gemalto
security to be free

Forum Mondial e-democratie
World e-Democracyforum

e-Gov 2.0: The keys to success

Choosing and building the pathway to success
Best practices and success factors

e-Gov 2.0: The keys to success – a preface from André Santini

e-Gov 2.0 is more than just a term banded about by experts. It is the result of the exponential growth of the Internet and information technologies over the last fifteen years or so. From the very beginnings of the web, it was always envisioned that tools could be developed that would make it easy for users to publish content they had written, filmed, or recorded themselves online. Back then, it was predicted that there would be increasing interaction between organizations and Internet users, but little did anyone imagine the sheer wealth of content that would be available, nor the impact it would have on 21st century society

For ten years now, the World e-Democracy Forum has debated the issues as state and society alike have gravitated towards second-generation Internet services. This White Paper comes at an opportune moment. The role of the Internet and mobile technologies in the election of Barack Obama as President of the United States bore out the conclusions reached by experts from France and across the world at the Issy-les-Moulineaux forum. We are now able to understand the growing and essential role that these technologies will play in our daily lives. Politics will never again be conducted as they were in the 20th Century, and those who are the quickest to realize this will be the ones who benefit most.

The government has understood this change. It can still improve, but it has shown great adaptability in shifting to a truly customer-centric approach as swiftly and effectively as any private sector organization. What we are seeing today across the world is an irreversible change in mentality.

In this White Paper, you can read about some of the best practices from across the globe. Experimentation must now give way to widespread implementation. This study tells us all we need to know about the tools, the motivations and the stakeholders required to build a digital society from which everyone benefits.

André Santini
Former French Secretary of State for the Civil Service
Mayor of Issy-les-Moulineaux

e-Gov 2.0: The keys to success

Choosing and building the pathway to success
Best practices and success factors

Eric Billiaert
Etienne Veyret

White paper **June 2009**

e-Government 2.0 – The Keys to success

FOREWORD

This report is intended as a follow-up to the previous report by the same authors – e-Government 2.0: Identification, security and trust. Exploring European Avenues.

The first report explored the foundations of e-Government and the role played by electronic identification (e-ID) in the emergence of innovative citizen services, both in enhancing service quality and in improving security and trust. It was a benchmarking exercise that aimed to identify the most visible successes and best practices on view in Europe in late summer 2007, in the run-up to the EU intergovernmental conference in Lisbon. The conclusions of the report suggested that the future lies in a resolutely citizen-centric approach, dubbed "e-Government 2.0".

This second report goes one step farther. It aims to support e-Government projects and to assist public authorities in devising and reinforcing their e-Government policies. Specifically, it identifies and examines the foundations of a successful e-Government program and looks at ways in which public support can be obtained for what some refer to as "the modernization of the State", i.e. the adoption of the "2.0" citizen-centric approach.

In putting the citizen at the center of all public services and government departments, public authorities are in effect doing what telecoms operators, banks and supermarkets did ten years ago – accepting the reality that, in the modern world, the customer is king.

Consumerism is a ubiquitous, truly planetary phenomenon, the defining culture of the twenty-first century. In recent years, the doctrine has even gained prevalence in the political sphere, as elected officials on both sides of the Atlantic have, to an unprecedented extent, allowed survey results to dictate their social policy.

While the most common goal of e-Government 2.0 programs is increased efficiency in public services and public-sector bodies, we shall see that, in fact, although those involved might not say so explicitly, this goal is often of secondary importance to modernizing the social contract and finding ways of strengthening social cohesion.

For some fifteen years now, profound changes have transformed the relationship between the individual and the collective. As economic deregulation and globalization continue to erode many of the guiding principles of the past, a considerable desire has developed for a new set of principles for the post-industrial era. There is a desire to qualify what can be considered authoritative and trustworthy in the new digital age and to identify the keys to modern social cohesion and sustainable social harmony.

This emerging desire is the motivation behind the modernization process we examine in this report. The adoption of a citizen-centric approach is a response to a profound need to rebuild a system of values in the face of the uncertainties of globalization and the overriding imperative to compete – a need to establish a framework that the majority of citizens can use to understand the modern world, to provide citizens with guidance, instill in them a sense of responsibility and involve them to the greatest possible extent in order to counter the growing risk of distrust and resignation.

The challenge is to build a system strong enough to promote the values required to achieve (or at least move towards) social harmony, which in turn leads to economic and social efficiency, solidarity, order, guidance, a sense of enduring authority … in short, all the ingredients of a society that is respectful of difference and attentive to the needs of each individual. This is the noble ambition of harnessing new technologies to counter social exclusion and insecurity in order to help people with limited mobility break free of their solitude. This aspect is generally referred to as "e-Inclusion".

Considering that human well-being and development are central components in the whole approach, it is hardly surprising that the primary focus is placed on the modernization of identity, identification, and trust in the identity of others.

e-ID was at the heart of our first report, and it is central to this one as well. This time, though, we concentrate on the services that go hand-in-hand with these modern, more secure forms of identity.

After all, **it is the use of these services, and the everyday benefits they are perceived to offer, that will ultimately justify the considerable effort invested in the "e-Government 2.0" modernization program.**

This report will explore how, in a national government identification system based on e-ID and the distribution of secure identity documents, "public e-services" can be developed to modernize all aspects of the state and society, and how to ensure that these services are successful and accepted by citizens.

This report presents lessons learned from the experiences of the past ten years, case studies, models, methods, and recommendations to help you make informed decisions and focus on the right priorities in your own projects.

The aim of e-Government 2.0 is to bring citizens closer to public authorities and public services.

We would like to thank the following contributors below:

Frank Robben (Belgium)
Frank Leyman (Belgium)
Anabela Cataneo Pedroso (Portugal)
Raphaël Bartolt (France)
Marjan Suselj (Slovenia)
Madeleine Siösteen-Thiel (Sweden)
Mohamed Al Mazrouei (United Arab Emirates)
Abdalla Askar (United Arab Emirates)
Franck Henry (France)
Luc Vanneste (Belgium)
Dr Professeur Reinhard Posch (Austria)
Michel Frenkiel (France)
Christophe Alviset (France)
Eric Legale (France)
Karel de Vriendt (European Union)
Evika Karmagioli (Greece)
Reine-Claude Mader (France)

For their time and dedication.

Meudon, June the 25th, 2009

e-Gov 2.0 : the keys to success

Choosing and building the pathway to success
Best practices and success factors

Summary

e-Gov 2.0 : the keys to success

Choosing and building the pathway to success
Best practices and success factors

1.1 Keys to the success of e-Government 2.0

Fifteen years of One-to-One Marketing and a profoundly altered economic landscape

Fifteen years ago, when the Web was still very much in its infancy, Don Peppers and Martha Rogers pioneered the concept of One-to-One marketing and customer relationship management in a seminal book that is still used as a reference to this day.

Today, we are living in a high-mobility, image-centered, digitalized world without boundaries. The Internet has turned this state of affairs into a daily reality. The common structure that used to underpin societies has been replaced by a multiplicity of experiences – the old foundations, “one identity, one profession and one territory”, have given way to the new trio of “difference”, “jobs”, and “social and economic networks”. This is individualism at its peak.

Previously, public authorities made collective decisions. Now, they have to consider each individual. One-to-One marketing has become a new tenet of the prevailing orthodoxy and an essential element of any economic or social analysis.

Modernization of the state or modernization of society?

There can be no society, however, without a “Social Contract” setting out the rules that need to be followed to achieve social harmony, which is, after all, a society’s primary purpose. The fragmentation of traditional models as a plethora of new economic and social realities have emerged – local, global, physical, virtual and digital – has left the immense majority of our contemporaries feeling lost and bewildered.

Thus, our first obligation in this new environment is to re-examine our Social Contracts and to ensure that the new set of rules governing economic and social activities are fully incorporated in every act of daily life.

This is why, in most cases, it is considered that politicians should lead this transformation, often at the very highest level of nations and governments.

e-Government as a new beacon for social cohesion?

Indeed, if e-Government 2.0 (so-called because it endeavors to take into account the specific needs of each individual) is an attempt to modernize the relationship between the individual and the collective through local or national authorities, then we are in essence adapting, remodeling and reinforcing the Social Contract.

Although e-Government 2.0 may rely on innovative, state-of-the-art technologies, it remains above all a project powered by political will, and it cannot succeed without this crucial ingredient. At the heart of the approach lies a public values system, which unifies all the new rules and frameworks and serves as a guiding light throughout the transformation process. The term "e-Government 2.0 program", used frequently in many countries, is most appropriate.

But the sheer scale of the task means there can be no overnight revolution. Though the law is the instrument by which new rules are created, the judicial branch, paradoxically, moves at its own pace and is rarely at the forefront of change. Likewise, public education authorities are enthusiastic but often do not have the budgetary resources to effect a fundamental transformation. Local initiatives often progress at a faster rate than national programs and can therefore be useful testing grounds. Of all government departments, finance ministries are the most comfortable with the notion of modernizing in order to offer better value for money. Social services and welfare systems yield the most obvious return on investment in political terms, and can allow significant savings to be made at a time when welfare systems are at breaking point…**It is therefore essential to ensure that each sector progresses at its own pace, according to its ability to adapt to the new rules and modern digital tools.**

A program that must be designed as a whole, but rolled out one phase at a time.

It is the rules by which a group chooses to live that bind it together. However, the program’s primary focus will initially be on the sovereign rights of the state – namely, a state’s right to identify its citizens and to be able to recognize all citizens, nationals or not, via an appropriate form of identification. The state’s sovereign powers are also what safeguard each individual’s identity against fraud, and allows people to use their ID in a secure fashion while exercising their rights and fulfilling their obligations to the community. Under the same heading, we also look at ways of ensuring trust and the enduring authority of government in all facets of the modernization process.

This is the foundation on which a number of sector-specific initiatives can be built, according to the needs of each nation and each city, in sectors such as Social Affairs, Health, Justice, Tax and Finance.

As an e-services initiative, the program follows the traditional Front Office-Middle Office-Back Office model.

Back Offices often comprise the current core of public services. They can be optimized.

But the real novelty is the additional layer of service and closeness to citizens provided by integrated portals or Front Offices through which citizens can monitor their situation on a daily basis. It is this additional layer of proximity that spawned the term "**Citizen 2.0**" (by analogy with WEB 2.0). We shall refer to this as "**Citizen-centric government**".

1.2 How far have the most advanced states gone?

Many states have begun their e-Government program in the way described above: by designing, producing or rolling out secure electronic identity cards, generally referred to as **"e-ID cards"** or simply "e-ID's". The most common applications for these smart cards are in **travel documents, electronic ID's, electronic signatures, municipal cards**, key cards used to access secure areas or business infrastructures, social security cards, etc.

