PKI Massification in Canada and Digital Certification

Graham Stubbs

Corporate Security Branch
Ontario Government

May 06, 2009

Ontario

- **Geography of Ontario - It's a Big Place**

- **Size**
  - Ontario is Canada's second largest province, covering more than one million square kilometres (415,000 square miles) - an area larger than France and Spain combined.

- **Water**
  - Ontario's quarter million lakes and countless rivers and streams hold about one-third of the world's fresh water.

- **Natural Resources - Minerals and Mining**
-
  - Ontario has been one of the world's leading mineral producers for more than a century.
  - Today, Ontario is one of the world's leading mineral producers of gold, copper, zinc, platinum, palladium, cobalt and silver.
  - Ontario ranks as the world's second largest producer of nickel.
  - It produces more than 30 different metal and no-metal mineral products. including salt, gypsum, lime, nepheline syenite, calcium carbonate and structural materials (sand, gravel, stone).
  - The sedimentary rocks of the south are also the site of Ontario's oil and gas industry.
  - Ontario is Canada's leading petroleum-refining region. Five refineries produce 27 million cubic metres (170 million barrels) of oil a year, which is enough to meet local needs with some left over for export.

Ontario

Ontario

- **Population**
  - With a population of more than **12 million people**, eighty per cent live in urban centres, largely in cities on the shores of the Great Lakes.
  - The largest concentration of people and cities is in the "Golden Horseshoe" along the western end of Lake Ontario including the Greater Toronto Area, Hamilton, St. Catharines and Niagara Falls. About five million people live in the "Golden Horseshoe."
  - **Greater Toronto Area (GTA) – Population Approx 5.5 Million**
    - The Greater Toronto Area is one of North America's fastest-growing urban areas. As an economic area, the GTA consists of the City of Toronto and four regional municipalities in a total area of 7,125 km2 (2,751 sq mi). This covers an area roughly equivalent to the surface area Lake Simcoe, on its northern reaches. Vast parts of the GTA remain farmland and forests, including protected sections of the Oak Ridges Moraine, Rouge Park and the Niagara Escarpment.
    - The work force is made up of approximately 2.9 million people, more than 100,000 companies, and a CA$ 109 billion gross domestic product. If it were a country, the GTA's GDP would rank approximately 16th in the world. The GTA is Canada's business and manufacturing capital by a large margin. The GTA is home to a number of post-secondary educational institutions, including 4 universities and 7 colleges, most with multiple campuses.

Background

Office of the Corporate Chief Information Officer (OCCIO)

- The Office of the Corporate Chief Information Officer (OCCIO) is responsible for providing corporate leadership for Information and Information Technology (I&IT) for the provincial government.
- Eight I&IT Clusters help ensure that I&IT is aligned with the Government's business directions.
- The I&IT organization of the Ontario Government has the responsibility to ensure that information and information technology is managed effectively to be adaptable to change, cost-effective, service-oriented and ultimately result in better public services.

Background

Office of the Corporate Chief InformationOfficer (OCCIO)

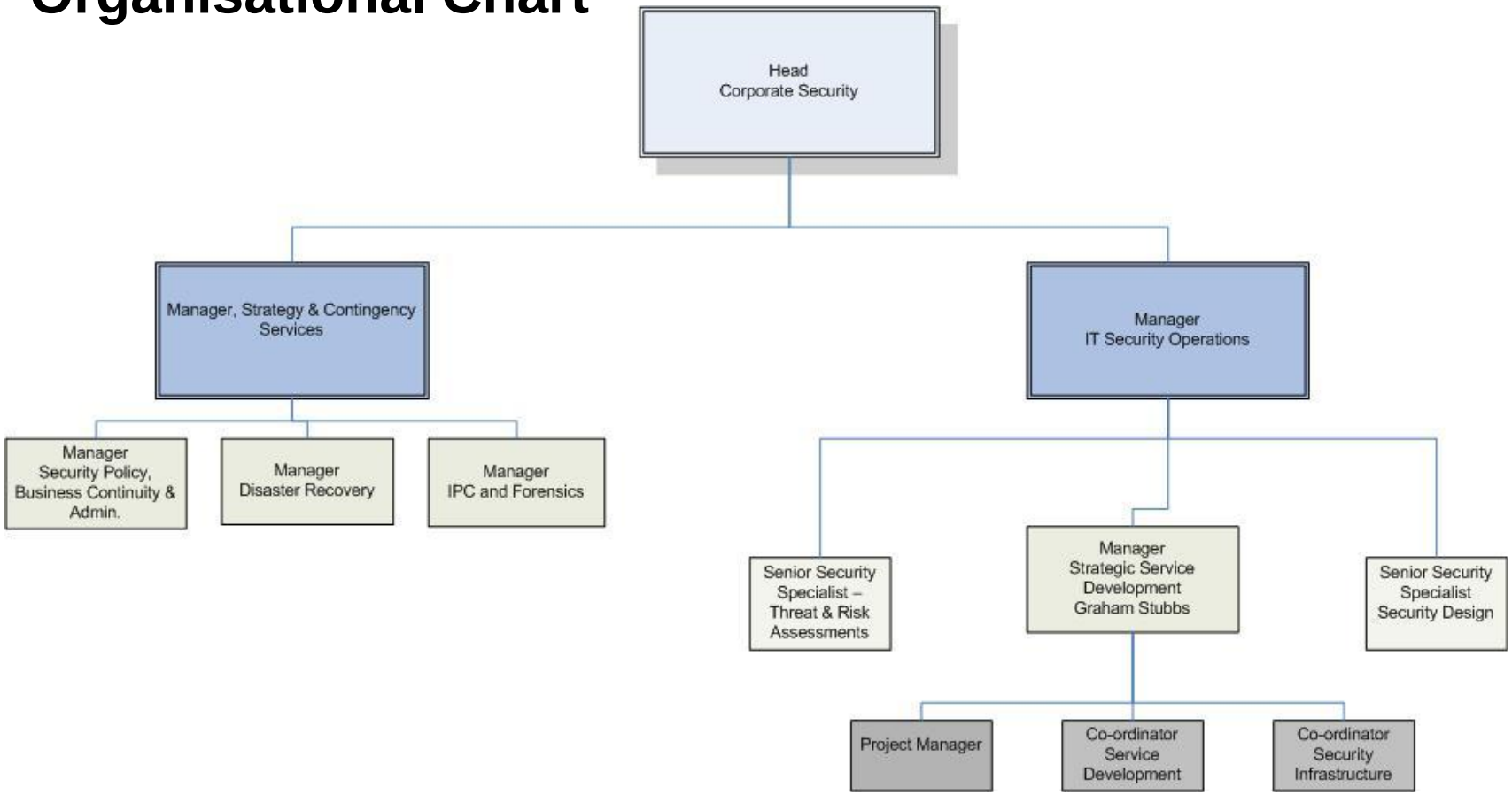
- **Vision**

  An Ontario where people, Information and technology drive innovation and excellence in public service.

