Joint Security and Privacy Committee

NEMA COCIR JIRA

International Medical Informatics

Management of Machine Authentication Certificates

This Paper was developed by the

Joint NEMA-MITA/COCIR/JIRA/ Security and Privacy Committee (SPC)

The Paper has been approved by:

MITA (Medical Imaging & Technology Alliance, a Division of NEMA)-USA

COCIR (European Coordination Committee of the Radiological and Electromedical Industry)

JIRA (Japan Industries Association of Radiological Systems)

May 2007

www.nema.org/medical/spc
Secretariat: MITA (Medical Imaging & Technology Alliance, a Division of NEMA)
www.medicalimaging.org
1300 North 17th Street, Suite 1752, Arlington, VA 22209 USA
Tel: 703-841-3200, fax: 703-841-5900
E-mail: svastagh@medicalimaging.org

1. Summary/Introduction

This paper helps healthcare providers and medical device engineering organizations decide how to use digital certificates to secure machine to machine communications.

There is a focus on privacy and security in healthcare. The breaches in security over the past five years have shown that using a “moat” approach of firewalls without further internal security is not effective. To properly secure a network environment the machines (e.g., imaging device, PACS archive, laptop, a system implementing an IHE profile, internet kiosk) that are going to receive or transmit sensitive data must be identified. This introduces a need to authenticate both machine identities and person identities. The focus of this paper is machine identity management.

The data protection regulations in the US (HIPAA), Europe (EC Privacy Directive), Japan (Personal Information Protection Law), etc., require that hospital information networks be protected. One approach is to employ strict network isolation security. This is not practical, because healthcare professionals need access to intranet/internet facilities, e.g., drug information. The authentication of machines and people is a practical solution. The problems of authenticating persons is extensively discussed elsewhere under subjects such as private key infrastructures (PKI).

The major communications standards used in healthcare (DICOM, HL7, IPSEC, TLS, and HTTPS) all define how to authenticate machines by means of private keys and public certificates. IPSEC, TLS, and HTTPS are also used extensively in non-medical contexts. The Integrating the Healthcare Enterprise (IHE) integration profile “Audit Trail and Node Authentication (ATNA)” describes the technical details of how these and other standards should be used as part of a secure healthcare network. The commercial and healthcare standards all utilize a certificate based authentication mechanism that can be used in conjunction with various PKI infrastructure systems.

Some sites may already have machine authentication infrastructures in place or may have agreed with their vendors to an alternate approach. This paper and its guidelines do not apply to those situations. Such sites should follow the procedures and administrative requirements already defined by their infrastructure.

This paper does not discuss the much larger issue of deciding on the policies and trust relationships that must be established between the different components of the healthcare system. Those involve local regulatory constraints, operational relationships, professional relationships, etc. Machine authentication is a common component of the policy enforcement mechanisms that are put in place to manage and enforce those policy decisions. Using machine authentication is not a substitute for establishing appropriate policy, it is a mechanism to help enforce a policy.

The guidelines in this document are intended for sites and vendors that have decided to use a PKI infrastructure for machine authentication. This paper does not attempt to provide implementation specifications. Sites with PKI infrastructures for humans may wish to extend them to cover machines in addition – they may find this document useful. This document provides guidelines for machine authentication and the related infrastructure. Vendors and customers following these guidelines will reduce their development, acquisition, deployment, and operational costs.

Authentication mechanisms for people have many complex legal, privacy, accreditation, hiring, firing, role/function, and authorization issues that do not arise for machines. The management of machines can be handled within the IT organization, and does not require a human resources organization. Machines have inventory, service, and repair issues that can be managed within the IT organization.

These guidelines for machine authentication are simpler than the PKI management recommendations found in most security literature because managing the authentication of machines is much simpler than authenticating individuals.