Too often, however, the process has been approached from a technological viewpoint. Many advanced countries are now attempting to demonstrate that, beyond the security benefits for both states and individuals, e-ID can **provide citizens and businesses with real services and benefits, without infringing upon new rules on data protection and civil liberties**.
This also makes it easier to obtain the political support needed to deploy these very high-budget projects.
Another challenge, particularly at this time of economic crisis, is to demonstrate that the e-Gov 2.0 approach and the associated use of smart cards yield an excellent return on investment, if not financially then at least politically. Many states and local authorities are attracted by the versatility of these electronic ID documents and encourage their use in multiple everyday activities (transport, access to public buildings, and payment for public services).

The market for these cards is highly promising, but nevertheless remains poorly structured, and its level of maturity varies from country to country. Belgium, for instance, is already on its second generation of cards. Asia, the Middle East and Latin America are making great strides towards universal use of e-ID, France will soon be debating bills to authorize the issuance of such documents, while the United Kingdom, having introduced a bill that was considered groundbreaking for a country that has no history of identity cards, is still hesitating.
Furthermore, there is still debate over the best way of convincing target customers, and there are questions on which practices are best for such projects. However, in the ten years that these programs have been in operation, a number of general trends have emerged in many countries, and the different ways of achieving public acceptance and success are becoming clearer.
This is probably the ideal moment in the transformation process, which will take at least a generation, to take a step back and analyze the current state of affairs so as to identify the fundamentals and the keys to success.

1.3 Objective and contents of this White Paper

The objective of this study is to demonstrate the benefits of smart card systems for the public and private sectors and for citizens, using specific examples.

Barriers to acceptance – political, legal, technological, socio-economic, and cultural – will also be examined.

We have opted to present the results of our study as follows:

e-Government 2.0: building the pathway to success

This chapter highlights the lessons learned from seven representative case studies of the most successful e-Gov programs from across the world to identify the keys to success and the applications valued most highly by citizens and businesses. We shall examine examples of eGov programs in the following areas:

- The Sovereign role of the State: e-ID and forms of identity
- The Fiscal sector
- The Social sector
- The Health sector
- Community-based services and personal services
- The Financial sector
- The Public sector and the modernization of the civil register

What do businesses and citizens expect from e-Gov 2.0?

In examining citizens' attitudes to these programs, we shall consider, among other things, the results of working groups organized by the CLCV (the French National Consumers Association) on the theme of trust and distrust in citizens' views of e-Government.

This chapter also deals with the cognitive relationship the citizen have with his/her understanding of traceability, a subject that remains elusive and whose inextricable relationship with our choice to have an open world of freedom and responsibility is still widely misunderstood.

The keys to successful implementation of an e-Government 2.0 program

This is a more theoretical chapter, which reviews all the decisive factors in the design, implementation and running of an e-Government program.

Particular attention is paid to data protection and to the conditions required to increase uptake and build public confidence in e-Government.

This chapter also reviews feedback from working groups on the distribution and generalization of e-Government services through major partners such as banks or telecoms operators.

Conclusion: from e-Government to Citizen-centric government?

We shall review all the lessons learned from past experiences in order to understand the essence of an e-Government approach and the conditions required to ensure success for public authorities and citizens alike, through a modern relationship that benefits from the advantages of e-Services but also from a host of structural elements and from the knock-on effects of the modernization of the State.

What follows is a series of observations and interpretations. In no way do they constitute absolute truths or universally-applicable methods to be followed to the letter. The case studies, feedback and recommendations in this report are intended purely to guide the choices of each State when it comes to deciding on priorities and paths to follow, and to highlight the key elements that have, in many advanced states, brought real success, recognized by their own citizens and in some cases beyond their borders.

e-Gov 2.0 : the keys to success

Choosing and building the pathway to success
Best practices and success factors

2.1 The sovereign role of the State: identity is at the heart of the e-Government 2.0 approach

As we saw in Chapter 1, behind the term “Citizen-Centric 2.0” lies a fundamental change in the “Social Contract”.

Governments are the custodians of the authority vested in them by their citizens. This sovereign role lies at the very heart of their function.

With the citizen placed at the heart of all public-sector services modernization projects, implementing e-Government is the greatest challenge governments face. The task is more cultural and organizational than it is technical. It simply involves a conception of Public Governance in which public authorities act as service providers, managing public- or even private- information in order to improve collective and individual well-being. The aim is to achieve a level of efficiency and a quality of service commensurate with citizens’ new requirements in terms of the social and economic functioning of states and their public-sector services.

States have often failed to shake off the habit, inherited from centuries past, of managing citizen-users as “subjects” of a central power. In a way, the twenty-first century has restored a fundamentally democratic approach, in which the State belongs to the citizens. With the demand for better, more personalized service that meets every individual need, the roles of the stakeholders seem to be changing: the authorities are seen as managers, while each citizen is ultimately considered to be the owner of his or her identity and the related data required for public governance.

However, measures taken to bolster security and to combat fraud – sovereign matters *par excellence* – are very well accepted by citizens, contrary to what the media might sometimes suggest. These are the natural counterparts to the new demand for trust in all exchanges between citizens and the authorities. **The relationship of trust between the citizen and the public authorities is therefore central to this process of remodeling the “Social Contract”.**

Identity is the link connecting the individual to the community. Protecting identity against fraud or theft is the key to maintaining confidence in this link. It is crucial to be able to verify that a person is who he or she claims to be when exercising his or her rights and duties as a citizen. Digital technology has only heightened this essential need.

Identity, a powerful symbol of equality among citizens

Whereas, in the twenty-first century, identity has come to express the differences between citizens, it was originally a concept that expressed their equality. When, in 1793, French mathematician and jurist the Marquis de Condorcet laid the foundations of "social mathematics", he studied the relationship between the individual and the collective in an effort to formalize the foundations of the democratic system. In choosing the mathematical term “Identity” to represent the algebraic concept of equality among citizens in terms of their legal rights and obligations, he expressed the definition of the word that has persisted ever since – the state of one thing being the same in nature as another, of two things being one.
One nation, constituted by the sovereign people and their chosen representatives. One republic. Multiple individuals who, by “identically” accepting the rules of the community to which they choose freely to belong, attain the status of citizens.

Identity is a principle with two dimensions, and the link between the individual and the collective.

Electronic ID cards

An electronic ID (e-ID) card fulfils various roles: it acts as a traditional means of identification, as a travel document, and finally, as a passkey to the each citizen's personal data.

Many international regulations and standards have been established on e-ID, most of which are applied by States.

The public has become accustomed to smart cards through their use in the banking system, and as a result their reliability is no longer questioned. e-ID cards are now also being used as a means of accessing an array of services that were previously difficult to synchronize.
The e-ID card can be used for identification, but also for authentication and electronic signature. Thus, this system enables several previously complex information paths to be simplified.

It can be used as:

- A representation of sovereign authority, certifying that the holder is in a legitimate legal position with respect to his or her national jurisdiction.
- A means for citizens to access services and exercise their rights and duties with respect to the public authorities.
- A genuine seal of authenticity that the citizen can use to authenticate his or her actions regardless of the exchange formats and media used, since the data used to ensure security and trust also guarantee the legal validity of any transactions certified in this way.

Giving citizens their identity back

By making citizens a central part of the creation of a modernized state— giving them an active role rather than a peripheral role as a passive user of public services— public services are simultaneously, de facto, repositioning themselves. Identity is made up of a private set of data, of which the State is the custodian.

The conception of the State-Citizen relationship has been profoundly modified. We are entering a new era, in which this relationship can be expressed as a "contract" of rights and obligations. Citizens register for services and fulfill their obligations, and in return they benefit from the rights and guarantees offered by the community's social model. This is the very basis of the "Social Contract".

The e-ID card is also a passkey to a system in which everyone has their place and can therefore make their contribution and have their say (through elections and referendums, for example): e-Democracy.
At a time when security has become a priority, particularly in international transactions, e-ID seems essential. It is a guarantee given by one State to another within a network of trusted and interoperable national systems.

Case study: The United Arab Emirates adopt e-ID to help build a modern society

The United Arab Emirates have adopted e-ID to help build a modern, competitive, and prosperous society. The government aims to reach an ideal level of societal development by promoting this modern conception of the Social Contract.

To this end, the Emirates intend to join the standards already widely promoted by the European Union. It should be noted that the UAE began their program in the early 2000s and are thus among the pioneers of this societal transformation.

The United Arab Emirates' e-ID card program was launched in 2000. This young federation, created in 1971, comprises seven Gulf States, including the ambitious and dynamic Abu Dhabi and Dubai. The legal framework was strengthened in 2004 and 2007 to extend the powers of the authority in charge of creating the national register and distributing e-ID cards.
The pilot program began in 2005 and the e-ID card was officially launched in 2007.

98% of Emiratis were registered in April 2009, and by 2010 all citizens will have a card, which is now required by law.

A specific card distribution program was devised in order to give every citizen access to the records center.

The aims of issuing the card are as follows:

1. To combat fraud and forgery with highly secure biometric e-ID cards
2. To simplify identification and authentication procedures
3. To maximize ROI for government investments in IT infrastructure
4. To prepare for the future, when a number of services will be delivered through the card.

The successful introduction of the card is the starting point for a vast e-services project based around it, and puts the Emirates, with their remarkable swiftness of action, at the forefront of the e-Government scene.

Objectives:

- To move towards a greater public sector culture
- To provide customer/citizen-centric services
- To provide better quality services through technology and the resulting efficiency gains
- To improve the skills and experience of public-sector employees through training, education and improvement of public practices
- To widen access and create more efficient mechanisms to ensure interoperability and share information between government entities

Responsibility for all phases of the program was entrusted to an independent public authority, the **EIDA (Emirates Identity Authority)**.

For the purposes of this project, the EIDA adopted a state-of-the-art Public Key Infrastructure (PKI). Its goal was to simplify administrative procedures in all aspects of daily life.

The program will concern all citizens aged fifteen and over. The law has been altered and a framework of trust created to ensure that this medium is recognized for all public, semi-public and private services.

The Emirates have set up an interoperable national infrastructure linking all state administrative services, particularly the Ministries of Labor, Justice, Education, Health, and Economics, the Interior Ministry and the Central Bank of the United Arab Emirates.

The budget for the program is 55 million dollars, and distribution of the cards is now accelerating, with nearly 7,000 people registering and being issued with cards every day at the 22 registration centers opened across the country.
e-ID has been adopted very rapidly. Since 2007, it has been mandatory for anyone starting a new job or enrolling in a university course. Take-up has been further accelerated by the fact that electronic services, and even some non-electronic services, will no longer be provided to citizens and residents without a card after an as of yet unspecified deadline.

“Mobile Van Service rendezvous points” help to spread the word to citizens across the country and accelerate the registration of the whole population. (Source: EIDA 2009)

The EIDA intends to extend the use of e-ID in the near future to gradually replace work permits, health cards, driver's licenses and, of course, travel documents. Since April 2007, the card has included the “e-Dirham” function, an electronic payment method that can be used to settle all debts owed to the public authorities and which is supported by the Emirates’ major banks.

