A New Taxonomy for Analyzing Authentication Processes in Smart Card Usage Profiles

R.Chandramouli
National Institute of Standards & Technology, Gaithersburg, USA
mouli@nist.gov

ABSTRACT

As part of E-Government and security initiatives, smart cards are now being increasingly deployed as authentication tokens. The existing classification of authentication factors into – What you Know, What You Have and What You Are- does not provide a good framework for characterizing the strength and robustness of authentication processes involved in smart card-based authentications. The purpose of this paper is to identify the entities involved in this type of authentication processes, study the threats to those processes in terms of these entities involved, and then determine the list of properties associated with these entities that need to be verified to detect exploitation of these threats. A new taxonomy called Smart Card-based Authentication Taxonomy (SBCA) has been developed by classifying the property verification approaches under three authentication classes. The authentication profiles specified in two well-known recent government smart card specifications have been analyzed using the taxonomy to determine the relative strengths and assurances provided by these profiles.

1. INTRODUCTION

As part of E-Government and Security initiatives, Smart Cards or ICCs (integrated chip cards) are now being increasingly deployed as authentication tokens (for identity verification). Typical applications include controlling physical access to secure facilities, logical access to government IT systems and for encrypting and signing documents transferred between government personnel [8]. The systems that implement physical access control are called PACS (Physical Access Control Systems) and those implement logical access control are called LACS (Logical Access Control Systems). In any LACS (whether or not it uses smart cards), the user is allowed entry into the IT application system after verification of a claimed identity through a process called authentication. It is common practice to classify the various authentication mechanisms under the following classes called Authentication Factors:

- What you Know (AF1)
- What you Have (AF2)
- What you Are (AF3)

The above taxonomy for authentication mechanisms seems logical when the entity to be authenticated is a human user. However, when authentication is performed based on a set of electronic credentials resident on a smart card, using the above taxonomy does not facilitate robust characterization of the various authentication processes involving smart cards in terms of their relative strengths and consequent assurance levels. More specifically, using the above taxonomy for characterization of authentication profiles specified in many real-world smart card –based authentication scenarios provides elevated assurance levels (and a false sense of being more secure) than what is truly the case. For example, when a computer application authenticates a user based upon the credential presented through a smart card (a smart token) and the user is required to provide a PIN to activate the card so that it can be read by the authenticating system, the whole process is erroneously characterized as two-factor authentication consisting of what the user knows and what the user has. There is a flaw in this characterization since the application is in fact only authenticating the user purely based on what the user has (electronic credentials present on a token) without any other form of authentication. The PIN that the user provides is in fact not a secret shared between the computer application and the user. The PIN in this context is strictly a secret shared between the smart token and the user and merely serves to establish the binding between the user and the token and does not in any way enhance the authentication assurance from the application point of view.

The reason the interaction dynamics is different when a smart card is used in an authentication mechanism is due to the fact that there are three primary entities involved: *electronic credentials*, *smart card* and the *card holder*. Hence a different taxonomy is required for analyzing this process. This is the prime motivation for this paper. The approach used for arriving at this taxonomy is to study the entities and their interactions involved in this authentication technology and the possible threats that could subvert the integrity of these interactions. To provide assurance against these threats, the properties of the entities involved in smart card-based authentication that need to be verified are to be determined. This is the focus of section 2. The classification taxonomy for the smart card-based authentication process that follows from threat analysis and property verifications is described in section 3. We have called it the SBCA taxonomy where the acronym SBCA stands for Smart Card-based Authentication. In section 4, we analyze the authentication profiles specified in two U.S government smart card specifications in terms of our taxonomy in order to obtain a clearer understanding of their strengths and assurance levels. In section 5, a brief comparison with related approaches is made. Section 6 provides some benefits of using the SBCA taxonomy for improving the overall security of the authentication process in the usage scenarios where smart cards are deployed for identity verification.

2. THREAT ANALYSIS FOR SMART CARD_BASED AUTHENTICATION PROCESS

In order to understand the threats involved in smart card-based authentication processes, it is first necessary to understand the lifecycle activities involved in issuance of smart cards. Smart cards are generally issued by an issuing enterprise or an issuing authority to legitimate/authorized individuals (after some form of identity proofing) for the purpose of carrying out a specific task (entering a building or accessing an IT system). To enable this business process, a centralized repository called Identity Management System (IDMS) is often used by an enterprise. An IDMS server provides the dual functions of gathering/importing electronic credentials from multiple sources and then distributing (provisioning) these credentials (or appropriate subsets) to various authentication points. Typical sources of credentials are:

- An organization's Human Resource or Personnel Management systems – for supplying basic demographic information about a person ,nature of affiliation of the person to the organization (employee, contractor etc) and possibly a unique number associated with the person (an Employee Number, a large unique number for electronic identification etc).
- Enrollment or Registration systems – for collecting and transmitting information about identity proofing documents (birth certificates, passports etc), biometric information such as fingerprints, facial image etc.

