

Build Government Interoperability Through Open Standard Technology

Goodwin Ting

Global Gov, Sun Microsystems Inc.
McLean, VA Virginia, USA
goodwin.ting@sun.com

Anne Rasanen

Global Gov, Sun Microsystems
Inc.
McLean, VA Virginia, USA
anne.rasanen@sun.com

Marco Pappalardo

Marketing, Sun Microsystems Italy
Milano, MI, Italy
marco.pappalardo@sun.com

Abstract

In this paper, we describe the business drivers and challenges for government interoperability; identify key conditions needed to achieve true interoperability; demonstrate how select technologies enable interoperability while still preserving required distinctness; and provide several examples of both successful and unsuccessful implementations from around the world.

Keywords

Policy harmonization, workflow, data exchange, identity management, open standards, federated identity, service-oriented architecture, open document format, multi-level security.

INTRODUCTION

The world is flat: people and businesses are connected and interwoven today in unprecedented ways and interacting at a pace unimaginable just a generation ago. The restrictions and limitations of time, space, and borders have largely been eliminated in many sectors such as finance, transportation, and telecommunications.

A major contributor to the reduction of barriers in these sectors is the ability of disparate systems to interoperate with one another: an ATM card from Citibank will work in an ATM kiosk from Unicredit halfway around the world, seamlessly. In the area of government services to its citizens and businesses, however, these physical and logical limitations still mostly exist. While many government organizations worldwide have indeed taken steps towards better interoperability, some have progressed further than others. The rest of this paper will review some key implementation challenges and technologies to enable government interoperability on a pervasive scale.

INTEROPERABILITY IN GOVERNMENT

Business Requirements

As the rest of the world have embraced and adopted business processes and technologies to enable 24x7 transactions, governments in Europe and elsewhere are struggling to keep up with the pace of change. Citizens and businesses are demanding that governments provide the level of services which they have now grown accustomed to with other industries. Compare the relative ease and amount of effort needed to book travel reservations to far-away destinations, and get access to one's funds from a local ATM machine

upon arrival – to the efforts required to pay one's taxes or get access to medical records while away from one's home region or country.

Along with this rise in demand for ubiquitous and streamlined government services, political and economic factors are also forcing governments to rethink how they interact and collaborate with each other. Within the European Union, transnational directions such as open borders, single currency, common defence framework, and other regulatory standardization initiatives all require enhanced interoperability in order to continue successfully and move to the next levels of efficiency and responsiveness.

With citizen and business consumers on one side, and policy directions on the other, the twin business drivers for improved public sector services have placed government interoperability squarely in the spotlight, and elevated interoperability requirements as a major challenge for government agencies, systems integrators, application developers, and technology vendors alike.

Evolution of Non-interoperability

Historically, government agencies and functions were designed, developed and have evolved to fulfill two primary functions: protection of group interests, and delivering service to its constituencies.

Protecting group interests may be at a city level, provincial level, or national level, and include such desired outcomes as:

- Sovereignty, including territorial defence and policy making.
- Economic stability and growth, including regulatory functions and compliance enforcement.
- Social stability and growth, including law enforcement, civil protections, and revenue collection and redistribution.
- Protection and retention of group assets, such as mineral rights, land, water sources.

Constituent services can also be at different governmental levels, and include key services for driving economic and social growth such as:

- Public education.

- Social benefits such as welfare, unemployment, retirement, and health care.
- Enabling services such as business licensing and motor vehicle registration.
- Quality of life services such as maintenance of parks, libraries, public venues.

The development and evolution of government organizations and operations to meet these two major core functions have typically taken mostly independent paths, fulfilling overall business objectives without detailed coordination between distinct and separate groups – interoperability was not a significant design objective. This process has resulted in silos of procedures, processes, data, and personnel. Consequently, government agencies are playing catch-up to meet the current operational requirements in an interlinked world as demanded by citizens and businesses, and dictated by policy directions. The stakes are often quite high – officials are elected and voted out of office based on their ability to deliver on these functions.

