Chapter 5

e-Governance Implementation

David Spiteri Gingell

The previous chapters have established that the best route to the attainment of e-government is through the design of a holistic strategy that seeks to transform government, and subsequently transform a country, into an information society or information economy.

It has also been explained that the design of the strategic process to achieve such a transformation demands that the strategy is designed over a generational horizon. Transformation will not happen overnight. It will require various stages of maturity – with each level of maturity leading to subsequent stages of development until these too reach a level of maturity.

Small states have to face unique challenges, which will impact the tempo and pace of the implementation process. This, however, does not mean that e-government is not attainable. It is important to underline that a considerable number of the constituent parts to achieve e-government do not carry major costs. Moreover, the economics of ICT have changed rendering the cost of technology cheaper and more affordable. Furthermore, the technology itself has changed. Mobile telephony has now proved that it is a strong enabler for the attainment of e-government, as invariably it is less expensive to implement than dark fibre infrastructure, more affordable to citizens and overcomes the challenge of distance.

An approach to the attainment of e-government should therefore be designed to be multi-pronged from the outset of the implementation process, particularly with regards to the establishment of the underlying soft and hard infrastructure necessary for its successful implementation.

5.1 Legislative, regulatory and policy components

5.1.1 E-commerce legislation

A cyber-legislative framework should, to the extent possible, precede the implementation of an e-government strategy in order to ensure legal effect, confidence and trust, and protection against misuse and abuse. The launch and implementation of an e-government strategy can be critically undermined, and potentially result in political embarrassment, in the event that an appropriate cyber-legislative framework is not in place. Without e-commerce legislation, electronic transactions will have no legal validity or effect.

The absence of legal validity and effect will create jurisprudence and legal issues. Thus, e-commerce legislation must be in place, ideally prior to the initiation of e-services.

Electronic commerce legislation can be designed to act as a vehicle to intensify the uptake of e-government interaction – between government institutions and citizens as well as businesses – by rendering it mandatory for a person to interact electronically with any government entity where any law of the country requires or permits a person to: (i) give information in writing; (ii) provide a signature; (iii) produce a document; and/or (iv) record information. An electronic commerce and transactions law and regulatory framework should address a number of principles. These include:

- the importance of a secure legal basis for electronic communications, contracts, signatures and transactions so as to:
    - encourage economic activity; and
    - allow for the provision of government services over electronic communications media.
- protection of both the consumer and the service provider;
- the need to set minimum rules for providers of 'information society services', though avoiding barriers to entry into this business; and
- the international rules relating to e-commerce.

Box 5.1 Good examples of e-commerce legislation

The United Nations Commission on International Trade Law (UNCITRAL) Model Law on E-Commerce of 1996 (UN 1999) provides an excellent basis to draft an e-commerce and transactions act. Other good models which have withstood the test of time are:

- The Maltese Electronic Commerce Act
- The Australian e-Commerce and Transactions Act
- The Irish Electronic Commerce Act

See: UNICITRAL 1999; Government of Malta 2002; Australian Government 1999; Office of the Attorney General 2000

The principles to be applied in drawing up an e-commerce legislative and regulatory framework include:

- The regulatory framework must be flexible enough to keep up with advances in technology.

- The regulatory framework should observe the principles of self-regulation and subsidiarity, and should refrain from adopting mandatory authorisation systems for signature certification of service providers, although voluntary accreditation schemes could prove useful.
- As electronic signatures must be legally recognised, basic requirements and responsibilities for qualified certificates must be specified.
- Electronic signatures that are based on a qualified certificate issued by a signature certification service provider and which fulfil the requirements established, should be mandatorily recognised as satisfying the legal requirement of a hand-written signature. They should be admissible as evidence in legal proceedings in the same manner as hand-written signatures.
- Electronic signatures used within closed groups, for example where contractual relationships already exist, should not automatically fall within the scope of a legislation as contractual freedom should prevail in such a context.
- The regulatory framework should ensure legal recognition – in particular across borders – of electronic signatures and of certification services. This involves clarifying the essential requirements for signature certification service providers, including their liability.
- The service provider must be able to transmit the data concerning the identity of a user adopting a pseudonym to the public authorities upon request, with the prior consent of the person in question.
- Commercial communications (advertising, direct marketing etc.) – which are embraced by electronic communications – are perceived to constitute an integral part of most electronic commerce services. Such clarifications should be issued on the basis of regulations.
- Electronic commerce will not develop fully if concluding online contracts is hampered by certain requirements that are not adapted to the online environment. Thus an e-commerce legislative and regulatory framework should embrace electronic documents, which include contracts. The legislative framework should propose parameters of when a document is valid, which include time and place of receipt, time of dispatch and storage.
- Liability of intermediary service providers should be planned for, such as:
  - the mere transmission of information over their communications network;
  - temporary storage of information in their network (caching); or
  - storage of information (hosting).

5.1.2 Data protection and privacy legislation

The second component is data protection and privacy legislation, which will secure the rules of how government entities are to employ 'personal data'. The presence of data protection legislation will increase the level of trust and confidence in the use and take-up of e-services.

There are, essentially, three models of data protection legislation design. One is the EU legislative model, the parameters of which are established by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data (EU 1995). The EU legislative model provides for the heavy regulated use of data, and is basically premised on the philosophy that use of data may be abused and hence a tight regulatory regime is necessary to mitigate for such abuse. However, the directive was drawn up before the widespread use of the internet, and the arising business models, including e-government, which this spawned. During the late-1990s and the early-2000s, considerable debate took place between some member states and the European Commission on the need to effect a lighter regime based on the principle of good and reasonable use, as it was otherwise believed that the benefits that could accrue from the implementation of an e-government business model would be constrained.

The *Swedish Personal Data Act* (Government of Sweden 1998) is a good example to follow in the event that a country is seeking to introduce a strong regulatory regime for data protection legislation with a minimalist bias.

A second model is the design of legislation on the principle of good and reasonable use stated above. In essence this model establishes that all use of data is permissible unless otherwise restricted or governed by ad hoc legislation. This model reflects the degree and maturity of the trust that citizens hold in government and other institutions.

A third model combines data protection principles with freedom of information. Few countries have followed this particular design. In part this is because data protection is directed towards safeguarding the individual's right to privacy, while freedom of information is directed towards entrenching open government and placing governing institutions under direct public scrutiny and accountability for decisions taken.

The appropriate model that a country should adopt to design its data protection legislation should balance, on the one hand, the political culture of the polity and the level of trust and confidence by citizens in the governing institutions with, on the other hand, the degree of information sharing flexibility it seeks to achieve to optimise the opportunities of e-government and the cyber-world, as well as the cost it is ready to pay and impose on business, for a highly regulated regime.

The provisions in the Swedish legislation with regards to the *Competent Authority* are sparsely defined. The drafters of data protection legislation may consider that allowing such discretion in the interpretation of the said powers to the Competent Authority could potentially undermine the spirit that the legislation seeks to achieve; this is given that the role of the Competent Authority could be dependent on the person holding the office of the said Authority. The drafters may argue that such a broad degree of discretion would not be in the nation's best interests, as a Supervisory Authority that adopts a 'purist' approach could arguably result in over-regulation. This in turn could lead to increasingly heavy administration regulation costs, as well as the restriction of the use of data for virtual e-government services. The drafters, therefore, may conclude that it is important that the responsibilities of the Competent Authority are specified in detail within the legislation – thereby minimising to the extent possible the level of administrative discretion. In this regard, the drafters of the legislation may conclude that the definition of the powers of the Competent Authority as specified in the *Italian Personal Data Protection Code* is a good model to follow (see: www.dataprotection.it/codice_privacy_english.htm).

5.1.3 Computer misuse legislation

In terms of establishing the legislative, regulatory and policy instruments necessary for the successful implementation of e-government, the third component is computer misuse legislation. The cyber-world, and thus e-government, gives rise to new crimes that are not governed by traditional criminal legislation. The absence of computer misuse legislation will leave a government and citizens vulnerable to e-crimes as they occur.

In designing computer misuse legislation, the following good practices and principles should be taken into consideration:

- The legislation should be technologically neutral, both in terms of the threats it seeks to provide safeguards against, as well in terms of the definition of what constitutes technology. As has been experienced over the past ten years, threats evolve continuously and as rapidly, indeed if not more so, as technology innovation. Seeking to identify types of threats and technologies will increase the risk for continuous amendments to legislation, as new threats and technologies emerge. This will constraint the effectiveness of the legislation and will render its administration cumbersome at best.