When using machine authentication by certificates, healthcare providers must:

- *provide a certificate authority as part of their IT administration. They cannot simply depend on their vendors to provide machines with keys and certificates. This network infrastructure can be provided through third party contracts.*
- *decide which of the authentication approaches described below they will use.*
- *establish and maintain the other servers and services, e.g., Certificate Revocation List (CRL) servers, needed for their selected approach.*

To be prepared, equipment suppliers (vendors) must:

- *be able to authenticate communications by the approaches described below.*
- *provide a means of maintaining a local private key on those machines.*
- *provide applications and administrative interfaces necessary for all the applications that need secured communications.*

2. Scenarios

In the healthcare environment it is often necessary to authenticate the machines that are communicating independently of the authentication of the people who are involved. The following scenarios are examples of how machine authentication should take place in healthcare workflows.

2.1 Staffed Machines

Authenticating the user of a staffed machine is not sufficient to authenticate the machine. The machine needs to be authenticated before transmitting or receiving sensitive data. For example, the authenticated user might be at an Internet café computer. The public computer will be denied access. This is independent of any person authentication. The user authentication is needed for access controls and audit trails related to that user’s activity (treated elsewhere in other documents).

2.1.1 Image Creating Modalities

A typical staffed machine is an image creating modality, e.g., an angiography system. Often the identification of the machine operator takes place, but not the rest of the surgical team. Bidirectional authentication of machines is needed when:

- user identification is not appropriate for some situations. For example, an angiography system has a study to send to the PACS, it needs authentication of the PACS system to ensure that it does not send it to a rogue system. User authentication is not an appropriate authentication in this case.
- the machine queries the worklist to obtain patient information, the HIS/RIS system needs to know whether this query should be answered. The patient scheduling information should not go to any machine in the hospital; it should only go to the authorized machines.
- an automatic security system will record and alert on unusual worklist queries, e.g., querying the angiography schedule from a obstetrics nursing station, and not report normal queries, e.g., querying the angiography schedule from an angiography system . Similarly, the angiography system needs assurance that it has reached the HIS system and has not been diverted to an unauthorized machine.
- an angiography system delivers finished studies and updates the worklist status it is again important to identify the machine rather than the person. As above, a security system will probably report and alert on attempts to store angiography results that do not originate at an authentic angiography system.

The machine authentication mechanisms address these issues.

2.1.2 The Radiologist’s Workstation

In another example the radiologist reading CT results will be authenticated and authorized as a person. The machine will be independently authenticated. Now that the radiologist has been properly identified and the machine is cleared to receive and will protect the data, viewing CT results can proceed. Machine authentication also permits secure pre-loading of studies onto the radiologist’s workstation before the radiologist arrives and logs in.

2.1.3 Service Laptops directly accessing the Hospital LAN

The security issues surrounding service laptops extend beyond machine authentication for the laptop. It is complicated by trust agreements between vendors, healthcare providers, and others. This paper does not deal with all the other issues that arise in this context. The machine communications authentication described here can become part of an overall laptop solution.

2.2 Access to Servers

In our example, a physician using a browser accesses a web server for patient information. It is assumed that the user is properly identified, authenticated and authorized. The physician needs to ensure that the connection is to the correct web server and that it has been authenticated. There is a mechanism to enable the server to authenticate the physician's machine.

Web servers, browsers, and PCs should be configured to use the client certificate authentication of the local machine. The instructions for this can be found in the documentation for the particular products.

There is a common misconception that the "view only" use of a browser eliminates the need for machine authentication. This ignores the threat of malware (such as screen scrapers and keyboard loggers) that intercept communications. Browsers also maintain cached pages that might not be cleared completely, also exposing personal information. This is true regardless of whether SSL or VPN technology has protected the communications. The machine authentication information can be used to identify whether the connection is from a machine that is known to be taking all of the extra steps needed to protect privacy.

It can also be used to ensure that unknown machines are treated differently. There may be good reasons to permit limited access from public access kiosks. The machine authentication can be used to enable granting limited access to authorized staff from such machines. The limited access can be designed with the assumption that these unknown machines are likely to have malware or maintain caches that will expose the information that is delivered.

2.3 Autonomous Machines

There are many kinds of autonomous machines in use in healthcare. These are both analytical systems like computer aided diagnosis systems, and measurement systems like portable patient monitors. For example, a portable patient monitor takes a variety of patient health measurements automatically, signal alarms, as well as receive instructions from other systems. There may also be a clinical care provider present, but the system must operate even without staff present.

