Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada

Cyber Authentication Renewal Project

Executive Overview

June – 2006

30 minute Brief

Canada

Agenda

- Background
- Business Problem Assessment
- Business Vision
- Transformation Strategy
- Next Steps

Background:
Project Scope

- Online electronic service delivery (1-channel)
- Horizontal GC-wide authentication
- Both internal & external subscribers
- ePass
- Services that rely on cyber authentication:
  - Identity Management
  - Authorization
  - Transactions
- No classified or Protected C systems

Background:
Project Triggers

Global trend	-	enterprise services
Global trend	-	shared services
TB commitment	-	shared services
TB direction	-	contestable services
MAF	-	distributed responsibility
Policy Suite Renew	-	window of opportunity
ID Management	-	credential element
IT Security Strategy	-	GC-wide initiatives

Background:
Approach

- Engage key stakeholders
  - Service Canada, CRA, PWGSC, CSE, TBS
- Short & focused on business
  - 5 week effort, précis like deliverables
- Focus on problems, vision and activities
  - Needs follow-on overall planning
- Breadth over depth
  - Details in follow-on projects

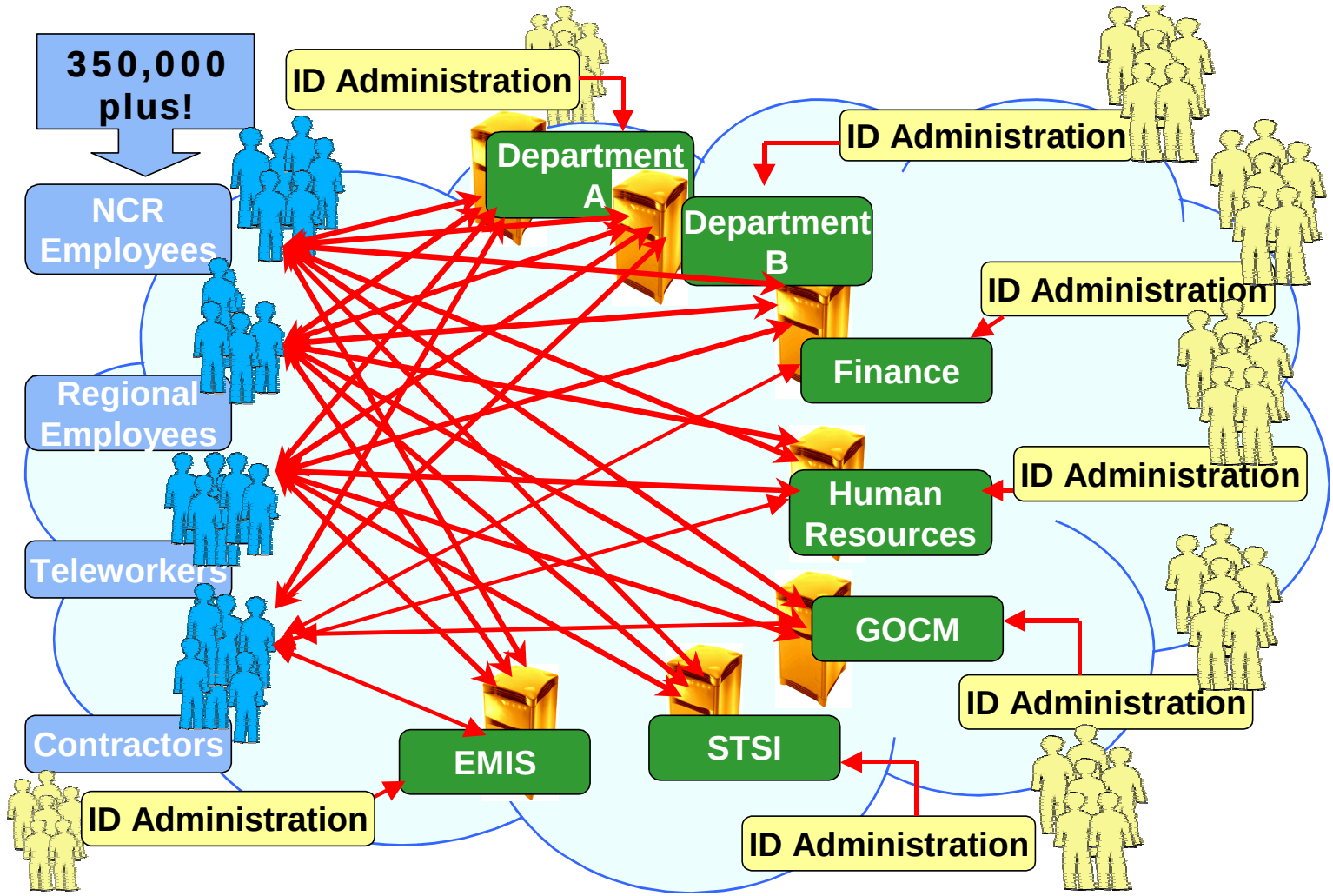
Business Problem Assessment:
Target Groups