The typical authentication points (also called target systems) to which an IDMS provisions credentials to support smart card-based authentication are:

- Physical Access Control Systems (PACS) – consists of a PACS server (which receives information from IDMS needed for enforcing physical access) and a PACS panel (which contains a cache of the information from PACS server needed for fast authentication –such as the Unique Identification Number of the person to be allowed physical access, the expiration date for this number, the name of the person and in some cases the photograph).
- Logical Access Control Systems (LACS) - this can include any type of IT resource that can support smart card-based authentication – such as an Operating System (Work Station), Single Sign-on (SSO) modules, access control (entitlement) servers etc.

In addition to the authentication points, there is another target to which an IDMS has to provision the credentials in order to support smart-card based authentication. That target is what is known as the Card Management Systems (CMS). The CMS is a software module that can establish secure sessions with a smart card, load programs that: (a) perform the functions of populating credentials (called card personalization) and (b) execute the function calls required for authenticating those credentials. A CMS also interacts with PKI Certificate Authority (CA) servers, to request and obtain digitally signed public key certificates (attesting the credentials) and populate these digital certificates on the smart card to form an integral part of the card-based credential set.

Coming back to our discussion of the three entities involved in smart card-based authentication – electronic credential, the smart card and the card holder, we could easily see that the authentication processes are nothing but a set of transactions between these entities and the authentication points (i.e., PACS and LACS) discussed above. The security of the authentication processes therefore depend upon the integrity of these transactions. Hence, it is necessary to identify the factors that will affect the integrity of these transactions. The factor identification exercise then leads us to examine the threats associated with the entities participating in the transaction. The three primary entities are:

- Electronic Credentials Resident on the Card (E1)
- The Smart Card itself – the physical card stock (E2)
- The Card Holder – the legitimate human being authorized to use the card (E3)

In addition there is the following secondary entity:

- The authentication databases at the authentication points (PACS & LACS) (E4)

Out of the four entities listed above, managing the threats to the authentication databases (E4) through security countermeasures is under the daily operational control of the organization. However the entities (E1, E2 and E3) go outside the scope of this continuous operational control once the smart card is issued to a human being affiliated with the organization. Hence, in this paper, our focus is on these three entities. Out of these entities, Credentials is an example of an electronic entity, the Smart Card is an example of physical entity while the Card Holder is an example of human entity. The list of threats to these entities that are relevant from the authentication process viewpoint is as follows:

- Threats to Electronic Credential Entity
- Threats to Smart Card
- Threats to Card Holder
- Threats to Smart Card – Credential Binding
- Threats to Card Holder – Smart Card Binding
- Threats to Card Holder – Credential Binding

Out of the last three threats, the threats to Smart Card-Credential binding are considered under the Smart Card entity while the other two are consider under Card Holder entity. Let us therefore analyze in details the threats to the three primary entities: Credential, Smart Card and Card Holder in the following sections.

2.1 Threats to Credential Entity

In the legitimate use scenario, the authentication system would expect the credential present on the card to have been issued by the right authority and its contents are identical to the one populated by the issuer. Based upon this trust assumption, the authentication system can then proceed to verify the validity or correctness of the credential, its currency (not past its designated expiration date) and its status (revoked, terminated or suspended). However, it is possible that the credential could have been obtained from an illegitimate source or the credential could have been altered or tampered with (done mostly to substitute with credentials that have higher privileges or access rights). The countermeasures to verify whether these threats have been exploited are to perform verification of additional properties such as credential's origin and integrity (in addition to correctness, currency and status). The origin of the credential is verified by examining the associated seal (digital signature) provided by the issuer and in turn verifying with a trusted authority who can attest to the cryptographic key used in generating the seal. The integrity of the credential can be verified by using the same attested key to compare the seal with the content of the credentials. In summary, the properties to be verified are the following:

- Credential Correctness
- Credential Currency
- Credential Status
- Credential Origin
- Credential Integrity

2.2 Threats to Smart Card Entity

The authentication system would expect only the cards issued by the rightful authority to be presented for granting authentication. The threat that breaks this expectation is that the card with legitimate credentials that is issued by the right authority could be cloned or duplicated. Hence the card issued by the issuer and the card presented for authentication is no longer the same. To detect cloning or duplication, the card can be verified to possess a unique tamper-proof identifier known to the issuing system (such as a unique number associated with the integrated circuit chip of the card) or a unique tamper-proof secret such as a cryptographic key whose presence on the card can be verified as a result of an operation that the card is directed to perform and whose creation is known to the issuing system.

