current generation of government contactless cards. This focuses on solutions that will support cards based on ISO 14443 Parts 1-4 [ISO01], such as those using Philips’ DESFire chips. These cards comply with NIST’s Government Smart Card Interoperability Specification (GSC-IS) version 2.1, Appendix G [SDW+03]. The general techniques described in this document should also be applicable to other contactless memory cards, including those with other symmetric key schemes (e.g. HID’s iClass).

The techniques described in this document are primarily compared in their ability to permit strong authentication and authorization within federated environments where a single central access control system is not possible. This support for federated access control also leads to the ability to perform authentication and authorization in disconnected settings where no communication is available to central management servers.

2 SECURE CONTACTLESS AUTHENTICATION

The process of authentication uses one or more factors to securely determine the identity of a cardholder. These factors may be fully independent (printed photo, contactless card serial number), or may be interconnected (e.g. contact chip PIN and PKI applet). An effective authentication factor will uniquely and unambiguously identify a specific individual, binding to their universal identifiers. Different authentication factors also vary in their level of protection against modification or duplication. Finally, some factors that may be appropriate in a closed environment with guaranteed network

connectivity may not be usable in federated or disconnected settings.

The following sections describe various factors that may be used with contactless DESFire cards to perform authentication.

2.1 *DESFire card unique identifier (CUID)*

Every DESFire card is manufactured with a unique and read-only card unique identifier (CUID), which is made up of a one byte manufacturer code (e.g. Philips: 0x04) and a six byte card number that is set by the manufacturer. Barring a manufacturing error, no two legitimate DESFire cards should have the same CUID.

The card CUID can be retrieved by any ISO 14443 reader within range of the card. This CUID is read in clear text form during the card selection and anti-collision processing, which precedes any other card actions.

Pro: The serial number is unique and unambiguous. The UID of a legitimate card cannot be modified.

Con: The serial number has no cryptographic or protocol-level protections to prevent an attacker from asserting the same serial number as any real card. By implementing ISO 14443 directly, an attacker can imitate any desired CUID.

The CUID only represents a basic assurance factor for authentication.

2.2 *Stored identification string*

In addition to the manufacturer's CUID, it is possible to write a more extended identification string into the card memory that represents the cardholder. Example encodings would include a SEIWG-012 string [SEIWG02] or a PAI IWG Card Holder Unique Identifier (CHUID) [PAI IWG04]. Under current proposals, this string would be written to the card in a known location where it would be generally available in a "read-only" mode.

These identification strings can contain a larger amount of unique identification such as organizational affiliation and unique personnel identification number within that organization.

A digital signature on the CHUID by a trusted authority can be used to prevent the forgery of modified CHUIDs.

Pro: For legitimate cards issued by the government, a stored identification string such as a SEIWG-012 offers a unique identifier that also includes affiliation information for cross-organizational interoperability. This string cannot be modified on a valid card without access to the issuer's master key.

Con: The stored identifiers are not strongly bound to either the cardholder or the physical card, so they may be easily duplicated or imitated onto another card.

By implementing ISO 14443 directly, an attacker can imitate any desired CHUID. Digitally signed CHUIDs prevent the assembly of arbitrary false identifiers, but this does not provide any protection against the complete duplication of a valid CHUID onto another real or emulated card.

A stored identification string only represents a basic assurance factor for authentication.

2.3 *Symmetric key authentication*

High-end ISO 14443 cards such as the DESFire offer strong mutual authentication and over-the-air encryption using symmetric (secret) keys. For example, a DESFire application can be configured to only permit access by reader that knows a secret Triple-DES key that is stored on the card itself. Only readers that know this shared secret key are capable of accessing the application. Separate keys may be enabled for different types of operations (reading, writing, card management) on each card.

Typically, each card has its own secret key or keys which can be derived using an application "master key" (which is present on every reader) and some other card-specific identifiers (such as the card serial number). This means that each card doesn't have the same secret key, so a compromise of one card's key does not compromise any other cards. On the other hand, every reader in a domain must share the same master key(s).

Pro: Strong "something you have" factor for smaller environments. Key cannot be copied or cloned without access to domain master key.