- **Subscribers** - entities that hold credentials and present them on-line to acquire service
  - Examples: employees, contractors, agents, citizens, businesses
- **Credential Service Providers** - entities that provide, maintain and govern credentials
  - Examples: programs, departments, ePass, provinces, municipalities, banks
- **Relying Parties** - entities that accept credentials on-line from subscribers in a specific context
  - Examples: programs, provinces, municipalities

Business Problem Assessment:
Summary of Problems

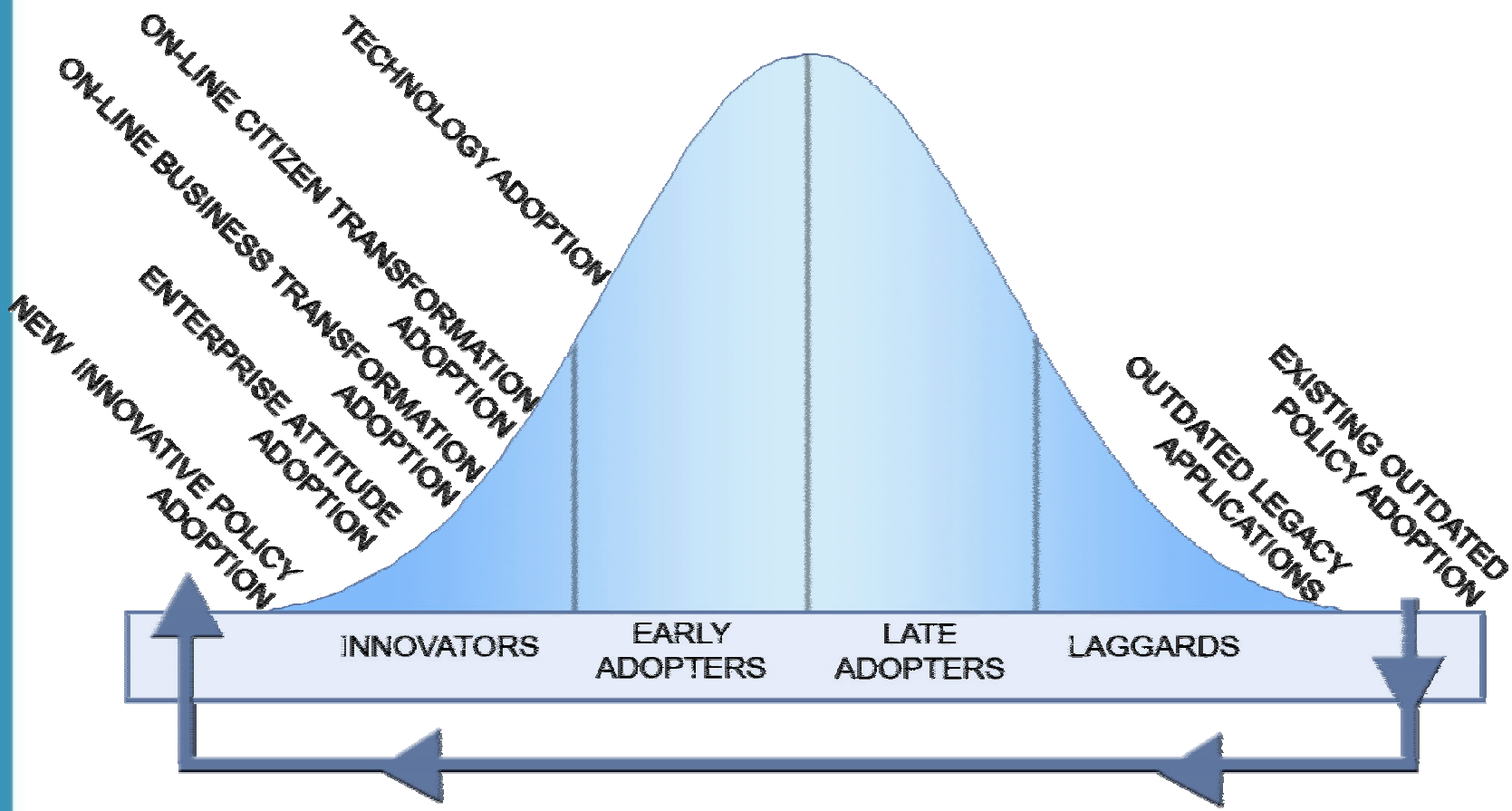
- Usability
  - Need simple subscriber experience
- Good Solution Design
  - Need agile, non-duplicated, balanced, federated solution
- Management and Governance
  - Need horizontal, consistent, multi-jurisdictional governance
- Privacy and Legislation
  - Need balanced privacy solution & clear legal framework
- Security and Integrity
  - Need comprehensive IDM with assurance levels & traceability
- Relying Party / Provider Service
  - Need business collaboration agreements & clear costing model

