eHealth Ontario PKI Certification Policy Manual

Part One: Concept of Operations

Part Two: Certification Policies

Version: 1.1 – 2005 January 25

Ontario
eHealth Ontario

Document Control

Document Identification

Title	*Certification Policy Manual*
Location:	
Maintained By:	eHealth Ontario
Published Form:	Adobe Acrobat Portable Document Format – Non revisable
Sensitivity:	Medium
Distribution:	Public
Conditional Release:	

Revision History

Version	PMA Approval Date	Publication Date
1.0	2004 June 30	
1.1	2005 January 25	

Copyright Notice

Table of Contents

Table of Figures

Part One – Concept of Operations

I. Introduction

This document contains the eHealth Ontario Agency's ("eHealth Ontario" or the "Agency") policies related to registering End Users of the eHealth Ontario information infrastructure, enrolling Registrants for specific Services provided by the eHealth Ontario to Client Organizations, and issuing Authentication Credentials which include but are not limited to the use the eHealth Ontario Public Key Infrastructure (the "PKI"). It has two parts:

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

- **Part Two – Certification Policies**
  Part two states the policies that have been approved by the eHealth Ontario Policy Management Authority (PMA) and recommended to the eHealth Ontario Chief Executive Officer (CEO) for both the PKI and non-PKI Registrations and Enrolments.

Both parts of the document are publicly available at. www.ehealthontario.on.ca.

The following order of precedence is to be followed with respect to any matter requiring the interpretation of any conceptual, policy or practice statement issued by eHealth Ontario:

- Regulation 43/02 under the *Development Corporations Act.*
- The eHealth Ontario Certification Policy.
- The eHealth Ontario Certification Practice Statement.
- Agreement(s) signed between eHealth Ontario and any Participant.
- The Concept of Operations.

II. Terminology

DEFINITIONS

The following define the terms used in the Concept of Operations, in the CP or in the CPS.

"Acceptable Use Policy" – requirements and best practice guidelines regarding security, privacy, confidentiality and acceptable use of Services provided by eHealth Ontario information infrastructure as issued and modified by eHealth Ontario from time to time.

"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).

"Agency" – the eHealth Ontario Agency.

"Aggregate Liability Amount" – the total amount of damages for which a PKI Participant would be liable to any other PKI Participant in respect of each Certificate.

"Assurance" – See **Level of Assurance.**

"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 but not limited to 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.

"Authority Revocation List" -- A list of revoked Cross Certificates (similar to CRL) used to evidence the revocation of a trust relationship with another CA.

"Certificate" – an electronic file in a format that is in accordance with ITU-T Recommendation X.509 and that 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.

"Certificate Authority" – a Certificate Authority is an entity that is responsible for authorizing and causing the issuance of a Certificate. A 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.

"Certificate Authority Software" – the application software required to manage the Keys and Certificates of Registrants.

"Certificate Policy" -- 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" – a comprehensive description of how all of the policy requirements stated in the CP will be implemented and maintained including the practices, which a Certification Authority employs in issuing and revoking Certificates, and providing access to them.

"Certificate Revocation List" – 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

"Client Organization" – an eHealth infrastructure initiative (e.g. Ontario Family Health Network, Ontario HIV Treatment Network, Integrated Services for Children Information Systems, Community Care Access Centres, Ontario Laboratory Information Systems, Ontario Health Network, others approved by the Lieutenant Governor in Council) that has entered into an agreement with eHealth Ontario for the provision of Services, products and technologies related to the operation of a secure province-wide information infrastructure for the collection, transmission, storage and exchange of information about health matters (including personal information).

"Computer Application" – an identifiable computer software process that generates or receives communications or transactions on behalf of an individual or organization which it represents as an "agent". It may be any software process used in healthcare information systems including those without any direct role in treatment or diagnosis. Examples of the types of Computer Application involved include:

- Health Network System host application.
- Core Applications developed through the Health Information Infrastructure Project (HIIP).
- Ontario Laboratory Information System (OLIS).
- Clinical Management System host application.
- Core Data Set (CDS) and Emergency Health Record (EmHR) host applications.
- ISCIS application
- Hospital Information Systems (HIS) that initiate or receive transactions independent of any specific user (e.g. periodic feeds to ISCIS).

"Confidentiality" – generally, a property of data that indicates the extent to which these data have not been made available or disclosed to unauthorized individuals, processes or other entities. With reference to technology systems, a security service (including PKI) which consists of encrypting data before it is stored or transmitted. The encrypted data is not comprehensible to any unauthorized individual. In PKI, confidentiality is achieved using the **Confidentiality Key Pair**.

"Confidentiality Key Pair" – a pair of asymmetric cryptographic keys composed of a public encryption key and a corresponding private decryption key.

"Cross Certificate" – a Certificate that establishes a network trust relationship between two Certification Authorities (peer-to-peer). For each trust relationship, CAs may issue a Cross Certificate to the other CA (i.e. a pair of Cross Certificates).

"Cross Certification" – a process by which a trust relationship between two CAs is established and managed for purposes of interoperability. Typically, Cross Certification consists of an agreement signed by the CAs to establish a trust relationship by the issuance of Cross Certificates, one for each of the CAs public verification keys. The Cross Certificate is used by Registrants associated with the CA that generated it to validate Certificates of Registrants associated with the other CA.

"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.

"eHealth Initiative" – See: **Client Organization**.

"eHealth Ontario" – the corporation formerly known as ***Smart Systems for Health Agency***, established by Ontario Regulation 43/02 under the *Development Corporations Act*.

"Electronic Signature" – electronic information that a person creates or adopts in order to sign a document; that is in, attached to, or associated with, the document, and that is compliant with the requirements set out in the *Electronic Commerce Act, 2000 (S.O.2000, c.17)*.

"End User" – a Registrant who is enrolled for a specific Service and issued Authentication Credentials, including but not limited to, PKI credentials, for purposes other than the management of Registration, Service Enrolment or Authentication Credentials.

"Enrolment" – the process of enrolling a Registrant as being authorized to access specific Service(s). 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. A Registrant may be enrolled for multiple Services.

"Enrolment Authority" – an entity that is delegated responsibility by an RA for the performance of tasks associated with enrolling Registrants for specific Services. An EA is

responsible for Service Enrolment processes within the organizational domain(s) for which they have been delegated permission. An EA requests, but does not issue or sign Authentication Credentials.

"Federal Information Processing Standard" – Federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. Federal agencies are expected to apply these standards as specified, unless a waiver has been granted in accordance with Agency waiver procedures.

"Governing Body" – an organizational authority that determines policy and procedures that may impact the eHealth Ontario CA.

"Individual" – a Registrant in his/her own right as a person. A variety of Individuals may be registered including:

- Health professionals who are recognized under the *Regulated Health Professions Act* or by equivalent provincial or national authority to be qualified to perform certain health services.
- Persons employed by a healthcare professional or organization who are not health professionals (e.g. receptionist, secretary office/business manager).
- Non-regulated healthcare providers who provide healthcare services that are not regulated but who are active in the community and sponsored by a registered healthcare organization (e.g. drug or alcohol education officer, OFHN).
- Employees of third party service providers such as health insurance organizations, health care educational institutions, and health related support organizations, etc.

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

"Infrastructure Services" – the organizational structure within eHealth Ontario that has responsibility for providing technology-based services to all eHealth Ontario clients and End Users.

"Integrity" – 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.

"Key" – See: **Confidentiality Key Pair, Digital Signature Key Pair**

"Level of Assurance" – the degree of confidence that a system or product implements a security policy. In PKI, the degree of confidence that can be placed on the association between a Registrant and the Registrant's public key.

"Local Registration Authority" – an entity that is delegated responsibility by an RA for the performance of tasks associated with identifying and authenticating Registrants. An LRA is responsible for Registration and Service 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.

"Management Certificate" – see PKI Management Certificate.

"Non-repudiation" – a condition whereby a Registrant cannot deny having digitally signed a message, transaction or file.

"Object Identifier" – the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the eHealth Ontario PKI they are used to uniquely identify the policies and cryptographic algorithms supported.

"Organizational Unit" – a Registrant that is established for the purpose of supporting one or more functional areas within an organization where there is a requirement to either address communications to the Organizational Unit, or to generate communications from the Organizational Unit, independent of knowledge by the sender or recipient of who the person(s) are that staff that unit. Organizational Units are created in order to support activities such as submitting a request for an appointment to a clinic, or notices advising of a change of policy for a department, etc. Some examples of likely Organizational Units are: Emergency Department, Accounting Department, Cancer Clinic, etc. of a specific hospital.

"Participant" – eHealth Ontario, and any party that has entered into an agreement with eHealth Ontario in connection with the use of the Services provided by the CA.

"Policy Management Authority" – the authority created by the eHealth Ontario Board of Directors to which responsibility and accountability has been delegated for setting policies related to the Registration, Service Enrolment and Authentication infrastructure, including but not limited to the PKI,; approving service implementation plans, and approving Cross Certification agreements with equivalent organizations and other Certificate Authorities.

"Public Key Infrastructure" – a system of policies, processes and technologies that allow End Users to use Public/Private Key Pairs in order to:

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

These Public/Private Key Pairs are encrypted and are issued by a Certificate Authority.

"PKI Management Certificate" – a Certificate issued by the CA to its employees to be used solely in the performance of their duties and responsibilities as PKI Personnel

"PKI Participant" – See **Participant.**

"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.

"Registrant" – a Individual, Computer Application or Organizational Unit which has been registered and assigned a unique identity as an End User of the eHealth Ontario information infrastructure for purposes other than the management of the information infrastructure.

"Registrant Agreements" -- agreements signed between the CA and Registrants setting out the rights and obligations of these parties.

"Registration" – the process by which a unique identity is established for any Participant of the eHealth Ontario information infrastructure with an associated defined Level of Assurance. This process is generally the responsibility of a Local Registration Authority, but may also be performed by a Registration Authority or the Certificate Authority.

"Registration Authority" – an entity that is delegated responsibility by the CA for the performance of tasks associated with identifying and authenticating Registrants. An RA is responsible for Registration and Service Enrolment processes within the organizational domain(s) for which they have been delegated permission. An RA requests, but does not issue or sign Authentication Credentials.

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

"Regulation" – Ontario Regulation 43/02 under the *Development Corporations Act*.

"Repository" – the single repository operated for all Registrants and other Participants of the PKI. All Certificates issued by all CAs, and all CRLs relating thereto, shall be published in the repository.

"Revoke" – to revoke a Certificate means to end the originally specified operational period of a Certificate from a specified time forward.

"Root", "Root Certificate Authority" – the top-level Certificate Authority that signs and manages its own root Certificate, Certificates issued to other Certificate Authorities that it may establish; and the cross certificates it issues to other Certification Authorities with which it cross certifies.

The CA is the Root Certificate Authority for the PKI.

"Services" – the service(s) described and defined in the Certification Policy Manual and the Certification Practice Statement.

"Service Enrolment" – See **Enrolment.**

"Service Level Agreement" – an agreement between a Client Organization, as a Service recipient, and eHealth Ontario, as the service provider, that specifies what Services are to be provided and the conditions associated with providing these Services.

"Sponsor" – a designated person who is appointed and responsible within the management organization of a Sponsoring Organization to perform duties assigned by the CA.

"Sponsoring Organization" – an organization that has entered into an agreement with eHealth Ontario to perform defined duties with respect to identifying Individuals, Organizational Units and Computer Applications for registration in the eHealth Ontario information infrastructure and for enrolment in a specific Service.

ACRONYMS

The following acronyms are used have the associated meaning when used in the Concept of Operations, the CP or the CPS.

ARL	Authority Revocation List
CA	Certification Authority
CAST	Symmetric Cipher named after the inventors Carlisle Adams and Stafford Tavares
CCTV	Closed circuit television
CIT	Corporate Information Technology
CMP	Certificate Management Protocol
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DAP	Directory Access Protocol
DES	Data Encryption Standard
DN	Distinguished Name
DNS	Domain Name Server
DSA/DSS	Digital Signature Algorithm / Digital Signature Standard
FIPS	Federal Information Processing Standard
HR	Human Resources
HTTP	Hypertext Transfer Protocol
I&A	Identification and Authentication
IETF	Internet Engineering Task Force
IS	Infrastructure Services
ISO	Information Security Officer
ITU	International Telecommunications Union
LDAP	Lightweight Directory Access Protocol
RA	Registration Authority
OA	Operational Authority
OID	Object Identifier
PA	Policy Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PMA	Policy Management Authority
PUB	Publication

RDN	Relative Distinguished Name
RFC	(IETF) Request For Comments
RSA	Rivest-Shimar-Adleman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SEP	Secure Exchange Protocol
SHA-1	Secure Hash Algorithm
S-HTTP	Secure Hypertext Transfer Protocol
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

III. Policy Foundations

The Smart Systems for Health Agency is an agency of the Ministry of Health and Long-Term Care established by Ontario Regulation 43/02 under the *Development Corporations Act*. Its overall mandate is to create a province-wide electronic information network enabling secure electronic communication among Ontario's health service providers. Under the Regulation, the Agency 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 the Agency's information infrastructure.

