CENTER for MEDICAL INTEROPERABILITY

The Center for Medical Interoperability Specification Identity

CMI-SP-F-ID-D01-20190311

DRAFT

Notice

This specification 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.

Document Status Sheet

Document Control Number:	CMI-SP-F-ID-D01-20190311			
Document Title:	Identity			
Revision History:	D01			
Date:	March 11, 2019			
Status:	~~Work in Progress~~	**Draft**	~~Issued~~	~~Closed~~
Distribution Restrictions:	~~Author Only~~	~~The Center/Member~~	~~The Center/ Member/ NDA Vendor~~	**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 in specification format 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 Specifications are subject to the Engineering Change Process.
Closed	A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through The Center.

Contents

Figures

Tables

1 Scope

1.1 Introduction and Purpose

- The Center for Medical Interoperability is a 501(c)(3) organization led by members to change how medical technologies work together. Specifically, CMI aims to improve information flow and make technology function seamlessly in the background to achieve the best possible outcomes for patients. This goal of interoperability is in support of CMI's members' commitment to improve patient safety, care quality and outcomes, and reduce clinician burden and waste.

- This document specifies identity of Connected Components. Connected Components include medical devices, gateways, interoperability platforms, and other servers that connect to these CMI architecture elements as illustrated in Figure 1. These components may be hardware or software-based. Identity is the basis on which trusted connectivity and usage must be based. CMI identity will be based on a Public Key Infrastructure (PKI) certificate which will include a public key, unique identifier, and other information as defined in the CMI Certificate Policy. Certificate management will be rooted to the CMI Certificate Authority supported and facilitated by multiple subordinate certificate authorities.

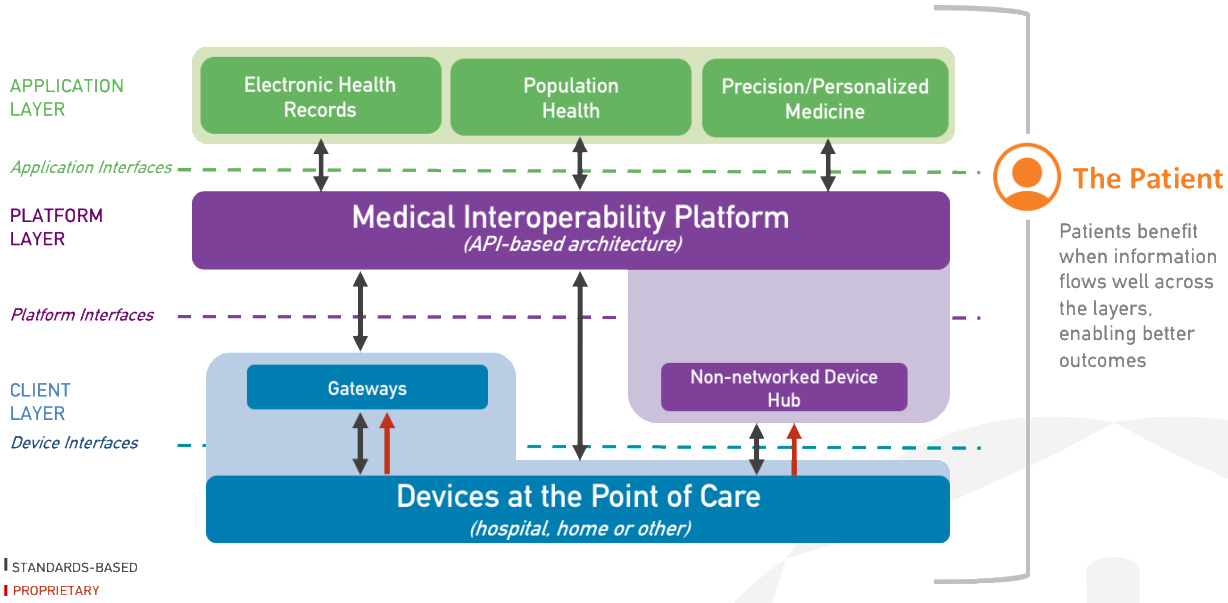

Figure 1: High-level Architecture

A core element of identity is use of a unique identifier. The unique identifier used for CMI identity comprised of a string, uniquely identifying both the requesting organization (typically a vendor) and the actual connected component. The identifier will be used in the CMI RSA and ECC Subscriber Certificates. When paired with a private key, the identifier and associated certificate creates an immutable identity which can be used by a variety of functions to enable secure interoperability.

1.2 Requirements

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

"SHALL"	This word means that the item is an absolute requirement of this specification.
"SHALL NOT"	This phrase means that the item is an absolute prohibition of this specification.
"SHOULD"	This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
"MAY"	This word means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

2 References

2.1 Normative References

This specification uses the following normative references.