However, a moment of reflection reveals that it is not merely enough to verify whether the particular card is one of the valid cards in the batch procured and used by the organization. The integrity of the card issuance and subsequent authentication process (during usage) depends upon the ability to associate a particular smart card (carrying or possessing a unique identifier) with a unique credential set associated with a particular holder. This particular binding or association is needed to exercise control over use of cards reported missing or lost. The properties to be verified for the physical entity (smart card) then become:

- Possession of a tamper-proof Unique Identifier
- Possession of a tamper-proof Valid secret
- Binding between the Card and the Credential set using issuance inventory data
- Binding between the Card and the Credential set using cryptographic Methods

2.3 Threats to Card Holder Entity

The card issuing authority and the authentication system would expect only the user to whom the card was issued uses the card. The events that could nullify this expectation are that the smart card is lost or stolen and before the legitimate holder can inform the authority of the loss/missing state, an unauthorized user who has got possession of the card uses the card to perform functions not authorized for that individual. In this situation, the legitimate binding between the card and its lawful holder is lost. This property can be verified using two different approaches as follows:

- Binding between the Card Holder and the Card through Proof by Knowledge
- Binding between the Card Holder and the Card through Proof by Trait

However, the binding between the card holder and the card can be faked by tampering with a stolen card. To detect this threat exploitation, the binding between the card holder and the credential needs to be verified. This can be achieved using the following property verification approach:

- Binding between the Card Holder and Credential through Cryptographic Methods

Table 1 – Authentication Classes and Properties to be Verified in SBCA Taxonomy

Authentication Class	Properties Verified	Threats Addressed
Credential Authentication (CLA)	Credential Correctness (CL-P1)	Use of Tampered Card
	Credential Currency (CL-P2)	Use of Obsolete Card
	Credential Status (CL-P3)	Use of Revoked Card
	Credential Origin (CL-P4)	Unauthorized Source
	Credential Integrity (CL-P5)	Data Tampering
Card Authentication (CDA)	Possession of a tamper-proof Unique Identifier by the card (CD-P1)	Cloning or Duplication of a credential on an unauthorized card stock
	Possession of a tamper-proof valid Secret by the card (CD-P2)	Cloning or Duplication of a credential on an unauthorized card stock
	Binding between the Card and the Credential set using issuance inventory data (CD-P3) (subsumes CD-P1)	Loss of control over cards reported missing or lost as well as Cloning or Duplication of a credential on an unauthorized card stock
	Binding between the Card and the Credential set using Cryptographic Methods (CD-P4) (subsumes CD-P2)	Loss of control over cards reported missing or lost as well as Cloning or Duplication of a credential on an unauthorized card stock
Card Holder Authentication (CHA)	Binding between the Card Holder and the Card through Proof by Knowledge (CH-P1)	Impersonation by stealing the card
	Binding between the Card Holder and the Card through Proof by Trait (CH-P2)	Impersonation by stealing the card

	Binding between the Card Holder and the Credential through Cryptographic Methods (CH-P3)	Impersonation by stealing the card as well as tampering with/retrieving Card Holder Identifier Data

3. SMART CARD-BASED AUTHENTICATION (SBCA) TAXONOMY

Having analyzed the threats to the entities involved in smart card-based authentication and the properties to be verified to detect the exploitation of those threats, we now proceed to develop the overall authentication taxonomy. We do this through a two-step process as follows:

- Designate an authentication class by grouping together property verifications associated with an entity
- Develop a canonical authentication process description associated with each property verification

The designated authentication classes and the properties verified under each class in the SBCA Taxonomy are shown in Table 1. As discussed in the previous section, some of the property verifications are in response to potential threats, while others stem from the core authentication process logic. Table 1 captures these corresponding threats addressed as well.

The purpose of developing the canonical authentication process description for each of the property verifications is to identify the minimal set of functions (or baseline security mechanisms in case the property verification address the security threats) that each property verification process has to support. These process descriptions under the three authentication classes are given in sections 3.1, 3.2 and 3.3 respectively

3.1 Credential Authentication Class – Canonical Process Descriptions for Property Verifications

From Table 1, one could see that this authentication class involves five property verifications. From a process viewpoint, these five property verifications can be grouped as followed.

