Technical Implementation Guidance:

Smart Card Enabled Physical Access Control Systems

Version 2.3

Approved by:

Government Smart Card Interagency Advisory Board

Prepared by:

Physical Access Interagency Interoperability Working Group

December 20, 2005

Executive Summary

Agencies of the United States Federal Government are pervasive users of physical access control systems (PACS). Across the country and around the globe, government employees, civilian contractors, and visitors require access to secured facilities under the control of federal agencies. To date, agencies have procured full systems and system components with little or no central guidance. This has resulted in cost inefficiency and technical incompatibility.

Efforts including the GSA's Government Smart Card Interoperability Specification (GSC-IS) and the Department of Defense's mandate that gave birth to the Common Access Card (CAC) laid the foundation to rectify this situation. With a common credential comes the opportunity to promote interoperability among PACS across federal agencies.

It was determined that the procurement of PACS and components requires a standardized approach to ensure that agencies deploy equipment that meet both their specific needs and, at the same time, facilitate cross-agency interoperability. The Physical Access Interagency Interoperability Working Group (PAIIWG) within the Government Smart Card Interagency Advisory Board (GSC-IAB) is charged with creating and documenting guidance for such an approach.

In this guidance, it is specified that a Federal Agency Smart Credential (FASC), such as a NIST standards compliant Personal Identity Verification (PIV) card, shall have a standardized token identification scheme called the Card Holder Unique Identifier (CHUID) which is to be used as the individual identifier. The CHUID is defined to provide the basis for interoperable identification of individuals and to extend capabilities over magnetic stripe technology for Physical Access Control System applications. It contains a series of mandatory and optional tagged objects. Some of these include the Federal Agency Smart Credential Number (FASC-N), the Global Unique ID (GUID), and the Asymmetric Signature.

The FASC-N provides a point of departure for a migration strategy for current technology and is based on the SEIWG-012 number. The FASC-N is the primary identification string to be used on all government issued credentials. The Federal Government has defined the GUID as a mechanism to enable issuance and acceptance of physical access credentials beyond federal agency participation. The GUID is defined as an IPv6 address and is anticipated to become the standard for credential numbering in federally managed PACS. The Asymmetric Signature mitigates risks of tampering with the credential information written by the issuer.

A range of assurance profiles – low, medium, and high – are associated with an extensible data model on FASC cards. These assurance profiles provide for increasing integrity of the transaction between the card, the reader and the system, enabling assurance that a genuine card is present, and the bearer requesting access is the legitimate individual assigned to the credential, for the access request. Using the methods prescribed for each assurance profile a PACS can function for the intended

purpose, at the adequate level of integrity and security warranted by the specific environment, and facilitate cross-agency interoperability across the population of FASC cardholders. Currently this guidance does not require nor preclude the use of additional authentication factors such as PIN and/or biometric input in conjunction with the FASC card applications. When the use of additional authentication factors is warranted by an application, this guidance recommends including these factors in concert with cryptographic operations.

It should be noted that this guidance is not intended to stipulate or exclude any specific method of communication from the reader to the panel. This guidance recommends a minimum level of security and interoperability between a token, typically a FASC card, and reader. A principal consideration in this guidance is to permit the continued use of existing PACS infrastructure with minimal change, typically reader replacement. This guidance allows partial credential data to be transmitted from the reader to the panel in legacy system upgrades to simplify migration for using FASC cards.

This guidance reflects current U.S. Government technical requirements that supersede specifications in GSC-IS v2.1 identified in Section 5.

1 Introduction

Government agencies in the United States have been making significant strides in the area of secure credentialing for personnel, contractors, and visitors. These efforts are increasing the security of facilities, property, data, and most importantly people. A number of significant technical obstacles have arisen since this credentialing revolution began. Each has been or is being addressed through the dedicated efforts of working groups made up of agency personnel, contractors, and vendor representatives.

For example:

1. A need was identified for a standardized credential that would help agencies procure a card that would meet the goals of the envisioned government-wide interoperability. This issue is addressed through the ongoing work of the National Institute for Standards and Technology (NIST).

2. A need was identified for a standardized approach to the issuance of a Federal Agency Smart Credential (FASC). The effort is addressed in the ongoing work of the Federal Identity Credentialing Committee (FICC) through their document titled “Policy Issuance Regarding Smart Cards Systems for Identification and Credentialing of Employees.”

3. A need was identified for a standardized numbering scheme for use on agency-issued credentials such that a card issued by one agency could be used when that cardholder visits a facility run by another agency. This need is addressed in the ongoing work of the Data Model Working Group under the Government Smart Card – Interagency Advisory Board (GSC-IAB) and FICC.

4. A need was identified for a range of assurance profiles associated with an extensible data model on credential cards. These cards would be used throughout the PACS industry, to include both federal and non-federal deployments. This need is addressed in the ongoing work of the GSC-IAB’s Architecture Working Group.

The dedicated efforts including, but not limited to, those highlighted above establish the groundwork for interoperability at the card level. For practical interoperability in the field, however, a next tier of specifications must be established. The systems in which the card is to operate must be defined such that successful operation is assured. This will enable the vendor community to develop and provide product to meet government-wide needs with reasonable confidence that their efforts will have an opportunity for return. Additionally, it will enable agencies to procure systems with the knowledge that it will operate with the credential.

Two of the most fundamental systems that require such specification are those used for physical access control and those for logical access control. Efforts to recommend logical access systems and technologies are underway in the Office of Management and

Budget's E-Authentication Committee through documents such as "E-authentication Guidance for Federal Agencies. (OMB M-04-04 12-16-2003)"

The procurement of physical access control systems and components requires a standardized approach to ensure that agencies deploy equipment that meet both their specific needs and, at the same time, facilitate cross-agency interoperability. This work is the purview of the Physical Access Interagency Interoperability Working Group (PAIIWG) under the GSC-IAB.

1.1 Purpose of this guidance

The purpose of this guidance is to define specifications and standards required to enable agencies to procure and implement hardware and software for physical access control systems (PACS), such that these systems will:

1. Operate with the Federal Agency Smart Credential (FASC), such as NIST standards based Personal Identity Verification (PIV) cards.

2. Facilitate cross-agency, federal enterprise interoperability.

3. Allow existing legacy PACS to operate with FASC compatible card readers until the time comes for its upgrade.

Representatives from a wide variety of agencies and organizations were involved in the preparation of the ideas and concepts synthesized herein. Groups including National Institute of Standards and Technology (NIST), Department of Defense (DoD), National Aeronautics and Space Administration (NASA), Department of the Interior (DoI), Department of State (DoS), Department of Treasury, General Services Administration (GSA), Department of Transportation (DoT), Department of Homeland Security (DHS), and others have expressed agreement with the concepts put forward. Each step was vetted at an industry day and then brought to a vote by the FICC and Government Smart Card Interagency Advisory Board (GSC-IAB). The GSC-IAB, in cooperation with NIST, has acted as the specification agent and communication link with Industry.

1.2 A scenario for cross-agency interoperability

Through the concepts presented herein along with the work of the various specifying entities, the future of physical access control at federal agencies will look like the following example in which 'Bob' represents a typical cardholder.