- One of the key difficulties with regards to prosecuting a person in relation to a computer crime is that of proving the person's intent to actually commit a crime. Too often, legal actions against computer crime offences fail as a result of this. A potential safeguard against this scenario is to design computer misuse legislation in such a manner that the kernel determining whether a person is guilty of an offence stems from the fact that the person acted 'without authorisation' when the act was carried out. Legislation can be furthered strengthened if the burden of proof to show that a person has acted with/without authorisation is placed on the person accused of the offence. This is the approach that Malta took with regard to its computer misuse provisions.

- However, adopting such an approach demands that the government entity responsible for ICT, or in a decentralised environment each entity that has responsibility for ICT resources, has to adopt a rigorous approach to security policy design and its dissemination. This will ensure, for example, that access to any ICT resources carries a notification that informs users that such access is legal only if the person seeking it is authorised to do so. Access rights and privileges, for example, should be formalised so that an accountability trail is in place. This safeguards persons who have been assigned authorisation and establishes with absolute clarity those who have not been provided with authorisation. It is important to note that the absence of formal security policies and measures would render the task of proving in a court of law that an individual acted without authorisation difficult for the government entity concerned.

It is pertinent to underline that many organisations form protection strategies by focusing solely on infrastructure weaknesses; they fail to establish the effect on their most important information assets. This leads to a gap between an organisations' operational and information technology (IT) requirements, placing the assets at risk. Approaches to information security risk management may be incomplete: they could fail to include all components of risk (assets, threats and vulnerabilities). Thus the planning and implementation of comprehensive and robust information security architecture is of paramount importance in the cyber-world – which e-government defaults into.

Box 5.2 Examples of methodologies relating to information security management

Risk management assessment – OCTAVE

The Operationally Critical Threat, Asset and Vulnerability Evaluation SM (OCTAVE^{SM}) is an approach to information security risk evaluations that is comprehensive, systematic, context-driven and self-directed. The approach is embodied in a set of criteria that define the essential elements of an asset-driven information security risk evaluation. The OCTAVE criteria require the evaluation to be led and performed by a small, interdisciplinary analysis team of the organisation's business and IT personnel. Team members work together to make decisions based on risks to critical information assets. Finally, the OCTAVE criteria require catalogues of information to measure organisational practices, analyse threats and build protection strategies. These catalogues are: (i) catalogue of practices – a collection of good strategic and operational security practices; (ii) generic threat profile – a collection of major sources of threats; and (iii) catalogue of vulnerabilities – a collection of vulnerabilities based on platform and application.

(*Continued*)

Box 5.2 Examples of methodologies relating to information security management (cont.)

OCTAVE-S was developed in response to the needs of smaller organisations (of around 100 people or less). It meets the same criteria as the OCTAVE method, but is adapted to the more limited means and unique constraints of small organisations. OCTAVE-S uses a more streamlined process and different worksheets, but it produces the same type of results. Before you use OCTAVE-S, consider the two primary differences in this version of OCTAVE: (i) OCTAVE-S requires a small team of three to five people who understand the breadth and depth of the company; and (ii) OCTAVE-S includes only a limited exploration of the computing infrastructure. Small companies frequently outsource their IT completely and do not have the ability to run or interpret the results of vulnerability tools.

Information security architecture methodology – SABSA

The Sherwood Applied Business Security Architecture (SABSA) is a model and a methodology for developing risk-driven enterprise information security architectures, and for delivering security infrastructure solutions that support critical business initiatives. The primary characteristic of the SABSA model is that everything must be derived from an analysis of the business requirements for security, especially those in which security has an enabling function through which new business opportunities can be developed and exploited.

The process analyses the business requirements at the outset, and creates a chain of traceability through the strategy and concept, design, implementation and ongoing 'manage and measure' phases of the lifecycle to ensure that the business mandate is preserved. Framework tools created from practical experience further support the whole methodology. The model is layered, with the top layer being the business requirements definition stage. At each lower layer a new level of abstraction and detail is developed, going through the definition of the conceptual architecture, logical services architecture, physical infrastructure architecture and finally at the lowest layer, the selection of technologies and products (component architecture).

The SABSA model itself is generic and can be the starting point for any organisation. However, by going through the process of analysis and decision-making implied by its structure, it becomes specific to the enterprise and is finally highly customised to a unique business model. It becomes in reality the enterprise security architecture, and it is central to the success of a strategic programme of information security management within the organisation.

Information security governance – COBIT

Control Objectives for Information and related Technology (COBIT®) provides good practices across a domain and process framework, and presents activities in a

(Continued)

Box 5.2 Examples of methodologies relating to information security management (cont.)

manageable and logical structure. COBIT's good practices represent the consensus of experts. They are more strongly focused on control, and less on execution. These practices help optimise IT-enabled investments, ensure service delivery and provide a measure against which to judge when things do go wrong. The business orientation of COBIT consists of linking business goals to IT goals, providing metrics and maturity models to measure their achievement, and identifying the associated responsibilities of business and IT process owners. The process focus of COBIT is illustrated by a process model that subdivides IT into 4 domains and 34 processes in line with the responsibility areas of plan, build, run and monitor, providing an end-to-end view of IT. Enterprise architecture concepts help identify the resources essential for process success, i.e., applications, information, infrastructure and people.

COBIT 5, the latest edition of ISACA's globally accepted framework, was set to consolidate and integrate the COBIT 4.1, Val IT 2.0 and Risk IT frameworks and also to draw significantly from the Business Model for Information Security (BMIS) and Information Technology Assurance Framework ITAF (ISACA 2013). At the time of writing, it was perceived that COBIT 5 would be a major strategic improvement providing the next generation of Information Systems Audit and Control Association ISACA's guidance on the enterprise governance of IT. Building on more than 15 years of practical usage and application of COBIT by many enterprises and users from the business, IT, security and assurance communities, COBIT 5 was to be designed to meet the current needs of stakeholders and align with the most up-to-date thinking in enterprise governance and IT management techniques.

5.1.4 Liberalisation of the telecommunications sector

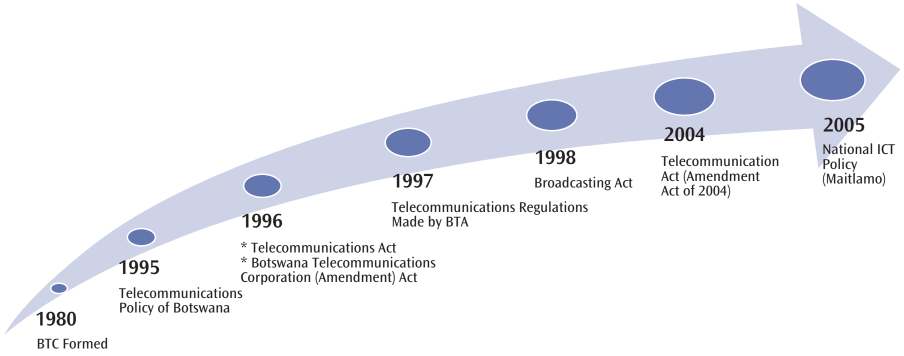
The uptake of internet connectivity by households is directly correlated to the cost – be that through dial-up or broadband connectivity. The cost of access to internet connectivity is, in turn, directly correlated to the liberalisation of the telecommunication process and the state of its maturity. Given this strong correlation, a process of telecommunications liberalisation is one of the first sectoral reforms that will support the implementation of an e-government strategy.

International experience shows that the liberalisation of a country's telecommunications sector results in a lowering, through competition, of user fees to access internet and mobile services. The uptake of e-government can only take place if citizens and entrepreneurs have access to the technology and can afford accessibility to the technology. An environment where technological choice is limited and access to technology is not affordable will result in the failure of the e-government strategy.

Figure 5.1 Telecommunications reform in Botswana: a policy model

Since the mid-1990s, Botswana has pursued a policy of telecommunications liberalisation. This process is considered to be a model worthy of emulation. The participation and protection of domestic telecommunication users, transparency in decision-making, the creation of an independent regulatory agency and the introduction of competition in the form of private mobile phone providers are among those features that are recommended for replication.

Botswana telecommunications liberalisation process:


1980
BTC Formed
1995
Telecommunications Policy of Botswana
1996
* Telecommunications Act
* Botswana Telecommunications Corporation (Amendment) Act
1997
Telecommunications Regulations Made by BTA
1998
Broadcasting Act
2004
Telecommunication Act (Amendment Act of 2004)
2005
National ICT Policy (Maitlamo)

Functions of the Botswana Telecommunications Authority:

(1) The Authority shall supervise and promote the provision of efficient telecommunication services in Botswana.

(2) Without derogating from the generality of the provision of Subsection (1), the Authority shall –

(a) take all reasonable steps to promote the provision, throughout Botswana, of such telecommunication services, as will satisfy all reasonable demands for them including emergency services, public call box services and directory information services;

(b) promote the interests of consumers, purchasers and other users of telecommunication services in respect of the prices charged for, and the quality and variety of, such services and equipment or terminal equipment supplied for the purposes of such services; and

(c) promote and maintain competition among persons engaged in commercial activities for, or in connection with, the provision of telecommunication services, and promote efficiency and economy on the part of persons so engaged.

