GUID-based Bridge Authentication Process

Introduction

Authentication of identity for the purposes of access control is accomplished through three factors today (something a person has, something a person knows, something a person is) and potentially more factors in the future, and the token representing what a person has refers to the digital certificate or GUID on the smart card. This paper explores the usage of GUIDs for Physical Access Control (PACS) and discusses how the current GUID defined in FIPS 201, SP800-73 and PACS 2.2 can be leveraged to smoothly migrate existing PACS systems in a transitional pathway to a desired end-state in 5-8 years. This is an important topic as cost, disruption to facilities and the ability to squeeze ROI out of existing PACS are critical needs, and the security of today's PACS systems will be challenged as they are extended beyond their initial design.

The usage of prox 125 KHz contactless enabled through multi-technology credential stock and multi-technology PACS readers is well-accepted as a transitional strategy, and thus not discussed, although assumed to be another integral aspect to PACS migration.

On the other hand, usage of a digital certificate (X.509) issued by a FBCA Certificate Authority is too bulky to be utilized effectively for fast-transaction time PACS in the next 5-8 years, especially given the state-of-the-art in today's PACS systems. Also, the importance of using a large number of bits such as the GUID for authentication is illustrated through the concept of the birthday problem[i], and birthday attacks[ii]. The birthday problem is an intuitive paradox that states that when meet someone for the first time you have a 1 in 365 chance (0.27%) that they will have the same birthday as you. With every person you meet after that, the chances increase, but not on a linear scale. After meeting 23 people, the probability of any of them having the same birthday jumps up 50%, and it is over 99% when there are 60 people. The birthday attack mathematically exploits this to identify collisions and can be mitigated by utilizing very large numbers, rendering exploitation computationally infeasible over the long term.

What are GUIDs

The term GUID is short for ***G****lobally* ***U****nique* ***Id****entifier*, a unique 128-bit number, also related to UUID (***U****niversally* ***U****nique* ***Id****entifier*) which was standardized by the Open Software Foundation (OSF) as part of the Distributed Computing Environment (DCE) to enable distributed systems to uniquely identify information without significant central coordination. GUIDs are produced by the Windows OS or by some Windows applications to identify a particular component, application, file, database entry, and/or user. For instance, a Web site may generate a GUID and assign it to a user's browser to record and track the session. A GUID is also used in a Windows registry to identify COM DLLs[iii]. Other industry-standard IT subsystems like Oracle utilize GUIDs[iv]. GUIDs were initially introduced as a way to replicate huge datastores and avoiding data collision due to duplicate primary keys. Everyday companies use GUIDs to replicate terabyte sized datastructure while maintaining record uniqueness. Since the inception of GUIDs, GUIDs have become common place for managing a wide variety of network related objects.

GUIDs are 32 hex digits (16 byte) numbers, grouped into chunks of 8-4-4-4-12. This gives us 2^128 or about 10^38 numbers that can uniquely identify different assets throughout space and time. The IPv6 addressing scheme is suggested as a centralized entity to manage GUIDs[v]. Theoretically, because the number of possible GUIDs is so high, there will never be a GUID collision though possibly one may occur and having a centrally managed GUID generation process guarantees GUID uniqueness throughout space and time.

The usage of a GUID also exists as a component of a CHUID (Card Holder Unique Identifier) and was made a mandatory element dating back to SP800-73, Draft 2, 3/8/05. In both PACS 2.3 and ISO/IEC 24727, usage of the GUID is identified as a characteristic of an emerging system[vi], and its usage is promoted for interoperability[vii].

GUIDs are as secure if not more secure than digital certificates as a part of an authentication scheme, depending upon the implementation. They do not contain any data themselves, and are only meaningful when joined into a structure that associates data to the GUID. These corresponding association directories are built to interoperate upon open standards such as LDAP and x.509, using efficient, sub-system layer replication facilities to meet high-availability and high-security systems levels. In addition GUIDs can be encrypted, or be a component of an encrypted asymmetrical PKI key. Overall, the usage of GUIDs is an agile approach for PACS, and is already accepted by current enterprise IT Security professionals.

