Smart Card Alliance

Recommendation on the Credential Numbering Scheme for the FIPS 201 PIV Card Global Unique Identifier

A Smart Card Alliance Physical Access Council White Paper

Publication Date: March 2009

Publication Number: PAC-09001

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

Table of Contents

Executive Summary

The Smart Card Alliance has published a number of white papers on the value of high assurance, interoperable identity credentials based on Federal Information Processing Standard (FIPS) 201. There are three issues within FIPS 201 that non-federal government entities cannot comply with:

1. The Federal Agency Smart Credential Number (FASC-N) schema is limited to federal agencies.
2. There is no definition for a commercial equivalent to the National Agency Check with Inquiries (NACI) for identity proofing.
3. The Federal Public Key Infrastructure (PKI) Common Policy cannot be used outside of the federal government.

This paper discusses the first issue and provides a credential numbering schema that will work for federal as well as non-federal issuers.

In the current Personal Identity Verification (PIV) card data model, there is a reserved space for a Global Unique ID (GUID). The Smart Card Alliance Physical Access Council (PAC) recommends that the best option for generating and populating the GUID field is defined in the Internet Engineering Task Force (IETF) Request for Comments (RFC) 4122. RFC 4122 defines a method that provides a globally-unique, 128-bit number that fits in the reserved space of the GUID.

The GUID addresses numbering as managed by the *issuer* of the credential, not the *relying party*, such as a physical access control system (PACS) or a local network. This paper proposes that additional work should be done on mutual registration for PIV. This mutual registration process will allow the GUID to be registered with a PACS system so that the credential can be given a local credential number and other attributes, potentially including an authentication key or Internet Protocol version 6 (IPv6) address.

Requirements for the GUID

This paper presents a proposal by the Smart Card Alliance Physical Access Council (PAC) on the population of the GUID field found within the Cardholder Unique ID (CHUID) of a PIV card. Past industry submissions to the Physical Access Interagency Interoperability Working Group (PAIIWG), as early as April 2004, recommended that the GUID be in IPv6 address format. The intent was to have an industry-standard numbering schema that is not owned by the federal government, yet yields a number space large enough to avoid collisions within and between domains.

Over time, working committees for FIPS 201 sought a desirable end state for a PIV card to be IP addressable. This would enable protocols like Transport Layer Security (TLS) and environments like full Java with Remote Method Invocation (RMI) mechanisms to operate easily. Hence several agencies see value in IPv6 as the target addressing schema, reinforcing the desire to have the GUID be an IPv6 address.

The data model for PIV is defined within NIST SP800-73 and provides the foundational definitions for the GUID. NIST SP800-73-2 Part 1, Section 3.1.2 specifies the GUID as follows:

> "The Global Unique Identifier (GUID) field must be present, and may include either an issuer assigned IPv6 address or be coded as all zeros. The GUID is included to enable future migration away from the FASC-N into a robust numbering scheme for all issued credentials."

During development of the "Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems" (TIG SCEPACS) v2.3 document and discussions related to the data model for PIV, members of the community involved received an email from the IETF that contained the following:

> "… Concerns have been raised by members of the American Registry for Internet Numbers (ARIN - www.arin.net) membership and the IETF on the use of an IPv6 address as the Globally Unique Identifier within the smart card. …
>
> … Generally, the IETF has been trying to discourage the use of IP addresses (IPv6 and IPv4) as anything other than the location of an endpoint within an IP network. Given that, the definition of the GUID as an IPv6 address raises some concerns. …"

This communication triggered a great deal of discussion within the PAIIWG community and resulted in a search for a new numbering schema for the GUID. In studying this issue, some key points have come to light that describe the challenges. Fundamentally, IP network addresses belong to the network operator (the relying party), not to the manufacturer of the network adapter (the issuer) that connects to the network. IP addresses are *dynamically assigned numbers* that are ephemeral for the duration of a network connection. Media Access Control (MAC) addresses, though, are assigned by the network adapter manufacturer and are *static* to the device, staying with the adapter for its useful life. In an IT network, protocols such as Dynamic Host Control Protocol (DHCP) are used to make a mapping between a network adapter's MAC address and the local IP address required to communicate in that particular network. The assignment of the IP address is specific for the network node the device is connected to.