Once fully operational, the Agency's information infrastructure will enable healthcare providers to collect, use, manage, and share health-related information, including personal health information, electronically, anywhere in the province, while maintaining the confidentiality, integrity and security of the information involved. It will connect over 150,000 healthcare providers across 24,000 sites throughout Ontario, including physicians, community and continuing care providers, hospital and laboratory personnel, pharmacists, and public health professionals.

To meet this mandate, the Agency has implemented policies and processes covering:

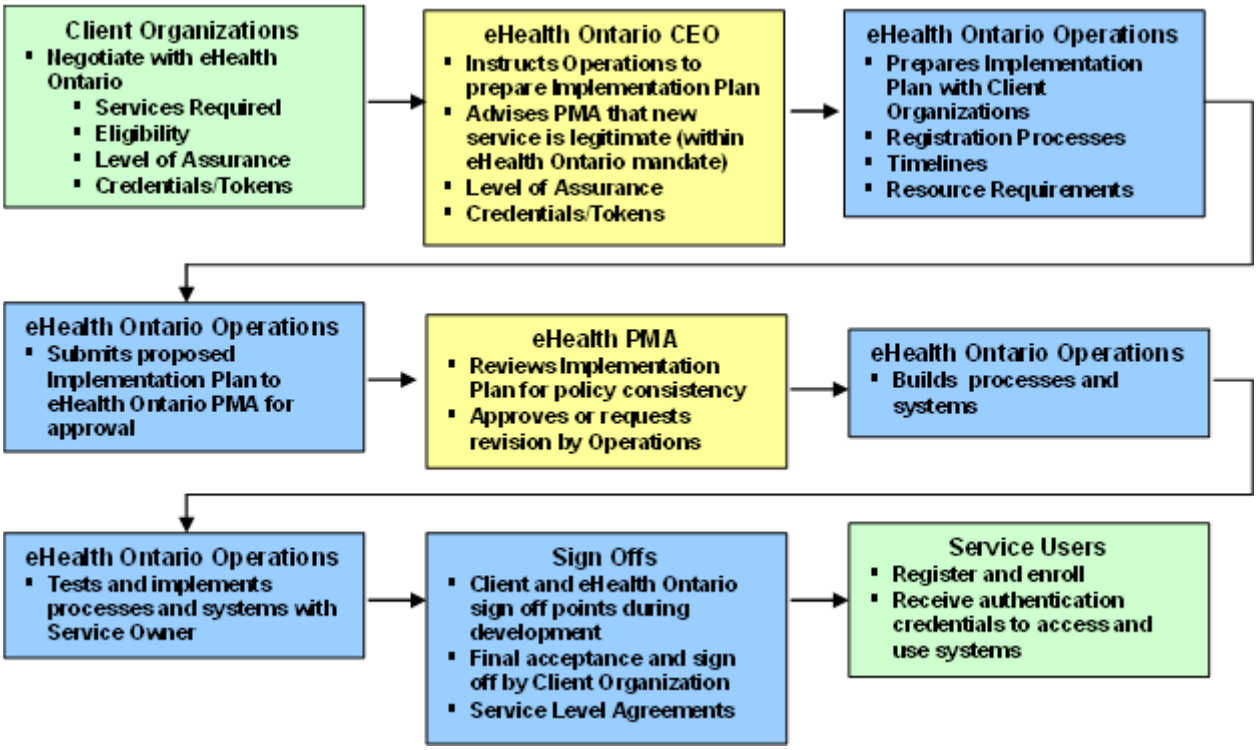
- Service Planning & Implementation.
- Levels of Assurance
- Registration and Enrolment.
- Authentication.
- Participant Roles and Responsibilities.
- Participant Agreements

These policies and processes are described in the following sections.

IV. Service Planning & Implementation

The Agency fulfills its mandate by providing Services in connection with Client Organizations specified in the Regulation, and other Services with the prior approval of the Lieutenant Governor in Council. In this regard, it delivers a variety of Services, products and technologies, including but not limited to the PKI, in order to meet the business requirements that are defined by Client Organizations. Figure 1 illustrates the Service Planning and Implementation process used by the Agency. The steps in the process are described following the figure.

Figure 1 Service Planning and Implementation



The first step in any provision of services involves negotiations between eHealth Ontario and a Client Organization. At a minimum, these negotiations define:

- The types of Services that will be provided.
- The End Users or classes of End Users who are eligible to be enrolled for these Services.
- The Level of Assurance required by the Service.
- The Authentication Credentials and/or tokens that will be distributed to End Users to access the Service.

When these negotiations are sufficiently mature, it is the responsibility of the Chief Executive Officer (CEO) to:

- Instruct operations to prepare a service implementation plan.

- Advise the Policy Management Authority (PMA) that a new service offering is being planned and that it falls within the Agency's mandate.

At this point, operations has the responsibility to prepare a service implementation plan in consultation with the Client Organization and other parts of eHealth Ontario. At a minimum, the service implementation plan covers:

- The Registration, Service Enrolment and Authentication processes that will be used to deliver the service.
- The role of Sponsoring Organizations, including the requirements for creating Registration Authorities and Local Registration Authorities.
- Privacy and Threat/Risk Assessments.
- Timelines for implementation.
- Resource requirements.

It is the responsibility of eHealth Ontario to submit the service implementation plan to the PMA for approval.

In addition, the Policy Secretariat is responsible to provide the PMA with any required briefing material. At a minimum, this material includes Threat/Risk and Privacy Impact assessments for the Service Implementations Plan.

The PMA is responsible to:

- Review the service implementation plan for consistency with approved policies, including the Certification Policy and the Certification Practice Statement.
- Consider any policy issues, including but not limited to amendments to the CP or CPS, associated with the implementation of the service.
- Approve the service implementation plan, service specific policies or policy changes, and/or request revisions to meet policy concerns.

If revisions are requested, these are prepared by operations and the service implementation plan or relevant parts of it are returned to the PMA for approval.

Once the service implementation plan has been approved, operations is responsible to:

- Build the processes and systems required for service.
- Test and implements processes and systems with the Client Organization.

Operations is responsible for obtaining Client Organization sign-offs at relevant points during the developmental process and final sign off following testing. A service level agreement between the Agency and Client Organizations is concluded prior to any system being fully implemented.

The service planning and implementation process is complete when systems become available to End Users to register in the information infrastructure, enroll for Services and receive authentication credentials to access and use systems. Subsequent changes to systems are managed using standard change management processes.

V. Levels of Assurance

eHealth Ontario provides Registration and Authentication Services, including the use of PKI Certificates, to Clients, at four Levels of Assurance 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: Rudimentary, Basic, Medium, and High. PKI Certificates are issued by the Agency only when a Medium of High Level of Assurance has been established for a Registrant.

Client Organizations negotiate and select the Level of Assurance meeting their business requirements for the Services being provided through the information infrastructure. In making their selection, Client Organizations should consider the following guidelines with respect to the applicability and appropriateness of the different Levels of Assurance.

Rudimentary Assurance is appropriate for information that has a sensitivity level of "unclassified" that is normally used for public information and internal communications such as internal documents, and unclassified communications, normally intended for communications between staff. If compromised, this information could reasonably be expected to cause no significant injury or losses to the parties involved and require only administrative action for correction.

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. As set out in the Agency's limitation of liability policy [CP, section 2.2.4], the liability of any PKI Participant in respect of a Medium assurance Certificate is limited to an aggregate amount of $50,000.

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 set out in the Agency's limitation of liability policy [CP, section 2.2.4], the liability of any PKI Participant in respect of a High Assurance Certificate is limited to an aggregate amount of $1,000,000.

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

VI. Registration & 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 he/she is enrolled in Service. 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, their registration information will be captured and stored for future use. Although initial Registration is normally linked to a Service Enrolment and an organizational context (e.g. membership in a sponsored group, employment by a Sponsoring 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 Sponsoring 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.

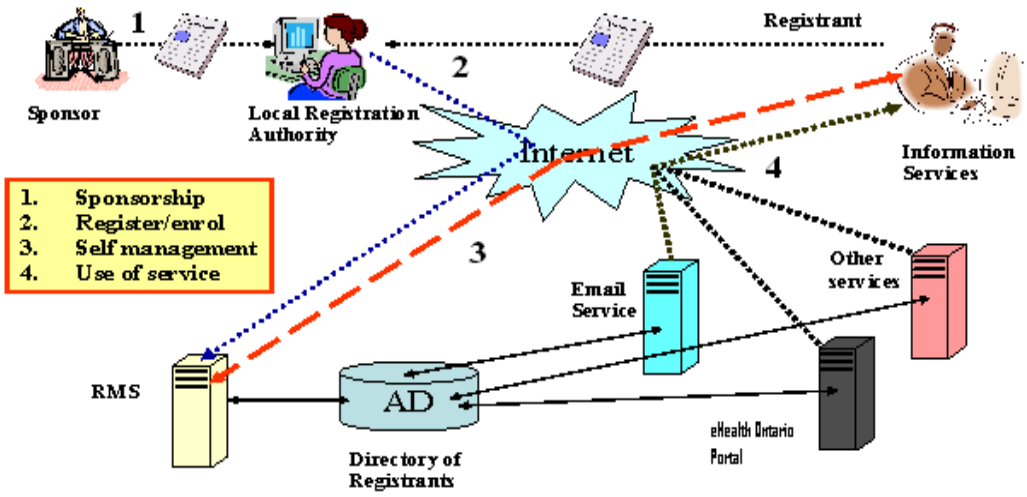
eHealth Ontario uses a distributed multi-organization service model for the delivery of Registration and Enrolment. This involves accrediting individuals identified by their respective organizations to act as Registration Authorities (RA), Local Registration Authorities (LRA) and Enrolment Authorities (EA) who can perform various Registration and Enrolment functions. This model reflects requirements arising from both the organizational diversity of Ontario's health care sector and its geographic distribution across the whole province. It allows the Registration and Enrolment functions to be performed by RAs, LRAs or EAs who are closer to, and have a pre-existing knowledge and relationship with, the Registrant. It also provides a significant degree of registrant self management to ensure that every Registrant is able to participate in the process as required using convenient and accessible electronic channels as often as possible.

Figure 3 provides a high level overview of this service model and registration and enrolment processes from the perspective of the user community, including both organizations and Registrants. This model has four basic elements:

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

Descriptions for each element are provided after the figure.

Figure 2 Sponsorship, Registration & Enrolment Model



Sponsorship

Sponsorship is basically the process of certifying the eligibility and providing identifying information for an Individual, Organizational Unit or Computer Application to be registered and enrolled. The Agency requires that every Registrant be sponsored. This is done by organization that has been registered as a Sponsoring Organization. Designated persons within Sponsoring Organizations act as Sponsors. The primary functions of Sponsoring Organizations and Sponsors are:

- To validate that specific Individuals, Organizational Units or Computer Applications are eligible to be registered in the information infrastructure and enrolled into products and services available through it.
- In some instances, provide the information required for Registration or Enrolment to an RA or LRA with the consent of Registrants.
- To identify the organization's requirements for RAs, LRAs or EAs, and to suggest to the CA the individuals who have the ability to perform these duties.
- To ensure that RAs, LRAs, EAs 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 Sponsoring Organizations. In some cases, the Client Organization that has negotiated an agreement with eHealth Ontario may also act directly as a Sponsoring 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. In others cases, either the Client Organization or eHealth Ontario may identify organizations to act as Sponsors for their employees. For example, a hospital or medical practice might serve as the Sponsoring Organizations for their employees.

Sponsorship may be performed outside of the normal Registration and Enrolment processes. For example, a Sponsoring 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. These features of sponsorship will be determined as part of the service implementation plan prepared by operations and approved by the PMA. Sponsoring Organizations enter into an agreement signed with eHealth Ontario at the time they are identified and registered.

Sponsorship and the registration of Sponsoring Organizations are very important to the overall process of registration and enrolment to help achieve the following:

- Minimize instances of registered non-users.
- Delegate authority to register closer to potential Registrants and establish the organizational domain within which RAs, LRAs and EAs may operate.
- Increase confidence in the identity of Individual Registrants and establish the organization domain within which they are being enrolled and issued Authentication Credentials for specific Services.
- Attribute the responsibility for the use and security of Authentication Credentials issued to Organizational Units and Computer Applications to the Sponsoring Organization and a responsible person who has been previously registered in the information infrastructure and assumes responsibility for these Registrants.
- Distribute the responsibility for accessing and using Services amongst eHealth Ontario, the Sponsoring Organization and 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 the End Users of the information infrastructure is established to a defined Level of Assurance by verifying that an organization or individual 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, including personal health information, which is exchanged by health care providers using Services provided through the infrastructure. Through a series of processes and checkpoints, an individual'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 are you?
2. Can you prove your identity?
3. Are you entitled to be a Registrant?