In particular, this function can be used to purchase public service e-stamps from designated points of sale. The citizen inserts his or her identity card in a point-of-sale terminal and the price of the stamp is debited from the card. The official document is then printed if necessary. It will bear the e-stamp with the date and time of payment and the amount paid.

A wide array of public services is currently available through public service portals. These include:

- Payment of taxes
- Social security (unemployment benefit, child benefits, direct payment of medical treatment by insurers and reimbursement of medical costs)
- Student registration and purchase of special student insurance policies
- Requests for official documents – passport, driver’s license, vehicle registration documents, planning permission, etc.).
- Obtaining originals and copies of documents such as birth certificates and marriage certificates
- Making formal complaints or statements to the police online
- Accessing national libraries
- Changing address

In addition, a range of online services is being rolled out **for businesses**, to help boost their competitiveness: taxation, tax declaration, business creation and registration, statistical declarations, customs declarations, environmental or ecological declarations, public procurement, etc.

The importance of communication has not been overlooked in the UAE (photo source: 2008 EIDA brochure). It is considered as a crucial aspect in managing what is a major transformation of the relationship between citizens and the authorities. Campaigns to convince people of the merits of the program and instill new practices will be conducted over a number of years.

The Sovereign role of the State: Conclusion

e-ID acts as a link between the public authorities and the citizen. It can only gain strength by sustaining the values inherent in this relationship. It is therefore necessary to plan a large-scale communication investment that will position this media as a symbol for social cohesion and effective citizenship.

Mexico’s microprocessor card driver's license: a multi-purpose document

In Mexico, a country with more than 110 million inhabitants and some 50 million drivers, migration to smart card driver’s licenses has brought numerous advantages to regions and citizens alike, and is all the more effective for the fact that these cards are recognized nationwide as a form of identification.

The card’s capacity to store various information concerning the driver, such as his or her accident history or past breaches of the highway code, represents an unquestionable advantage for the police and for the authorities responsible for issuing driver's licenses.
This kind of smart card, the effectiveness of which in reducing traffic accidents, insurance costs, identity theft and administrative fraud has been demonstrated on a daily basis since 2007 in the state of Nuevo León, was adopted by three other states in 2008 (Mexico State, Sonora and Vera Cruz) and looks set to be implemented in other regions too.
The success and popularity of the e-License are such that Mexico could adopt a basic national card as part of the modernization of the country.

Between 2006 and 2008, the results indicate a 22% decrease in injury accidents, a 34% decrease in DUI (Driving Under the Influence of alcohol) accidents, and a decrease of 39% in road fatalities. In the same period of time, the number of vehicles increased by 19%.

The issuance process is immediate but thorough. Each citizen's photograph and fingerprints are taken and the card is electronically signed. The visible signs of security, both in the issuance process and on the document itself, as well as the electronic chip, give the holder a sense of confidence in the card.

2.2 The Fiscal sector: Real financial challenges, strategic challenges for e-Government

The collection of taxes and duties is, by its very nature, the area in which the State has the most trouble ensuring citizen participation. Consequently, states invest much time and energy in

- Securing uptake among citizens and creating an enduring relationship with them
- Maximizing tax revenues
- Minimizing fraud

Tax collection has always been the cornerstone of good governance. It has also been the cause of most revolutions.
e-Government is by no means a panacea, but it does offer a number of solutions to the questions and problems that arise. It can help to change citizens' attitude towards taxation.
For businesses, meanwhile, the advantages are of a different kind – e-Government is essentially a way of simplifying and streamlining processes.

Worried about ROI? Put tax at the center of your e-Government 2.0 program.

"One of the reasons why it was so important to achieve success in the launch of the "My Tax Account" initiative was that Finance Ministries often have the major say in whether or not investments are made in e-Government programs. It is reassuring for officials to see that, although such programs require considerable investment and resources, they yield a rapid and significant ROI when applied in the fiscal sphere. Tax, like social security, is an area in which lightening the administrative burden can quickly bring about positive results, not least in boosting the competitiveness of businesses.
This is how we find ourselves in the rather paradoxical situation of tax payment systems spearheading the modernization of states.
A second paradox lies in the fact that, as the payment of taxes is one of the most fundamental examples of a citizen fulfilling his or her obligations to the state, it is part of the process of reinforcing the "Social Contract" It can therefore be accompanied by major communications campaigns on citizen participation in the modernization of the state. This is why the public authorities must in turn fulfill their obligation of transparency, as a manifestation of the new spirit on which trust in e-Government rests. Thus, the fiscal sector, somewhat surprisingly, is at the heart of the migration to a citizen-centric culture."

Gilles Grapinet, Co-Director of Information Technology, Minister of Finance, France

Simplified procedures are one of the main factors that encourage uptake among citizens in relation to online tax services.

If identification, authentication and signature can be performed using a secure document such as an e-ID card, then public acceptance will be greater still, as the need to manage certificates on their computers remains the most common cause of mistrust of such systems among citizens.

As in all areas of e-Government, the most significant benefits are:

- Considerable savings in paper
- Faster, more accurate tax revenue estimates
- Very limited potential for error compared to paper declarations

More than in any other area of e-Government, the key to success lies in getting citizens onboard. As e-tax services are often among the first services launched by states, mass participation of citizens and businesses is necessary to create a catalyzing effect on other e-Government services.

Part of the Swedish government's tax site: "Login and declare". In 2009, electronic declarations can be made over the internet, by telephone or by SMS using a form of electronic ID available on identity cards, bank cards and mobile phones. In a country of 9 million people, over 2 million declare electronically.

Case study from France: online declaration and payment of tax

"My Tax Account": the State gives citizens their data back

Since the tax authorities launched their online services, private individuals have been able to declare and pay their tax in the same way they manage their bank account. It is no longer a question of simply paying their taxes, but of managing them…

Citizens can use their "tax account" to:

- Declare their income
- Find out instantly how much tax they owe
- Pay online
- Manage their standing orders and direct debits
- View their fiscal calendar
- Print all kinds of tax documents

In Belgium, TAX-ON-WEB and "My MINFIN" serve similar purposes. Using your identity card and authentication, you can view what personal information is on file with the tax department, as well as your payment history, real estate contracts, preferred contacts, all written communication with the tax agency, and more.

Every effort has been made to simplify the citizen's task and make tax collection a "participative" process. It is no longer a case of the State taking, but of the citizen contributing.

The most cumbersome aspect to manage remains the certificates used for identification, authentication and electronic signature, which some find somewhat esoteric. An alternative solution – an e-ID system using a card reader connected to the citizen's computer to facilitate electronic signature – is soon to be launched in France.

The Fiscal sector: Conclusion

Paperless tax procedures not only benefit the State, but also make the citizen's life easier. They are also a powerful vector for transparency and trust in e-Government.

2.3 The Health sector: putting the patient at the center of modernization

The health sector holds an important place in our societies, as evidenced by funds appropriated to it, the role the state plays, and the large number of associated parties with various functions that it connects.

Because medical advances have resulted in increased life expectancies, and because citizens are being actively encouraged to take personal responsibility for their health, the number of people in need of medical care has increased. As a result, public healthcare systems are coming under severe financial strain.

With such demand for medical care, health services and related public-sector services are overwhelmed and spend more time managing than treating. Unless effective solutions are found to cope with this high demand, the system will ultimately lose all credibility.

E-Government's challenge is to process administrative tasks faster and more efficiently, and reduce the number of intermediate steps. The goal is to provide a single point of access where the patient will only pay his deductible, as determined by the principle of the Third Party payer.

Making Back Office savings in order to put the citizen at the heart of a modernized health system

Marjan Sušelj, Systems Director for the Slovenian e-health card scheme

"The goal of our strategic e-Health 2010 plan is to join up health information systems nationwide, thus ensuring that electronic services and transparent information can be provided to all stakeholders in a secure and efficient fashion."

The significant advances expected from the modernization process are:

For citizens:

- **Better information, increased responsibility for and active management of their health.**

For healthcare professionals:

- **An integrated clinical process in which information is transmitted quickly and effectively, easier access to sources or expert systems, and secure communication between healthcare providers.**

For government bodies and public health authorities:

- **Integration of different medical fields, a comprehensive view of the patient's health with interaction between sub-cases from different fields, better management of the adverse effects of medication*, better statistical or even epidemiological visibility, a more reliable aid for making decisions and establishing general approaches.**

*** Iatrogenicity (medical errors including mis-medication) is not an anecdotal subject. In the United States, the total number of iatrogenic deaths in 2001 was 783,936. The number of deaths due to heart disease was 699,697, and the number of deaths due to cancer was 553,251.**

Source: American Iatrogenic Association 2002

Most e-Government programs in this area are aimed at facilitating exchanges of information and helping medical professionals concentrate on care and treatment rather than management, notably through:

- **Much faster registration of patients at treatment centers**. This can be crucial, as the time that elapses before a patient is seen can directly affect the effectiveness of some treatments.

- No up-front fees to pay at most health centers, with costs paid directly by health insurance authorities.

The next stage in the restructuring of the relationship between patients, healthcare professionals and public-sector authorities is obviously the introduction of digital transaction technologies and the creation of e-Health cards, sometimes referred to as “Personal Health Records” or “PHRs”.

Personal Health Records allow healthcare professionals to access all the information concerning a patient's health immediately, regardless of their location, thus avoiding hesitation in urgent situations and optimizing quality of service.

Personalization, of course, is inextricably bound up with identification. As secure cards, based to a large extent on a standard smart card model, PHRs can be linked to e-ID almost immediately.

Using e-Health cards brings numerous benefits from an administrative point of view. Countries that have adopted this technology have noted a significant decrease in fraudulent reimbursement claims, as well as smoother, more efficient interaction between patients, healthcare professionals and health insurance authorities.

PHRs enable care to be streamlined, avoiding the need for multiple interventions and providing a coherent structure for the treatment of each patient. There are also advantages for government health policy: a well treated patient does not have to keep coming back every day. e-Health is not a commercial venture, and emphasizing **the role of the public authorities in safeguarding the relationship of trust** between the patient and his or her qualified medical doctor is a good way of building the public acceptance that is so vital to this process of modernization.

The next step is to involve private health insurance providers in established card schemes and then to link up different countries' systems so that patients can receive effective healthcare anywhere in the world.

Use of PHRs inevitably helps health service workers to work more effectively together and pool information about the patient. All too often at present this does not happen, with people “protecting their turf” as if the information belonged to them.

Preventive applications are still in their infancy, but a number of innovative services are beginning to appear in this field, be it for statistical monitoring or simply for managing access to certain drugs.
For some of the less advanced countries, setting up an e-Health system represents a quantum leap and a crucial stage in their development; such is the widespread modern day acceptance that a healthy population is a crucial prerequisite for growth and prosperity. These countries often evolve from having virtually no collective healthcare provision to adopting a modern, patient-centric approach.