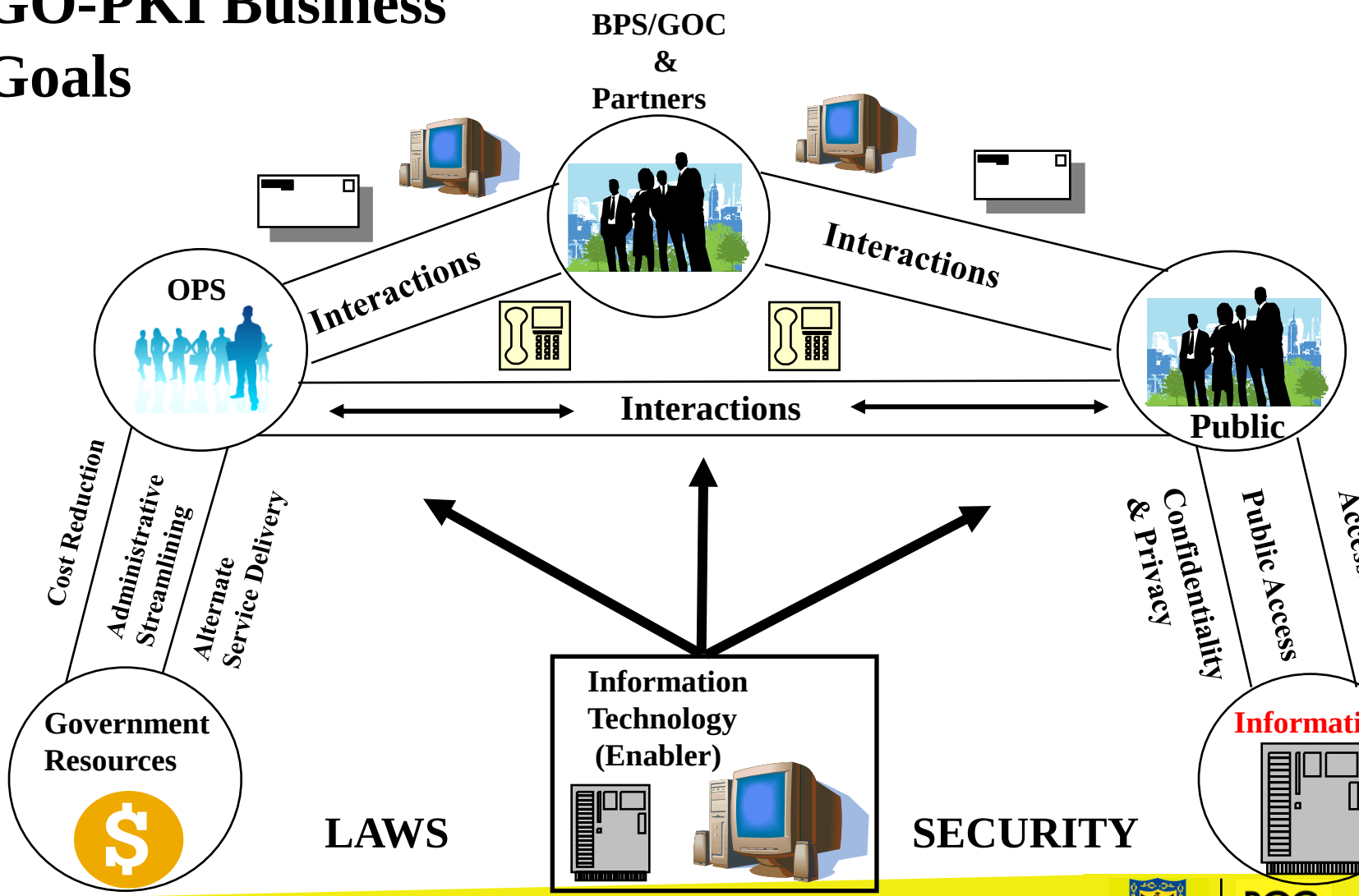
- **Mission**
  - Manage the government's investment in I&IT to optimize value.
  - Provide strategic advise and leadership on the effective use of I&IT.
  - Ensure the security and integrity of all systems and networks, and the protection of privacy.
  - Support business continuity, and effect business transformation.
  - Be socially responsible stewards of the public trust and encourage transparency in all dealings.
  - Provide business solutions that deliver results.