The Problems with Authentication today

Concerns by Privacy Advocates – "The first and foremost of these is the active opposition of privacy advocates, who see in a U.S. Federal PKI a significant challenge to individual privacy. They believe that issuance of a single electronic identity document will enable the government to aggregate too much personal information in a single place and make that information available to Agencies with power to do much harm. These advocates acknowledge, however, that just such a circumstance is already occurring in the private sector business marketing environment, where on-line firms, credit card companies, banks and even spyware-enabled websites are aggregating personal information into data banks used to try to sell ever more goods and services."[viii]

Cost – Both in terms of actual monetary outlay as well as performance, utilizing the Federal PKI Bridge in PACS is very costly, and involves full-scale equipment replacement. For entities not needing the same rigorous degree of standards compliance for their PACS zones/readers, the price tag is overwhelming.

1. Cost – FBCA-approved certificates and associated infrastructure
2. Performance – FBCA CRL is over 31M in size (bowling ball down the Internet)

a. Push is only guaranteed every 18 hours
b. Limited bandwidth during emergencies

Sanctity of the Trust Model – the relationship between logical/physical PIV and E-Authentication guidance is not clearly correlating, as well as the association between PKI assurance levels, which establish the identification requirements for obtaining a Federal PKI certificate. The HMAC (Hashed Message Authentication Code) signature for Medium Assurance by a PACS system is created over the FASC-N and Expiration Date by calculating a 3DES CBC signature using a site secret key or a site public key, and the result is truncated to 32 bits. Coupled with the prohibition to not modify the FASC-N and expiration date after issuance, but not the GUID, the capability to immediately beginning to enjoy the benefits of a higher-assurance level system without undue 'forklift upgrades' is achievable.

Key Compromise - Since PKI certificates also carry data, the risk of a compromised key could be that confidential data is leaked.

GUID-based PACS System Characteristics

Identity management and access control are enhanced by usage of the already-mandatory GUID field of the CHUID for PACS for a number of reasons. Since many PACS head-end systems do not yet address over 75 bits of information per userid/transaction, using a 128 bit unique primary-key system is more realistic compared to PKI-based systems. Also, speed of each transaction is improved dramatically, since a much smaller packet of data is being transmitted. Lastly, this function can be added on to existing PIV cards as they exist by the standards today, and meet Medium Assurance levels with HMAC.

In addition, agency users can also utilize certificates via the federal bridge or a locally established bridge acting as their own certificate authority. Using an appropriately-secured GUID process guarantees security, speed in replication and visibility of select sets of data between agencies with minimal risk.

Components:

1. Transaction tracking mechanism (GUID, UUID, Certificate).
2. Authentication medium (smartcards, chips, and any other data storage medium whether its embedded, imbedded, attached, not attached etc..
3. Authentication factor (something a person has, something a person knows, something a person is, place in time, etc.)
4. Storage mediums (relational data structures, active directory, chips and other mediums).

Integrity and reliability of identity information is done through transaction and data tracking through storage devices and authentication mediums through the use of

1. GUID – globally unique identifiers

2. UUIDs – universally unique identifiers

3. Certificates (any type)

4. Other unique markers as they are developed.

GUIDs, UUIDs, certificates and other markers are used to uniquely identify a single data object across local, regional, national and international structures whether they are storage structures or authentications mediums. A data object can be a record that represents any piece of data within the data store uniquely correlated through connected or disconnected space and time through any of the above markers. Considering the fact that certain attributes of personal, private or other operational data can't be transmitted in some cases, the unique marker/identifier provides a means to validate an object without the loss or compromise of sensitive data. If sensitive data needs to be accessed the unique marker/identifier can be used as a lookup structure to a storage medium or to an authentication medium for additional sensitive data. In addition sets of selected data can be transactionally, snapshot, or merge replicated across enterprises as need.

By using these markers and identifiers it is possible to replicate data objects across multiple remote data stores locally, regionally, nationally or internationally without losing integrity. This also allows for near real-time updates for immediate identity visibility.

In cases where correlation from local data stores and identities are required for reliance by peer or federal entities, there will be a correlation process between an OCSP server (federal side) to the local marker based or certificate based identity structure. Because the federal bridge structures and the local marker structures both process identity data in accordance with FIPS 201 requirements the local store (native) can be used as well as the federal stores through an OCSP connection. Overall, this allows for near real-time operating characteristics at all levels while also supporting federal bridge identity requirements.