Con: Access to master key would compromise every card in that domain, permitting duplication of any card and access to any reader. Key protection issues significantly constrain the number of places that this authentication factor can be used. Cross-domain authentication in federated environments is largely impractical, particularly in disconnected environments due to master key management issues.

Symmetric keys on cards represent a high assurance factor for authentication in closed environments, but are not secure for use in inter-agency or disconnected environments.

2.4 *Raw biometric templates*

Some deployments of contactless storage cards such as DESFire use biometric templates to perform authentication using a "something you are" authentication factor. They do this by storing a raw biometric template in the card storage area in a read-only form. This template can be read off the card and compared against a user to help confirm the identity of the user.

This template can be represented using an older proprietary scheme, or could use forthcoming standard

representations defined under ISO/IEC 19794 [ISO04] or INCITS 377+ [INCITS04].

Pro: The biometric is tightly bound to the user.

Con: The biometric is not bound to the card or any identifying serial number, so it may be trivially copied to another card or emulator. This does not offer a useful identification factor in inter-agency or disconnected environments. The lack of any cryptographic protection would allow any biometric to be presented from a card.

Raw biometric templates constitute a low assurance factor due to their lack of strong binding and copy protection.

2.5 *Signed biometric interchange files*

Rather than storing raw biometric templates on cards, some groups have promoted the storage of one or more biometric templates on the contactless card with a digital signature to protect them from modification. These files would typically be written using a standardized signed interchange format such as CBEFF [PDR+01] or X9.84-2003 [ANSI03].

Pro: The basic representations in these standards provide a digital signature around the biometric template, which prevents the creation of arbitrary templates for non-registered users.

Con: Standard CBEFF and X9.84 do not provide strong binding to the card or any identification factors. The biometric template for any registered user can be copied to another real or emulated card, which provides no protection against duplication. Once a user has been registered (so they have a signed biometric template), they can reuse the generated interchange file indefinitely. In addition, if the card contains more than one biometric template, the reader must retrieve all of the biometric values (the entire CBEFF) before signature validation can be performed, which will negatively impact transfer speeds for the user. If each biometric template were split into a separate signed file, the time to retrieve one template would be reduced, but the total storage requirement would increase significantly due to the overhead from the interchange file format (dozens of bytes) and the digital signature (approximately 150 bytes for RSA-1024).

Simple signed biometrics provide only basic assurance for interoperable and disconnected environments.

2.6 *Signed biometric interchange files with card ID binding*

Groups such as the Interagency Advisory Board task force are considering extending biometric interchange formats such as CBEFF to include the card serial number (CUID) in the signed CBEFF body to provide a stronger binding between the biometric

template(s) and the card itself. As long as the CUID is treated as the primary identifier for the user, this provides protection against the transfer of identity to other cards.

Pro: Adding the card's CUID into the signed interchange file provides a strong binding to a unique identifier which mitigates against copying templates between cards.

Con: The CUID identifier may not be a sufficient reference ID for interoperability, since the CUID may not be securely known by other entities. This identifier is also not tied into the digital identity represented on the contact half of the card. As in **Error! Reference source not found.**, above, this representation will be expensive in either IO times or memory if more than one biometric template is stored on the card.

Adding the external CUID into the signed message provides a high assurance authentication factor.

2.7 *Signed biometric templates with card ID and certificate binding*

To provide a stronger binding to the user's overall digital identity, it would be straightforward to extend the logical scheme proposed by the Interagency Advisory Board Data Model Task Force to bind the biometric template to both the card (via CUID) and the user's more general digital identifier [IAB04]. This could be done by including the relevant serial number and issuer information from the cardholder's Identification digital certificate. This would provide binding to a universal unique identifier which would be strongly represented on both the contact and contactless interfaces.

The stored biometrics could be bundled together with this identifying information and bound using a single digital signature, as shown in Figure 1, below.