Corporate Security Branch

Organisational Chart



GO-PKI Business Goals



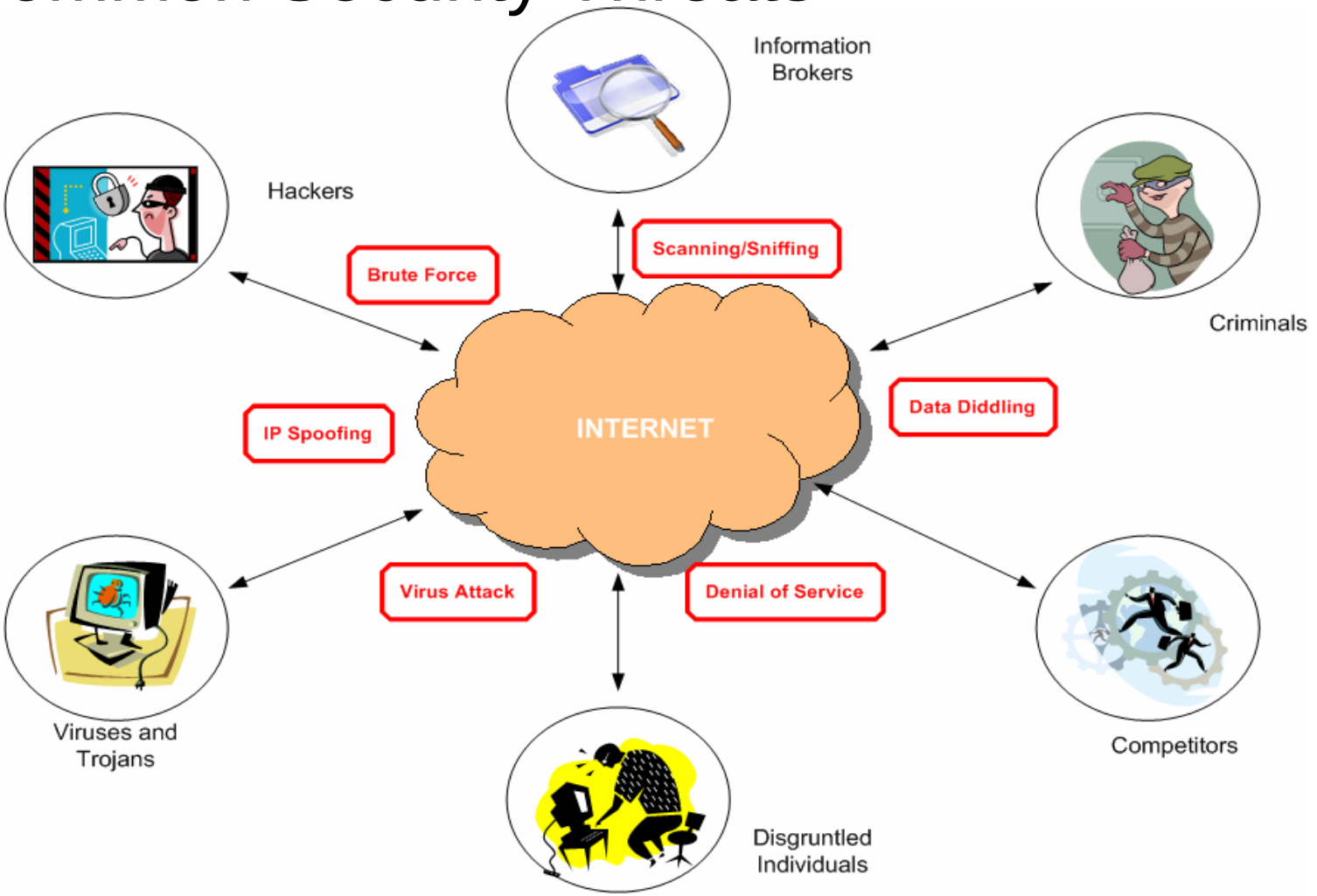
Initial GO-PKI Business Drivers

- Ministry of Health Primary Care Pilot
- Secure Internet Access
- Ontario energy Board Electronic Regulatory File System
- Lobbyist Registration Registration System
- Secure Internet e-mail and Remote Access
- Electronic Commerce
- Corporate Internet/Intranet

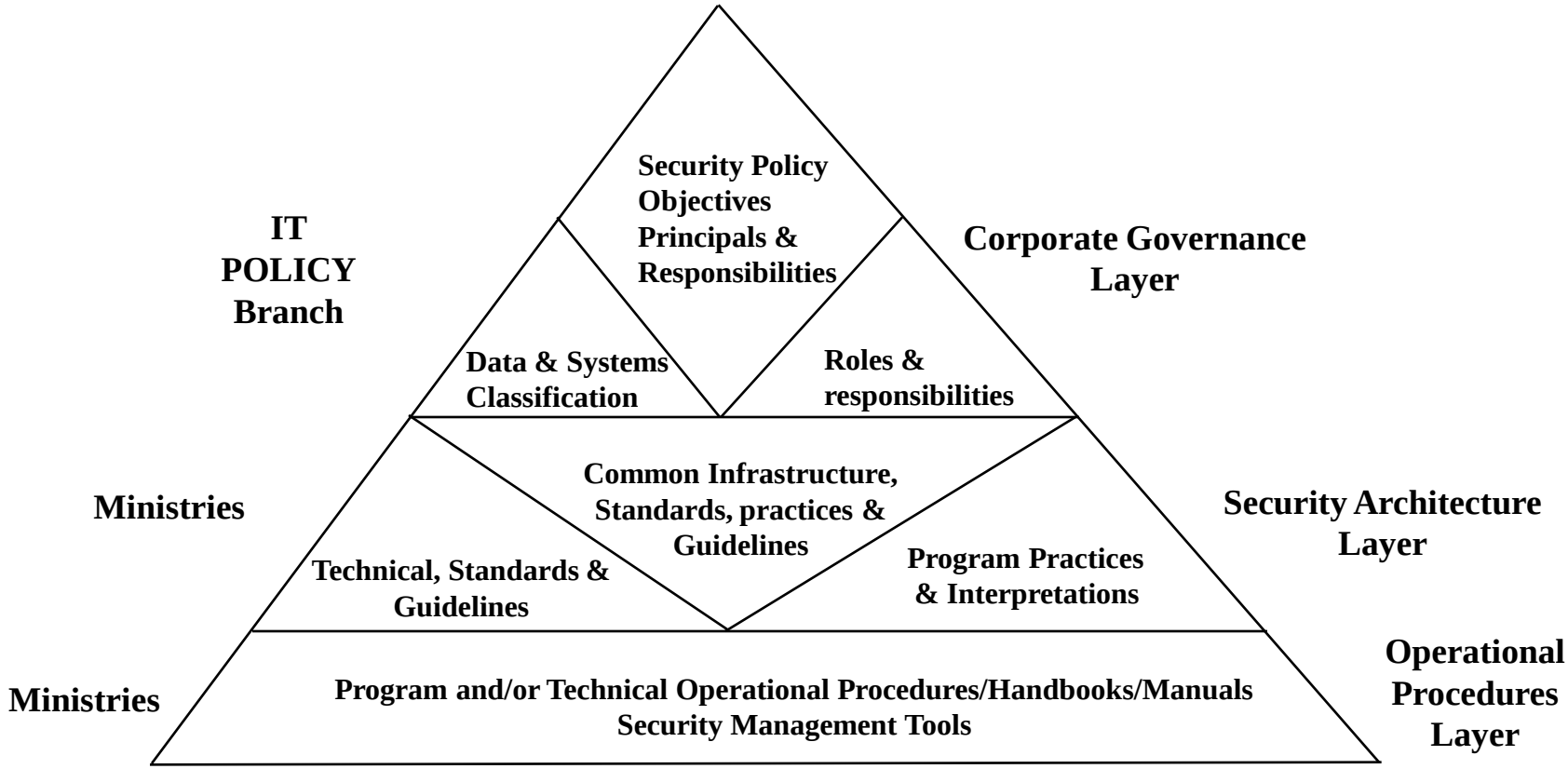
PKI Benefits

- Preserve Government Accountability & Credibility
- Protect Confidentiality & Privacy of Personal Information under Government care
- Promote Secure electronic Commerce & Global Information Exchange over the Internet
- Provide Secure single Window Approach to Government Service Delivery to the Public.
- Common Policy and Interface Standards
- Easier Cross-Certification (Interoperability & Common Policy) with External Organizations & Other Governments and Partners

Common Security Threats



Security Strategy Model



Why Use PKI ?