The simplification of procedures for patients and medical professionals alike makes it possible to offer quality medical care at the point of need.

Case study from Slovenia:

e-Health helps provide high-quality medical care that puts the patient's health first.

In Slovenia, the roll-out of latest-generation e-Health solutions has improved online services designed for medical professionals.

Slovenia was one of the first countries in Europe to introduce health smart cards. Launched in 1996, the Slovenian e-health card program was rolled out on a national scale in summer 2000. The “e-Health 2010” program, which plans to roll out a new generation of health cards, also requires compatible terminals to be installed to allow healthcare professionals to consult their patients’ medical records securely, and create and sign electronic documents for social security purposes on a daily basis.

It is in this context that the Slovenian public health insurance authority has just signed a four-year contract for the installation and maintenance of 2,800 new-generation card terminals. Approximately 12,000 medical professionals are currently equipped with health card terminals in Slovenia.

This new smart card is the first of its kind in Europe to use a Java Public Key Infrastructure (PKI). Complete with an electronic signature function for healthcare professionals, it will help make the online health system more secure.

ZZZS, the Slovenian public health insurance authority responsible for the national health insurance card system, will integrate the systems and supply the cards to citizens. The whole solution will be compatible with existing infrastructures. In 2008, Slovenia decided to implement full interoperability between e-ID and Health-ID with a high level of data protection.

In 2000, Slovenia was one of the very first countries, after France (1997) and Belgium (1999), to introduce public health insurance cards with built-in microprocessors.

Today, the country is in the process of renewing and updating the two million electronic health insurance cards already in circulation within its borders. By rolling out latest-generation e-Health solutions, Slovenia is improving online services for healthcare professionals, helping them complete their administrative tasks more swiftly, and exchange medical information and communicate with hospitals and other healthcare professionals in a simple and secure way.

Japan introduces biometrics and e-ID to help fight smoking

In an effort to protect minors from the harmful effects of smoking, Japan is using a biometric e-ID card, which also provides access to a host of other e-Services.
A new e-Service has emerged in the field of preventive medicine in Japan.

Packets of cigarettes can be purchased from vending machines. As a result, it is difficult to stop minors from obtaining cigarettes. To prevent this, a smart card and a related e-Service has been developed. Cigarettes can now only be purchased with a personal prepaid card.

This card contains a photograph of the holder and the vending machines are equipped with face recognition technology. Thus the packet is only released when there is facial match.

The Health sector: Conclusion

E-Health offers some of the fastest returns on investments and an excellent political gain through better social medical coverage of citizens. Secure and coordinated efforts in the Back Offices allows for variety of national and local services to be created at a marginal cost. The initial return would be even greater if multiple forms of identification are avoided. This could be done by cooperating with other national projects by sharing e-Identification and coordinating identity management.

2.4 Social sector: achieving national and international interoperability

The beginnings of a real social Europe?

The global economic crisis, the opening-up of borders, increased mobility and businesses' use of low-cost employees to boost their competitiveness have combined to destabilize society and bring insecurity to critical levels.

But it is difficult to conceive of global regulation on issues that are subject to so many different legal frameworks.

And yet, while the modern world is one of flux and mobility, global growth and prosperity are inconceivable without at least some universal rules.

The interoperability of social systems is therefore, after that of healthcare systems, one of the most important aims in the new socio-economic world order that is emerging in the early part of the twenty-first century. It is no surprise to see ICTs and digital exchanges come to the aid of such a project. This is a first-rate opportunity for e-Government and related e-services.

The Member States of the EU make Europe are the ideal place in which to attempt to create such an order.

Belgium, already a pioneer in e-ID and e-Government and in management of an integrated social security system (public and private insurance, professionals and businesses, citizens, national governmental bodies, local authorities and community-based organizations, etc.) is once again at the forefront of innovation in this area of e-Government, exploring ways of encouraging international social interoperability.

Case study: "Limosa" facilitates recruitment management in Belgium

Limosa, a project run by Belgium's central social security agency, the Banque Carrefour de la Sécurité Sociale (BCSS), enables free circulation of workers. It ensures that workers are better insured, and businesses better protected.

Since April 2007, any paid work performed on a salaried or self-employed basis by foreign workers in Belgium has had to be declared to the Belgian authorities.

Thanks to the free movement of workers within the European Union, foreign businesses and self-employed people can easily operate in Belgium.

Stopping social dumping, the slavery of the twenty-first century

"Spot checks have shown that some unscrupulous foreign employers and self-employed people couldn't care less about Belgian labor regulations. Sometimes, they even hatch deliberately fraudulent schemes. The consequences are socially and economically unacceptable: exploitation of workers, social dumping, dangerous working conditions and unfair competition. These abuses are also a considerable drain on our social security system. The Limosa system acts as an effective barrier against all these attempts to pervert the laws governing access to employment."

Peter Vanvelthoven, Belgian Minister for Employment

In this context, however, it is essential that all rules applicable in Belgium concerning working conditions and variable remuneration are abided by. Since April 2007, all foreign workers who come to work temporarily in Belgium have had to declare themselves electronically. Thus, the public authorities are aware of who comes to work in the country and in what conditions they work.

A one-stop shop is available on www.limosa.fr in English, French, Dutch and German.

These were the circumstances in which the Limosa project emerged.

A project led jointly by the Minister of Employment and the Minister of Health, Limosa aims to:

- Improve the monitoring and inspection of foreign activity in Belgium.
- Provide comprehensive and reliable statistics to inform social policy.
- Simply administrative procedures for the various parties involved in cross-border working.

The first phase of the project, the mandatory Limosa declaration, began in 2007. Before coming to work in Belgium, all foreign workers and self-employed persons must fill out a declaration. To do this, they can use a user-friendly web application on www.limosa.be. This application immediately provides them with an acknowledgement of receipt (Limosa-1), which they must show to their customers in Belgium.

Failure to present this acknowledgement of receipt must be reported to the authorities immediately by the customer (via the portal www.securitesociale.be or www.limosa.be).

Foreign entrepreneurs who complete the mandatory declaration benefit from a number of advantages. For instance, they do not need to draw up working regulations, a staff register, or Belgian salary-related documents. According to Minister Vanvelthoven, “the Belgian inspection services will know exactly who is working where and for how long, and will therefore be able to carry out much more targeted inspections. We can now counter the exploitation of foreign workers much more effectively.”

In the second phase, implemented during the course of 2007, the data from the mandatory declaration was incorporated in a central database and augmented with data concerning work permits, professional licenses and residence permits. The inspection services concerned can use this data to help them in their duties. The centralization of this information helps the inspection services to detect cases of fraud more rapidly.

The third phase is the creation of a one-stop shop where foreign entrepreneurs can satisfy all their administrative obligations via a single electronic application. Each of the authorities concerned receives the data it needs to process the application. From an economic point of view, mandatory declaration helps keep Belgian businesses competitive. Thus, working or running a business in Belgium remains an attractive proposition for those who operate within the rules.

In conclusion of the Social sector:

E-Government enables what was previously thought to be impossible. It is the emergence of a new social order with the portability of social benefits outside the country’s borders based on agreements between countries for interoperability of their social frameworks. It is a project that will span multiple generations.

2.5 The Financial sector: banks are not in competition with the State

A promising alliance, but one that must be handled with care

The success of **e-Government also depends on how frequently the services are used** and on public acceptance of new media. Some people may be put off by the need to have both a card and a reader, but they can be won over if they consider that the system offers real benefits, enduring quality of service and ease of access in return for little financial outlay.

Although e-ID is the key to building a modern "social contract", it nonetheless remains subject to the fundamental need to win public acceptance.

The partners most likely to accelerate the widespread uptake of e-Government e-services are those who have for many years found them confronted with the same stumbling block, due to difficulties in equipping customers, and who have managed to build a critical mass of customer loyalty.

Banks and telecoms operators are the most obvious potential partners.

- Banks, because they remain the standard-setters in terms of secure payment authorization (a facility required by some e-Gov public services) and the most credible provider of such services in the eyes of citizens.
- Telecoms operators, because they have similar credibility in the field of transmitting digital data in a secure and reliable way.

However, keeping the public's trust, and ensuring that citizens are confident that partners cannot – without their knowledge or against their will – use the system for their own ends, is a major factor in the success of such a partnership.

The financial sector no longer has to prove its ability to handle new technologies, since the introduction of credit and debit cards, and related services, many years ago was ahead of its time. In an increasing number of countries, the direct result of this has been the combination of identity cards with credit cards or related applications: examples include certified national identity information "carried" by credit cards (Finland, Sweden, Austria) or in mobile phone SIM cards (Finland, Estonia, Sweden) and electronic purses built into national identity cards (Oman, UAE).

Extremely close attention must, however, be paid to the fact that, in the public's collective consciousness, money and the public service ethos do not go together (although this feeling is stronger in some cultures than others). Hence the importance, when building such a partnership, of projecting a strong public image and emphasizing the stringent selection criteria by which financial partners are chosen to help deliver public e-Services.

Creating wider distribution channels for public e-Services

The banking world has already shown that it is well capable of handling new information technologies. Indeed, it has set something of a benchmark in the field. Banks operate nationally and internationally within a system regulated by specific authorities. They have employed systems of trust for centuries, and banker-customer confidentiality has long been considered more robust even than doctor-patient confidentiality. Banks have played heavily on their traditional reputation for trustworthiness in promoting their e-services policies, emphasizing from the very start the high-quality, personalized service guaranteed by their very nature as banks.

It makes sense, then, for States to involve the financial world in their comprehensive e-Government programs.

The advantages are as follows:

- A partner that has already secured the loyalty of millions of citizens through its e-Services.
- A partner that understands, from its own professional experience, the need to observe rules and ensure trust, including in the digital world.
- A partner that has already revolutionized its approach in order to adapt to consumer culture – customer-focused and capable of tailoring its offer to the needs of every individual.

Furthermore, it is in the financial sector, along with the health and social sectors, that the greatest number of transactions and interactions with citizens occur on a daily basis.

Banks are therefore strong partners in delivering electronic services to citizens.

The most advanced “Citizen-Centric” models work on the principle that citizens should be able to choose which services they wish to receive or "consume", and how they wish to consume them, and many efforts are being made to apply this policy to e-Government e-services.

Allowing the citizen to choose the operator that delivers their e-ID card makes them feel like the masters of their own identity.

Case study: Austria allows citizens to choose the format of their e-ID

In Austria, the government’s sovereign right to issue ID cards to its citizens has been delegated to banks and telecoms operators.

An agreement has been reached with the state which ensures a secure issuance framework.

