EGovernment and the Secure Channel Vision

www.icorp.ca

Copyright 2000 icorp.ca

1 eGovernment and the Secure Channel Vision

eGovernment will fundamentally change the way the Government of Canada (GoC) operates and relates to its stakeholders. eGovernment or the Government On-Line (GoL) initiative, identifies a future in which citizens can log onto *one* Internet site, easily find the government services they are looking for, and use that site to conduct online transactions; a future in which businesses fill out *one* Internet form for all their municipal, provincial, and federal environmental regulatory compliance requirements; a future in which government officials make all purchases and payments electronically, saving millions of dollars. The technology for these applications is available now, awaiting implementation by the GoC.

Among the benefits of eGovernment are savings in money and time for government, businesses, and consumers. If banks can cut their transaction costs by 90 percent through online banking, similar savings for government are likely. Moreover, users of eGovernment services will benefit from continuous access to higher quality services. Most importantly, the relationship between government and citizens can evolve from its traditional hierarchical and arms-length one to a more reciprocal one where citizens are genuine stakeholders in their government. These concepts are at the core of Departmental eService delivery intentions, which to date have not been well developed. The many and varied relationships, as identified in the attached diagram (*copyright icorp.ca inc*.), need to be well articulated by both Departmental requirements and by the GoC eGovernment Secure Channel infrastructure.

eGovernment

The nature of eGovernment, including government on-line, is multi-faceted and multi-dimensional. A well thought out eGovernment strategy must address each of the elements included below.

	Government	Business	Citizen
Government	Gov. to Gov. (G2G) • International • Fed./Prov. • Municipal	Gov. to Bus. (G2B) • Services • Information • Regulations • eSurveys	Gov. to Cit. (G2C) • Services • Information
Business	Bus. to Gov. (B2G) • Procurement • Tax Conformance • eSurveys	Bus. to Bus. (B2B) • eCommerce • Parterships • R&D	Bus. to Cit. (B2C) • eRetail • Service/Support • eSurveys
Citizen	Cit. to Gov. (C2G) • Tax Conformance • Passports • Service Requests	Cit. to Bus. (C2B) • eRetail	Cit. to Cit. (C2C) • Auctions • eMarketplace

To-date progress towards eGovernment has been slow and not linked to government reinvention. Rather, most IT applications have focused on improving the efficiency of existing operations or providing one-way information dissemination, instead of fundamentally changing the way businesses and citizens interact with government.

So how do the assumptions underlying the Secure Channel Vision (SCV) get validated? What will be the impact on the SCV when Departmental eGovernment strategies have been developed and implemented? Will the two be synchronized?

icorp.ca inc. has undertaken a considerable amount of research in this regard and is offering the following observations and strategic perspectives for the SCV as articulated in the draft Secure Channel RFP dated early September 2000 (www.pwgsc.gc.ca/sgocc) .

1.1 Secure Channel Integration and Synchronization

The Secure Channel is being established to provide the connectivity and underlying support services necessary to deliver GoC program information and services electronically. These support services will need to include access, authentication, authorization, confidentiality, inter-communication, data integrity, non-repudiation and brokering. As the SCV is supported by GoL strategies, set out in the Treasury Board's SII initiative, the secure channel infrastructure needs to be designed to meet Departmental eGovernment service delivery requirements.

It is important that the SCV and the secure channel project be driven by GoC business model needs and not driven by technology alone. The many different business needs across government will require different SVC features. For example, the Canada Customs and Revenue Agency's customer-transaction channel needs the highest level of security, as will a number of National Defence activities (e.g., procurement information, operational coordination). Further, the business communication security needs of Industry Canada's Marketplace regulatory organizations (i.e., Corporations Canada, Measurement Canada, Canadian Intellectual Property Office, and Office of the Superintendent of Bankruptcy) would be high, but not as high as those of CCRA and DND. Elements of Health Canada's activities, such as the Canada Pension Plan and Employment Insurance, might require an even lower security level for its GoL activities.

Overall, the SCV's success will depend on how well it meets the practical business requirements of each federal organization.

Furthermore, the Secure Channel design needs to reflect the fundamental principles of "*what government does*" and "*how government works*." That is, eGovernment is by nature quite different from B2B, and these differences need to be reflected in the design as well.