Why Use PKI ?

"On the Internet, nobody knows you're a dog."

PKI

What is PKI ?

PKI Concepts

PKI stands for Public Key Infrastructure. It consists of policies, processes, procedures, and technology. By providing a set of Public and Private Keys it allows users to encrypt and digitally sign documents and conduct secure transactions over open networks such as the Internet.

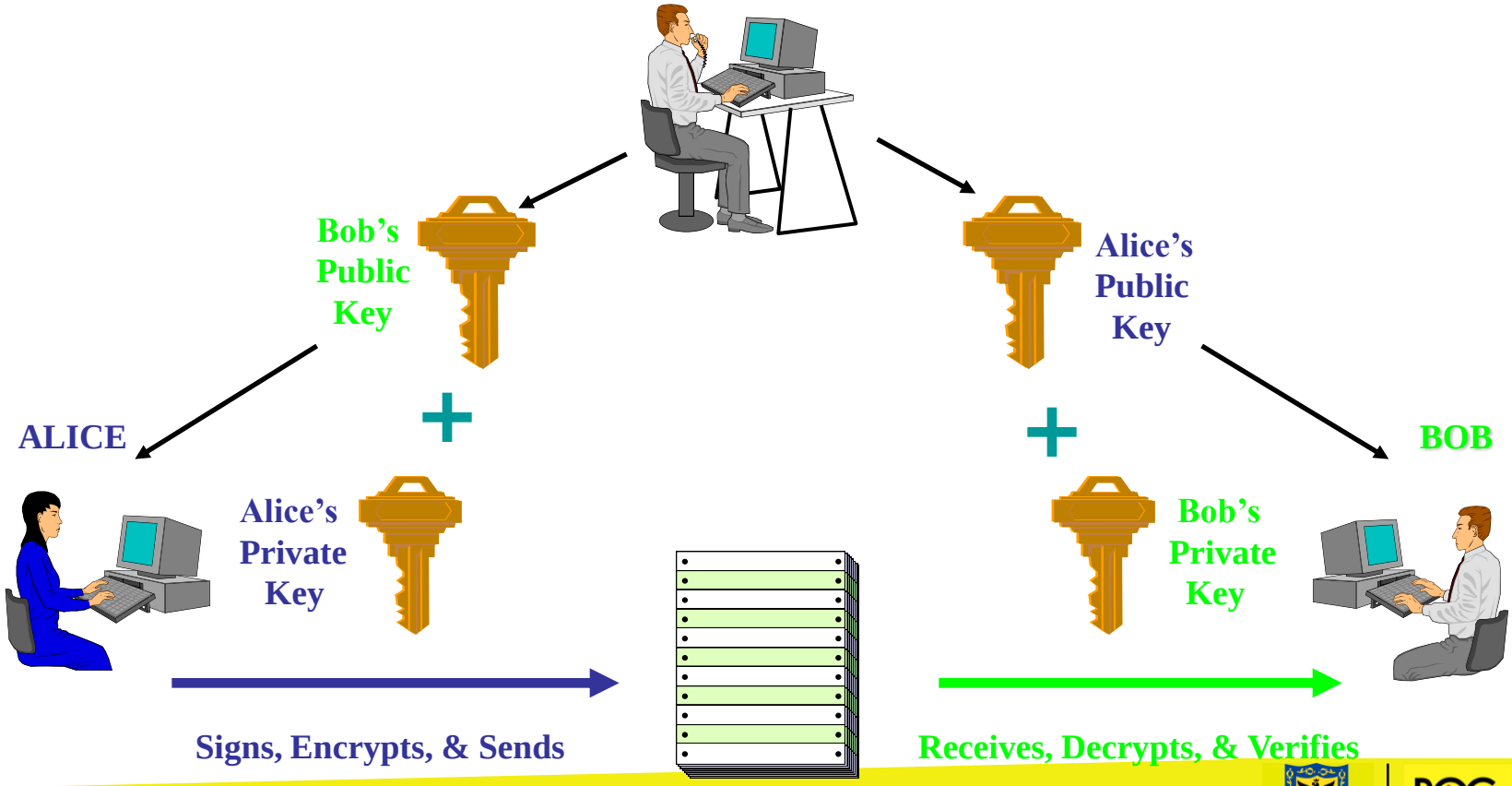
PKI provides a complete end to end solution to solve the following security issues.

Issue	Solution Mechanism
Confidentiality	Encryption
Access control	Encryption
Integrity	Digital signature
Authentication	Digital signature
Non- repudiation	Digital signature

PKI Concepts

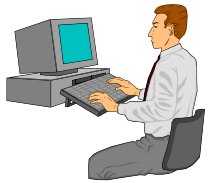
Authentication/Digital Signatures/Encryption/Non-Repudiation

CERTIFICATE AUTHORITY/DIRCTORY (GO-PKI)

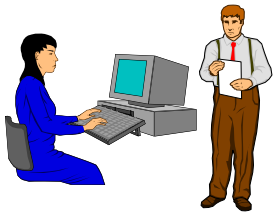


GO-PKI Trust Model

END-USER

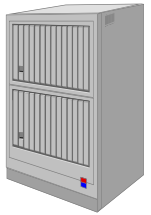


LRA



CA

DIRECTORY



End-user takes credentials to the Local Registration Authority. →

LRA identifies and authenticates user and forwards the registration form to the CA. →

Certification Authority creates CA and Directory entry →

Directory Entry

End-user loads PKI client software on workstation. User creates profile using Auth & Ref codes and stores profile on the workstation →

← LRA passes activation codes to End-User

← CA passes activation codes to LRA

Entering Auth & Ref Codes creates transaction to the CA →

CA posts the public key certificate to directory →

Stores certificate.