[CMI-DOC-TD]	“Terms and Definitions”, Center for Medical Interoperability, Mar. 2019 https://medicalinteroperability.org/specifications/D01/CMI-DOC-TD-D01-20190311.pdf
[CMI-SP-F-CP]	“Certificate Policy”, Center for Medical Interoperability, Mar. 2019. https://medicalinteroperability.org/specifications/D01/CMI-SP-F-CP-D01-20190311.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

[IETF-RFC5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008

https://tools.ietf.org/html/rfc5280

2.2 Informative References

This specification uses the following informative reference.

[CMI-TR-F-SEC] "Security Considerations for Foundational Efforts", Center for Medical Interoperability, Mar. 2019.

https://medicalinteroperability.org/specifications/D01/CMI-TR-F-SEC-D01-20190311.pdf

2.3 Reference Acquisition

Center for Medical Interoperability, 8 City Boulevard, Suite 203 | Nashville, TN 37209;
Phone +1-615-257-6410; http://medicalinteroperability.org/

3 Terms and Definitions

This document relies on the terms and definitions specified in [CMI-DOC-TD].

4 Abbreviations and Acronyms

This specification uses the following abbreviations and acronyms:

ABAC	Attribute Based Access Control
API	Application Programming Interface
CP	Certificate Policy
EST	Enrolment over Secure Transport
FQDN	Fully Qualified Domain Name
HIBCC	Health Industry Business Communications Council
ICCBBA	International Council for Commonality in Blood Banking Automation
IMEI	International Mobile Equipment Identity
NIAP	National Information Assurance Partnership

OUI	Organizational Unique Identifier
PKI	Public Key Infrastructure
RBAC	Role Based Access Control
SCEP	Simple Certificate Enrollment Protocol
SN	Serial Number
UDI	Unique Medical Device Identification
UUID	Universally Unique Identifier

5 Identity

CMI defines identity as "The set of characteristics, including PKI certificates, network addresses, and user accounts (user ID and password) by which and individual or device is uniquely recognizable." This technical report overviews CMI's approach to identity. Identity will be comprised of a public key and unique identifier that is included in a subscriber certificate as specified in in [CMI-SP-F-CP]. The certificate may include other information as specified in the [CMI-SP-F-CP], such as network addresses, certain permanent configuration information, and other information. Identity will be applied to all network components that are part of the CMI architecture. Connected Components include medical devices, gateways, interoperability platforms, and other servers that connect to these CMI architecture elements. These components may be hardware or software based.

The CMI identifier will be an assigned code that ensures an identity will be unique across the entire scope of CMI's trust system. Since the identifier is included in the subscriber certificate, the CMI scope includes both space and time. An identifier SHALL never be reused and any certificate containing an identifier SHALL be revocable and SHALL eventually expire. There may be other useful functions enabled by certificate based identity or the corresponding identifiers, such as indicating the manufacturer of the device or even care system or device type. These other uses are out of scope of this document.

Connected Components and servers to which they connect may participate in other trust systems. Consequently, these systems and end devices may have certificates in addition to CMI issued certificates for use by vendors and system operators (such as the hospital or care provider).

5.1 Identity Overview

Identity in the CMI trust ecosystem includes at minimum a unique identifier and a PKI public key that are included in a subscriber certificate as specified in the CMI certificate policy. The identifier uniquely identifies a Connected Component on the network and within the data liquidity scope in which it participates. Common uses of device identity include, but are not limited to:

- Network and service access authentication
- Device verification when performing authentication (is this the correct device?), including device-to-device authentication
- Identification of devices for management, provisioning, or patient association by Platform applications

CMI considered multiple options for device identifiers including MAC address, the FDA Unique Medical Device Identification (UDI), and GSMA International Mobile Equipment Identity (IMEI). The MAC address on medical devices may be associated with a module or network interface card that is replaceable and so is not suitable as a device identifier. Moreover, components with both wireless and wired interfaces will have multiple MACs. Not all CMI architecture elements are controlled under the FDA guidelines and so may not have a UDI. IMEIs are primarily used on cellular networks to identify mobile devices. However, most CMI devices will not be connecting to cellular networks and many will not be considered mobile.

Two certificate issuance models for identity management need to be considered by the Center. One is a static certificate issuance process in which a certificate is permanently associated to a single specific device and, typically, will not change during the life cycle of the device by the manufacturer. If the device is found to be compromised, the certificate may be revoked. If the certificate expires, the device will not be able to access the network or services. (There are processes that might be used for renewing or issuing new certificates, but these require further research relative to CMI use cases.) Consequently, the CMI identifier may not be useful for some licensing or right-to-use models.