1. Bob is issued a FASC card from his employer, Agency A. At the point of issuance, he is enrolled into the physical access control system at his main office location. His card enables him to gain entry to his place of work.

2. Months later, Bob is sent to work on a project at another of Agency A's facilities located in another state. When Bob reports for duty to the new location, the security manager for that location enrolls Bob into the PACS for that facility. Bob can now use his ID card to gain access to the new facility in addition to his original office.

3. In addition, Bob's work finds him on a project team that meets at another agency, Agency B's, facility. The security manager at Agency B enrolls Bob in the PACS and the same credential issued by Agency A now electronically identifies Bob at the control points at Agency B's facility.

In each of these three scenarios, it is anticipated that registering Bob to the PACS involves some combination of the following four basic procedures:

1. Validate the credential Bob presents. Is it valid? Has it been tampered? This may involve using the Asymmetric Signature, physical inspection, expiration verification.

2. Confirm Bob is the correct bearer of the presented credential. This may involve PIN or biometric confirmation to the credential or verification by the issuer.

3. Confirm management authorization for Bob to have access.

4. Bind Bob's CHUID to the PACS system and assign appropriate access rights.

1.3 Summary of this guidance

Until now, the scenario described above was not possible. Procurement and implementation decisions have been decentralized and without guidance. The result is an array of incompatible technologies– card media, data formats, software, card readers and components–among agencies and even facilities within an agency.

This guidance suggests the following successive steps to achieve the level of interoperability among agencies issuing the same credentials.

First, the card media to be used was established. A smart card complying with the ISO/IEC 7816 (contact) and ISO/IEC 14443 (contactless) standards was selected.

Second, a standard numbering is detailed (see Section 2: Card Specifications/Requirements).

Third, a card reader specification is then detailed (see Section 3: Reader Specifications/Requirements). At this point, any PACS following the specifications will be able to locate and read the appropriate data from the credential.

Fourth, a minimum set of data elements maintained in an agency PACS database is specified (see Section 4: Database Specifications/Requirements).

Final sections specify the discrepancies between certain requirements established in this guidance and those specified in the current version of the GSC-IS, outline the challenges and opportunities that this effort creates for the PACS vendor community, and highlight conclusions.

This guidance is not intended to address data model registration and configuration control issues. These issues will be addressed in separate documents.

2 Card specifications, requirements

Across the federal enterprise, the primary point of integration is the card itself. Requisite physical elements are defined in NIST Internal Report (IR) 6887 2003 (GSC-IS v2.1), featuring identification technologies. By using a standardized federal identification number and the industry's most widely accepted standard technologies including contactless smart card, ISO 14443, contact smart card, ISO 7816 and magnetic stripe, ISO 7811, the foundation exists to enable single-credential access control among conforming federal agencies.

The key to credibility, non-repudiation and reciprocity is the definition and acceptance of a credential token identification numbering schema for use across all Federal Agencies that is uniquely assigned to one and only one individual. For deployed systems, this is the FASC-N. For emerging systems, it is the GUID. Both are contained in the CHUID for consistent means of access by PACS solutions allowing for ease of migration. The responsibility for issuing this number to federal personnel is decentralized to the various federal agencies, with the ultimate responsibility for ensuring uniqueness residing with each agency's CIO, or other duly designated agency official. For the FASC-N, this is achieved through an assigned Agency Code and subordinate system code and credential number. For the GUID, it will be a registered IPv6 address allocated to the CIO's office by ARIN (American Registry for Internet Numbers) and unique for every card. If the binding between the cardholder and card is broken in the event that the card is lost, stolen, or destroyed, the same FASC-N is issued. It is being investigated by the PAIIWG whether the FASC-N can be mapped to the low order bits of the GUID for ease of migration. Please refer to Section 6.1 for an overview of the FASC-N construction rules. In Section 6 it is noted that when a Social Security Number (SSN) is used in the FASC-N as the Person Identifier code and other FASC-N identifier fields are set to zero then the FASC-N is exactly the SEIWG-012 definition, which has been in use for over ten years. The FASC-N was constructed to insure legacy compatibility with existing systems that are based on the SEIWG-012 definition.

Physical interface challenges between FASC cards and readers will be addressed by conforming to the GSC-IS v2.1 and/or appropriate NIST standards and supporting special publications. The contactless technology specified in the GSC-IS v2.1 calls for compliance with ISO/IEC 14443 standard parts 1-4. GSC-IS v2.1 Appendix G establishes a requirement for contactless smart cards to provide the ISO 7816-4 commands for Select File and Read Binary and requires that if cryptography is present it must use a FIPS approved algorithm. This guidance and GSC-IS v2.1 do not require that contactless smart card technologies be validated to FIPS 140 at this writing. If the contactless functionality is provided as a secondary interface to a contact Integrated Circuit Chip (ICC) then the contactless functionality will be subject to the same FIPS 140 validation requirements as the contact ICC. Federal agencies may choose to implement contact, ISO 7816 standard, in addition to or in place of contactless smart card technology for PACS deployments. The data model for PACS must be transparently available on both the contact and contactless technology of a FASC card.

This guidance is specific for the PACS data model and does not address other required data elements such as the Card Capabilities Container (CCC) that are required on GSC-IS v2.1 compliant FASC cards and/or NIST standards compliant PIV cards. While it is required that the CCC exist, this guidance recommends specific locations for the PACS data so it may be accessed without first reading the CCC.

2.1 Card Holder Unique Identifier

The Card Holder Unique Identifier (CHUID) is defined to simplify interoperability and to extend capabilities over magnetic stripe technology for Physical Access Control System applications. The CHUID arose from the requirement to extend the number space limitation imposed by maintaining the legacy compatibility of the FASC-N with the SEIWG-012. The CHUID container is an Elementary File (EF) that is a required part of the data model for both separate or combined contact and contactless technology FASC cards.

The mandatory (TLV) records within the CHUID are: FASC-N, GUID, Expiration Date, and Asymmetric Signature. Use of all other fields are optional, determined by issuing agency requirements . When used, optional fields shall be honored per this specification by all agencies.

The FASC-N must always be present in the CHUID EF. If the FASC-N is the only Tag Length Value (TLV) record in the CHUID EF then the Buffer Length TLV header is not expected. If there are multiple TLV records in the CHUID EF then the Buffer Length TLV header as defined in GSC-IS Section 8.3 may exist for file system contact and contactless smart card technologies. The purpose of the Buffer Length TLV header is to allow a reader to determine the overall CHUID length during the first read operation in a device independent manner and is recommended when multiple TLV records exist. This is especially important to reduce transaction times in contactless applications by minimizing the number of required read operations.