Business Problem Assessment:
Example of Problem in Employee Space



Business Problem Assessment:

Cyber Authentication Adoption

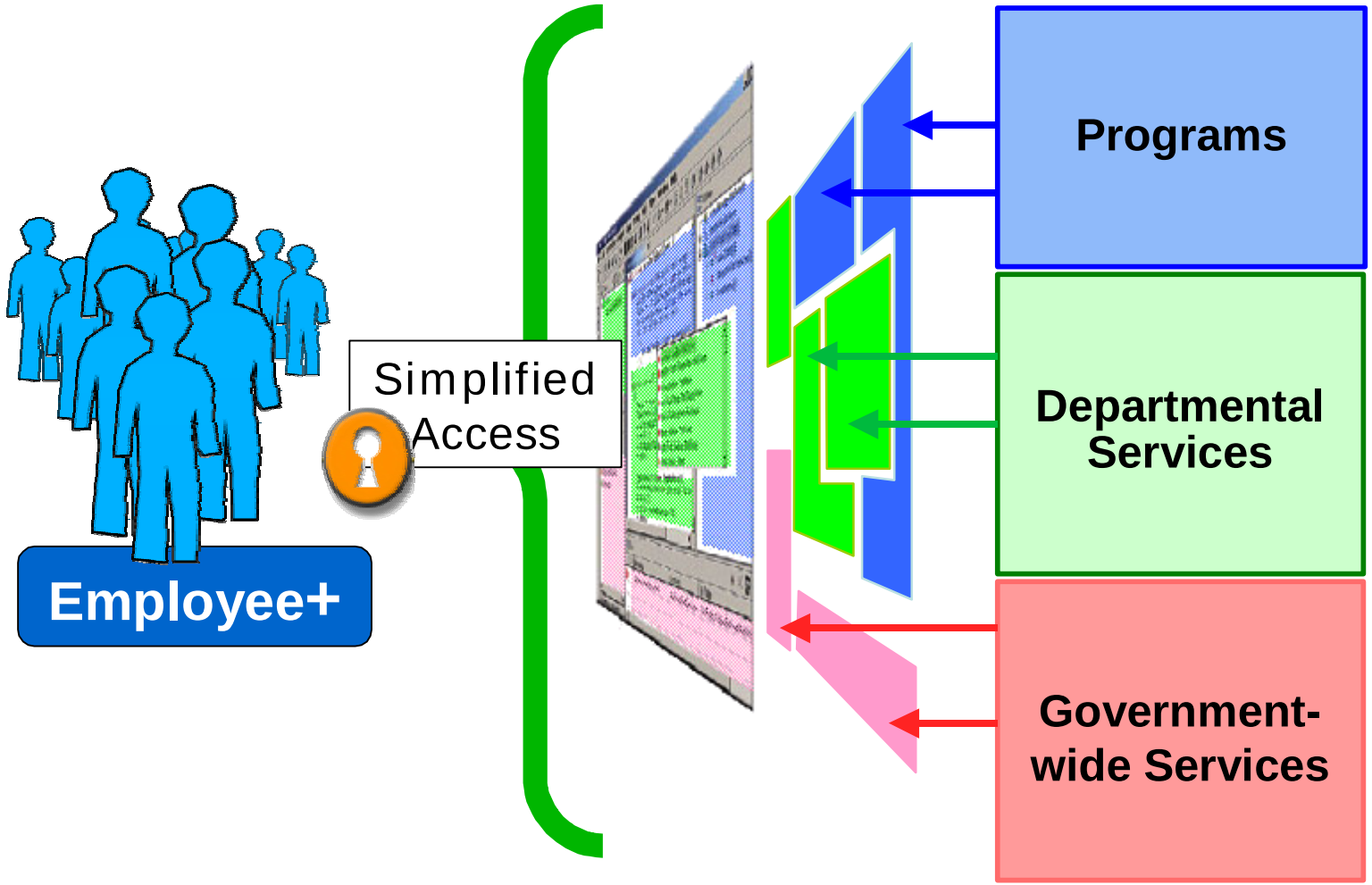


Business Vision:
Vision Statement

Online clients of GC services require privacy and identity protection while using seamless online authentication services that are effective and of an assurance appropriate to the business risks.

Business Vision:

Example of the Vision in Employee Space



Business Vision:
Key Innovations 1

Innovations are new processes, capabilities, standards, methods, and tools often **contrary to established norms**.

- Client-controlled information service
  - Enables control, consent and minimal disclosure
- Citizen/Business use of external CSP credentials
  - Enables citizen credential choice
- Establish credential control assurance levels
  - Enables program flexibility in meeting business needs
- Establish identity assurance levels
  - Enables program flexibility in meeting business needs

Business Vision:
Key Innovations 2

- Establish *Credentialing Federation Council*
  - Service user governance on business issues / privacy / security
- Establish interoperability framework
  - Enables contestable market services
- Combine logical & physical access for employee
  - Enables single use credential for GC access
- Establish GC employee authoritative source
  - Enables rapid, cost effective, and secure solutions

Business Vision:
Benefits 1

Employees, citizens and businesses will …

- Experience seamless access to government services, departments and jurisdictions
- Have a choice of credential service providers
- Have appropriate control over and consent for information sharing

Business Vision:
Benefits 2

Government will …

- Enable subscriber authentication for all programs
- Avoid duplication of effort & costs
- Provide higher integrity information
- Harness contestable market benefits
- Act as an integrated enterprise
- Offer self-service to subscribers
- Potentially reduced service delivery costs

Business Vision:
Benefits 3

A Federated approach…

- Improves government alliances with autonomy
- Allows growth through improved interoperability and decreased deployment time
- Avoids single points of failure
- Deploys faster using existing authentication services

Transformation Strategy:
Principles

