The Center for Medical Interoperability Technical Report
Considerations for Certificate Lifecycle

CMI-TR-CLC-D02-2019-05-31

Draft

Notice

This technical report is the result of a cooperative effort undertaken at the direction of the Center for Medical Interoperability™ for the benefit of the healthcare industry and its customers. You may download, copy, distribute, and reference the documents herein only for the purpose of developing products or services in accordance with such documents, and educational use. Except as granted by The Center in a separate written license agreement, no license is granted to modify the documents herein (except via the Engineering Change process), or to use, copy, modify or distribute the documents for any other purpose.

This document may contain references to other documents not owned or controlled by The Center. Use and understanding of this document may require access to such other documents. Designing, manufacturing, distributing, using, selling, or servicing products, or providing services, based on this document may require intellectual property licenses from third parties for technology referenced in this document. To the extent this document contains or refers to documents of third parties, you agree to abide by the terms of any licenses associated with such third-party documents, including open source licenses, if any.

DISCLAIMER

This document is furnished on an "AS IS" basis and neither The Center nor its members provides any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein. Any use or reliance on the information or opinion in this document is at the risk of the user, and The Center and its members shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, or utility of any information or opinion contained in the document.

The Center reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein.

This document is not to be construed to suggest that any company modify or change any of its products or procedures, nor does this document represent a commitment by The Center or any of its members to purchase any product whether or not it meets the characteristics described in the document. Unless granted in a separate written agreement from The Center, nothing contained herein shall be construed to confer any license or right to any intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

Table of Contents

Document Status Sheet

Document Control Number:	CMI-TR-F-SEC
Document Title:	Security Considerations for Foundational Efforts
Revision History:	D02 IPR Review
Date:	04/21/2019
Status:	Draft
Distribution Restrictions:	Public

Key to Document Status Codes

Work in Progress An incomplete document designed to guide discussion and generate feedback that may include several alternative requirements for consideration.

Draft A document considered largely complete but lacking review by Members and vendors. Drafts are susceptible to substantial change during the review process.

Issued A generally public document that has undergone Member and Technology Supplier review, cross-vendor interoperability, and is for Certification testing if applicable. Issued technical reports are subject to the Engineering Change Process.

Closed A static document, reviewed, tested, validated, and closed to further engineering change requests to the technical report through The Center.

1 Scope

1.1 Introduction and Purpose

This technical report outlines some considerations for certificate lifecycles. Specifically, the report discusses the rationale for security of PKI based identities, private key storage, and certificate validity periods. At this point in time this report is informative only and is intended to foster comprehensive discussion of these factors with the goal of ensure foundational efforts by The Center are well supported by members and implementable by vendors.

1.1.1 Introduction

Public Key Infrastructure is the basis for trust for the CMI interoperable health architecture. The CMI Public Key Infrastructure issues certificates for all connected components that attest the validity of the identity of those components and binds certificates to identities using public/private key pairs through asymmetric cryptography. The result is attestable and approved identity association for all connected components. This process is the foundation that allows all secure interoperability within the architecture.

The Public Key Infrastructure (PKI) certificates matter a great deal to assuring the security of the CMI architecture. In 2017, private financial data of 145M individuals in 3 countries was compromised at Equifax. The breach leveraged a vulnerability in their Apache servers that allowed 9000 queries to 51 databases over a 76 day period. The volume of data exfiltrated from Equifax was impressive, and yet they failed to detect the exfiltration. The root cause of failing to detect the data leak was due to use of an outdated certificate. Specifically, the attackers were able to use an "outdated certificate to… avoid tripping packet-inspecting security components". [DR-Equifax] Further details can be read in the Government Accounting Office report on the event. [GAO-Data-Protection] In fact, 90% of companies are attacked by adversaries using three-year-old vulnerabilities. [BC-Vulnerabilities]

The technology and practices to implement PKI are very mature and best practices are well known. Ensuring the integrity of the PKI system requires only a few critical principals be rigidly applied:

- Certificate requests must be validated by an authority truly accountable for the outcome before signed certificates are issued by the certificate authority.
- Certificates must not be issued indefinitely. They must have an expiration that is determined based on the likelihood of their associated private key being compromised as a function of time.
- Certificates whose keys are known or suspected of being compromised must be revoked and authentication processes must validate whether keys are revoked prior to authorization.
- Certificate expiration must not be ignored. An expired certificate is not valid and access or authorization must not be provided.

- Finally, if an architecture leverages a PKI solution that allows for dynamic certificate issuance, or automated certificate renewal, those processes must not circumvent any of the previous four principals.

Of course, there are many other factors that must also be included to successfully implement a trust system using PKI. However, those must be executed sympathetic to the principals above.

This document discusses three areas of consideration in using PKI for secure clinical architectures. These are key storage, certificate expiration periods, and notions on a secure certificate renewal process under development at CMI. The reader is expected to be somewhat knowledgeable of PKI, but should not need to be an expert.

2 Informative References

This technical report uses the following informative references. References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific. For a non-specific reference, the latest version applies.