The CHUID data model provides an extensible approach for overcoming the limitation of BCD digit encoding when using the NIST Special Publication 800-87 Agency Code in the FASC-N. As several agency codes use alphabetic characters, the CHUID provides a specific tagged field for Agency Code for alphanumeric values. Details are provided in *Section 6.4.*

GSC-IS v2.1 compliant contact-less smart cards are required to power-up such that CHUID EF (0x3000) may be directly addressed by a Select File command as specified in ISO/IEC 7816-4.. As a result, only the FID portion of the AID is required and the RID may be ignored on a contact-less smart card. However, for a contact smart card the RID must be specified. For a file system smart card the CHUID EF must be in the MF 0x3F00 directory and for a Virtual Machine smart card the CHUID EF is appended to RID 0xA000000116 to form the AID for the CHUID. Note: For legacy implementations if the EF (0x3000) is not found then EF (0x0007) should be attempted to accommodate legacy implementations. These legacy implementations are expected to be retired within three years of the publication of this technical implementation guidance.

To accommodate an extensible data model and for simplicity of PACS reader implementation if more than one TLV record exists for the CHUID container, then for both contactless and file system smart cards a TLV record may exist, indicating the length of occupied space of the container as described in GSC-IS Section 8.3.

Federal agencies shall only enroll CHUID credentials that are validated through the issuing agency or where the Agency Code is 9999 indicating the issuer is a non-federal entity. The FASC-N is not designed to insure uniqueness for non-federal issuers. For non-federal issuers additional TLV elements must be specified to insure uniqueness of the FASC. If an Agency Code of 9999 is present in the FASC-N, then the DUNS TLV record in the CHUID container will indicate the identity of the credential issuer. It is anticipated that the Tag 30 TLV record will always exist for industry compatibility for PACS that use the System Code and Credential Number as a credential identifier.

For issuers not defined in SP 800-87, a FASC-N can be constructed using an Agency Code of 9999; however this will not provide uniqueness of the FASC-N for federal agency applications. If a non-federal issuer has a requirement for federal interoperability, then a sponsoring agency may assign a specific System Code(s) to the issuer. When an Agency Code of 9999 is specified an issuer must include an additional TLV record in the CHUID, such as the DUNS, to insure uniqueness of the CHUID. It is the responsibility of the sponsoring agency to maintain records of specific System Code assignments for both internal and external issuers of FASC-Ns.

When cryptographic checksums are computed for the medium and high assurance profiles of the CHUID container TLV records, neither the tag(s) nor the length(s) shall be included when assembling the plain text prior to the cryptographic operation.

For full federal interoperability of a PACS it must at a minimum be able to distinguish fourteen digits (comprised of the agency, system, and credential number) when matching FASC-N based credentials to enrolled card holders. This minimum is to insure uniqueness among all federally issued FASC cards. A fewer number of digits may be matched but uniqueness will not be guaranteed across all FASC card holders. Legacy systems that are unable to support the fourteen digits from FASC-N or the full GUID can not ensure uniqueness of the credential number. These systems must be evaluated for risk according to local security requirements. Agencies should budget to replace these systems.

For new PACS procurements, Agencies should procure systems that grant or deny access based on uniquely reading the agency, system, and credential number of the FASC-N currently and be able to migrate to using an IPv6 address for future implementation of the GUID. Those agencies wanting to use the medium or high assurance profiles should procure systems that are capable of processing and accepting the Hashed Message Authentication Code (HMAC) in addition to the FASC-N field or the GUID (IPv6 address).

The Asymmetric Signature is a mandatory field written by the FASC issuer. It permits validation of the FASC CHUID data with no knowledge of the issuer signing secret. This method may be used in any card assurance profile to provide additional assurance and integrity of FASC CHUID data. Using specified algorithms and key sizes a HMAC is generated, signed and stored in this TLV element with the public part of the issuer signing key pair and algorithm ID.

The proposed structure follows a logical translation of the fields defined for the FASC-N to TLV values based on those fields in the data model format found in GSC-IS 2.1. Please see Figure 1 and Figure 2 below for more information on the CHUID data model and CHUID data element definitions.

Figure 1. CHUID Data Model.

(Card Holder Unique Identifier) CHUID File / Buffer EF 3000 Always Read			
Data Element	Tag	Type	Max. Bytes
Buffer Length	EE	Fixed	2
FASC-N (SEIWG-012)	30	Fixed	25
Agency Code	31	Fixed	4
Organization Identifier	32	Fixed	4
DUNS	33	Fixed	9
GUID	34	Fixed	16
Expiration Date	35	Date (YYYYMMDD)	8
RFU	38-3C		
Authentication Key Map	3D	Variable	512
Asymmetric Signature	3E	Variable	2816
Error Detection Code	FE	LRC	1

Figure 2 CHUID Data Element definitions.

Data Element	Max Bytes	Description
Buffer Length	2	Mandatory TLV record. Exists when a TLV record in addition to the FASC-N exists in the CHUID for contact File System and contact-less smart cards. The Buffer Length TLV record is defined in GSC-IS Section 8.3
FASC-N	25	Mandatory TLV Record. Federal Agency Smart Credential Number is defined in Section 6 of this document
Agency Code	4	Optional TLV Record. Recommended when the SP 800-87 code for the government agency issuing the credential contains alpha characters
Organizational Identifier	4	Optional TLV Record. Recommended when the SP 800-87 code for the FASC-N OI field contains alpha characters
DUNS	9	Optional TLV Record. Recommended when the FASC-N Agency Code = 9999. D&B DUNS number for non-federal FASC-N issuer
GUID	16	Mandatory TLV Record. A registered IPv6 address allocated to the CIO's office by ARIN and unique to the card
Expiration Date	8	Mandatory TLV Record. Card expiration date, YYYYMMDD
Authentication Key MAP	512	Optional TLV Record. May exist for High Assurance Profile applications.
Asymmetric Signature	2816	Mandatory TLV Record. Issuer defined algorithm, public key and signature.
LRC	1	Optional TLV Record Longitudinal Redundancy Code

2.2 CHUID Low Assurance Profile

The Low Assurance Profile does not require or permit an addition to or modifications of any TLV records within the CHUID beyond what is encoded during initial credential issuance. Internal FASC keys are not used to authenticate the FASC card during a PACS access transaction. This mode of operation most closely emulates the operation of a magnetic stripe card.

2.3 CHUID Medium Assurance Profile

The Medium Assurance Profile does not require or permit an addition to or modifications of any TLV records within the CHUID beyond what is encoded during initial credential issuance. Internal FASC keys are not used to authenticate the FASC card during a PACS access transaction.

2.4 CHUID High Assurance Profile

The High Assurance Profile requires the use of token internal cryptographic security functions. These security functions are based on FIPS 140 validated security modules using FIPS approved cryptographic algorithms and require the identification of specific keys since a token may be used in multiple high assurance profiles where each protected area has a different Site Secret Key (SSK) or Site Public Key (SPK). Requirements for FIPS 140 validation of FASC card products are outside the requirements described in this document.

The Authentication Key Map defined in the following subsection provides for the identification of the cryptographic algorithm, key storage location, and other data needed to execute the High Assurance Profile challenge and response.