When the monitor sends data to a hospital record repository the repository must know unambiguously which monitor is sending the data and the monitor must know that it is sending data to the correct repository. This is a security issue with safety consequences. Misidentification could result in mislabeling alerts or reports, or in loss of data if it is sent to the wrong location.

Portable patient monitors also move and can be fully operational while moving. So the simple administrative solution of using network addresses breaks down or becomes very labor intensive and error prone when the monitors can move between local networks. The monitor authentication must allow mobile activities and must not require substantial administrative effort. Machine authentication can help solve these problems.

2.4 Unauthenticated Machines

When the routine communications all utilize machine authentication, any unauthenticated machine access attempts can be denied, and reported. The most important of these communications are those that convey private data.

Communications like cafeteria schedules and other public data should be minimized or eliminated from machines that also are used for personal data. These communications might be with unauthorized machines.

3 How Machine Authentication Works

The approach used to authenticate machines in the medical protocols requires:

- establishing private/public key pairs for each machine.

  These keys may be internally generated by the machine or may need to be externally generated and provided to the machine. The private keys must be carefully protected from copying or modification because they are the primary means of identifying the machine.

- distributing public certificates.

  Public certificates wrap the public key that pairs with its private key. These certificates include their own expiration dates and must be replaced at intervals and can be openly distributed to other systems. The possessor of a public certificate can verify that another machine possesses the corresponding private key. There are two major approaches for verification:

  - direct comparison (see section 3.1) and
  - trusted signature chain (see section 3.2).

- securing the communications channel.

  The channel setup includes challenge response tokens that utilize the private key and public key. TLS, IPSEC, SSL and other secure transport protocols handle this during session initiation. The higher level protocols HTTP, DICOM, and HL7, that are used for medical data exchange, all have support defined for using TLS. They need to be configured with the appropriate certificates for the sites where they are used.

3.1 Direct comparison

This approach is suitable for networks with few communication partners per machine. Each machine is given in advance the public certificates for all of the machines that are authorized to use this network. To authenticate a partner, a machine compares the incoming connection information with the certificates on its list.

Figure 1 summarizes the installation steps needed for direct comparison:

1. the private/public key pair is created, and public certificate issued. This could be self-signed or CA signed.

2. the public certificate is distributed to the other machines. This could be through manual distribution, on media, or through a service like LDAP. The distribution mechanism must be trusted.
3. the public certificates of the other machines are installed on the new machine. This could be through manual distribution, on media, or through a service like LDAP. The distribution mechanism must be trusted.

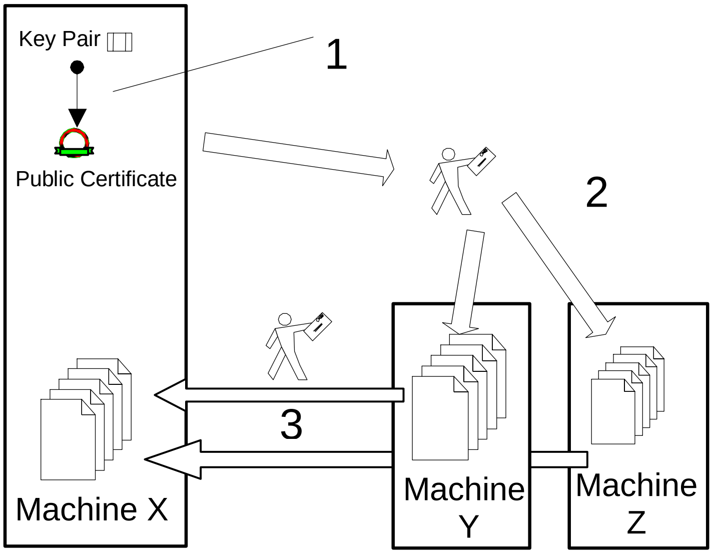

Figure 1 - Installation process for direct comparison

The corresponding public certificates must be removed from the other machines when a machine is removed, a private key is compromised, a certificate expires, and when connections to a machine are no longer appropriate. This is the direct comparison equivalent of revocation.