(3) The Authority shall have, and may exercise and perform, such other powers and functions as may be conferred on it by, or under this or any other Act.

(4) The Board may, in writing, delegate any of the powers and functions of the Authority to the Chief Executive or any other officer of the Authority.

(5) The Minister may, after consultation with the Board, give the Board directions of a general or specific nature regarding the exercise of its powers and the performance of its functions, which directions shall not be inconsistent with this Act or with the contractual or other legal obligations of the Authority, and the Authority shall give effect to any such directions.

(6) Subject to the provisions of Subsection (5), the Authority shall not be subject to the direction of any other person or authority in the exercise of its functions under Parts V, VI, VII and VIII of this Act (see: www.elaws.gov.bw/pr_export.php?id=157).

An immediate first step is the drafting of the enabling act for the setting up of a communications regulator. The legislation should be principle-based and should focus on the roles and responsibilities of the regulatory authority. Legal frameworks for the various telecommunications sectors – fixed telephony, mobile, internet and VoIP (Voice over Internet Protocol) spectrum etc. – should be introduced as subsidiary legislation.

The independence of national regulatory agencies is one of the fundamental underpinnings of successful liberalisation and in achieving competition. Such independence creates the conditions that: are conducive to investment; incentivise new market entrants with the prospect of a level playing field; achieve a stable regulatory landscape; and achieve one that is not susceptible to political whim. In order to foster independence, several formal safeguards have been employed to achieve such a balance (infoDev and ITU 2012). These include:

- Providing the regulator with a distinct statutory authority, free of ministerial control.
- Prescribing well-defined professional criteria for appointments.
- Involving both the executive and the legislative branches of government in the appointment process.
- Appointing regulators (the director general or board/commission members) for a fixed period of time and prohibiting their removal (subject to formal review), except for clearly defined due cause.
- Where a collegiate (board/commission) structure has been chosen, staggering the terms of members so that they can be replaced only gradually by each successive government.
- Providing the agency with a reliable and adequate source of funding. Ideally, charges for specific services or levies on the sector can be used to fund the regulator to insulate it from political interference through the budget process.
- Exempting the regulator from civil service salary limits to attract and retain the best-qualified staff and to ensure adequate good governance incentives.
- Prohibiting the executive from overturning the agency's decisions, except through carefully designed channels – such as new legislation or appeals to the courts based on existing law.

However, sector-specific regulatory expertise is an uncommon commodity at the best of times, and understandably more so in a smaller country. Therefore, government should consider extending a telecommunications regulator's jurisdiction to address sector competition either concurrently, i.e. the two agencies collaborating, or exclusively for the telecommunications regulator to adjudicate on competition matters within its jurisdictional sectors.

Policy mechanisms for both delivering and financing the desired level of service include market-based reforms, mandatory service obligations, leveraging new technologies (e.g. mobile devices), leveraging new business practices (e.g. pre-paid cards), cross-subsidies, access deficit charges and public–private partnerships. Of these, the most successful have been the market-based reforms associated with the liberalisation of the mobile sector, supported by a stable regulatory environment and the subsequent exponential growth in customers in developing countries.

The ICT Regulation Toolkit developed by infoDev in conjunction with ITU is a rich resource for capacity building and could serve as a vital reference in the design of a telecommunications liberalisation strategy (Box 5.3).

Box 5.3 ICT Regulation Toolkit

The toolkit is intended to assist regulators with the design of effective and enabling regulatory frameworks to harness the latest technological and market advances. Its most prevalent themes are the impact of changing technology, the role of competition and the regulatory implications of the transition from traditional telephony to next generation networks. The toolkit incorporates the following modules:

- Regulating the Telecommunications Sector: Overview
- Competition and Price Regulation
- Authorisation of Telecommunications Services
- Universal Access and Services
- Radio Spectrum Management – Legal and Institutional Framework
- New Technologies and Impact on Regulation

Source: infoDev and ITU 2012

5.2 Development of ICT architecture and standards

5.2.1 The provision of electronic mail and internet access to government employees

One immediate first step, if not already achieved, is to provide internet access and an electronic mail (email) account to every employee within a government entity. This will have two pervasive impacts. First, particularly if this is followed by a policy decision that mandates that all communication between entities is to be carried out by electronic mail and documents, it will instil an e-culture among public officers and government employees. A consequential ripple effect is that such a step will also facilitate communications between government entities and external constituents.

Second, given that in small and island states the government is normally the largest employer, the provision of electronic communications and internet access translates into a good step in engendering an information society, as a large proportion of persons in employment would be exposed to ICT.

Such an approach may have a greater impact should the diffusion of ICT within households still be limited. In such a situation, access to electronic communications and the internet from the office or terminals for public officers who are not necessarily deskbound (police officers, teachers, nurses) will initially be the primary gateway to the e-world. The experience of Malta has shown that the adoption of this approach, together with steps taken to increase affordability of computer hardware and internet access would, within a relatively short time, nudge such employees to invest in home connectivity as they recognise the power of the internet in terms of knowledge, information and other opportunities.

5.2.2 Enterprise architecture

The development of the e-government platform should be preceded by an enterprise architecture. An enterprise architecture enables the entity assigned responsibility for implementation to establish a road-map that will allow for optimal performance of the e-government value chain within an efficient, scalable, modular, coherent and interoperable underlying ICT framework.

Simply stated, enterprise architectures are blueprints for systematically and completely defining the current ICT (baseline) or desired (target) environment. Enterprise architectures are, therefore, essential for evolving information systems and developing new systems that optimise their mission value – in this case, a seamless e-government value chain. If defined, maintained and implemented effectively, such institutional blueprints assist in optimising the interdependencies and interrelationships along the e-government value chain and the business operations of the myriad government entities that will be interlocked to it and the underlying ICT framework (US Government 2001).

In general, the essential reasons for developing an enterprise architecture include:

(i) alignment – that is, ensuring that the reality of the implemented enterprise is aligned with management's intent;

(ii) integration – that is, ensuring that the business rules are consistent across the organisation, that the data and its use are immutable, interfaces and information flow are standardised, and the connectivity and interoperability are managed across the enterprise;

(iii) change – that is, facilitating and managing change to any aspect of the enterprise;

(iv) time-to-market – that is, reducing systems development, applications generation, modernisation timeframes and resource requirements; and convergence – that is, striving towards a standard ICT product portfolio (US Government 2001).

There is no single methodology on how an enterprise architecture process should be performed. It is argued that the enterprise architecture process should be fitted to the individual organisation. In fact there are various enterprise architecture frameworks that can be adopted by an organisation – such as the Zachman Enterprise Architecture Framework, the Open Group Architecture Framework (TOGAF) and Service Oriented Architecture (SOA) (see Annex 5.1).

5.2.3 Design of interoperability standards

Unless a government introduces interoperability standards to be adopted by all agencies within the government at the outset, then the e-government strategy will be susceptible to failure. E-government means that government entities need to network with one another, with data seamlessly exchanged between one agency and the others to allow e-services to take effect.

An e-government interoperability framework (e-GIF) is a set of policies, technical standards and guidelines. It covers ways to achieve interoperability of public sector data and information resources, information and communications technology (ICT) and electronic business processes. It enables any agency to join its information, ICT or processes with those of any other agency using a predetermined framework based on 'open' (i.e. non-proprietary) international standards. An e-GIF performs the same function in e-government as the road/highway code does on the roads. Driving would be excessively costly, inefficient and ineffective if road rules had to be agreed each time one vehicle encountered another.

From a technical standpoint, e-government interoperability is achieved when the coherent, electronic exchange of information and services between systems takes place. E-government interoperability relates specifically to the electronic systems that support business processes between agencies, government and people, and government and business.

This does not mean a central agency simply dictating common systems and processes. Interoperability can be achieved by applying a framework of policies, standards and guidelines that leave decisions about specific hardware and software solutions open for individual agencies, or clusters of agencies, to resolve.

An e-GIF will:

- help government agencies to work more easily together electronically;
- make systems, knowledge and experience re-usable from one agency to another;
- reduce the effort needed to deal with government online by encouraging consistency of approach; and

- reduce reliance on tapes and disks to exchange data, as these carry their own security issues and are not scalable for the level of interoperability many services will need in future (New Zealand State Services Commission 2008).

Moreover, the internet and the value it can deliver to government and people, relies on an agreed, standards-based approach. By using the same standards-based approach, agencies support the infrastructure of technologies that they increasingly rely on to deliver services and conduct the business of government. Adopting common standards also helps governments in various jurisdictions to interoperate. This becomes important when dealing with matters that can only be handled on a regional or global basis.