Despite the fact that you may have worked with an individual for 20 years, have you ever seen their driver's license? Do you really know that they are who they claim to be or do you take it for granted? Although this type of proof of identity may sound extreme, the fact that all of the individuals who are registered undergo some level of identity check is the cornerstone of the trust required by the information infrastructure. This is known as the Level of Assurance, and it ensures that you are doing more than just taking someone's word for their identity.

Registration will happen most times only once for a Registrant if their registration Level of Assurance never changes. 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 is valid over multiple organizations.

Registration Requirements for Levels of Assurance

eHealth Ontario uses registration processes to establish identity at four 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. **Rudimentary**
   a. The submission of these Registration applications may be online and do not require any verification of information or identity. It accepts the Registrant's attestation of identity.

2. **Basic**
   a. The Registrant must be sponsored by a Sponsoring Organization registered by eHealth Ontario.
   b. The Registrant must be involved in the process
   c. The registrant must provide TWO pieces of identification one of which must be government issued containing a photograph. Only one of the documents presented as proof identity must be government issued. The second may be issued by a type of institution approved by eHealth Ontario in its CPS. Both documents must show the same first and last name for the Registrants.
   d. The applicant must provide to the LRA originals or photocopies of their identity documents.
   e. These documents must be reviewed by the LRA.

3. **Medium**
   a. The registrant must be sponsored by a Sponsoring Organization registered by 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. The applicant must provide two pieces of identification both of which must be government issued and provide the Registrant's legal name (first and last). One of these government issued documents must contain a photograph.

e. The applicant must provide to the LRA originals or notarized copies of the identity documents
f. These documents must be reviewed by the LRA.

4. High

a. The registrant must be sponsored by a Sponsoring Organization registered by eHealth Ontario.
b. The Registrant must be involved in the process
c. A face to face interview must be performed where the registrant presents their supporting identity documents to the LRA.
d. The applicant must provide two pieces of identification both of which must be government issued and provide the Registrants legal name (first and last). One of these government issued documents must contain a photograph.
e. The applicant 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 3 Summary of Levels of Assurance

Identity Assurance Level	Sponsorship Required	Registrant involved in process	Face to face required	Identity Documents	Identity Document Verification		
					Reviewed	Recorded	Verified
Rudimentary	No	No	No	N/A	No	No	No
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	Yes	2 pieces of identification (notarized copy or originals), both of which are government issued, one containing a	Yes	Yes	No

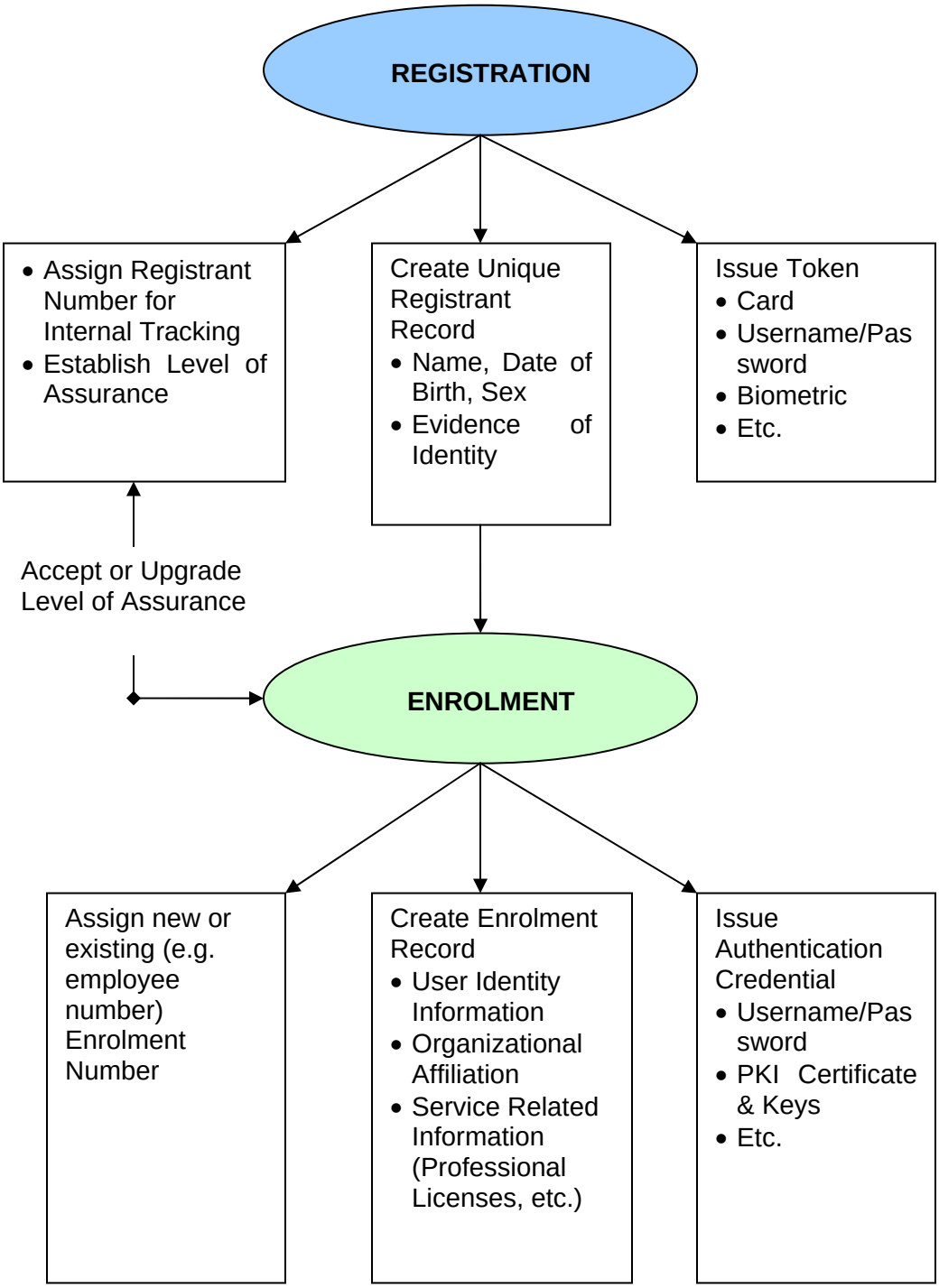
Identity Assurance Level	Sponsorship Required	Registrant involved in process	Face to face required	Identity Documents	Identity Document Verification		
					Reviewed	Recorded	Verified
				photo.			
High	Yes	Yes	Yes	2 pieces of identification (notarized copy or originals), both of which are government 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 Services and products 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 an applicant being sponsored by an organization to be enrolled into a Service or product. It allows the RA or LRA to establish the Level of Assurance in the real-world identity of an applicant before enrolling them into the Services or products 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.

Figure 4 Registration and Enrolment Linkages



The Level of Assurance required by a Registrant to access a specific service is defined by the Client Organization in its agreement with eHealth Ontario at the time this Service is set up within eHealth Ontario. This means that a Service or product which requires a medium Level of Assurance will not allow Enrolment of Registrants who are identified as having a rudimentary or basic Level of Assurance. If the requisite Level of Assurance is documented in an existing Registrant record, the enrolment may proceed in that basis. If not, the Level of Assurance for a Registrant will first have to be upgraded 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 Sponsoring Organization may be used (e.g. employee number). For privacy purposes, it 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 policies.
- Confirming the Registration information provided by the Sponsoring 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 to the 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. Electronic information systems are being used in the health care environment to transmit health-related information (including personal health information) in increasingly sensitive and critical circumstances. 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.

VII. 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 or product 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 PKI Certificates one which he/she uses to access the email at organization A and the other he/she uses 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 (Confidentiality). 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.

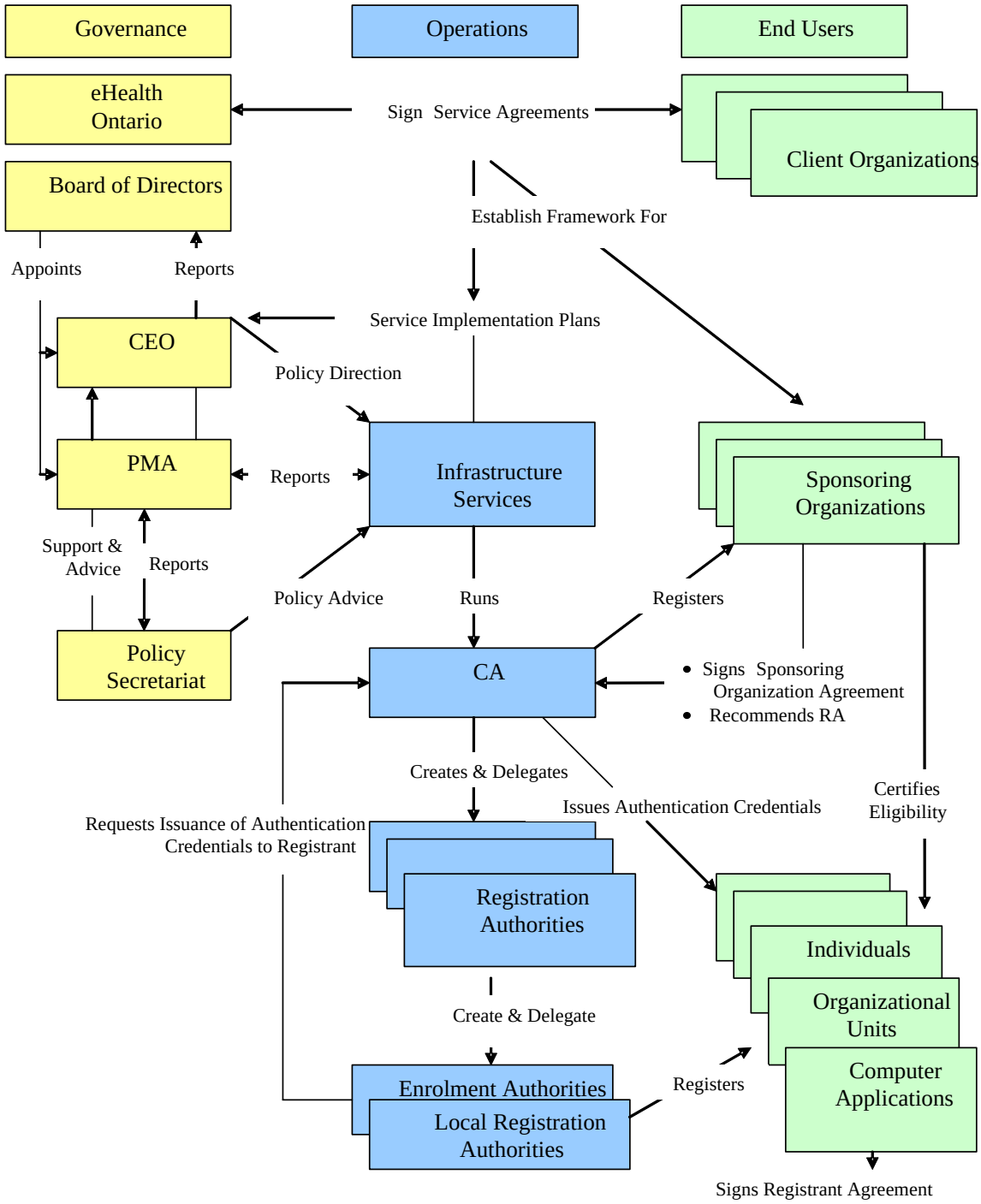
In the healthcare environment, the use of PKI allows the senders and recipients of information to be sure of the source of the document or information, that it has not been changed since it was created, and that its confidentiality has been protected during the transmission. Using PKI allows organizations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

VIII. Summary of Roles and Responsibilities

The eHealth Ontario model incorporates interacting roles and responsibilities for multiple Participants. Figure 5 summarizes three distinguishable sets of roles, responsibility and accountability relationships: Governance, Operations and End Users. The sections that follow describe the accountability of each set of stakeholders depicted in the figure.

Figure 5 Participant Relationships and Roles

(See next page)



IX. Governance

The primary governing bodies of eHealth Ontario with respect to Registration, Service Enrolment and Authentication are the Board of Directors, Chief Executive Officer (CEO), Policy Management Authority (PMA) and the Policy Secretariat.

Board of Directors

The Board of Directors (Board) is responsible and accountable for overall leadership of eHealth Ontario. It is responsible to establish and appoint members to the Policy Management Authority, to set Certificate policies concerning the operations of the Certificate Authority and Public Key Infrastructure, and to consider and approve applications for cross-certification with the Certificate Authority.