Figure 2 summarizes the steps taken when establishing machine authentication during communication:

1. The initiating machine (machine X) generates a token based on its private key and the token is sent to the receiving machine
2. The receiving machine (machine Y) checks the token against the public certificate that has been stored as known machine authentications.
3. The authenticated machine identity is checked against the system access control mechanism to determine whether the connection should proceed.

The process is repeated in the reverse direction so that the initiating machine can authenticate the receiving machine.

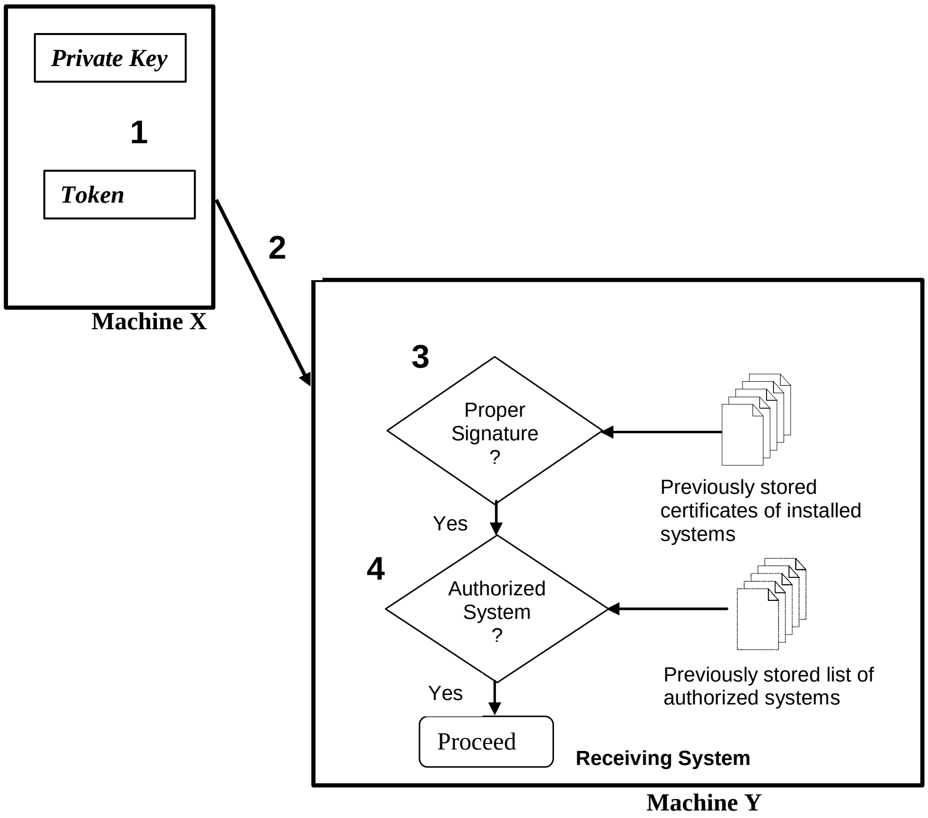

Figure 2 - Authentication process for direct comparison

3.2 Trusted Signature Chain Comparison

This approach involves a third machine, acting as a certificate authority (CA), that is trusted by the IT administration. This CA generates signed public certificates for private keys. Other systems in the network use these signatures to assure that these certificates are for machines that are authorized to use the network.

Figure 3 summarizes the steps when a new machine is installed:

1. The public certificate for the trusted CA is installed on the new machine.
2. The new machine generates a public/private key pair (or has one generated for it by the CA).
3. The new machine sends the request to the CA to generate a signed public certificate.
4. The signed public certificate is sent back to the new machine for future use. Note that there are no actions needed on other machines, unlike the direct comparison above.

