eHealth Ontario
It's working for you

eHealth Ontario PKI Certification Policy Manual

Part One: Concept of Operations

Part Two: Certification Policies

Version: 1.5

Document ID: 4274

Document Owner: Cyber Security Operations

Ontario
eHealth Ontario

Document Control

The electronic version of this document is recognized as the only valid version.

Approval History

APPROVER(S)	TITLE/DEPARTMENT	APPROVED DATE
Mark Carter	Manager, Cyber Security Governance	2016-12-02
Aniko Simon	(Acting) Director of Cyber Security	2016-12-02
Adina Saposnik	VP of Cyber Security	2016-12-21

Revision History

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
1.0	2004 June 30	Initial Draft	N/A
1.1	2005 January 25	Updates by Legal	N/A
1.2	TBD	Partial update	N/A
1.3	2016 November 23	Updated to reflect changes to external hosting of CA	Steve Brierley
1.4	2016 December 2	Final Review	Aniko Simon / Mark Carter
1.5	2016 December 14	Legal Review	R. Pearse/A. Simon/S. Brierley

Document ID

4274

Document Sensitivity Level

Low

Table of Contents

Table of Figures

1. Introduction

This document contains the eHealth Ontario policies related to registering and enrolling Registrants, and issuing Authentication Credentials, which include use of the Public Key Infrastructure (or PKI) provided by eHealth Ontario to its Clients pursuant to the PKI Services Schedule. This document is the Certification Policy Manual referred to in the PKI Services Schedule. It has two parts:

- **Part One – Concept of Operations** provides an overview of basic concepts and processes that eHealth Ontario has adopted for implementing the PKI Service and registering, enrolling and authenticating individuals for these services.

- **Part Two – Certification Policies**
  Part Two states the policies that have been approved by the Policy Authority (PA) and recommended to the eHealth Ontario VP of Cyber Security (VPCS) for both the PKI and non-PKI Registrations and enrolments.

2. Terminology

DEFINITIONS

Unless the context otherwise requires, words importing the singular include the plural and words importing gender include all genders. Capitalized words have the meanings set out in the eHealth Ontario Services Agreement and the PKI Services Schedule, as applicable, unless otherwise defined below:

"Accreditation" – a procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks.

"Activation Data" – private data, other than PKI Keys, that are required to operate systems or cryptographic modules that need to be protected (e.g. PIN, passwords).

Aggregate Liability Amount" – the total amount of damages for which a Client would be liable in respect of each Certificate.

"Authentication" – any process designed to verify the identity of an individual or any other entity, or to establish the validity of a transmission, message or originator.

"Authentication Credential" – a credential, including a User ID, password, token, PKI Certificate, or any combination of these, that is issued to an End User to allow the authentication of the End User's identity to a system or application.

"Certificate Policy" or **"CP"** – a set of rules that indicate the applicability of Keys and Certificates to a particular community, or class of applications, with common security requirements.

“Certificate Practice Statement” or **“CPS”** – a confidential internal document that is a comprehensive description of how all of the policy requirements stated in the CP will be implemented and maintained by eHealth Ontario including the practices that the CA employs in issuing and revoking Certificates.

“Certificate Revocation List” or **“CRL”** – a list of revoked Certificates that is created, time stamped and signed by the same CA that issued the Certificates. A Certificate is added to the list if it is revoked (e.g., because of suspected Key compromise, distinguished name (DN) change) and then removed from it when it reaches the end of the Certificate’s validity period. In some circumstances the CA may choose to split a CRL into a series of smaller CRLs

“Confidentiality Key Pair” – a pair of asymmetric cryptographic keys composed of a public encryption key and a corresponding private decryption key. In PKI, confidentiality is achieved using the **Confidentiality Key Pair**.

“Digital Signature Key Pair” – a pair of asymmetric keys composed of a private signing key and a corresponding public verification key and used to authenticate the identity of the sender of a message and/or to ensure that the original content of a message or document is unchanged.

“Directory” – a directory system that conforms to the ITU-T X.500 series of recommendations.

“Distinguished Name” – a name appearing in a Certificate that uniquely identifies the Public Key owner. A distinguished name is composed of at least the following components common name, organization, country, serial number.

“Enrolment” – the process of enrolling a Registrant as being authorized to access the PKI Service. Enrolment assumes that Registration has established identity to a specified Level of Assurance and that the due diligence required for Enrolment can be satisfied by the due diligence applied to Registration.

"Individually Accountable" – evidence that uniquely and unambiguously attributes an action to the individual or entity performing the action.

“Integrity” – the condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed during transfer, storage and retrieval. In a security service (including PKI) that prevents unauthorized modifications of data or transactions to occur. In PKI, integrity is established and verified using a Digital Signature Key Pair.

“Level of Assurance” – the degree of confidence in the processes leading up to and including an authentication, providing assurance that the entity claiming a particular identity, is the entity to which that identity was assigned.

“Non-repudiation” – the ability to ensure that a party to a communication cannot deny the authenticity of their sending of a message that they originated.

“Object Identifier” or **“OID”** – the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class, used for PKI to uniquely identify the policies and cryptographic algorithms supported.

“Policy Authority” or **“PA”**– the eHealth Ontario authority that has the responsibility and accountability for setting policies related to the Registration, Enrolment and Authentication infrastructure, approving service implementation plans.

"Primary Point of Contact" or **"PPC"** – the Policy Authority (PA) designates a Primary Point of Contact (PPC) who will be responsible for performing key functions regarding the overall operation of the PKI for eHealth Ontario. These functions include:

- Submitting change requests for any modifications to the baseline Certificate contents to eHealth Ontario's service provider (a.k.a. Entrust); and
- Submitting change requests for any modifications to the security policies enforced through the PKI to eHealth Ontario's service provider.

The PPC is a member of the PA group and must accept these responsibilities in writing.

"Public Key Infrastructure" or **"PKI"** – a system of policies, processes and technologies that allow Registrants to use Public/Private Key Pairs in order to:

- Authenticate the identity of Registrants;
- Securely and privately exchange information over the Internet or other networks (e.g. virtual private networks); and
- Digitally sign messages and transactions.

These Public/Private Key Pairs are encrypted and are issued by the CA.

"Public/Private Key Pair" – two mathematically related keys, having the properties that:

- One key can be used to encrypt a message that can only be decrypted using the other key
- Even knowing one key, it is computationally infeasible to discover the other key.

"Registration" – the process by which a unique identity is established for any Registrant with an associated defined Level of Assurance. This process is generally the responsibility of an LRA, but may also be performed by a Registration Authority or the CA.

"Registration Authority" or **"RA"** – an individual that is delegated responsibility by the CA for the performance of tasks associated with identifying and authenticating LRAs. The role of RA is assumed by eHealth Ontario personnel in its Security Operations Team and the ONE ID Connector application.

"Registration Management System" – the system maintained by the CA to record the unique identity of Registrants.

"Repository" – the single repository operated by eHealth Ontario for listing all Registrants and Clients that receive PKI Services. All Certificates issued by all CAs, and all CRLs relating thereto, will be published in the Repository.

"Root Certificate Authority" – the Root Certificate is a certificate issued by a trusted authority under digital signature and the CA is the Root Certificate Authority for the PKI Service.

"Service Owner" - means an individual or organisation that provides one or more Sponsored Services. A Service Owner may be eHealth Ontario or a third party that owns or operates a Sponsored Service.

"Sponsor" – a designated individual of a Client who is appointed and responsible, within the management organization of a Sponsorship Organization, to perform duties assigned by the CA.

ACRONYMS

The following acronyms used in this document have the associated meaning set out below:

FIPS	Federal Information Processing Standard
HTTP	Hypertext Transfer Protocol
ITU	International Telecommunications Union
PKIX	Public Key Infrastructure X.509
RSA	Rivest-Shimar-Adleman
URL	Uniform Resource Locator

EXTENDED INFORMATION FOR SOME DEFINITIONS

The Certificate uses an electronic file in a format that is in accordance with ITU-T Recommendation X.509 and contains the public key of a Registrant, together with related information, digitally signed with the Private Key of the Certificate Authority that issued it, and that includes the ID for the Certificate Policy in the *Certificate Policy* field. A Certificate:

- Names or otherwise identifies its Registrant.
- Contains a Public Key that corresponds to a Private Key under the control of the Registrant.
- Identifies its operational period.
- Contains a Certificate serial number and is digitally signed by the CA issuing it.

The 3 types of Certificate used are: Root CA, Issuing and Registrant, as further described in Part II, Section 1.1.3.

The CA performs two essential functions:

- It is responsible for identifying and authenticating the Registrant named in a Certificate, and verifying that the Registrant possesses the Private Key that corresponds to the Public Key that will be listed in the Certificate.
- It creates and digitally signs the Registrant's Certificate. The Certificate issued by the CA then represents that CA's statement as to the identity of the Registrant named in the Certificate and the binding of that Registrant to a particular Public-Private Key Pair.

A CA can perform the functions of a registration authority (RA) and can delegate or outsource this function to separate entities. For the purposes of this document, CA refers to the eHealth Ontario operated CA hosted and managed by Entrust (and not the Entrust root CA).

A Local Registration Authority (**LRA**) is responsible for Registration and Enrolment processes within the organizational domain(s) for which they have been delegated permission. An LRA requests, but does not issue or sign Authentication Credentials. This role is assumed by the eHealth Ontario ONE ID Business Delivery Team.

Trusted Agents (**TA**s) are engaged by the eHealth Ontario RAs or LRAs to perform certain, limited registration activities. If used, the TAs shall satisfy all of the requirements of an LRA, but shall be restricted to performing identity proofing as a proxy for the RAs or LRAs. This role is assumed by the eHealth Ontario external business partners.

Part One – Concept of Operations

1. Policy Foundations

eHealth Ontario is a Crown agency established pursuant to Ontario Regulation 43/02 under the *Development Corporations Act*. Under this Regulation, eHealth Ontario is authorized to:

- Provide information management services, or technology services, or both, in connection with the facilitation or operation of any of the systems or infrastructure initiatives specified in the Regulation, or others with the prior approval of the Lieutenant Governor in Council.

- Collect directly or, with the consent of the person to whom it relates, indirectly collect personal information and use or disclose it, in order to verify the identity of persons registering to use Services provided by eHealth Ontario's information infrastructure.

To meet this mandate, eHealth Ontario has implemented policies and processes covering:

- Levels of Assurance
- Registration and Enrolment.
- Authentication.
- Client Roles and Responsibilities.
- Agreements to provide Services to its Clients.

These policies and processes are described in the following sections.

2. Levels of Assurance

eHealth Ontario provides Registration and Authentication Services, including the use of Certificates, to Clients that have executed a PKI Services Schedule, at three Levels of Assurance, each corresponding to the degree of effort taken to prevent damage that would result from the improper, unauthorized or fraudulent use of either identities or Authentication Credentials. The Levels of Assurance supported are: Basic, Medium, and High. PKI Certificates are issued by eHealth Ontario only when a Medium of High Level of Assurance has been established for a Registrant.

- **Basic Assurance** is appropriate for information that has a low sensitivity level, within eHealth Ontario and the health sector environment, and that is generally available to the eHealth Ontario employees and Registrants. If compromised, this information could reasonably be expected to cause only minor injury or losses to the parties involved and require only administrative action for correction.