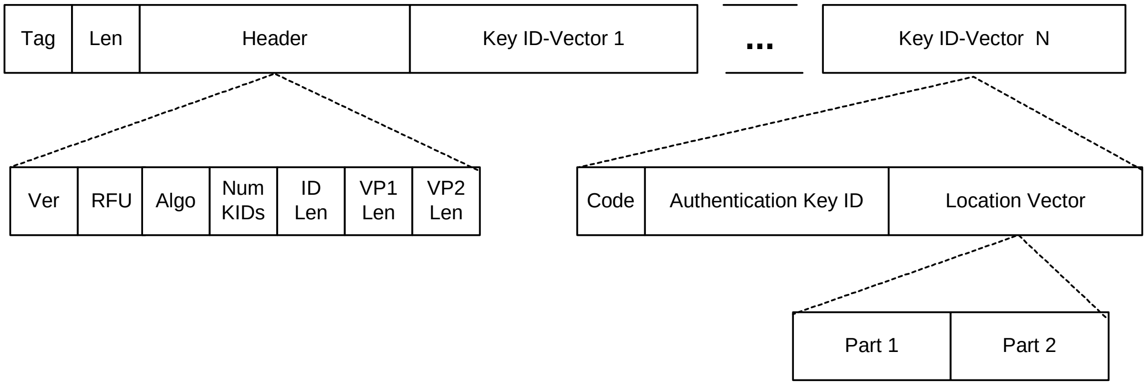
To be compliant, a High Assurance Profile implementation must use the ISO 7816-4 and 7816-8 APDU commands defined in Section 5.1 of GSC-IS v2.1. Currently this means that only contact cards can implement a conformant High Assurance Profile. It is expected that conformant contactless implementations can be fielded once FIPS certified dual interface cards become available. Until that time, any High Assurance Profile implemented on contactless cards will be Agency Specific, and outside the scope of this technical implementation guidance.

Note: there is no prohibition on an Agency using FIPS approved algorithms with vendor specific card edge commands for securing contactless card to reader access transactions, taking advantage of existing proprietary authentication commands for contactless smart cards. Vendor specific implementations, by their very nature, may not be interoperable with future compliant implementations, nor should there be any expectation that these implementations will be compliant in future technical implementation guidance.

2.4.1 Authentication Key Map

An Authentication Key Map Table is used to provide a map between the Agency Key ID and the associated key. This table consists of a structured TLV data record shown in Figure 3. As shown in the diagram, this card-resident table is made up of a header portion plus repeating elements of a key ID and associated vector information, which points to the key location. Defining the key table in this manner provides the flexibility to identify up to 255 keys plus it allows for variations in card types, key lengths, and location identifiers necessitated by different card types (for example, VM, file, and contactless cards).

Figure 4. Authentication Key Map Table (Tag 3D)



Description:

- Tag: The one byte tag for the key map. As defined previously, the value for this tag is 3D.

- Len: Length of entire table definition. The length field is one or three bytes according to the GSC Specification

- Ver: The version number of the Key Map Table, which is currently 1

- RFU: One byte Reserved for Future Use (must be present)

- Algo: A one-byte code indicating the algorithm used to compute the key value. The algorithm codes are specified in Algorithm Identifiers for Authentication APDUs, and included in this document in Section 9, References.

- Num KIDs: One byte binary number that specifies the number of table entries

- ID Len: The length in bytes of the Authentication Key

- Code: A one-byte value that indicates the construction and use of the derived card key according to the following definition (note that bit values are cumulative):

  bit 1: Pin required
  bit 2: Authentication using SEIWG
  bit 3: Authentication using CUID
  bit 4: Authentication using GUID
  bit 5: Reserved
  bit 6: Reserved
  bit 7: Reserved
  bit 8: Reserved

- Authentication Key ID: Key ID of a particular key. Each card may contain multiple authentication keys. The Key ID is used to identify the availability and location of a particular key and tells the card authentication device which key to use for authentication. Key IDs are set up and published through Memorandums of Understanding (MOU) between participating agencies.

- Location Vector: The Location Vector is made up of two parts. Combined, these parts identify the location of the key on the card. For example, with a file system card, part 1 could be the DFID and part two could be the EFID, or the key number depending on the particular card. Java cards may have only part 1 as the application ID. Other combinations are possible.

Each entry in the Authentication Key Map Table points to a unique cryptographic key that is computed based on the Card data Unique Identifier (CUID) and the CHUID. Using standard ISO 7816 methods for challenge-response authentication, these keys can be used to validate the authenticity of the card. In addition, because of the method of calculating each card-unique key, the data used to calculate the key (CUID + CHUID) is validated at the same time. Other data elements could also be included in the calculation to validate these elements as well. Most notably, this could include the user PIN. When the PIN is included in the key calculation, it is not necessary to store the PIN on the card since it is used in the calculation of the challenge-response.

Key computations are outlined as follows:

- A plain-text string is concatenated from the following possible elements (identified by the code element in the Key Map Table):
  - Card Unique Identifier (CUID) + Card Holder Unique ID (CHUID)
  - CUID + CHUID + PIN
  - CUID
  - CUID + PIN
  - GUID
  - GUID + PIN

- A Chain-Block-Cipher CBC is computed for the plain-text string with an initial 8 byte zero vector and a 128-bit Site Secret Key (SSK) using the algorithm specified in the Key Map Table. The result of the computation to this point is the Message Authentication Code used in the Medium Assurance Profile.

- The remaining CBC cycles with the same SSK are completed to generate the cryptographic key to be injected on the token for the key specified in the Key Map.

2.5 Asymmetric Signature

The asymmetric signature field is implemented as a SignedData Type, as specified in *RFC 3852, Cryptographic Message Syntax.* All security objects MUST be produced in Distinguished Encoding Rule (DER) format to preserve the integrity of the signatures within them.

SignedData Type

The processing rules in RFC3852 apply.

m mandatory – the field MUST be present
x do not use – the field SHOULD NOT be populated
o optional – the field MAY be present
c choice – the field contents is a choice from alternatives

Value		Comments
SignedData		
version	m	Value = v3
digestAlgorithms	m	
encapcontentInfo	m	
eContentType	m	id-gsc-is-chuidSecurityObject
eContent	x	It is recommended that issuers not use this field
certificates	m	Issuers shall include only a single X.509 certificate which can be used to verify the signature in the signerInfos field.
crls	x	It is recommended that issuers not use this field
signerInfos	m	It is recommended that issuers only provide 1 signerInfo within thiis field
SignerInfo	m	
version	m	The value of this field is dictated by the sid field. See RFC3852 for rules regarding this field.
sid	m	
issuerandSerialNumber	m	It is recommended that issuers support this field over subjectKeyIdentifier.
subjectKeyIdentifier	c	
digestAlgorithm	m	The algorithm identifier of the algorithm used to

		produce the hash value over encapsulatedConetnt and SignedAttrs.
signedAttrs	m	Issuers may wish to include additional attributes for inclusion in the signature, however these do not have to be processed by receivers except to verify the signature value.
signatureAlgorithm	m	The algorithm identifier of the algorithm used to produce the signature value, and any associated parameters.
signature	m	The result of the signature generation process.
unsignedAttrs	o	Issuers may wish to use this field, but it is not recommended and receivers may choose to ignore them.

CHUID Security Object

The `chuidSecurityObject` is outlined as follows:

Key computations are outlined as follows:

- A bit-wise string is concatenated from the data found in the following TLV elements:
    - FASC-N
    - Agency Code (if present)
    - Organization Identifier (if present)
    - DUNS (if present)
    - GUID
    - Expiration Date
- A Message Authentication Code is computed on this string using the `digestAlgorithm` specified in the `SignedData` object.