However, there are multiple scenarios in which one time issuance described above is very restrictive. This is particularly true for host systems (servers, desktops, laptops), software elements, or modular systems. Cryptographic processors and key stores (sometimes implemented as TPMs) may fail and need to be changed. Software based systems may not be bound to hardware and static issuance may rely on white box cryptography (obfuscation of the certificate and key store) which is more vulnerable than hardware based solutions. It may be beneficial to include certification or compliance information in the certificate (so it can be attested). But, since compliance levels may change over time, certificates containing such information should be updated.

Consequently, online certificate issuance solutions may be attractive. One established method of doing this include the Simple Certificate Enrollment Protocol (SCEP). A more recent approach evolving from SCEP is Enrollment of Secure Transport (EST). These types of identity management may provide significant benefit. However, any online certificate issuance solution will significantly increase the complexity of identity management implementation. This complexity will increase the cost of certificate issuance and will certainly increase the attack surface of the CMI trust ecosystem.

Actual specification of the issuance methods are outside the scope of this document. However, the issuance method may impact the certificate lifetime and also the revocation method.

Significant consideration was applied to development of the CMI identifier. Even selecting an element that could be used to identify vendors proved challenging. In 2013, the IEEE began restructuring their Registration Authority as shown in IETF Internet Draft OUI Registry Restructuring (https://tools.ietf.org/html/draft-ieee-rac-oui-restructuring-01). IEEE now issues a primer on their Registry Authority which can be viewed at https://standards.ieee.org/develop/regauth/tut/eui.pdf. Two alternatives were to use the IANA Private Enterprise Number (PEN) or a CMI issued company identifier. Ultimately, the choice was to use the most commonly available identifier already possessed by medical device manufacturers, namely, the IEEE MA-L (MAC Address Block Large) which is previously referred to as an OUI. The IEEE provides an alternative which is also accepted, the IEEE CID (Company Identifier).

5.2 Recommendations

This document is a specification, anticipating that these recommendations will be included in CMI specifications (possibly in an evolved version of this document). Consequently, the recommendations below are presented as requirements using the normal CMI terminology for requirements.

5.3 Trust Considerations

The CMI trust ecosystem will provide a basis for secure interoperability of care environments at the link, network, and data liquidity layers. The basis for this trust will be a PKI based certificate issuance process with a single root that will include unique identifiers and associated public and private key pairs. This will allow cryptography to support authentication, authorization, privacy, confidentiality, and attestation for multiple purposes. A PKI certificate, which includes the identifier and the public key, amongst other information indicated below, is the digital identity that will provide all trust and security actions. Consequently, it is essential that identity, that is the PKI certificate, be issued, asserted, and used in accordance with CMI recommendations and requirements.

Connected Components (devices, gateways, and platforms) SHALL all be issued an identity and to connect to CMI compliant networks. Any other software or hardware element (application) that connects to a device, gateway, or platform SHOULD also have an identifier.

- Clinician (user) and administrator identity is out of scope of these recommendations. However, care systems are highly encouraged to implement strong access control, preferably in accordance with NISTs role based access control (RBAC) or attribute based access control (ABAC) guidelines for authentication and authorization for staff access to CMI components. An application programming interface (API) for secure staff access to devices, gateways, and platforms may need to be specified in the future.

5.3.1 Identifier

The identifier unique identifies the device within the ecosystem. It uniquely identifies the entity that requested the Certificate and the device to which the Certificate is assigned. In its simplest form, this could be just a number. However, it may be useful for other security and management

purposes to have a unique identifier that is attested. For example, an attested unique identifier may be useful for access control policies or inventory management. In some cases, this may even be used as a physical label on the device (though this is not required by CMI).

The identifier SHALL be included in the component certificate as an X.509 field as indicated in the subscriber profiles later reviewed in this document. The identifier SHALL be a single UTF-8 string composed of four elements separated by a colon (":"). These elements will indicate the version of the identifier, the vender identity, the type of component identity, and the component identity as summarized below with each element encoded in UTF-8 format:

[Version]:[VendorID]:[Type]:[ComponentID]

Details on each element are below.

- Version: Included to ensure future proofing of the identifier and SHALL be a three digit decimal number between "001" and "999". Connected Components identified in accordance with this release SHALL use version string "001".