- **Medium Assurance** is appropriate for information that has a medium sensitivity level, within eHealth Ontario and health sector environment, and that is intended for use by specific employees and Registrants. If compromised, this information could reasonably be expected to cause serious injury or financial losses to one of the parties involved or require legal action for correction.

- **High Assurance** is appropriate for information that has a high sensitivity level, within eHealth Ontario and the health sector environment, and that is extremely sensitive and of the highest value. This information is intended for use by named and authorized individuals only. If compromised, this information could reasonably be expected to cause extremely grave injury, the loss of life, or major financial losses to one of the parties involved, or require legal action for correction or result in imprisonment.

As of the date that this Certification Policy Manual has been approved by eHealth Ontario, Clients receive Certificates with Medium Level of Assurance.

The Registration requirements for meeting these levels of assurance are identified in the following section.

3. Registration and Enrolment

There is a distinct difference between Registration and Enrolment. Registration is the process of validating the real-world identity of a Registrant to a defined Level of Assurance before Enrolment. Enrolment is the process of signing up Registrants for access to a specific Service, such as email, portal, etc.

Registration will happen only once for most Registrants if their Registration Level of Assurance never changes. Once a Registrant is registered, the information for Registration will be captured and stored for future use. Although initial Registration is normally linked to an Enrolment and an organizational context (e.g. membership in a sponsored group, employment by a Sponsorship Organization, etc.), an individual Registration is not limited to just one service or organization. It may be valid and used for enrolment in multiple Services and Sponsorship Organizations.

Enrolment may happen many times as Registrants are signed up for different Services or product offerings. An Enrolment, unlike Registration, is linked to an organizational context. This means that a Registrant may be enrolled into the same service multiple times based on the sponsorship by their organization for access to this service.

eHealth Ontario uses a distributed multi-organization service model for the delivery of Registration and Enrolment. This involves: the CA accrediting eHealth Ontario individuals to act as Registration Authorities (each an "**RA**") and RAs accrediting a Client's local registration authorities (each an "**LRA**") to perform various Registration and Enrolment functions. This model allows the Registration and Enrolment functions to be performed by LRAs who are closer to, and have a pre-existing knowledge and relationship with, a Client's Registrants.

The high level overview of this service model and registration and enrolment processes has four basic elements:

- Sponsorship
- Registration and Enrolment
- Self-Management
- Use of Services

Descriptions for each element follow.

Sponsorship

Sponsorship is the process of certifying the eligibility and providing identifying information for Registrants (Individual tor Computer Application) to be registered and enrolled. eHealth Ontario requires that every Registrant be sponsored, and this is done by an organization that has been registered as a Sponsorship Organization. Designated persons within a Sponsorship Organization act as Sponsors and their primary functions are:

- To validate that specific Representatives or Computer Applications of a Client are eligible for Registration and are Enrolled in accordance with applicable policies and procedures.
- In some instances, provide the information required for Registration or Enrolment to an RA or LRA, as applicable, with the consent of Registrants.
- To identify the Client's requirements for LRAs and to suggest to the CA or RA, as applicable, the individuals who have the ability to perform these duties.
- To ensure that LRAs and Registrants from their organizational domain are aware of, and comply with, policies governing Registration, Enrolment and access to the information infrastructure and the Services provided through it.

A variety of organizations may act as Sponsorship Organizations. In some cases, a Client may also act directly as a Sponsorship Organization or it may designate another organization to act on its behalf. For example, a regulated health profession's college or professional organization may sponsor its members into the products and services for which they have been given the authority to act as a Sponsor.

Sponsorship may be performed outside of the normal Registration and Enrolment processes. For example, a Sponsorship Organization may bulk load information about Registrants into the Registration Database through a project or notify an RA/LRA either manually or electronically about the Registrant's sponsorship and provide details about the Registrant.

It should be noted that sponsorship is not the same as Registration and Enrolment. Sponsorship is the process of nominating a Registrant. Registration is the process of validating the real-world identity of a Registrant before they are registered into the infrastructure. Enrolment is the process of granting a Registrant access privileges as an End User of specific Services, such as e-mail or other service, within the organizational domain for which he/she is being sponsored.

Registration

Registration provides the basis on which trust in the unique identity of End Users is established to a defined Level of Assurance by verifying that Registrant exists, has a name and is entitled to use that name. This trust is essential to meeting eHealth Ontario's obligations with respect to maintaining the confidentiality and security of health-related information. Through a series of processes and checkpoints, an individual's or Computer Application's identity will be verified. In order for this model to work three basic questions that must be answered for each potential registrant:

1. Who or what are you?
2. Can your identity be proven?
3. Are you entitled to be a Registrant?

This is known as the Level of Assurance, and ensures that identity is confirmed and not just taken for granted.

For most Registrants, Registration happens only once. Once a Registrant is registered their Registration information will be captured and stored for future use. Registration is not based on an organizational context and can remain valid irrespective of whether an individual works with multiple organizations.

Registration Requirements for Levels of Assurance

eHealth Ontario uses registration processes to establish identity at three Levels of Assurance. The major difference between these levels is that the confidence regarding the identity of a Registrant is increased with each higher Level of Assurance.

1. **Basic**
   a. The Registrant must be sponsored by a Sponsorship Organization registered with eHealth Ontario.
   b. The Registrant must be involved in the process.
   c. If the Registrant is an individual, they must provide TWO pieces of identification, one of which must be photo-identity issued by a government in Canada. The second document may be issued by a type of institution approved by the PA. For individual, both documents must show the same first and last name.
   d. If the Registrant is an individual, they must provide the LRA with originals or photocopies of their identity documents.
   e. These documents must be reviewed by the LRA.

2. **Medium**
   a. The Registrant must be sponsored by a Sponsorship Organization registered with eHealth Ontario.
   b. The Registrant must be involved in the process.
   c. There must be a face to face interview directly with the LRA or attested to by the Sponsor for the presentation of supporting identity documentation.
   d. If the Registrant is an individual, they must provide two pieces of identification, both of which must be issued by a government in Canada and provide the Registrant's legal name (first and last). One of these government issued documents must contain a photograph.
   e. If the Registrant is an individual, they must provide to the LRA originals or notarized copies of the identity documents
   f. These documents must be reviewed by the LRA.

3. **High**
   a. The Registrant must be sponsored by a Sponsorship Organization registered with eHealth Ontario.

b. The Registrant must be involved in the process

c. If the Registrant is an individual, a face to face interview must be performed where the Registrant presents their supporting identity documents to the LRA.

d. If the Registrant is an individual, they must provide two pieces of identification both of which must be issued by a government in Canada and provide the Registrant’s legal name (first and last). One of these government issued documents must contain a photograph.

e. If the Registrant is an individual, they must provide to the RA originals or notarized copies of their identity documents.

f. These documents must be reviewed and visually verified by the RA as to their authenticity.

The following table summarizes these Registration requirements.

Figure 1: Summary of Levels of Assurance

Identity Assurance Level	Sponsor ship Required	Registrant involved in process	Face to face required	Identity Documents	Identity Document Verification		
					Reviewed	Recorded	Verified
Basic	Yes	Yes	No	2 pieces of identification (photocopied or originals), one of which is government issued with a photo.	Yes	No	No
Medium	Yes	Yes	No	2 pieces of identification (notarized copy or originals), both of which are government issued, one containing a photo	Yes	Yes	No

High	Yes	Yes	Yes	2 pieces of identification (originals only), both of which are government issued, one containing a photo.	Yes	Yes	Yes

Enrolment

Enrolment is the process by which a Registrant obtains authorization for a specific service or product. An Enrolment, unlike Registration, is linked to an organizational context. This means that a Registrant may be enrolled into the same service multiple times based on the sponsorship by their organization for access to this service. Enrolment may occur at the same time as Registration, for a first time Registrant, or subsequently for existing Registrants. It may also require the collection, use and disclosure of additional information relevant to the service or product in question.

Sponsorship, Registration and Enrolment are linked processes. Sponsorship allows the organization to decide who will be eligible to have access to the Services within their organizational context, and to revoke access privileges when a Registrant's relationship with the organization changes (e.g. if the Registrant no longer needs a Service because of a change in responsibilities or if the Registrant leaves and is no longer associated with the organization). Registration cannot happen without a Registrant being sponsored by a Sponsorship Organization. It allows the RA or LRA to establish the Level of Assurance for the real-world identity of a Registrant, before enrolling them into the Services, by reference to the evidence required at Registration or documented in an existing Registration record. Enrolment cannot occur before a Registration record has been created, and is founded on the unique and trusted identity established through the Registration process. The following diagram illustrates the links between Registration and Enrolment.

The Level of Assurance required for a Registrant to access a specific service depends on the Level of Assurance that is configured for that service. This means that a Registrant must have a medium or high level of assurance before they can be enrolled into a service or product which requires a medium Level of Assurance. If the requisite Level of Assurance is documented in an existing Registrant record, the enrolment may proceed on that basis. If not, the Level of Assurance for a Registrant will first have to be upgraded by an LRA to the Level of Assurance required for enrolment in a particular Service.

Provided the Registrant's Level of Assurance is sufficient, the Enrolment process then uses the identification information to create its own Enrolment record for the specific Service involved. Part of this record may be an Enrolment number. A new Enrolment number may be created, or one that already exists within the Sponsorship Organization may be used (e.g. employee number), and for privacy purposes, should not be the same as the Registrant number. The Enrolment record may also capture the identification information that it requires from the Registrant record (e.g. name, sex, date of birth). It will also include information specific to the enrolment such as organizational affiliation or additional eligibility information (e.g. professional qualifications if required for the service).

As an outcome of the enrolment process, the Authentication Credentials needed to access the Service involved are issued to the Registrant.

Self-Management

Once Registration and Enrolment are complete, Registrants are provided with information (for example, User IDs and initialized passwords) that will allow self-management using electronic channels. The types of self-management activities involved may include:

- Setting passwords by changing the initialized password, and subsequent password changes required by eHealth Ontario access policies.
- Confirming the Registration information provided by the Sponsorship Organization, usually in the case of bulk registrations.
- Providing “shared secrets” that may be used to confirm identity when a password is not available (e.g. forgotten passwords).
- Accepting terms and conditions and Privacy Policy for Registration and Enrolment.
- Providing or updating service-specific, optional or additional information (e.g. contact information such as phone number or address).

Use of Service

The final outcome of Registration and Enrolment is the issuance of Authentication Credentials that allow Registrants to use the services for which they have been enrolled. To facilitate secure access control to these systems, it is necessary to authenticate End Users to the systems that they are accessing. This is usually done electronically through User IDs and password, although other security devices may supplement these to provide stronger Authentication. In the case of eHealth Ontario, Registrants may be issued, and need to use, different Authentication Credentials depending on the number of different Services that they have enrolled for and the organizational context of the enrolments involved.