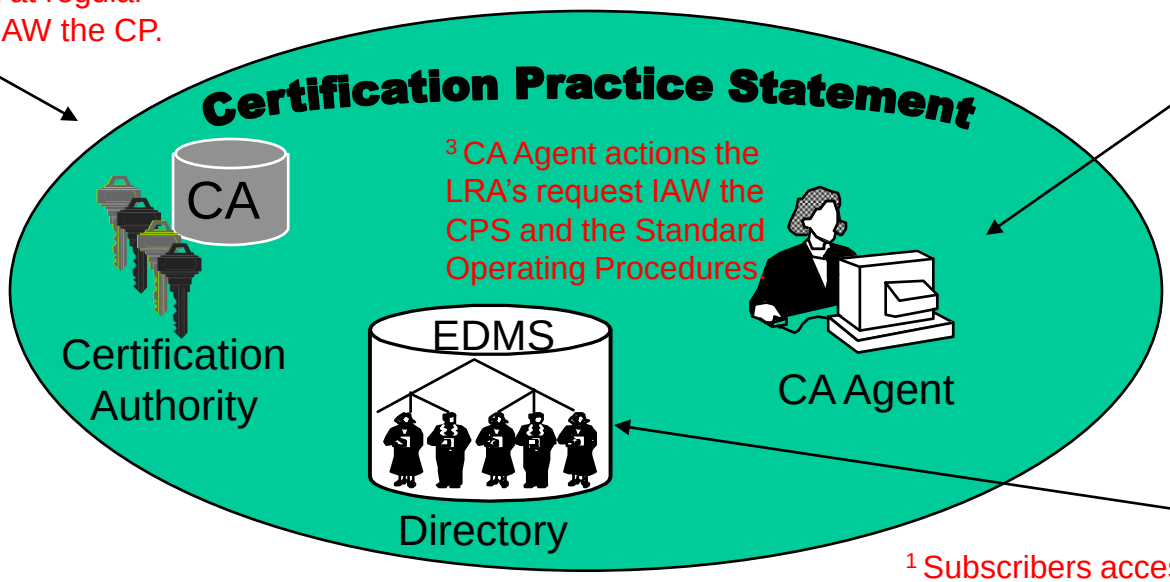
Certificate Life Cycle Management

[4] The CA publishes to the directory the certificate revocation lists.

The CRLs are published at regular intervals IAW the CP.

Role of CA

Registration Authority (LRAs)



[2] LRA informs CA Agent of:

- Subscriber key compromise
- Password reset request
- Subscriber termination
- Subscriber name change

Subscribers

[1] Subscribers access the directory to retrieve other subscribers certificates and the most up to date CRLs.

What does a Certificate Looks Like

DN: cn=Bob Smith, ou=MBS, c=CA — Unique name of owner

Serial #: 8391037 — Unique serial number

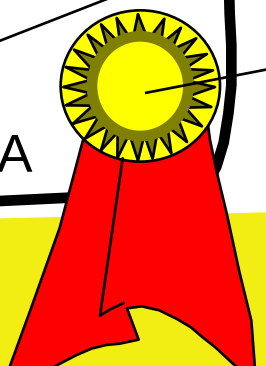
Start: 1/5/00 1:02
End: 7/5/01 1:02 — Period of validity

CRL: cn=CRL2, ou=MBS, c=CA — Revocation information

Key: — Public key

CA DN: ou=MBS, c=CA — Name of issuing CA

CA's digital signature on the certificate



PKI Services

Certificate Life Cycle

Key Management

- Issuance of Certificate
- Password reset and recovery of lost profile
- Name change
- Termination
- Revocation of a compromised certificate
- Publishing of Certificate Revocation List (CRLs)

The GO-PKI initiative and Business case was approved in 1997 to:

- Release an RFP for an 18 month pilot with Options to proceed with full production implementation & vendor of Record Agreements for the next 5 years plus an option for a further 3 more years
- Establish a common security infrastructure under the Security Architecture layer to provide data encryption and digital signature services to the Ontario government ministries and agencies.
- Facilitate more efficient and effective Government service delivery, public information access and electronic commerce across public and commercial networks, while maintaining cost-effective security for Government data and applications.
- A request for proposal (the GO-PKI RFP) was issued in December 1997 to select a vendor or consortium of vendors to provide technology infrastructure goods and services for the GO-PKI initiative.

The RFP requirements were based on the following business drivers:

- Smart Systems for Health, Primary Care and Clinical management users
- Integrated justice/Provincial Police
- Children's Aid Society, case workers
- Ontario business Connects, Secure Web Access
- Workforce Information Network, HR/Time & Attendance
- Internal Audit Restructuring project, Secure Files
- Ontario Energy Board Regulatory File System
- Government translation Services, Secure Web and Encryption Services

RFP & Evaluation

RFP Schedule:

Release of GO-PKI RFP	December	15, 1997
Proponent Briefing Session	January	05, 1998
Notification of Intent to respond	January	09, 1998
Completion of RFP Evaluation	March	30, 1998
Approval of RFP Evaluation Results	March	31, 1998
RFP Award	April	15, 1998
Completion of Acceptance Tests	June	15, 1998
Completion of Contract Negotiations	July	15, 1998
Phase 1. (Initial Year) Contract Starts	July	15, 1998

RFP & Evaluation

RFP Proponents

- 45 Organizations requested copies of the RFP.
- 13 Organizations attended the proponent briefing session.
- 7 Proponents indicated their intent to respond to the RFP.
- 1 Proponent submitted a response consisting of marketing materials only.
- 4 proponents submitted proposals to the RFP.

RFP Evaluation Methodology

- **RFP Proposal Qualification**
  - Submission requirements in RFP Sections 1-6 all met (terms & conditions)
  - Mandatory requirements in RFP Section 7 all met (abide by Proforma Agreement)
- **Detailed RFP Proposal Qualification**
  - Total Evaluated Cost of Proposal (50 Points)
  - Implement ability & Operability of solution (40 Points)
  - Corporate Viability of Proponent (10 Points)

RFP & Evaluation

Successful Vendor

On September 22, 1998 the Ontario Government signed a contract with Entrust Technologies for the provision of PKI technologies and PKI enabling system integration services to the Ontario Government.

- **Contract Highlights**
  - Enterprise Licences and other 3rd party hardware and software products to support PKI implementations across the Ontario Public Service, the Broader Public Sector and potentially up to 12 million Ontario Citizens.
  - System integration services for PKI implementation, support and PKI-enabling of business drivers.
  - Liability for direct and indirect/consequential damages.
  - Off-ramp: termination with out cause upon notice
  - Sharing of information with other governments.