- VendorID: Identifies the organization (typically a vendor or care entity) applying identity to the Connected Component. SHALL be a UTF-8 string corresponding to the 24-bit hex formatted representation of least significant bits of either an IEEE MA-L or a full IEEE CID. The MA-L or CID used SHALL be properly issued by the IEEE to the organization applying the identity to a Connected Component. Information on these registered identities is available at the following IEEE URLs:

    - OUI restructuring -- https://tools.ietf.org/html/draft-ieee-rac-oui-restructuring-01

    - Registry authority -- https://standards.ieee.org/develop/regauth/tut/eui.pdf

    - IEEE MA-L (was OUI) -- https://standards.ieee.org/develop/regauth/oui/index.html

IEEE CID -- https://standards.ieee.org/develop/regauth/cid/index.html

- Type: The identifier may be useful for a wide range of security and management functions. The type field allows functions to determine the type of ComponentID included in the identifier. The Component IDs compliant with this document release are shown below. The appropriate Type SHALL be on of these valid types: "MAC", "SN", "UUID", "HOST", "FQDN", "UDI".

- ComponentID: The component of the identifier that ensures the CMI identifier is globally unique. It SHALL correspond to the Type as discussed above. The organization SHALL assure that all identifiers included in certificate requests are unique within their scope and the CA or sub-CA that issues certificates SHALL assure the identifiers of any certificates they issue are unique.

    - "MAC" - SHALL be the most significant bits of a MAC address which is the remaining portion not used by the MA-L vender identity portion of the IEEE issued MA-L. That

is, the portion that identifies the network component, not the organization asserting the identity. The MAC SHOULD be part of an address block properly issued by the IEEE and owned by the organization asserting the identity.

- "SN"-A serial number according to the needs of the asserting organization. Typically used by equipment manufacturers or software providers. This is probably the most flexible ComponentID type and SHOULD be the default type unless the ComponentID is being used for other security or management purposes as specified by the using medical organization.
- "UUID"-A Universally Unique Identifier provides a 128 bit unique name that can be used as a Uniform Resource Name. It is one way servers and clients that are based on software may be identified. UUIDs SHALL be compliant with IETF RFC 4122.
- "HOST"-Host names are commonly applied to software systems on installation by care facility IT staff. There is no universal approach to creating and asserting host names, but host names used for identifiers SHOULD comply with IETF RFCs 956, 1123, and 1178.
- "FQDN"-Fully Qualified Domain Names are used by DNS to map information resources on servers to IP address. Use of FQDNs SHALL be in compliance with IETF RFC 1035.
- "UDI"-Unique Device Identification issued by an FDA accredited UDI issuing agencies. Accredited issuing agencies at this time are G1, Health Industry Business Communications Council (HIBCC), and the International Council for Commonality in Blood Banking Automation (ICCBBA). (See https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/UniqueDeviceIdentification/ChangesbetweenUDIProposedandFinalRules/default.htm.)

- The elements discussed above SHALL be encoded in the order shown and SHALL be delineated by a UTF-8 colon, ":".
- The device identity is reflected by the device certificate, which SHALL be issued according to [CMI-SP-F-CP]. The certificate SHALL include the identifier (see Section 5.3.3). The certificate SHALL be in compliance with ITU X.509 and IETF RFC 5280.

5.3.2 Certificate PKI Hierarchy

- The CMI PKI is a three tier infrastructure with a CMI Root CA at tier 1 that issues intermediate CA certificates (i.e., sub-CAs) at tier 2. The tier 2 sub-CAs issue compliant end-entity Subscriber certificates at tier 3 (see figure below). Three different CA chains anchored to a CMI Root CA have been identified: Manufacturer, Care Provider, and Code Verification. Additional CA claims may be added in the future. The CMI will make the Root CA and intermediate CA certificates available to Subscribers. (Note: Subscribers in this context is any element that requires a PKI certificate.)