- Credential Correctness (CL-P1), Credential Currency (CL-P2) and Credential Status (CL-P3)
- Credential Origin (CL-P4) and Credential Integrity (CL-P5)

<u>CL-P1, CL-P2 and CL-P3:</u> All electronically issued credentials are verified to be correct by checking against entries in the database maintained by the issuing organization or authority (CL-P1). In physical access control situations, the cache of the database containing credentials usually resides in a module called "Panel" of a physical access control system (PACS). An organization with multiple facilities and multiple facility access points may have many panels. Hence the list of credential numbers needed for authentication for each of the panels located at various sites is refreshed periodically from a centralized enterprise database containing organization-wide credential numbers. The logic of the verification processes for correctness, currency and status depends upon the methodology adopted for the database refresh process. If the refresh process involves populating only the active set of credentials (current and not carrying any status flags – revoked, terminated or suspended), then the database comparison for correctness (CL-P1) implicitly performs verifications for currency (CL-P2) and status (CL-P3) as well. On the other hand, if the refresh logic sends in all the credentials appropriate for the panel along with expiration dates and status information, then explicit verification processes have to be performed for correctness, currency and status. The more frequently the panel entries are refreshed; more assurance is obtained for all three verification processes (CL-P1, Cl-P2 and CL-P3). Authentication against panel entries refreshed daily provides better assurance than authentication against panel entries refreshed only once a week.

<u>CL-P4 and CL-P5:</u> A credential found on a presented card, even if it is verified to be correct, current and not carrying revoked/terminated/suspended status cannot be deemed to be valid unless it carries a proof of authenticity with respect to its origin (CL-P4) and its integrity (CL-P5). The most common proof of authenticity in a smart card-based credential is a digital signature. The digital signature string is generated using a private key and the entity that signed the credential demonstrates its own credential by providing a certificate that contains the corresponding public key so that the signature can be verified. Trust in the certificate is established by establishing a trust anchor chain from a known trusted third party to the party that actually signed the certificate (called Certificate Validation). The currency of the certificate is established by verifying the non-presence of the certificate in the list of revoked certificates called Certificate Revocation List (CRL) or obtaining the currency status or through a query directed against a software module called On-line Certificate Status (OCSP) responder. Verification of the digital signature of the credential using the public key present in a trusted, current certificate then establishes the fact that the credential originated from the right authority (CL-P4) and has not been tampered with (CL-P5).

3.2 Card Authentication Class – Canonical Process Descriptions for Property Verifications

Referring again to Table 1, we see that this authentication class contains four property verifications:

- Possession of a tamper-proof Unique Identifier (CD-P1)
- Possession of a tamper-proof valid Secret (CD-P2)
- Binding between the Card and the Credential set using issuance inventory data (CD-P3)
- Binding between the Card and the Credential set using cryptographic Methods (CD-P4)

<u>CD-P1:</u> Any organization that has issued smart cards has to keep an inventory of the list or range of unique identifiers associated with the card stock it has personalized. This is to ensure that valid credentials are not cloned or duplicated on external card stock and presented to the organization's authentication system. This will

result in unnecessary proliferation of credentials with attendant security risk. Hence every card presented to the authentication system must be verified for possessing the unique identifier that falls within the range or list of numbers in the organization's card stock inventory. This verification provides the required assurance only if the unique card identifier is tamper-proof.

CD-P2: Another approach for the organization to ensure that the card presented during the authentication process is one of the cards issued by it, is to verify that the card possesses a valid secret. In this process, the card demonstrates possession of a secret by revealing an artifact related to the secret and then participating in a cryptographic protocol. This cryptographic protocol is called the challenge-response protocol using asymmetric keys. The secret the card possesses is therefore the private key and the artifact related to the secret that the card presents is the public key embedded in a PKI certificate. The private key is tamper proof and cannot be revealed without destroying the physical entity (plastic card). The PKI certificate on the card is signed/issued by a trusted authority and carries the name of the asymmetric algorithm. The authenticating system reads the certificate, establishes trust in the certificate through PKI Certificate validation, verifies that the certificate is current using CRL or OCSP mechanisms and then sends a challenge that is consistent with the key size of the asymmetric algorithm through an appropriate APDU. The card encrypts the challenge using its hidden private key and sends back the encrypted challenge as a response to the APDU. If the authenticating system, on decrypting this encrypted challenge using the public key gets back the challenge it sent, then it indeed authenticates the smart card (physical entity) by virtue of the following:

- It contains a trusted certificate issued by the valid issuing authority
- The card is in possession of the valid secret (private key) associated with the public key string listed in the certificate.

CD-P3: The process for verifying the binding or association (property) between the smart card (physical entity) and credentials (electronic entity) depends upon how the uniqueness property of the smart card is verified. If the uniqueness property is verified through testing the unique identifier (such as the integrated circuit chip ID), then this verification process involves retrieving the unique credential (or credentialing number) that the card carries and then comparing the retrieved combination (Card Identifier – Credential Number) with combinations recorded in the organization's card issuance database.