4. Authentication Using Public Key Infrastructure

The outcome of Registration and Enrolment is an eHealth Ontario Authentication Credential. A Registrant could have more than one eHealth Ontario Authentication Credential issued to them as each Service may have different requirements for Authentication. For example, one Service may require a User ID and password but another Service may require a PKI certificate. These Authentication Credentials are also linked to an organizational context. This means that a Registrant may have different User IDs and passwords for access to the same Service under different organizations. In other words, if a Registrant works for two organizations (A and B), and has access to email in both organizations, which requires a PKI credential, the registrant will have two Certificates, one which is used to access the email at organization A and the other is used to access the email at organization B. While the goal is to use the same Authentication Credentials to allow for single sign on, this functionality does not currently exist without additional software/hardware being implemented by the Service Owner.

PKI presents distinct advantages as a system of hardware, software, rules and practices that help permit the secure exchange of sensitive information and the conduct of business transactions over public and private networks, including the internet. These advantages are derived from the use of:

- PKI Certificates that bind an electronic identity to a real world identity that has been verified to defined Levels of Assurance.
- Digital Signature Key Pairs that permit the authentication and non-repudiation of messages or transactions sent by an End User.
- Confidentiality Key Pairs that allow the transmission of information over networks using highly secure encryption and decryption algorithms.

In the healthcare environment, the use of PKI allows the senders and recipients of information to be sure of the source of the document or information (Authentication), that it has not been changed since it was created (Integrity), and that its confidentiality has been protected during the transmission. It does this through the use of Digital Signature and Confidentiality Key Pairs as described below.

- Objective: Sender wants to send a digitally signed e-mail so the recipient trusts it came from the sender
- The Role of Digital Signature Key Pairs:
- The sender uses his/her Private Key to digitally sign the contents of the e-mail
- The e-mail is sent to the recipient as normal but also includes the sender's Public Key to allow for verification of the signature
- The recipient uses the sender's Public Key to verify the integrity of the sender's e-mail message
- The PKI provides the assurance to the recipient that the Private Key used to sign the e-mail belongs to the sender
- Objective: Sender wants to send an e-mail encrypted only for the recipient
- The Role of Confidentiality Key Pairs:
- The sender must retrieve the recipient's Public Key from the PKI directory.
- The sender's e-mail security software uses the recipient's Public Key to encrypt the message.
- The e-mail is sent to the recipient as normal.
- The recipient uses his/her Private Key to decrypt the e-mail message.

Using PKI allows organizations to improve their business processes and extend secure electronic service delivery to their business partners and to the communities that they serve.

In the healthcare environment, the use of PKI allows the senders and recipients of information to be sure of the source of the document or information, that it has not been changed since it was created, and that its confidentiality has been protected during the transmission. Using PKI allows organizations to improve their business processes and extend secure electronic service delivery to their business partners and to the communities that they serve.

5. Governance

The primary governing bodies of eHealth Ontario with respect to Registration, Enrolment and Authentication are the Vice President of Cyber Security (VPCS), Policy Authority (PA) and the Primary Point of Contact (PPC).

VP of Cyber Security (VPCS)

The VPCS is responsible and accountable for the management and the implementation of the PKI Service. The VPCS's duties include but are not limited to:

- Inform the eHealth Ontario oversight committee for security related policies and issues (known as the Strategic Committee) of any changes to this policy.
- Recommending membership of the PA

- Chairing meetings of the PA.
- Advising the PA about the service offerings pursuant to agreements negotiated with Clients.
- Providing direction for the development of relevant policies by the PPC for submission to the PA for approval.
- Providing direction for the development of service implementation plans by ONE ID Business Services for approval by the PA.
- Promulgating final policy decisions approved by the PA.
- Ensuring that remedial actions are taken based on the results of audits and PKI policy-monitoring reports.

Policy Authority (PA)

The PA's primary responsibility is to establish and maintain a trusted environment providing confidence in the integrity and security of Registration, Enrolment and Authentication products and services offered through eHealth Ontario, including any PKI certificates issued by eHealth Ontario. Under its Terms of Reference, the PA is responsible to:

- Establish and approve appropriate mechanisms, controls and reporting structures for the management of the infrastructure products and Services related to Registration, Enrolment and Authentication.
- Develop and support implementation of policies, standards, directives and guidelines that ensure the credibility, integrity, reliability and security of the infrastructure.
- Provide direction through policies, standards and directives to ensure the harmonization, inter-operability and appropriate linkages of the infrastructure, eHealth initiatives and other service clients.
- Consider, and where applicable, approve requests for eHealth initiatives and other service clients to participate in the infrastructure.

Primary Point of Contact (PPC)

The eHealth Ontario Cyber Security department is responsible for providing PPC support to the PA and other parts of eHealth Ontario including:

- Selecting, defining and recommending policies to the PA.
- Providing policy direction to ONE ID Business Services.
- Assisting ONE ID Business Services in the development of practices and procedures by reviewing the CPS to ensure consistency with the CPM.
- Submitting change requests for any modifications to the baseline Certificate contents to the MSO PA (Entrust).
- Submitting change requests for any modifications to the security policies enforced through the PKI to the MSO PA (Entrust).

6. Operations

The primary operational bodies for the PKI Service are the PA, the RAs, and the LRAs.

Policy Authority (PA)

The PA is responsible and accountable to the VPCS for the operation and management of Registration, Enrolment and Authentication processes by:

- Designing, implementing, and operating its certification practices to reasonably achieve the requirements of PA approved policies, including the CPM.
- Creating and delegating authority to RAs following a review of the prospective RAs ability to perform the duties and obligations of an RA.
- Providing Registration, Enrolment and Authentication services for non- PKI related applications as approved by the PA.
- Development and management of the technology infrastructure.
- Conducting internal audits to monitor compliance with approved policies and reporting results to the VPCS.

The PA is the Root Certificate Authority for eHealth Ontario and may perform any or all duties or assigned any or all of its duties to a subordinate RA.

The PA may use one or more representatives or agents to perform its obligations, provided that PA retains overall responsibility for complying with this Certification Policy Manual.

Registration Authority (RA)

Individuals eligible to be RAs include:

- eHealth Ontario personnel in its Security Operations Team and the ONE ID Connector application.
- Those identified and accredited by the PA.
- Those employed by an organization that (a) performs Registration, Enrolment and Authentication services for profit, and that (b) have an agreement with eHealth Ontario or a Sponsorship Organization to perform these duties.

RAs are registered at a high Level of Assurance and issued a Certificate and digital encryption and signature Key Pairs.

Each RA is granted access privileges to the Registration Management System and is responsible for:

- Registering and delegating responsibilities to the LRAs needed to meet the needs of the Sponsorship Organization.
- Ensure that LRAs perform the duties assigned to them in conformity with the policies and practices approved by the PA, including the CP.
- Perform, as needed, the duties of LRAs or EAs.

An RA acts only on behalf of Sponsorship Organizations and Services for which he/she has been accredited by the PA.

Every RA must sign an Enrolment Form, approved by the PA.

Local Registration Authority (LRA)

LRAs carry out the day-to-day Registration and Enrolment activities required by the Sponsorship Organization for which they have been created as LRAs. Individuals eligible to be LRAs include:

- Those identified by the RA.

- Those nominated by a Client or a Sponsorship Organization, and accredited by the PA as LRAs.

LRAs are registered at a medium Level of Assurance (minimally) and issued an Authentication Credential sufficient to meet the security requirements of the Sponsorship Organization or Service in respect of which he/she is acting as a LRA.

Each LRA is granted access privileges to the Registration Management System and is responsible for:

- Registering sponsored Representatives and Computer Applications of a Client in the infrastructure.
- Enrolling Registrants in the Services for which they are being sponsored by that Client.

An LRA acts only on behalf of the Client or Sponsorship Organization and Services for which he/she has been accredited by the RA.

Every LRA must sign a Local Registration Authority Agreement with the PA.

7. End Users / Registrants

Two types of organizations have roles with respect to the PKI Service:

- Clients have a formative role in selecting the services that will be provided by eHealth Ontario and determining the conditions for access to these services.
- Sponsorship Organizations play an operational role in recommending the Registration Authority for their organizational context and identifying End Users for registration and service enrolment.

Please refer to the applicable definitions and roles for Clients, Representatives, End Users and Registrants as set out in the Services Agreement and PKI Services Schedule.

8. CLIENT Agreements

In order to receive PKI Services from eHealth Ontario, Clients must have in place a Services Agreement and sign the PKI Services Schedule. Such agreements ensure that a Client has in place mechanisms and procedures to ensure that its Sponsors, LRAs and Registrants are aware of, and agree to abide with, the stipulations in this policy that apply to them. After these agreements have been signed by a Client and accepted by eHealth Ontario, the PA or representative may require Client Representatives to complete a Registration Process, as outlined in the following eHealth Ontario document (available on request):

- “Getting Started with Computer Application Registration v1.2”

Part Two – Certification Policies

1. Introduction

1.1. Overview

Certification Policies (CP) are issued under the authority of the VP of Cyber Security (VPCS) of eHealth Ontario, as approved by the eHealth Ontario Policy Authority (PA), and effective as of the date set out in this Certification Policy Manual, and amended from time-to-time. This Certification Policy Manual establishes policy requirements for the effective management of the eHealth Ontario Public Key Infrastructure (PKI).

The policies established by this Certification Policy Manual have been developed in conformity with applicable enterprise policies as they are approved and amended from time to time. These policies include:

- eHealth Ontario Information Security Policy
- eHealth Ontario Privacy Policy

These policies may be consulted in the interpretation of this Certification Policy Manual.

1.1.1. Policy Objective

Well-defined, trusted processes are required to accommodate the health sector's needs and to facilitate health care delivery, and are based on user registration processes that are aligned with business, operational, security and confidentiality requirements. eHealth Ontario has established a Registration process to issue Authentication Credentials, including when required PKI Certificates, Confidentiality Key Pairs and/or Digital Signature Key Pairs.

The objective of the policies set out in this Certification Policy Manual is to ensure uniformity, consistency and coherence in the policies and practices followed by eHealth Ontario to establish and maintain an acceptable Level of Assurance and trust in the security services provided by eHealth Ontario while promoting the interoperability of health-related information systems in Ontario.

1.1.2. Policy Statement

eHealth Ontario will establish and manage the use of Registration, Enrolment and Authentication processes as components of its information infrastructure in support of achieving the following objectives:

- Provide trusted, secure electronic means for communicating health care information.
- Protect the privacy of health care information.
- Ensure security and integrity in transmitting messages and transactions containing health related information (including personal health information).
- Confirming, in accordance with a defined Level of Assurance, the identity of

individuals and Computer Applications that use electronic means to communicate health care information.

1.1.3. Policy Application

The CP set out in this Certification Policy Manual applies to the PA and all Registrants. The CP contains specifications for the management and use Authentication Credentials, including Certificates and Public/Private Key Pairs issued to Registrants. It also specifies the requirements for the management and use of Certificates and Public/Private Key Pairs issued to PA, RA and LRA personnel for the performance of their duties.

The CP defines the requirements applicable to the Root Certificate Authority within the PKI Service.