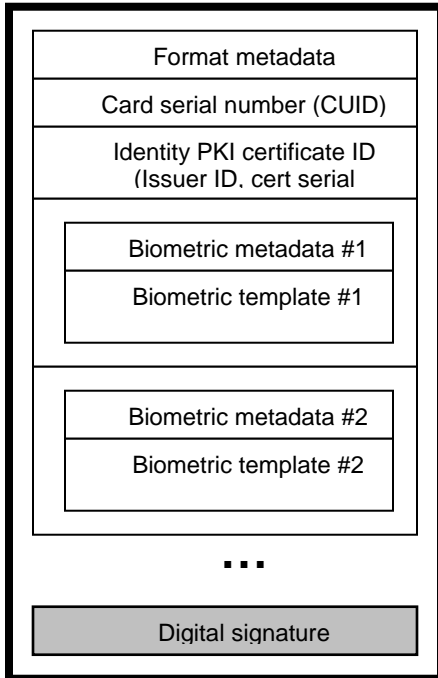


Figure 1

Alternately, each separate biometric template (fingerprints, hand geometry, iris scans) could be stored in a separate digitally signed format that is bound to the card and user, as shown in Figure 2, below.

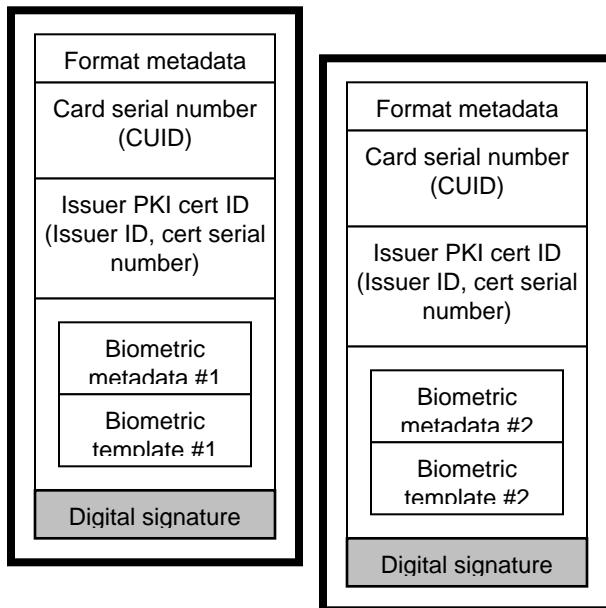


Figure 2

This logical representation could be expressed through a CBEFF Patron format in the same manner as the IAB's proposed data format. This representation

could be as simple as adding a certificate identifier field into the IAB proposal.

Alternately, a different encoding could be used. For example, an X.509 Attribute Certificate [ISO01b] would provide a signed, extensible data format that uniquely binds the cardholder's identity certificate to one or more biometric templates, the CUID, and any other issuer-defined fields as needed. This would offer compatibility with existing standards and encodings with greater future flexibility.

Pro: Binding the biometric to the card's CUID and the user's cert ID provides a mapping that ties the biometric, the card, and the high-level digital identity of the user. This also permits a unified approach to identity management and validation, since the cert ID can serve as a universal identifier for all transactions. This could allow inter-agency identification through a federated identity instead of relying on pre-registration.

Con: If more than one biometric template is stored on the card, then this scheme will be either inefficient in data transfer times or storage usage. If one signature encapsulates all templates, then all templates must be transferred before any can be used. This may consume a significant amount of time due to the limited data transfer rates for contactless cards. If, on the other hand, each template is put into a separate digitally signed file, then the retrieval of one template is efficient, but a significant portion of the limited memory capacity of the card will be wasted with redundant data and extra digital signatures.

With either representation, digitally signed biometrics bound to cert and card IDs represent a high assurance authentication factor.

2.8 Signed biometric references with card and cert ID binding

As an optimization to the bound biometric templates described in 2.7, above, CoreStreet believes that the data storage and bandwidth aspects of signed, bound templates can be reconciled by signing secure references to biometric templates rather than the templates themselves.

Under this scheme, a digitally signed authentication file (e.g. Attribute Certificate) would be placed onto the card. Like the previous architecture, this message would bind together the card CUID, the cardholder's identity cert ID, and biometric information. However, rather than storing the entire biometric templates within the signed authentication file, this scheme would only store a one-way secure hash of each biometric template, as shown in Figure 3, below.