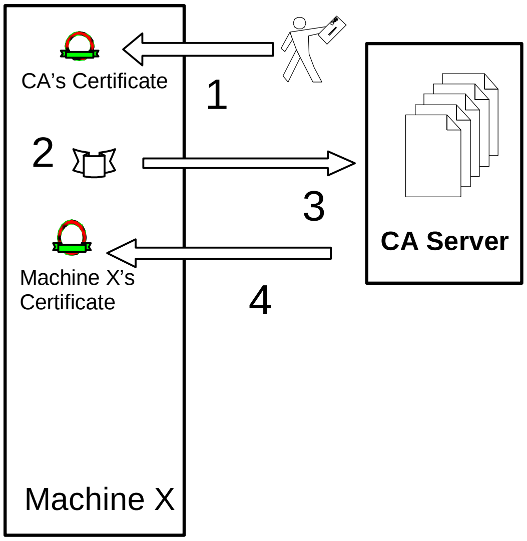

Figure 3 - Installation process for trusted signature chain

The public certificates for a machine must be revoked when that machine is removed, its private key is compromised, or when connections to a machine are no longer appropriate. This eventually results in a growing revocation list. Certificate expiration dates permit this list to be trimmed eventually, but it is normal to maintain revoked certificates on the list for an extended period past expiration.

Figure 4 summarizes the steps taken when establishing machine authentication during communication:

1. The initiating machine generates a token based on its private key.
2. The token is sent to the receiving machine
3. The receiving machine checks whether the token was signed by a private key that corresponds to a certificate that has been signed by an approved certificate authority.
4. The receiving machine checks whether this particular public certificate has been revoked. This is usually done by checking with a revocation server that is typically a function provided by the CA.
5. The authenticated machine identity is checked against the system access control mechanism to determine whether the connection should proceed.

The process is repeated in the reverse direction so that the initiating machine can authenticate the receiving machine.

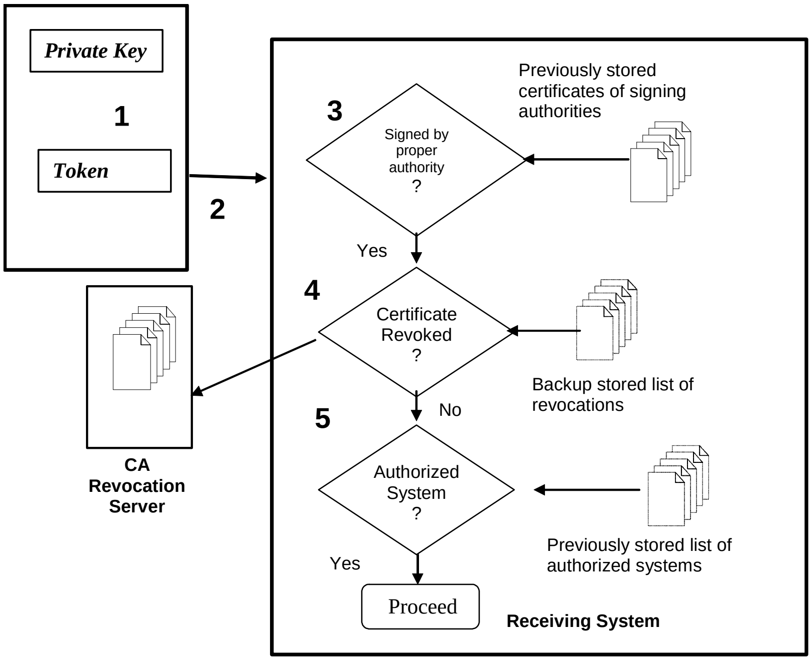
Private Key
1
Token
2
3
Signed by proper authority ?
Previously stored certificates of signing authorities
Yes
4
Certificate Revoked ?
Backup stored list of revocations
No
5
CA Revocation Server
Authorized System ?
Previously stored list of authorized systems
Yes
Proceed
Receiving System

Figure 4 - Authentication process for trusted signature chain

3.3 Deciding between direct comparison and trusted signature chain

The decision whether to use direct comparison or trusted signature chain comparison is the major choice to be made by the IT administration. Both are equally effective for authentication purposes and both can be suitable for healthcare systems. The tradeoff is between different kinds of network facilities that must be installed and different kinds of routine administrative labor required to maintain operations. In general, smaller network facilities will select the direct comparison approach, and larger network facilities will select the signature comparison approach. But there is no single size where one becomes preferable. Therefore, the SPC recommends that equipment vendors be prepared for both environments.

TLS, SSL, and IPSEC all support both approaches, and support a hybrid that combines them. The higher level protocols like HTTP, DICOM, and HL7 that are used for medical data exchange, all have support defined for using TLS. They need to be configured with the appropriate certificates for the sites where they are used.