In the modern government environment, different agencies must maintain and deliver on their traditional core mission, while at the same time meet the more recent requirement to collaborate with other agencies towards a larger goal. This collaboration requirement spans multiple hierarchies and within each level:

- At the central government level within each country: the pensions administration needs to interact with the unemployment bureau with the income tax division.
- At the regional/local/municipal levels within each country: the local police force needs to interact with the local census bureau with the local fire district.
- Central and regional/local governments also need to interact with each other and collaborate on a wide range of functions.
- At the supranational level between EU member states to coordinate policies and operations on law enforcement, transportation, education accreditation, and a host of others services.
- Between the EU member states and the rest of the world for a wide variety of functions.

In addition to the organizational challenges and barriers to interoperability represented by these hierarchies and intra-level divisions, there are also policy and technological obstacles which need to be addressed to achieve effective interoperability.

Interoperability Challenges and Scenarios

Besides organizational and political considerations associated with government interoperability at a macro level, there are also several specific challenges which need to be addressed at the implementation stages. These include:

harmonized policies; workflow and services interoperability; data exchange and information sharing; cross-organizational identity and role management; and compatible security frameworks.

Harmonized Policies

In order to facilitate cross-agency (at any level) cooperation and collaboration, and to gain operational efficiency in providing services, government organizations must develop policies which can be harmonized with each other. Unless it is a newly formed entity, organizations typically already have policies in place. When multiple organizations have to work together to jointly deliver a service, then those respective policies need to be flexible and compatible enough so that all parties involved know how to accommodate each other to effectively achieve the common goal. At a simplistic level, distinct policies from separate agencies can be cross-mapped or normalized to each other at specific intersecting points; at a comprehensive level, policies can be merged completely or even developed jointly.

A very typical example of policy harmonization is in the first responders community during times of emergency. Many nations maintain separation between the police force, emergency medical responders, and fire brigades. When a critical event occurs, these separate forces converge at the event site, and must coordinate both within their own forces as well as with each other to establish chains of command, plan the joint response, and coordinate on the execution of that response. Policy harmonization ensures that the procedures, roles and responsibilities, actions, and outcomes of each individual organization efficiently contributes to the overall objective. Indeed, failure to harmonize policies in these situations can result in delays or ineffective responses resulting in significant loss of life and property: the 2005 Hurricane Katrina-caused flooding in New Orleans and subsequent breakdown in coordination between different emergency response agencies at the city, state, and federal levels is a tragic example.

While organizations which have a long history of working together – such as the first responder community – have developed and implemented harmonized policies to ensure interoperability, many other government organizations have yet to do so. There are multiple reasons for this: newly-leveled requirements to interact with other agencies; the emergence of ad hoc and non-persistent collaborative scenarios (“why take the time to harmonize if these events don't occur that often?”); and the simple fact that policy harmonization is often complicated, effort-consuming, and contentious.

Workflow and Services Interoperability

As governments respond to demands to streamline operations, increase service levels, and provide unified services, they are increasingly turning to technologies to digitize

workflow and automate services. This trend towards e-Government service provisioning has forced agencies to examine how they operate, the roles and responsibilities of each participant in the process, and in some cases re-design legacy procedures to benefit from the transformation to e-Government.

In order to properly develop and automate workflows and services, policy level considerations must first have been addressed. Therefore, successfully implementing workflow and services interoperability requires that policies and policy harmonization aspects to interoperability are also in place.

Unlike policy harmonization which does not require technology to implement successfully, workflow and services interoperability occurs at the intersection of business processes and technological capabilities. To implement government interoperability for workflows and services requires not just the business and operational level agreements between and within agencies, but also the selection of the appropriate technical tools, standards, and formats. The current state of maturity of the Internet and web services technologies ensure that the end user has plenty of choices in products and suppliers to meet the desired business objectives.

An common application of workflow and services interoperability is in the area of e-Customs. Many entities (both governmental and commercial) and transactions are involved in the process to receive goods at a port of entry for import into a country. Properly designed and well implemented workflow and e-services offer great benefits to all parties concerned: faster payments for goods; real-time revenue collection for the customs agency; reduced dock time for shippers; shortened product delivery times for businesses and consumers; increased accuracy in goods declarations and import compliance; and improved border security. Similarly, interoperability failures in the workflow and services anywhere along the process chain results in delays and lost revenues and even possibly spoiled goods.