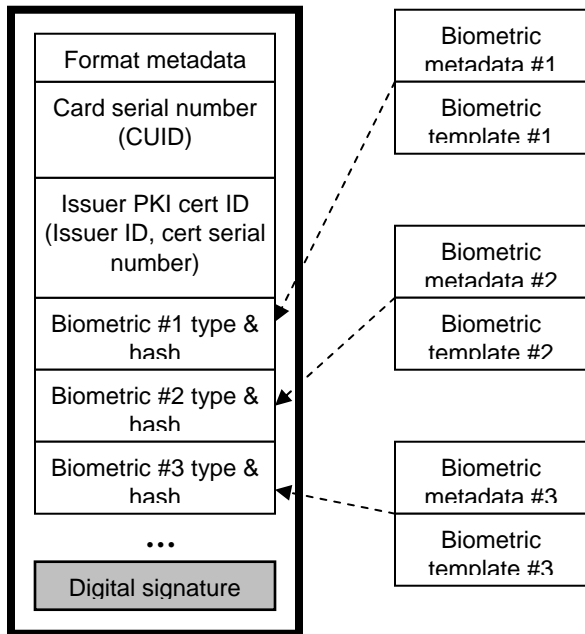


Figure 3

Using this scheme, the card stores a single authentication file, with a single copy of the binding information and the digital signature. For each biometric template on the card, this authentication file will contain a indicator of type (e.g. INCITS 377 Fingerprint Minutiae template) and a one-way secure hash of that particular biometric file. This would only add around 30 bytes per biometric to the base authentication file.

The biometrics themselves would be each stored in a separate file on the card. Each biometric would be unsigned. However, the single signature on the authentication file could be used to confirm the integrity of any of the referenced biometrics. We would recommend that the individual biometric templates be stored in separate card files in the same order that they are represented in the authentication file. For example, an application could be provisioned on the DESFire card with the following files:

File ID: 0	Signed authentication file (e.g. Attribute Certificate)
File ID: 1	Biometric template file #1: Finger #1 minutiae
File ID: 2	Biometric template file #2: Finger #2 minutiae
File ID: 3	Biometric template file #3: Iris template
...	...

Using this scheme, a reader capable of authentication using a particular biometric technology (e.g. Iris scan) could initially read File #0 to retrieve the signed master authentication file. This would contain strong binding to the card (which would be verified against the retrieved CUID) and the user's digital identity (attribute certificate). This initial file would be relatively small (200-300 bytes) since it does not contain any of the biometrics.

After reading and verifying the authentication master file, the reader could determine that the desired template type (iris template) is located in File #3. This template could be retrieved without touching any of the other biometric templates on the card. Its integrity could be confirmed by hashing its bytes and comparing against the master authentication file.

Pro: Permits strong authentication in federated and disconnected environments with minimum of wasted data and communication. Optimal scheme when multiple independent biometrics are represented on the card.

Con: Small storage overhead (~30 bytes) if only a single biometric template is stored on the card. Data model and representation not defined by existing standard (e.g. CBEFF).

Use of this type of strongly bound signed biometric represents a high assurance authentication factor.

2.9 Contactless PKI

For comparison, it must be noted that cards are currently available that can perform asymmetric operations on a contactless (ISO 14443) interface. For example, Oberthur currently distributes FIPS-certified contactless cards based on Philips chips that can perform RSA operations on both contact and contactless interfaces. While this technology has not been selected for the current generation of government smart cards, the protocol-level compatibility could permit a simple transition in the future.

These contactless capabilities could be enabled by either linking the contactless antenna to the contact chip (dual-interface) or else by integrating an independent contactless chip (combo card).

Pro: Provides strong authentication without requiring access to biometric information.

Con: Dual-interface cards may introduce security and privacy concerns if access becomes available to sensitive applications on the contact chip. Combo cards may significantly increase per-card costs over simpler symmetric chips like DESFire.

Use of contactless cards with private key capabilities would represent a high assurance factor.