2.1 United States Government References

[GAO-Data-Protection] "DATA PROTECTION: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach" August 2018

https://www.gao.gov/assets/700/694158.pdf

[PPD-21] Presidential Policy Directive/PPD-21, “Critical Infrastructure Security and Resilience”, February 12, 2013

https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[EO-13636] Executive Order (EO) 13636, “Improving Critical Infrastructure CyberSecurity”, February 12, 2013

https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[FDA-OTS-1] "Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Devices, U.S. Department of Health and Human Services, Food and Drug Administration, Center for Devices and Radiological Health, Office of Compliance, Office of Device Evaluation" , September 9, 1999

https://www.fda.gov/downloads/MedicalDevices/.../ucm073779.pdf

[FDA-OTS-2] "Guidance for Industry Cybersecurity for Networked Devices Containing Off-the-Shelf (OTS) Software", January 14, 2005

https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077823.pdf

[FDA-CS-1] "Content of Premarket Submissions for Management of Cybersecurity in Devices, Guidance for Industry and Food and Drug Administration Staff", October 2, 2014

https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm356190.pdf

[FDA-LC] "Infusion Pumps Total Product Life Cycle Guidance for Industry and FDA Staff", December 2, 2014

https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm209337.pdf

[FDA-510K] "Deciding When to Submit a 510 K for a software change to an existing device", August 8, 2016

https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM514771.pdf

[FDA-CS-2] "Postmarket Management of Cybersecurity in Devices - Guidance for Industry and Food and Drug Administration Staff Document", December 28, 2016

https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

[FDA-PM] "Design Considerations and Pre-market Submission Recommendations for Interoperable Devices", January 26, 2016.

https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482649.pdf

[NIST-800-30] NIST SP 800-30, " Guide for Conducting Risk Assessments" , Sep 2012

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[NIST-800-37] NIST SP 800-37, Rev.1, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach”, February 2010

http://dx.doi.org/10.6028/NIST.SP.800-37r1

[NIST-800-38A] NIST SP 800-38A, “Recommendation for Block Cipher Modes of Operation - Methods and Techniques”, December 2001

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

[NIST-800-53] NIST SP 800-53, Rev. 4, “Security and Privacy Controls For Federal Information Systems and Organizations”, April 2013.

http://dx.doi.org/10.6028/NIST.SP.800-53r4

[NIST-800-64] NIST SP 800-64 Rev. 2, “Security Considerations in the System Development Life Cycle”, October 2008

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf

[NIST-800-61] NIST SP 800-61, Rev. 2, “Computer Security Incident Handling Guide”, January, 2004

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[NIST-800-65] NIST SP 800-65, “Integrating IT Security into the Capital Planning and Investment Control Process”, January 2005

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-65.pdf

[NIST-800-67] NIST SP 800-67, Rev 1, “Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher”, Jan 2012

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-67r1.pdf

[NIST-800-77] NIST SP 800-77, “Guide to IPsec VPNs”, December 2005

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-77.pdf

[NIST-800-160] NIST SP 800-160, “Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems”, November 2016

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

[FIPS-46-3] FIPS 46-3, “Data Encryption Standard (DES)”, October 1999

http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[FIPS-140-2] Security Requirements for Cryptographic Modules, FIPS 140-2, May 25, 2001.

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[FIPS-180-2] FIPS 180-2, “Secure Hash Standard (SHS)”, August 2002

http://csrc.nist.gov/publications/fips/fips180-2/FIPS180-2_changenotice.pdf

[FIPS-185] FIPS 185, "Escrowed Encryption Standard”, February 1994

http://csrc.nist.gov/publications/fips/fips185/fips185.pdf

[FIPS-186-2] FIPS 186-2, “Digital Signature Standard (DSS)”, January 2000

http://csrc.nist.gov/publications/fips/archive/fips186-2/fips186-2.pdf

[FIPS-197] FIPS 197, "Advanced Encryption Standard”, November 2001

http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[FIPS-198] FIPS 198-1, “The Keyed-Hashed Message Authentication Code (HMAC)”, July 2008

http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf

[FIPS-199] FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems”, Feb 2004

http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

[FIPS-200] FIPS 200, “Minimum Security Requirements for Federal Information and Information Systems”, March 2006

http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

[NSA-IATF-3.1] “Information Assurance Technical Framework (IATF)”, Release 3.1, NSA IA Solutions Technical Directors, September 2002

https://apps.dtic.mil/dtic/tr/fulltext/u2/a606355.pdf

2.2 Industry and International References

[DR-Equifax] "GAO Says Equifax Missed Flaws, Intrusion in Massive Breach" 9/10/2018

https://www.darkreading.com/attacks-breaches/gao-says-equifax-missed-flaws-intrusion-in-massive-breach/d/d-id/1332776

[BC-Vulnerabilities] "90% of Companies Get Attacked with Three-Year-Old Vulnerabilities" August 24, 2017

https://www.bleepingcomputer.com/news/security/90-percent-of-companies-get-attacked-with-three-year-old-vulnerabilities/

[IETF-RFC7030] Enrollment over Secure Transport

https://tools.ietf.org/html/rfc7030

[AAMI-TIR57] AAMI TIR57/Ed. 1, "Principles for device information security--risk management", June, 2016

http://my.aami.org/store/detail.aspx?id=TIR57-PDF

[IEC-80001-1:2010] ISO/IEC 80001-1 Ed.1: Application of risk management for it-networks incorporating medical devices – Part 1: Roles, responsibilities, and activities.

https://www.iso.org/standard/44863.html

[IEC 27005] ISO/IEC 27005:2011, " Information technology -- Security techniques -- Information security risk management", June, 2011

https://www.iso.org/standard/56742.html

[IEC 15408] ISO/IEC 15408-3:2008, "Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements", Aug, 2008

https://www.iso.org/standard/46413.html

[IEC 14971] ISO/IEC 14971:2007, "Medical devices -- Application of risk management to medical devices", Mar 2007

https://www.iso.org/standard/38193.html

[IEC 29147] ISO/IEC 29147:2014, "Information technology -- Security techniques -- Vulnerability disclosure", Feb, 2014

https://www.iso.org/standard/45170.html

[IEC 30111] ISO/IEC 30111:2013, “Information technology -- Security techniques -- Vulnerability handling processes”, Nov, 2013