One successful example of workflow and services interoperability is the Singapore Tradenet e-Customs solution developed by Crimson Logic and implemented at the Port of Singapore to facilitate customs clearance and other functions. This system automates a variety of workflows and data exchange and provides interoperability between government and commercial organizations at one of the world's largest port facilities.

Data Exchange and Information Sharing

Information and data are at the heart of any government service: citizen records, economic data, business licenses, GIS information, records of past transactions – terabytes of information which are generated, collected, sorted and used daily by dozens of agencies to carry out their functions.

Without the right data, streamlined and interoperable government services are meaningless.

Even within a government organization, the management of information and data is a major challenge: are the data accurate and current? Is any necessary piece of information missing? Who has the ability to view the information? Who has the authority to modify the data? How long should the data be kept? How does the organization ensure privacy and security around the information they have been entrusted with?

As in the case of workflow and service interoperability, policy harmonization is a mandatory precursor to successful data and information interoperability. Concurrently, technology and the selection of the proper data management tools, data formats, and interchange protocols are critical components to successful and effective government interoperability. Before the advent of the digital age, data interoperability and information sharing was relatively straightforward: text or diagrams on paper can be copied and distributed, and data repositories were physical filing systems.

Today's governments face data interoperability challenges created by technological advances: different types of databases; incompatible document formats; analog and digital formats for information; multimedia content; dynamically generated or non-persistent data; older formats which are no longer supported; and other effects too numerous to list.

Information sharing has also emerged as a key aspect of interoperability for governments. Agencies must share information to collaborate efficiently – taxes are based on incomes; pension eligibility and payments are based on recipient's age and prior income; educational investments may be based on census and other economic data. For each agency to independently collect and manage its own set of data translates to unnecessary duplication of efforts and high costs for government administration, as well as increased opportunity for errors and fraud.

A practical example of the utility of interoperable systems for data exchange and information sharing is the US income tax system. Most Americans typically pay income taxes to both the federal government as well as to their state tax agencies. The federal Internal Revenue Service (IRS) exchanges information with each state revenue agency to ensure proper tax payments or credits to each tax filer, and audits for fraud. The IRS also exchanges taxpayer information with other federal agencies such as the Social Security Administration and the Centers for Medicare & Medicaid Services to properly account for other government payments or deductions which affect the tax filer.

Cross-Organizational Identity and Role Management

Within government agencies and companies, organizational hierarchies and job functions of each employee are usually well-defined. There is a clear chain of command, and within

the organization it is clear who to go to for functions such as procurement, spending approval, press releases, and many other business and operational decisions. For the citizen requiring a government service – especially at a traditional government office – it is also fairly clear who to turn to for what type of help.

As government organizations move to a digital, e-government operational model, the distinctness of identities often becomes blurred within an agency. And as agencies increase collaboration with other agencies, the hierarchical structures and roles of individuals within each organization frequently do not dovetail clearly with each other.

Cross-organizational identity and role management is another major challenge for government interoperability, and is dependent on the successful harmonization of policies amongst agencies: who is authorized to do what under which conditions, and whose decisions take precedence over which others.

Once the policies are defined and in place, technology can be used to enable identity management and enforce roles assigned to those identities.

Harmonized policies; workflow and services interoperability; data exchange and information sharing; and cross-organizational identity and role management are four major challenges and parameters for enabling true government interoperability. Of the four, policy harmonization is the overarching parameter which the others depend on; if the policies are erroneous or incomplete, then the other aspects of interoperability will inevitably have flaws.

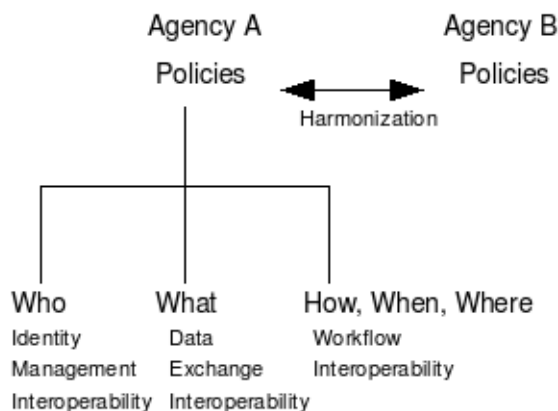


Figure 1 – Relationship of Interoperability Parameters

Figure 1 shows the relationship between the interoperability parameters - government services as delivered through efficient workflows (how, when, where the service is provided) by the appropriate people (who delivers the service) using the correct data (what information is needed).