The New Zealand e-Government Interoperability Framework is a good practice model to follow (New Zealand State Services Commission 2008). (For further details on interoperability standards, see Annex 5.2).

Box 5.4 Transition to an e-government interoperability framework: New Zealand

The adoption of the e-GIF must allow for a sensible transition. Recognising this, the New Zealand Cabinet agreed on 13 June 2002 that current information systems, software applications and electronic data/information resources did not need to comply immediately with the e-GIF. However, any new information system, software application and electronic data/information resource (or current instances of these being redeveloped or replaced), along with systems for interfacing with these, must comply with the e-GIF. The only exceptions are:

- if developers are certain that interoperability will never be a requirement; or
- if the current version of the e-GIF does not, and could not, include policies, standards or guidelines concerning the technologies the agency needs (not wants) to employ.

If an agency has one of these exceptional instances, it needs to consider the customer perspective. Although the agency system may have been developed to operate in isolation, New Zealanders may one day need it, transparently or otherwise, to work with other services from other agencies. Is it certain that the new system, application or resource will never need to support or interact with any new, enhanced or replacement system, application, interface, service, process or resource? Experience shows that in most cases, the e-GIF will apply.

The absence of an interoperability framework will most likely result in a situation where agencies introduce e-services independently of one another. The likelihood is that, in striving to introduce their respective e-services, they will adopt their own sets of standards. In the event that this happens, then interoperability would require expensive retrofitting to be achieved. This is an unnecessary and unwarranted financial cost that should be avoided.

5.2.4 Development of a government central portal

An unco-ordinated approach towards the introduction of websites across government entities may complement difficulties in tracking down the right organisation for the right services that prevails today with regard to traditional service delivery. The interface between the public and the e-government world must be seamless to the greatest extent possible by establishing a clear, simple, and transparent gateway for the user. The best way to achieve this is to design a central portal, owned by the entity responsible for e-government initiatives, which provides the user with electronic access to both entities and services. Services can be shown individually or designed around a cluster to facilitate the search for the appropriate service. One particular methodology is to design the clusters around a person's life journey: health; education; employment; leisure; family affairs etc.

The immediate visible impact in terms of the scale of activity being adopted by the government in rendering basic e-services available to the polity is considerable. Initially, such an approach will only meet the first phase of the e-government pathway, discussed in Chapter 1, in that it will provide information to the public and establish an electronic channel between the public and with each and every entity within government.

Too often, focus is directed towards launching a website as against managing the website once it is launched. Too often, websites remain static and electronic communication channelled through them fails to receive the same level of attention as conventional mail communication. A static website is a strong negative signal of the fact that an e-culture has not taken root within the organisation responsible for it. Static websites can only become dynamic if they are managed.

Furthermore, the e-government platform should, from the outset, ensure that no part of society is marginalised in the e-environment as a result of access being hindered due to language barriers. Thus, all e-services should be designed on a bi- or multi-language platform to secure full accessibility.

5.2.5 Transactions and e-services

In tandem with the introduction of a government website, each government entity should review its forms and place each form for electronic access through the website. This provides an excellent channel for the end user to be able to interact electronically with the government entity without the need to physically obtain the forms from the relevant organisation.

The design implementation of important e-government sub projects that can be carried out in the immediate and short term track of e-government activities that includes ‘throw away’ solutions provides an excellent way forward in balancing, on the one hand, the time required to introduce a robust e-government platform and, on the other, the need to mobilise fast to create a sustainable momentum and credibility in the initiative.

Transactional e-services are the trigger for an electronic service without any physical intervention. The short-term track should provide a series of transactional solutions. It is these solutions that will demonstrate the true revolution of e-government. In adopting transactional e-services in the short-term track, there should be upfront recognition that to a large extent this will be a ‘throw away’ investment.

In identifying transactional short-term e-services for the short-term track, the following considerations should be taken into account:

- Identification of existing back-end applications that with investment of a level of effort can allow for web-enabled services – either in terms of adding a front-end or by appropriate modification.
- Identification of payment-based transaction services that can be designed through a temporary e-payment services provider.
- Identification of service-related applications that impact a wide cross-section of audiences, as against sectoral-based audiences in so far as this is possible.
- Identification of transactional e-services that are of minimum risk. It is pertinent to underline that an over-ambitious service that has a high level of risk may result in a potential fall-out, which could jeopardise the entire e-government strategy if it goes wrong.

In the long-term, the e-government platform should be:

- Able to cope with a variety of channels.
- Capable of providing access to all government back-end services from all delivery channels.
- Structured to accommodate different back-office requirements.
- Based on proven, widely available and used technology.
- Scalable to accommodate growing and changing usage requirements with cheap incremental increases in size.
- Equipped to handle digital authorisation.
- Capable of handling unpredictable volumes of traffic.
- Capable of handling an m-government gateway.
- Capable of handling an e-payment gateway.

The e-government platform should be flexible, scalable and modular, based on a three-tier architecture designed to integrate new delivery channels and add new e-services with minimal additional investment (Figure 5.2).

A three-tier architecture should be used to insulate the access channels from the complexity of the government back office, with web technology providing the portal or gateway between the channels and the individual service requested. The key concept of the three-tier architecture is the use of middleware technology to provide a brokerage capability. The middleware will link components to allow them to interact without the need to have knowledge of the other component's location, hardware platform or implementation technology.

5.2.6 The need for redundancy and consolidation[1]

Thus, the e-government platform must be designed around full redundancy (that is the provision of additional or duplicate aspects of equipment that will function in case an operating part of system fails) architecture at, at least, three end points. First, a country should ensure that its telecommunications provider/s, either within a monopolistic or liberalised environment, have in place two different entry points from two different international service providers. This will ensure that, in the event that one of the entry points suffers damage – for example an underwater cable being torn by a trawler – connectivity will continue to be provided through the second entry route.

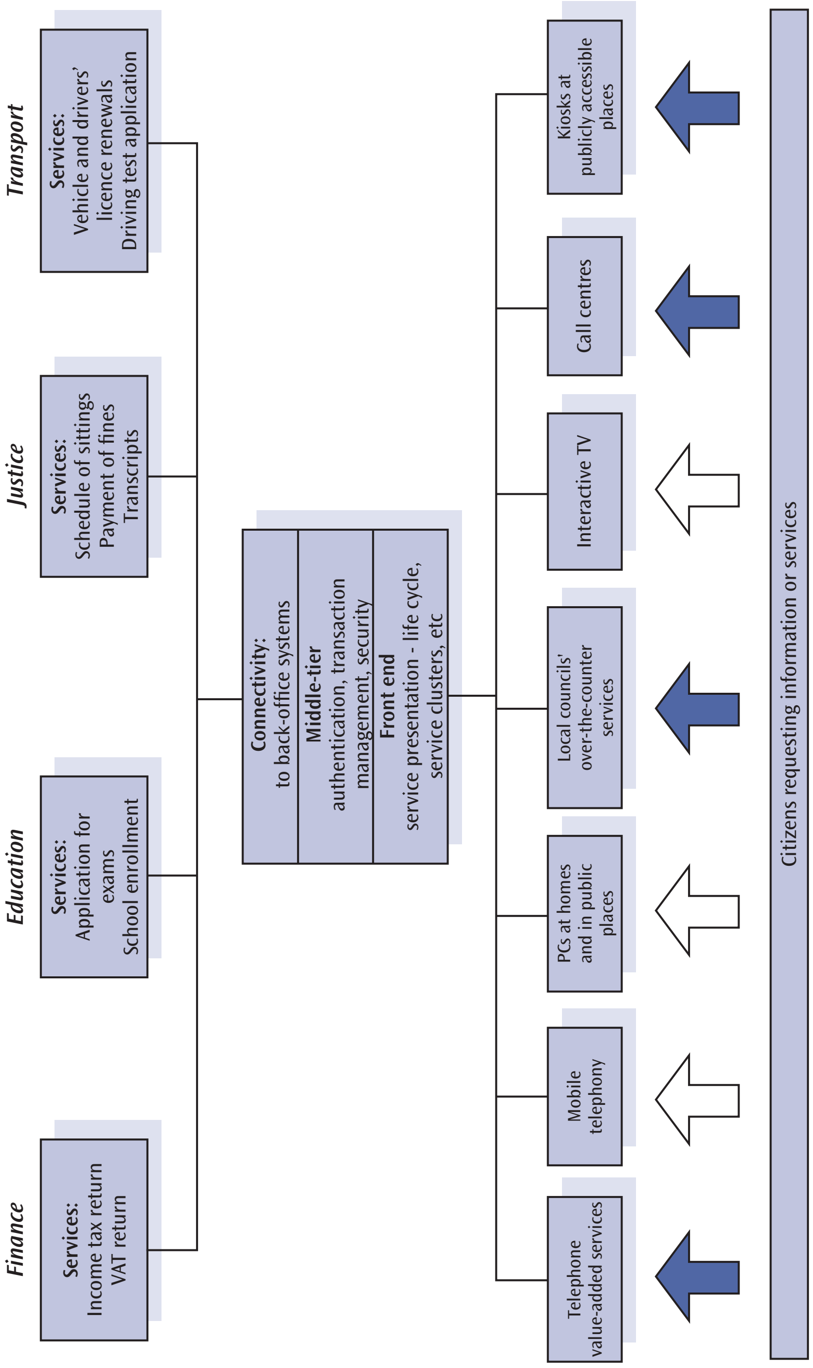
Second, the country should ensure that local connectivity from the international connectivity gateway(s) to the data centre wherein the e-government technology infrastructure is sited, accesses the location from two different end points, and ideally from two different service providers.