https://www.iso.org/standard/53231.html

[IETF-RFC2196] IETF RFC 2196, “Site Security Handbook”, September 1997

https://tools.ietf.org/html/rfc2196

[IETF-ID-SCEP] IETF Internet-Draft, draft-gutmann-scep-05, “Simple Certificate Enrolment Protocol”

https://www.ietf.org/id/draft-gutmann-scep-05.txt

[IEC 62443-1] IEC TS 62443-1-1:2009 “Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models”, Sep 2009

https://webstore.iec.ch/preview/info_iec62443-1-1%7Bed1.0%7Den.pdf

[IEC 62443-2] IEC TR 62443-2-3:2015 “Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment”, Jun, 2015

https://webstore.iec.ch/publication/22811

[DT-Sec] Diabetes Technology Society, “Cybersecurity Standard for Connected Diabetes Device Security”, 2016

https://www.diabetestechnology.org/dtsec-standard-final.pdf

[DT-CDD] Diabetes Technology Society, “Protection Profile for Connected Diabetes Devices”, May, 2016

https://www.diabetestechnology.org/dtsec-protection-profile-final.pdf

[NEMA-MDS-2013] HIMSS/NEMA, “Manufacturer Disclosure Statement for Medical Device Security”, October, 2013

https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx

[CMI-DOC-TD] Terms and Definitions

https://medicalinteroperability.org/specifications

[BlueKrypt-Keylength-31] "Cryptographic Key Length Recommendation" - v 31.0 - June 10, 2018

https://www.keylength.com/en/4/

[CAB-CERT-LT] "Ballot 193 – 825-day Certificate Lifetimes" March 2, 2017

https://cabforum.org/2017/03/17/ballot-193-825-day-certificate-lifetimes/

2.3 Reference Acquisition

- Center for Medical Interoperability, 8 City Boulevard, Suite 203, Nashville, TN 37209; Phone +1-615-257-6410; http://medicalinteroperability.org/
- Internet Engineering Task Force (IETF) Secretariat, 48377 Fremont Blvd., Suite 117, Fremont, California 94538, USA, Phone: +1-510-492-4080, Fax: +1-510-492-4001, http://www.ietf.org

3 Terms and Definitions

This specification uses the terms and definitions in [CMI-DOC-TD]

4 Abbreviations and Acronyms

This specification uses the following abbreviations:

ECC	Elliptical Curve Cryptography
FIPS	Federal Information Processing Standard
IDS	Intrusuion Detection System
NIAP	National Information Assurance Partnership
PKI	Public Key Infrastrucuture
RSA	Rivest, Shamir, Adelman

5 Private Key Storage

Health system infrastructure has a great deal of variation in the types of components that are interconnected. There are entire texts devoted to this variation and a great deal of taxonomy and ontology work has been performed across the industry to try to provide a basis for intelligent discussion amongst professionals. For this discussion, we need to be concerned with variation specifically related to how components store the private key to which a certificate is bound and also how easy it may be for unauthorized personnel or processes to access the component. As we are primarily interested in networked data liquidity, we are mostly interested in Connected Components. This may be a medical device, platform services, a gateway, or any other type of networked resource which a health care system may connect. Unconnected components are not in scope.

It is increasingly common for keys and other cryptographic functions to be protected on dedicated, especially secure hardware. Several chip manufacturers, including Texas Instruments and Microchip, provide secure modules to be integrated onto solutions specifically for this purpose. For hardware based medical Connected Components, the degree of security can be graduated according to how easy an adversary, or other unauthorized party, may access the device to access the key. Trusted environments are those in which only authorized personnel can be expected to access a Connected Component (via physical or remote means); untrusted environments are areas in which it is not reasonable to expect only trusted personnel can access the Connected Component. In contrast, software based Connected Components may increase uncertainty on how keys might be stored.

We have identified three characterizations that fit within the context and scope discussed above. These are:

- Hardware based Connected Components in trusted environments.
- Hardware based Connected Components in untrusted environments.
- Software based Connected Components.

For readers with technical background here, use of Trusted Platform Modules and Hardware Security Modules will be considered in future vesions of Center Specifications. Similarly, dynamic trust issuance solutions such as IETF Enrollment over Secure Transport [IETF-RFC7030] may impact solutions in this space in the future.

The Center has specified key storage requirements for all three of the characterizations above. These are documented fully in CMI Specification Identity in section 6.13. The key security requirements for each characterization are discussed in the following sub-sections. It should be noted that compliance with these requirements may often be very hard to prove. Center certification of compliance of a given device for many of these requirements must simply be attested by the entity submitting devices for certifications (whether based on hardware or software). Moreover, the Center PKI Certificate Authority (or Registration Authority in the case of renewed certificates) has very little ability (perhaps none) to prove how certificates and keys are handled. This is usually attested by the organization responsible for the certificate subscriber through a business contract with the Certificate Authority.

Hardware based Connected Components in trusted environments

- The Connected Component SHOULD meet FIPS 140-2 security requirements for all instances of private and public permanent key storage.

- The Connected Component SHOULD meet FIPS 140-2 level 1 physical security requirements (production grade enclosure) if it will operate in a trusted environment that is only accessible by authorized hospital staff.

- An ECC or RSA Connected Component certificate, private key, and issuing CA certificate as defined in The Center's Certificate Policy SHALL be security installed in the Connected Component by the manufacturer.

- An ECC or RSA root certificate defined in The Center's Certificate Policy and authorized by The Center SHALL be installed in the Connected Component as a trust anchor for validating received certificates.

5.1 Hardware based Connected Components in Untrusted environments

- The Connected Component SHOULD meet FIPS 140-2 security requirements for all instances of private and public permanent key storage.

- The Connected Component SHOULD meet FIPS 140-2 level 3 physical security requirements (production grade enclosure) if it will operated in an untrusted environment where the public may have access.