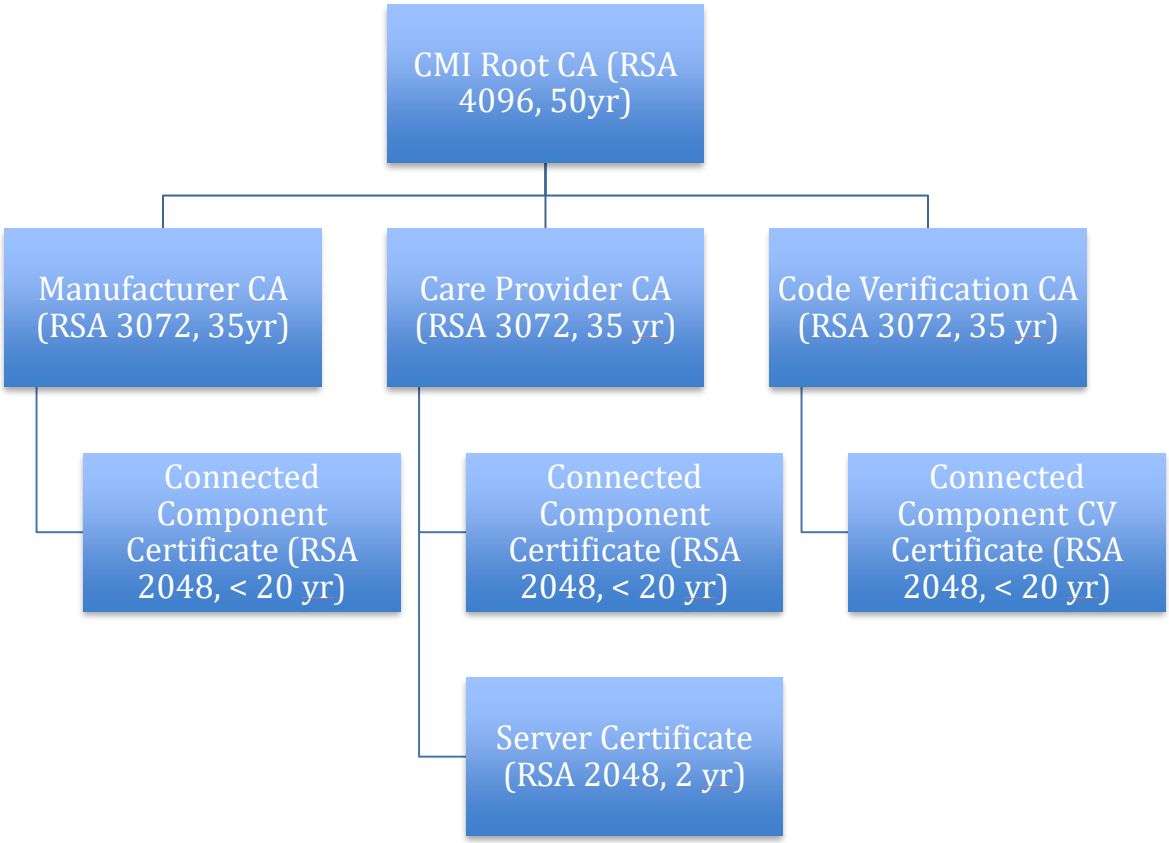

Figure 2: Certificate Hierarchy

The CMI Root CA is the apex of its Root CA Domain. The Root CA will issue the sub-CA certificates to approved CA service providers. The sub-CAs will issue certificates to authorized Subscribers, which will embed the certificates in compliant devices.

Subscribers should install the CMI authorized Root CA certificate in the trust anchor store of their devices to validate received certificates. The end-entity certificate, its private key, and all sub-CA certificates for a given CA chain should also be installed on the device. During the TLS authentication messaging exchange the end-entity and all sub-CA chain certificates should be sent to the other end point.

Software based elements that are issued certificates should use reasonable best practices to protect them. Online issuance, such as Enrollment over Secure Transport (RFC 7030), SHOULD issue certificates with relatively short validity periods, preferably 90 days and certainly not longer than two years. The CMI certificate PKI is managed by CMI. CAs are hosted and secured by an experienced, trusted 3rd party approved by CMI. Sub-CAs are centralized and support end-entity subscriber certificate issuance to different medical device manufacturers and hospitals. Manufacturers and hospitals do not operate their own sub-CA unless given approval by CMI. This helps maintain the trust/assurance level of the CMI PKI.

5.3.3 Certificate Profiles

CMI PKI Certificates SHALL conform to [IETF-RFC5280]: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008.

CMI PKI Certificates SHALL contain the identity and attribute data of a subject using the base certificate with applicable extensions. The base certificate SHALL contain the version number of the certificate, the certificate's identifying serial number, the signature algorithm used to sign the certificate, the issuer's distinguished name, the validity period of the certificate, the subject's distinguished name, information about the subject's public key, and extensions as defined in the following certificate profile tables.

Table 1: RSA Root CA Certificate Profile

Version		**v3**		
Serial number		Unique Positive Integer assigned by the CA and not longer than 20 octets.		
Issuer DN		c=US o=CMI ou=RSA Root CA01 cn=CMI Root CA		
Subject DN		c=US o=CMI ou= Root CA01 cn=CMI Root CA		
Validity Period		50 yrs		
Signature		Sha512WithRSAEncryption (1.2.840.113549.1.1.13)		
Subject Public Key Info algorithm keysize parameters		RSA (1.2.840.113549.1.1.1) 4096-bits NULL		
Extensions	OID	Include	Criticality	Value
keyUsage	{id-ce 15}	X	TRUE	