Note: The `signature` is calculated on the resulting message authentication code using the `signatureAlgorithm` specified in `SignedData` object. This signature is *not* part of the CHUID security object. It is part of the `SignedData` object.

3 Reader specifications, requirements

Equipped with a standardized credential, the cardholder is now ready to initiate an access transaction with a Physical Access Control System (PACS). The assurance profile relating to an access control transaction is classified as low, medium or high. The same credential can be utilized for low and medium assurance profiles without site-specific information stored on the credential. For the high assurance profile a Site Secret Key (SSK) must be used to compute the credential site-specific diversified key which is injected into the credential at the key location specified in the Key Map TLV record in the CHUID EF.

It is important to note that elements within this guidance are intended to describe and specify the transaction between card and reader. Specifications and requirements pertaining to interaction between reader and PACS panel and beyond are manufacturer-specific and are reviewed and approved by the PACS system manager.

3.1 Decoding the CHUID

Physical Access Control card readers must, at a minimum, extract unique token identifier information from the smart card. Readers may be required to perform or participate in validation checks on that information through cryptographic verification and/or challenges with the card. The specific token information and checks used are determined by a combination of the data needed by the access control system the reader is attached to, and the level of confidence/risk that system is configured to enforce.

The unique elements readily available for physical access use in the CHUID are either the first three fields of the FASC-N (with corresponding Agency Code and DUNS tags from the CHUID) or the GUID. The elements supporting validation checks are the Expiration Date, Authentication Key Map, and Asymmetric Signature.

The processing of the FASC-N, GUID and Asymmetric Signature are consistent, regardless of the assurance level profile selected.

3.1.1 Decoding the FASC-N

A PACS may use the FASC-N structure for the unique token identifier.

The reader shall read the Agency Code, System Code and Credential Number from the FASC-N as the basis of the unique token identifier, forming 14 BCD digit number. PACS should use this entire number if possible. No other values within the FASC-N should be used to form the unique token identifier.

For deployed implementations that cannot recognize 14 digit identifiers, the System Code and Credential number should be concatenated together forming a combined 10 BCD digits. This guidance does not recommended that PACS should rely solely on the 6 BCD digit Credential Number.

If the Agency Code is 9999, the reader may provide an option to the PACS to read the DUNS TLV field and combine that with the System Code and Credential Number to form the basis of the unique token identifier.

3.1.2 Decoding the GUID

If the GUID is present and non-zero, readers should use this value as the unique token identifier. The GUID is a 16 byte (128 bit) value. It should be used in its entirety if the PACS is capable of supporting this length.

Facilities may elect to use the low order bits or some calculation based on the GUID if the PACS is not capable of supporting this length. If this is done, the local facility must recognize the risk that the credential numbers may not be unique and there is a possibility of seeing two different individuals with the same locally registered partial credential number. It is up to the local facility to manage this risk. Facilities should consider managing their investment and upgrade strategy to enable use of the entire GUID as early as practical.

3.1.3 CHUID Validation Checks

CHUID assurance profiles are used only to authenticate the FASC at a PACS point of entry (i.e. access control point). The FASC is only one factor of Identity Authentication, something you have. The FASC can be used alone or in combination with the other two factors of Identity something you know, PIN, and something you are, biometrics.

The reader should provide options to a local facility that enables credential validation checking. If the Asymmetric Signature does not verify, it should be rejected by the reader.

If a credential is being used after the Expiration date has passed, it should be rejected by the reader. This level of validation checking may be done by the PACS instead of the reader, shutting access privileges off for credentials that it knows to be expired based on initial registration of the token to the system.

3.2 Low Assurance Profile

A unique identifier (e.g. credential number) is read from the card and passed to the access control system. No validation, authentication or cryptographic checks are done.

The reader output mode is set to match the controller input.

1. The transaction begins as the cardholder presents the credential to a reader.

2. The reader initializes the credential and retrieves the CUID.

3. The reader Selects File FID 0x3000, if not found for legacy implementations FID 0x0007 is attempted.

4. The reader Read Binary Length equals 27 bytes.

5. If the first tag is EE (container byte 0) then the next byte (container byte 1) will always be 0x02, indicating the Length of the CONTAINER LENGTH value, followed by 2 bytes of actual CONTAINER LENGTH. The remaining number of bytes to read from the container is computed using the container length value in container bytes 2 (LSB) and 3 (MSB) of the Buffer Length TLV Record.

6. The reader decodes the FASC-N TLV record and may extract the Agency Code, System Code, Credential Number, Credential Series and Individual Credential Number. The reader transmits data in a method prescribed by the security system panel manufacturer that may include the entire FASC-N or all or part of selected elements of the FASC-N.

3.3 Medium Assurance Profile

The Medium Assurance profile is designed to confirm that a credential presented to a reader has not been modified since it was initially presented to the system during enrollment. When registering the credential to the system, an HMAC is calculated and stored in the PACS system along with or in addition to the credential for the individual. When the credential is presented at a reader, the reader re-constructs this HMAC using the security keys. If the PACS system sees the same HMAC as defined in the access record, there is a reasonable assurance that the credential has not been altered or duplicated.

The reader is configured with the Site Secret Key or Site Public Key and the output mode is set to match the controller input.

1. The cardholder presents the credential to a reader - the transaction begins.

2. The reader initializes the credential and retrieves the CUID.

3. The reader Selects File FID 0x3000. , if not found for legacy implementations FID 0x0007 is attempted.

4. The reader Read Binary Length equals 27 bytes.

5. If the first tag is EE (container byte 0) then the next byte (container byte 1) will always be 0x02, indicating the Length of the CONTAINER LENGTH value, followed by 2 bytes of actual CONTAINER LENGTH. The remaining number of bytes to read from the container is computed using the container length value in container bytes 2 (LSB) and 3 (MSB) of the Buffer Length TLV Record.

6. If the remaining number of bytes to read is “not zero” then the remaining bytes of the CHUID are read.

7. A bit-wise string is concatenated from the CUID + values from TLV elements present with Tags 30-39 with values ordered by increasing tag value. Null strings are not permitted for either the CUID or FASC-N. Only the values from the CHUID not the tags or lengths are included in the plain-text string. The reader using a site specified algorithm computes a Hashed Message Authentication Code (HMAC). For systems where the panel is designed to perform cryptographic operations the reader may omit this step and simply pass the data to the panel.

8. The reader decodes the FASC-N TLV record and may extract the Agency Code, System Code, Credential Number, Credential Series and Individual Credential Number. The reader transmits data in a method prescribed by the security system panel manufacturer that may include the entire FASC-N or all or part of selected elements of the FASC-N and all or part of the computed HMAC as determined by the PACS implementation.

3.4 High Assurance Profile

The High Assurance profile requires that a credential presented to the system must be capable of a full, cryptographic mutual authentication protocol.

The Profile is processed according to the data model present in the CHUID. In accordance with section 2.4 of this document this section applies to conformant contact cards.