The state mandates that banks and telecoms operators issue e-ID’s and allows them to promote themselves as official partners of public e-Gov policy. It can, however, withdraw this right at any time if the rules governing this public-private partnership are not observed.

Thus, the government does not abdicate its sovereign power. It simply delegates the issuance of the cards to duly accredited partners.

Banks and other partners act as middlemen between State and citizens. They must remain as neutral as possible on the governmental nature of the service. But partners can include these rigorously monitored services in their own service offers.

"The role of the public authorities is to deliver identification certificates to citizens and to offer them the widest possible choice of ways of using them. The citizen must have the right to choose his or her preferred mode of access, whether it be on a bank card, a mobile phone or a social security card. The role of the authorities is to ensure that the means of access and the method for installing the identity certificate is secure and protects the citizen against fraud."

Professor Dr. Reinhard Posch, Austrian Federal Chief Information Officer

The State acts as a guarantor, intervening only in the role of regulator and inspector. It is the State that lays down the rules and ensures that they are applied.

Austria: Electronic identification and electronic signature are offered as standard on Maestro and Visa cards by nearly all Austrian banks.

Everyone- citizen, the financial operators and the States- benefits from this system. They become partners in ensuring the success of the widest possible range of services for the citizen, whom the operator will continue to refer to as a customer.
Austria has done the same thing – as have Finland, Sweden, and Estonia – with telecoms operators, issuing a SIM card containing e-ID for mobile phones and “mobile Government” (m-Government) services.

Sweden: On the site www.elegitimation.se – “your accreditation on the net" – we find TELIA, Sweden’s main telecoms operator, as well as the savings banks and major banks. BankID is the national electronic identification and signature solution used by government departments, local authorities, banks and many businesses. The system has more than a million users, making a total of 3 million transactions per month (source: BankID, March 2008).

2.6 Assistance of individuals: personalizing protection and assistance for certain categories of the population

e-Government to improve the provision of assistance to individuals

Challenges

By combining the strength of on-line services with the contribution offered by community-based mediation services, e-Government 2.0 creates a modern vision of Public-sector Services through a personalized approach aimed at satisfying citizen's needs. It maintains the founding principles of public-sector services: universal applicability, accessibility and trust in a relationship that is free of any time or location constraints.

The use of e-Government in the field of provision of assistance to individuals meets the local needs expressed by our citizens as they are forced to deal with the growing uncertainty present in the globalised, deregulated social-economic development of our societies.

In addition to being easy to use, one of the keys to e-Government's success lies in the frequency of its use, and in the extent of the perception of the benefit to each individual. In this respect, the provision of services to individuals is a prime candidate for the success of e-Government.

Benefits

The major advantage that is immediately apparent in the field of provision of services to individuals is that by its very nature it meets the fundamental end goal of e-Government, that is: Reconciling citizens with public-sector administration and community services to reinforce social cohesion, with improved service operating costs. Those services representing the best field of application relate to health, social management, education, exercising individual rights in making use of local services (childcare, care for the elderly, assistance to disabled citizens, prevention and safety services, etc.)

This field more than any other illustrates the extent to which the main use of e-Government consists in facilitating, for each citizen, access to and exercising of their rights and duties with respect to the community.

- For public authorities and communities offering services to individuals, there are short-term political benefits, reinforcing social cohesion and day-to-day quality of life. In the medium-term, direct and on-line management offer opportunities for increasing productivity and a reduction in processing costs in return for an improved service.
- For those individuals benefitting from these services, access to social benefits is simplified. The frequency of meetings between individuals and their community is greater, offering a more open vision of local activity. These resources offer those covered the opportunity to rediscover a certain amount of independence. As a result, third parties involved in providing their protection are offered greater comfort.

Expert opinion: Reaching an optimum success ratio with e-Government.

"The success of any on-line service, e-Government included, can be measured by its membership rate. Success depends primarily on criteria such as the frequency at which substantial benefit is perceived when making use of the service.

The substantial benefit and ease of learning and of use compensate for an inevitable resistance to change, and the factor of risk perception when using new tools.

The Level of success can be summarized by the following equation:

$$NS = f\,[(Fu * Bp) / (Rp * Rc)]$$

NS = The level of success is a function of Fu = Frequency of use and Bp = Benefit Perceived or significance of the new advantage, divided by Rp = Risk Perceived and Rc = Resistance to change

The frequency must be at least several times per month. The first expected benefit is time saved and greater freedom. The first risk perceived remains that associated with on-line payment, and the resistance to change depends strongly on whether or not the newly acquired points of reference are retained. "

Michel Frankiel, European Commission expert in IT security issues and President of Mobilegov

CASE STUDY No.1: Let us protect our children

"Were it not for internet child protection devices, there would not be the same trust in the digital economy. This is a responsibility that lies with all participants."

Nadine Morano, Secretary of State for the Family, France, 2008.

Kids- ID: Belgian child protection services, both within Belgium and abroad

In 2007, the pilot scheme for the issue of "Kids-ID", the new Belgian electronic identity document for children under 12 was successful from the start, especially as Belgium has been marked by several tragedies in terms of pedophilia and child abductions.

The Fedict, the Belgian Federal public-sector service in charge of e-Government projects, recently introduced the national deployment of the Kids-ID program. This launch, which took place in March 2009, followed the go-ahead given by the government on December 19, 2008.

In a country touched by several high-profile pedophilia cases, Belgium has introduced protection services for 6-12 year-olds, to be implemented both in person and via the internet. This has brought about the introduction of a smart card ID for children, much like those that already available to adults.
The Kids-ID program was started up in early 2007 with a pilot scheme, developing into a nationwide program at the end of 2008.

The Kids-ID project is based upon the association of an interactive protection service, an internet service, and a specific version of the application of the Belgian national ID card. Kids-ID is the same size as a credit card and holds secure information. It offers three functions:

- It is first and foremost an official electronic identity and travel document that is compliant with the ICAO standard valid in most European countries and contains the identity data and the child's photo stored on the electronic chip. The parents' name is also featured on the card.
- Secondly, it protects the child in emergency situations. If the child is lost or has an accident, the card features a telephone number that can be used to contact the child's relatives. The caller dials the special number, entering the eleven digits which identify the child on the national register. The call is immediately transferred to the first number in a list that may feature up to seven contacts selected by the parents at the time of issuing of the card. If this person cannot be reached, the call is redirected to the second number in the list, and so on, until somebody answers. If none of the contacts can be reached, the request is redirected to Child Focus, a Belgian foundation for child assistance, accessible 24/7, which can be assisted by the national police force if required.
- Lastly, the Kids-ID card may be used on the Internet for safer access to on-line chat rooms and for services requiring ID. An integrated PIN code automatically identifies the child and only allows him/her access to those internet services that he/she is allowed to use.

Kids-ID is not obligatory for children staying in Belgium. Parents may, if they wish, activate the cascading call service, by telephone or via this website, available in three languages. A 3 Euro contribution to the cost of the card is invoiced to local authorities. Kids-ID is a fine example of cooperation with Child Focus, the Foundation for Missing and Sexually-Abused Children, a member of Missing Children Europe. Communication is directed toward parents and strongly supported by communities.

These highly-secure cards offer endless possibilities. In the near future, it is envisaged that they may be used as library cards, sports membership cards or perhaps even school attendance cards. They are also expected to replace the Social Security (SIS) card for children.

It is very apparent that these two subjects are major preoccupations in the majority of countries. Recent profiling studies in Belgium - University of Ghent and Fedict 2008 - also highlight specific, homogeneous user groups (single-parent families, senior citizens, jobseekers, students, etc.) for whom adapted solutions could be put together. These are excellent opportunities to contribute to creating a digital strategy that is more inclusive and secure.

CASE STUDY No.2: Toulouse, France's fourth largest city, is ensuring the comfort of its elderly residents using the TISSEO e-card

Recently put in place by Toulouse Town Hall, the TISSEO card is intended for Toulouse residents aged 65 and over. It offers a wide range of services, including free access to the town's entire transport network and free entry to local public amenities (swimming pool, libraries, museums, etc.), as well as a large number of reduced tariffs for the majority of the town's cultural and sporting organizations. This offer is combined with an interactive internet service providing information on local news and events, enabling the user to get involved in or make reservations for activities held in the town.

This service exemplifies the potential for inclusion and strengthening of social cohesion offered by management of assistance to individuals and now available thanks to new technologies.

The European Commission has adopted an action plan and a new research program designed to improve the quality of life of older people through information and communication technologies (ICTs).

Entitled "Ageing Well in the Information Society", this action plan aims to provide new answers to the challenge of an ageing European population. By 2020, 25% of Europeans will be over 65, while the costs of pensions, health and long-term care will grow threefold between now and 2050.

Conclusion

The provision of assistance to individuals responds to a substantial increase in citizen demand and, beyond simply transposing existing services in an inflexible manner, enables real innovation to reinforce social cohesion, making use of new technological resources, as illustrated above.

2.7 Public sector: modernizing the civil register

e-Government as a way of improving the reliability of documents

Challenges

The development of e-Government is based on building a secure infrastructure to coordinate efforts to improve the reliability of all documents issued. These documents enable individual citizens to exercise their rights and responsibilities via digital means. Clearly, document theft and fraud are sources of social injustice as the community may inadvertently allocate resources to an ill-intentioned individual feigning another person's identity, thus depriving the genuine citizen of that to which he or she is legally entitled.
The first element of reliability that one should be able to expect, to avoid creating a climate of mistrust across the e-Government program, is the theft-proof nature of the procedure involved in issuing and distributing documents.

Where do the weaknesses in the system lie? They are found at two stages of the document production process:

- Presentation of forged supporting documents when registering the application.
- Reception and validation of the application by the registrar, either when the application is registered or during the examination of the application before the document is physical produced.

Benefits and operating procedures

This requires implementation of two sub-projects to contribute to securing these two delicate stages:

- Converting the civil register to a paperless system
- Producing secure Public Official cards

Converting the civil register to a paperless system

The central element providing proof of the authenticity of the identity of individuals requesting secure documents is of course the extract from the civil register.
Converting the civil register to a paperless system is therefore based on at least two main aims:

- The digital transmission of extracts via a secure channel, avoiding fraudulent actions by intermediaries with access to non-secure copies.
- Gradual creation of a digital repository of civil registry documents, which will rapidly become the parent database for all identification documents. Bearing in mind that it is always possible to adopt a proactive approach to speeding up the digitization of archives rather than simply waiting to receive document renewal requests.

For countries who consider their archive data to be insufficiently reliable, it is also possible to proceed with national registration in the form of a census campaign. Some countries have then opted for biometric registration, taking the view that citizens' digital and/or facial biometry remains the most reliable source for unmistakably identifying them. The "one for one" biometric inspection is performed when a civil register supporting document is transmitted, thus enabling its authenticity to be verified.