Chief Executive Officer

The CEO is responsible and accountable to the Board for the efficacious management of eHealth Ontario and the implementation of the PKI. The CEO's duties include but are not limited to:

- Recommending membership of the PMA to the Board of Directors based on achieving broad representation from stakeholder organizations;
- Chairing meetings of the Policy Management Authority.
- Advising the PMA about the Service offerings pursuant to agreements negotiated with Client Organizations.
- Providing direction for the development of relevant policies by the Policy Secretariat for submission to the PMA for approval.
- Providing direction for the development of service implementation plans by Infrastructure Services for approval by the PMA.
- Entering into agreements with and terminating written agreements for Cross Certification on behalf of Smart Systems for Health;
- Promulgating final policy decisions approved by the PMA.
- Ensuring that remedial actions are taken based on the results of audits and PKI policy-monitoring reports.

Policy Management Authority

The PMA's primary responsibility is to establish and maintain a trusted environment providing confidence in the integrity and security of Registration, Service Enrolment and Authentication products and services offered through eHealth Ontario, including but not limited to any PKI certificates issued by eHealth Ontario. Under its Terms of Reference, the PMA is responsible to:

- Establish and approve appropriate mechanisms, controls and reporting structures for the management of the infrastructure products and Services related to the Registration, Service 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.
- Establish and approve applicable policies, practices and guidelines to be followed to cross-certify with equivalent organizations and systems external to eHealth Ontario to maintain required levels of reliability and security.
- Consider Cross Certification requests with other PKI's.

Policy Secretariat

The eHealth Ontario Privacy and Security Office is responsible for providing Policy Secretariat support to the PMA and other parts of eHealth Ontario including but not limited to:

- Selecting, defining and recommending policies to the PMA.
- Developing and recommending Cross Certification agreements.
- Providing policy direction to Infrastructure Services.
- Assisting Infrastructure Services in the development of practices and procedures by reviewing the Certificate Practice Statement to ensure consistency with the Certificate Policies.
- Providing secretariat support to the PMA.

X. Operations

The primary operational bodies of eHealth Ontario are Infrastructure Services (IS), the Certification Authority (CA) and the distributed network of Registration Authorities (RA), Local Registration Authorities (LRA) and Enrolment Authorities (EA).

Infrastructure Services

Infrastructure Services (IS) provides technology-based services to all clients and End Users, as well as providing the regular information technology function within eHealth Ontario. The Chief Technology Officer is responsible and accountable to the CEO and the PMA for implementing approved policy and the overall management of the Registration, Service Enrolment and Authentication services through:

- Interpretation of approved policies, including the Certificate Policy and creation and management of operating policies and practices, including the Certification Practice Statement.
- Development of service implementation plans pursuant to agreements between eHealth Ontario and Client Organizations and submitting them to the PMA for approval.
- Establishment and management of the Certificate Authority in accordance with approved policies and acceptable business practices.
- Overall management of the technical infrastructure.
- Advising and reporting to the PMA and CEO regarding physical, personnel, operational and technical security.

Certification Authority

The CA is responsible and accountable to the Chief Technology Officer for the operation and management of Registration, Service Enrolment and Authentication processes and systems, including but not limited to the PKI by:

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

The CA may use one or more representatives or agents to perform its obligations, provided that CA retains overall responsibility for complying with policy.

Registration Authority

The CA is the Root RA for eHealth Ontario and may perform any or all duties assignable or assigned to a subordinate RA.

Persons eligible to be RAs include:

- Persons suggested by a Client Organization or a Sponsoring Organization.
- Persons identified and accredited by the CA.
- Persons employed by an organization that (a) performs Registration, Service Enrolment and Authentication services for profit, and that (b) have an agreement with eHealth Ontario or a Sponsoring Organization to perform these duties.

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

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

- Register and delegate responsibilities to the Local Registration Authorities and Enrolment Authorities needed to meet the needs of the Sponsoring Organization for which the RA has been created following a review or audit of the prospective LRA's or EA's ability to perform the duties and obligations of an LRA or EA.
- Ensure that LRAs and EAs perform the duties assigned to them in conformity with the policies and practices approved by the PMA, including the CP and the CPS.
- Perform, as needed, the duties of LRAs or EAs.

A Registration Authority acts only on behalf of any Sponsoring Organizations(s) and Services for which he/she has been accredited by the CA.

Every Registration Authority signs a Registration Authority Agreement with the CA.

Local Registration Authority

Local Registration Authorities carry out the day-to-day Registration and Enrolment activities required by the organization for which they have been created as LRAs. Persons eligible to be LRAs include:

- Persons identified by the RA.
- Persons suggested by a Client Organization or a Sponsoring Organization, and accredited by the CA as LRAs.
- Persons employed by an organization that (a) performs Registration, Service Enrolment and Authentication services for profit, and that (b) have an agreement with eHealth Ontario or a Sponsoring Organization to perform these duties.

LRAs are registered at a medium Level of Assurance (minimally) and issued an Authentication Credential sufficient to meet the security requirements of the Sponsoring 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 to:

- Register sponsored Individuals, Organizational Units and Computer Applications in the infrastructure.
- Enroll Registrants in the Services for which they are being sponsored by the Sponsoring Organization.

An LRA acts only on behalf of any subunit of the Sponsoring Organizations(s) and Services for which he/she has been accredited by the RA.

Every LRA signs a Local Registration Authority Agreement with the CA.

Enrolment Authority

Enrolment Authorities are limited to carrying out the Enrolment of existing registrants for new or additional services within the organization domain for which they have been created as EAs.

- Persons identified and accredited by an RA.
- Persons suggested by a Client Organization or a Sponsoring Organization, and accredited by an RA as EAs.
- Persons employed by an organization that (a) performs Registration, Service Enrolment and Authentication services for profit, and that (b) have an

agreement with eHealth Ontario or a Sponsoring Organization to perform these duties.

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

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

- Enroll existing Registrants in the services for which they are being sponsored by the Sponsoring Organization.

An Enrolment Authority acts only on behalf of any organizational subunit of a Sponsoring Organizations(s) and the Services for which he/she has been accredited by the RA.

Every EA signs a Enrolment Authority Agreement with the CA.

XI. End Users

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

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

Client Organizations

As noted in Section III, Client Organizations initiate the process of planning and implementing services by negotiating and signing Service Level Agreements (SLA) with eHealth Ontario. These negotiations may be conducted directly by Client Organizations listed in Regulation for specific infrastructure initiatives or by their designated agents. Client Organizations are responsible through SLAs for determining the following:

- The services that will be provided by eHealth Ontario.
- The Level of Assurance required in determining the identity of End Users and the Authentication Credentials required for the service access.
- Any other criteria that must be met to be enrolled for the service.
- The classes of entities who are eligible to apply for access to the Service.

Sponsoring Organizations

A Sponsoring Organization is an organization that has signed a Sponsoring Organization Agreement with eHealth Ontario as a PKI participant to perform specified duties and ensure that persons appointed by the Sponsoring Organization to perform these duties do

so in compliance with the policies set in the CP and CPS. Sponsoring Organizations are registered in the information infrastructure only to facilitate the registration of End Users, and may be Client Organizations, or other organizations identified by Client Organizations or eHealth Ontario, through the Service Planning and Implementation Process described in Section III.

Designated persons are appointed and responsible as Sponsors by the management organization of the Sponsoring Organization to perform duties assigned by the CA including but not limited to:

- Attesting that specific named Individuals, Organizational Units, or Computer Applications have a legitimate business requirement to be registered in the infrastructure and enrolled in a Service for which the Sponsor has been designated.
- Recommending the Registration Authority to perform duties as delegated by the CA for the Sponsoring Organization.
- Suggesting an appropriate Distinguished Name for Registrants.
- Supplying or confirming the information required for Registration or Service Enrolment to the RA or LRA.
- Informing the RA if the Sponsoring Organization's relationship with a Registrant is terminated or has changed.
- Promulgating PKI policy and guidelines, and monitoring their application.
- Providing organizational perspective and input into PKI policy and policy implementation.

End Users

End Users are Registrants who have been enrolled and issued authentication credentials for specific Services. eHealth Ontario registers and enrolls three types of End Users:

- Individuals in their right as persons (e.g. regulated health care professionals, non-regulated employees of health care professionals or organizations, non-regulated health care providers, etc.)
- Organizational Units established for the purpose of supporting one or more functional areas within a Sponsoring Organization where there is a need to either send or receive communications independent of knowing which staff of the Organizational Unit sends or receives the message.
- Computer Applications that generate or receive communications or transactions on behalf of an individual or organization which they represent as “agents”.

Every End User is required to sign an agreement with eHealth Ontario accepting the Terms and Conditions of Registration and Enrolment in the service.

When PKI is used End Users are issued Certificates and associated Private and Public Key Pairs that are used to ensure the secure exchange of sensitive information as described in Section VII.

The CP is binding on each Registrant that applies for and/or obtains Certificates, by virtue of the Registrant Agreement, and governs each Registrant's performance with respect to their application for, use of, and reliance on, Certificates. The right to reasonably rely on CA issued certificates is limited to the following persons:

- Registrants,
- Registrants of other CAs that have cross-certified with the CA.

XII. Participant Agreements

The CA shall enter into agreements with Participants and parties, including other CAs with which it is cross-certified. Such agreements shall:

- Ensure that a Sponsoring Organization has in place mechanisms and procedures to ensure that its Sponsors, RAs, LRAs EAs and Registrants are aware of, and agree to abide with, the stipulations in this policy that apply to them;
- Establish that any CA with whom it cross-certifies complies with all CPs that are mutually recognized; and
- Through compliance inspection, verify to cross-certifying CAs that eHealth Ontario complies with this CP.

Figure 6 Participant Agreements

AGREEMENT TYPE	SIGNATORIES	DESCRIPTION
Service Agreements	eHealth Ontario Client Organization	Agreements, signed between eHealth Ontario and Client Organizations specifying the Services to be supplied by eHealth Ontario and conditions associated with these Services.
Cross Certification Agreements		
Sponsoring Organization Agreements	eHealth Ontario Sponsoring Organization	Agreements signed between the CA and organizations that wish to be PKI Participants for purposes of establishing RAs, LRAs or EAs and acting as Sponsors to identify Registrants. The form of these agreements is specified in the CPS.
Registration Management Agreements	eHealth Ontario RA, LRA, EA	Agreements signed between the CA and individuals accredited to act as RAs, LRAs or EAs. The form of these agreements is specified in the CPS.

AGREEMENT TYPE	SIGNATORIES	DESCRIPTION
Registrant Agreements	CA Registrants	Agreements signed between the CA and Registrants providing notice of the Registrant's rights and obligations under the Certification Policies. At a minimum, Registrant Agreements cover: • The truth accuracy and completeness of the personal information provided or confirmed to be registered as a End User of the information infrastructure and enrolled in specific services provided by eHealth Ontario. • The consent to the collection, storage, use and disclosure of personal information for purposes related to registration, enrolment and issuance of authentication credentials. • The allowable uses of any Authentication Credential issued. • The obligation to keep any Authentication Credential secure and confidential. • The obligation to advise the CA of any change in information or any compromise of an Authentication Credential. • The procedures for communications between the Registrant and the CA or RA/LRA/EA with respect to any matter including: changes in service delivery or policy, changes of information, suspected compromise of an Authentication Credential, renewal, suspension or revocation of a registration, enrolment or authentication credential, etc. The form of these agreements is specified in the CPS.

Part Two Certification Policies

1.0 Introduction

1.1 Overview

Certification Policies (CP) are issued under the authority of the Chief Executive Officer (CEO) of eHealth Ontario as approved by the eHealth Ontario Policy Management Authority (PMA). It establishes policy requirements for the effective management of the eHealth Ontario Public Key Infrastructure (PKI). Registrants should consult the CP at www.ehealthontario.on.ca for details regarding Certification policies as well as policies for Certificates and Public/Private Key Pairs issued under it.

The policies established by this CP have been developed in conformity with applicable enterprise policies as they are approved and amended from time to time. These policies include but are not limited to:

- *Enterprise Security Policy – PSO* 001.
- *Enterprise Privacy Policy – PSO* 002.

These policies may be consulted in the interpretation of the CP.

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. Smart Systems for Health 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 this policy 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 the Agency while promoting the interoperability of health-related information systems in Ontario.

1.1.2 Policy Statement

The Smart Systems for Health Agency will establish and manage the use of Registration, Service 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, Organizational Units and Computer Applications that use electronic means to communicate health care information.

1.1.3 Policy Application

The CP applies to the CA, all Registrants and all parties with which the Agency has Cross Certification Agreements. It contains specifications for the management and use Authentication Credentials, including but not limited to PKI Certificates and Public/Private Key Pairs issued to Registrants. It also specifies the requirements for the management and use of PKI Certificates and Public/Private Key Pairs issued to CA, RA, LRA and EA personnel for the performance of their duties.