CD-P4: On the other hand, if the uniqueness property is verified through testing the possession of the valid secret, then the verification is enabled by including the unique credential as one of the fields in the PKI certificate. The binding between the certificate and the credential is established when the digital signature of the certificate is verified. Since the binding between the card and the certificate (its public key) is already established through the card's demonstration of its possession of a valid secret (private key held by the card) (through the challenge-response cryptographic protocol), the binding between the card and the credential is established through the transitive relationship.

3.3 Card Holder Authentication Class – Canonical Process Descriptions for Property Verifications

The credential residing on the card may have been validated for having originated from the right authority (CL-P3) and proved to be not tampered with (CL-P4). Even the binding between the Card and the Credential may have been established using the issuance database (CD-P3) or through cryptographic methods (CD-P4). Still a security problem exists when the card itself is being used by a person to whom it is not rightfully issued. This problem can only be solved if the binding between the card holder and the card can be established at the time of usage. The binding can only be established use one of the following two property verification approaches.

- Binding between the Card Holder and the Card through Proof by Knowledge (CH-P1)
- Binding between the Card Holder and the Card through Proof by Trait (CH-P2)

In addition the faking of this binding through card tampering can be detected by performing the following property verification:

- Binding between the Card Holder and the Credential through Cryptographic Methods (CH-P3)

CH-P1: In this approach, the card authenticates the user of the card based on a shared secret such as PIN. The strength of authentication depends upon the size of the secret. The security of the process comes from the fact that the initial secret is either granted by the authority that issues the card (and made known to the user through a secure communication channel – face to face verbally or postal mail) or chosen by the user of the card in the physical presence of an official of the issuing authority. Subsequently the secret can be changed to a value the user wants (subject to some entropy/strength requirements) but since the change process requires demonstration of knowledge of the existing secret, the security is maintained. Apart from exhaustive search (called password cracking) whose difficulty increases with the size of the secret, the other threats to the security of this process are social engineering (giving out the secret to another human) and negligence of the user (writing down the secret and leaving it at a place where it can be seen or easily accessed). This form of authentication setup is conceptually similar to a system administrator setting up an userid for a user cleared for access with an initial password to access a system that can then be changed by the user.

CH-P2: Another method of authenticating the cardholder is by using a biological characteristic of the person such as fingerprint biometrics or hand geometry. An example of this is the one where the card may store a biometric data such as fingerprint templates. The user authenticates to the card by providing fingerprints which are then extracted, converted to templates and then matched with the ones found on the card (by special devices called scanners and augmented with special software modules called template generators and template matchers). This form of authentication is called biometric authentication. The matching of the live scan biometric (the one provided by the user) with the stored biometric (one on the card) can take place either outside the card or on the card itself if the card contains the matcher program running within itself (such cards are called match-on cards).

CH-P3: The previous two property verifications (CH-P1 & CH-P2) merely establish the binding between the card and the card holder. This binding could easily be faked if the person who has stolen the card guesses the PIN correctly or injects his/her biometric data into the card. Hence an additional property to be verified is the binding between the card holder and the credential. To enable this verification, the unique credentialing number is often combined with the card holder identifier information (e.g., biometric template) and digitally signed. The verification of this signature establishes the binding between the card holder and the credential while simultaneously performing the origin authentication of both the card holder identifier information and the credential.

3.4 Analysis of the set of Property Verifications for overall Authentication Assurance

Practical smart card-based authentication mechanisms will involve subsets of the property verifications in the SBCA taxonomy shown in Table 1. The choice of a given subset determines the assurance level associated with the authentication mechanism. However we find that the following set of property verifications are common to all authentication mechanisms due to the fact that these verifications involve testing the validity of the credentials read from the card and credential validation forms the core function of any authentication process:

- Credential Correctness (CL-P1)
- Credential Currency (CL-P2)
- Credential Status (CL- P3)

However, it is important to note that any authentication mechanism with a high level of assurance should include verifications relating to all the possible combinations of binding between the three entities involved in smart card-based authentication, i.e., Credential, Card and Card Holder. Hence, a high assurance authentication mechanism should involve the following property verifications:

- Card to Credential Binding (using CD-P3 or CD-P4)
- Card Holder to Card Binding (using CH-P1 or CH-P2)
- Card Holder to Credential Binding (using CH-P3)

Further we find that even within the same type of property verification, one particular property verification approach provides more assurance than another. For example within the Card to Credential Binding, we find the authentication process based on cryptographic method (CD-P4) provides higher assurance than the one based merely on database comparison (CD-P3). Similarly, verification of the binding between the Card Holder and Card through biometric data matching (CH-P2) is certainly more robust than matching of the shared secret such as PIN (CH-P1).

4. ANALYSIS OF GOVERNMENT SMART CARD-BASED SPECIFICATIONS USING THE SBCA TAXONOMY

In this section, we look at the authentication processes specified in two recent U.S government smart card usage profiles and assess their assurance capabilities using the property verification approaches outlined in our SBCA taxonomy and the subsequent analysis outlined in section 3.4.