- An ECC or RSA Connected Component certificate, private key, and issuing CA certificate as defined in The Center's Certificate Policy SHALL be security installed in the Connected Component by the manufacturer.

- An ECC or RSA Connected Component certificate issued for use on software based Connected Components SHOULD have relatively short (<2 years) Certificate expiration periods).

5.2 Software based Connected Components

- The Connected Component SHOULD store keys securely.

- The Connected Component SHOULD meet FIPS 140-2 level 1 (cryptographic module to be executed on general purpose computing system).

- The Connected Component SHOULD implement security requirements as specified in NIAP Protection Profile for Application Software (NIAP). In particular, storage of credentials SHOULD comply with FC-STO-EXT.1.

- The Connected Component SHOULD use secure HW such as a TPM.

- The Connected Component SHOULD apply access controls to protect certificates, private keys, and issuing CAs.

- A mitigating control, such as IDS, SHOULD be used to to detect unauthorized access to [credentials] installed on the component. Both external and internal mitigating controls SHOULD be used.

- An ECC or RSA Connected Component certificate, private key, and issuing CA certificate as defined in The Center's Certificate Policy SHALL be securely installed by trusted technical staff. Associated cryptographic material and software SHALL be controlled at all times.
- An ECC or RSA Connected Component certificate issued for use on software based Connected Components SHOULD have relatively short (<2 years) Certificate expiration periods).

6 Certificate Expiration Periods

6.1 Considerations in Choosing Expiration Periods

An interesting aspect about the expiration period of PKI certificates is that the expiration is not really about the certificate. Rather, it's about the private key. Specifically, the expiration period is a set date in time reflecting how long the private key can be kept safely. There are two primary factors in determining this date. The first is how long might it take to factor (break) the key through brute force. For example, lets guess that today it might take up to 20 years to exhaustively factor a 2048-bit RSA key (this period of time is illustrative only). This is, however, a random process, and luck applies. So average luck would force the key in 10 years. So, perhaps the expiration period for a for an RSA based certificate for a 2048-bit key should be less than 10 years.

The second factor in determining the certificate expiration period must consider that the location in which the private keys are stored may be directly compromised. How likely this is depends on how securely the key is stored. A key stored in software is generally easier to compromise than something stored on a Trusted Platform Module.

In addition to the primary factors, we can also consider how long a given type of subscriber should be authorized to access resources. If we know, for example, perhaps the given calibration of a networked sensor is only suitable for three years and the sensor will (should) be disposed of at that time. Deploying a corresponding certificate with an expiration period of three years seems prudent and will help ensure an adversary cannot use the key and certificate from the device if somehow compromised after disposal.

Finally, when certificates are used for authentication, part of the verification process includes checking the validity of the certificate of the issuing Certificate Authority (e.g., certificate chaining). Consequently, there is a relation in a given subscriber certificate and the validity period of the certificate for the issuing Certificate Authority. A Certificate Authority should not issue subscriber certificates valid beyond their own validity period.

There is, as already stated, a wide range of devices, uses, and environments used or encountered in health care. The cybersecurity risks of the key compromise vary accordingly as do the consequences of key compromises. In reality, the choice of a certificate expiration period is actually a bet of how long a given key can be protected for a given application. Factors against the desired outcome include:

- The ability to protect keys continually decreases over time because the ability to factor keys continually improves – non-linearly and non-predictably.
- Systemic faults in cryptography solutions are frequently discovered and operational errors in the distribution and management of keys may occur and be realized at some random future time.
- There are anticipated threats to cryptography, including use quantum computing to accelerate cryptanalysis, that will decrease the period of time a given key type and length can be protected.

It is important to accept that the bet made is not an "if a key will be compromised" but, rather, "how long will it be till a key is compromised". In other words, the design constraint is that any specified certificate expiration period chosen now will, at some non-deterministic point of time in the future, be proven insufficient.

Consequently, the organizations that are responsible for the cybersecurity outcomes – hospitals and vendors – should choose appropriate key expiration. This should be done after diligent analysis of the risks for a specific environment, the specific systems used to provide care, and the use cases in which the keys will be used to protect patients' interests. This choice should be made at the time Certificate Signing Requests are submitted to the PKI Certificate Authority.

6.2 Examples of Certificate Validity Periods

While choice of expiration periods must remain the responsibility of security professionals at hospitals and vendors, it is useful to provide an example of possibly prudent certificate validity periods. Some samples are provided below. These should be considered in context of the time this report was written (September 2018) and represent the longest expiration periods that might be considered responsible at that time.

- Manually deployed and installed certificates on hardware based devices: As long as the anticipated life of the device or as long as the maintenance or refresh cycle of the device, not to exceed 20 years assuming reasonable protection of the private key.
- Manually deployed and installed certificates on software based deployment on devices with a Trusted Platform Module (or equivalent): Same as above, assuming verification is performed to validate that the Trusted Platform Module is, in fact, where the key and certificate are actually deployed. (Even on systems with Trusted Platform Modules, applications must be coded to leverage the module.)
- Deployment on servers or software systems: As short as vendors and hospitals can operationally accommodate, not to exceed 2 years. This may seem a very short period of time, but is consistent with guidelines from both NIST [BlueKrypt-Keylength-31] and the CA/Browser Forum [CAB-CERT-LT] at the time of writing.
- If and when automatic renewal is used to support dynamic deployment of new certificates: Perhaps only 90 days. However, some science and engineering is required to fully understand the failure modes that may be introduced by such a strategy.

- Regardless of the deployment models above, certificate expiration should never be longer than the expiration date of the signing Certificate Authority.