Securing the registration system

To prevent secure documents being traded as goods, officials working anywhere in the system will be provided with Public Official Cards and, in their role as registrars, will personally validate each of the information exchange and modification stages involved in producing the document.

In conclusion, for the civil register sector: the first e-ID documents to be delivered, establishing an excellent pilot basis, will be Public Official Cards. As the first documents to be registered in a secure manner, they will play an active role in supporting security throughout the document system.

Case Study: An exemplary roll-out in Hong-Kong

Hong Kong is a special administrative region of China. It is a world-class commercial and financial hub, with a population of 7 million. With origins as a British Colony in 1842, it was granted back to China in 1997, and today is fundamentally different than the rest of the People's Republic of China. The personal data privacy ordinance, passed on December 20, 1996 introduced the framework for the creation, utilization, and distribution of personal data in Hong Kong. An electronic transaction ordinance, passed in January of 2000, served as the legal base for the creation of one of the first PKI networks in the world.

In 2003, Hong Kong took example from Finland, Brunei, Malaysia, and Macao, and started its own national identity card program. The card, which was first deployed for police, labor department, and immigration personnel, is offered to any Hong Kong citizen in two versions. There is a child card for those over 11 and under 18, and an adult card for those over 18. In less than four years, the new card phased out its predecessor, and is now held by more than seven million citizens and foreign residents. The new polycarbonate card features a microprocessor, and is capable of storing personal data, a digital photograph, and two fingerprint scans. It functions as the country's primary identity document, and is required for employment, voting, and receiving social services.

Since its introduction, the card has been presented as a versatile, highly secure device with a multitude of functions, including a driver's license or ICAO travel document. It also permits faster crossing of borders thanks to automatic control checks (e-Channel) which verify the card holder's fingerprint. This biometric fingerprint control of a passenger takes just 12 seconds on average. The card has also been adopted by the city's public libraries, a symbolic place Hong Kong.

The use of the card for e-Services is activated voluntarily at the post office, using the "e-Service" certificate. This service was free for the first year, and is subject to a fee as of April 2007. This authentication and signature function is a key element in the development of e-Services in Hong Kong, for public applications (deeds) as well as private (encrypted and signed documents and contracts). It is based on a PKI (Public Key Infrastructure). Hong Kong banks were among the first to offer secure e-Banking services.

Certain domains, like sports, have joined the movement with services such as online betting (e-Win of the Honk Kong jockey club). This sport is of national importance in Hong Kong.
Since 2004, to accelerate the adoption of the card, over 500 computers and card readers have been set up for public use in post offices, public service agencies, and in 200 Hong Kong libraries

The services that are currently accessible by e-Services include:

- Change of address
- Application for voter registration
- Notification of premature termination of employment contracts of imported and foreign domestic workers
- Renewal of driver's licenses and vehicle licenses
- Appointment scheduling for driver's license tests
- Application for business or branch registration
- Filing of tax return and interactive tax enquiry
- Financial transactions, including those with Hong Kong Stock Exchange
- Transfer of secure information in enterprises

The success of Hong Kong's new identity card is due in part to a strong and constant political will, solid technical and legal infrastructures, a document that is visibly more modern and secure than its predecessor- a boost to national pride, the perception that, since launch, the card would protect the rights of its citizens and their uniqueness, the installation of self-service terminals and integration in libraries, online betting, and more "classic" examples of e-Government such as eTax. The use of an electronic signature, like in many other places, is still rather weak in 2009.

e-Gov 2.0: The keys to success

Choosing and building the pathway to success
Best practices and operating procedures

What citizens expect

To be able to meet citizens' expectations in a representative manner, we turned to three studies based on citizen focus groups, some using internet users some not, organized by the following, respectively:

- The CLCV (*Confédération Consommation Logement et Cadre de Vie* - Housing and lifestyle consumer confederation), one of France's largest nationwide consumer and user associations, represented by Reine Claude Mader, its president.
- The DMSP (Research Center - Paris Dauphine University - Dauphine Marketing Strategy Perspective), using Caroline Miltgen's work on trust and personal data, in France and across Europe.
- The Institute for Prospective and Technical Studies with its March 2009 report for the European Commission.

They indicate that:

- Expectations are high for an approach resolutely focused on citizens' day-to-day concerns, both on a national level and, above all, at local level
- We are still at the start of the educative cycle and citizens do not yet have the maturity of experience that will enable them to spontaneously express exactly what they want in the way of transformation in Public Services
- They find it easier to describe what improvements they wish to see in the quality of service provided
- Lastly, the vast majority still view Public Services as restrictive or representing an obligation. Whilst consumers demand the same quality of service and consideration of their needs from Public Authorities as they expect from their bank or telephone operator, there is still a **long way to go before they consider themselves to be in an active, responsible relationship with Public Services, whereby they can make use of State services to organize their everyday life**.

If a cultural transformation needs to take place in order for this to happen, it is down to the public authorities to provide the teaching required.

It has been considered and demonstrated in previous chapters that the secure identity document, "e-ID", acts as a bridge between citizens and the community via the Public Authorities, and is the keystone to the transformation and to the e-Government program as a whole. This document and its use will therefore be the focus of our breakdown of the results of the three studies.

The two questions that we have examined relate to:

- The position of citizens with respect to these new documents
- The instinct to protect personal data and the conditions necessary to ensure citizens are willing to transmit their data, and by which methods, to obtain services via the Internet.

CLCV focus groups on secure documents

The introduction of secure identity documents in France has not really captured the imagination of the general public.

To get to know consumer opinion, the CLCV organized three focus groups, each made up of 10 consumers. Members were selected according to the following criteria: members of the first group had to not be members of the CLCV, the second had to be members of the CLCV exercising no specific responsibilities, and the third had to be executives or individuals with professional responsibilities.

The following information was observed from discussions with the focus groups:

The current situation surrounding identity:

- French citizens consider it normal to have to carry ID. This is not the case in every country, and the response would be somewhat different if the same question were to be posed in Ireland or the United Kingdom.
- They do not have any particular problem with the identity documents that they hold
- The current system for issuing documents is straightforward (they can be obtained locally)
- It is not too costly: only the issuing of passports has to be paid for (€89)
- Renewal in the event of loss or theft is relatively straightforward as it simply requires the same procedure to be followed as used to obtain the original document
- There is no experience of the acute level of identity theft that can be seen in England

Aside from the question of identity on the internet, the majority of citizens are satisfied with the way things are at present.

Comments: The justification of any significant change therefore needs to be supported by:

- The reuse of any reference points acquired that have not been subject to any specific remarks
- Communication on the added value of the project, to offer a clear demonstration of the new advantages it offers

With regard to the general public, the necessity to move towards more secure documents needs to be highlighted, particularly for those citizens who do not travel abroad. It should also be noted that the question of secure documents is not something the general public is well aware of. To this end, the teaching aspect needs to be developed.

Recent debates organized on the Internet, which saw 3,000 internet users take part, brought the following subjects to the fore:

- French citizens are very conscious of the question of identity, but there are many questions raised as to the end goal of these projects: why use technology that we do not yet understand?
- Issuing conditions (simplification, rapidity)
- Cost of secure documents? Do security and the benefits of the new services come at a price?
- Methods of conserving and consulting data/conditions for storing this data: are they private sites? It is currently widely believed that the entire process is managed by the French Interior Ministry.
- Limiting functions strictly to the identified holder of the document: is it possible for a card to be used for other means than those intended?
- There is a fear amongst consumers, as highlighted by the CNIL (*Commission Nationale Informatique et Libertés* - the French data protection authority), of information being acquired fraudulently on contactless smart cards.
- What controls are in place, in particular concerning the subcontractors involved in processing personal data? Consumers are wary of their personal data being recorded. In particular, they wonder what controls Public Authorities will carry out on subcontractors.
- A final question: what influence will the new security systems have on other secure instruments, such as debit and credit cards? What interaction will there be, and how much convergence?

In conclusion, we need to examine how we can gain consumers' trust, and what measures need to be taken in order to achieve this.

The computerizing of data, and the way in which it makes it easy to record information about individuals, has led a number of participants to ask questions regarding the protection of human rights, both at national and international level.

Contacts: CLCV – 17 rue Monsieur – 75007 PARIS (France) - Tel.: +33 (0)1 56 54 32 10 – www.clcv.org – e-mail: clcv@clcv.org

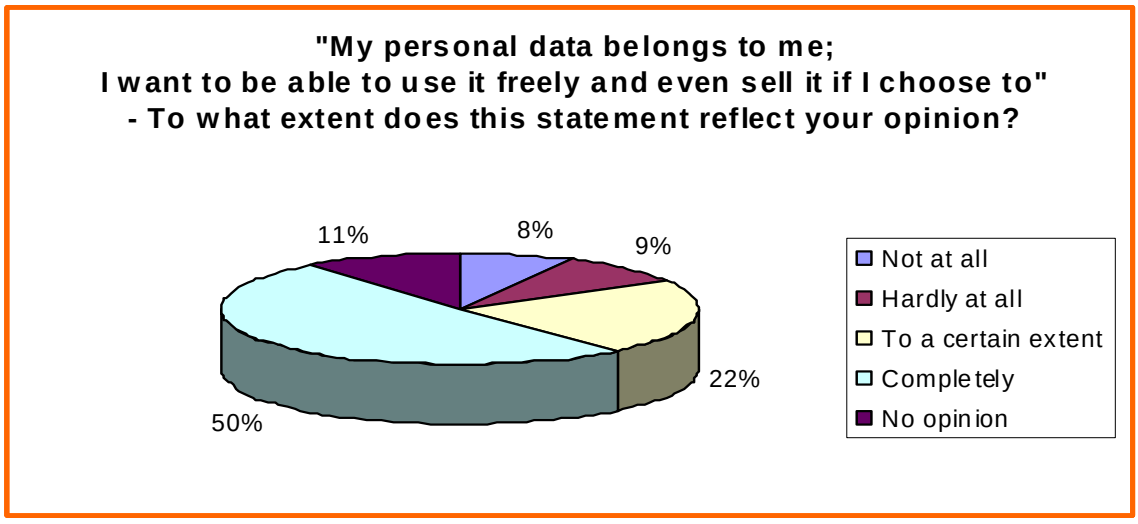
DMSP focus groups on personal data, e-ID and trust in e-Services

The results set out below are taken from a study carried out in 2005-2006 concerning different groups of adults and the conditions for communicating personal data.

A graph and two tables are provided to complete this information.

What relationship do citizens have with regard to their personal data? Concerning identity data or data relating to one's health and social status, to what extent is data kept private or made public?