4 Failure and Continuity of Operations

Any failure in the authentication system has the potential to interfere with providing healthcare services. When using trusted signature chain this includes failures of the CRL service, other servers, or network communications with these servers. Procedures, fail-over, and backup mechanisms must be planned so that this kind of failure does not interfere with necessary services.

After a disaster there is often a flurry of emergency and temporary machine replacements to recover from the losses that occurred during the disaster. The procedures and facilities planning for authentication controls must take this into consideration. These machines will need authentication services. The SPC break glass white paper discusses some of these issues. (See www.nema.org/medical/SPC). Special care is needed to establish backup and local alternatives to deal with loss of network access during disasters.

The decision between the use of direct comparison and trusted signature chain should include consideration of how the full system will maintain operation during disasters and failures and how it will recover from disasters and failures.

5 Conclusion

The certificate management procedures needed for identifying and authenticating machines are different from those used for people. The software provided for most systems can accommodate both, but the documentation often only covers personnel. The vendors and healthcare providers can meet the needs of machine identification as well.

When using machine authentication by certificates, healthcare providers must:

- *decide which of the authentication approaches to use (see section 3 above).*
- *if using a trusted signature chain approach, provide a certificate authority. They cannot simply depend on their vendors to provide machines with keys and certificates. This network infrastructure can be provided through third party contracts.*
- *if using direct comparison, obtain certificates for manual installation. This can be from any certificate authority, internal or external.*
- *establish and maintain the other servers and services, e.g., Certificate Revocation List (CRL) servers, needed for their selected approach.*

To meet the variety of needs worldwide, the vendors must:

- *be able to authenticate communications by the different approaches described above.*
- *provide a means of maintaining a local private key on those machines.*
- *provide applications and administrative interfaces necessary for all the applications that need secured communications.*

Technical Annex Guidelines for use of Certificates

These guidelines separate healthcare operational responsibilities and vendor product requirements providing some technical details to both.

A.1 Organizational Responsibilities

When establishing local procedures both the facility IT organization and equipment vendors must take actions.

A.1.1 Facility IT Organization

The organization must choose the authentication approach. This organization must:

- Establish and maintain the policies, procedures, servers, and administration of the authentication system chosen. Particular care must be taken to ensure that certificate management for authentication purposes is controlled to protect against unauthorized modifications.
- Maintain adequate records and backups of authentication information.
- Maintain the local certificate revocation system. With direct comparison this requires a manual process to remove the untrusted certificate from each machine. With trusted signature chain this can be either manual revocation list distribution or revocation service management.
- Have procedures to replace keys and certificates that have been lost or compromised in a timely fashion to minimize patient care delays.
- Manage certificate expirations.
  1. New certificates must be in place before the old ones expire to avoid interfering with healthcare operations.
  2. Expiration is recommended to be two (2) years, although local considerations can change this.
  3. Creating replacement certificates follows the same procedure as creating new certificates.
- Establish machine access policies that will make use of the authentication information. Include in these policies rejection of non-authenticated machines, examination of machine authentication failures, etc.
- Design for continuity of operation during failures and disasters. Coordinate this activity with vendors. It is likely that in a disaster network connectivity and server access may fail. See section 4.
- Coordinate with other departments that may have operational responsibilities as part of the authentication procedures. For example, the biomedical engineering department may be responsible for equipment repairs and would then be involved in the authentication process. This must include consideration for authentication of local spares that may be swapped in on a temporary basis.

A.1.2 Medical Equipment Vendors

The equipment vendors must design products and service procedures that:

- Provide service support tools for their products that can be used for both the direct comparison and trusted signature chain approaches.
- Provide service documentation and coordinate service procedures with the facility IT organization to manage upgrades, expirations, and machine replacements. This includes sufficient tools and documentation to support activities such as local equipment swaps.
- Coordinate procedures with facility IT and with other vendors for upgrades, expirations, and replacements. When using direct comparison the certificate lists on other vendor machines may need to be updated as a result of service activity.
- Address how remote service activities may take advantage of the authentication structure.
- Address how remote service activities that affect machine authentication will be coordinated with the facility IT organization and other vendor equipment.
- Problems with machine authentication are detected and correctable in such a way that they do not affect patient safety.