GO-PKI Initial Cost Estimate

- **$1 million for PKI Pilot**
- **$21 Million for 8 – Years of GO-PKI Production Implementation & Operations of Corporate Infrastructure**
- **Total Infrastructure Operating Costs - $2.5 Million per year**
- **Costs do not include Ministry Licensing & specific Application or Ministry Interfaces**

Initial Fulltime Resources Required to Support GO-PKI Services:

- **Operational Support - 3 Senior Security Offices and 3 Admin Officers**
- **Service Development - 1 Developer, 1 Integrator and 1 Business Analyst**
- **Policy -1 Policy Analyst**

GO-PKI Infrastructure Implementation

- Build of initial GO-PKI Infrastructure.
- Commissioning of Certificate Authority (Witness Ceromony) and creation of Corporate Registration Authority (RA) and Local Registration Authority (LRA).
- Implementation of Disaster Recovery Site
- Develop full production GO-PKI business case based on projected costs from the RFP process and comprehensive government business requirements analysis.
- Pilot Testing for Business Drivers including Primary care for Health, Integrated |Justice/OPP, HR and others.
- GO-PKI Operational Policies for Initial Implementation.
- GO-PKI Policy Management framework in place.
- Cross-Certification with PKI's from other jurisdictions, such as the Federal government and other levels of government as required.

Scope of User Rollout

- Rollout PKI Certificates to 65,000 employees within 12 months
- Organization — 26 ministiers
- Rollout — Desktop client
- Register 65,000 employees for PKI
- Employees to accept Subscriber agreement
- Shared Secrets for Password Recovery
- Password recovery Options
- Automated email
- Enable Peoplesoft HR application

GO-PKI Implementation

PKI rollout methodology

- Phased Rollout to Ministry (26 ministries)
- Select 1 ministry as a Pilot
- Test out Communications Plan as part of the Pilot
- Test out delivery of Auth and Ref Codes
- Test Bulkload processors
- Verify accuracy of data
- Set-up Helpdesk Call Centre
- Standardize storage of .epf file
- Automate where possible
- Corporate Project team and Governance (Steering Committee)
- Assign Project Team for each ministry
- Ser # of DN used as Program Identifier (Employee id)
- Disaster Recovery Site Mirror Image of production

GO-PKI Architecture

Baseline GO-PKI System Architecture

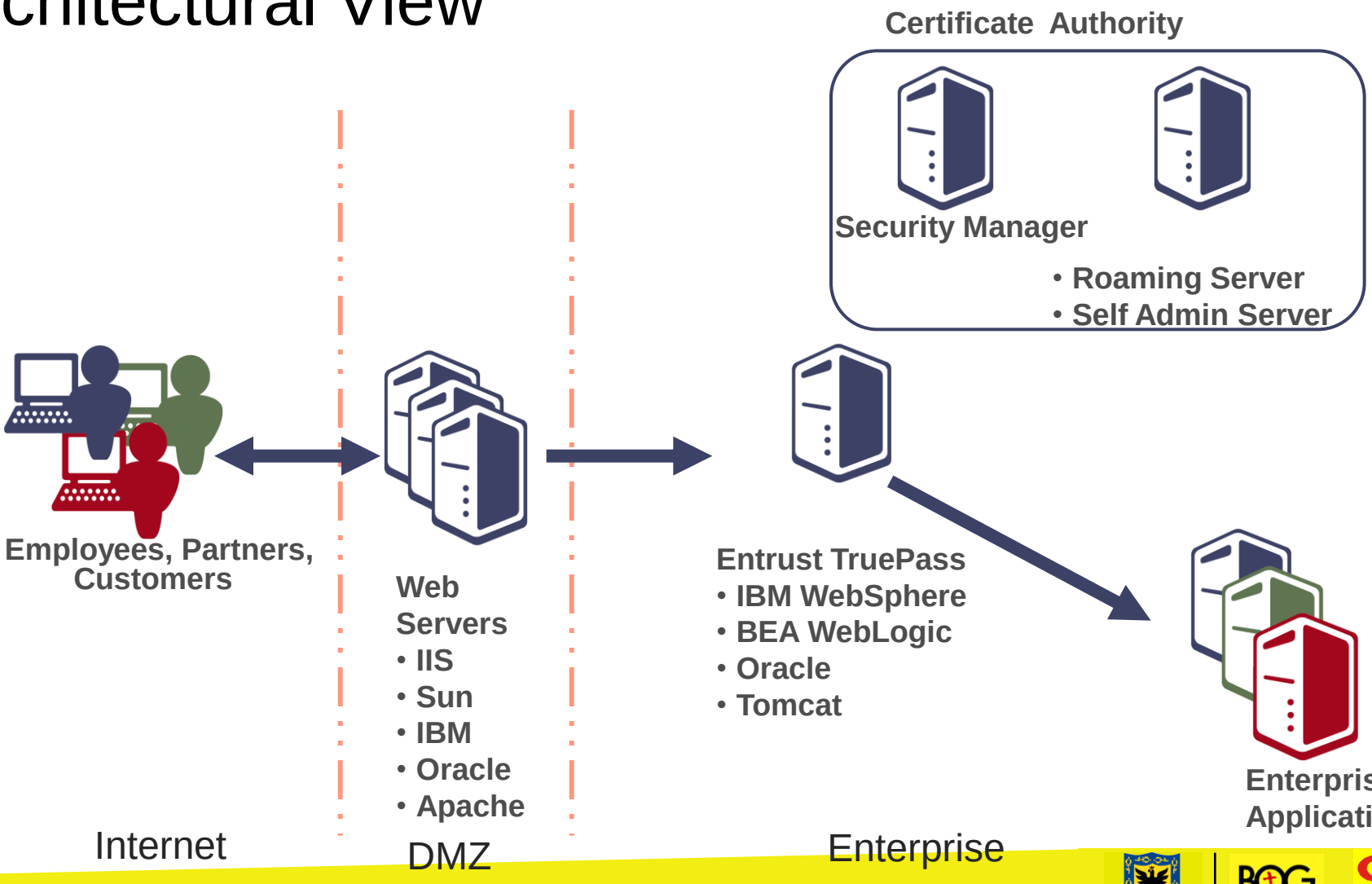
- Test, development and contingency facilities
- Password and profile automated recovery system
- Biometric system – voice recognition system
- Interactive Voice Response (IVR) system
- Registration and activation code facility automation system
- Certification Authority hardware storage
- Network redundancy for the Certification Authority and the Master directory
- System Monitoring capabilities
- Secure remote management facilities
- GO-PKI Operation Center facilities