The response speaks for itself:



Identity management leads individuals to make choices. Set out below is the order of the criteria that enable citizens to assess whether they wish to subscribe to a service for which personal data must be communicated:

1. Context in which the information is requested (public/commercial)
2. Type of contact person requesting the data - familiarity favoured over a more public setup
3. Type of data requested and degree of sensitivity (e.g. postal address and credit card details vs. e-mail address).
4. Type of advantages that may be obtained in exchange

In looking to characterize the behaviour of citizens who communicate personal data, there have also been attempts to break down different behaviours. In the table below, we combine this with a study performed some time ago (1995), to demonstrate the relative stability of this data. Nevertheless, overall perception of risk increased by 6% in the ten years between the studies.

Legitimists accept the view of the Authorities, whilst Pragmatists base their acceptance on perceived benefits.

Date and author of the study	Reticent	Cautious or Legitimist	Pragmatic	Benevolent
Alan Westin 1995	**25%**	**55%**		**20%**
Caroline Miltgen 2006	**31%**	**24%**	**25%**	**20%**

To conclude the study, the groups were asked **what their reasons would be for using pseudonyms when accessing e-Services.** Again, the results are broadly consistent. The main motivation is not so much to hide or to take on another identity, but **to protect one's real identity**. This shows that there is a real awareness of the need to protect one's identity and the confidentiality of personal data, given the continuing uncertainty about the digital world and the somewhat random reliability encountered: we can never really be sure of what is going on behind the e-Service screen that we are accessing. This is where **Authority logos, signs and codes are recommended** to convey the guarantees and feeling of security that are necessary in order to achieve widespread public acceptance.

Reason given for using a pseudonym	Security dimension	Freedom dimension
To protect my privacy	35%	
On principle	26%	
To not be recognized	21%	
To be more imaginative		9%
To be better listened to and understood		6%
To pretend to be someone else		4%

"Young people and emerging digital services" study published in March 2009, carried out by The Institute for Prospective and Technical Studies on behalf of the European Commission

This study helps us to understand the image of e-Services and the burgeoning idea of trust amongst the generation that is likely to benefit most from this transformation, with a much more developed internet culture. The study, carried out in 2008, was based on 5,265 complete responses and 6,000 partial responses from young people aged between 15 and 25, in France, the United Kingdom, Germany and Spain. Firstly, it revealed that a certain proportion of the young people consulted are well aware of the risks the Internet poses with regard to personal data, and that the majority are awaiting the arrival of new **technical** and preventative solutions.

Analyses of factors encouraging the use of electronic identity systems (e-ID):

- Several factors are likely to encourage the use of e-ID systems. The young people consulted want to receive assurance that their personal data is protected and that the transactions they perform are secure. In France, 71% of young people insist on the importance of guarantees and 65% want there to be labels and logos to that effect. In Germany, 67% say they want guarantees but only 34% ask for labels or logos.
- The demand focuses much more on guarantees than on control elements. Above all what is asked for is for the perceived risk to be fully covered.

Factors encouraging the use of e-ID systems	Yes (as a %)	Guarantee or Control
The assurance that the law on data protection is complied with	72	G
The guarantee that the data is not sold on or reused	69	G
A label or logo proving that the service is secure	52	G
An individual file of my data and transactions so that I know what information about me is held	49	C
Obtaining a receipt after providing information	49	C
Information on the information system	54	C
Information on how the data I have provided is used	59	C
Testimonies of people who have used the system	42	C

Analysis of factors encouraging the use of electronic services

Firstly, 92% of the young people questioned insist on the service protecting their privacy and 88% insist on being able to check the data they submit. These reactions appear across each of the study's scenarios; it is important for them to have a central place in the promotion and use of e-Services.

Factors encouraging the use of e-Services	%
If my privacy is completely respected	92
If I can choose which personal data I want to provide	88
If the service is free	86
If the service saves me time	83
If it is very easy to register	79
If my friends have strongly recommended it to me	68

Who should offer these services?

Entity	%	Institution	Company	Non-profit
A government organization	25	0.79		
The central authority - the State	33	0.77		
Local authorities	18	0.70		
A company that you are familiar with	34		0.70	
A specialist service provider	23		0.57	
A non-profit organization	30			0.95

There were several possible responses. The result is very telling: greater trust is placed in what is familiar and what has already experienced and witnessed.
Secondly, the trust index is highest for institutions mostly clearly associated with protecting and guaranteeing the common good: at the top of the list are NGOs and non-profit organizations, which are assumed to be set up to defend the common good and to operate within a voluntary framework. Next are those organizations that present Authority signs and codes. Last on the list are private or unknown public organizations.
This also tends to indicate that simply possessing Authority is not enough; it needs to be publicized and promoted.

To summarize the three studies, citizens wish to be taken into consideration and respected as individuals, but it is down to the Public Authorities to guide them towards transforming and reaffirming "social cohesion".

One of the major consequences and a key factor in the success of this transformation is that citizens' **trust in and acceptance of** the **codes, signs and products** need to be optimum. It is important to bear in mind that simultaneous acceptance of the three factors, "Codes - Signs - Products" is essential to avoid inconsistency and a loss of trust. In taking this step, citizens see the consistency that is needed between thought, word and deed.

e-Gov 2.0 : the keys to success

Choosing and building the pathway to success
Best practices and success factors

4.1 Governance of a national e-Government system

Identify the modernization challenges faced by the state

The central challenge, and the most frequent motor of e-Government policies is above all to provide a modern, competitive framework for the development, both economic and social, of the State, with regard to:

- Providing an essential contribution to human, social and economic development, to the benefit of citizens, with a major impact on the quality of social cohesion and, in particular, for the most underprivileged members of society (dubbed "e-inclusion" programs).
- Providing strategic support to revitalize the competitiveness of companies: offering a modern framework that reduces bureaucratic red tape in order to encourage company creativity and the provision of capital, and promote economic development. To this end, the legal framework promoting electronic exchanges is drawn up - digital trust rules - to which systems such as electronic signature also make a direct contribution.

This fundamental movement with regards to development represents political advantages, such as:

- A strengthening of democracy and improvement to citizens' quality of life.
- The inclusion of all citizens in the effort to promote modernization and the strengthening of social cohesion through the capacity to reconcile citizens with the public-sector authorities using on-line digital administration tools and the related modern communication technologies.

Set out the progressive stages of the modernization procedure

The introduction of an e-Government program represents a major political decision, which involves all administrative bodies and which results in a far-reaching cultural transformation in service relations practices between public service providers and users. This procedure may last several years, so it is necessary to ensure the different stages are designed to run in parallel, and to launch pilot projects demonstrating the political will, the potential results and benefits that may be generated by the program.

Governments most often **adopt a three-stage procedure** to achieve the development objectives mentioned above. This involves:

- First of all, establishing trust in digital exchanges that the country can't do without.
- Providing secure ID documents based on a reliable civil register, to offer every individual access to each of the State's modernized services, to promote national and international mobility, with a view to protecting citizens' Identity and fighting fraud and cybercrime. Such secure documents also help countries participate in international cooperation with regard to the regulation of migration. It is also the first real, tangible result of the transformation program, yet without application services: it may be likened to a motorway without traffic flow or exits. This is why the first usage allocated to these documents is the ability to use them as a travel document, standardizing them in line with ICAO requirements.
- Developing services in the social, economic, health and education sectors. This policy includes the opening of community-based services and citizen information centers to ensure that support of this modernization is provided as locally as possible in all territories and to all sections of society, covering all events occurring as part of everyday life.

Canada's multiservice one-stop shop offers a needs-based approach. This is the fruit of an accomplished marketing approach in which citizen demand is at the heart of the service's design.

Establishing an environment of trust in the State's modernization

For the State to be modernized, all of the means offered by IT and communications technologies need to be put to use in order to establish flexible, interactive relations, without space or time constraints, between citizens and public service providers. The transition towards multimedia communication is an opportunity to rework old texts and revise the often overly formal and unsuitable framework of archaic rules. We can take as an example the texts relating to intellectual property law, where with regard to filing forms, the note "signed by his/her hand" was replaced by "signed by him/her in person" in the version authorizing digital filing certified by an electronic signature.

The expansion of communication involving digital and multimedia technologies has led to the need for these new communication channels to be included within the framework of a mutual "pact of trust" between citizens and the State, so that the legal requirements can be clearly indicated and, above all, easily identified.

Thus a "pact of trust" of this sort is at the heart of the company modernization policy.

It is based on two essential founding elements:

- The first specifies, in particular, the legal requirements in terms of secure identification.
- The second shall explicitly authorize the use of the digital channel for all acts and transactions, and the general validity conditions for these exchanges.

Ensuring identification reliability

The reliability and security of identification documents are testament to the identity of those taking part in the exchange, and ensure the protection and confidentiality of the data exchanged.

These documents are produced upon presentation of recognized civil-register documents, or corresponding certificate extracts (birth certificates, population registries, etc.).

The civil register is, from this point of view, the parent database, certifying the authenticity of identities and family ties. Modernizing it and ensuring its reliability is generally the keystone to the whole procedure and the first of the corresponding projects. **The civil register, with its reliability ensured in this way, generates "founding documents"**, providing a base on which **secondary secure documents** (electronic or biometric) can be produced (public official's card, ID card, passport, resident permit, driving licence, health card, social security card, etc.)

Adapting the legal and regulatory framework

The legal and regulatory framework beyond the strict authorization to proceed by digital channel shall be covered from a global perspective, encapsulating the complete e-Government program. Its aim is to produce a legal basis for all of the rules establishing the "framework of trust".

It is operative once it ensures the continuity of rights in all circumstances and all communication channels with the same legal security, specifying in particular:

- The validity of written documents, contracts and digital exchanges, of digital identification and electrical signature in compliance with international standards,
- Rules governing citizens' electronic relationship with respect to public services and to e-commerce,
- The definition of Private Data (DCP) for each citizen and the rules to ensure its protection,
- The rules governing digital management of the civil register, including, for those countries that have opted for it, the rules of use for associated biometric databases.

Managing and unifying the program and its challenges, and measuring the results

The entire procedure generally relies on tight coordination between each of the State services involved in enabling such a plan to succeed, focusing in particular on:

- Inter-ministerial coordination, often under the auspices of the Prime Minister, at times the Finance Minister, who strategically manages the State's modernization procedure,
- A technical or operational inter-ministerial committee for the "Modernization of Public Services",
- An inter-ministerial technical platform providing a link between the various ministries, offering assistance to the different public services concerned, covering in particular the IT operation for the creation, distribution and inspection of the validity of secured documents (also see below, "basic architecture of an e-Government system"). This structure shall be referred to below as the "National Technical Service for Secure Documents"; it shall be ensured in particular that this is in close relation with the civil register which constitutes the highest-level reference in terms of "root" identification.

In a number of states who wished to establish a strong association between the regional and local authorities and the national e-Government procedure, a group of regional representatives has been created **in which all the levels supporting the e-Government deployment are represented.**

Some countries, such as Belgium and Austria, have even established their own approach for the marketing and targeting of their services, based on this representative group. Because the regional level is necessary in order to guarantee success at a local level and community-based support, it is clearly advantageous to associate them within the foundations of the program in local life.