Flying between Rome and Athens on any given day is a real-world example of governmental and organizational interoperability. Harmonized policies exist between the

Italian and Greek air navigation service providers: ENAV and the Hellenic Civil Aviation Authority (HCAA), respectively. Under the harmonized policies, both agencies have similar workflows for managing air traffic in their distinct and separate air space, and workflow interoperability at the moment and place of hand-off between the two country's air spaces. Since the policies are harmonized, it is also quite clear what data need to be exchanged, and what are the identities, roles, and responsibilities of the air traffic controllers and pilots who are from different organizations.

Compatible Security Frameworks

While security framework compatibility is not a requirement for government interoperability, it is a key consideration for a *successful* interoperability project. Government organizations – ranging from the military to the tax agency to public hospitals – handle large amounts of sensitive information: military secrets, citizens' private data, potential policy directions which can affect the welfare of citizens and companies.

With the sheer quantities of data available and the ease with which information – and mis-information – can proliferate, security and privacy have become extremely hot issues. Data exchange and information sharing between government organizations, or between governments and the private sector, must follow defined policies such as: who has access to the data, what they can do with the information, and how the information is managed and used. Workflows and services can be designed to ensure compliance with the data exchange and information management policies, and security policies for identity management can ensure that only the authorized people can access the relevant data.

However, if different agencies have different security frameworks which cannot interoperate – policies, technical implementations, workflow controls – then all participating agencies in the collaboration effort can be negatively affected by the “weakest link” in the group, and the data and workflows of all the agencies can become compromised. In those cases where agencies have completely incompatible security frameworks, a likely result is that no collaboration is possible at all: if one agency only deals in top secret information, and another agency has no capability for working with top secret data, then any attempts for the two agencies to collaborate will never even reach the starting line.

An interoperable security framework is especially critical for the military. When NATO member forces join together for military exercises or peacekeeping missions, the different national forces must share certain information with each other in order for the joint mission to proceed smoothly. At the same time, each member force must protect its national military secrets when that information is not relevant to the success of the joint mission. Without a common security framework such as security classifications and compartmentalizations, it would be impossible to selectively share sen-

sitive but required information while protecting other classified data. Similarly, without an interoperable identity and role management framework such as military rank, these joint missions would not have the necessary command structure to execute effectively.

Technologies for Enabling Interoperability

Although policy harmonization is not dependent on technology, and the other parameters for government interoperability can also be accomplished (theoretically) without significant use of technology, the reality is that governments and their contractors can achieve major efficiencies and increased effectiveness by adopting specific technological approaches designed to promote interoperability.

With the advent of the Internet and web-based services, product companies have placed more emphasis on standards adherence and technology interoperability. Even technologies which were initially designed to compete for the same market – such as Java Enterprise Edition (JavaEE) and .Net – have evolved to co-exist with each other within the same architecture. The primary reasons for this direction towards technology interoperability are: end users do not care about the implementation technologies or products as long as the services provided meet their requirements; and the market is now so diverse and the product choices so varied that product vendors have to provide interoperability to reach the widest possible customer base. The rest of this section reviews some key technologies which map to the interoperability parameters discussed previously, and serve as a starting point in the design and implementation of any government interoperability project.

Open Standards

After harmonization of policies, one of the major challenges for achieving interoperability – whether it is at the workflow, data, or identity level – is the selection of the right technologies for implementation. A key consideration in this selection is whether the technology being considered is widely adopted and supported by multiple product vendors, and whether the technology complies with industry-recognized open standards.

Over the past decade, a family of web services standards have been ratified to foster interoperability between products from various companies. These standards range from data formats to publish/subscribe services to business process interfaces. Historical competitors such as IBM, Microsoft, and Sun Microsystems have all either adopted these standards for their products or adapted their products to be compatible with other products using these standards. Increasingly, government and commercial services being developed and offered have been abstracted away from dependencies on the underlying operating system or hardware platform. The following describes some standards-based technologies for workflow and services, data compatibility, and identity management.