7 Certificate Renewal

It essential that expired certificates be rejected during access and authorization attempts. To ensure valid Connected Components are able to perform necessary clinical functions with no or minimal risk related to certificate management, the Center is developing a process for automatic renewal of certificates. This section overviews the basic notions of this process.

7.1 Rationale

Intuitively, it might seem updating or renewing a certificate should occur in the same way certificates are issued. However, this is not actually completely necessary. We should establish an on-line, automated renewal process to allow Connected Components that are valid and necessary to receive new certificates when their current certificates are expiring. Moreover, this process should apply to systems that are hardware or software based regardless of whether the vendor or the hospital installed the certificate. Finally, since the Connected Component already has a current valid certificate, it actually seems more secure to do on-line automatic certificate renewal than on-line, automatic certificate issuance (using a process such as Enrollment over Secure Transport).

The process proposed will automate proactive certificate expiration management. Certificate renewal requests can be submitted prior to expiration by the Connected Component on which the expiring certificate is deployed. Corresponding alerts (alarms/notifications) of expiration can be triggered prior to expiration, and can even include escalation according to how soon the certificate will expire.

Some engineers have suggested that we specify a grace period for certificate renewal. However, given a process to gracefully manage certificate expiration this seems unnecessary.

7.2 Initial Requirements

What might the design requirements be for certificate renewal management? The Center has compiled the following requirements, which are anticipated to become normative as specifications are completed:

- Certificate renewals SHALL be submitted 2 months prior to expiration by the device on which the certificate is expiring.
    - An information alert (“blue”) SHALL also be sent to the appropriate management servers.
    - NOTE: We could provide varied behavior by including an extension that allows certs to be renewed proactively (a renewal period window).

- An alert SHALL be sent to the appropriate management servers 1 month prior to expiration by the device; this SHALL be a “yellow” alert and SHALL escalate to “red” as expiration nears.
    - A peer MAY optionally notify that a peer’s cert is expiring.
- Certificate renewal requests SHALL be vetted and subsequently signed by an appropriate Registration Authority and forwarded to the appropriate Certificate Authority.
- Certificate renewals SHALL be issued only for currently valid certificates (certificates included in renewal Certificate Signing Request SHALL NOT be expired and must chain to a valid Certificate Authority).

7.3 Initial Sequence Diagram

The easiest way to illustrate this process is to provide a sequence diagram. This is shown in Figure 1. The diagram shows interactions and functions performed by a Subscriber, Registration Authority (RA), Management Entity, and Certificate Authority (CA). The Subscriber is a Connected Component on which a CMI PKI certificate has previously been installed. The Registration Authority is responsible for ensuring that the Connected Component is valid and should receive a new certificate. The Registration Authority is likely within the hospital, but may alternatively be a function provided by a vendor or perhaps even the CMI. The Management Entity is an IT resource that provides a capability for managing certificate status – it might be a manager or managers or integrated into another resource (perhaps even a Gateway or Platform Services). It’s primary function here is to provide IT staff awareness of certificate life cycle functions. Finally, the Certificate Authority provides final signing that attests the validity of a new certificate.

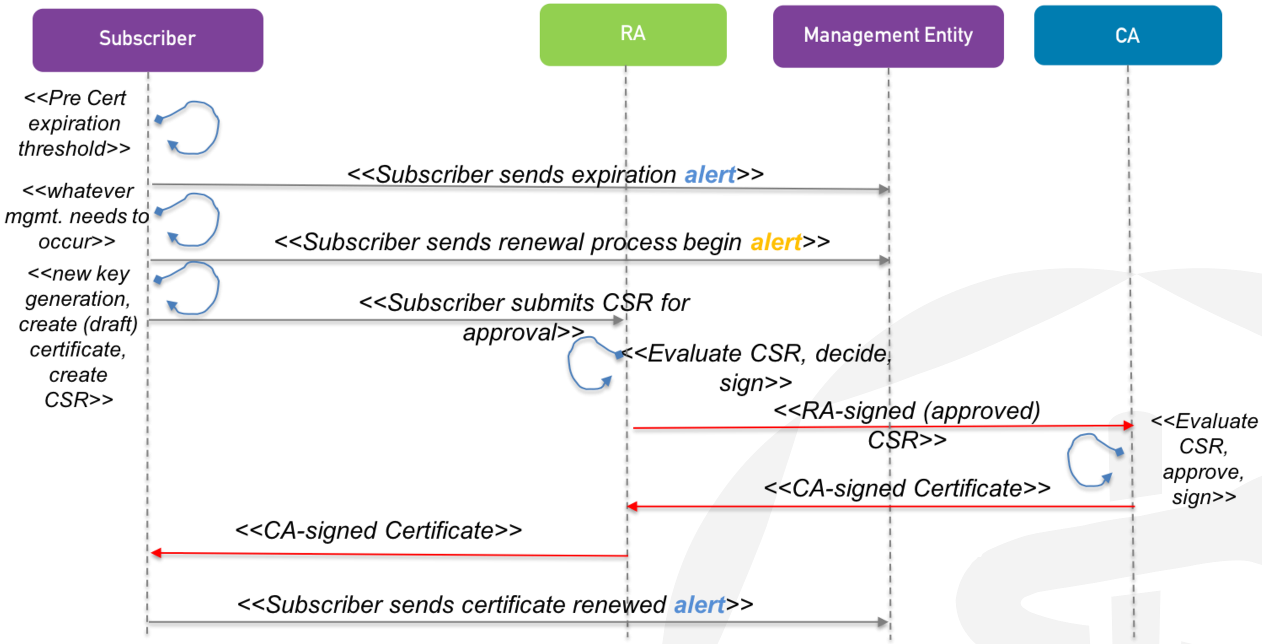
Subscriber
RA
Management Entity
CA
<<Pre Cert expiration threshold>>
<<Subscriber sends expiration alert>>
<<whatever mgmt. needs to occur>>
<<Subscriber sends renewal process begin alert>>
<<new key generation, create (draft) certificate, create CSR>>
<<Subscriber submits CSR for approval>>
<<Evaluate CSR, decide, sign>>
<<RA-signed (approved) CSR>>
<<Evaluate CSR, approve, sign>>
<<CA-signed Certificate>>
<<CA-signed Certificate>>
<<Subscriber sends certificate renewed alert>>