Third, the economics of today's information technology have changed. The cost of technology has fallen, while the costs of licences and skilled labour have increased. Thus, the economics of information technology render a centralised and consolidated IT data centre cost effective, as the total cost of ownership is much cheaper than running a fragmented data centre environment in which centres are set up in key ministries and departments.

Data centres have ancillary costs – air-conditioning equipment, back-up generators, fire systems, monitoring tools etc. – which if replicated in every data centre created, will render the cost of operations prohibitive. Moreover, a fragmented data centre approach will increase the investment required considerably to ensure redundancy and, therefore, continuity of service in the event of planned or unplanned downtime.

Thus, the actual e-government platform should be fully redundant and designed on an 'Active–Active' basis, so that downtime on one particular part of the technology would allow the other redundant part to secure continued service provision without providing any denial of service outage.

Figure 5.2 Conceptual model of a three-tier e-government architecture


Finance
Services:
Income tax return
VAT return
Education
Services:
Application for exams
School enrollment
Justice
Services:
Schedule of sittings
Payment of fines
Transcripts
Transport
Services:
Vehicle and drivers' licence renewals
Driving test application
Connectivity:
to back-office systems
Middle-tier
authentication, transaction management, security
Front end
service presentation - life cycle, service clusters, etc
Telephone value-added services
Mobile telephony
PCs at homes and in public places
Local councils' over-the-counter services
Interactive TV
Call centres
Kiosks at publicly accessible places
Citizens requesting information or services

5.3 ICT infrastructure

The level of existing infrastructure also affects a country's ability to enable users to connect to the internet. The procurement and laying of dark fibre is expensive, although new technologies such as optical fibre have reduced the cost of laying fibre over short distances. Invariably, internet users are more likely to start taking root within urban communities.

Access to the internet can also be provided through satellites, particularly low earth orbit or geostationary satellites. Nevertheless, depending on the regions, different types of satellite systems have a wide range of different features and technical limitations, which can greatly affect usefulness and performance in specific applications.

5.3.1 Kiosks

In the early stages of the e-government implementation process, particularly while the telecommunication liberalisation process is in transition, the price to internet access will act as a hurdle for particular cohorts of the population to access e-services. This can be mitigated by low-cost delivery measures. These include:

- the establishment of internet kiosks in popular sites such as supermarkets, squares etc.;
- the establishment of internet kiosks in rural communities; and
- the placement of computer terminals with full internet access in town, village and rural schools and libraries.

In adopting such low-cost delivery measures, the government entity responsible for e-government implementation should seek strategic partnerships with private industry and telecommunications transport providers to finance, in part or in whole, the hardware and the cost of connectivity.

Experience shows that the introduction of such internet kiosks during the early stages of the implementation of e-government is a strategic action given that, at this stage of the implementation, access to and affordability of the internet may limit the up-take of e-government. Thus, the presence of internet kiosks at the stage when the implementation of the e-government strategy may be at its most vulnerable, may act as valuable channel in enabling access and in nurturing an information society.

Box 5.5 Setting up a multi-facility centre at a weekly marketplace in India

In its efforts to test its method for bringing ICTs to remote communities, Satpura Integrated Rural Development Institution (SIRDI) established a multi-facility centre at a weekly marketplace in Sawalmendha. Thousands of people from the surrounding 68 villages visit the market every week to purchase essential products and conduct routine work. SIRDI set up similar centres in Taluka Town, Bhainsdehi and the district town of Betul, and established a communication network between these villages and Sawalmendha.

The project addressed both technical and social issues. From a technical perspective, the main issues were to test how ICTs can be made to work in remote areas with limited infrastructure. Computers and other instruments were tested in harsh conditions and did not break down. Telephone lines were unreliable, however, and it took several months to activate the internet connection. In addition, the power supply in the state of Madhya Pradesh was limited. Electricity was available between four and eight hours per day, which was insufficient to charge the batteries of the uninterrupted power supply (UPS) and inverters. Hence, the generator backup planned as part of the project proved useful.

From a social perspective, the project sought to test whether weekly markets can provide a 'door-step' for access to ICTs, to assess the impact of the use of ICTs on tribal communities and understand the social and psychological factors that influence use or non-use of ICTs. The project noted that because of the beneficiaries' low literacy rate and general lack of awareness about ICTs, the community could not really benefit on a large scale during the short project period. It was also noted that response from villages was much healthier in those villages where SIRDI had already been working, and where social workers were already based. During the later stages of the project, local youth started taking interest in the activities of the centre and in learning internet technology skills. The percentage of requests for help submitted by women remained consistent throughout the project period at about 35 per cent.

5.3.2 National internet exchange

An administration should also consider creating a national internet exchange (NIE), particularly in the early stages of the development of the information society, in order to eliminate the situation where local traffic traverses costly international links and where one of the gateway providers may end up having a monopoly on the international gateway and internet exchange. If such a situation arises, connectivity to the internet will be expensive due to the relatively high costs of international data circuits.

The lack of a local interconnection scheme will mean that an email sent from one subscriber in the country to another will have to traverse through such costly links.

Moreover, it is also highly likely that the bandwidth on these international lines will be heavily over-subscribed, since such bandwidths are expensive and may be over-utilised. This in turn will result in poor and slow performance to access local sites – including the e-government platform.

The creation of a NIE provides a designated central exchange point, which prevents local traffic having to traverse costly international links. A national exchange independent of any gateway operator would also benefit from complete autonomy. Otherwise the situation may arise, with the advent of multiple international data gateway operators as the telecommunications sector matures, where one of the gateway providers is also responsible for managing an internet exchange.

5.3.3 Call centre provision of e-services

An e-government strategy that bases its delivery channels uniquely on the internet may discriminate against cohorts of the population who are not technology savvy and/or cannot afford or do not have access to technology. Nonetheless, most small and island states have a large penetration of fixed-line telephony. Although fixed-line technology as a delivery channel for e-services is often forgotten or introduced as an afterthought, it constitutes a highly effective way for the provision of e-services.

There are two ways in which an e-service can be provided through a fixed-line delivery channel. The first is where the user interacts with a call centre for the activation of an e-service transaction. In essence, the user contacts a call centre and, following identification, the call centre will activate the particular e-service transaction. In this case, a human 'air bubble' interface is created where the call centre agent acts as an intermediary on behalf of the user. The second is where the user interacts with a voice automated e-service transaction delivery channel, which is activated following user identification through a fixed-line call.

5.3.4 M-government

Moreover, the application of m-government – that is, the provision of e-services through mobile telephony – can be an extremely effective way to roll out e-government. This is particularly the case with 'push down' e-services, whereby a citizen may require a service without the need to transact back with the government agency service provider.

For example, m-services can be quickly introduced for the dissemination of information relating to weather changes in zones that may susceptible to quick climatic changes, the provision of weather forecasts to farmers in rural villages, the provision of health education etc.

M-government should be a strategic component in the design and implementation of an e-government platform, as it is far more cost effective to deploy than fixed telephone lines or fibre. This is particularly the case in countries where core infrastructure is limited to the capital city and large towns, because the penetration of mobile telephony is far more likely to be universal than internet connectivity. M-government increases the tempo of e-/m-services interaction uptake and the attainment of an information society. M-government is explored further in the following chapter.

5.4 Conclusion

The implementation of e-government strategies will take time. Laws take time to draft and the process leading up to the liberalisation of telecommunications infrastructure is complex, taking years before the full effects of a competitive market come into play. Investments in the ICT capacities of the population also bring change slowly.

As with any other policy instruments, the pressure for delivery by both the political administration and the polity at large will be extremely high. A five-year delivery strategy does not fit within the political agenda of parties in government. What is more, experience shows that implementation of policy instruments that have a long timespan before delivery becomes demonstrable will lose impetus and political support, as attention will start to move towards other policy initiatives and changes in the socio-economic environment.