- Adopt a GC wide enterprise perspective
- Encourage contestable markets
- Citizen/business choice on credentials used
- Provide a harmonized client experience
- Support cross-jurisdictional interaction
- Establish horizontal governance
- Adopt service model for joined up service delivery

Transformation Strategy:
Policy Initiatives

Establish	-	authentication program
Influence	-	*Policy on Service to the GC* and the *Enterprise Architecture*
Extend	-	*Common Look and Feel* to include an online transactions standard
Establish	-	online transaction audit - electronic records as documentary evidence standard
Establish	-	credential control assurance standard
Establish	-	GC credential policy
Displace	-	*Electronic Authorization and Authentication Policy* to other policy instruments

Transformation Strategy:
Enterprise Initiatives

Establish - authentication responsibility centre

Adopt - Enterprise wide behaviour

Establish - funding model to encourage enterprise behaviour

Establish - communications, stakeholder engagement and education strategy

Transformation Strategy:
Implementation Considerations

- Requires strategic & tactical outlook
- Must exploit a window of opportunity
  - Departmental maturity levels rising
  - Stakeholder education has evolved
  - Current IDM/authentication momentum
- Risks
  - Lack of cultural change within the GC
  - Lack of buy-in by programs
  - Lack of sufficient resources
  - Complex implementation plans
  - Dependencies on IDM Project

Transformation Strategy:
Critical Success Factors

- User Awareness and Consistent Experience
- Stakeholder involvement and buy-in
- Independence and loose coupling of services
- GC-wide Leadership and Stewardship
- Horizontal governance (policy instruments)
- Clear accountabilities
- Funding/Resources

Transformation Strategy:
Out of Scope Observations

- Join Physical & Logical Employee Access
  - Adopt and ride Personal Identity Verification (PIV) market developing in the US
- Choose IDM Assurance Levels Wisely
  - IDM assurance levels must correlate with Credential control assurance levels
- IDM Deliverables & Timeframe
  - Tightly coupled dependencies

Next Steps:
Lead Projects

- Departmental consultation for 2 months
  - Leading to establishment of a responsibility centre
- Establish the authentication program
- Co-ordinate IDM project & the authentication project