Figure 1: Certificate renewal sequence diagram

8 Certificate Revocation

Certificates are revoked by the CA when there is no longer confidence in the security of the keys associated with a certificate, such as when a device has been compromised. Certificates may also be revoked by the CA when the certificate and associated keys are no longer needed, such as when a device is no longer safe to use. This raises serious concerns for clinical reliability. Of course, revocation is an absolutely necessary process to ensure the security of any system using PKI. So the challenge in the clinical environment is to enable proactive management of certificate revocation in a manner that scales well for technical staff.

There are three circumstances of how revocation may occur. These are listed below:

- Self-revocation: A Connected Component may revoke its own certificate – self-revocation. This is useful for an expiring certificate that has been renewed as described above. It is also useful when the Connected Component has reached end-of-life and is no longer useful.
- Revocation by the RA: Hospital staff or vendors may recognize that a Connected Component is no longer useful or lose confidence in the component (because of suspected or known tampering or compromise). They may then have the Registration Authority responsible for the Connected Component revoke the certificate(s) associated with the component.
- Revocation by CA: The CA may be advised by a 3rd party that a Connected Component is unsafe or has been compromised (not directly responsible for the certificates issued to a Connected Component).

Traditionally, certificate revocation is a manually intensive deliberate process executed by staff at the CA. The CA receives a revocation request (on-line, through email, or even phone) by an entity vetted a priori (e.g., they have a business relationship and have been verified by the CA). The CA then does a rather exhaustive validation that the certificate has in fact been compromised with the responsible entity. Once confident the revocation requested is valid and warranted, the CA will execute the processes to add the revoked certificate to the revocation verification systems in use (typically CRLs and OCSP servers). The deliberate process here, which can take days to weeks, ensures that revocation cannot be leveraged as a denial of service attack vector.

However, this process does not meet the need of the health industry. Revocation occurs far too slowly and does not adequately advise clinical IT staff of changes in Connected Component status. A more automated process that includes some form of alerts of revocation is necessary.

The first two cases above – self-revocation and revocation by the RA – are being requested by trusted entities directly responsible for the outcome of their request. The associated revocation request can still be signed by a current and verifiable certificate – namely, that of the Connected Component or the RA. Therefore, signed revocation requests by self (the Connected Component) or the RA can be automatically processed. The RA handles both cases and is responsible for advising a management entity so IT staff can be aware of the revocation. The RA will relay self-signed and will send RA-signed revocation requests directly to an entity (server) managed by the CA that issued the certificate. It must be emphasized that this entity is part of the CA and the CA will implement appropriate procedures and practices necessary for securely processing automatic revocation request to prevent misuse.

In the case where a 3rd party requests revocation, manual processes requiring human verification at the CA and RA are still required. In some cases, the CA may be compelled to revoke certificates against the objection of the responsible RA (e.g., in the case the RA has been compromised or has not executed certificate responsibilities in accordance with the guiding Certificate Policy). However, when revocations occur in this way, the CA can send appropriate notifications to the RA and the RA can send corresponding alerts to the a management entity so IT staff can again be aware of the revocation.

These three processes are illustrated in the following figures. The diagrams shown are notional, reflecting designs still under consideration at the time of writing this document.

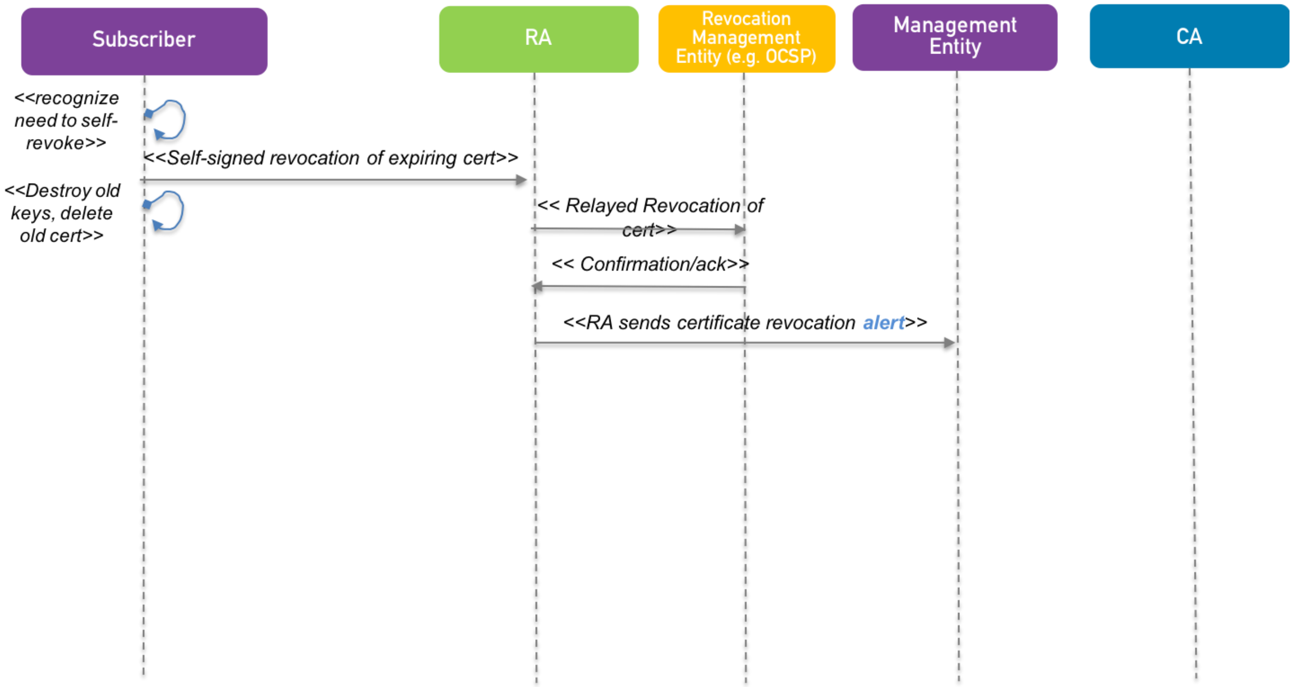
Subscriber
RA
Revocation Management Entity (e.g. OCSP)
Management Entity
CA
<<recognize need to self-revoke>>
<<Self-signed revocation of expiring cert>>
<<Destroy old keys, delete old cert>>
<< Relayed Revocation of cert>>
<< Confirmation/ack>>
<<RA sends certificate revocation alert>>