The CP defines three (3) types of Certificate used in the PKI Service:

- **Root CA Certificate:** The Root CA Certificate is a Certificate issued to eHealth Ontario's Certificate Authority (the "**CA**") by its service provider (Entrust) and signed by the CA. This Certificate is used to verify the signature of Registrant Certificates.
- **Issuing Certificate:** This is an intermediate certificate created by the Root Certificate Authority for the purpose of issuing certificates to Registrants. By doing this the Root Certificate can be isolated and protected from being compromised.
- **Registrant Certificates:** Certificates signed by the CA and issued to individuals and Computer Applications. These Certificates will be used for Digital Signature, and confidentiality purposes.

This CP also defines two separate policies for Public/Private Key Pairs issued by the CA:

1) Digital Signature Key Pairs and Certificates; and
2) Confidentiality Key Pairs and Certificates. In this CPM the type of Certificate policy will be identified where applicable.

- **The Digital Signature Key Pair policy** is for the management and use of Certificates and Digital Signature Key Pairs used for verification, authentication, integrity and key exchange. For instance, the certificates issued under these policies could be used for verifying the identity of electronic mail correspondents or for remote access to a computer system, verifying the identity of sponsored registrants or other legal entities, or protecting the integrity of software and documents.

- **The Confidentiality Key Pair policy** is for the management and use of Certificates and Confidentiality Key Pairs used for encryption, key establishment, and key transfer. The certificates issued under these policies are suitable for providing confidentiality for applications such as electronic mail or Web communications against unauthorized disclosure.

1.2. Policy Identification

The following policies set out in this Certification Policy Manual are called the *Certification Policies* (CP).

The Object Identifier (OID), registered with the Canadian Open Systems Interconnection Registration Authority (COSIRA), for this CP is: 2.16.840.1.114027.200.3.10.42

The policies under which Certificates are issued by eHealth Ontario have been assigned a unique

OID subordinate to the CA Certificate Policy OID Arc, having a root of 2.16.840.1.114027.200.3.10.42.x where *x* is equal to 1 and is henceforth incremented by 1 for each associated policy identifier.

The specific OIDs for policies defined in this CP are:

id-BasicCert	2.16.840.1.114027.200.3.10.42.1	ID ::= {id-cp2} [Not used]
id-MediumCert	2.16.840.1.114027.200.3.10.42.2	ID ::= {id-cp3}
id-HighCert	2.16.840.1.114027.200.3.10.42.3	ID ::= {id-cp4}

All Certificates issued under this CP identify the policy supporting their issuance. Certificates are only issued by eHealth Ontario at Medium and High Levels of Assurance.

1.3. Agreements

In addition to this CPM and the CA, each Client is subject to terms and conditions of the agreements identified in Section 8 of the Part I, *Concept of Operations*. In addition, Client Representatives may be required to accept such other additional terms and conditions specific to their roles, as identified in Section 8 of the Part I, *Concept of Operations.*

1.4. Certificate Applicability

Certificates issued under this CP are intended for use by Registrants.

The CA supports two (2) Levels of Assurance for the issuance of Certificates. The applicability of these levels is discussed in the *Concept of Operations,* [See: Part I, Section 3, Registration Requirements for Levels of Assurance], and summarized in the following table.

Figure 2: Summary of Certificate Applicability

<table>
<tr><td colspan="2"><b>Medium:</b> information or material with a medium sensitivity level, within eHealth Ontario and health sector environment, and that is intended for use by specific employees and Registrants.</td></tr>
<tr><th>Digital Signature</th><th>Confidentiality</th></tr>
<tr><td>This policy is suitable for the Integrity and Authentication of transactions that could result in serious adverse impact or loss.</td><td>This policy is suitable for transactions that if falsified or compromised could cause serious injury, loss of reputation, confidence or privacy.</td></tr>
<tr><td colspan="2"><b>High:</b> information with a high sensitivity level, within eHealth Ontario and the health sector environment, and that is extremely sensitive and of the highest value.</td></tr>
<tr><th>Digital Signature</th><th>Confidentiality</th></tr>
<tr><td>This policy is suitable for the Integrity and Authentication of transactions that could result in major adverse impact or loss</td><td>This policy is suitable for transactions that if falsified or compromised could cause significant injury, loss of</td></tr>
</table>

Certificates may be issued to Representatives of a Client for whom a Medium or High Level of Assurance has been established and may be used for Authentication, Confidentiality, Integrity and Non- Repudiation of message or transaction between the Registrant and with any other Registrant or system. Certificates issued to Representatives of a Client are identified with OIDs identifying that they are issued to individuals registered at a specified Level of Assurance.

Certificates issued to Computer Applications may be used for Authentication, Confidentiality, Integrity and Non-Repudiation of information exchanged with the Computer Application. Computer Application certificates are also identified with a specific OID. The person registered as responsible for a Computer Application is identified and registered.

1.5. Contact Details

The contact information for the PA is:

The PKI Policy Authority
eHealth Ontario, Department of Cyber Security
415 Yonge Street, Suite 1900
Toronto, ON M5B 2E7
Tel: (416) 586-4264
Fax: (416) 586-4363

2. General Provisions

2.1. Obligations

2.1.1. Policy Authority Obligations

The PA is responsible for initiating, establishing and operating all systems required for the Registration, Enrolment and Authentication for the PKI Services as provided by eHealth Ontario to its Clients.

Where necessary, this CP distinguishes the different users and roles accessing CA functions.

2.1.2. Certificate Authority Obligations

The responsibilities of the CA include:

- Signing a Root Certificate for the overall PKI Service in a high assurance environment in accordance with a specified root key generation ceremony.
- Issuing Certificates to itself in accordance with this CP.
- Providing CA Root services required to support the operations of the PKI.
- Identifying, authenticating and certifying CA personnel and RA and LRA officers.
- Generating Digital Signature Key Pairs, Confidentiality Key Pairs and Certificates for End Users in a manner that ensures trust and integrity.
- Providing Registrants with material and information needed to activate and use Digital Signature Key Pairs, Confidentiality Key Pairs and Certificates in a manner that ensures trust and integrity.
- Entering into a binding agreement with each RA and LRA that commits them to the obligations in this CP when they are registered and enrolled into these roles.
- Taking all reasonable efforts, including training, to ensure that Clients are aware of their respective rights and obligations including, where applicable, rights and obligations with respect to the operation and management of any Keys, Certificates or End User hardware and software used in connection with the PKI Service.
- Renewing and replacing of Certificates (as applicable).

- Revoking Certificates that are issued by the CA.
- Issuing and publishing Certificate Revocation Lists (CRL) and Authority Revocation Lists (ARL) on a regular schedule.
- Providing notification of Certificate status and revocation by providing access to at least one Repository holding relevant CRLs and ARLs.

2.1.2.1 CA Personnel Obligations

CA personnel, including personnel associated with specific PKI Service roles (e.g. Administrators, Master Users, and Security Officers), must be individually accountable for actions they perform.

Such personnel are obliged to:

- Maintain their cryptographic tokens in a secure manner according to established eHealth Ontario procedures for handling of such tokens.
- Ensure that their Private Keys are only used to access and operate CA applications.
- Not disclose to anyone any information needed to access their cryptographic tokens or utilize their Private Keys, including, without limitation, their passwords.
- Conform to all requirements and follow all instructions associated with the root key generation ceremony.
- Conform to all other requirements as may be specified from time to time by the PA.

If required, CA personnel may be issued Registrant Certificates and Keys to be used for purposes other than CA use.

2.1.3. Registration, Local Registration and Enrolment Authority Obligations

2.1.3.1 RA Obligations

RAs act as agents of the CA. RAs are responsible for carrying out the following duties in conformity with the CP:

- Creating and delegating authority to LRAs.
- Verifying the accuracy and authenticity of identification information submitted for LRAs.
- Ensuring that LRAs perform Registration, Enrolment and Authentication duties in conformity with the CP.
- Arranging security awareness and other training required for the performance of these duties.
- Revoking LRA permissions when no longer required.
- Verifying the accuracy and authenticity of information submitted by or for Registrants when performing the duties of an LRA.
- Performing other duties as may be reasonably consistent with the duties of an RA.

The RA may make use of existing CA or other approved databases as an agent to verify a Registrant's data by comparing it with information in the CA databases. The RA provides this verification on behalf of the CA as part of its delegated obligations.

RAs must be individually accountable for actions they perform and are subject to internal and external compliance audit processes as determined by the PA.

2.1.3.2 LRA Obligations

LRAs are created and delegated authority by RAs. LRAs are responsible for carrying out the following duties in conformity with the CP:

- Verifying the accuracy and authenticity of information submitted by or for Registrants when performing the duties of an LRA.

- Ensuring that Registrants are aware of their obligations.
- Arranging security awareness and other information and training required by Registrants.
- Performing other duties as may be reasonably consistent with the duties of an LRA.

The LRA may make use of existing CA or other approved databases as an agent to verify the Registrant's data by comparing it with information in the CA databases. The LRA provides this verification on behalf of the CA as part of its delegated obligations from the RA.

LRAs must be individually accountable for actions they perform and are subject to internal and external compliance audit processes as determined by the PA.

2.1.4. Registrant Obligations

Registrants may be individual Representatives of a Client or Computer Applications of a Client.

Client remains responsible for ensuring that its individual Registrants are made aware or their obligations with respect to the PKI Service to comply with the CP and PKI Services Schedule, including the Acceptable Use Policy.

In addition to the above, Representatives acting on behalf of a Client for a Computer Application are obligated to:

- Install technical and administrative controls over the use of Authentication Credentials for the Computer Application to ensure that it is used in a manner consistent with the CP and the PKI Services Schedule, including the Acceptable Use Policy.
- Where the technical administration is accessible to multiple persons:
  - maintain a list of authorized users
  - prevent use by other parties;
  - maintain a log of all use of the related Authentication Credential, including the date and time and identity of the person or persons using the Authentication Credential; and
  - ensure that all users of the account have received security training appropriate to the function for which the Authentication Credential is issued.

2.2. Liability

2.2.1. CA Requirements

The CA will ensure that its certification and repository services, issuance and revocation of Certificates, and issuance of CRLs and ARLs are in accordance with the CP. It will also take reasonable efforts to ensure that all RAs and LRAs follow the requirements of the CP when dealing with any Certificates containing this policy's OID or the associated Keys.

2.2.2. Disclaimers of Warranties and Obligations

The disclaimers applicable to the PKI Service are set out in Section 5 of the PKI Services Schedule.

2.2.3. Limitations of Liability

Each Certificate will be classified as being a member of one of the two classes of Certificates as shown in the first column of the table immediately following this paragraph. Pursuant to Section 6 of the PKI Services Schedule, in respect of each Certificate, in no event will the

Aggregate Liability Amount of eHealth Ontario or a Client exceed the amount shown in the row of the second column of such table which corresponds to the applicable class of such Certificate. The foregoing limitations do not apply to any claim arising from the fraud or wilful misconduct of eHealth Ontario or Client or any of their Representatives, or breach of Applicable Laws by eHealth Ontario or Client or any of their Representatives.

Figure 3: Aggregate Liability Amounts

Class of Certificate	**Aggregate Liability Amount**
Class 1 – Medium	$ **50,000**
Class 2 – High	$ **1,000,000**

2.3. Interpretation and Enforcement

2.3.1. Escalation of Issues

Within the PKI domain, in the event of any issues that arise and are related to the operation of the PKI Service, Client and eHealth Ontario will work together in good faith to resolve the issue in accordance with the following process.