3 BIOMETRIC CONSIDERATIONS

The previous descriptions of biometric-based authentication assume the existence of ideal biometric algorithms that are acceptable for widespread usage. For real-world applications, the use of biometric templates may introduce several issues.

3.1 Privacy

The collection of biometric information by government agencies can raise concerns that this data may be misused. For example, a database containing the fingerprint templates of all government-affiliated individuals could be a tempting target for someone wishing to establish the owner of a latent fingerprint. Similarly, a database of face images could be searched to identify lawful protestors.

This concern for biometric searches (1-to-N) may be lessened by an approach that only stores biometric information on user cards. The schemes, above, would permit an attacker up to a meter away from a user to silently pull the user's biometric templates along with the user's serial number(s).

This attack should be contrasted with the ability of a nearby attacker to gather equivalent data through more prosaic means. For example, a facial image on the card would be more difficult to capture than a snapshot from a digital camera. A fingerprint template would be no easier to retrieve than a latent fingerprint left by the cardholder.

More importantly, the biometrics on the card should not be tied to identifying biographic information. The schemes, above, recommend binding the biometrics only to arbitrary serial numbers, not biographic identifiers such as name or social security number. This means that a passive reader in the Pentagon Metro station may be able to silently retrieve a large number of government fingerprint templates, but these would be no more useful for building an identification database than random fingerprints from the subway's poles.

3.2 Forgery

Another possible concern with the use of biometric templates is the potential for an attacker to use the template as a basis for a forged biometric that could fool some sensors. For example, a facial image suitable for face recognition could also be used to create a printed image capable of fooling some face recognition systems.

This property of biometrics also prevents the effective revocation of the biometric factor if it is ever compromised. Unlike a private key, which can be revoked and replaced, a duplicated finger cannot be comfortably discarded.

The ability of an attacker to forge a biometric authentication factor depends on the countermeasures provided by the biometric vendors. For example, advanced fingerprint sensors attempt to detect the difference between live fingers and duplicates using proprietary detection of temperature, moisture, conductivity, etc.

3.3 Interoperability

In spite of ongoing efforts to standardize biometric templates and sensors, unacceptable incompatibilities may exist between templates and algorithms from multiple vendors. It is believed that these interoperability issues will improve as the relevant standards are finalized, but this may not provide an adequate solution for the current generation of cards.

This may require a fallback from efficient representations (e.g. fingerprint minutiae) to bulkier forms (e.g. full fingerprint images) that may exceed the storage capacity of contactless cards.

4 SECURE CONTACTLESS AUTHORIZATION

If contactless authentication is performed using only factors that are bound to the card's serial number (CUID) or domain-specific authentication string (e.g. CHUID), then any solutions to validate and authorize the cardholder will be inherently limited to the physical access domain, since there is no strong tie to the digital identity represented on the contact interface of the card.

If, however, the authentication is tightly bound to the cardholder's digital identity, as represented by their identification public key certificate, then the same unique identifier can be used for both contactless physical access and contact PKI transactions.

This property permits a unified approach to securely managing the privileges and revocation of a cardholder. For example, OCSP [MAM+99] or CRLs could be used to determine whether the cardholder has been revoked, and this same scheme would be usable for both physical and logical access. Privileges could be securely delivered for use in both physical and network environments.