4.1 PACS 2.3 Specifications

To promote interoperability among smart card based physical access control systems (PACS) across various agencies of the U.S Federal government, the Physical Access Interagency Interoperability Working Group (PAIIWG) within the Government Smart Card Interagency Advisory Board (GSC-IAB) drafted this specification [9]. The two salient features of this specification are:

- Standardized container for Credentialing Elements (called CHUID) containing a series of optional and mandatory tagged objects. One of the mandatory elements is FASC-N (Federal Agency Smart Credential Number). The container includes a tag for storing the asymmetric digital signature of the credential.
- A graded set of assurance profiles – Low, Medium and High – that provide for increased assurance for the authentication of credentials read from the CHUID container.

Let us now analyze the authentication processes specified under the PACS 2.3 assurance profiles in terms of the authentication processes in our SCBA taxonomy to determine the assurance levels that each of them provide.

PACS 2.3 Low Assurance Profile: Under this profile, the card reader first reads the Card Unique Identifier (CUID) and then the contents of the CHUID container. The entire contents or a subset of the CHUID container elements that constitute the credentials are sent to the security panel of the PACS. The smart card holder is allowed entry into the physical facility based on the matching of the credentials sent by the reader with the list of credential numbers present in the panel. Since the list of credential numbers is refreshed periodically (weekly, daily or several times within a day depending upon the type of physical facility), this authentication mechanism verifies the Correctness, Currency and Status of the credential (CL-P1, Cl-P2 & CL-P3). No other property verification approach is used in this process.

PACS 2.3 Medium Assurance Profile: In this process, the PACS security panel stores along with the list of correct, current credential numbers, the HMAC (Hashed Message Authentication Code) of the concatenation of the credential data from CHUID and the Card Unique Identifier (CUID), thus creating a cryptographic binding between the credential and the specific card from where the credential is expected. The HMAC is computed using a site-specific secret key and a site-specific cryptographic algorithm. When a user presents the card, the reader retrieves the CUID and reads the CHUID contents. Using these two, it computes the HMAC using the same site-specific secret key and algorithm. The selected credential elements read from CHUID along with the computed HMAC are sent to the panel. Authentication is done based on matching of the credential as well as the matching of the associated HMACs. Further, the matching of the HMACs implicitly provides assurance that the credential has not been tampered with. This process therefore performs correctness, currency, status and integrity verification of credentials (CL-P1, CL-P2, CL-P3 & CL-P5) and binding of the card to the credential (CD-P3) through HMAC matching. Card

Holder to Card binding and Card Holder to Credential binding properties are not verified. However an interesting aspect of this authentication process is that the authentication system expects a HMAC computed using a site-specific algorithm and a site-specific key. Hence, this process provides authentication of an additional entity (i.e., the card reader which is an infrastructure entity).

PACS 2.3 High Assurance Profile:This process verifies whether the card is in possession of a cryptographic key that is derived using the site-specific secret key and a concatenated text string made up of Card Unique Identifier (CUID) and CHUID contents. During authentication, the reader retrieves CUID, reads the contents of CHUID and computes the cryptographic key based upon a site-specific secret key using the algorithm information in a data structure called Authentication Key Map. To verify whether the card is in possession of the same cryptographic key, the reader sends a random challenge and receives the encrypted challenge (encrypted by the card using the cryptographic key injected into it) from the card as a response. The reader then encrypts the challenge using its generated cryptographic key and looks whether the two cryptograms (one computed by it and the other received from the card) match. Finally of course the extracted credentials are sent to the PACS security panel for matching. This process therefore performs correctness, currency, status and integrity verification of credentials (CL-P1, CL-P2, CL-P3 & CL-P5) and binding of the card to the credential (CD-P4). Thus we see that the same property verifications as found in PACS 2.3 Medium Assurance Profile are performed in this profile. However the verification approach used for Card to Credential binding (CD-P4) is based on a cryptographic protocol and is therefore much more robust than the corresponding approach (CD-P3 and HMAC based) used in the Medium Assurance Profile. Since the success of the cryptographic protocol depends upon the reader's ability to generate the right cryptographic key based on the combination of site specific secret key and the card and credential data read from the card, this serves to authenticate the reader as well.

The results of the analysis of the authentication processes used in PACS 2.3 Authentication Profiles in terms of the property verification approaches outlined in SBCA Taxonomy are summarized in Table 2 below.