A.2 Technical Guidelines

A.2.1 Guidelines for Healthcare Providers

A.2.1.1 Certificate authority

The enterprise may subcontract some or most of this, but it cannot avoid this responsibility. The enterprise may choose to simply be a self-signing authority with no relationship to the national authentication hierarchies. In this case the self-signing authority might not be recognized by other computer networks.

The enterprise certificate authority must provide or at least authorize private keys and public certificates for all machines that are under enterprise control. If the enterprise has selected direct comparison, it can choose to use keys and certificates that are created by the machine itself, or by the machine vendor. For this approach the identity of the signing authority is unimportant, and self signed certificates are acceptable. The enterprise itself provides copies of the certificates to the other machines on the network and this act provides the authentication security. The enterprise must be able to provide both keys and certificates for machines as their old ones expire, and may prefer to provide its own keys and certificates rather than deal with vendor provided ones.

If the enterprise has selected a trusted signature chain based approach, the public certificates must be signed by the enterprise certificate authority. This can be a standalone certificate authority available from many vendors and operated by the enterprise. This duty can also be subcontracted, but the trust should be limited to the subroot assigned for this specific enterprise.

The enterprise CA may be part of a national or regional chain of CAs, or it may be a private CA operating on its own authority. These requirements are normal features for all CA products and services.

A.2.1.2 Media distribution

Keys, certificates, and CRLs can be moved on media. The media must be either carefully protected or securely destroyed after use. X.509 certificates are small, only a few thousand bytes, so the choice of media is driven by the operational needs of distributing it, using it, and securing it. CDROM media is inexpensive, usually easy to use, easy to distribute and control, and easy to destroy by shredding. Portable flash memory devices can also be used, but special procedures must be used to ensure 100% erasure when their use is complete.

A.2.1.3 Network distribution

The labor effort needed to transfer certificates for direct comparison can be reduced by using a Certificate Server. With a Certificate Server each individual machine can query a trusted server to obtain public certificates. The individual machine only needs to have the location of the trusted server and its public certificate. The communications between the individual client machines and the certificate server do not need to be encrypted because the public certificates can be public knowledge.

The use of a certificate server does introduce a potential reliability and performance bottleneck.

A.2.1.4 Expiration and replace policies

- Expiration is recommended to be two (2) years, although local considerations can change this.
- Creating replacement certificates should follow the same procedure as creating new certificates. Re-issuing old certificates with revised expiration dates is a poor security practice.

Most medical equipment is in a low threat environment and may set key lengths at 1024.

A.2.2 Guidelines for Vendors

A.2.2.1 Public/private key pairs management

Machines must provide a means of generating or accepting as well as protecting private keys. Some machines can generate their own private key because they have an adequate random number generator. Those machines should use PKCS#8 to request a public certificate from the hospital certificate authority. All machines should be able to get their public/private key pair from the certificate authority, using PKCS#12.

Machines must accept new keys from authorized service staff to replace keys that have been lost or compromised.

A.2.2.2 Certificate Contents

The certificate may contain additional information describing the system that is used by field service and other staff to understand the purpose of a particular certificate. The key size selection and expiration are the only mandatory fields.

A.2.2.2.1 Key Size

The equipment must support key lengths from a 512 bit minimum, up to 4096 bit maximum. The actual key length used is defined by site policy. For financial and other purposes, as of September 2006 the Web Services Interoperability (WS-I) organization recommends a length of 1024.

A.2.2.2.2 Machine Identification

It can be useful to encode the machine serial number, asset tag identifier, and similar information into the descriptive fields of the certificate. This helps operational users to identify the correct certificate for use on other systems. This should only be done for information that is not likely to change.

A.2.2.2.3 Network Identification

Hostname and similar information can be useful, and can be encoded into the certificate. This should not be done with information that is likely to change during network reconfigurations, because that could invalidate certificates.

A.2.2.2.4 Organization Information

Organization name and related information can be encoded into the certificate.

A.2.2.2.5 Certificate Purpose

These certificates can be used for encryption, signature, and node authentication. A different certificate must be used for digital signatures by people. This signature only implies that this machine created the data.