The CP defines the requirements applicable to the Root Certificate Authority within the PKI operated by eHealth Ontario.

The CP defines two (2) types of Certificates used in the PKI:

- **Root CA Certificate:** The Root CA Certificate is a self-signed Certificate issued to the CA by eHealth Ontario. This Certificate is used to verify the signature of Registrant Certificates.
- **Registrant Certificates:** Certificates signed by the CA and issued to Individuals, Organizational Units 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 CP 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.

1.1.4 Policy Interpretation

1.1.4.1 Interpretation

The CA is governed by Ontario Regulation 43/02, applicable laws of Ontario and Canada, and applicable policies concerning the enforceability, construction, interpretation and validity of this CP [See: Section 2.4].

The following order of precedence is to be observed in any matter requiring policy interpretation:

- Regulation 43/02 under the *Development Corporations Act.*

- The Certification Policy.
- The Certification Practices Statement.
- eHealth Ontario enterprise policies as approved and amended from time to time.
- Agreement(s) signed between eHealth Ontario and any PKI Participant.
- The Concept of Operations.

1.1.4.2 References

Unless otherwise specified, all references to "sections" in the CP refer to:

- The sections of this CP.
- The corresponding sections of the CPS when the CPS is referenced.

1.1.4.3 Formatting

The contents of this CP follow the framework and recommended elements defined by the Internet Engineering Task Force ("IETF") Request for Comment ("RFC", RFC 2527).

1.1.4.4 Terminology

Pronouns and any variations thereof will be deemed to include the feminine and masculine and all terms used in the singular will be deemed to include the plural, and vice versa, as the context may require.

The words "include" and "including" when used herein is not intended to be exclusive and means, respectively, "include, without limitation," and "including, but not limited to".

Acronyms and terms used in this CP have the same meaning as defined in the Glossary, *Concept of Operations* Section II, Terminology.

DEFINITIONS

"Acceptable Use Policy" – requirements and best practice guidelines regarding security, privacy, confidentiality and acceptable use of Services provided by the information infrastructure as issued and modified from time to time.

"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).

"Agency" – the Smart Systems for Health Agency.

"Aggregate Liability Amount" – the total amount of damages for which a PKI Participant would be liable to any other PKI Participant in respect of each Certificate.

"Assurance" – See **Level of Assurance.**

"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 but not limited to 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.

"Authority Revocation List" -- A list of revoked Cross Certificates (similar to CRL) used to evidence the revocation of a trust relationship with another CA.

"Certificate" – an electronic file in a format that is in accordance with ITU-T Recommendation X.509 and that 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.

"Certificate Authority" – a Certificate Authority is an entity that is responsible for authorizing and causing the issuance of a Certificate. A 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.

"Certificate Authority Software" – the application software required to manage the Keys and Certificates of Registrants.

"Certificate Policy" -- 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" – a comprehensive description of how all of the policy requirements stated in the CP will be implemented and maintained including the practices, which a Certification Authority employs in issuing and revoking Certificates, and providing access to them.

"Certificate Revocation List" – 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.

"Client Organization" – an eHealth infrastructure initiative (e.g. Ontario Family Health Network, Ontario HIV Treatment Network, Integrated Services for Children Information Systems, Community Care Access Centres, Ontario Laboratory Information Systems, Ontario Health Network, others approved by the Lieutenant Governor in Council) that has entered into an agreement with eHealth Ontario for the provision of Services, products and technologies related to the operation of a secure province-wide information infrastructure for the collection, transmission, storage and exchange of information about health matters (including personal information).

"Computer Application" – an identifiable computer software process that generates or receives communications or transactions on behalf of an individual or organization which it represents as an "agent". It may be any software process used in healthcare information systems including those without any direct role in treatment or diagnosis. Examples of the types of Computer Application involved include:

- Health Network System host application.
- Core Applications developed through the Health Information Infrastructure Project (HIIP).
- Ontario Laboratory Information System (OLIS).
- Clinical Management System host application.
- Core Data Set (CDS) and Emergency Health Record (EmHR) host applications.
- ISCIS application
- Hospital Information Systems (HIS) that initiate or receive transactions independent of any specific user (e.g. periodic feeds to ISCIS).

"Confidentiality" – generally, a property of data that indicates the extent to which these data have not been made available or disclosed to unauthorized individuals, processes or other entities. With reference to technology systems, a security service (including PKI) which consists of encrypting data before it is stored or transmitted. The encrypted data is not comprehensible to any unauthorized individual. In PKI, confidentiality is achieved using the **Confidentiality Key Pair**.

"Confidentiality Key Pair" – a pair of asymmetric cryptographic keys composed of a public encryption key and a corresponding private decryption key.

"Cross Certificate" – a Certificate that establishes a network trust relationship between two Certification Authorities (peer-to-peer). For each trust relationship, CAs may issue a Cross Certificate to the other CA (i.e. a pair of Cross Certificates).

"Cross Certification" – a process by which a trust relationship between two CAs is established and managed for purposes of interoperability. Typically, Cross Certification consists of an agreement signed by the CAs to establish a trust relationship by the issuance of Cross Certificates, one for each of the CAs public verification keys. The Cross Certificate is used by Registrants associated with the CA that generated it to validate Certificates of Registrants associated with the other CA.

"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.

"eHealth Initiative" – See: **Client Organization**.

"Electronic Signature" – electronic information that a person creates or adopts in order to sign a document; that is in, attached to, or associated with, the document, and that is compliant with the requirements set out in the *Electronic Commerce Act, 2000 (S.O.2000, c.17).*

"End User" – a Registrant who is enrolled for a specific Service and issued Authentication Credentials, including but not limited to, PKI credentials, for purposes other than the management of Registration, Service Enrolment or Authentication Credentials.

"Enrolment" – the process of enrolling a Registrant as being authorized to access specific Service(s). 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. A Registrant may be enrolled for multiple Services.

"Enrolment Authority" – an entity that is delegated responsibility by an RA for the performance of tasks associated with enrolling Registrants for specific Services. An EA is responsible for Service Enrolment processes within the organizational domain(s) for which they have been delegated permission. An EA requests, but does not issue or sign Authentication Credentials.

"Federal Information Processing Standard" – Federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. Federal agencies are expected to apply these standards as specified, unless a waiver has been granted in accordance with Agency waiver procedures.

"Governing Body" – an organizational authority that determines policy and procedures that may impact the CA.

"Individual" – a Registrant in his/her own right as a person. A variety of Individuals may be registered including:

- Health professionals who are recognized under the *Regulated Health Professions Act* or by equivalent provincial or national authority to be qualified to perform certain health services.
- Persons employed by a healthcare professional or organization who are not health professionals (e.g. receptionist, secretary office/business manager).
- Non-regulated healthcare providers who provide healthcare services that are not regulated but who are active in the community and sponsored by a registered healthcare organization (e.g. drug or alcohol education officer, OFHN).
- Employees of third party service providers such as health insurance organizations, health care educational institutions, and health related support organizations, etc.

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

"Infrastructure Services" – the organizational structure within eHealth Ontario that has responsibility for providing technology-based services to all the clients and End Users.

"Integrity" – 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.

"Key" – See: **Confidentiality Key Pair, Digital Signature Key Pair**

"Level of Assurance" – the degree of confidence that a system or product implements a security policy. In PKI, the degree of confidence that can be placed on the association between a Registrant and the Registrant's public key.

"Local Registration Authority" – an entity that is delegated responsibility by an RA for the performance of tasks associated with identifying and authenticating Registrants. An LRA is responsible for Registration and Service 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.

"Management Certificate" – see PKI Management Certificate.

"Non-repudiation" – a condition whereby a Registrant cannot deny having digitally signed a message, transaction or file.

"Object Identifier" – the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the PKI they are used to uniquely identify the policies and cryptographic algorithms supported.

"Organizational Unit" – a Registrant that is established for the purpose of supporting one or more functional areas within an organization where there is a requirement to either address communications to the Organizational Unit, or to generate communications from the Organizational Unit, independent of knowledge by the sender or recipient of who the person(s) are that staff that unit. Organizational Units are created in order to support activities such as submitting a request for an appointment to a clinic, or notices advising of a change of policy for a department, etc. Some examples of likely Organizational Units are: Emergency Department, Accounting Department, Cancer Clinic, etc. of a specific hospital.

"Participant" – eHealth Ontario, and any party that has entered into an agreement with eHealth Ontario in connection with the use of the Services provided by the CA

"Policy Management Authority" – the authority created by the eHealth Ontario Board of Directors to which responsibility and accountability has been delegated for setting policies related to the Registration, Service Enrolment and Authentication infrastructure, including but not limited to the PKI,; approving service implementation plans, and approving Cross Certification agreements with equivalent organizations and other Certificate Authorities.

"Public Key Infrastructure" – a system of policies, processes and technologies that allow End Users to use Public/Private Key Pairs in order to:

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

These Public/Private Key Pairs are encrypted and are issued by a Certificate Authority.

"PKI Management Certificate" – a Certificate issued by the CA to its employees to be used solely in the performance of their duties and responsibilities as PKI Personnel

"PKI Participant" – See **Participant.**

"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.

"Registrant" – a Individual, Computer Application or Organizational Unit which has been registered and assigned a unique identity as an End User of the information infrastructure for purposes other than the management of the information infrastructure.

"Registrant Agreements" -- agreements signed between the CA and Registrants setting out the rights and obligations of these parties.

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

"Registration Authority" – an entity that is delegated responsibility by the CA for the performance of tasks associated with identifying and authenticating Registrants. An RA is responsible for Registration and Service Enrolment processes within the organizational domain(s) for which they have been delegated permission. An RA requests, but does not issue or sign Authentication Credentials.

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

"Regulation" – Ontario Regulation 43/02 under the *Development Corporations Act*.

"Repository" – the single repository operated for all Registrants and other Participants of the PKI. All Certificates issued by all CAs, and all CRLs relating thereto, shall be published in the repository.

"Revoke" – to revoke a Certificate means to end the originally specified operational period of a Certificate from a specified time forward.

"Root", "Root Certificate Authority" – the top-level Certificate Authority that signs and manages its own root Certificate, Certificates issued to other Certificate Authorities that it may

establish; and the cross certificates it issues to other Certification Authorities with which it cross certifies.

The CA is the Root Certificate Authority for the PKI.

"Services" – the service(s) described and defined in the Certification Policy Manual and the Certification Practice Statement.

"Service Enrolment" – See **Enrolment.**

"Service Level Agreement" – an agreement between a Client Organization, as a Service recipient, and eHealth Ontario, as the service provider, that specifies what Services are to be provided and the conditions associated with providing these Services.

"Smart Systems for Health Agency" – the corporation established by Ontario Regulation 43/02 under the *Development Corporations Ac.*

"Sponsor" – a designated person who is appointed and responsible within the management organization of a Sponsoring Organization to perform duties assigned by the CA.

"Sponsoring Organization" – an organization that has entered into an agreement with eHealth Ontario to perform defined duties with respect to identifying Individuals, Organizational Units and Computer Applications for registration in the information infrastructure and for enrolment in a specific Service.

ACRONYMS

ARL	Authority Revocation List
CA	Certification Authority
CAST	Symmetric Cipher named after the inventors Carlisle Adams and Stafford Tavares
CCTV	Closed circuit television
CIT	Corporate Information Technology
CMP	Certificate Management Protocol
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DAP	Directory Access Protocol
DES	Data Encryption Standard
DN	Distinguished Name
DNS	Domain Name Server
DSA/DSS	Digital Signature Algorithm / Digital Signature Standard
FIPS	Federal Information Processing Standard
HR	Human Resources
HTTP	Hypertext Transfer Protocol
I&A	Identification and Authentication
IETF	Internet Engineering Task Force
IS	Infrastructure Services
ISO	Information Security Officer
ITU	International Telecommunications Union

LDAP	Lightweight Directory Access Protocol
RA	Registration Authority
OA	Operational Authority
OID	Object Identifier
PA	Policy Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PMA	Policy Management Authority
PUB	Publication
RDN	Relative Distinguished Name
RFC	(IETF) Request For Comments
RSA	Rivest-Shimar-Adleman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SEP	Secure Exchange Protocol
SHA-1	Secure Hash Algorithm
S-HTTP	Secure Hypertext Transfer Protocol
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

1.1.5 Approval by PMA

The CP is effective on the date set for its publication by the PMA, and on the date(s) set as it is amended from time to time by the PMA.

1.2 Policy Identification

This policy document is called the *Certification Policies* (CP).

The Object Identifier (OID), registered with the Canadian Open Systems Interconnection Registration Authority (COSIRA), for this CP is: 2.16.124.113588.100.