- **Level 1 – Resolution by the PPC (Primary Point of Contact)**. Issues will be initially reported to the PPC who will make reasonable efforts to resolve the issue. An issue not settled by the PPC within 15 days will be referred to the PA for resolution.

- **Level 2 – Resolution by the PA.** The PA will make reasonable efforts to settle the issue within 15 days of escalation, provided that, if it is not resolved within such period of time, the matter will be escalated to the VPCS.

- **Level 3 – Resolution by the** Vice President of Cyber Security **(VPCS).** An issue not settled by the PA within the time period stipulated above will be referred to the VPCS for resolution. The VPCS will make reasonable efforts to settle the issue as soon as reasonably possible after escalation.

Issues related to the operation of the PKI Service include things like suspected corruption of a Certificate, the issuance of a Certificate to a wrong Registrant, etc. Any resolution of an issue by the VPCS will be final.

2.4. Publication and Repositories

The CA will operate the Repository, an on-line repository in which Certificates issued to Registrants as well as Certificate Revocation Lists and Authority Revocation Lists are stored. The CA will establish adequate access controls for the Repository. PKI certificates are published in the Repository as they are issued. Certificate Revocation Lists and Authority Revocation Lists are published in accordance with the Operational Requirements of the CP as further described in Part II, Section 4 below.

2.4.1. Publication of CA Information

The CA will:

- Include within any certificate it issues the URL of a web site maintained by, or on behalf of, the CA;
- Ensure the publication of its CP, digitally signed by an authorized representative of the CA.
- Ensure, directly or through agreement with the Repository, that operating system and Repository access controls will be configured so that only authorized CA personnel can write or modify the online version of the CP;
- Provide or a summary of key provisions when necessary for the purposes of any audit, inspection or accreditation;
  - Provide the CA's Certificate for its signature Key in the Repository; and
  - Publish a Certificate Revocation List (CRL).

2.4.2. Frequency of Publication

The CA will publish its CP and related documents within 14 days following the approval from the PA on the eHealth Ontario website. C ertificates issued by the CA must be published within 6 hours after issuance in the Repository. Information relating to the revocation of a Certificate must be published in accordance with Part II, Section 4.4.4 and in the CRL.

2.4.3. Access Controls

The Repository will be continuously available to Registrants, subject to reasonable scheduled maintenance and the CA's terms of access. The CA will impose access controls on Certificates, Certificate status information, or CRLs at its sole discretion. The CA will provide information concerning its access controls as required to allow integration between systems upon the written request of a Client.

2.5. Compliance Audit

The Certification Authority will be audited for conformity with industry standards and to provide attestation of compliance with this CP. The auditing of the root key generation ceremony (performed by Entrust Inc. on Oct 5th, 2016, and subsequently audited by Deloitte) will be considered the initial audit for the purposes of this CP. Compliance audits are expected to be performed on a 36 month cycle thereafter. The auditor must be an independent third party authorized and accredited to provide such audits.

2.5.1. Topics Covered by Audit

The purpose of such audit will be to verify that the CA has in place a system to ensure the quality of the CA services and that the CA complies with the requirements of this Certification Policy Manual and the related requirements of the PKI Services Schedule and Services Agreement. The audit requirements will extend to selected RAs and LRAs and EAs to demonstrate continuing compliance.

The Auditor will review the operation of the CA and deliver a confidential audit report within 30 days of the completion of the Audit to the VP of Cyber Security. The Audit report will advise whether or not the CA and supporting infrastructure:

- Has appropriately designed and implemented certification practices to reasonably achieve the requirements of this CP;

- Whether such certification practices have operated with sufficient effectiveness, since the last audit, to achieve the requirements of the CP;
- Whether the CA implements and complies with the technical, procedural, and personnel practices and policies; and
- Whether the RAs and LRAs implement and comply with the technical, procedural, and personnel practices and policies delegated to them.

2.5.2. Actions Taken as a Result of Deficiency

The VPSC will notify the PA of the outcome of any internal or external audits and proposed remedies to rectify any deficiency as quickly as possible after receipt of the audit report.

The VPCS will also report on the outcome of internal and external audits, including measures taken to remedy any discrepancies, to the Board of Directors of eHealth Ontario.

Failure to comply with this Certification Policy Manual or failure to implement remedial measures determined appropriate by the PA as a result of an audit may result in the suspension or revocation of Certificates issued to RAs and LRAs.

2.5.3. Communication of Results

The results of compliance audits are considered particularly sensitive Confidential Information of eHealth Ontario and are not generally communicated outside eHealth Ontario unless required by Applicable Laws.

The PA, with input from the auditor, will determine if Clients need to be informed of any deficiency identified by an audit, and the action taken to remedy it.

2.6. Confidentiality Policy

2.6.1. Types of Information to Be Kept Confidential

All information that is not considered by the CA to be public domain information is deemed to be eHealth Ontario Confidential Information, and will be dealt with in accordance with Section 8 of the Services Agreement.

Information regarding Registrants that is submitted on applications for Certificates by a Client but which is not included in the Certificate will be deemed to be Confidential Information and may not be released by the CA without prior written consent of the Registrant, unless otherwise required by Applicable Laws.

The Digital Signature Private Key of each Registrant is to be held only by the Registrant and must be kept confidential by them except in the case of roaming certificates. In the case of roaming certificates, the repository of Digital Signature Keys must be maintained in a PA approved environment with sufficient safeguards to ensure confidentiality and Integrity of the Keys. Any disclosure by the Registrant is at the Registrant's own risk. In the case of a Computer Application, the owner or the manager will be responsible for the use of the Certificate.

Confidentiality Private Keys will be backed-up by CA, in which case these Keys must be protected in accordance with Part II, Section 6. The Registrant must keep a copy of their Confidentiality Private Key confidential. Disclosure by the Registrant is at the Registrant's own risk.

Information pertaining to the CA's management of a Registrant's Digital Signature Certificate may only be disclosed to the Registrant, the employer or where required by Applicable Laws.

The CPS is Confidential Information and will not be released by the CA without the prior written consent of the VPCS, and then only subject to a separate written agreement setting out requirements to keep the CPS strictly confidential, unless otherwise required by Applicable Laws.

2.6.2. Types of Information Not Considered Confidential

CRLs and certain information on a Certificate, such as the name, title, contact information or designation of an individual that identifies the individual in a business, professional or official capacity and corporate information appearing on a Certificate are not considered sensitive and will be made available to the Clients for PKI availability and validation purposes.

2.6.3. Disclosure of Certificate Revocation or Suspension Information

Any requests for the disclosure of information about the reason for a Certificate suspension or revocation must be signed by the Client seeking such information and delivered to the eHealth Ontario VPCS. Such information may be provided in confidence at the sole discretion of the VPCS, or as required by Applicable Laws.

3. Identification and Authentication

3.1. Initial Registration

Subject to the requirements noted below, applications for Certificates may be communicated:

- From the Registrant to an RA or LRA, and authorizations to issue Certificates may be communicated from an authorized RA or LRA to the CA via the Registration Management System.
- Through an alternative registration process (e.g. a bulk load).

Applications must be complete and accompanied by all of the required Registration information.

3.2. Registration Information Requirements

3.2.1. General Information Requirements

3.2.1.1 Individual Registrants

The following table lists the primary identity and service related information required to register individual Registrants.

Figure 4: Registrant Information Requirements for Representatives

INFORMATION REQUIREMENTS	
Primary Identity Information	**Service Related Information**
Legal Name	Organizational Affiliation
Preferred Name	Organizational Title
Gender	Contact Information

Date of Birth	
Supporting Documents/ Identity Evidence	
Professional Licenses/Certificates	
Registration Identification Number	

3.2.1.3 Computer Applications

The information required to register a Computer Application is listed in the following table,.

Figure 5: Registrant Information Requirements for Computer Applications

INFORMATION REQUIREMENTS	
Primary Identity Information	**Service Related Information**
Application Name	Organizational Representative(s)
Application Identifier	Organization Registration Number
Application Contact Person	
Contact Information	
Registration Identification Number	

3.2.2. Types of Names

The CA Certificate will have a clearly distinguishable and unique X.500 Distinguished Name in the certificate subject name field in accordance with PKIX Part 1. The Distinguished Name will be "cn=xxx,ou=abc,dc=ssh,dc=com"

For the purpose of this policy, the Distinguished Name for Certificates issued to individual Registrants will be based on the Individual's legal name. This name will become the basis of a unique X.500 Distinguished Name in the certificate subject name field in accordance with PKIX Part 1.

Computer Application Certificates issued will have a clearly distinguishable and unique X.500 Distinguished Name in the certificate subject name field in accordance with PKIX Part 1.

The Registration Management System, any Directory and Certificates may also use preferred names for Individual Registrants.

3.2.3. Need for Names to be Meaningful

All Certificates issued by the CA will include an identifier that represents the individual Registrant or Computer Application to which the Certificate was issued. This identifier in the case of individual Registrants will directly correspond to the subject's legal name. For Computer Applications a corresponding "identifiable name" is required. The designated owner of the Computer Application will also appear in the DN of the certificate.

3.2.4. Rules for Interpreting Various Name Forms

The CA may further stipulate how names are to be interpreted by publishing such rules from time-to-time.

3.2.5. Uniqueness of Names

All Certificates issued by the CA will include an identifier that represents the individual Registrant or Computer Application to which the certificate was issued. The CA will take reasonable steps to ensure that each identifier will be unique in order such that no two certificates within the PKI will have the same identifier.

3.2.6. Registrant Name Claim Dispute Resolution Process

CA will be the naming authority and will investigate and correct, if necessary, any name conflicts or disputes brought to its attention at the time of the initial Registration.

Every Registrant must demonstrate the right to use a particular name.

3.2.7. Recognition, Authentication and Role of Trademarks

The use of trademarks is reserved to registered trademark owners.

3.2.8. Method to Prove Possession of Private Key

In all cases where the subject named in a certificate generates its own keys, that party shall be required to prove possession of the private key that corresponds to the public key in the certificate request. Proof of possession must be commensurate with the level of assurance being requested in the subsequent certificate. Cryptographic proof using the generated keys or in person proof using validated software and hardware are two examples of meeting this stipulation.

In the case where a key is generated directly on the party’s token, or in a key generator that benignly transfers the key to the party’s token, then the party is deemed to be in possession of the private key at the time of generation or transfer. If the party is not in possession of the token when the key is generated, then the token shall be delivered to the subject via an accountable method.

For all certificates other than High Assurance, when keyed hardware tokens are delivered to certificate subjects, the delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subjects. The CPS shall define a time limit for which a keyed module may be delivered to the intended Subscriber. If proof of successful delivery cannot be obtained in this timeframe, the RA or LRA shall revoke any certificates issued for keys contained in the module.

3.2.9. Identification and Authentication of an Organization

3.2.9.1 Sponsorship Organizations

An application for Registration of a Sponsorship Organization must be made by an individual who is authorized to act on behalf of the organization.

Certificates and Digital Signature Key Pairs are not issued to Sponsorship Organizations.

The information required to register a Sponsorship Organization is identified in the following table.