GO-PKI Architecture

GO-PKI Architecture Sub-Systems

- Certification Authority sub-system
- Registration Authority sub-system
- Directory sub-system
- Communication sub-system
- Security controls sub-system
- Backup and Restore sub-system
- Development and Interim Contingency (DR) facility sub-system
- Logging and audit sub-system
- Remote system administration sub-system
- Fault and performance monitoring sub-system
- GO-PKI operation sub-system

Architectural View



Lessons Learned

Lessons learned:

- You need a Killer App and Senior Manager Champion
- Accuracy of User data
- User knowledge of email address
- Wide spectrum of user IT knowledge (eg. From admin to engineers)
- Email identifiers
- Little expertise in PKI
- High Dependency on Consultants
- Dependency on Knowledge transfer
- High Cost of PKI Consultants, also in high demand
- Very few implementations of similar size
- Management of External Client Groups
- Rollout timeframes very aggressive
- Automation tools very basic both from CA/Directory and registration tools
- Thick client on Desktop (Entrust Direct)
- Subscriber signing of Liability Agreement.
- Manual Password recovery services, Voiceprint
- Test Environment that is a Mirror Image of production

THE GO-PKI TRUST MODEL

- When Programs use GO-PKI, they are placing their trust in the GO-PKI Trust Model.
- This trust is built on a strong governance structure, formal roles and responsibilities, technology, and comprehensive policies and procedures that are in place for GO-PKI services.
- Any compromise of the Trust Model can result in serious repercussions that can destroy the effectiveness and reputation of the GO-PKI implementation.
- The ongoing vigilance of everyone involved in GO-PKI is essential to the maintenance of the Trust Model.
- The Government must be in a position to demonstrate that all components of the Trust Model are in place.
- The Government must be in a position to Cross-certify with other jurisdictions.

The Governance Model of the GO-PKI utilizes three distinct governance roles:

The Policy Management Authority (PMA) is responsible for:

a) GO-PKI policy governing the creation and operation of the GO-PKI CA and RAs, any inter-operability agreements with PKIs operated by other organizations, and

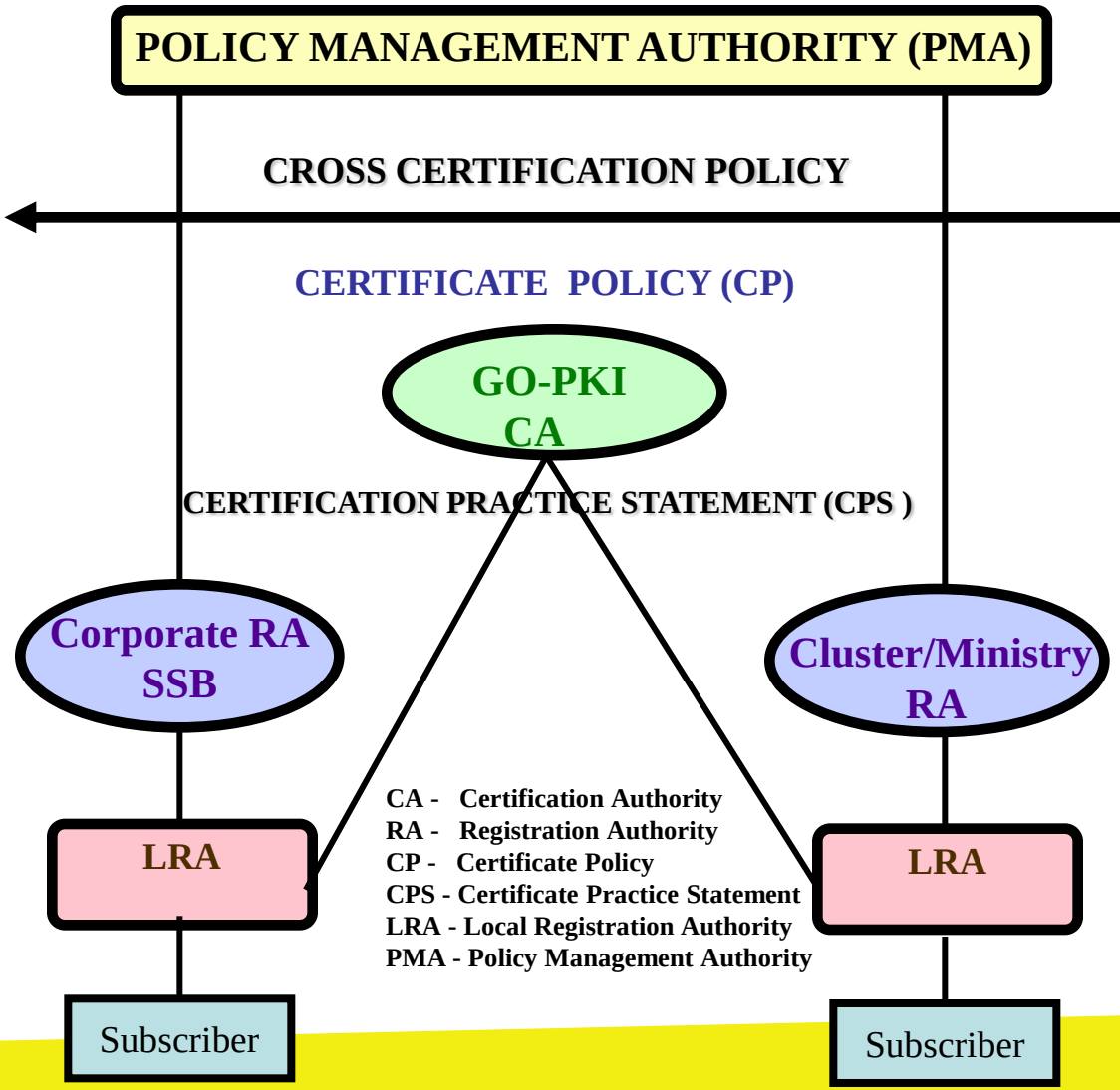
the approval of new uses of GO-PKI and any registration model developed by a program area to issue GO-PKI certificates.

b) The **Certification Authority (CA)** which is operated by Corporate Security is responsible for:

the day-to-day technical operation of the GO-PKI,

the issuance of GO-PKI certificates to individuals that have been duly registered.

C) A **Registration Authority (RA)** is appointed by the PMA for each domain.