Both the strategy design and the process of e-government implementation will be modular in form and incremental in terms of implementation. The strategy, and future iterations of the strategy over the generational horizon, will ensure consistency and coherency as the process of e-government implementation proceeds over time.

Annex 5.1 Enterprise architecture frameworks

Zachman Enterprise Architecture Framework (EAF)

John Zachman is regarded as the person who introduced the idea of 'Information System Architecture' (ISA). He considered information system design by analogy to the work steps and the representations of the classical architect and producers of complex engineering products. When developing an IT system, it is obvious that many parties are involved. Business people have business requirements, which should be translated into ICT requirements and next be transformed into a combination of software and hardware that fulfils those requirements.

It is to be noted that Zachman EAF is not an information system architecture, but a set of such architectures. The Zachman EAF relies on the fact that architecture is relative to the perspective from which one looks at it, and to the question that is in mind when drawing the architecture. As such, the EAF presents two dimensions. The first dimension concerns the different perspectives of the different participants in the systems development process. The second dimension deals with the six basic English questions: what, how, where, who, when and why.

The Open Group Architecture Framework (TOGAF)

TOGAF is open standard, is governed by the OpenGroup and is not aligned with any technology or vendor. TOGAF is based on the US Department of Defence 'Technical Architecture for Information Management'. The first version was released in 1995 and it is currently at Version 9. It is directed to enable the design, evaluation and building of the right architecture for an organisation. There are four subset types of architecture in TOGAF: (i) the business (or business process) architecture – this defines the business strategy, governance, organisation and key business processes; (ii) the applications architecture – this kind of architecture provides a blueprint for the individual application systems to be deployed, their interactions and their relationships to the core business processes of the organisation; (iii) the data architecture – this describes the structure of an organisation's logical and physical data assets and data management resources; and (iv) the technology architecture – this describes the software infrastructure intended to support the deployment of core, mission-critical applications. This type of software is sometimes referred to as 'middleware'.

TOGAF has three key parts. First, the Architecture Development Method (ADM) – a series of phases which broadly outline the steps required to design and implement a typical IT solution. These range from initial concept through design, implementation and change management. Second, the Enterprise Continuum – assets that originate from the ADM and established industry standards (HTML, compliance, etc.). Third, the Resource Base – tools used to support the ADM cycle. These would include any architecture software systems used to manage the TOGAF process.

Service Oriented Architecture

The widespread emergence of the internet in the mid-1990s as a platform for electronic data distribution, along with the advent of structured information, revolutionised the ability to deliver information to any corner of the world. While the introduction of Extensible Mark-up Language (XML) as a structured format was a major enabling factor, the promise offered by SOAP- based web services (see Annex 5.2) triggered the discovery of architectural patterns that are now known as Service Oriented Architecture (SOA). Service Oriented Architecture is an architectural paradigm and discipline that may be used to build infrastructures enabling those with needs (consumers) and those with capabilities (providers) to interact via services across disparate domains of technology and ownership. Services act as the core facilitator of electronic data interchanges yet require additional mechanisms in order to function. Several new trends in the computer industry rely upon SOA as the enabling foundation. These include the automation of Business Process Management (BPM), composite applications (applications that aggregate multiple services to function) and the multitude of new architecture and design patterns generally referred to as Web 2.0.

Annex 5.2 Securing government interoperability[2]

Security

Security is critical for the success of e-government, as it enables trust and confidence in its services. In securing e-government, one must ensure data confidentiality, data integrity, citizen identification and non-repudiation. Thus, e-government raises transaction security concerns. The success of e-government, therefore, depends on the capability to guarantee that the transaction environment is available, reliable and secure.

A security framework for e-government can be categorised into three areas:

(i) Citizen authentication and authorisation. This ensures citizen identification and non-repudiation.

(ii) Transaction transport security. This incorporates methods for securing data during transition to ensure data confidentiality and integrity.

(iii) Business continuity. These are the methods directed to ensure that the service is available even in the event of a non-planned shutdown.

Citizen authentication is the process of verifying and confirming the identity of the person accessing data or services. Authorisation is the process of allowing access to the data or services, controlled by the individual's access levels. Within an e-government framework, the users who will be using the services offered via the portal can assume one, or a combination, of the following three roles:

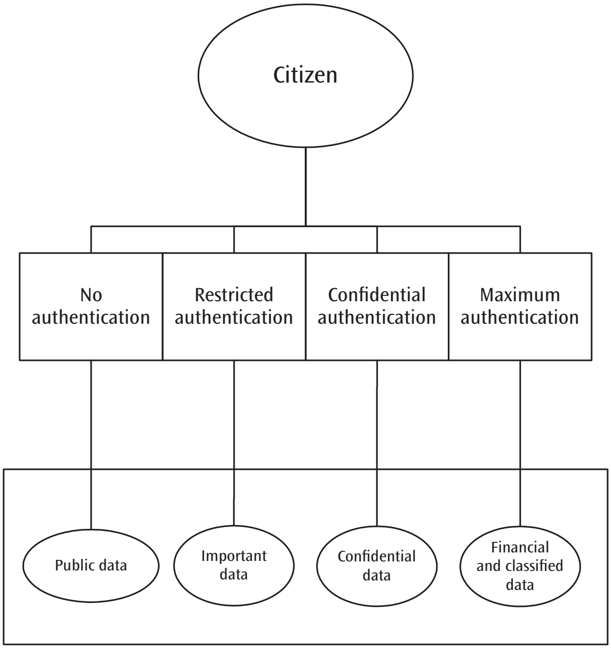
- **Individual**: An individual can access data or services on his or her own behalf.
- **Agent**: An agent is an individual or organisation that can access data or services on behalf of another individual/s or organisation/s provided that consent is granted to the agent by the data subject (individual or organisation).
- **Organisational representative**: An organisational representative is an individual that can access data or services on behalf of an organisation(s) provided that consent is granted to the data subject (representative by the organisation).

The data and services to which an individual has access at any time while assuming any of the roles listed above will be determined by his or her profile, which will be maintained by a directory service. In view of this, and the nature of the data and services being offered within e-government, a four-level authentication model can be established (Figure 5.3). Different authentication levels will allow different user roles to access different services.

Table 5.1 Example of a four-tier authentication framework

No authentication	Data or services intended for the general public. No authentication should be required.	Viewing of an electronic document of a legislation
Restricted authentication	Documents or services of certain importance. A low level of authentication will be required to protect against misuse or loss (i.e. password).	Viewing of status of a particular court case
Confidential authentication	Personal documents or services affecting personal data. A higher level of authentication may be required to protect against significant problems or losses (i.e. password and pin code).	Viewing of social security benefits
Maximum authentication	Strictly confidential personal data or financial transactions. Full authentication may be required to protect personal safety and/or prevent considerable financial loss (i.e. digital certification).	Viewing personal medical records

Figure 5.3 Four-level authentication model



As data or personal information is passed from one entity to another via a medium, there is always the risk that this data is intercepted. Consequently, it may be stolen, misused, modified or denied (non-repudiation). This means that the confidentiality and integrity of the data will be jeopardised. As importantly, it may undermine trust and confidence in e-government.

Nevertheless, the level of security applied should reflect the degree of risk faced. The full approach of a digital certificate-based e-government security framework will be expensive to attain – both in terms of putting into place the appropriate technology and the procurement of necessary digital certificates, and also in the management and administration of the digital certificates.

Given the costs that would need to be financed balanced against the level of risk, the protection of the first three layers of the authentication model discussed above will constitute a high level of unnecessary engineering.

Thus, in tandem with the identification of the authentication model that one wishes to adopt, it is argued that it is of equal importance to determine the level of security to be applied for each e-service introduced. A digital certification security framework should be adopted only when the level of risk demands that the full protection armoury is to be applied, and always with regards to the use of sensitive personal data – such as health personal data.

Data interchange

Extensible Markup Language (XML) is a meta-language designed to create tags to define, transit, validate and interpret data. The use of XML-enabled middleware simplifies the development of data access components, especially when the number of data sources involved in data interchange increases

When the use of such middleware is deemed appropriate, systems should be designed with the use of these products in mind. The use of middleware conditions how data access components are designed and if a middleware product is introduced after a system is designed and developed, the data access components would need to be retrofitted – which would require unnecessary additional cost.

The purpose of an XML schema is to define and describe a class of XML documents by using the following constructs to constrain and document the meaning, usage and relationships of their constituent parts:

Data types Provide for primitive data typing, including byte, date, integer, sequence etc.

Entities An XML document may consist of one or many storage units, called entities. They all have content and are all identified by name.

Elements An element can contain text, other elements, a mixture of text and elements, or nothing at all.