JavaEE-based SOA Frameworks

A common approach to developing re-usable and interoperable business services is through a service-oriented architecture (SOA). Although SOAs have been around for decades, the development and widespread adoption of web services standards have added new capabilities and extended SOAs into the mainstream of information technology (IT) and application development.

Since services are designed to be logical representations of business processes, when properly built they can be re-used as components to develop entire business workflows. And because these services are built upon open standards, the services from different organizations can easily interoperate with each other to achieve true business integration and government interoperability from a workflow standpoint.

Another benefit of SOA frameworks is the ability to more easily link in the data required as part of the business process or service, enabling greater and smoother data exchange and interoperability. Finally, the use of SOA frameworks permits a more uniform view of all the information that is part of the workflow.

An example of the use of SOA technologies for government interoperability is the UK National Health Service (NHS) Spine project. Using a Java EE-based SOA approach, the project successfully creates at the point of service delivery a “single patient view” of the patient's healthcare information from across multiple systems and data locations. The NHS SOA approach also manages the integration of disparate business processes across a number of different systems.

Service-oriented architecture frameworks are available from major vendors such as IBM's SOA Foundation, Oracle's SOA Suite, and Sun Microsystems' Java Composite Application Platform Suite (Java CAPS) used by the NHS.

Open Document Format (ODF)

Data exchange and information sharing is an integral aspect of government interoperability, and one of the most complex challenges. Digital information is diverse and represented in a variety of ways: documents, pictures, videos, charts, audio clips, database records, even information which is generated ad hoc during a particular step in the workflow and which may be non-persistent.

Various formats have been developed to represent these different types of data, including industry standard formats such as xml, mp3, mpeg and PDF. But, until recently, there were no industry standards for editable office documents which make up a significant percentage of the digital information generated and used by governments: documents such as memos, forms, charts, spreadsheets, and presentations. While popular formats exist which enabled governments and businesses to exchange information, the lack of an industry standard and incompatibilities between different

versions of the same applications posed a challenge for governments who have to comply with requirements for information management, long-term document retention, and records archival for historical preservation.

The Open Document Format was created to address the lack of an industry standard for electronic office documents, and its adoption helps close a gap for data exchange and digital information interoperability. This relatively recent standard has been incorporated into products from several vendors such as IBM and Sun Microsystems, as well as in open-source software community-developed projects such as KOffice. Many governments are prototyping the adoption of ODF as a default requirement, while NATO has recently announced the inclusion of ODF in its list of mandatory standards for interoperability.

Federated Identity Management

Identity management systems – originally centered around Microsoft Active Directory and other products based on the lightweight directory access protocol (LDAP) – have evolved to include more comprehensive capabilities than just managing user credentials through directory services. Modern ID management systems include:

- The creation, management, and deletion of digital identities and credentials.
- The management of user access to systems through both traditional (such as challenge/response) and non-traditional (such as fingerprint biometrics) means of authentication.
- The management of user entitlements (what the user is permitted to do or access) based on the user's profile, role, location, and other factors.

These new capabilities have enabled organizations to strengthen IT security, provide enhanced and increasingly targeted services to users, and often reduce the cost and complexity of managing user accounts and services through automation and user self-service.

However, most identity management approaches today are based on a (physically or logically) centralized model, with an overall repository hosting user credentials, profiles, access policies, and other parameters required to manage user accounts and attributes. This centralized model works well for distinct and separate organizations such as companies, but does not facilitate inter-organizational interactions required for true government interoperability. Employees of one government agency cannot access the systems of another government agency unless a new user account is created on the second agency's systems. Similarly, citizens who want to access a variety of government services may need to create multiple accounts, one each for each agency they need to interact with.

While the duplication of accounts and credentials is a workable solution for access to multiple government services managed by different government entities, it represents at best an inconvenience to the user and at worst a major security and efficiency detractor. For government employees who need to collaborate across agencies on short notice – such as during times of emergency, the lack of an interoperable identity management solution is a serious defect.

The Liberty Alliance – a consortium of businesses (both IT and non-IT companies), educational institutions, and government agencies – has developed standards, protocols, and procedures for enabling federated identity management across multiple, separate, and autonomous ID management systems. Using the federated ID management approach, government agencies can achieve identity and role management interoperability and enable users of one agency to securely access systems of another agency, while preserving the user attributes as defined by the policies of each agency.