The reader is configured with one or more Site Secret Keys matched to a global Agency Key ID entry. Because there is no universal credential number format for physical access control system (PACS) vendors, each reader is configured to match its output to the requirements of the PACS panel.

1. The cardholder presents the credential to a reader - the transaction begins.

2. The reader initializes the credential (Answer to Reset or Request for Answer to Select) and retrieves the CUID.

3. The reader selects the appropriate security container.

4. The reader reads the appropriate data required to calculate the challenge-response authentication. Depending on the nature of the required authentication this may include any of the CHUID, CUID, PIN, or other data. The optional tag EE may be used to determine the length of the buffer; however, for single container card structures (i.e. where the length and values are not in separate buffers) this tag is not necessary.

5. The reader decodes the TLV and extracts the Agency Code, System Code, Credential Number, Credential Series and Individual Credential Number from the FASC-N.

6. The reader retrieves the Authentication Key Map Table from the card. If the Authentication Key Table Map TLV Record does not exist or match cannot be found in the table for any of the reader's secure keys, then the access mode reverts to medium level security, however, the system may be configured not to accept this method.

7. A plain-text string is concatenated from the following possible elements (identified by the code element in the Key Map Table):

    - Card Unique Identifier (CUID) + Card Holder Unique ID (CHUID)

    - CUID + CHUID + PIN

    - CUID

    - CUID + PIN

    - GUID

- GUID + PIN

8. A Chain-Block-Cipher CBC is computed for the plain-text string with an initial 8 byte zero vector and a 128-bit Site Secret Key (SSK) using the algorithm specified in the Key Map Table. The result of the computation to this point is the Message Authentication Code used in the Medium Assurance Profile.

9. The remaining CBC cycles with the same SSK are completed to generate the cryptographic key injected on the token for the key specified in the Key Map.

10. At this point, the generated key should match the identified key stored on the card. A challenge-response is used to authenticate the card key as follows: A random number (challenge) is sent to the card. The card computes a cryptogram using the identified secret key and sends this cryptogram to the reader. The reader computes its own cryptogram using its key and the same random number. If the two cryptograms match, the card and data have been authenticated.

11. The credential number is extracted from the CUID or CHUID as is appropriate to the PACS and sent to the panel.

4 Database specifications, requirements

The Physical Access Control System (PACS) receives and compares the output from the readers to determine if access will be granted. Access is granted based on both the successful authentication of the credential and authorization to enter the requested area. The output of the reader, depending on the assurance profile, may include a Message Authentication Code (MAC). For the medium and high assurance profiles the MAC stored in the PACS database may be generated either with an integral credential issuing feature of the PACS or by a separate external card issuing capability. In either case the MAC generation requires knowledge of the specific Site Secret Key. The PACS may audit attempted use of a credential when authentication fails in the medium and high assurance profiles since a portion of the data is transmitted in the clear that is derived from the plain-text FASC-N.

A user may have more than one MAC for a given site, but only one MAC will match a specific Site Secret Key. The complexity is significantly increased for PACS that enables multiple Site Secret Keys for a single combined Agency and System Code since all combinations of the credential and reader/panel duplicate Agency and System Code combinations must be attempted.

It is highly desirable that the SSK only be maintained in Hardware Security Modules (HSMs) by the PACS system and within a SAM module for access control readers. It is also necessary to transport the SSK to each reader used in Medium and High Assurance Profiles. The only practical means of transporting the SSK to readers without uplink capability are with a specially programmed token or replacement of the SAM module. It is highly desirable to maintain SSKs via a secure electronic upload to the readers.

The Defense Cross-Credentialing Identification System (DCIS) is available for the purpose of verifying the validity of an individual’s identity. Results to DCIS queries will offer only a positive or negative response. DCIS queries are performed only during credential enrollment and at other times not related to access control checks when a token is presented to a reader.

5 Differences from the current GSC-IS 2.1 specification

The efforts to develop an interoperable PACS environment have brought to bear a number of discrepancies between this guidance and the current GSC-IS 2.1 (NISTIR 6887). This section identifies these items such that they might be considered for amendment in the next revision of the GSC-IS. Non-conforming items include:

5.1 GSC-IS v2.1 Appendix C

GSC-IS Appendix C	Specification in this Guidance
All references to SEIWG	FASC-N
Access Control	CHUID
Maximum Length 59	Maximum Length TBD
Access Control File/ Buffer	CHUID File / Buffer
SEIWG Data	FASC-N Data
Max Bytes 40	Max Bytes 25
PIN (TLV)	Removed
Domain (TLV)	Removed

5.2 GSC-IS v2.1 Appendix D

GSC-IS Appendix D	Specification in this Guidance
SEIWG	CHUID
EF 0007	EF 3000
Max Bytes 41	Max Bytes TBD
SEIWG File / Buffer	Removed

5.3 GSC-IS v2.1 Appendix G.3

GSC-IS Appendix G.3	Specification in this Guidance
SEIWG File/ Buffer	CHUID File / Buffer
EF 0007	EF 3000
SEIWG Data	FASC-N Data
Max Bytes 40	Max Bytes 25

5.4 Rationale for changes

For a credential to interoperate between agencies, a common numbering scheme is required. Looking across the federal government, one numbering scheme that was used pervasively was the Department of Defense's SEIWG-012. It was defined by the Security Equipment Integration Working Group (SEIWG) for use across all branches of the military.

It was determined that the SEIWG-012 number should serve as the basis for the definition of a new number to be used across all agencies of the federal government. The new number is called the Federal Agency Smart Credential - Number (FASC-N) to eliminate confusion with legacy systems that implemented SEIWG-012 and make use of the SSN data element.

The FASC-N and its predecessor the SEIWG-012 consist of the same number of characters. The only change is that the 9-digit Social Security Number is eliminated from the FASC-N and the 7-digits of unused "Reserved" space from the SEIWG-012 are used in the FASC-N. This total of 16-digits is filled with a Person Identifier (10-digits), Organizational Category (1-digit), Organizational Identifier (4-digits), and Person / Organization / Association Category (1-digit).

GSC-IS v2.1 specifies a maximum of 40 bytes for storing the SEIWG data while this guidance specifies a maximum of 25 packed bytes of data for storing the full FASC-N (SEIWG) data.

The FASC-N consists of 32 numeric characters of meaningful data. In addition, it contains a single numeric character called the Longitudinal Redundancy Check (LRC) that serves as a means by which a reader can mathematically validate its reading of the preceding data. In keeping with the accepted practices for magnetic stripe reading, the FASC-N shall include 7 additional characters that tell a magnetic stripe reader where meaningful data begins and ends as well as where blocks of data within the string of numbers are separated.

Data on the FASC-N is encoded using a process called Binary Coded Decimal (BCD). It uses 5 bits per character (4 data bits and 1 parity bit) and results in a 16-character set. Encoding the full 40-character FASC-N in BCD digit format results in 200 bits of information. Rather than transmit the data one character at a time, the data can be packed such that each transmitted byte contains 8 meaningful bits (e.g. the full 5 from Character One plus the first 3 from the Character Two). These 200 bits can thus be transmitted in the form of 25 bytes (200 bits divided by 8 bits per byte). Thus the 40-character FASC-N becomes a 25-byte BCD encoded transmittal. For more details on the makeup of the FASC-N, refer to Section 6.1.