Attributes Attributes are used to assign values to elements, including default values.

Notations Notations identify by name the format of certain entities and elements, or the application to which a processing instruction is addressed.

Schema constructs may also provide for the specification of implicit information, such as default values. Schemas document their own meaning, usage and function. Thus, the XML schema language can be used to define, describe and catalogue XML vocabularies for classes of XML documents, sometimes referred to as 'instance documents'.

The following usage scenarios describe XML applications that should benefit from XML schemas. They represent a wide range of activities and needs that are representative of the problem space to be addressed. They are designed for use during the development of XML schemas, as design cases that should be reviewed when critical decisions are made.

1. **Publishing:** Distribution of information through publishing services. Involves collections of XML documents with complex relations among them. Structural schemas describe the properties of headlines, news stories, thumbnail images, cross-references etc.

2. **Electronic commerce transaction processing:** Libraries of schemas to define business transactions within markets and between parties. A schema-aware processor is used to validate a business document and to provide access to its information set.

3. **Supervisory control and data acquisition:** The management and use of network devices involves the exchange of data and control messages. Schemas can be used by a server to ensure the validity of outgoing messages, or by the client to allow it to determine what part of a message it understands. In a multi-vendor environment, the server discriminates data governed by different schemas (industry-standard, vendor-specific) and knows when it is safe to ignore information not understood and when an error should be raised instead. Applications include media devices, security systems and process control.

4. **Traditional document authoring and editing governed by schema constraints**: One important class of application uses a schema definition to guide an author in the development of documents. A simple example might be a memo, whereas a more sophisticated example is a complex request form. The application can ensure that the author always knows what to enter, and might even ensure that the data entered is valid.

5. **Query formulation and optimisation:** A query interface inspects XML schemas to guide a user in the formulation of queries. Any given database can emit a schema of itself to inform other systems what can be considered as legitimate and useful queries.

6. **Open and uniform transfer of data between applications and databases:** XML has become a widely used format for encoding data (including metadata and control data) for exchange between loosely coupled applications. The representation of the data exchange by XML schema definitions simplifies the task of mapping the data exchange to and from application internal data models.

7. **Metadata interchange:** There is growing interest in the interchange of metadata (especially for databases) and the use of metadata registries to facilitate interoperability of database design as well as DBMS (data base management system), query, user interface, data warehousing and report generation tools.

Common government-wide business functions which make use of commonly used data should be encapsulated into business logic components that are common to all applications. This will facilitate the provision of integrated government services. For these components to be used to their maximum benefit, this exercise should be complemented by the production of XML-based data schemas relating to these common business functions.

These can be reused throughout government applications to reduce the costs and risks of developing data interchange systems. It is these common business functions which should be considered first for production of XML schemas.

Data architecture standards regarding the structure of the ‘Person’ and ‘Address’ entities, together with the validation rules that must be applied, should be designed within XML schemas. The design of such generic standards will enable enhanced data integration and exchange facilities through the use of agreed naming conventions and a mandatory record structure for the common data administration elements required in all data entities across all classifications.

This will result in a standardised data framework that will cut across all the administrative, corporate and function/service-specific data layers. Such a data architecture framework is intended to ensure that every item of data can be traced back to its author, the date and time, together with the business process triggering the update.

It will also create a standard security and access levels mechanism that can be used to filter records or individual attributes according to the authorisation held by the user. At the content level, other entities will be added to the government information-sharing platform where the data falls under public domain and the use of such data is considered critical for application integration purposes.

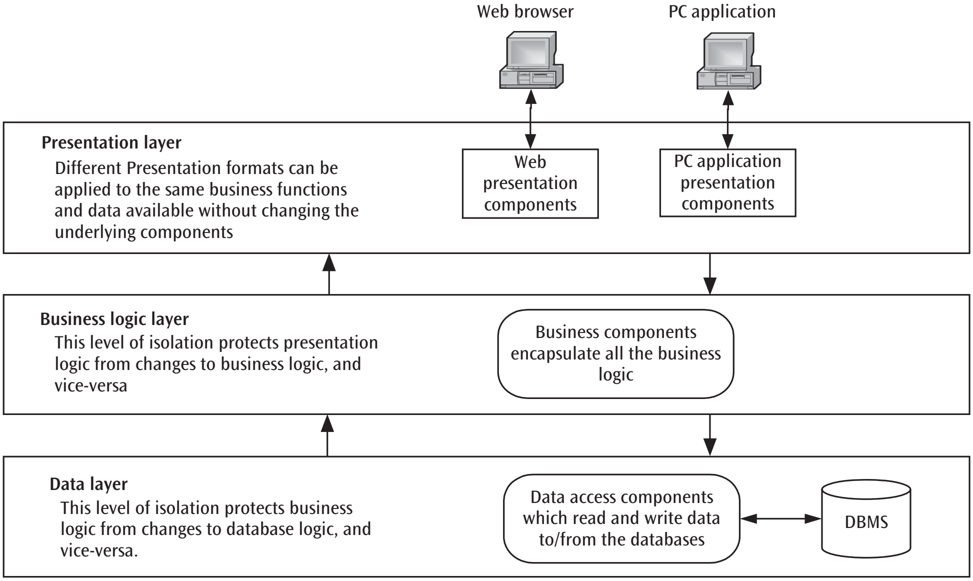
Component coupling and cohesion

Coupling refers to the way data is exchanged between components. Loose coupling is generally better than tight coupling. The loosest, and therefore preferred, type of coupling is data coupling, where data is transferred as parameters via well-defined interfaces. The tightest, or least desirable, coupling involves components directly referencing shared variables. Tight coupling often indicates that components are not insulated from one another, and are not designed to be separate and independent. Tightly coupled components are usually complex, difficult to maintain and monolithic. As a result there is very little flexibility regarding physical distribution of components. Two applications that communicate with each other via message queues, but which are otherwise independent of each other, would be considered loosely coupled.

Cohesion reflects the degree to which one component implements one function or a group of similar functions. For example, cohesive components do not implement multiple, disparate services, such as presentation and application logic. Highly cohesive components are typically more understandable and thus easier to maintain. Additionally, cohesion promotes logical and physical software distribution flexibility which, in turn, promotes system scalability. An application composed of logically separate presentation, application and data management components would be considered highly cohesive.

Software coupling and cohesion directly affect software modularity and interface design. As a result, coupling and cohesion directly affect the flexibility and complexity of software architectures. For example, when software component interfaces are based on widely accepted standards, as illustrated in Figure 5.4, logical software tiers can promote component interoperability and substitutability. That is, logical tiers can allow components within one tier to be changed without affecting other tiers.

Figure 5.4 Use of components in a typical three-tier architecture


Web browser
PC application
Presentation layer
Different Presentation formats can be applied to the same business functions and data available without changing the underlying components
Web presentation components
PC application presentation components
Business logic layer
This level of isolation protects presentation logic from changes to business logic, and vice-versa
Business components encapsulate all the business logic
Data layer
This level of isolation protects business logic from changes to database logic, and vice-versa.
Data access components which read and write data to/from the databases
DBMS

Message queuing

Message queuing enables distributed applications to reliably exchange mission-critical data regardless of hardware, operating system or available connectivity. Message queuing is roughly analogous to an email system. When an email message is sent, the note is addressed and sent to the intended recipients. One is not usually concerned about the underlying delivery route of the email message or when the recipients pick it up. Likewise, one can log into an email server and pick up messages at his or her discretion without maintaining a direct link with those who have sent the email.

Message queuing works in much the same manner as an email system, except that applications (not people) are sending data (not notes). Like email, the sending application does not have to be concerned about delivery routes or when the receiving application will pick up the message. The receiving application can pick up new messages whenever it is appropriate, without necessarily maintaining a direct link with the sending application.

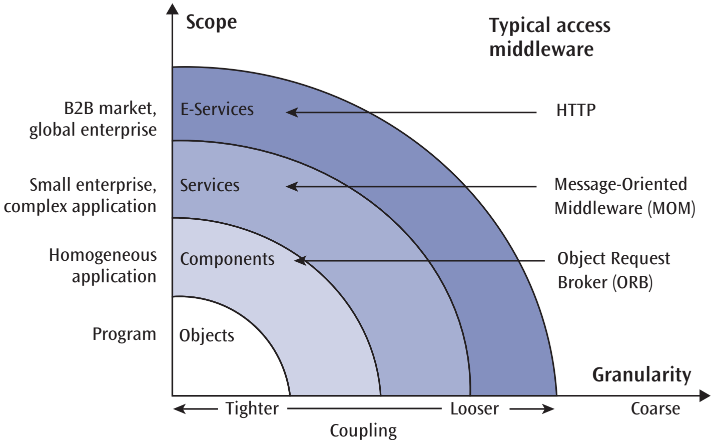
Objects, components, services and e-services

The scene of application development has seen a transition of its design and development paradigms, from objects to components and, more recently, services and e-services. However, each remains a valid development solution, having benefits to give in different circumstances.