A.2.2.2.6 Expiration

The recommended expiration policy is to assign certificates a two-year life. Local risk analysis may change this. Longer validity periods increase the risks of theft and exposure. Shorter periods increase the maintenance costs of replacing expired certificates.

A.2.2.2.7 Encoding

The system should support both BER and DER encoding because both are commonly found.

A.2.2.2 Media distribution

The equipment must be able to accept public/private key pairs, public certificates and CRL from media. The equipment must be able to export both certificate requests and public certificates on media.

A.2.2.3 Network distribution

The client machine may need to ensure that it is communicating with the authoritative source of public certificates, so the public key of the server must be manually installed on the client machines. The DICOM configuration management services defines the use of an LDAP server to provide public certificates for DICOM equipment. The equivalent standards for finding certificates for HL7 and Web Services have not been written. LDAP services are an effective means of providing the public certificates for both people and machines.

The client machines should cache public certificates and the CRL or provide a means of manually storing public certificates and the CRL locally to avoid performance and reliability issues. This cache can be used when the certificate server is not available, either because of problems or because the client machine is operating in a mobile environment.

A.2.2.3 Private key use

The machines must have strong internal security to protect the private key. The means to accomplish this vary widely, but the private key must be protected against copying or viewing, because its exposure would permit improper use and masquerading by other systems.

Applications should share the machine private keys when practical. There is no functional need to use a different kind of certificate for machine authentication over different communications protocols and for different applications. For example, an application that implements both HL7 and DICOM communications can share the same key for both. But it may be impractical for some of the software installed on one system to share a single key. We recommend having a limited number of private keys per machine to simplify management of certificates. Reducing the number of keys and certificates reduces the record keeping burden on the certificate authority and IT administration.

A.2.2.4 Separation of access control from authentication

Machines should not use the machine authentication certificate as a substitute for access controls. For example, a client machine may be restricted to access only one service of many that are available on a server machine. The access control step is not described in detail in this white paper.

A.2.2.5 Authentication mechanisms

The equipment must support both direct comparison and trusted signature chain, because the healthcare provider will choose the authentication method.

A.2.2.6 Continuity assurance

The authentication mechanisms should be configurable to accommodate changes due to disaster and other problems. All should be rapidly re-configurable down this list. All equipment must support 3, 4, and 5 below. 1 and 2 are at the vendor’s discretion.

1. Chained signature, access to remote revocation service – must gracefully degrade to 3 in the event of problems
2. Direct, server distribution of trusted certificates – must gracefully degrade to 4 in the event of problems
3. Chained signature, revocation list manually distributed.
4. Direct, trusted certificates manually distributed
5. Authentication disabled (break glass)

The machine must have tools to support the return to normal operation after a period of operation in downgraded mode.

Acronyms

BER	Basic Encoding Rules for ASN.1 encoding an object into a byte sequence
CA	Certificate Authority
CAD	Computer Aided Diagnosis
CRL	Certificate Revocation List
CT	Computed Tomography
DER	Distinguished Encoding rules for encoding an ASN.1 object into a byte sequence
DICOM	Digital Image Communications for Medicine (a standards development organization). (http://medical.nema.org)
HIPAA	Health Insurance Portability and Accountability Act
HIS	Hospital Information System
HL7	Health Level 7 (a standards development organization). (http://www.hl7.org)
HTTP	Hypertext Transport Protocol, RFC-2616
HTTPS	Hypertext Transfer Protocol (secure). The TLS protected version of HTTP.
IHE	Integrating the Healthcare Enterprise
IPSEC	Internet Protocol Security
IT	Information Technology
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
PACS	Picture Archive and Communication System
PKCS	Public Key Cryptography Standards, see http://www.rsasecurity.com/rsalabs/node.asp?id=2124
PKI	Public Key Infrastructure
RIS	Radiology Information System
SOAP	Simple Object Access Protocol
SPC	Security and Privacy Committee
SSL	Secure Socket Layer
TLS	Transport Level Security, RFC-2246
ATNA	Audit Trail and Node Authentication (an IHE profile)
WS-I	Web Services Interoperability (http://www.ws-i.org/)