Table 2. Characterization of PACS 2.3 Authentication Profiles

Authentication Profile	**Property Verification Approaches**	**Additional Property Verifications**
Low	Credential Correctness (CL-P1) Credential Currency (CL-P2) Credential Status (CL-P3)	
Medium	Credential Correctness (CL-P1) Credential Currency (CL-P2) Credential Status (CL-P3) Credential Integrity (CL-P5) – *through HMAC* Binding of Card to Credential (CD-P3)	Authentication of the Reader (Infrastructure element)
High	Credential Correctness (CL-P1) Credential Currency (CL-P2) Credential Status (CL-P3) Credential Integrity (CL-P5) Binding of Card to Credential (CD-P4) – *through a cryptographic protocol*	Authentication of the Reader (Infrastructure element) *The cryptographic key injected into the card is based on a site-specific key. Hence limits the use of the card to specific designated sites where that key is used.*

4.2 FIPS 201 Specifications

In response to a Presidential Directive called HSPD-12, the U.S Government developed a set of specifications for use of smart cards to provide physical access to federal facilities and logical access to government IT systems using a set of uniform, interoperable and tamper-proof credentials. These specifications are embodied in a document called FIPS 201 [5] and its various companion documents [1,2,6]. In terms of the credentialing elements, FIPS 201 uses the same CHUID container defined in PACS 2.3 specifications (discussed in previous section) with some minor variations. FIPS 201 outlines a set of authentication use cases classified into three graded assurance levels – "SOME confidence", "HIGH confidence" and "VERY HIGH confidence". As we did in the discussion of PACS 2.3 specifications, let us now analyze the FIPS 201 authentication processes in terms of the property verification approaches in our SBCA taxonomy. (The summary is shown in Table 3).

SOME Confidence: One of the processes under this assurance level is "Authentication Using the PIV CHUID". Under this process credential elements in the CHUID container are read by the card and their origin and integrity are verified using the associated digital signature. Eventually, the credentials that are read from the CHUID container are sent to the PACS system for matching against a periodically refreshed list. This process therefore performs correctness, currency, status, origin and integrity verification of credentials (CL-P1, CL-P2, CL-P3, CL-P4 & CL-P5) thus covering all property verifications relating to credentials. The Card to Credential binding, Card Holder to Card binding and Card Holder to Credential binding properties are not verified under this process.

HIGH Confidence: FIPS 201 provides a single authentication process called "Authentication using PIV Biometric" under this assurance level and labels it as BIO. This process calls for the user of the smart card to provide his/her fingerprint biometric data through a live scan and also provide a PIN to enable the reader to read the stored biometric data on the card. A key credentialing element FASC-N is embedded in the data structure containing the biometric data and verification of the digital signature associated with biometric data implicitly verifies the origin and integrity of the credential. This process therefore performs correctness, currency, status, origin and integrity verification of credentials (CL-P1, CL-P2, CL-P3, CL-P4 & CL-P5) thus covering all property verifications relating to credentials. The Card Holder to Card binding property is verified through the verification approach CH-P2 as the card holder is authenticated to card using biometric matching. The Card Holder to Credential binding is verified through the verification approach CH-P3 as the identifying credential is embedded with biometric data structure. The only property that this process does not verify is the Card to Credential binding.

VERY HIGH Confidence: The authentication process (BIO) described in the previous section, when carried out under the watch of an attendant (when the user is submitting fingerprints to a scanner especially) is classified under VERY HIGH Confidence assurance level. In addition, another authentication process called “Authentication using PIV Asymmetric Cryptography” (labeled as PKI) is specified under this level. This authentication process calls for the card to encrypt a challenge sent by the reader system using the private key of a private-public key pair the card holds (Challenge-Response Cryptographic protocol). This process therefore verifies the property that the card possesses a tamper-proof valid secret (CD-P2). To enable the card to perform this private key operation, the card holder is required to provide a PIN thus performing the Card Holder to Card binding verification using the CH-P1 approach. A key credentialing element FASC-N is embedded in the certificate that contains the public key that corresponds to the private key held by the card. Hence validation of the signature of the PKI certificate using the issuer’s public key implicitly validates the origin and integrity of the credential, in addition to verifying the PKI certificate to credential binding. Further since the Card to PKI Certificate binding is established through the challenge response cryptographic protocol, we have transitively obtained the verification of Card to Credential binding through the verification approach CD-P4. The only property not directly verified in this process is the Card Holder to Credential binding but that property occurs transitively due to Card Holder to Card and Card to Credential bindings that have already been established.