The Global System for Mobile (GSM) communications has a very similar model to DHCP, enabling a mobile phone to roam. Each phone has a unique hardware number assigned to it, called the International Mobile Subscriber Number (IMSI). When that phone is roaming, a temporary number is assigned to communicate with the local network. This assignment is temporal and when that phone returns from roaming, it is no longer used.

Based on these two operational models, the members of the PAC believe a ***two number architecture*** is required:

- A *static* number, the GUID, that is assigned by the issuer of the credential (Identity Authority).
- A *dynamic* local ID number assigned by the relying system granting an access authorization to the legitimate user of the credential through a protocol analogous to DHCP.

This paper proposes a new numbering scheme for the GUID based on available standards to mitigate the identified issues with IP addresses. It also discusses potential methods for acquiring the dynamic local ID number for relying systems using the credential. It is critical to note that this local ID number *may* be an IPv6 address, as determined by that local system's operational requirements.

In summary, the following are critical requirements that have been identified for the GUID. The schema must:

- Be agnostic to the need for a registration authority (name space management authority),
- Not require the government, or any issuing party, to own the numbering scheme for centralized management of the namespace, and
- Provide a sufficiently large number space to credential all possible populations with a statistically insignificant risk of collision.

Proposal for the GUID

A standard that seems suitable for use as the GUID that is widely used within the Internet is RFC 4122 (quoted below):

> "RFC 4122
>
> A Universally Unique IDentifier (UUID) URN Namespace
>
> Abstract
>
> This specification defines a Uniform Resource Name namespace for UUIDs (Universally Unique IDentifier), also known as GUIDs (Globally Unique Identifier). A UUID is 128 bits long, and can guarantee uniqueness across space and time. UUIDs were originally used in the Apollo Network Computing System and later in the Open Software Foundation's (OSF) Distributed Computing Environment (DCE), and then in Microsoft Windows platforms.
>
> This specification is derived from the DCE specification with the kind permission of the OSF (now known as The Open Group). Information from earlier versions of the DCE specification have been incorporated into this document."

A subsequent section to the abstract defines the motivation for this standard that is very closely aligned with the requirements defined for the GUID.

> "2. Motivation
>
> One of the main reasons for using UUIDs is that no centralized authority is required to administer them (although one format uses IEEE 802 node identifiers, others do not). As a result, generation on demand can be completely automated, and used for a variety of purposes. The UUID generation algorithm described here supports very high allocation rates of up to 10 million per second per machine if necessary, so that they could even be used as transaction IDs.
>
> UUIDs are of a fixed size (128 bits) which is reasonably small compared to other alternatives. This lends itself well to sorting, ordering, and hashing of all sorts, storing in databases, simple allocation, and ease of programming in general.
>
> Since UUIDs are unique and persistent, they make excellent Uniform Resource Names. The unique ability to generate a new UUID without a registration process allows for UUIDs to be one of the URNs with the lowest minting cost."

The PAC recommends that the PAIIWG and the National Institute of Standards and Technology (NIST) adopt RFC 4122 as the governing standard for the GUID in the PIV data model. It provides:

- Decentralized issuance with statistically irrelevant possibility of collisions.
- Large number space that can credential all populations.
- No requirement for a registration authority.

The PAC recommends that the GUID, as defined by RFC 4122, be used throughout a PIV credential in place of the FASC-N as the connecting identifier. The FASC-N has several weaknesses:

- It can only be issued by Federal agencies.
- It requires a central registration authority for agency codes.
- It contains Personally Identifiable Information (PII) data (the Person Identifier field).

The GUID as proposed mitigates these risks by providing a numbering schema that can be issued by any authority. It does not contain any PII data, as the person identifier is not part of the GUID definition.

As such, the GUID becomes the credential number, that is controlled by the issuer and that can safely become part of a credential set with no risk to the cardholder. The PAC recommends that General Services Administration (GSA) amend the Federal PKI Common Policy to adopt the RFC 4122-formatted GUID. The PAC also recommends that NIST amend PIV-relevant documents to specify the GUID within signed objects that currently contain the FASC-N.

Recommendations for the Primary Number within PIV

RFC 4122 provides multiple formats for the 128 bit UUID number. Each format has its merits. For universal interoperability, the PAC recommends stating that relying parties ***use the entire 128-bit GUID*** for all operational uses of the GUID to guarantee uniqueness across all relying infrastructures.