Version		**v3**		
keyCertSign				Set
cRLSign				Set
basicConstraints	{id-ce 19}	X	TRUE	
cA				Set
pathLenConstraint				Not set
subjectKeyIdentifier	{id-ce 14}	X	FALSE	
keyIdentifier				Calculated per Method 1
subjectAltName	{id-ce 17}	O	FALSE	

Table 2: RSA Sub-CA Certificate Profile

Version	**v3**
Serial number	Unique Positive Integer assigned by the CA and not longer than 20 octets.
Issuer DN	c=US o=CMI ou=RSA Root CA01 cn=CMI RSA Root CA
Subject DN	c=<Country Code> o=<Organization Name> ou=RSA <Sub-CA Type> <ID#> cn=CMI RSA <Sub-CA Type>
Validity Period	30 yrs
Signature	Sha512WithRSAEncryption (1.2.840.113549.1.1.13)
Subject Public Key Info algorithm	RSA (1.2.840.113549.1.1.1)

Version		**v3**		
keysize parameters		3072-bits NULL		
Extensions	OID	Include	Criticality	Value
keyUsage	{id-ce 15}	X	TRUE	
keyCertSign				Set
cRLSign				Set
basicConstraints	{id-ce 19}	X	TRUE	
cA				Set
pathLenConstraint				0 (zero)
subjectKeyIdentifier	{id-ce 14}	X	FALSE	
keyIdentifier				Calculated per Method 1
authorityKeyIdentifier	{id-ce 35}	X	FALSE	
keyIdentifier				Calculated per Method 1
subjectAltName	{id-ce 17}	O	FALSE	
certificatePolicies	{id-ce 32}	X	FALSE	
certPolicyId				<Certificate Policy OID, TBD>
policyQualifiers				Not set
authorityInfoAccess	{id-pe 1}	X	FALSE	
AccessDescription				
accessMethod				OCSP
accessLocation				Responder HTTP URI

<Sub-CA Type> is one of the following values not including the quotes: “Medical Device”, “Enterprise Device”, “Member”, “Code Verification Certificate”.

<ID#> indicates the ID number of the CA and is populated when the CA certificate is issued. For Example, “CA0001.”

Table 3: RSA Subscriber Certificate Profile

Version		**v3**		
Serial number		Unique Positive Integer assigned by the CA and not longer than 20 octets.		
Issuer DN		c=<Country Code> o=<Organization Name> ou=RSA <Sub-CA Type> <ID#> cn=CMI RSA <Sub-CA Type>		
Subject DN		c=<Country Code> o=<Organization Name> ou=CMI <Device Type> Certificate cn=<Device Identifier>		
Validity Period		20 yrs		
Signature		Sha384WithRSAEncryption (1.2.840.113549.1.1.12) *or*,		
Subject Public Key Info algorithm keysize parameters		 RSA (1.2.840.113549.1.1.1) 2048-bits NULL		
Extensions	**OID**	**Include**	**Criticality**	**Value**
keyUsage	{id-ce 15}	X	TRUE	
digitalSignature				Set
keyEncipherment				Set
subjectKeyIdentifier	{id-ce 14}	X	FALSE	

Version		**v3**		
keyIdentifier				Calculated per Method 1
authorityKeyIdentifier	{id-ce 35}	X	FALSE	
keyIdentifier				Calculated per Method 1
subjectAltName	{id-ce 17}	O	FALSE	
certificatePolicies	{id-ce 32}	X	FALSE	
certPolicyId				<Certificate Policy OID, TBD>
policyQualifiers				Not set
extKeyUsage	{id-ce 37}	O	FALSE	
__KeyPurposeId				TLS client auth for medical device and gateways and TLS server auth for platform application and other servers
cRLDistributionPoint		O	FALSE	
authorityInfoAccess	{id-pe 1}	X	FALSE	
AccessDescription				
accessMethod				OCSP
accessLocation				Responder HTTP URI

<Sub-CA Type> is one of the following values not including the quotes: “Medical Device”, “Enterprise Device”, “Member”, “Code Verification Certificate”.

<ID#> indicates the ID number of the CA and is populated when the CA certificate is issued. For Example, “CA0001.”

<Device Type> is one of the following values not including the quotes: “Medical Device”, “Enterprise Device”, “Platform”, “Code Verification Certificate”.

<Device Identifier> is a globally unique identifier that is persistent as documented in Section 5.3.1.

<extKeyUsage> is optional but if the certificate supports a TLS/SSL client, client auth and server auth should be indicated as appropriate to the use of the certificate.