Figure 6: Sponsorship Organization Information Requirements

INFORMATION REQUIREMENTS	
Primary Identity Information	**Service Related Information**

Corporate Name	
Business Name	
Business Number	
Organizational Representative(s)	
Organizational Title	
Contact Information	
Registration Identification Number	

3.2.10. Identification and Authentication of Registrants

3.2.10.1 Identification and Authentication of Individual Identity

An individual may be registered in his/her own right as an individual Registrant or as the designated contact for a Computer Application. The Sponsor must verify the requirement of the Registrant to receive Keys to be used for an eHealth Ontario approved application. The Sponsor will certify the Registrant to the RA or LRA. The RA or LRA must verify the identity of the Registrant and keep a record of the type and details of identification used.

The following table specifies the minimum requirements for identification and Authentication of Registrants who are individuals by RAs and LRAs according to the relevant Levels of Assurance:

Figure 7: Minimum Requirements for Identification and Authentication of Individual

Medium		**High**	
Digital Signature	**Confidentiality**	**Digital Signature**	**Confidentiality**

Authentication of identity by sponsor or RA/LRA. Must provide 2 pieces of ID (**<u>notarized copies or originals</u>**) at least one must be government issued photo ID OR If the individual has previously been registered using a process that satisfies the CA as being comparable and demonstrating a documented and verifiable relationship with an acknowledged health sector regulatory body, administrative Agency or other designated organization, and there have been no changes to the information presented, the individual may be identified and authenticated using this privately shared information. A record must be maintained of the type and details of the identification used.	In person presentation of him or herself to the CA, RA or LRA for authentication prior to token initialization. AND Must present 2 pieces of ID (notarized copies or originals) one must be government issued photo ID) OR Use of shared database. A record must be maintained of the type and details of the identification used.

The minimum requirements for storage of Authentication Credentials are as follows:

Figure 8: Minimum Requirements for Storage of Authentication Credentials

Medium		High	
Digital Signature	Confidentiality	Digital Signature	Confidentiality
Roaming Software Certificates Smart Cards/Tokens		Smart Cards/Tokens Software (for applications only) Hardware Security Modules	

3.2.10.3 Identification and Authentication of Computer Applications

Computer Applications may be registered by a Sponsorship Organization that is the owner of the Computer Application. The registration must be requested by a person with authority to act on behalf of the Sponsorship Organization and indicate the "Contact Person" for the Computer Application. The Contact Person must be registered independently as an individual.

If there is an existing agreement between the CA and the Sponsorship Organization, additional Authentication of the identity of the Computer Application Unit may not be required.

3.3. Routine Rekey

The CA will allow Keys to be updated automatically within three months prior to the expiration of one of the Keys provided that the Certificate has not been revoked. Authentication of Registrant's identity need not be repeated but may be confirmed through the use of a shared secret.

3.4. Rekey After Revocation

Re-keying of Certificates for Registrants who's Certificates have been revoked will generally not be permitted until the Identification and Authentication requirements are repeated. The participating RA may allow exceptions in the following situations where the cause for revocation has been remedied and re-keying has been re-approved by the CA:

- An organizational change results in changes to the Distinguished Names of several employees; or
- An End User is temporarily unable to present himself or herself in person, for example because of extended travel, and the revocation was not due to a key compromise.

3.5. Authentication of Revocation Requests

Participating RAs/LRAs/EAs will permit Registrants or another person authorized to act on behalf of the Registrants to request revocation of a PKI certificate in which the Registrant is identified as the subject in the certificate. [See; Part II, Section 4.4]

4. Operational Requirements

4.1. Application for a Certificate

4.1.1. eHealth Ontario Registrant Application

The CA will ensure that all procedures and requirements with respect to an application for a Certificate are set out in a confidential document.

The Sponsor will initiate the Certificate application process by identifying to the appropriate RA, LRA or TA the names of the Registrants. Sponsorship Organizations must ensure that each application be accompanied by:

- Required identity information.
- Proof of the End User's identity.
- Consent for the collection, storage, use and disclosure of the information.
- Proof of authorization for any requested certificate attributes.
- A public verification key generated by or supplied to the End User.

Bulk applications on behalf of End-Users are permitted to be made only by persons authorized to make such applications subject to agreements with Sponsorship Organization.

Acceptance the applicable terms and conditions governing the use of the Certificate is not mandatory at the time of application. However, Clients are required to ensure compliance by all Registrants of the applicable terms and conditions governing use of the Certificate, as compliance is mandatory prior to valid use of the Certificates.

An application for a Certificate does not oblige CA to issue a Certificate.

4.2. Certificate Issuance

The issuance and publication of a Certificate by the CA indicates a complete and final approval of the Certificate application by the CA.

The CA Certificate will be self-generated and self-certified.

Certificates issued to CA personnel will be signed by the CA and require multi-person control by the CA.

4.3. Certificate Acceptance

Registrants who receive Management of Registrant Certificates confirm acceptance of the Certificate and profile by logging in to the PKI-enabled application for the first time.

Periodically an RA confirms the state of new Certificates issued to Registrants. The state of the Certificate should be "active":

- For a high Level of Assurance, within one (1) working day next following the receipt of the necessary data for activation and initialization.
- For a medium Level of Assurance, within two (2) working days next following the receipt of the necessary data for activation and initialization.

If the state is not active, the RA should conduct an investigation to determine if the Certificate should be suspended or revoked.

4.4. Certificate Revocation and Suspension

4.4.1 Circumstances for Revocation Request

A Registrant, RA, LRA or TA will inform eHealth Ontario if they become aware of any inaccuracy of the information in a Certificate (i.e., information in error at time of the Certificate's creation or information which has become obsolete since the time of Certificate creation).

The CA will revoke a Registrant's certificate when it is no longer wanted or required, or when the Certificates are no longer trusted. Some of the specific reasons include:

- Dismissal or suspension for cause.
- Termination of a business relationship.
- Compromise or suspected compromise of Private Keys, Registrant passwords and PKI profile file.
- Change in a Registrant's role or permissions.
- Failure of the Registrant to meet their obligations under the policy.

The CA may revoke a Certificate if there is a reason to believe that the Registrant has failed to meet material obligations, or there is suspicion of compromise of Private Key, or there has been use of the Certificate for unethical or illegal activities.

4.4.1.1 Permissive Revocation

An RA, LRA, Registrant, Client or Service Owner may request revocation of a Registrant's Certificate at any time for any reason.

4.4.1.2 Required Revocation

A RA, LRA, EA, Registrant or Service Owner is required to promptly request revocation of a Certificate:

- Whenever the Private Key, or the media holding the Private Key, associated with the Certificate has been compromised, or is reasonably suspected of having been compromised.
- Whenever an individual is no longer affiliated with, a member of, employed by, or under contract with the Sponsorship Organization.

A CA will revoke a Certificate in accordance with Part II, Section 4.4.3:

- Upon request of the RA, LRA, Registrant, Client or Service Owner.
- Upon failure of the Registrant to meet its material obligations under this CP, any applicable Certificate practices, or any other applicable agreement, regulation, or law applicable to the Certificate that may be in force.
- If knowledge or reasonable suspicion of compromise is reported to the CA.
- If the CA, RA or LRA determines that the Registration was not properly made in accordance with the CP.
- If the CA, RA or LRA determines that the Certificate was not properly issued or used in accordance with the CP.

In the event that the CA ceases operations, all Certificates issued by the CA will be revoked prior to the date that the CA ceases operations.

4.4.2 Who Can Request Revocation

The revocation of a Certificate may only be requested by the:

- Registrant in whose name the Certificate was issued.
- Sponsor.
- CA.
- RA or LRA.
- Service Owner.

The CA must perform a suitable investigation to determine the validity of this request and take appropriate action.

The CA is obligated only to acknowledge receipt of such a request, with no obligation of confirming or denying the existence of the Registrants Certificate, status of revocation requests, or outcomes of revocation request, except as provided in Part II, Section 4.4.9.

4.4.3 Procedure for Revocation Request

Requests to revoke a Certificate may be received as set out below.

A revocation request may be generated electronically by a Client and sent to eHealth Ontario in accordance with the notice requirements in the PKI Services Schedule. An RA, LRA or CA Security Officer each will initiate the request utilizing their private signing key to authenticate the request.

Authorized personnel, requiring multi-person control, will perform revocation requests within four (4) hours or less following the suspicion or detection of a compromise, the failure of adherence to this Certification Policy Manual, or any other event necessitating revocation as determined by the CA at its sole discretion. The rationale for such a revocation will be documented, requiring m of n (multi-person control) Security Officers each utilizing their private signing key, and archived.

A revocation request, and any resulting actions taken by the CA, will be recorded and retained. In the case where a certificate is revoked, full justification for the revocation will also be documented.

The CA will notify Registrants by posting revoked certificates to the
CRL or ARL), as appropriate.

4.4.4 Time to Process Revocation Request and Certificate Revocation List - Frequency

The CA will publish updated CRLs at least once every 6 hours, with next scheduled update periods specified every 72 hours.

4.4.5 Circumstances for Suspension

Individual Registrant and Computer Application Certificates may be suspended.

4.4.6 Who Can Request Suspension

The suspension of a Certificate may only be requested by the:

- Registrant in whose name the Certificate was issued.
  - Sponsor/Client.
  - CA.
  - RA or LRA.
  - Service Owner.

4.4.7 Procedure for Suspension Request

Requests to suspend a Certificate may be received as set out below.

A suspension request may be generated electronically by a Client and sent to eHealth Ontario in accordance with the notice requirements in the PKI Services Schedule. An RA or LRA or CA Security Officer each will initiate the request utilizing their private signing key to authenticate the request.

Authorized personnel, requiring multi-person control, will perform suspension requests within four (4) hours or less following the suspicion or detection of a compromise, the failure of adherence to this Policy, or any other event necessitating suspension as determined by the CA in its sole discretion. The rationale for such a suspension will be documented, requiring m of n (multi-person control) Security Officers each utilizing their private signing key, and archived.

A suspension request, and any resulting actions taken by the CA, will be recorded and retained. In the case where a Certificate is suspended, full justification for the suspension will also be documented.

The CA will notify Registrants by posting suspended certificates to the Certificate Revocation List (CRL) every four (4) hours.

4.4.8 CRL and ARL Issuance Frequency

The CA will ensure that it issues an up to date CRL at least every four (4) hours. The CA will ensure that its CRL issuance is synchronized with any Directory synchronization to ensure the accessibility of the most recent CRL to Registrants. When a Certificate is revoked due to key compromise the updated CRL will be issued immediately.

4.4.9 Certificate Revocation List Checking Requirements

Certificates may be stored locally in the Registrant's Public Key application but, before use, the Registrant will check the status of the certificate against the current CRL.

When a Registrant downloads a Certificate Revocation List from the Directory, the Registrant will verify the Certificate Revocation List by validating its digital signature.

4.4.10 On-line Revocation/Status Checking Availability

The CA does not support on-line revocation/status checking other than via CRLs as described in Part II, Section 4.4.9.

4.4.11 On-line Revocation Checking Requirements

In any Key compromise situation, the person detecting the compromise must file a report immediately upon the detection of the compromise with the CA, indicating the detailed circumstances under which the compromise occurred. If accidental on the part of the Registrant, no further action is required. Otherwise, the CA will determine if a possible follow up investigation and potential remedial action are required.