Many government entities at the national, state/provincial, and city levels have incorporated aspects of federated identity management to achieve intra-governmental access or deliver cross-agency citizen services. At the federal or central level, these include: Australia, Belgium, Denmark, Italy, Norway, Portugal, Turkey, and the United States. State and provincial governments adopting federated identity management include: Tuscany Regional Government, Social Security Agency (INPS), Ministry of Transportation in Italy, New York, New Jersey, Massachusetts, Pennsylvania, and California in the US, the Canadian province of British Columbia, and the Victoria state government in Australia. At the city government level, cities using federated ID management for cross-agency interoperability include: Shenzhen in China, Sunderland in the UK, and Pierrefitte and Vandoeuvre-les-Nancy in France.

Multi-level Secure Operating Systems

Service-oriented architectures, industry standard data formats, and federated identity management are important technologies for fostering government interoperability. But, in many parts of government – such as in defence and law enforcement, a common security framework is necessary to ensure that interoperability is strongly secured and that access to information is protected according to the harmonized security policies between organizations.

An information technology model called multilevel security (MLS) is frequently used by government agencies which have to manage information with different levels of sensitivity; manage users with different levels of authorizations; and enable cross-organizational or cross-domain collaboration. MLS-based operating systems enable these fine-grained security policies and controls on workflows and

applications, data, and identity and role management of users within the organization and across different organizations.

Table 1. Illustration of Hierarchical and Compartmental Security Across Organizations under MLS

France Police	Italy Police - Turin	Italy Police - Rome
Fr National	Italy National 1	
Cross-border		Not defined
Fr Regional A	Italy National 2	
Fr Regional B	Turin Regional	Rome Regional

Table 1 illustrates some typical challenges associated with interoperability issues when different organizations with different policies have to collaborate with each other. In this fictional scenario (for illustration purposes), the French police have four levels of security policies: at the national level, cross-border, regional level A, and regional level B. The Italian police, however, have only three levels of security policies: national level 1, national level 2, and regional which is different between Turin and Rome.

Using MLS techniques, the French police and the Italian police in Turin can map their respective policies and determine how to harmonize security policies for cross-border interoperability. Once the different organizations' hierarchies and their relationships and equivalence to each other are determined, then the policies governing how workflows, data exchange, and identity management can be developed for optimal interoperability. An MLS operating system (such as Trusted Solaris from Sun Microsystems or Security Enhanced Linux from Red Hat) can then provide the common security framework to enforce compliance with the policies which have been developed and agreed upon between the different entities.

CONCLUDING OBSERVATIONS

Government interoperability has become a concrete requirement, driven by both citizen and business demands as well as national policies for collaboration. This collaboration takes place between different national governments, different agencies within the national and regional/local levels, and between different levels of government within a country. While interoperability can result in many benefits – such as cost reductions, improved citizen services, enhanced national security, and increased efficiencies in operations – it also presents significant challenges to implementation.

These challenges include policy harmonization between the participating organizations which is prerequisite to the successful implementation of government interoperability. Harmonized policies define the framework to clearly and effectively address the other key components necessary to interaction and collaboration between multiple government

agencies: workflow and services interoperability; data exchange and information sharing; and cross-organizational identity and role management.

The use of information technology to improve government services has also contributed to interoperability obstacles. To minimize these problems, the selection of open standards-based IT products as part of the agency's architecture is paramount – without harmonized policies and open standards-based products, interoperability projects will inevitably fail.

Service oriented architectures using Java EE based technologies are recommended for the development and implementation of business workflow and services. Adoption of industry standard data formats such as XML and Open Document Format (along with many others, depending on the type of digital content involved) will greatly reduce the complexities and costs for information sharing and data exchange. Federated identity management solutions and its extension to role and policy-based administration of entitlements has emerged as a necessity for government interoperability and ubiquitous e-government citizen services. Environments requiring strong security and differentiated user access to information with varying levels of sensitivity will benefit from the fine-grained security mechanisms of a MLS operating system. Together, this set of technologies can help overcome the major challenges to government interoperability, and help deliver on the two major functions expected of governments everywhere – to protect and serve its constituents.