Table 4: ECC Root CA Certificate Profile

Version		**v3**		
Serial number		Unique Positive Integer assigned by the CA and not longer than 20 octets.		
Issuer DN		c=US o=CMI ou=ECC Root CA01 cn=CMI ECC Root CA		
Subject DN		c=US o=CMI ou=ECC Root CA01 cn=CMI ECC Root CA		
Validity Period		50 yrs		
Signature		ecdsa-with-Sha512 (1.2.840.10045.4.3.4)		
Subject Public Key Info algorithm parameters		 EC (1.2.840.10045.2.1) Secp521r1 (1.2.840.10045.3.1.35)		
Extensions	**OID**	**Include**	**Criticality**	**Value**
keyUsage	{id-ce 15}	X	TRUE	
keyCertSign				Set
cRLSign				Set
basicConstraints	{id-ce 19}	X	TRUE	
cA				Set
pathLenConstraint				Not set
subjectKeyIdentifier	{id-ce 14}	X	FALSE	
keyIdentifier				Calculated per Method 1

Version		**v3**		
subjectAltName	{id-ce 17}	O	FALSE	

Table 5: ECC Sub-CA Certificate Profile

Version		**v3**		
Serial number		Unique Positive Integer assigned by the CA and not longer than 20 octets.		
Issuer DN		c=US o=CMI ou=ECC Root CA01 cn=CMI ECC Root CA		
Subject DN		c=<Country Code> o=<Organization Name> ou=ECC <Sub-CA Type> <ID#> cn=CMI ECC <Sub-CA Type>		
Validity Period		30 yrs		
Signature		ecdsa-with-Sha512 (1.2.840.10045.4.3.4)		
Subject Public Key Info algorithm parameters		 EC (1.2.840.10045.2.1) Secp384r1 (1.2.840.10045.3.1.34)		
Extensions	**OID**	**Include**	**Criticality**	**Value**
keyUsage	{id-ce 15}	X	TRUE	
keyCertSign				Set
cRLSign				Set
basicConstraints	{id-ce 19}	X	TRUE	
cA				Set

Version		**v3**		
pathLenConstraint				0 (zero)
subjectKeyIdentifier	{id-ce 14}	X	FALSE	
keyIdentifier				Calculated per Method 1
authorityKeyIdentifier	{id-ce 35}	X	FALSE	
keyIdentifier				Calculated per Method 1
subjectAltName	{id-ce 17}	O	FALSE	
certificatePolicies	{id-ce 32}	X	FALSE	
certPolicyId				<Certificate Policy OID, TBD>
policyQualifiers				Not set
authorityInfoAccess	{id-pe 1}	X	FALSE	
AccessDescription				
accessMethod				OCSP
accessLocation				Responder HTTP URI

<Sub-CA Type> is one of the following values not including the quotes: “Medical Device”, “Enterprise Device”, “Member”, “Code Verification Certificate”.

<ID#> indicates the ID number of the CA and is populated when the CA certificate is issued. For Example, “CA0001.”

Table 6: ECC Subscriber Certificate Profile

Version	**v3**
Serial number	Unique Positive Integer assigned by the CA and not longer than 20 octets.
Issuer DN	c=<Country Code> o=<Organization Name>

Version		**v3**		
		ou=ECC <Sub-CA Type> <ID#> cn=CMI ECC <Sub-CA Type>		
Subject DN		c=<Country Code> o=<Organization Name> ou=CMI <Device Type> Certificate cn=<Device Identifier>		
Validity Period		20 yrs		
Signature		ecdsa-with-Sha384 (1.2.840.10045.4.3.3)		
Subject Public Key Info algorithm parameters		 EC (1.2.840.10045.2.1) Secp256r1 (1.2.840.10045.3.1.7)		
Extensions	**OID**	**Include**	**Criticality**	**Value**
keyUsage	{id-ce 15}	X	TRUE	
digitalSignature				Set
keyAgreement				Set
subjectKeyIdentifier	{id-ce 14}	X	FALSE	
keyIdentifier				Calculated per Method 1
authorityKeyIdentifier	{id-ce 35}	X	FALSE	
keyIdentifier				Calculated per Method 1
subjectAltName	{id-ce 17}	O	FALSE	
certificatePolicies	{id-ce 32}	X	FALSE	
certPolicyId				<Certificate Policy OID, TBD>
policyQualifiers				Not set
extKeyUsage	{id-ce 37}	O	FALSE	

Version		**v3**		
_KeyPurposeId				TLS clientauth for medical device and gateways and TLS serverauth for platform application and other servers
cRLDistributionPoint		O	FALSE	
authorityInfoAccess	{id-pe 1}	X	FALSE	
AccessDescription				
accessMethod				OCSP
accessLocation				Responder HTTP URI

<Sub-CA Type> is one of the following values not including the quotes: “Medical Device”, “Enterprise Device”, “Member”, “Code Verification Certificate”.