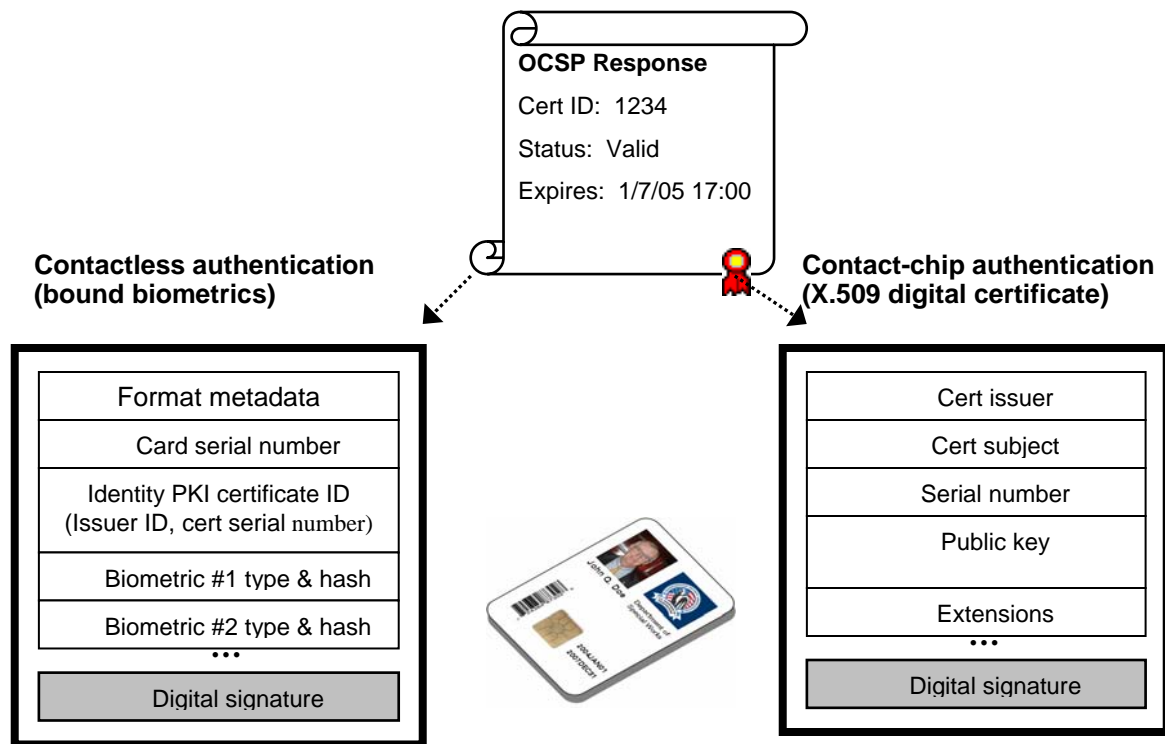


Figure 4

4.1 Unified authorization messages

Figure 4 shows the same authorization message, in the form of a digitally signed OCSP Response, being used for physical and logical access for the same card. This authorization message could be represented using any other desired standard such as a digitally signed SAML assertion [OASIS02], an X.509 attribute certificate, etc.

This scheme also provides a smooth migration to dual-interface cards where the same general applications would be available though either the contact or contactless (T=CL) interfaces. By logically identifying users using their cert ID today in a DESFire contactless environment, there is an easier migration to a future when the public key identity applet itself is available for secure asymmetric challenge-response authentication.

4.2 Offline authorization

If authentication factors such as signed, bound biometrics are available on the contactless interface, then strong authentication can be performed in offline settings without any access to an online directory. Similarly, secure authorization can also be performed in offline settings by storing signed authorization messages on the contactless interface.

Each authorization message is strongly bound to the cardholder's digital identity by including the cardholder's identity certificate ID within the signed message body. Any reader can inspect the authorization message to confirm its integrity and timeliness, and then use the validation and privilege information to grant access.

Rather than proscribe a particular authorization message format for the entire government to permit inter-agency and offline authorization, CoreStreet recommends that the government permit the allocation of a reusable "authorization container" on the contactless card that may be used to store any authorization information used within an individual organization.

Figure 5 shows the structure of a possible general authorization container on a contactless DESFire card.