6 Federal Agency Smart Credential – Number (FASC-N)

The FASC-N is a BCD credential number definition that maintains transparent interoperability with the SEIWG-012 credential number but redefines the use of the SEIWG-012 SSN and Reserved fields. Most systems do not use the last 16 digits of the SEIWG-012 credential number format during an access control authorization transaction and would be unaffected by this redefinition.

In the *Technical Implementation Guidance – Smart Card Enabled Physical Access Control Systems* – Final Version 1.0 dated 2 July 2003 a “New SEIWG Number Format” is defined in Appendix A – Credential Number Content and File Specification. This specification redefines the nomenclature of the SEIWG-012 credential for certain fields for new DoD Physical Access Control System deployments. To avoid confusion with the existing use of the SEIWG-012 credential number format the “New SEIWG Number Format” will be known herein after as the Federal Agency Smart Credential – Number (FASC-N). The overall structure of the FASC-N, including the credential size and the relative positions of the SS, five FSs, ES and LRC are unchanged from the SEIWG-012 credential number format. The entire FASC-N, a total of 40 characters, is encoded as described below for the SEIWG-012 credential number as a 200 bit (25-byte) record. The only difference between the SEIWG-012 and the FASC-N credential number is the use definition of the BCD digits between the last FS and the ES as described below.

6.1 FASC-N Data Elements

In the FASC-N the Agency Code, System Code and Credential Number, Credential Series, and Individual Credential Issue are defined exactly as in the SEIWG-012 credential number. Some systems refer to the Credential Series as the Series Code and the Individual Credential Issue as the Credential Code; the functional use of these field definitions remains unchanged. The next 16 digits are defined as described. The only incompatibility that could arise is when a system requires a SSN following the fifth FS. Most systems determine access control authorization based only on the system code and credential number and disregard the remaining digits, therefore these systems are unaffected by the redefinition of the SSN field. The use of the SSN in either the SEIWG-012 credential number or FASC-N Personnel Identifier is strongly discouraged to minimize risks of unauthorized SSN disclosure during access control transactions. It should also be noted that population of the PI field can lead to the same types of Privacy Act and Identity Theft issues. The FASC-N is comprised of a total of 40 characters encoded as BCD digits as shown below.

Figure 5. Federal Agency Smart Credential – Number (FASC-N).

SS	**AGENCY CODE**	FS	**SYSTEM CODE**	FS	**CREDENTIAL NUMBER**	FS	**CS**	FS	**ICI**	FS	**PI**	**OC**	**OI**	**POA**	ES	LRC

Figure 6. FASC-N field definitions.

Field name	Length (BCD digits)	Field description
AGENCY CODE	4	Identifies the government agency issuing the credential
SYSTEM CODE	4	Identifies the system the card is enrolled in and is unique for each site
CREDENTIAL NUMBER	6	Encoded by the issuing agency. For a given system no duplicate numbers are active
CS	1	CREDENTIAL SERIES (SERIES CODE) Field is available to reflect major system changes
ICI	1	INDIVIDUAL CREDENTIAL ISSUE (CREDENTIAL CODE) Recommend coding as a "1" always
PI	10	PERSON IDENTIFIER Numeric Code used by the identity source to uniquely identify the token carrier. (e.g. DoD EDI PN ID, TWIC credential number, NASA UUPIC)
OC	1	ORGANIZATIONAL CATEGORY 1 - Federal Government Agency 2 - State Government Agency 3 - Commercial Enterprise 4 - Foreign Government

OI	4	ORGANIZATIONAL IDENTIFIER
		OC=1 – NIST SP800-87 Agency Code
		OC=2 – State Code
		OC=3 – Company Code
		OC=4 – Numeric Country Code

POA	1	PERSON/ORGANIZATION ASSOCIATION CATEGORY 1 – Employee 2 – Civil 3 – Executive Staff 4 – Uniformed Service 5 – Contractor 6 – Organizational Affiliate 7 – Organizational Beneficiary
SS	1	Start Sentinel. Leading character which is read first when card is swiped
FS	1	Field Separator
ES	1	End Sentinel
LRC	1	Longitudinal Redundancy Character

6.2 ISO 7811/2 Encoding

DoD Specification SEIWG-012 Magnetic Stripe Coding (MSC) does not itself specify an encoding schema. Rather, it refers to ISO 7811/2–1985, Identification Cards – Recording Technique Part 2 Magnetic Stripe, of which the applicable sections are 8.2, 9.2.2, 11.1 and 11.2. The ISO 7811 encoding scheme uses BCD 4 bit code with odd parity. This method is retained for the FASC-N to ensure backward compatibility as noted in Section 5.4. Coding is least significant bit first and parity bit last, as shown in Figure 7:

The value of the Parity Bit for each character is defined such that the total quantity of 'one' bits recorded for a character, including parity bit, shall be odd. The Longitudinal Redundancy Check Character uses the same bit configuration as the data characters, and is calculated as follows:

The value of each bit in the LRC character, excluding the parity bit, is defined such that the total number of one bits encoded in the corresponding bit location of all characters of the data message, including the start sentinel, field separators, data, end sentinel, and LRC character shall be even. The LRC parity bit is for the LRC character itself, and is calculated as described in the preceding paragraph.

Thus, the 40-character FASC-N credential is encoded as a 200 bit (25-byte) record.

Figure 7. Packed BCD 4-Bit Decimal Format with Odd Parity.

B0	b1	b2	b3	Parity	Corresponding character
0	0	0	0	1	0
1	0	0	0	0	1
0	1	0	0	0	2
1	1	0	0	1	3
0	0	1	0	0	4
1	0	1	0	1	5
0	1	1	0	1	6
1	1	1	0	0	7
0	0	0	1	0	8
1	0	0	1	1	9
1	1	0	1	0	Start Sentinel
1	0	1	1	0	Field Separator
1	1	1	1	1	End Sentinel

(Note this table is modified from that used in ISO 7811/2 Section 9.2.2 Table 2 in order to provide better readability of the left-to-right layout used in the examples that follow)

6.3 FASC-N Encoding on Smart Cards

There is no specification or standard for encoding magnetic stripe formats on digital media. In order to ensure the greatest compatibility with existing algorithms and encoding programs, the ISO 7811 bit-wise schema described above will be used for encoding FASC-N onto the digital media of smart cards. That is, the bits will be encoded on the card in the same manner in which it's done on a magnetic stripe credential, so that the transmission of bits from a smart card will be identical to that from a magnetic stripe. This provides the greatest compatibility with legacy systems and existing infrastructure.

Example

The following two figures show how the 40 character FASC-N credential would be encoded as a 200 bit string. The least significant bit of the Start Sentinel would be encoded on/transmitted from the card first (as the most significant bit of the first byte outputted), and the parity bit of the LRC would be encoded/transmitted last (the least significant bit of the 25th byte). Figures 8 and 9 show the binary data stream, Start Sentinel (left) to LRC (right).

Figure 8. FASC-N data as it is stored on the card.