<ID#> indicates the ID number of the CA and is populated when the CA certificate is issued. For Example, “CA0001.”

<Device Type> is one of the following values not including the quotes: “Medical Device”, “Enterprise Device”, “Platform”, “Code Verification Certificate”.

<Device Identifier> is a globally unique identifier that is persistent as documented in Section 5.3.1.

<extKeyUsage> is optional but if the certificate supports a TLS/SSL client, client auth and server auth should be indicated as appropriate to the use of the certificate.

5.3.4 Installation and Protection of Secrets and Certificates

- To ensure the integrity of the trust architecture, secrets and certificates SHALL be protected. The intent of protecting these cryptographic elements is to deter cloning or counterfeiting devices, tampering with devices to change their authorized functions or use, and to acquire credentials for the purpose of introducing unauthorized devices into trusted networks. Furthermore, it is important to protect any keys used to encrypt sensitive data whether at rest or in motion. Consequently, the Connected Component SHALL store the Connected Component Certificate private key in a manner that deters (makes difficult) unauthorized disclosure and modification.

- Installation and protection of secrets (keys) and certificates will depend on the nature of the component and the type of environment in which the Connected Component will operate. The current health industry state of the art does not specify, however, how keys and other

secrets will be protected. Below are guidelines based on [FIPS-140-2] that are desired and may become mandatory in the future.

- 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 securely installed in the Connected Component by the manufacturer.
    - An ECC or RSA root CA 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.
- 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 (tamper detection and key zeroization) or higher if it will operate in an untrusted environment where the public may have access. The Connected Component SHALL meet [FIPS-140-2] level 1 if it does not meet requirements of [FIPS-140-2] level 3.
    - 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 in the Connected Component by the manufacturer.
    - An ECC or RSA root CA 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.
- 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 specified in NIAP Protection Profile for Application Software (NIAP). In particular, storage of credentials SHOULD comply with FCS-STO-EXT.1.

- The Connected Component SHOULD use secure hardware such as a Trusted Platform Module.
- The Connected Component SHOULD apply access controls to protect certificates, private keys, and issuing CA certificates.
- A mitigating control, such as Intrusion Detection Systems, SHOULD be used to detect unauthorized access to certificates, private keys, and issuing CA certificates installed on the network component. Both external and internal mitigating controls SHOULD be used.
- An ECC or RSA Connected Component certificate, private key, and issuing CA certificate SHALL be securely installed in the Connected Component 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.

- It must be noted that while the use of white box cryptography is better than not addressing cryptographic security at all, existing solutions are known to be vulnerable to a wide variety of attacks. Consequently, it is highly recommended that hardware based security mechanisms be used. It is possible that on-line certificate issuance such as described by Enrollment over Secure Transport (IETF RFC 7030) may mitigate some vulnerabilities of software based Connected Components and may provide a more scalable, extensible trust ecosystem. Similarly, use of Hardware Security Module servers may provide benefits. These areas will be further studied by the Center.
- The [FIPS-140-2] guidelines are based on protection profiles derived from the Common Criteria for Information Technology Security Evaluation. Excellent insight on secure implementation of cryptographic modules and their use can be found in the following National Information Assurance Partnership (NIAP) documents:
- NIAP Protection Profile for Application Software
- NIAP Protection Profile for General Purpose Operating Systems
- NIAP General Purpose Operating Systems Protection Profile / Mobile Device Fundamentals Protection Profile Extended Package (EP) Wireless Local Area Network (WLAN) Clients

Appendix I. 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 a variety of discussions, reviews and input: **Stuart Hoggan, Jeffrey Brown** and **Dr. Max Pala**.

This effort was conducted within The Center's **Security** Working Group, whose members have included the following part-time and full-time participants during the time period that we discussed this version of the document:

WG Participant	**Company Affiliation**
Andrew Dobbing	Laird
Bill Hagestad	Smiths Medical
Bill Pelletier	GE
Bo Dagnall	HPE
Bruce Friedman	GE
Doug Smith	Laird
Jay White	Laird
Jeffrey Brown	GE
Kai Hassing	Philips
Ken Fuchs	Draeger
Dr. Max Pala	CableLabs
Song Chung	Welch Allyn
Soundharya Nagasubramanian	Welch Allyn
Stefan Karl	Philips
Stuart Hoggan	CableLabs

- *Steve Goeringer (Security Working Group Lead), David Fann, Trevor Pavey, Sumanth Channabasappa; and, Ed Miller (CTO) -- The Center*