Table 3. Characterization of FIPS 201 Authentication Use Cases

Authentication Use Cases	**Property Verification Approaches**	**Additional Property Verifications**
SOME Confidence	Credential Correctness (CL-P1) Credential Currency (CL-P2) Credential Status (CL-P3) Credential Origin (CL-P4) Credential Integrity (CL-P5)	
HIGH Confidence	Credential Correctness (CL-P1) Credential Currency (CL-P2) Credential Status (CL-P3) Credential Origin (CL-P4) Credential Integrity (CL-P5) Card Holder to Card binding (CH-P2) Card Holder to Credential binding (CH-P3)	
High	Credential Correctness (CL-P1) Credential Currency (CL-P2) Credential Status (CL-P3) Credential Origin (CL-P4) Credential Integrity (CL-P5) Card to Credential binding (CD-P4) Card Holder to Card binding (CH-P1)	Card Holder to Credential binding occurs transitively due to Card Holder to Card and Card to Credential bindings.

5. COMPARISON WITH RELATED APPROACHES

Smart card-based authentication schemes appear in two categories of published literature. One category appears in various research papers in technical professional journals. The other category appears in technical specifications for large-scale smart card deployments. The central theme of the research papers has always to present new and novel schemes that are robust enough to withstand all types of known and potential attacks. Examples are: An improved scheme for asymmetric smart card authentication which is resistant to not only replay and active attacks but also hostile attacks [3], Password-based authentication schemes using smart card that are resistant to logic attacks [7,10], smart card-based biometric authentication schemes that provide assurance against replay attacks [4] and so on. Because the core focus of research community is on security robustness, certain other factors such as scalability, performance and usability may not be given their due consideration in their proposed schemes. On the other hand, the authentication schemes proposed in technical specifications relating to smart card deployments in industry or government, are generally chosen because they have some track record of earlier deployments and found to be usable with reasonable performance overheads. However, it was generally found that those technology choices are macro-level selections without an analysis of the core properties each of the mechanisms verify in the context of the entities participating in the authentication transactions. The purpose of this paper is to bring some formalism into the process of specifying authentication schemes for real-world smart card deployments by providing a framework to analyze authentication mechanisms in terms of some fundamental property verification approaches.

6. BENEFITS AND CONCLUSIONS

The SBCA taxonomy with its authentication classes and associated property verification approaches provides a framework for analyzing the authentication profiles or authentication use cases specified in real-world smart card deployment specifications. This is already demonstrated in the paper by using the taxonomy to characterize two government smart card usage specifications. Analyzing authentication profiles/schemes chosen or selected in the smart card usage specifications in terms of SBCA taxonomy provides a formal approach to determine whether the assurance levels assumed for those profiles/schemes are realistic. Apart from facilitating top-down analysis, the list of property verification approaches in the SBCA taxonomy, can be used to build a combination that is appropriate for a given deployment scenario and then an authentication mechanism that includes those property verification approaches can then be chosen and specified.

Further the SBCA taxonomy development paradigm is flexible and extensible. For example, when new threats are discovered for the three entities (Credential, Smart Card, Card Holder) or the binding between the entities, additional property verification approaches can easily be added. Also, when new entities are added to the authentication scheme, additional property verification approaches are to be added as well. For example, in our SBCA taxonomy, we have assumed that the card reader is an integral part of the authentication system or connected to the authentication system through a closed network connection. On the other hand, if a smart card-based authentication system involves remote readers connected through an open network to the authentication system, additional property verification approaches relating to integrity of communication between the readers and the authentication system, integrity of reader operation (as the readers may be tampered or compromised) must be developed and incorporated into the taxonomy.

7. REFERENCES

[1] Biometric Data Specification for Personal Identity Verification, SP 800-76, **http://csrc.nist.gov/publications/nistpubs/800-76/sp800-76.pdf**

[2] Cryptographic Algorithms and Key Sizes for Personal Identity Verification, SP 800-78**,** **http://csrc.nist.gov/publications/drafts/800-78-1/draft-SP_800-78-1-070306.pdf**

[5] FIPS 201 – Personal Identity Verification of Federal Employees and Contractors**,** **http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf**

[6] Interfaces for Personal Identity Verification. NIST Special Publication SP 800-73-1. http://csrc.nist.gov/publications/nistpubs/800-73-1/sp800-73-1v7-April20-2006.pdf

[7] Kumar, M. New Remote User Authentication Scheme Using Smart Cards, *IEEE Transactions on Consumer Electronics.* Volume 50, Issue 2, May 2004 Page(s):597 - 600

[8] Securing e-business applications using Smart Cards, IBM Systems Journal, Vol 40, Number 3, 2001 - **http://www.research.ibm.com/journal/sj/403/hamann.html**

[9] Technical Implementation Guidance: Smart Card-Enabled Physical Access Control Systems – Version 2.3, **http://smart.gov/iab/documents/PACS.pdf**

[10] Wang, X.,Zhang, J.,Zhang, W.,Khan, M.K., Security Improvement on the Timestamp-based Password Authentication Scheme Using Smart Cards. *In Proceedings of IEEE International Conference on Engineering of Intelligent Systems* April 2006.