Figure 2: Automated certificate self-revocation with alerting

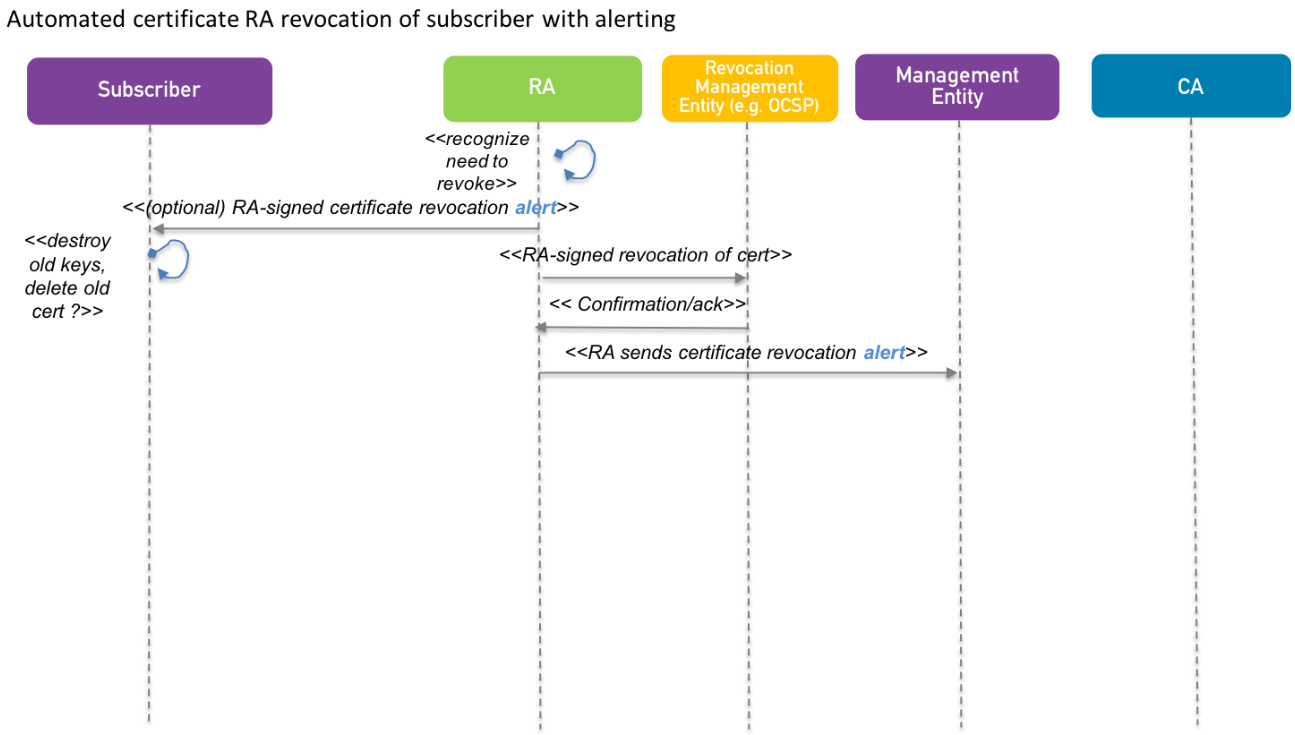
Automated certificate RA revocation of subscriber with alerting
Subscriber
RA
Revocation Management Entity (e.g. OCSP)
Management Entity
CA
<<recognize need to revoke>>
<<(optional) RA-signed certificate revocation alert>>
<<destroy old keys, delete old cert ?>>
<<RA-signed revocation of cert>>
<< Confirmation/ack>>
<<RA sends certificate revocation alert>>