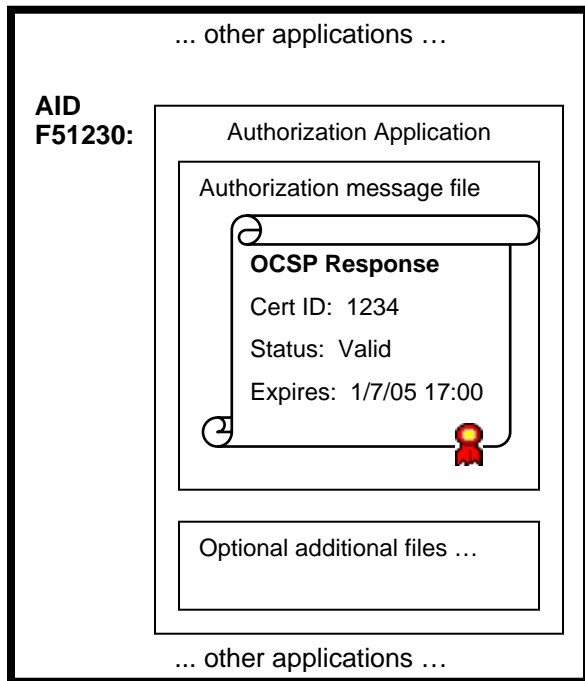


Figure 5

For example, the inter-agency standards bodies could define an application identifier (AID) and file number which has free read/write access. A cardholder with this applet could arrive at one agency, which may put a signed OCSP response onto her card to indicate validity and privileges. Offline readers in that agency would retrieve this OCSP message and use it to determine access privileges. At a second agency, the cardholder's card may be loaded with a signed SAML assertion of the user's privileges, which would be used to determine access at offline readers within that second agency.

The three important characteristics of this authorization container are:

- Standardized location on the card (3-byte AID on DESFire cards)
- Unrestricted read/write access
- Sufficient space for signed data (ideally, at least 1kB)

In Figure 5, the authorization message file is currently holding an authorization message in the form of an OCSP Response, but the authorization message could be any digitally protected format that is strongly bound to the identification credential.

This scheme would permit the greatest flexibility for supporting inter-agency and offline authorization by allowing each organization to locally specify their chosen representation, while guaranteeing that the card hardware in use by different agencies will interoperate.

5 CONCLUSIONS

The current generation of contactless identification cards have limitations which make it difficult to provide strong authentication for large, federated environments. Various approaches achieve different choices to balance scalability, security, and performance for physical access control.

If strong authentication is required for federated environments, we believe that this can only be achieved using either strongly bound biometrics or contactless public key support. Unfortunately, these approaches may run into issues of privacy and cost which could prevent them from being adopted. Lower-assurance alternatives may result in a higher risk of compromise through cloned identification credentials.

Strong federated authorization, on the other hand, may be possible under either scheme through the use of signed authorization messages for access control.

6 REFERENCES

- [ANSI03] American National Standards Institute. *Biometric Information Management and Security for the Financial Services Industry*. ANSI X9.84-2003. 2003.
- [INCITS04] InterNational Committee for Information Technology Standards. *Information Technology – Finger Pattern Based Interchange Format*. January 2004.
- [IAB04] Interagency Advisory Board (IAB) Data Model Task Force. *IAB Data Model Task Force Report v0.6 (Draft)*. October 2004.
- [ISO01] International Standards Organization. *Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Parts 1-4*. ISO/IEC 14443. 2000-2001.
- [ISO01b] International Standards Organization. *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*. ISO/IEC 9594-8. August 2001.
- [ISO04] International Standards Organization. *Information technology -- Biometric data interchange formats*. ISO 19794. Under development, 2004.
- [MAM+99] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams. *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*. IETF RFC 2560. June 1999.
- [OASIS02] Organization for the Advancement of Structured Information Standards

- (OASIS). *Guidelines for using XML Signatures with the OASIS Security Assertion Markup Language (SAML)*. Draft 02. September 2002.
- [PAIIWG04] Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems, Version 2.2*. July 2004.
- [PDR+01] Fernando Podio, Jeffrey Dunn, Lawrence Reinert, Catherine Tilton, Lawrence O'Gorman, M. Paul Collier, Mark Jerde, Brigitte Wirtz. *CBEFF: Common Biometric Exchange File Format*. NISTIR 6529. January 2001.
- [SDW+03] Teresa Schwarzhoff, Jim Dray, John Wack, Eric Dalci, Alan Goldfine, Michaela Iorga. *Government Smart Card Interoperability Specification, Version 2.1*. NIST Interagency Report 6887. July 2003.
- [SEIWG02] Security Equipment Integration Working Group, US Department of Defense. *Access Control Technologies for the Common Access Card*. April 2004.