



Treasury Board of Canada
Secretariat

Secrétariat du Conseil du Trésor
du Canada

Public Key Certificate Support for Canada's Government OnLine

Mike Just

Treasury Board of Canada, Secretariat

2nd Annual PKI Research Workshop



Canada



Outline

- Canada's Government OnLine (GOL) Initiative
- epass
 - Overview
 - Getting an epass
 - Managing an epass
- Privacy
- Concluding remarks



Canada's GOL

- Online federal government services to individuals
 - Taxes, employment, benefits, health, ...
 - Citizens, businesses, non-Canadians, ...
- Consistent interface across programs
 - Common Look-and-Feel (CLF), accessibility, ...
- Complementary to other service channels, e.g. in-person, phone



Canada's GOL...

- Client-authenticated services
 - Start small so as to lessen risk
 - Currently: Address Change Online (ACO)
 - Next: Employment record management for businesses
- Privacy and security
- Common authentication infrastructure
 - epass issuance and management
- Individual identification managed at each program
 - Retains information silos



epass Overview

- epass: Collection of an individual's public and private key credentials
- Registration and enrolment
 - epass registration (generation and issuance)
 - Identification to government program
 - Program mapping of certificate identifier to an application-specific identifier



Registration and Enrolment

- Registration with Common CA
 - Obtain one or more epasses
 - Indexed by MBUN (Meaningless But Unique Number managed by CA)
 - Supports roaming individuals
 - No link to individual received or maintained at CA
 - Holds challenge questions and answers for recovery and self-revocation



Registration and Enrolment...

- Enrolment with government program
 - Identification of individual
 - Binding of MBUN to PID of identified individual
 - PID (Program Identifier) managed by program



Registration and Enrolment...

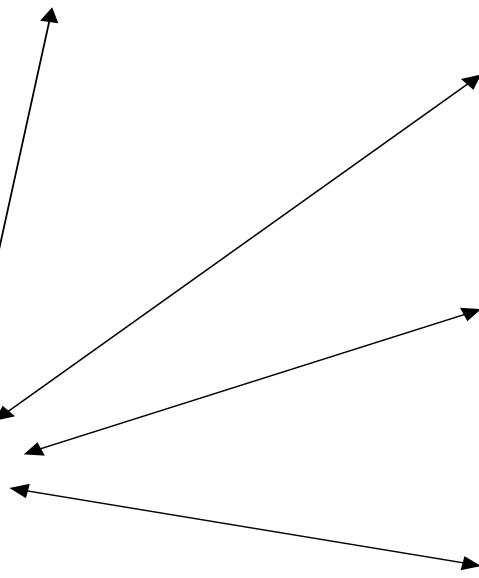
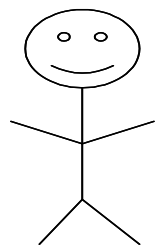
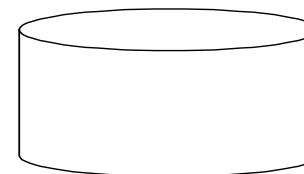
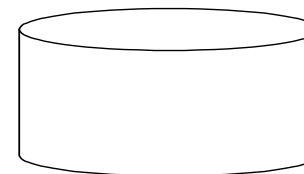
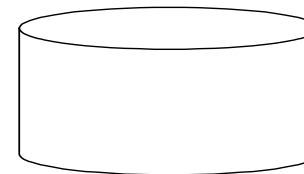
Central CA	
UserID	Encrypted Creds
J1969	XXXXXXXXXX

Program A	
MBUN	PID
1035	123456

Program B	
MBUN	PID
1035	133498

Program C	
MBUN	PID
1035	998321

Program Specific
Repositories



Canada



Enrolment Example

- Canada Customs and Revenue Agency (CCRA)
Address Change Online (ACO)
- Online identification of individual
 - Date of birth
 - Line 150 from previous tax submissions
 - Access code from previous tax assessment
 - Social Insurance Number (SIN)
- PID is the SIN
- MBUN from epass mapped to PID at program



Canada



Mapping MBUN to PID

- epass MBUN is mapped to PID, and mapping is held only at the program
- Programs continue to key on PID (not MBUN) as MBUN may change
 - Individual re-registration
 - Individual may choose to associate new epass with PID



epass Management

- Renewal
 - 5-year certificate lifetime
 - Updates attempted at 50% of lifetime
- Revocation
 - Self-revocation of epass supported
 - Answers recovery questions
 - Limited cases for administrative epass revocation
 - Per-program de-activation of MBUN-PID mapping



epass Management...

- Recovery
 - Individual provides answers to registered questions
 - New epass with same MBUN (“account recovery”)



epass Use

- Central logon and retrieval of epass
 - Standard browser plus Java applet
- epass credentials used to authenticate to program
- Persistent signatures and encryption
 - E.g. signed address change



Privacy

- Choice
 - epass optional for obtaining government services
 - More than one epass
- Separation between epass registration and program enrolment
 - CA is central, but has no identifying information
 - Individual maintains relationships in context, with each program



Privacy...

- Data matching
 - Legislation and policy
 - Changes in MBUN encourage PID indexing
 - More than one epass
- Pseudonymity



Concluding remarks

- Common CA for epass issuance and management
- Individual identification managed by each program
- System will continue to evolve over time
- Contact information
 - Email: Just.Mike@tbs-sct.gc.ca
 - Phone: +1-613-952-6738