The policies under which Certificates are issued by eHealth Ontario have been assigned a unique Object Identifier (OID) subordinate to the CA Certificate Policy OID Arc, having a root of 2.16.124.113588.100.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-RudimCert	2.16.124.113588.100.1	ID ::= {id-cp1} [Not used]
id-BasicCert	2.16.124.113588.100.2	ID ::= {id-cp2} [Not used]
id-MediumCert	2.16.124.113588.100.3	ID ::= {id-cp3}
id-HighCert	2.16.124.113588.100.4	ID ::= {id-cp4}
id-person	2.16.124.113588.100.5	ID ::= {id-cp5}
id-application	2.16.124.113588.100.6	ID ::= {id-cp6}
id-organizational unit	2.16.124.113588.100.7	ID ::= {id-cp7}

id-RA	2.16.124.113588.100.8 ID ::= {id-cp8}
id-LRA	2.16.124.113588.100.9 ID ::= {id-cp9}

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 CP, the CA, all Participants and any parties with which the Agency has Cross Certification Agreements are subject to terms and conditions of the agreements identified in the *Concept of Operations,* [Section XII, Figure 6].

The form of the agreements is specified in the CPS.

Agreements are signed in writing or using Electronic Signatures as provided for in CPS

1.4 Certificate Applicability

Certificates issued under this CP are intended for use by those Registrants that are Participants in PKI where one or more of Registrant identification, authentication, authorization, confidentiality, integrity, non-repudiation or digital signature is desired.

The CA supports four (2) Levels of Assurance for the issuance of PKI Certificates levels corresponding to sensitivity levels defined in the draft Province of Ontario Corporate Security Information Classification Operating Procedures. The applicability of these levels is discussed in the *Concept of Operations,* [See: Section V, Levels of Assurance], and summarized in the following table.

Figure 7 Summary of Certificate Applicability

Medium: 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.	
Digital Signature	**Confidentiality**
This policy is suitable for the Integrity and Authentication of transactions that could result in serious adverse impact or loss.	This policy is suitable for transactions that if falsified or compromised could cause serious injury, loss of reputation, confidence or privacy.

High: information with a high sensitivity level, within eHealth Ontario and the health sector environment, and that is extremely sensitive and of the highest value.	
Digital Signature	**Confidentiality**
This policy is suitable for the Integrity and Authentication of transactions that could result in major adverse impact or loss	This policy is suitable for transactions that if falsified or compromised could cause significant injury, loss of reputation, confidence or privacy.

PKI Certificates may be issued to Individuals 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 Individuals are identified with OIDs identifying that they are issued to individuals registered at a specified Level of Assurance.

Organizational Unit Certificates can only be used for Confidentiality and Integrity purposes. An Organizational Unit certificate issued by the CA will not support Non-Repudiation of the End-User signing on behalf of the organizational unit. The person registered as responsible for the Organizational Unit acknowledges the obligation assigned to the Organizational Unit Certificate within the applicable registration agreement. A specific OID, is assigned to identify Certificates issued to Organizational Units.

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 PKI Policy Authority is:

The Secretary,
Policy Management Authority
Smart Systems for Health Agency,
415 Yonge Street, Suite 1900
Toronto, ON M5B 2E7
Tel: (416) 327-9741
Fax: (416) 327-9705

2.0 General Provisions

2.1 Obligations

2.1.1 Certification Authority Obligations

The CA is responsible for initiating, establishing and operating all systems required for the Registration, Services Enrolment and Authentication services provided by eHealth Ontario to Client Organizations, including the eHealth Ontario PKI, in conformance with the CP and CPS and applicable laws of Ontario and Canada.

Where necessary, this CP distinguishes the different users and roles accessing CA functions. Where this distinction is not required, the term Certification Authority refers to the total Certification Authority entity, including the software and its operations. The responsibilities of the CA include:

- Signing a Root Certificate for the PKI 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, LRA and EA officers.
- Generating Digital Signature Key Pairs, Confidentiality Key Pairs and Certificates for End Users in a manner that ensures trust and integrity.
- Providing End Users 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, LRA and EA that commits the RA, LRA and EA to the obligations in this CP.
- Ensure that CA Personnel, RAs, LRA, EAs and Registrants are aware of relevant policies and practices through the CP, CPS, RA/LRA/EA appointment form and Registrant Agreement.
- Taking all reasonable efforts, including training, to ensure that Participants 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.
- Renewing and replacing of Certificates (if 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.

2.1.1.1 CA Personnel Obligations

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

A recipient of a PKI Management Certificate is obliged, to:

- Maintain their cryptographic tokens in a secure manner according to established eHealth Ontario procedures for handling of such tokens.
- Ensure that Management Certificate 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 with 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 PMA.

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

2.1.2 Registration, Local Registration and Enrolment Authority Obligations

2.1.2.1 RA Obligations

RAs act as agents of the CA. RAs are responsible for carrying out the following duties in conformity with the CP, CPS and applicable laws of Ontario and Canada:

- Creating and delegating authority to Local Registration Authorities and Enrolment Authorities.
- Verifying the accuracy and authenticity of identification information submitted for LRAs and EAs.
- Ensuring that LRAs and EAs perform Registration Service Enrolment and Authentication duties in conformity with the CP, CPS and applicable laws of Ontario and Canada.
- Arranging security awareness and other training required for the performance of these duties.
- Revoking LRA and EA 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 PMA. [See: Section 2.7.]

2.1.2.2 LRA Obligations

LRAs are created and delegated authority by RAs. LRAs are responsible for carrying out the following duties in conformity with the CP, CPS and applicable laws of Ontario and Canada:

- 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 and accept the terms and conditions of Registrant Agreements
- 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 PMA. [See: Section 2.7.]

2.1.2.3 EA Obligations

EAs are created and delegated authority by RAs. EAs are responsible for carrying out the following duties in conformity with the CP, CPS and applicable laws of Ontario and Canada:

- Enrolling existing Registrants for new Services.
- Verifying at the time of the Enrolment, the continuing accuracy of information submitted by or for Registrants.
- Ensuring that Registrants are aware of their obligations and accept the terms and conditions associated with the new service for which they are being enrolled
- Arranging security awareness and other information and training required by Registrants.
- Performing other duties as may be reasonably consistent with the duties of an EA.

The EA 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 EA performs these duties on behalf of the CA as part of its delegated obligations from the RA.

EAs must be individually accountable for actions they perform and are subject to internal and external compliance audit processes as determined by the PMA. [See: Section 2.7.]

2.1.3 Registrant Obligations

Registrants may be Individuals, Organizational Units or Computer Applications. Registrants are required to enter into a binding Registrant Agreement with the CA that obligates the Registrant to the following:

- Submit any information required to be submitted to a CA, RA, LRA, or EA in connection with Registration and/or Enrolment in a complete and accurate manner.
- Provide appropriate consent to the collection, storage, use and disclosure of Registrant information.
- Generate Private Key Pairs using a trustworthy system or use a Key Pair generated in a secure hardware token by the CA.
- Take reasonable precaution to prevent any loss, disclosure, or unauthorized use of the Private Key.
- Use any Authentication Credential exclusively for eHealth Ontario authorized Services consistent with the CP, CPS and the relevant Acceptable Use Policy.
- Acknowledge receipt of security training appropriate to the functions for which an Authentication Credential is issued.
- Follow prescribed procedures to advise the CA to revoke an Authentication Credential upon any actual or suspected loss, inappropriate disclosure, or other compromise.

In addition to the above, registrants acting on behalf of an Organizational Unit or a Computer Application are obligated to:

- Install technical and administrative controls over the use of Authentication Credentials for the Organizational Unit or Computer Application to ensure that they are used exclusively for eHealth Ontario authorized Services consistent with the CP; CPS and the relevant 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
  - ensure that all users of the account have received security training appropriate to the function for which the Authentication Credential is issued.

2.1.4 Obligations of Registrants Relying on Certificates

Rights and obligations of Registrants relying on a Certificate issued to another Registrant are covered by this policy. A Registrant must not rely on a Certificate unless:

- The purpose for which the Certificate is used is authorized under the CP, CPS and relevant Acceptable Use Policy.
- The Certificate is used only in accordance with the Public Key Infrastructure X509 (PKIX) standard for Certificate validation.
- The Registrant confirmed the current status of the Certificate against the appropriate CRL in accordance with the requirements stated in Section 4.4.10. As part of this verification process the Digital Signature of the CRL must also be validated.
- The Level of Assurance and use of the Certificate is appropriate given the Registrant's risk analysis of the application.
- The reliance was reasonable and in good faith in light of all the circumstances known to the Registrant at the time of reliance.

The rights and obligations of a registrant belonging to an external PKI are addressed in the Cross Certification Agreement between eHealth Ontario and the external PKI.

2.1.5 CA Repository Obligations

The CA repository will operate in a continuous mode. Certificates, CRLs and ARLs must be available in accordance with the requirements of Section 4.4.9.

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 is in accordabce with the CP and CPS. It will also take reasonable efforts to ensure that all RAs, LRAs, EAs and Registrants follow the requirements of the CP and CPS when dealing with any Certificates containing this policy's OID or the associated keys.

The CA, RAs, LRAs and EAs will ensure that their Identification and Authentication procedures are implemented as required by Section 3.

2.2.2 Disclaimers of Warranties and Obligations

Except as expressly stated in the CP, CPS or any other agreement related to the PKI, CA disclaims all other warranties and obligations of any type. In particular, the CA may disclaim:

- Any warranties related to the accuracy, authenticity, reliability, completeness, currency, merchantability, or fitness of any information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of the CA;
- Any warranties related to the security provided by any cryptographic process implemented by the CA;
- Liability for representations of information contained in a certificate;
- Warranties of non-repudiation of any messages; and
- Liability for any software or applications.

The CA assumes no liability for use of Certificates issued by other CAs, or for use of CA Certificates outside of the CA domain.

2.2.3 Limitations of Liability

2.2.3.1 No Indirect Damages

Subject to **Section 2.2.3.4** (exclusions from limitation of liability), in no event shall any PKI Participant be liable for any indirect, special, incidental, consequential, or punitive damages, including, without limitation, for any loss of profits, loss of data, whether or not reasonably foreseeable, arising from, or in connection with, the use, delivery, license, performance or non-

performance of Certificates, digital signatures, or any Services offered, or contemplated, by this Certificate Policy or the Certificate Practice Statement, even if the party from whom damages are being sought has been advised of the possibility of such damages.

2.2.3.2 Aggregate Liability Amount varies by class of Certificate

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. Subject to **Section 2.2.3.4** (exclusions from limitation of liability), in respect of each Certificate, in no event will the Aggregate Liability Amount of any PKI Participant exceed the amount shown in the row of the second column of such table which corresponds to the applicable class of such Certificate.

Figure 8 Aggregate Liability Amounts

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

2.2.3.3 Further Conditions Applicable to the Aggregate Liability Amount

Subject to **Section 2.2.3.4** (exclusions from limitation of liability), for greater certainty, the Aggregate Liability Amount, in respect of each Certificate, applies to any claim made by any PKI Participant against any other PKI Participant in connection with the Services including, without limitation, whether the claim is based upon, or relates to:

(i) the reliance on, or use of, such Certificate;

(ii) how the CA issued, managed, used, suspended, or revoked, such Certificate;

(iii) the fact that such Certificate, upon which a Relying Party relied, had expired;

(iv) a contractual, tortious, or any other theory of liability; and

(v) a multiple number of digital signatures, or uses, associated with such Certificate, and its associated public/private key pair.

2.2.3.4 Exclusions from Limitations of Liability

This limitation of liability set out in **Sections 2.2.3 1 – 2.2.3..3** does not apply in respect of any claim (and, for greater certainty, including both cases that involve third party claims, and cases that do not involve third party claims) in which there is a judgement, or other final adjudication, adverse to the PKI Participant against whom a claim is made that establishes

that any acts or omissions of such PKI Participant that were material to the cause of action as adjudicated satisfies either of the two following conditions:

(i) were fraudulent, criminal, or wilful; or
(ii) were both:

(A) committed or omitted in bad faith; and

(B) unreasonable in the circumstances.

2.2.3.5 Apportionment of Damages Arising from Multiple Claims in connection with a Certificate.

If the amount of damages claimed in respect of a Certificate exceeds the relevant Aggregate Liability Amount for such Certificate, then the amount of damages available in respect of such Certificate shall be apportioned first to the earliest claims to achieve final resolution of any dispute, unless otherwise ordered by a court of competent jurisdiction. For greater certainty, but subject to **Section 2.2.3.4** (exclusions from limitation of liability), in no event shall any PKI Participant be obligated to pay more than the Aggregate Liability Amount in connection with such Certificate, regardless of the method by which any damages are apportioned among multiple claimants.