There will be issuers who seek to use a particular format of RFC 4122 for their own internal purposes. This should be allowed. Any such uses must be recognized to not be interoperable across all relying infrastructures.

Issuers must be allowed to define which numbering schema is primary for the credentials they issue. This requires a model where either the FASC-N or the GUID is primary. The PAC provides the following two means for primary numbers that interoperate no matter who issues the credential.

FASC-N as Primary Identifier

In this model, the issuer uses the FASC-N as the primary credential number. For compatibility with organizations using the GUID, the PAC recommends placing the FASC-N as part of the GUID. One method is to pack part of the FASC-N within an RFC 4122-compliant GUID as described below (in an extract from an email circulated in discussing this topic):

> "It is interesting to note that the node octets 0-6 can be encoded with the 1st 14 digits of the FASC-N. This would be a similar use case to the RFC 4122 UUID version 1, where the node field consists of an IEEE 802 MAC address. As such the maximum BCD encoding of the AgencyCode-SystemCode-CredentialID is 9999-9999-999999 with a binary equivalent of 5A-F3-10-7A-3F-FF which fits in the node definition from RFC 4122. THIS MEANS that the low order bits of the GUID would then BE the minimum recommendation (14 BCD digits) from SP 800-116 as the value for

matching FASC-N without translation for an issuer's primary PACS. This is a really good thing in maintaining a simple implementation for legacy compatibility.

```
0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          time_low                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       time_mid                |         time_hi_and_version   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|clk_seq_hi_res |  clk_seq_low  |         node (0-1)            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         node (2-5)                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

I recommend we consider this approach as a potential solution for the GUID numbering approach in the CHUID. I also suggest we contact the authors or current custodians of rfc4122 with this proposed use and ask if they offer any issues to consider. It is not in my opinion a foregone conclusion that an update or new RFC is required, since the RAND function used to generate the node in this case would just be the local FASC-N assigned value. While a formal analysis is appropriate it appears that the entropy would be quite sufficient to insure GUID uniqueness even considering a large number of issuers all using 9999 as the FASC-N [Agency Code]."

This model may be useful to an agency in considering their migration strategy away from the FASC-N towards the future of the GUID. In any case, the requirement to use the entire 128-bit GUID for interoperability allows any agency to adopt such a model with no detrimental effects to other infrastructures.

GUID as Primary Identifier

Currently, an Agency Code of 9999 states that the credential was issued by a non-federal issuer. This tells a relying PACS to look at the DUNS number within the CHUID for organizational affiliation. The DUNS number along with the System Code and Credential Number define a unique number for that credential.

The proposal is to use an Agency Code of 9995 (or any other agency code that is not yet assigned) to represent the specified GUID. If the FASC-N contains this agency code, then the next 128 bits of information is the GUID.

This solution minimizes changes to the PIV data model and the Federal PKI Common Policy. The references within these areas can continue to specify the FASC-N as the connecting number between signed objects in the PIV data model (all certificates and biometric containers).

Mutual Registration – Leveraging the GUID

As defined earlier in the problem statement, the GUID is a *static issuer-centric* numbering schema. A *dynamic relying party* numbering schema is also required. The Smart Card Alliance sees the need for a process that allows the credential to be registered with the relying system. It has been proposed to call this mutual registration. The mutual registration process may provide a second system number and optionally keying material for privacy and security. These artifacts would then be stored on the relying system and in the PIV credential. FIPS 201 defines that any issuing agency can add an application onto the credential that is parallel to, and does not alter, the PIV application on a credential. As such, additional applications could become a basis to support enhancements to the PIV application. Mutual registration defines a need to add an application to a PIV card that aids in the use cases that drive acceptance of PIV in a converged ID "one card" approach.

This mutual registration will enable the credential to have unique and different operational characteristics for a number of operating environments. In a deployed PACS that cannot consume either the FASC-N or the GUID, mutual registration may provide an assigned credential number that works with the local system. In a network, credentials could receive an IP address and a session key to secure communication with another network node.