Figure 3: Automated certificate RA revocation of subscriber with alerting

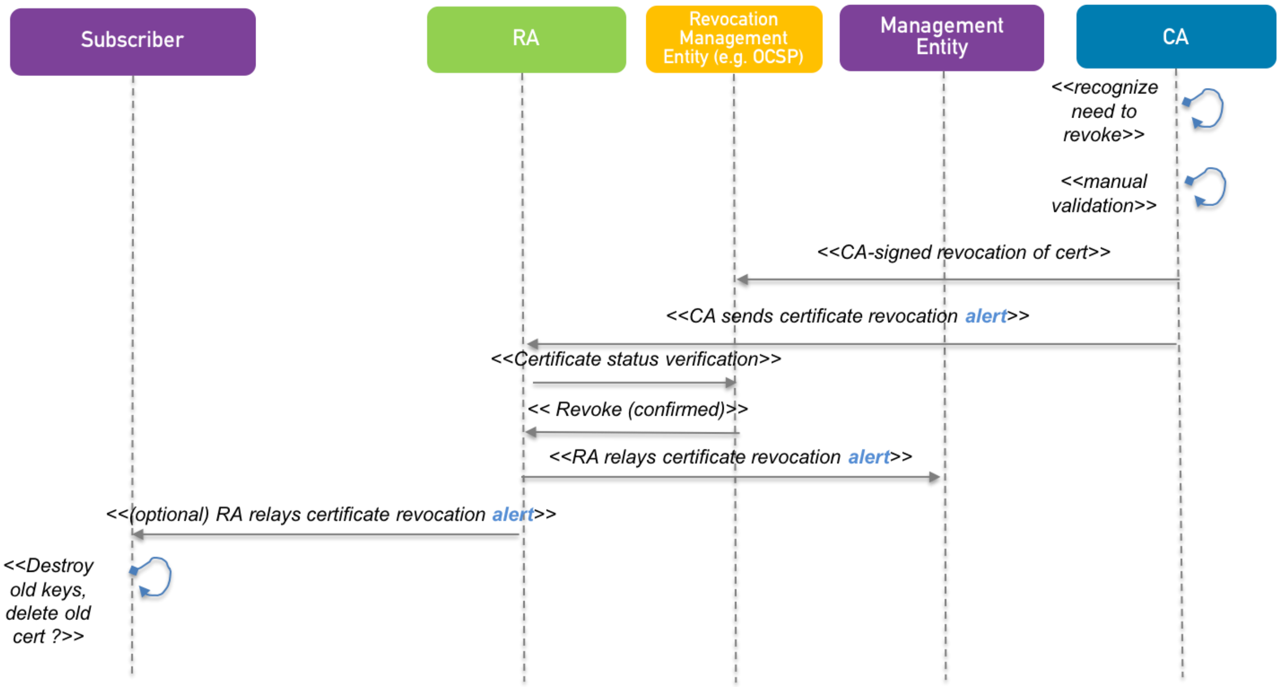
Subscriber
RA
Revocation Management Entity (e.g. OCSP)
Management Entity
CA
<<recognize need to revoke>>
<<manual validation>>
<<CA-signed revocation of cert>>
<<CA sends certificate revocation alert>>
<<Certificate status verification>>
<< Revoke (confirmed)>>
<<RA relays certificate revocation alert>>
<<(optional) RA relays certificate revocation alert>>
<<Destroy old keys, delete old cert ?>>

Figure 4: Certificate revocation by third party alert of subscriber with alerting

9 Conclusion

This document has outlined a variety of considerations for PKI certificate lifecycle management. Private key storage considerations were detailed and the Center's current specification on key storage were presented. This provided the basis for understanding issues related to determining certificate expiration periods. Specifically, choosing certificate expiration periods is very specific to the application in which the private key will be stored and used. A process for graceful management of certificate expiration was outlined. Finally, processes for graceful management of certificate revocation was presented.

These four areas bolster the foundational trust approach CMI uses for security. The approaches respond to real threats demonstrated in other trust systems; and, these approaches address the unique needs of clinical connected technologies.

10 Acknowledgements

The Center and its member companies would like to extend a heartfelt thanks to all those who participated in the development of this document.

Steve Goeringer authored this document. Special thanks to those who were directly involved via a variety of discussions, reviews and input: **Massimiliano Pala**, **Sumanth Channabasappa**, and **Chris Riha**.

This work was conducted within the Center's Security working group which is led by Steve Goeringer and, whose members have including the following part-time and full-time participants during the creation of this version of the document:

Chris Riha is the CMI Lead for this document, and was edited by Jesse Hanson . This document was primarily discussed and reviewed within The Center's Security Working Group, with additional input from the Architecture & Requirements, and Connectivity Working Groups. The part-time and full-time working group participants, additional offline reviewers, and their affiliations are listed below:

Working Group Participants	**Company Affiliation**
Aishwarya Muralidharan	vTitan
Alex Poiry	Cerner
Ali Nakoulima	Cerner
Andrew Meshkov	86Borders
Brian Long	Masimo
Brian Scriber	CableLabs
Bruce Friedman	GE Healthcare
Corey Spears	Infor
Darshak Thakore	CableLabs
David Hatfield	Becton Dickenson
David Niewolny	RTI
Eldon Metz	Innovision Medical
George Cragg	Draeger
Guy Johnson	Zoll
Ian Sherlock	Texas Instruments
James Surine	Smiths-Medical
Jason Mortensen	Bernoulli Health
Jay White	Laird
Jay White	Laird

Working Group Participants	**Company Affiliation**
Jeffrey Brown	GE
JF Lancelot	Airstrip
John Barr	CableLabs
John Hinke	Innovision Medical
John Williams	FortyAU
Kai Hassing	Philips
Ken Fuchs	Draeger
Logan Buchanan	FortyAU
M Prasannahvenkat	vTitan
Massimo Pala PhD	CablelLabs
Mike Krajnak	GE
Milan Buncick	Aegis
Neil Puthuff	RTI
Neil Seidl	GE
Ponlakshmi G	vTitan
Scott Eaton	Mindray
Stefan Karl	Philips
Travis West	Bridge Connector

- Sumanth Channabasappa (Chief Architect), Steve Goeringer (Security Architect), Chris Riha (Working Groups Lead), Paul Schluter, Bowen Shaner, Jacob Chadwell, David Fann, Spencer Crosswy, Dr. Richard Tayrien, Trevor Pavey; and, Ed Miller (CTO) - The Center