After revocation, the Registrant cannot log onto the PKI system and must be set up by a RA or LRA for Key recovery.

CA, RA and LRA compromises are investigated immediately

4.5. Security Audit Procedures

4.5.1 Types of Event Recorded

All significant events will be recorded in the CA audit logs. All logs will be time stamped with date and time of the event.

4.5.2 Audit Log Processing

Audit logs will be reviewed by CA personnel regularly and identified issues will be investigated, resolved and documented.

4.5.3 Retention Period for Audit Logs

Audit logs will be retained for the life of the CA and archived in accordance with the procedures specified by the PA.

4.5.4 Protection of Audit Logs

Access to audit logs will be protected by a combination of physical and procedural security controls specified by the VPCS taking into consideration industry best practices.

4.5.5 Audit Logs Backup

Audit log files will be backed-up and the backup media will be stored locally in a secure location. A consolidated copy of the audit log files will be sent to a secure off-site storage facility.

Retrieval of the backup audit logs will require multi-person control by Security Officers who are to be present at time of retrieval.

4.5.6 Notification Following a Critical Event

RAs, LRAs and CA application administrators will notify PKI Security Officers of any errors or other critical events and the CA will log the error in the manner specified by the VPCS.

All errors will be recorded and reported to the CA.

4.5.7 Vulnerability Assessments

The CA will ensure that incidents are assessed to ensure the integrity of the CA's ongoing operations.

4.6. Records Archival

4.6.1 Types of Record Archived

The CA will archive all material events, lists, certificates, keys, CRLs, ARLs, records, reports, agreements and correspondence.

Discrepancy and compromise reports and correspondence will be copied upon receipt and sent to a secure off-site storage facility. Original copies will be stored locally in a secure location.

4.6.2 Retention Period for Archive

All sensitive archived data will be retained in accordance with the procedures approved by the VPCS and in accordance with Applicable Laws.

4.6.3 Protection of Archive

The archive media will be protected either by physical security, or a combination of physical security and cryptographic protection. Additionally, the archive media will be provided adequate protection from environmental threats, such as temperature, humidity, and magnetism.

Subject to the requirements of Applicable Laws, only individuals authorized by the VPCS may view the archived records.

4.6.4 Archive Backup Procedures

CA Certificates, Certificate Revocation Lists, Authority Revocation Lists and Keys will be backed-up and stored locally in a secure location. A copy of the backup will be made and sent to a secure off-site storage facility.

4.6.5 Requirements for Time Stamping

The CA will ensure all logs, electronic or manual, contain the date and time of an event.

4.6.6 Archived Records and Archive Collection Systems

All material events, lists, Certificates, Keys, records, reports, agreements and correspondence will be archived.

Archived records will be transferred to separate physical media external to the CA host system.

4.6.7 Procedures to Obtain and Verify Archive Information

During an audit the auditor must verify the integrity of the archives, and if either copy is found to be corrupted or damaged in any way, it must be replaced with the other copy held in the separate location.

4.7. Key Changeover

CA will specify the Key changeover procedures. Key changeover procedures will allow for a "window" or "overlap" period (not to exceed three months) between the old keys and new keys.

4.8. Compromise of CA

The CA will assess the severity of any compromise to determine operational viability. The PA, with the advice of the CA, will determine the corrective measures deemed to be appropriate based on the procedures set out in the CPS.

Disaster Recovery and Business Continuity Plans for the CA, RA and LRA will be in place in accordance with the procedures specified by the VPCS.

5. Physical, Procedural and Personnel Security Controls

This section outlines the physical, procedural, and personnel security controls required of the CA, RAs and LRAs to protect their operations. eHealth Ontario's service provider for the PKI Service (currently Entrust) hosts and manages the physical infrastructure of the CA and is responsible for vetting its personnel that have access to the CA infrastructure.

5.1. Physical Security Controls

Physical security controls will be implemented to control access to the CA hardware and software hosted by eHealth Ontario's service provider. This includes the CA host computer, software and any external cryptographic hardware module and token.

The CA host computer will be in a secure space with appropriate access control systems, including:

- Manual and electronic monitoring for unauthorized intrusion at all times,
- Unescorted access limited to personnel identified on an access list.
- Personnel not on the access list to be escorted and supervised at all times.
- A site access log maintained at all times and audited periodically.

Access to the CA host computer will be controlled and will be limited to those personnel performing one of the roles described in this Certification Policy Manual. The secure space will be monitored by the CA.

RA and LRA and sites should be located in operation zones with physical security normally implemented for such areas in accordance with industry best practices, including:

- Be accessible only from a reception zone.
- Access limited to personnel who work within the zone and escorted visitors.
- Monitored for intrusion.

RAs and LRAs will implement, as a minimum, the following controls:

- Computers will have some form of access control feature and password-protected screen saver feature;

- Any password that allows access to Keys will be physically protected. Passwords will be memorized and not written down. If a password needs to be written down, it will be stored in a locked file cabinet or container accessible only by the RA or LRA.
- RAs and LRAs will not leave their computers unattended when their Private Key is in an unlocked state (i.e. when the password has been entered). The RAs' and LRAs' computers that contain private keys encrypted on a hard drive must be physically secured or protected with some form of access control.

All removable media and paper containing sensitive plain text information must be stored in secure containers, and disposed of in a secure and complete manner (e.g. by shredding).

5.2. Procedural Controls

The CA will ensure separation of duties for critical security functions. System access by CA personnel is to be limited to those actions for which they are required to perform in fulfilling their responsibilities.

5.2.1 Multiple Roles (Number of Persons Required per Task)

To ensure that one person acting alone cannot circumvent safe-guards, responsibilities are shared by multiple roles and individuals. Each account on the CA server has limited capabilities commensurate with the role of the account holder, as described in other related PKI installation and operations documentation.

5.2.2 Identification and Authentication for Each Role

Identification and Authentication mechanisms (such as passwords and tokens) are used to control account access for each role. All access by each role to accounts requires password or token identification and authentication.

5.3. Personnel Security Controls

The RA and LRA personnel will:

- Be appointed in writing by the PA;
- Receive proper training in relation to their assigned duties; and
- Be a full-time employee or other authorized individual not subject to frequent re-assignment or extended periods of absence.

The CA personnel must have appropriate security clearances as defined in the eHealth Ontario Security Policy. The RA and LRA personnel must meet reliability requirements defined in the CP and contained in the RA and LRA.

Any other personnel required for on-site support will be escorted in accordance with the security requirements set out in the applicable security requirements document for that site.

6. Technical Security Controls

This section refers to technical security controls that will apply to eHealth Ontario and its current service provider for the PKI Service (currently Entrust). Physical control of the CA resides with Entrust and the controls associated with the use of the CA reside with eHealth Ontario.

6.1. Key Pair Generation and Installation

6.1.1 Key Pair Generation

An automated process may be used to generate the Digital Signature Key Pair on behalf of the Registrant Certificates, provided that the Digital Signature Key Pair is transmitted to the CA personnel using a secure communication protocol. The Registrant's Confidentiality Key Pair will be generated by the CA and transmitted to the Registrant using a secure communication protocol.

The CA will generate Key material using only hardware cryptographic modules that have been certified to FIPS 140-2 Level 3.

CA Keys will be generated and stored in hardware cryptographic modules using a PA approved algorithm.

6.1.2 Private Key Delivery to End Entities

The Private Confidentiality Key must be either delivered to the Registrant in an on-line transaction in accordance with PKIX-3 Certificate Management Protocol, or via an equally secure manner approved by the PA.

6.1.3 Public Key Delivery to Certificate Issuer

Registrant Public Keys are transferred to the CA as part of the Certificate issuance process.

6.1.4 CA Public Key Delivery to Users

Registrants require the CA's Public Key Certificate to verify the Registrant's Certificate and to validate trust paths. Delivery of the CA's Certificate will be completed prior to or concurrent with Certificate issuance. The CA public verification key must be delivered to the prospective Certificate holder in an on-line transaction in accordance with PKIX-3 Certificate Management Protocol, or via an equally secure manner approved by the PA.

6.1.5 Key Sizes

CA will use RSA Key Pairs with a minimum of a 2048-bit prime modulus.

6.1.6 Hardware/Software Key Generation

The Digital Signature Keys for all high Level of Assurance certificates will be generated in a hardware cryptographic module approved by the PA.

6.1.7 Key Usage Purposes

Digital Signature Keys will be used for Authentication, Non-repudiation and message Integrity. They may also be used for session key establishment.

Confidentiality Keys will be used for exchange and establishment of Keys used for session and data confidentiality.

6.2. Private Key Protection

6.2.1 Standards for Cryptographic Module

CA cryptographic operations will be performed by a hardware cryptographic module certified to at least FIPS 140-2 Level 3.

6.2.2 Private Key Escrow

CA Private Keys and End User Confidentiality Private Keys will be backed-up. End User Private Digital Signature Keys will never be backed-up.

Registrant Confidentiality Private Key recovery may be requested:

- By the Registrant.
- By the Sponsorship Organization to recover encrypted data for an individual entitled to see the data when that Registrant is unavailable or unwilling to do so.
- By the Sponsorship Organization to recover encrypted data for a Computer Application.

6.2.3 Private Key Backup

Private Keys and Key histories maintained by CA will be backed-up daily when on-line in an encrypted form in accordance with Part II, Section 4.6 of this CP.

6.2.4 Private Key Archival

Private Digital Signature Keys will not be archived.

6.2.5 Private Key Entry Into Cryptographic Module

The CA Private Digital Signature Key will remain in the cryptographic module that generated them, subject to backup as per Pat II, Section 4.6

The Private Confidentiality Key must be either entered into the module in accordance with PKIX-3 Certificate Management Protocol, or via an equally secure manner approved by the PA.

6.2.6 Method of Activating Private Key

Private Keys are activated when:

- The Root Certificate is self-signed by the CA.
- The Registrant Certificate is signed by the CA.
- The Private Key is accessed by an application or Registrant (e.g., via login).

6.2.7 Method of Deactivating Private Key

The following are methods of deactivating Private Keys:

- Logging out of private key module.
- Private Key life span expiration.
- Private Key module timeout.
- Removal of the Private Key's hardware device.
- The Certificate is revoked or removed from the Directory
- The End User logs out of the PKI system or PKI-enabled application.

6.2.8 Method of Destroying Private Key

Upon expiration or revocation of a Certificate, or other termination of use of a Private Key, all copies of the Private Key in computer memory and shared disk space will be securely destroyed.

6.3. Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Public Keys are archived as part of Certificate archival.

6.3.2 Usage Periods for the Public and Private Keys

CAs will use their signing keys for certificate and CRL signing functions. CAs will not issue Certificates that extend beyond the expiration dates of their own Certificates and Public Keys. Therefore, their Certificate validity periods must be greater than those for Registrants.

The CAs private signing Keys will be used to sign Certificates for not more than one-half of the CAs Certificate lifetime.

The maximum Key/Certificate lifetimes for all CAs issuing Certificates under this policy will be as follows:

- Signature verification Certificate: will not exceed December 31, 2030 if RSA-2048 is used or 20 years if a longer key size is used.
- Private signature Key: will not exceed December 31, 2030 if RSA-2048 is used or 20 years if a longer key size is used.