PMA oversees the Governance of the GO-PKI Certificate Policy, approves RAs and Cross Certification Policy with other PKI's

MBS *i*SERV ONTARIO operates the GO-PKI CA in accordance with the Certificate Policy & the Certification Practice Statement

Ministry/Program /Cluster RA's are responsible for the nomination of the LRA & the development & approval of the registration model in accordance with the CP & CPS

LRAs on behalf of the RA interacts on a day-to-day basis with the GO-PKI CA & is responsible for the face to face Authentication of subscribers in accordance with the CP & CPS

The Policy Management Authority's responsibilities are to:

- Finalize the GO-PKI Governance Model and Conceptual Model for approval by Management Board of Cabinet
- Approve the submission to Management Board of Cabinet, including the recommendation to create a Policy Management Authority (PMA)
- Establish and approve appropriate mechanisms, controls and reporting structures for the management of the GO-PKI
- Approve the GO-PKI Certificate Policy (CP) and Certification Practice Statement (CPS)
- Ensure that the Root Certification Authority (Root CA) complies with the policies, standards and directives regarding GO-PKI
- Ensure through policies, standards and directives the harmonized operation of the GO-PKI and the inter-operability between its members, and appropriate linkages and supports to Electronic Service Delivery projects
- Establish and approve applicable policies, practices and guidelines to be followed to cross-certify with other CA's external to the OPS to maintain required levels of reliability and security in the GO PKI system
- Negotiate and approve cross-certification agreements with certification authorities external to the GO PKI, including inter-governmental and international agreements

The Policy Management Authority's responsibilities are to:

- Direct the Root Certification Authority (Root CA) to issue, downgrade or revoke cross-certification relationships
- Appoint registration authorities and determine security safeguards for their operational sites in accordance with this policy
- Consider, and where applicable, approve requests to use PKI by a project, a Ministry or Agency, including the level of assurance, the RA and LRA
- Consider, and where applicable, approve bulk applications/registrations
- Consider, and where applicable, make recommendations to admit members outside of Ministries and Schedule I and IV agencies
- Determine the dispute resolution process in the event of disputes between the Root CA and Domain Role-based CA's or between CA's, and appoint decision-makers
- Directing the creation and implementation of education and communications strategies that promote awareness of GO PKI objectives

Membership of the PMA

- membership to the PMA is applied for by potential members to the Chair or by invitation from the PMA itself The members of the PMA are senior managers with responsibility for delivering services to the public or internally to the government, and are actively planning, implementing or using the Public Key Infrastructure to do so.
- Members also include senior managers whose role is to support the implementation and operation of the PKI, or who have a major influence on its direction or support, including selected cluster CIO's and the Corporate Chiefs for Strategy and Service Delivery
- The Corporate CIO will determine initial members of the PPMA and invite them to convene. Subsequent

Support for the PPMA

A multi-disciplinary team of individuals (PMA Working group) provides advice to and supports the activities of the PMA. This team reports to the Head Security, who is also the permanent Secretary to the PMA. Disciplines that, at a minimum, must be represented on the support team are:

- Information Protection (Security)
- Audit
- Privacy
- Records Management
- Directory
- Networks
- Legal
- Policy
- Information Management
- Enterprise Architecture

Current Status of GO-PKI in Ontario

GO-PKI Applications Deployed (Approx 100,000 Certificates)

- Children's Aid Society
- Corporate Employee Portal, Workforce Integration Network (WIN)
- Service Delivery Model Technology (SDMT)
- Justice secure e-mail & E-File
- MNR secure e-mail
- VPN Secure Access from the Internet
- MoF File & Folder Encryption
- ONVIP Secure Web access
- Transportation Medical Update

GO-PKI Applications

- **Children's Aid Society**
  - Initial pilot for PKI in 1999 now moved into production services
  - Used by CAS caseworkers
  - File/folder encryption and secure transmission of files over the network to update central CAS databases

- **Workforce Integration Network (Corporate Employee Portal)**
  - First production application implemented for all employees April 2000
  - Peoplesoft HR application used for attendance reporting across the OPS
  - Functionality now expanded to Employee Portal including:
    - Human Resource Management tool, Time & Attendance (PeopleSoft)
    - Talent Management
    - Employee Travel Expenditure Claims (ETEC)
    - P Card
    - Delegation of Authority
    - French Translation Services (Requests and tracking)
    - Online Ordering (external suppliers)
    - IFIS (Oracle Financial)

GO-PKI Applications

- **Service Delivery Model Technology (Apr 2000)**
  - Ontario Works Program – MCSS & Municipal offices
  - Implemented across Municipal offices to provide secure access to social assistance system by municipal employees
  - Encryption, signing, secure email and authentication
  - Approximately 11,000 users
  - Enables payment enquiry by public subscribers

- **Justice Secure Email (Apr 2000)**
  - Secure email with Entelligence & Express
  - File/folder encryption using ICE
  - Approximately 10,000 users

GO-PKI Applications

- **Justice Secure E-File (2003)**
  - web-based environment that allows the submission and review of court forms and documents.
  - requires the use of digital certificates for identity authentication and applying digital signatures on the submitted documents and forms
- **Ministry of Finance Auditor Secure Notebook (2002)**
  - Provide full encryption of sensitive data on Ministry of Finance Auditors notebooks
- **OPP/WIN Integration (2003)**
  - Enables OPP employees to access Workplace Information Network portal using their OPP certificates.
- **Virtual Private Network Access (VPN)**
  - Implemented VPN access from remote networks to GO-NET
  - Requires use of PKI certificates for authentication and encryption over the network
- **Ontario Vital Statistics Improvement Project (2003)**
  - Web based application for registering and printing of vital statistics information eg. Birth certificates
  - Utilizing PKI for strong authentication, encryption and secure transmission over the network

GO-PKI Applications

- **Economic Business Cluster – ESDI**
  - provides a secure messaging Infrastructure component to handle XML and other format messages from service providers (SP) to Ministries
  - Custom API wrapper for Java toolkit & LUNA SA hardware encryption/digital signature
- **Ontario Court Judges File Encryption**
  - Files encryption on laptops and enables secure email
- **E-Pathologists**
  - allow a Pathologist to submit an “automated” copy of their Post Mortem report to the Office of the Chief Coroner over the Internet
- **Apprentice Support Application (ASA)**
  - allows Teachers from Colleges to Input Apprentices marks and status over the web.
- **Corporate Employee Portal now has over 45 applications protected by GO-PKI**

Current Status of GO-PKI in Ontario

Thank you