Data Ownership and Control

One of the key requirements in replicating data across multiple jurisdictions is control over the replicated data. Each local entity will own its own data and only share what is required by that agency by granting explicit control, down to the field level. This is accomplished through replication configuration parameters and mandatory access control. Replication is controlled through the data engine and prior to taking place needs to be configured through the data engine. The data administrator can define what sets of data to replicate or not replicate. Data can also be shared through a manual data push or an authorized data pull. This allows for data sharing to take place that may not fit into the data replication model. To guarantee the security aspects of certain sets of data, an artificial intelligent engine scrubs the data prior to that set of data leaving its trusted boundary. This filtering mechanism runs as a background process on the data as information is requested by different data consumers.

Generation of GUIDs

There are different methodologies for producing GUIDs. The version one (V1) GUIDs use a combination based upon MAC addressing. With this technique it is possible to determine the asset that created the GUID based on the GUIDs construction. This may be a weakness or a benefit depending on goals.

Other methods include using date timestamp data, content based, random data and others. As long as the defined constructor is implemented GUIDs can be generated in different manners and still be valid GUIDs, yielding the same level of uniqueness throughout space and time[ix].

The IPv6 namespace cost for assigning a block of addresses to be utilized as the GUID by ARIN are not free of charge, but less than the cost of a FBCA-approved certificate.

Advantages

The uniqueness of this particular implementation comes into play in a variety of ways.

- This is the first time anyone has used the GUID/UUID/Marker strategy to proof an identity
- Extends the process across hardware media in the form of a smartcard, logical layer, and the physical storage mechanism
- Provides a not used before process to hide or show specific sets of data based on user requirements and object related security
- Provides a unique process for real-time processing of credential data as well as other complimentary services to physical sites

The advantages of using GUIDs are

- No central management is required – there doesn't need to be a central managing entity to effectively use GUIDs, merge and correlate data throughout space and time. Using an un-centralized model still makes it possible (though not probable) to duplicate a record, however, in order to do so would require an order of magnitude beyond current capabilities. Managing GUIDs (IPV6, Internally generated GUIDs, composite GUIDs, etc.) does guarantee uniqueness.

- Security through obfuscation – It is difficult visualize what the GUID represents and they are difficult to debug. Thus if an older PACS system which transmits data between the internal components (head end, panels, readers) in cleartext were to be subject to a man-in-the-middle attack or is sniffed, the ability to utilize the information to inject false data would be lessened.

- GUIDs can be easily merged into other sets of data and still maintain uniqueness. They can be concatenated (joined with other fields) in ways that extend the meaning and thus are multi-purpose.

- GUIDs are already widely used in the IT world. GUIDs represent servers, users, networks and applications as well as other pieces of IT infrastructures. They are also required for replication in most database replication processes. GUIDs can also be used in the physical access control world as well. Physical access control applications can pass a 128 bit Unique card ID for physical authentication purposes.

- GUIDs can be replicated on a transactional basis, so if a new user is added to a network or a physical structure, that access can be replicated in near real time to other locations nationally with no intervention from a third party. This makes it very easy to maintain change control to network and facilities on a real time basis across the globe. This is especially useful in an emergency management scenario where assets may deploy to various jurisdictions and have a requirement to be authenticated to the scene.

- GUID usage can also support labeling processes, which is a mandatory access feature to ensure least privilege access.

- Because a GUID can uniquely be used to identify an individual, the GUID becomes an effective method for access control and identity management processes across centralized and un-centralized networks, physical structures, etc.

- Considering that GUIDs already exist in both worlds, it makes sense to extend the GUID to a converged access control process to control both network and physical access.

GUIDs compared to PKI Certificates

- PKI was initially introduced to encrypt data. Comparatively, PKI is bloated, requires key management and is expensive to implement and maintain. Overall, PKI requires more hardware, more bandwidth.

- Whereas GUID can replicate on a transactional basis PKI infrastructures must be maintained through CRLs (Certificate Revocation Lists) and OCSPs (Online Certificate Status Providers), etc. Not only is this a time consuming process based on update intervals but is a bandwidth intensive process as well. Certificates can vary in size but minimally, with no extra data, a base certificate is around 70-80 times larger than a GUID. A certificate with extra data can be 1000s of times greater than the size of a GUID. An HSPD-12 certificate with key pairs can be more than 500 times of the GUID. Bandwidth issues become a concern when there are large sets of certificate data to maintain especially in emergency environments where there may be limited bandwidth. In addition, it is not the certificate that performs identity verification as the token, the CHUID is still required and the CHUID is not a certificate. Certificates can perform token authentication, but again, the management process is much more extensive than with a GUID.