The design and development of systems should have, as their main focus, the provision of services. Service Oriented Architecture (SOA) has emerged as the best practice for systematic logical design of applications, offering greater reuse and more access to the business functions, or logical services, of the application from other applications. SOA is a logical architecture where definitive business functions of the application are exposed for programmatic access via a well-defined formal interface, with some means of identifying and locating the function and the interface when it is needed. SOA can be implemented both via a tightly coupled request/reply model and via a loosely coupled messaging model. It has also been implemented using either an object request broker (ORB) or messaging middleware. However, SOA services are typically intended for external (heterogeneous) access. Thus, the messaging model or messaging middleware are typically preferred for their implementation.

Each of these four programming styles may use either a tight or a loose coupling model. However, farther out along the x-axis (Figure 5.5), the link between programs typically becomes looser and the use of the loosely coupled messaging model and the messaging middleware become more beneficial. Conversely, if closer to the root of the diagram, it is more beneficial to use a tightly coupled request/reply programming model and ORB-style middleware.

Figure 5.5 Gartner development models for e-government services


Scope
Typical access middleware
B2B market, global enterprise
E-Services
HTTP
Small enterprise, complex application
Services
Message-Oriented Middleware (MOM)
Homogeneous application
Components
Object Request Broker (ORB)
Program
Objects
Granularity
Tighter
Looser
Coarse
Coupling

a) Objects

Objects are a natural evolution of the best programming practice: modularity. Long before object-oriented (OO) programming became mainstream, software engineers developed subroutines, Input/Output (I/O) modules and included files to encapsulate some of the application logic for reuse across the application or across applications.

The OO style of modularity is now mainstream. Most new applications are developed, at least in part, with the use of an OO programming platform (Java, C++ and Visual Basic). However, an object's scope of visibility is limited to the internal resources of a program, where it is instantiated. Object methods are invoked only from inside the program. Objects are incorporated inside the executable program so that the calling program and the object are more than tightly coupled, they are one.

b) Components

Scalable applications must be able to run across different servers. Thus, some of the methods may have to be invoked remotely. The caller and the server cannot be one in this case. To support remote invocation of object methods, the industry had invented ORBs. These programs, accessed via an ORB, are components.

The purpose of an ORB is to allow remote access to an object method with as little intrusion on the program or the programming model as possible. Thus, components are typically used in a tightly coupled, request/reply environment. This applies to all currently relevant component models, i.e., Distributed Component Object Model (DCOM), Common Object Request Broker Architecture (CORBA) and Java Remote Method Invocation (RMI).

The scope of components is bigger than that of objects, because they are visible to the remote programs. Many object methods are typically invoked on behalf of a single, remote procedure call (RPC). Components do not replace objects, but rather are built on top of them and component specifications are likely to support both the tightly coupled and the loosely coupled programming models.

It is a reality in application development that parts of applications will need to be rewritten because of changing requirements, legislation, changes in government policies etc. It is therefore very important to design components with business logic being kept separate from data access.

c) Services

Services represent definitive published business functions of an application. They can be implemented using a tightly coupled request/reply programming model or a loosely coupled messaging programming model. Tightly coupled services operate just like components, but are published to a target audience potentially consisting of heterogeneous client platforms.

The loosely coupled services are designed differently, using the messaging model. Messaging is the preferred model for services, given that they are typically invoked from other applications. The greater the degree of heterogeneity, the more likely that a loosely coupled model would work better. Loosely coupled services are designed to operate independently of their callers. The corresponding applications may run on different machines, on different application platforms and in different geographical regions.

d) e-Services

Business-to-business (B2B) interactions have become very important in today's information economies, in which both the business and technology differences are greater, the distances are longer and the possibilities for any co-ordination are further reduced.

Here, the program topology is likely to be loosely coupled in most cases. Enterprises are also not likely to have available the same proprietary messaging middleware. Thus, services offered across enterprises will tend to rely on existing messaging middleware and a standard method for formatting messages. Typically, this will be Extensible Markup Language (XML) messaging over HTTP or SMTP transports.

E-services are services deployed over a universal internet transport in an internet-standard format, such as XML over HTTP. Technically, any service may be converted to an e-service by routing it over HTTP and arranging the messages into an XML schema. Logically, however, e-services represent a separate domain of functional content, intended, authorised and advertised specifically for B2B access.

e) Simple Object Access Protocol (SOAP)

Simple Object Access Protocol (SOAP) allows the exchange of information in a decentralised, distributed environment using XML, making it usable in a large variety of systems, ranging from messaging systems to remote procedure calls (RPC). SOAP facilitates interoperability among a wide range of programs and platforms, making applications accessible to a broader range of users. It also combines the proven web technology of HTTP with the flexibility and extensibility of XML. Existing applications would need to be modified to accommodate this.

f) Universal Description, Discovery and integration (UDDI)

A 'web service' is a specific business functionality exposed by a company through an internet connection, for the purpose of providing a way for a third party to use the service. The Universal Description, Discovery and Integration (UDDI) specifications define a way to publish and discover information about web services. UDDI takes an approach that relies upon a distributed registry of businesses and their service descriptions implemented in a common XML format. Programs and programmers use the UDDI Business Registry to locate information about services and, in the case of programmers, to prepare systems that are compatible with advertised web services or to describe their own web services for others to call.

Notes

[1] See CIMU 2000a.

[2] Malta Information Technology and Training Services Ltd 2005.

References

Australian Government (1999), *Electronic Transactions Act 1999*, available at: www.comlaw.gov.au/Details/C2011C00445 (accessed 17 April 2013).

Central Information Management Unit (CIMU) (2000a), 'White Paper on the Vision and Strategy for e-Government', Office of the Prime Minister, Malta, October.

CIMU (2000b), 'White Paper on the Legislative Framework for Information Practices', Office of the Prime Minister, Malta, May.

EU (1995), 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Communities, No 281/31, 23/11/95, available at: http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf (accessed 17 April 2013).

Germanakos, P, G Samaras and E Christodoulou (2004), 'Multi-channel delivery of services – the road from e-Government to m-Government: Further technological challenges and implications,' available at: http://www2.media.uoa.gr/~pgerman/publications/published_papers/Multi-Channel_Delivery_of_eServices_from_eGovt_to_mGovt.pdf (accessed 17 April 2013).

Government of Malta (2002), *Chapter 426: Electronic Commerce Act*, 10 May 2002, available at: http://intranet.stmartins.edu/courses/cis323/Resources/chapt426.pdf (accessed 17 April 2013).

Government of Sweden (1998), *Personal Data Act (1994:204)*, available at: www.sweden.gov.se/content/1/c6/01/55/42/b451922d.pdf (accessed 17 April 2013).

infoDev and ITU (2012), *Accountability, Transparency and Predictability*, ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org/en/Documents.html (accessed 17 April 2013).

ISACA (2013), 'COBIT 5: A Business Framework for the Governance and Management of Enterprise IT', available at: www.isaca.org/COBIT/Pages/default.aspx (accessed 17 April 2013).

Malta Information Technology and Training Services Ltd. (2005), 'Interoperability Framework for e-Government', Office of the Prime Minister, Malta.

McCormick, KP (2013), 'Telecommunications Reform in Botswana: A Policy Model for African States', available at: www.sciencedirect.com (accessed 17 April 2013).

New Zealand State Services Commission (2008), *New Zealand E-Government Interoperability Framework*, available at: www.e.govt.nz/library/e-gif-v-3-3-complete.pdf (accessed 17 April 2013).

Office of the Attorney General (2000), *Irish Electronic Commerce Act, 2000*, Irish Statute Book, available at: www.irishstatutebook.ie/2000/en/act/pub/0027/print.html (accessed 17 April 2013).

United Nations (UN) (1999), *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998*, UN, New York, available at: www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf (accessed 17 April 2013).

United Nations Conference on Trade and Development (UNCTAD) (2003), *E-Commerce and Development Report 2003*, UNCTAD, New York and Geneva, available at: www.cnnic.net.cn/download/manual/international-report/edr03.pdf (accessed 17 April 2013).

United Nations Educational, Scientific and Cultural Organization (UNESCO) (2011), *UNESCO ICT in Education Policy Makers' Toolkit*, UNESCO Bangkok, available at: www.unescobkk.org/fr/education/ict/ict-in-education-projects/policy/toolkit (accessed 17 April 2013).

United States Government (2001), 'A Practical Guide to Federal Enterprise Architecture', Chief Information Officer Council, available at: www.gao.gov/bestpractices/bpeaguide.pdf (accessed 17 April 2013).