1101000001000011100101000**10110**00001000010000110000**10110**000011001101000
001000010001101**10110**00001**10110**10000**10110**100001000010000010000100001000
1100111001110011100110000010000100011001010000**11111**11100

Figure 9. FASC-N parsed by Character.

11010	00001	00001	11001	01000	**10110**	00001	00001	00001	10000	**10110**
SS	0	0	3	2	FS	0	0	0	1	FS
00001	10011	01000	00100	00100	01101	**10110**	00001	**10110**	10000	**10110**
0	9	2	4	4	6	FS	0	FS	1	FS
10000	10000	10000	01000	01000	01000	11001	11001	11001	11001	10000
1	1	1	2	2	2	3	3	3	3	1
10000	01000	01000	11001	01000	**11111**	11100				
1	2	2	3	2	ES	7				

Figure 10. FASC-N Data elements.

AGENCY CODE = 0032
SYSTEM CODE = 0001
CREDENTIAL# = 092446
CS = 0
ICI = 1
PI = 1112223333
OC= 1
OI=1223
POA=2

LRC = 7

6.4 Agency Code

The Agency Code numbering assignment is defined by SP 800-87 in accordance with the limitation described below. The U.S. Census Bureau in the Department of Commerce is responsible for maintaining the number assignments in SP 800-87. Any changes to SP 800-87 should be submitted to the National Institute of Standards and Technology (NIST), Mail Stop 8930, Gaithersburg, MD 20899.

The purpose of the SP 800-87 for Agency Code assignments is to provide a hierarchal, managed and unique number assignment to individuals. The use of SP 800-87 code provides the numbering assignment for the top level of the numbering hierarchy for the issuing agency. An individual may have multiple fully qualified numbers consisting of an Agency Code + System Code + Credential Number assigned, but a given fully qualified number shall only be assigned to a single individual.

The assignments of Agency Codes are made only to U.S Government Agencies. Authority to issue System Code and Credential Number assignments, subordinate to an Agency Code, may be delegated by a Chief Information Officer (CIO) to internal Agency officers or non-U.S. Government entities. Under the assigned Agency Code the CIO may not delegate the responsibility for Agency policy ensuring unique fully qualified number assignment to individuals.

Non-federal agencies may issue credentials using Agency Code 9999 within the FASC-N as defined in *section 2.1*.

6.4.2 Limitation of SP 800-87 for Agency Code Assignments

The FASC-N encoding may only use BCD digits. The SP 800-87 codes are four character positions in length and include numeric in all four positions as well as alpha characters in the last two positions. The alpha characters cannot be BCD encoded in the SEIWG-012 credential number or FASC-N; therefore not all SP 800-87 codes can be represented in the FASC-N.

This limitation is overcome by using the SP 800-87 number assignment for the Agency Code of the superior organization when an alpha character appears in the organization's SP 800-87 number assignment. For example, the SP 800-87 code for the Department of Defense is 9700, and the SP 800-87 code for the Defense Logistics Agency is 97AS. In this case the Defense Logistics Agency would use the SP 800-87 code for its superior organization, namely 9700 for the Department of Defense. The CIO for the Department of Defense would delegate issuing authority for a specified System Code or range of System Codes to a designated officer in the Defense Logistics Agency under the Agency Code of 9700.

The SEIWG-012 credential number and FASC-N encoding accommodate number assignments only under the authority of an issuing U.S. Government Agency. This permits the assignment of a SEIWG-012 credential number or FASC-N to non-

Government individuals, but only under the authority of an issuing U.S. Government Agency. All other SEIWG-012 credential number and FASC-N assignments are non-interoperable.

6.5 System Code

In order to insure uniqueness of the fully qualified number assignment the System Code number assignment is the responsibility of the CIO for the organization referenced by the Agency Code. The authority to assign a single and blocks of System Codes may be delegated by the CIO.

Agency CIOs are responsible for ensuring non-overlapping System Codes are issued for all interoperable systems issuing SEIWG-012 credential number or FASC-N codes within their Agency.

The combination of each Agency Code and System Code permit one million unique fully qualified numbers. If a particular issuing system requires more than one million credentials issued then that system would require an additional system code assigned corresponding to each million credentials that will be issued by that system.

6.6 Credential Number

In order to insure uniqueness of the fully qualified number assignment the Credential Number assignment is the responsibility of the CIO for the organization referenced by the Agency Code. Under the assigned Agency Code the CIO may not delegate the responsibility for Agency policy ensuring unique fully qualified number assignment to individuals. The authority to assign Credential Numbers may be delegated by the CIO.

Agency CIOs are responsible for insuring non-overlapping Credential Numbers are issued for all interoperable systems issuing FASC-N codes within their Agency.

The combination of an Agency Code, System Code and Credential Number is a fully qualified number that is uniquely assigned to a single individual.

7 Global Unique Identifier (GUID)

The Global Unique Identifier (GUID) is a 16-byte (128 bit) registered IPv6 address in accordance with RFC 2373. It is unique to each card token, and is taken from the allocation pool given to an Agency's CIO office by ARIN (American Registry for Internet Numbers).

It is being investigated by the PAIIWG whether the FASC-N can be mapped to the low order bits of the GUID for ease of migration.

Implementation of GUID in lieu of the FACS-N will:

- Ensure absolute uniqueness of credential numbers across all potential user populations – Federal, State, Local, Commercial (contractors) and international.
- Separate person identifiers from token identifiers, forming the foundation for enforcement of personal data access rules and the protection of cardholder privacy, both on the card and in system back ends.

8 Definitions:

BDC	-	Binary Coded Decimal
CHUID	-	Card Holder Unique Identifier
CSP	-	Credential Service Provider
CUID	-	Card Unique Identification Number
FASC	-	Federal Agency Smart Credential
FASC-N	-	Federal Agency Smart Credential Number
FICC	-	Federal Identity Credentialing Committee
GSC-IAB	-	Government Smart Card Interagency Advisory Board
GSC-IS	-	Government Smart Card Interoperability Specification
GUID	-	Global Unique Identification Number
NIST	-	National Institute for Standards and Technology
PACS	-	Physical Access Control System

PAIIWG	-	Physical Access Interagency Interoperability Working Group
SSK	-	Site Secret Key
TLV	-	Tag Length Value

9 References:

Algorithm Identifiers for Authentication APDUs

Algorithm Identifier	Algorithm-Mode	Key Length in Bits
0x00	3 Key Triple DES-ECB	192
0x01	2 Key Triple DES-ECB	128
0x02	2 Key Triple DES-CBC	128
0x03	3 Key Triple DES-ECB	192
0x04	3 Key Triple DES- CBC	192
0x05	RSA	3027
0x06	RSA	1024
0x07	RSA	2048
0x08	AES-ECB	128
0x09	AES-CBC	128
0x0A	AES-ECB	192
0x0B	AES-CBC	192
0x0C	AES-ECB	256
0x0D	AES-CBC	256
0x0E	ECC: Curve P-244	244
0x0F	ECC: Curve K-233	233
0x10	ECC: Curve B-233	233
0x11	ECC: Curve P-256	256
0x12	ECC: Curve K-283	283
0x13	ECC: Curve B-283	283