- In addition a certificate will cost an agency $70-80 per individual whereas under the GUID process it costs nothing to produce a GUID.

FAQs

1. The GUID is just a number string. Unless there is an international body assigned to pass out the numbers so no two people get the same numbers the chance of collisions (duplicates) is highly likely. Sure it is a large number, but human nature is to start with 1 and increment up.

   It is a number string however, it is not based on random assignment, sequential or chronological assignment. The GUID is generated through an algorithm that provides as part of its process a capability to generate a number that is unique. It is not very likely at all the number will be duplicated. Granted, there is a remote possibility the GUID may duplicate, however, if the GUID generating process is consistent throughout the lifespan of a process the GUID won't duplicate. Also, a composite GUID with management/allocation of the segments by a governing body (or a set of governance entities) would mitigate this concern.

2. In the TIG SCEPACS, it was anticipated that the GUID would be used for an IP v6 address (hence the 128 bits) and be issued by an appropriate organization for that purpose. More recently, I have heard it stated that the US Government is now committed to the FASC-N scheme forever. That is a problem since we don't have a strong champion to drive the data model for GUID implementation.

   Regarding the TIG SCEPACS it's not necessary for a controlling entity to provide GUIDs as the lifecycle space for GUIDS is more than adequate for access control applications. Only the method of generating the GUID has to remain consistent throughout the process. Yes, it seems like FASC-N will be around for a while (analogy is how difficult to root out Social Security number usage) and that is why the ICI of the FASC-N is initially set to '1' explicitly in SP800-73-2; this is the first generation of the FASC-N. However, the GUID and FASC-N are not mutually exclusive, and GUID is already part of the CHUID. Lastly, should we build infrastructure that is more profitable to the vendors, or strive towards solutions that are more complete, open and effective? Can there exist a champion for the latter?

3. A single number string is not the likely long term direction. Whether it grows from 26 bit Wiegand to 48 bit (as in the GSA APL) or 128 bit, we are more likely to see schemes that consist of parsable fields that mean something – just as the 48 bit FASC-N is constructed from an Agency Code, Site/System Code, and Credential Number.

A composite GUID may be an even better solution than an IPv6 address, since that would have some meaning by each segment for PACS reading. Accordingly, in the backend IdMS, a clustered GUID (consisting of multiple GUIDs, each representing a different algorithm, i.e., one time-based, one machine/network-based, etc.) could then be correlated and matched up as needed for a specific purpose. Compared to the alternative of a digital certificate, this schema is just as secure and arguably more, and has the upside of potentially not exposing actual data if compromised (as in the case of a digital certificate).

Based on the time span of technological advances, what is the definition of a long term direction? That which is considered cutting edge today won't be tomorrow, for example, nano-dotting, molecular positioning applications, etc. are on the horizon. New technologies aren't that far down the road will obsolete in most cases what we consider state of the art today. Our main problem is that some technology segments haven't kept up with cutting edge processes and are generations behind, requiring leapfrogging in an intelligent fashion, with an eye to futures we don't even yet realize will become de facto.

[i] Ciampa, M. (2005). *Security+ Guide to Network Security Fundamentals, Second Edition.* Boston: Course Technology.

[ii] http://en.wikipedia.org/wiki/Birthday_attack

[iii] http://www.webopedia.com/TERM/G/GUID.html

[iv] http://en.wikipedia.org/wiki/Globally_Unique_Identifier

[v] http://www.ietf.org/rfc/rfc2373.txt - GUID as a 16 byte (128 bit) registered IPv6 address (from ARIN)

[vi] http://www.smart.gov/iab/documents/PACS.pdf

[vii] http://www.tvworldwide.com/events/gsa/050504/ppt/050505_GSA_1115_Industry_delivery_of_PIV2_-_A.ppt

[viii] http://www.cio.gov/fpkipa/documents/altermanpaper.pdf

[ix] http://www.ietf.org/rfc/rfc4122.txt - A Universally Unique IDentifier (UUID) URN Namespace