In designing new technological capabilities, sometimes the "technology" tries to drive the systems, thereby limiting the practical usefulness of the systems. An important

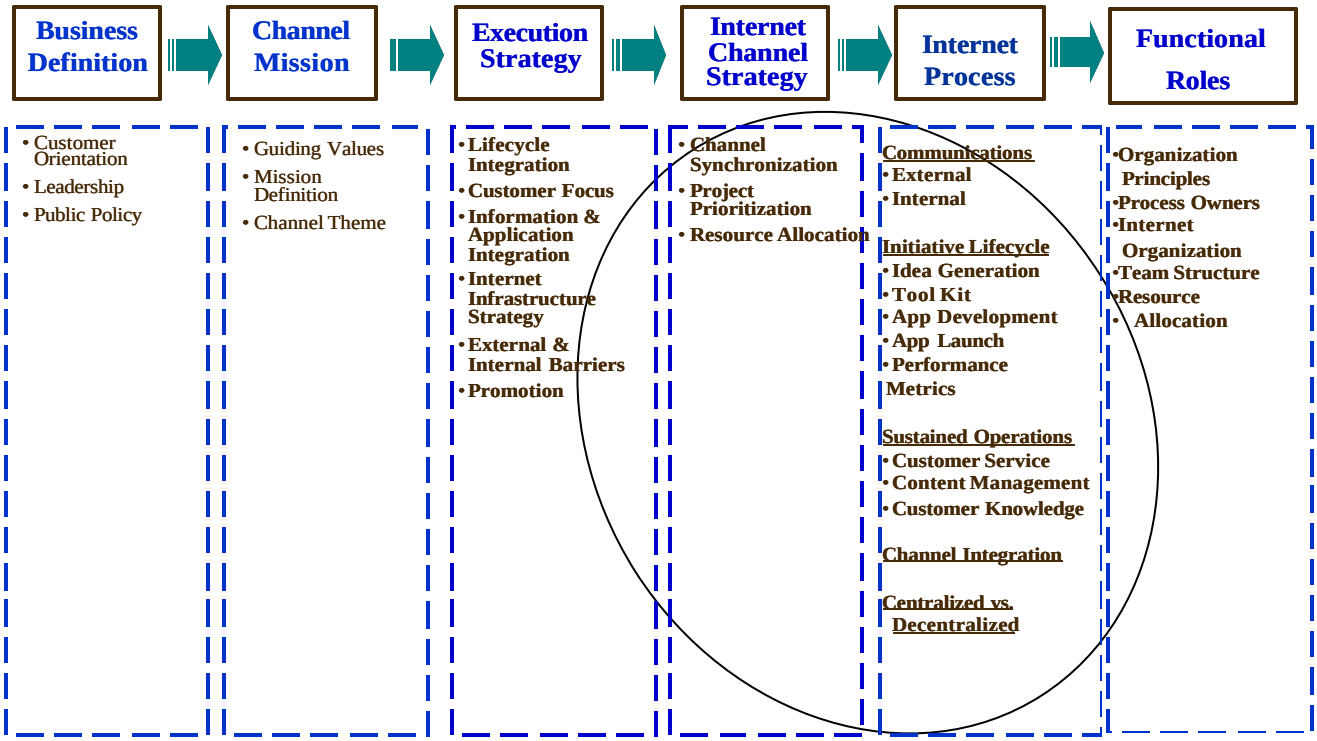
attribute of the Secure Channel must be that it reflects the different business needs of Departments.

It will be very important that the needs of eGovernment be very well articulated, as this will form the validation basis of the infrastructure design. The secure channel integration with Departmental eBusiness needs is critical to developing the right secure channel design. It will also help to ensure that the SCV is readily adopted by federal organizations.

Does the RFP address the critical business needs of the GoC in the future? Secure Channel integration and synchronization need to be validated together, not in isolation. We see a validation process for the SCV whereby:

- users (eGovernment stakeholders and potential service providers) are extensively consulted regarding their strategies and technology infrastructures;
- an environmental scan of both Departmental business needs and technological advances be undertaken;
- a gap analysis be undertaken between the current underlying assumptions of the SCV and the results of the environmental scans; and
- strategic and synchronized recommendations are made *(using a similar approach as identified in the diagram below).*

Secure Channel / eGovernment Synchronization Process



1.2 The Need for Synchronization

The Secure Channel is about a Trusted Services infrastructure. Although critical trusted service requirements will be administered by Departments, they have yet to undertake their GoL service delivery reengineering and formulate their Tier II plans.