It is also important to note that there is no requirement for interoperability associated with the local credential number assigned to the relying party system during mutual registration. It is entirely within the realm of the relying system to assign it for their local use only.

As such, the local number may be:

- A small random number
- A sequenced number
- An RFC 4122-compliant number
- An IP address for that local network (either IPv4 or IPv6)
- A structured number such as a FASC-N that is locally assigned

To facilitate mutual registration, it is important to notice that every relying party system (e.g., a PACS) must have a unique identifier. It is recommended that this issue be addressed during the development of the mutual registration application. The unique identifier is required for the card applet to be able to select the PACS entry in the card for that registered relying party system. It is recommended that the RFC 4122 UUID model be considered to provide this unique identifier.

Timing Considerations

The PAC recommends that the GUID be defined as an RFC 4122-compliant number as soon as possible. This is a very mature standard that has been successfully used throughout the Internet infrastructure.

The PAC also recommends that the mutual registration process be studied and defined as a true application within the PIV standards as soon as practical. This concept has the potential to mitigate privacy and security risks, but must be defined and made available as a card service for PIV cards. As such, it may take more time to come to consensus on this as a new standard for PIV cards.

It may be reasonable to seek a separate application identifier (AID) defining the mutual registration applet for PIV cards. At that time, it is further recommended by the PAC that the PIV data model be assessed for performance-based enhancements that will benefit contactless operations for PACS applications.

Summary

This paper has defined the problem of using IP addresses in a static mode, created by the issuer, for PIV credentials. It has also defined the need for a two-number architecture – issuer global static numbers and relying party locally-ascribed numbers – for the PIV card infrastructure.

The Smart Card Alliance Physical Access Council has consensus among its members in selecting RFC 4122 as the standard to define the GUID for the issuer-centric, static credential number.

RFC 4122 meets all known requirements for the foreseeable future of the PIV application environment. The PAC has recommended two methods to be considered to enable a GUID or a FASC-N to become the primary identifier as determined by the issuer of the credential.

The PAC recommends a rapid process to solidify and codify an applet based on mutual registration between the PIV credential and a relying party system.

Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Physical Access Council to recommend a credential numbering schema for the FIPS 201 PIV card GUID that will work for federal as well as non-federal issuers. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Physical Access Council members for their contributions to this report, including: BearingPoint; CertiPath; Cogent Systems; Computer Sciences Corp. (CSC); Datawatch Systems, Inc.; Diebold Incorporated; EDS; Hirsch Electronics; Identification Technology Partners (IDTP); IDmachines; IQ Devices; JMF Solutions LLC; Lockheed Martin; NASA; Probaris; Tyco International; U.S. Department of Defense; U.S. Department of State; XTec, Inc.

Special thanks go to **Steve Howard**, CertiPath, who led the development of the white paper, and to the following Physical Access Council members who contributed to the development and review of this white paper:

- **Reed Anderson**, U.S. Dept. of Defense
- **Todd Arnold**, XTec
- **Tim Baldridge**, NASA
- **Sal D'Agostino**, IDmachines
- **Mark Dale**, EDS
- **Tony Damalas**, Diebold
- **Lt. Col. Mark DiCarlo**, U.S. Dept. of Defense
- **Kimberly Dorsey**, Datawatch Systems
- **Marty Frary**, JMF Solutions LLC
- **Jim Hosmer**, Lockheed Martin
- **Steve Howard**, CertiPath
- **Harry Jackson**, XTec
- **Andy Jones**, XTec
- **Mike Kelley**, BearingPoint
- **Kevin Kozlowski**, XTec
- **Richard Lazarick**, CSC
- **LaChelle Levan**, Probaris
- **Gilles Lisimaque**, IDTP
- **Cathy Medich**, Smart Card Alliance
- **Kenneth Reed**, Datawatch Systems
- **Roger Roehr**, Tyco International
- **Steve Rogers**, IQ Devices
- **Mike Sulak**, U.S. Dept. of State
- **Lars Suneborn**, Hirsch Electronics
- **Dave Walker**, Cogent Systems

About the Smart Card Alliance Physical Access Council

The Smart Card Alliance Physical Access Council is focused on accelerating widespread acceptance, use, and application of smart card technology for physical access control. The Council brings together leading users and technologists from both the public and private sectors in an open forum and works on activities that are important to the physical access industry and address key issues that end user organizations have in deploying new physical access system technology. The Physical Access Council includes participants from across the smart card and physical access control system industry, including end users; smart card chip, card, software, and reader vendors; physical access control system vendors; and integration service providers.