The Key/Certificate lifetimes for all Registrants will be as follows:

- Signature verification and encryption certificates ::= 3 years maximum
- Private signature keys ::= 3 years maximum (100% of the certificate lifetime)

6.4. Activation Data

Activation Data refers to the data that must be supplied by the subject of a Registrant or Management Certificate to gain access to the private keys corresponding to the Public Keys in the certificate.

Inactive Management Private Keys will be protected from unauthorized use by encryption keyed with a password, a token or other Identification and Authentication information.

6.5. Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The CA will include the following functionality either provided by the operating system, or through a combination of operating system, CA application, and physical safeguards:

- Access control to CA services and roles.
- Enforced separation of duties for CA roles.
- Identification and authentication of CA roles and associated identities.
- Object re-use for Certification Authority random access memory.
- Use of cryptography for session communication and database security.
- Key management plan integral to CA design.
- Archival of CA and client history and audit data.
- Audit of security related events.
- Self-test of security related CA services.
- Trusted path for identification of CA roles and associated identities.
- Recovery mechanisms for keys and the Certification Authority application; and
- The CA equipment will be dedicated to administering a Key management infrastructure. It will only have installed applications or component software that was part of the Key

Generation Ceremony.

6.5.2 Computer Security Rating

Where possible, security critical elements of the CA will use Communications Security Establishment evaluations or any other accredited third party evaluated products.

6.6. Life Cycle Technical Security Controls

6.6.1 System Development Controls

The CA must use software that has been designed and developed under a formal development methodology adhering to principles of continuous security risk management, and that are supported by configuration management tools and third party verification of process compliance.

6.6.2 Security Management Controls

A formal configuration management methodology must be used for installation and ongoing maintenance of the CA system.

6.7. Network Security Controls

All applications used in connection with the PKI Service and the Repository will be protected through use of appropriate networking technologies and devices configured to allow only the protocols and commands required for CA services.

6.8. Cryptographic Module Engineering Controls

CA Digital Signature Key generation, CA Digital Signature Key storage and Certificate signing operations will be performed in a hardware cryptographic module rated to at least FIPS 140-2 Level 3 or otherwise verified to an equivalent level of functionality and assurance. All other CA cryptographic operations will be performed in a cryptographic module validated to at least FIPS 140-2 Level 2 or otherwise verified to an equivalent level of functionality.

The RA and LRA Administrator Digital Signature Key generation and signing operations will be performed in a hardware cryptographic module rated to at least FIPS 140-2 Level 2 or otherwise verified to an acceptable level of functionality and assurance approved by the PA. All other RA and LRA cryptographic operations will be performed in cryptographic modules rated at FIPS 140-2 Level 1 or otherwise verified to an acceptable level of functionality and assurance as approved by the PA.

Registrants that use high assurance tokens will use a hardware cryptographic module validated to at least FIPS 140-2 Level 2 or otherwise verified to an equivalent level of functionality and assurance.

Registrants that use medium or basic assurance tokens will use a cryptographic module validated to at least FIPS 140-2 Level 1 or otherwise verified to an equivalent level of functionality and assurance.

7. Certificate and Certificate Revocation List Profiles

7.1. Certificate Profile

All Certificates will be issued in the *X.509 version 3* formats and will include the Base

Certificate Policy identifier within the *Certificate Policies* field. The Certificate profiles for Certificates authorized by PKI are set forth in *Appendix A – Certificate Profiles* of this CPM.

7.2. Certificate Revocation List Profiles

Certificate Revocation Lists will be issued in the X.509 version 2 formats. The profile for Certificate Revocation Lists issued pursuant to this Certification Policy Manual is set forth in *Appendix B – CRL Profile* of this CPM.

8. Policy Administration

The PA administers this CP.

8.1. Policy Change Procedures

8.1.1 Notice

Registrants must periodically check the CA Repository for notice of modifications to this CP.

8.1.2 Comment Period

Changes to items within this CP that in the judgment of the PA will have no or minimal impact on the Registrants using Certificates and Certificate Revocation Lists issued by the CA may be made with no change to the CP version number and no notification to the Registrants.

Registrants will be provided with notification of significant changes to this CP resulting in a new CP version number. If the PA decides that it is advisable, a review and comment period not to exceed sixty (60) days may be provided for in the case of significant changes.

The PA will review comments and make further changes as appropriate. If the PA decides not to make any further changes following review period, the initially proposed modified document will be published in the CA Repository.

8.2. Publication and Notification Policies

8.2.1 Applicability and Acceptance of Changes

In order to allow entities to modify their procedures, as needed, all changes to this CP will become effective thirty (30) days after final publication on the Repository.

Use of or reliance on a Certificate after the 30-day period (regardless of when the Certificate was issued) will be deemed acceptance of the modified terms.

8.3. Policy Approval Procedures

The PA has approved this CP on 2016 November 30 and will approve any subsequent changes.

Appendix A – Certificate Profiles

The purpose of this appendix is to define the various Certificate profiles that will be issued as part of the CA. The CA supports the following Certificate types:

- Root CA Certificate
- Registrant Certificate
- Management Certificate.

1. Root CA Certificate Profile

The following fields of the X.509 version 3 certificate format are used in the CA certificate:

Algorithm Object Identifiers

Certificates issued under this CP will use at least one the following OIDs for signatures:

Signature Algorithm Identifier	OID
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Certificates under this CP will use the following OIDs for identifying the algorithm for which the subject key was generated:

Algorithm Identifier	OID
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

X.509 v3 Certificate Attributes/ Extensions	Critical/Non Critical	Optional	Notes
Attributes			
Version			• V3
SerialNumber			• integer
Signature			• sha-2 with RSA Encryptions
Issuer			• cn=SSHA CA, o=SSHA Corp, c= CA
Validity			• 20 years • notBefore and notAfter are specified
Subject			• cn=SSHA CA, o=SSHA Corp, c= CA
SubjectPublicKeyInfo			• sha-2WithRSAEncryption – {2.16.840.1.114027.200.3.10.2}
Extensions			

SubjectAltName	Non critical	Optional	- Not present.
PolicyMappings	Non critical	Optional	- Not present.
NameConstraints	Non critical	Optional	- Not present.
PolicyConstraints	Non critical	Optional	- Not present.
IssuerAltName	Non critical	Optional	- Not present.
SubjectDirectoryAttributes	Non critical	Optional	- Not present.
PrivateKeyUsagePeriod	Non critical	Not optional	- notAfter is always used - notBefore is never used
AuthorityKeyIdentifier	Non critical	Not optional	- contains a 32 byte hash of the subjectPublicKeyInfo in the CA certificate
SubjectKeyIdentifier	Non critical	Not optional	- contains a 32 byte hash of the subjectPublicKeyInfo in the certificate

X.509 v3 Certificate Attributes/ Extensions	Critical/Non Critical	Optional	Notes
BasicConstraints	Critical	Not optional	- cA=TRUE
CRLDistributionPoints	Non critical	Not optional	- only 1 distribution point name is included in each certificate - only element [0] (distributionPoint) is used and includes the full DN
KeyUsage	Non critical	Not optional	- must assert the nonRepudiation bit as required
CertificatePolicies	Non critical	Not optional	- must include reference to this Policy (OID tbd) - policyQualifiers not supported

2. Registrant Certificate Profiles

The following fields of the X.509 version 3 certificate format are used for Registrant and Management Certificates:

X.509 v3 Certificate Attributes/ Extensions	Critical/Non Critical	Optional	Notes
Attributes			
Version			- v3
SerialNumber			- integer
Signature			- sha-2WithRSAEncryption – {1.2.840.113549.1.1.5}
Issuer			- cn=SSHA CA, o=SSHA Corp, c= CA
Validity			- 3 years - notBefore and notAfter are specified

X.509 v3 Certificate Attributes/ Extensions	Critical/Non Critical	Optional	Notes
Subject			- cn=Registrant_ID, ou= RegistrantCA, o=SSHA Corp, c= CA - Registrant_ID refers to the unique identifier applied to the certificate applicant as a participant in the SSHA PKI.
SubjectPublicKeyInfo			- sha-2WithRSAEncryption – {2.16.840.1.114027.200.3.10.2}
Extensions			
SubjectAltName	Non critical	Optional	- Not present
PolicyMappings	Non critical	Optional	- Not present.
NameConstraints	Non critical	Optional	- Not present.
PolicyConstraints	Non critical	Optional	- Not present.

X.509 v3 Certificate Attributes/ Extensions	Critical/Non Critical	Optional	Notes
IssuerAltName	Non critical	Optional	• Not present.
SubjectDirectoryAttributes	Non critical	Optional	• Not present.
PrivateKeyUsagePeriod	Non critical	Not optional	• notAfter is always used • notBefore is never used
AuthorityKeyIdentifier	Non critical	Not optional	• contains a 32 byte hash of the subjectPublicKeyInfo in the CA certificate
SubjectKeyIdentifier	Non critical	Not optional	• contains a 32 byte hash of the subjectPublicKeyInfo in the certificate
BasicConstraints	Critical	Not optional	• Not present
CRLDistributionPoints	Non critical	Not optional	• only 1 distribution point name is included in each certificate • only element [0] (distributionPoint) is used and includes the full DN
KeyUsage	Non critical	Not optional	• DigitalSignature = 1 • NonRepudiation = 1 • KeyEncipherment = 0 • DataEncipherment = 0 • KeyAgreement = 0 • KeyCertSign = 0 • CRLSign = 0 • EncipherOnly = 0 • DecipherOnly = 0
CertificatePolicies	Non critical	Not optional	• must include reference to this Policy (OID tbd) • policyQualifiers not supported

Appendix B – Certificate Revocation List Profile

The purpose of this appendix is to define the Certificate Revocation List profile that will be used as part of the eHealth Ontario PKI.

X.509 v2 Certificate Attributes/ Extensions	Critical/Non Critical	Optional	Notes
Attributes			
Version			• v2
Signature			• sha-2WithRSAEncryption – {1.2.840.113549.1.1.5}
Issuer			• cn=SSHA CA, o=SSHA Corp, c= CA •
ThisUpdate			• Time of CRL issue
NextUpdate			• Time of next expected CRL issuance
RevokedCertificates			• List of revoked certificate information
Extensions			
AuthorityKeyIdentifier	Non critical	Not optional	• contains a 32 byte hash of the subjectPublicKeyInfo in the CA certificate
CRLNumber	Non critical	Non optional	• Incremented each time a particular CRL/ARL is changed
ReasonCode	Non critical	Not optional	• CRL entry extension
IssuingDistributionPoint	Critical	Not optional	• element [0] (distributionPoint) includes the full DN of the distribution point • element [1] (onlyContainsUserCerts) is included for CRLs • element [2] (onlyContainsCACerts) is included for ARLs • element [1] and [2] are never present together in the same revocation list • elements [3] and [4] are not used
IssuerAltName	Non critical	Optional	• Not present
HoldInstructionCode	Non critical	Optional	• Not present
InvalidityDate	Non critical	Optional	• Not present
CertificateIssuer	Non critical	Optional	• Not present
DeltaCRLIndicator	Non critical	Optional	• Not present