Departments will need to articulate their GoL strategies by developing:

- GoL eService delivery Departmental Business Plans;
- New Departmental business models based upon electronic services;
- eService delivery policies; and
- Departmental strategies for how they are going to get there.

It is important that the SCV be flexible to support both Departmental specific and Treasury Board strategies, to ensure that the Secure Channel digital security elements are consistent with Departmental trusted service delivery needs. Departments that embrace leading edge eGovernment strategies will:

- Enable full horizontal integration within and between Governments, across departments, organizationally and functionally.
- Facilitate Government transformation and change in its traditional role - from that of an implementer to that of a facilitator.
- Provide Citizens with greater visibility and insight into value chain activities.
- Become early movers to establish themselves as "portals" for certain government services, across jurisdictions.

1.3 Emerging Technological Advances

Although the Secure Channel Vision (SCV) addresses technological advances as we know them today, serious attention needs to be given to emerging network structures, wireless standards and computing device capacity.

There needs to be a critical appraisal of the assumptions underlying the RFP and the SCV. For example, great attention needs to be given to the next generation wireless standards, such as Bluetooth. Wireless Local Area Networks (LANs) using Bluetooth technology provides the ability of various wireless devices to sign-on automatically to a network (secure or unsecure) when they are turned on or when they enter an area, referred to as Personal Area Networks (PANs). The Sun Jini technology will also function on the same basis for spontaneous or ad hoc networking as Bluetooth. The SCV needs to more clearly articulate and anticipate these emerging wireless standards and ensure that the secure channel infrastructure can adapt accordingly.

For purposes of Trusted Services, how will the Secure Channel handle encrypted Bluetooth technology using digital certificates? For example, the Secure Channel could be used for identity verification purposes to authenticate a person entering a

building with a Bluetooth wireless-based security card. Or, Health Cards may be encrypted using wireless technologies for authorization purposes with a PIN number.

Likewise, throughput capacity across the network needs to be addressed more clearly. For example, if the Secure Channel were to use the CANARIE / Industry Canada *CA Net 3* fibre optic backbone, performance standards would need to be articulated to identify load capacity at critical points over the network.
More importantly, performance standards for Departmental infrastructures and capacity would also need to be articulated.

All critical Departmental eService delivery networks must be designed to cope with massive volumes of traffic and transactions.

The SCV and the requirements set out in the RFP also need to balance infrastructure openness and flexibility against rigorous security and confidentiality concerns.

1.4 Management of Digital Certificates

The Secure Channel will need to have the ability to handle very large volumes of issued digital certificates. GTIS needs to consider the options and alternatives to Certificate Authority management for the GoC and the millions of citizens who will be accessing the secure network. Consideration should be given to evaluating the alternatives to certificate management, including the option of outsourcing or partnering with a trusted organization.

For example, currently the technology to propagate digital certificate revocation across the globe is a minimum of 24 to 48 hours. If someone's digital certificate key has been compromised or expired, the GoC will be at risk for that period of time. If the underlying application where the digital certificate has been compromised is mission critical or a serious security breach has occurred, access for that individual must be discontinued immediately.

Equally important, the GoC or GTIS needs to articulate the digital certificate policy to truly authenticate an individual. This becomes a "chicken and an egg" dilemma. Therefore, the SCV and the GoC needs to articulate its certificate issuing revocation policies. Potential digital certificate ID requirements could include the following informational the state security level (Protected B & C);

- Birth certificate
- Passport
- Notarized documents
- Medical records
- Dental records
- DNA typing
- Retinal scans
- Digital finger-printing

These ID requirements will also need to be independently validated.

The articulation of the digital certificate issuing policy will have a significant impact on the design of the secure channel.

2 Experience and Capacity of icorp.ca inc.

icorp.ca inc. is an eBusiness strategy and research consulting firm with expertise in e-Business, iResearch and WebPortal design.

Our **eBusiness** consulting service helps clients define their digital strategies to implement eGovernment and the connected organization.

Our **iResearch** service investigates emerging practices and winning strategies for the digital economy. Our research tools include scenario development, policy research and eSurvey analysis.

WebPortal refers to our company's Internet product development sphere. Our key initiatives focus on fostering electronic marketplace development and secure portal interactions.

Our company's profile and our key eGovernment services are outlined on our website at www.icorp.ca and form an integral part of our response to your LOI for the Secure Channel. A summary of our multi-disciplinary team is provided on our website under Corporate Profile – Principals, which includes references to publications by members of the icorp.ca team, as well as reference books used in our iResearch.