2.2.3.6 Apportionment of Liability Among PKI Participants in Cases with Third Party Claims

If both of the following conditions are satisfied:

(i) any PKI Participant is named as defendant in any action (a "**Third Party Action**") brought by a party (a "**Third Party**") that is not a PKI Participant:

(A) whether solely or jointly with one or more other PKI Participants; and

(B) whether any such PKI Participant is named as a defendant in the original statement of claim, or is subsequently named as a defendant by any process, including, without limitation, a cross-claim or other action; and

(ii) two or more of such PKI Participants (each a "**Responsible Defendant**") are held to be liable for some proportion of the damages (the "**Third Party Damages**") payable to such Third Party;

then:

(iii) such Third Party Damages shall be deemed to be direct damages suffered by each Responsible Defendant;

(iv) each such Responsible Defendant shall be liable to pay to such Third Party that proportion of the Third Party Damages (the "**Proportionate Damage Amount**") for which such Responsible Defendant is found to be liable;

(v) for greater certainty, such Proportionate Damage Amount shall not be included in any calculation of any Aggregate Liability Amount in respect of each Responsible Defendant;

(vi) for greater certainty, each Responsible Defendant shall be liable only for its own Proportionate Damage Amount, and shall not be liable to any other Responsible Defendant for the Proportionate Damage Amount owed by any such other Responsible Defendant (i.e. no joint and several liability as among the PKI Participants); and

(vii) to the extent that the Third Party recovers an amount of Third Party Damages from any Responsible Defendant (a "**Disproportionately Paying Responsible Defendant**") which is greater than the Proportionate Damage Amount for which any such Responsible Defendant is found to be liable, then each other Responsible Defendant shall indemnify such Disproportionately Paying Responsible Defendant so that, after all amounts have been paid pursuant to such indemnification, the amount of money paid by all Responsible Defendants in connection with such Third Party Action will be equal to each such Responsible Defendant's Proportionate Damage Amount.

2.3 Financial Responsibility

2.3.1 Indemnification

No Stipulation

2.3.2 Fiduciary Relationships

As agents of the CA, RAs have a fiduciary responsibility to the Agency.

2.3.3 Administrative Processes

No Stipulation

2.4 Interpretation and Enforcement

2.4.1 Governing Law

The laws of the Province of Ontario, and the Government of Canada, will govern the construction, validity, interpretation, enforceability and performance of the CP, CPS and all relevant agreements. Any dispute related to the CP, CPS, relevant agreement, any Certificate issued by the CA or any Services provided by CA will be brought in the courts of the Province of Ontario and each person, entity, or organization hereby agrees that such courts will have personal and exclusive jurisdiction over such disputes.

2.4.2 Severability, Survival, Merger, Notice

Each provision of the CP, CPS and any relevant agreement will be interpreted in such manner as to be effective and valid under applicable law. All agreements will contain appropriate provisions governing severability, survival, merger or notice.

2.4.3 Dispute Resolution Procedures

Within the PKI domain, any dispute that is related to PKI Services, between Registrants, or between Registrants and the PKI CA or any other Participant, will be resolved using the following process before going to court.

- **Level 1 – Resolution by the Chief Technology Officer**. Disputes will be initially reported to the Chief Technology Officer who will make reasonable efforts to settle the dispute. A dispute not settled by the Chief Technology Officer will be referred to the PMA for resolution.

- **Level 2 – Resolution by the PMA** The PMA will make reasonable efforts to settle the dispute.

- **Level 3 – Resolution by the CEO** A dispute not settled by the PMA will be referred to the CEO for resolution.

Any resolution of a dispute by the Chief Executive Officer shall be final.

2.4.4 Force Majeure

Under this Policy, the CA may, in the Certificate, in an applicable contract, or in its CPS, disclaim its liability for any losses, costs, expenses, liabilities, damages, or claims, or any or settlement amounts arising out of or related to delays in performance or from failure to perform due to any causes beyond its reasonable control.

2.4.5 Conflict of Provisions

In the event of a conflict between provisions, the following order of precedence is to be followed:

- Regulation 43/02 under the *Development Corporations Act.*
- The Certification Policy.
- The Certification Practice Statement.
- Agreement(s) signed between eHealth Ontario and any Participant.
- The Concept of Operations.

2.4.6 Waiver

The failure of an PKI CA to enforce at any time any of the provisions of this CP, CPS, and related agreements or the failure to require at any time performance by any other party of any of the provisions of this CP, CPS, and related agreements will in no way be construed to be a present or future waiver of such provisions, nor in any way affect the ability of CA to enforce each and every such provision thereafter. The express waiver by CA of any provision, condition, or requirement of this CP, CPS, and related agreements will not constitute a waiver of any future obligation to comply with such provision, condition, or requirement.

2.4.7 Limitation Period of Actions

Any legal actions involving a dispute which is related to an PKI Certificate or any services provided involving an PKI Certificate will be commenced prior to the end of one (1) year after; the expiration or revocation of the PKI Certificate in dispute, or the date of provision of the disputed Service or Services involving the PKI Certificate, whichever is sooner. If any action involving a dispute related to a PKI Certificate or any Service involving a PKI Certificate is not commenced prior to such time, any such action will be barred.

2.5 Fees

No stipulation.

2.6 Publication and Repositories

The PKI CA will operate a Repository in which Certificates issued to End Users as well as Certificate Revocation Lists and Authority Revocation Lists are stored. The CA will establish adequate access controls for 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.

2.6.1 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 a 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 past and current versions of the CA's CPS or a summary of key provisions when necessary for the purposes of any audit, inspection, accreditation or cross-certification;
- Provide the CA's Certificate for its signature Key in an online Repository; and
- Publish a Certificate Revocation List (CRL).

2.6.2 Frequency of Publication

The CA shall publish its CP and related documents within 14 days following the approval from the Policy Management Authority. Where a CPS contains information relevant to the security of a CA, all or part of the CPS need not be made publicly available. Certificates issued by the CA must be published within 72 hours of the Registrant's acceptance of the certificate. Information relating to the revocation of a Certificate must be published in accordance with Section 4.4.4.

2.6.3 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 discretion, subject to agreement between the CA, Registrants and Sponsoring Organizations. The CA will disclose provisions for such access controls in its CPS or other related document.

2.6.4 Repository Access Protocol

The protocol for accessing the CA Repository is specified in the CPS.

2.7 Compliance Audit

Prior to the initial approval as a Certification Authority, the Certification Authority will be audited in conformity with industry standards to provide attestation of compliance with this CP. The auditing of the root key generation ceremony will be considered the initial audit for the purposes of this CP.

This audit policy will apply to any CA with which the CA enters into a Cross Certification agreement.

2.7.1 Frequency of Compliance Audit

The eHealth Ontario Privacy and Security Office will conduct an annual independent internal audit to demonstrate continuing compliance with this policy.

The Board of Directors will determine the frequency (not to exceed 3 years) of external audits to demonstrate continuing compliance with policy.

2.7.2 Identification/Qualifications of Auditor

The auditor who performs the Audit will be approved by the eHealth Ontario Board of Directors, or a delegated authority, and will be a licensed chartered accountant or will hold the Certified Information Systems Auditor (CISA), Certified Information Systems Security Practitioner (CISSP) designations or other designation approved by the PMA and will have experience in the application of public key cryptographic technologies and general computer security.

2.7.3 Auditor's Relationship to Audited Party

The auditor must have no relationship to the CA, any RA, LRA or EA, or any other service providers to the CA that would impair its independence and objectivity of the audit under generally accepted auditing standards.

2.7.4 Topics Covered by Audit

The purpose of such audit will be to verify that the eHealth Ontario CA has in place a system to ensure the quality of the CA services and that the CA complies with the requirements of this policy and its CPS. The audit requirements will extend to selected RAs, 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 eHealth Ontario Board of Directors. 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, LRAs and EAs implement and comply with the technical, procedural, and personnel practices and policies delegated to them.

2.7.5 Actions Taken as a Result of Deficiency

The Chief Privacy and Security Officer will notify the PMA 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 Chief Executive Office will report on the outcome of internal and external audits, including measures taken to remedy any discrepancies, to the Board of Directors.

Failure to comply with this policy or failure to implement remedial measures determined appropriate by the PMA may result in the suspension or revocation of Certificates issued to RAs, LRAs and EAs.

2.7.6 Communication of Results

The results of compliance audits are considered particularly sensitive information and are not generally communicated outside eHealth Ontario unless required by law.

In accordance with any Cross-Certification Agreements, the CA and any CA cross-certified with the CA must provide a copy of the results of the compliance inspection as part of the cross-certification process. These results will not be made public unless required by law.

The CA, with input from the auditor, will determine if Registrants need to be informed of any deficiency and the action taken to remedy it.

2.8 Confidentiality Policy

2.8.1 Types of Information to Be Kept Confidential

All information that is not considered by the CA to be public domain information is to be kept Confidential and may not be disclosed except as required by law.

Information regarding Registrants that is submitted on applications for Certificates but which is not included in the Certificate must be kept Confidential by the CA and must be used only

for the purpose for which it was collected. Such information must not be released without prior written consent of the Registrant, unless otherwise required by law.

Any disclosure of information is subject to the requirements of the Freedom of Information and Protection of Privacy Act (FOIPPA), or other relevant provincial or federal legislation.

2.8.2 Types of Information Not Considered Confidential

Certificates and CRLs, and personal or corporate information appearing on them and in public Directories, are not considered sensitive, however non-PKI information stored in Directory entries may be sensitive. The Certificate and CRL information will be made available to the Participants for PKI availability and validation purposes. Any public Directory will limit access to only non-sensitive information.

2.8.3 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 and delivered to the eHealth Ontario Chief Technology Officer.

Inspection information related to the revocation or suspension of a Certificate is to be considered sensitive and must not be disclosed to anyone for any purpose other than inspection purposes or where required by law.

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 PMA 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 an Application or an Organizational Unit, the application owner or the manager responsible for the Organizational Unit, 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 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 law.

2.8.4 Release to Law Enforcement Officials

Release of information to law enforcement officials will be governed by FOIPPA or other provincial or federal legislation.

2.8.5 Release as Part of Civil Discovery

The CA will comply with properly executed legal requirements to release information as part of civil discovery, consistent with the eHealth Ontario corporate policy.

2.8.6 Disclosure Upon Owners Request

No stipulation

2.8.7 Other Information Release Circumstances

No stipulation

2.9 Intellectual Property Rights

No stipulation.

3.0 Identification and Authentication

3.1 Initial Registration

Individuals and two types of institutional entities, Organizational Units and Computer Applications are eligible to be registered by the CA and enrolled for specific services.

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

- From the Registrant to an RA, LRA or EA and authorizations to issue PKI Certificates may be communicated from an authorized RA, LRA or EA to the CA via the Registration Management System.
- Through an alternative registration process (e.g. a bulk load) that has been approved by the PMA as part of a Service Implementation Plan (See: Concept of Operations, Section IV).

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 Individuals. They are defined in the CPS.

Figure 9 Registrant Information Requirements for Individuals

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 Licences/Certificates	
Registration Identification Number	

3.2.1.2 Organizational Units

The information required to register an Organizational Unit are listed in the following table and defined in the CPS.

Figure 10 Registrant Information Requirements for Organizational Units

INFORMATION REQUIREMENTS	
Primary Identity Information	**Service Related Information**
Unit Name	Organization Corporate/Business Name
Unit Contact Person	Organizational Representative
Contact Information	Organization Registration Identification Number
Registration Identification Number	

3.2.1.3 Computer Applications

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

Figure 11 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 Individuals 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.

Organizational Unit 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, Computer Application or Organizational Unit to which the Certificate was issued. This identifier in the case of Individuals will directly correspond to the subject's legal name. For

Organizational Units and Computer Applications a corresponding "identifiable name" is required. The designated owner of the Computer Application or Organizational Unit certificate's legal name 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 in its CPS.

3.2.5 Uniqueness of Names

All Certificates issued by the CA will include an identifier that represents the Individual, Organizational Unit 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

Prior to the issuance of a Certificate, the CA requires proof of possession of a Private Key before creating and signing a Certificate containing the associated Public Key through the use of activation codes.

For the corresponding Level of Assurance, the minimum requirements for delivering activation codes and protecting the codes in the delivery of a Certificate are as follows:

Figure 12 Minimum Requirements for Delivering Activation Codes

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

Medium		High	
Digital Signature	Confidentiality	Digital Signature	Confidentiality
Via 2 separate secure means. The specific means for delivery and protection is defined in the CPS.		In person delivery of Authorization Code as defined in the CPS. Other means of delivery of Reference Code as defined in the CPS.	

3.2.9 Identification and Authentication of An Organization

3.2.9.1 Sponsoring Organizations

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

Except as provided for Organizational Units, PKI Certificates and Confidentiality and Digital Signature Key Pairs are not issued to Sponsoring Organizations .

Applications for the registration of a Sponsoring Organizations must be made by an individual authorized to act on behalf of the organization.

The information required to register a Sponsoring Organization is identified in the following table and defined in the CPS.

Figure 13 Sponsoring 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	

3.2.9.2 Cross Certified Organizations

The CA can issue Cross Certificates to the external Certificate Authorities. To cross-certify the CA will assure itself, by seeking policy guidance from the PMA, that the requesting organization has a valid reason to cross certify with the CA.

