

# The Global Unique ID (GUID)

CardTech/SecureTech  
7.April.2009

**CertiPath™**  
Commercial PKI Bridge

operated by a joint venture of  
ARINC : Exostar : SITA



# Agenda



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

- Some history on Credential Numbering for Federal programs and credentials
- Why do we need a GUID?
- What was recommended
- What's left to do...
  - No, we are not done with this issue

# In the beginning...



- There was a new technology called a MagStripe
  - And we needed to use it for physical access
- The Security Engineering Interoperability Working Group (SEIWG)
  - Defined the SEIWG-012 data model
  - Three functions...
    - Agency affiliation
    - Credential numbering
    - Person Identification

# Some issues arose



- The PI (person identifier) field was your SSN
  - It was only 9 digits
  - Opened the door for a “modified” version of the SEIWG-012
- Needed better interoperability standards
- Enter the Federal Agency Smart Credential Number (FASC-N)
  - The PI was given 10 digits
  - DoD populated it with the new EDIPI (Electronic Data Interchange Person Identifier)
  - No longer your SSN

# And New Technology Arrived



- Smart Cards
  - And we have new problems...

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.

# PAIIWG defines the CHUID



- As smart cards came into the picture, the Physical Access Interagency Interoperability Working Group (PAIIWG) saw a need
  - Improve the credential numbering schema
  - Improve interoperability between GSC-IS compliant smart cards
  - Define the interface between the credential and a PACS reader
- Resulted in the development of the Technical Interoperability Guidance for Smart Card Enabled PACS (TIG-SCEPACS)
  - Defined the CHUID and levels of authentication
  - Addressed issues around Agency Codes that were non-numeric
  - Enhanced security definition with asymmetric signatures protecting the CHUID
  - Defined a new field → the GUID

# The GUID was a place holder



- The GUID was a concept for a large number in the format of an IPv6 address
  - Used industry standard half-word (16 bytes/128 bits)
  - Easy to process in memory (half-word boundaries in tables)
- Discussion on this opportunity to use IP addresses for secure protocols between relying systems and smart cards
  - Drove additional thinking on why we should use IPv6

# Still More Issues...



- The FASC-N can only be used by Federal agencies
- And outside bodies were concerned with the GUID

"... Concerns have been raised by members of the American Registry for Internet Numbers (ARIN - [www.arin.net](http://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. ..."

# Recommendations by the PAC



- Based on experience with DHCP and GSM
- Recommendation for a two number architecture
  - A *static* number, the GUID, assigned by the issuer
  - A *dynamic* number, issued by the relying party
- The static number must meet the following core requirements
  - No need for a registration authority to manage the number
  - No centralized namespace management
  - Sufficiently large numberspace to avoid collisions

# RFC 4122 for the GUID



- The Smart Card Alliance Physical Access Council adopted a recommendation for the GUID
  - Use the IETF RFC 4122 Universally Unique Identifier (UUID)
  - Thank you to Lockheed Martin for the idea

One of the main reasons for using UUIDs is that *no centralized authority is required to administer them ...*

UUIDs are of a fixed size (128 bits) which is reasonably small compared to other alternatives. ...

Since UUIDs are unique and persistent, they make excellent Uniform Resource Names. ...

# Are We Done Now?



- GSA just issued guidance that supports the use of RFC4122 for the GUID
  - This is finally settled
  - It works for Federal and Non-Federal Issuers alike
- But there is more to be done
  - Mutual registration for the dynamic portion of the two number architecture must still be defined

# We Need More Numbers



- To complete the task, we need to consider new methods and homes for
  - Person Identification Numbers
  - Agency Identification Numbers
  - Issuer Identification Numbers
  - Physical access systems for Mutual Registration with corresponding smart credentials

# We Need More Use Guidance



- NFI's using GUID
  - Federal Agencies may or may not support this model for their PACS
  - Will the PAIIWG assist in this process?
- Certificates need the GUID
  - Need to define subject.alt.name.GUID
- Biometric objects need the GUID

# Summary



- We've finally *solved* the GUID numbering problem
  - RFC 4122 to the rescue
  - Yipee
- But there is more to do
  - Mutual Registration
  - Definition of use throughout the PIV data model
  - New homes for PI and Agency