As there will be an existing agreement between the CA and the organization to be cross-certified, additional authentication of the identity of the organization may not be required.

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 or as the designated contact for an Organizational Unit or 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, LRA or EA. The RA, LRA or EA must verify the identity of the Registrant. The RA, LRA or EA must 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 LRA according to the relevant Levels of Assurance:

Figure 14 Minimum Requirements for Identification and Authentication of Individual Registrants

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

Medium		High	
Digital Signature	**Confidentiality**	**Digital Signature**	**Confidentiality**
Authentication of identity by sponsor or RA/LRA. Must provide 2 pieces of ID (**notarized copies or originals**) 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 15 Minimum Requirements for Storage of Authentication Credentials

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

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

3.2.10.2 Identification and Authentication of Organizational Units

Organizational Units may be registered by a Sponsoring Organization that is the owner of the Organizational Unit. The Registration must be requested by a person with authority to act on behalf of the Sponsoring Organization and indicate the Contact Person for the Organizational Unit. The Contact Person must be registered independently as an Individual.

As there will be an existing agreement between the CA and the Sponsoring Organization, additional Authentication of the identity of the Organizational Unit may not be required.

3.2.10.3 Identification and Authentication of Computer Applications

Computer Applications may be registered by a Sponsoring 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 Sponsoring Organization and indicate the Contact Person for the Computer Application. The Contact Person must be registered independently as an Individual.

As there will be an existing agreement between the CA and the Sponsoring 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 whose 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; Section 4.4]

RAs/LRAs/EAs will adhere to the procedures identified in the applicable CPS for authentication of revocation requests.

4.0 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 the CPS or a publicly available document.

The Sponsor will initiate the Certificate application process by identifying to the appropriate RA, LRA or EA the names of the Registrants. Sponsoring 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 Sponsoring Organization.

Acceptance the applicable terms and conditions governing the use of the Certificate is not mandatory at the time of application. However, acceptance of the applicable terms and conditions governing use of the Certificate is mandatory prior to valid use of the Certificates. Individuals that use Certificates without documented acceptance of the terms conditions of use, do so without the benefit of any warranty described or implied in this policy.

An application for a Certificate does not oblige CA to issue a Certificate. Any dispute concerning the refusal by the CA to issue a Certificate is subject to the Dispute Resolution Procedures. [See: Section 2.4.3].

4.1.2 Application for a Cross Certificate

The PMA will identify all procedures and requirements with respect to an application for a Cross Certificate for a CA external to eHealth Ontario in its Cross Certification procedures. A CA requesting Cross Certification through the PMA must ensure that each application is accompanied by:

- Its Certificate Policy.
- An external audit inspection report validating the Level of Assurance stated in the CP.
- The public verification key generated by the CA.

An application for a Cross Certificate does not oblige the PMA to issue a Cross 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.

The End User 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 EA shall 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.

Any Cross Certificate issued by the CA to an external CA will be revoked when the Certificate is no longer trusted or if the relationship is no longer required. Some specific reasons include:

- Compromise or suspected compromise of Private Keys.
- Corporate mergers or takeovers.
- Failure of the cross-certified CA to meet the obligations as stated in the Cross Certification agreement.
- Changes in the business relationship between the CA and the external CA.

4.4.1.1 Permissive Revocation

A RA, LRA, EA, Registrant, 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 Sponsoring Organization.

An CA will revoke a Certificate in accordance with Section 4.4.3:

- Upon request of the RA, LRA, EA, Registrant 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, LRA or EA determines that the Registration was not properly made in accordance with the CP or CPS.
- If the CA, RA, LRA, or EA determines that the Certificate was not properly issued or used in accordance with the CP or CPS.

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 (on behalf of himself/herself, an organization unit, or an application).
- Sponsor.
- CA.
- RA, LRA or EA.
- 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 Section 4.4.9.

The revocation of a cross-certificate can only be requested by:

- The PMA.
- The CA on whose behalf the cross-certificate was issued.

4.4.3 Procedure for Revocation Request

Requests to revoke a Certificate may be received by the means detailed in the CPS.

A revocation request may be generated electronically. An RA, LRA, EA, 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 Policy, or any other event necessitating revocation as outlined in the CPS. 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 Certificate Revocation List (CRL) or Authority Revocation List (ARL) as appropriate.

4.4.4 Time to Process Revocation Request and Certificate Revocation List Frequency

The CA will publish updated Certificate Revocation Lists (CRL) every four (4) hours or upon revocation of an End User Certificate.

4.4.5 Circumstances for Suspension

Individual, Organizational Unit 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 (on behalf of himself/herself, an organization unit, or an application).

- Sponsor.
- CA.
- RA, LRA or EA.
- Service Owner.

4.4.7 Procedure For Suspension Request

Requests to suspend a Certificate may be received by the means detailed in the CPS.

A suspension request may be generated electronically. An RA, LRA, EA, 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 outlined in the CPS. 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 suspension of a Cross Certificate can only be requested by:

- The PMA.
- The CA on whose behalf the Cross Certificate was issued.

Where a Cross Certificate is suspended the suspension will be published in the Authority Revocation List (ARL) of the CA.

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

4.4.8 Limits on Suspension Period

No stipulation.

4.4.9 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.

4.4.10 Certificate Revocation List Checking Requirements

CA 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.

4.4.11 On-line Revocation/Status Checking Availability

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

4.4.12 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 Registration Authority or Local Registration Authority for Key recovery.

CA, RA and LRA compromises are investigated immediately

4.4.13 Other Forms of Revocation Advertisements Available

No stipulation.

4.4.14 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.4.15 Special Requirements Re: Key Compromise

No stipulation

4.5 Security Audit Procedures

4.5.1 Types of Event Recorded

All significant events, as defined in the CPS, 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 in accordance with the procedures specified in the CPS:

- For a high Level of Assurance on a daily basis.
- For a medium Level of Assurance, at least once every week.

- For a basic Level of Assurance, at least once every two weeks.

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 in the CPS.

4.5.4 Protection of Audit Logs

Access to audit logs will be protected by a combination of physical and procedural security controls specified in the CPS.

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 in accordance with the procedures specified in the CPS.

Retrieval of the backup audit logs will require multi-person control by Security Officers to be present.

4.5.6 Audit Collection System

The audit collection system is identified in the CPS.

4.5.7 Notification Following a Critical Event

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

All errors will be recorded and reported to the CA as specified in the CPS.

4.5.8 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 in accordance with the procedures specified in the CPS.

Discrepancy and compromise reports, Cross Certification agreements, 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 specified in the CPS.

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 FIOPPA and other relevant legislation, only individuals authorized in accordance with the procedures established in the CPS 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 back up will be made and sent to a secure off-site storage facility in accordance with the procedures specified in the CPS.

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 according to the procedures specified in the CPS.

Archived records will be transferred to separate physical media external to the CA host system as outlined in the CPS.

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 in the CPS. 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

In accordance with the compromise procedures as outlined in the CPS, the CA will assess the severity of any compromise to determine operational viability. The PMA with the advice of the CA will determine the corrective measures as set out in the CPS or otherwise deemed to be appropriate.

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

4.9 Certificate Authority Termination

No stipulation.

5.0 Physical, Procedural and Personnel Security Controls

This section outlines the physical, procedural, and personnel security controls required of the CA, RAs, LRAs and EAs to protect their operations.

5.1 Physical Security Controls

Physical security controls will be implemented to control access to the CA hardware and software. 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 limited to those personnel performing one of the roles described in this Policy. The secure space will be monitored in accordance with procedures outlined in the CPS.

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

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

RAs, LRAs and EAs 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; LRA or EA.
- RAs, LRAs and EAs 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, LRAs and EAs computers that contains 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. Specific roles will be defined in the CPS.

Multi-person (m of n) control requires that at least m persons out of a total pool of n persons explicitly enable access to the CA private key. The designated personnel must identify themselves to the system that will perform the operations. This mechanism prevents any single party from gaining access to the CA, along with all actual m of n access control records, will be maintained and made available for audit.

For the PKI, m will be at least three (3) and n will be at least five (5).

Access control records of m of n will be maintained and audited periodically. Maintenance and service personnel will be escorted and supervised according to procedures outlined in the CA's CPS.

5.2.1 Trusted PKI Roles

Management personnel responsible for the CA will have limited capabilities commensurate with the role of the account holder. M of N of Management personnel are required to perform the following tasks:

- Creating subordinate certificates;
- Setting certificate lifetimes;
- Creation of accounts for security officers and administrators;
- CA master key updates;
- Recovery of security officer accounts; and
- Other tasks as required.

5.2.2 Multiple Roles (Number of Persons Required per Task)

To ensure that one person acting alone cannot circumvent safeguards, responsibilities at eHealth Ontario 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.

5.2.3 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 CA, RA, LRA and EA personnel will:

- Be appointed in writing by the Operational Authority;
- 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 *Enterprise Security Policy*. The RA, LRA and EA personnel must meet reliability requirements defined in the CP and contained in the RA, LRA and EA agreements.

Any other person required for on-site support will be escorted by Security Officers as stated in the CPS.

6.0 Technical Security Controls

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 140-1 Level 3.

CA Keys will be generated and stored in hardware cryptographic modules using a PMA approved algorithm as specified in the CPS.

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 PMA as specified in the CPS.

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 PMA as specified in the CPS.

6.1.5 Key Sizes

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

6.1.6 Public Key Parameters Generation

The CA will generate Public Key parameters in accordance with Federal Information Processing Standard (FIPS) 186.

6.1.7 Parameter Quality Checking

No stipulation

6.1.8 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 PMA.

6.1.9 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 140-1 Level 3.

6.2.2 Private Key Multi Person Control

The simultaneous intervention of m of n persons is required for operations on the CA's private signing key, as defined in Sections 5.1 and 5.2 of the CP.

6.2.3 Private Key Escrow

CA Private Keys and End User Confidentiality Private Keys will be backed-up as provided for in the CPS. End User Private Digital Signature Keys will never be backed-up.

End User Confidentiality Private Key recovery may be requested:

- By the End User.
- By the Sponsoring Organization to recover encrypted data for a person entitled to see the data when the End User is unavailable or unwilling to do so.

6.2.4 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 Section 4.6 of this CP and as further specified in the CPS.

6.2.5 Private Key Archival

Private Digital Signature Keys will not be archived.

6.2.6 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 6.2.4.

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 PMA as specified in the CPS.

6.2.7 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).

6.2.8 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.

6.2.9 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. Private Key destruction procedures are described in the CPS.

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

The CA's Private Digital Signature Key used to create Certificates will be valid for no more than twenty (20) years. The Certificate issued for the Certificate Authority's Public Signature Key will be valid for the period required for retention in archive, in accordance with the procedures in the CPS.

End-User Private Digital Signature Keys will be valid for up to two (2) years. CA personnel's Certificates issued for the Public Digital Signature Key will be valid for no more than the period required for retention in archive, in accordance with the procedures in the CPS.

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 CA 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.

6.6.3 Life Cycle Security Rating

No stipulation

6.7 Network Security Controls

All CA applications and Repositories will be protected through use of appropriate networking technologies and devices configured to allow only the protocols and commands required for CA services. Only required services will be turned on.

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 140-1 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 140-1 Level 2 or otherwise verified to an equivalent level of functionality.

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

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

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

7.0 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 CP.

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 Policy is set forth in *Appendix B – CRL Profile* of this CP.

8.0 Policy Administration

The PMA 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 PMA 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 users.

End Users will be provided with notification of significant changes to this CP resulting in a new CP version number. If the PMA 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 PMA will review comments and make further changes as appropriate. If the PMA 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

A copy of this CP is available in electronic format from eHealth Ontario at www.ehealthontario.on.ca.

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 CA 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 PMA has approved this CP on 2005 January 25 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:

X.509 v3 Certificate Attributes/ Extensions	Critical/Non Critical	Optional	Notes
Attributes			
Version			• V3
SerialNumber			• integer
Signature			• sha-1WithRSAEncryption – {1.2.840.113549.1.1.5}
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-1WithRSAEncryption – {1.2.840.113549.1.1.5} • RSA public key is 2048 bit public key
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 20 byte hash of the subjectPublicKeyInfo in the CA certificate
SubjectKeyIdentifier	Non critical	Not optional	• contains a 20 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-1WithRSAEncryption – {1.2.840.113549.1.1.5}
Issuer			• cn=SSHA CA, o=SSHA Corp, c= CA •
Validity			• 2 years • notBefore and notAfter are specified
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-1WithRSAEncryption – {1.2.840.113549.1.1.5} • RSA public key is 1024 bit public key
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 20 byte hash of the subjectPublicKeyInfo in the CA certificate
SubjectKeyIdentifier	Non critical	Not optional	• contains a 20 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-1WithRSAEncryption – {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 20 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