For example, the national identity card, e-ID, may be created in such a way that by default it paves the way for certificates that may be personalized, thus allowing **the ID document to be considered as a "citizen card"** offering access to specific services available at the holder's place of residence. This is the approach chosen in Portugal, Austria and Germany, where the "citizen card" has made it possible to better express the public will to put citizens at the heart of the entire e-Government 2.0 program.

4.2 Designing the global architecture for a national e-Government Program

Basic architecture of an e-Government system

The effectiveness of e-Government depends on its ability to efficiently deal with the needs of citizens or companies. This effectiveness inevitably depends on the capacity of State services to share and coordinate resources for the benefit of the user.

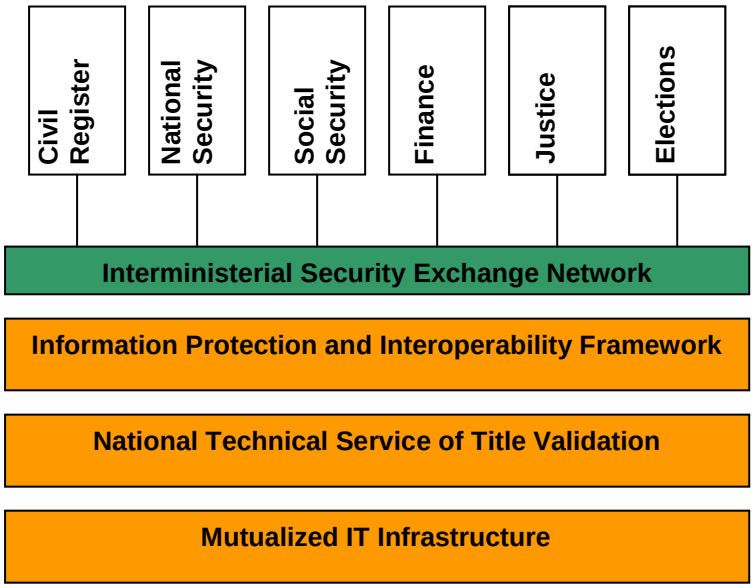
The majority of states implement a platform performing a role of workflow for administrative information via a shared platform, with a view to rationalizing spending whilst ensuring maximum basic services are provided for all administrations.

This shared architecture aims to:

- Implement the framework for future developments,
- Increase security and reliability (eliminate duplicate input)
- Ensure Inter-operability for all ministries
- Deliver considerable financial savings for the State's budget,
- Reduce effort and incremental investment for the modernization of businesses and domains
- Be able to meet, in a coordinated manner, the complex needs of citizens (e-Administration).

This three-level shared platform fulfils the following roles:

- Provide the architecture and high-speed network for inter-ministerial services
- Accommodate the back office for all e-Government applications, and front offices for those ministries that require it
- Offer hub services on behalf of all public services in order to be able to optimize and reduce the costs of controlling and validating the authentication of users for the State's electronic services, already deployed or currently undergoing deployment
- Facilitate the production and distribution of secure IDdocuments, including biometric documents where relevant
- **Put in place trustworthy services and the National Trusted Third party that the State requires** in order to obtain Certification Authority for X509 certificates for secure documents, in order to have access to and **promote widespread use of secure archiving, time-stamping and electronic-signature services.** To this end, it hosts the State's Certification Authority, the system for validating electronic signatures and authenticating all the elements that make up secure documents issued by the State
- **Put in place a public Trusted Third party that is autonomous and independent,** guaranteeing data and privacy protection and implementing the principles of end goals and proportionality in the inter-operability of public databases containing DCP (private data), in accordance with the terms of the law in force
- Where applicable, host, in a separate manner if possible, services allowing the Trusted Third party in charge of controlling and protecting citizens' privacy, to have the operating facilities of the authority allocated to it
- Host, where relevant, services of citizen portals or companies enabling better coordination and simplified access for the citizen to all applications developed by the State's other ministries and services.



Interministerial high-speed exchange workflow

Interoperability - Privacy protection and Trusted Third party

A key question concerning the implementation of an e-Government program wishing to comply with the standards recommended by the OECD, UN and EU in terms of the protection of private data, is finding the most suitable compromise between inter-operability and cross-checking of private data to achieve greater efficiency on the one hand, and separation of the domains in order to respect citizens' right to privacy on the other hand, with regard to health or finances, for example.

It should be noted that the definition and the method of protection of Private Data (DCP) varies according to the specific legal and regulatory framework operating in each state.

The two main principles governing that which is considered "the state of the art" in terms of inter-operability and DCP protection are:

- **The principle of end goals**: in an interoperability platform, each proponent is strictly only able to access the data for which he/she possesses mandates legally authorizing consultation.
- **The principle of proportionality**: in an interoperability platform, in response to a proponent's query, he/she only receives data that corresponds strictly to the query formulated.

Thus, for example, in response to the question, "is this citizen, named "X", holder of driving licence no. "Y", aged 18 or over? The response will be YES or NO, without any information as to the age or date of birth being provided.

It is specifically the role of an interoperability platform to implement the "**shared framework of trust**", verifying that the proponent is suitably authorized and the response is compliant with DCP protection rules. It may be set up either at a third party, subsequently known as the "Trusted Third party", or in the form of common exchange rules in a front access service for each of the services in charge of performing controls. In this case, this front-end service is referred to as a "**Trustworthy access point**".

Public Trusted Third parties for protecting privacy?

An increasing number of countries is entrusting this interoperability to one or more public-sector bodies in charge of ensuring personal data protection in compliance with the two principles set out above. These public-sector bodies, known as "Trusted Third parties", guarantee that privacy will be protected. Depending on the country concerned, they are sometimes made up of public-sector operators guaranteeing protection against any interoperability abuses of citizens' personal data - whether by companies, individuals or government bodies, and may have genuine legal powers to take disciplinary action or enforce compliance.

The diagram above also illustrates the layers of interoperability that it is important to regulate in exchanges between government bodies, both at national and international level. It should be noted that in a relationship of trust between two organizations, the founding element enabling mutual trust is for each party to recognize as reliable the organization method of the rules of trust of the other party within their own environment. This bilateral - or multilateral - agreement thus establishes what is referred to as a "Circle of Trust", and the set of rules accepted and made mutual lead to the establishing of the "Framework of Trust", where interoperability amongst members of the Circle of Trust is known to be in place.

Three architecture models for the interoperability of identities and services with e-Government

Three main models, enabling exchanges between citizens and the various government bodies to be regulated, currently dominate the choice of installations meeting interoperability needs.

- **The unique identification system** organizes the protection of data, e.g. by putting in place a national privacy protection body, which acts as a Trusted Third party and exchange operator. The aim is to protect citizens from interoperability abuses within the information domains and to check that the rules stipulated above are strictly complied with (Belgium). It should be noted that in Belgium the state has gone even further still by putting in place five Trusted Third party commissions for privacy protection, compartmentalized by domain (public-sector administration/interior ministry, finance, health, social matters and justice)
- **A multiple, unified** identification system, in line with the model proposed by Liberty Alliance, where a unique secret acting as a link between identifiers by information domain is held by the citizen and/or a public privacy-protection body providing a national service validating identifiers and enabling monitored interoperability amongst identifiers (Austria). Austria considers it to be the role of the state to guarantee the security of the founding identity "token", entrusting it to the citizen and the privacy commission, but it is then up to citizens to say in what format and with which distributing body they wish their "identity" to be held, bearing in mind that they may choose several options. These secondary identifiers taken from the same origin are not interoperable and do not enable a return to the civil register origin, this being protected.
- **A partitioned identification system** - where, by its construction, identifiers may only be connected by the citizen personally. The document, by way of convenience, may feature several identifiers in the form of a "portfolio" of identifiers, avoiding the need for the citizen to carry a large number of secure documents (Portugal).

Thus, each identification system will have its counterpart ensuring both the effectiveness of the response with regard to the need, and compliance of the control with the two founding principles of private data protection.

In Austria, the state guarantees the security of the founding identity token. Citizens choose the format they prefer: the citizen card is one option, but there is also the mobile telephone and the credit card…

In Portugal, the ID card features severable visible identifiers on the front and back of the card. The constitution prohibits the use of the unique central file for all domains.

4.3 Ensuring the identity system's reliability: the basis of trust in e-Government

When it comes to the question of modernizing the relationship between citizens and the community or public-sector bodies in order to improve the ability of each individual to exercise their rights and responsibilities, and even to ensure social justice, the fight against identity fraud clearly becomes a critical area in which progress must be made.

But what would be the point of issuing secure documents if the civil register and its source data are easy to falsify and even corrupt with an uncertain version history?

Strengthening the civil register's reliability

As seen in Portugal - where the state has devoted several years to validating its civil register reference database - citizens having two surnames and two first names, for which they are able to choose, and change, the order - the issue of consistency, reliability and harmonization of the civil register is a challenge often at the very heart of citizen identification policy, in order to obtain reliable, standardized guidelines needed to provide secure access to data and help combat fraud.

When it comes to the distribution of **secure documents, the advantage of starting by focusing on Public official** cards is also an essential point, ensuring the reliability of the requests received for secure documents, which will be electronically signed by certified officials, thus reducing the rare, but possible, temptation to commit internal fraud.

Towards a biometric Civil Register?

One starting point when consolidating or harmonizing the civil register is to look for the unmistakable element with the greatest reliability which enables an individual to be identified.
In many countries where names, addresses and dates of birth are standardized and reliable, this basis can be used as an identification reference system. Biometry is, in such situations, a simple attribute that makes it possible to secure the link between physical person and data.

In countries where semantic standardization work on citizens' names is not entirely finalized, we might reasonably assume that biometric recognition will most likely be the common element with the greatest reliability. This will as the basis of identification.

On this point, it should be noted that it is generally considered that although identification data is shared between the citizen concerned and the government bodies, the civil register data is however generally viewed as representing Private Data. Such data belongs to the citizen personally, who entrusts it to the State in the role of notary and archiver, and then presents it when requesting an official document issued by the State. The civil register, in this sense, may incorporate an individual's biometric data, as soon as this can be considered, barring accidents, as being permanently valid and reliable.

In the case of biometric databases compiled previously, the issuing of residence permits, new electronic identity cards and biometric passports will be an opportunity to update biometric data and check the doubly unmistakable relationship of fingerprints to name held on civil register.

Public official documents also enable a pilot sample of the distribution of secure documents to be produced.

This sample has proved to represent a non-negligible advantage in that it enables reliability of the back office to be improved and its switch to digital exchanges to be speeded up. This offers an initial opportunity to improve efficiency and reduce processing times for government bodies. The on-line services that are then to be implemented will offer even greater performance.

4.4 Modernizing the State - What needs to be changed? And what should be retained?

Strengthening democracy and social cohesion - A central theme at the heart of the project

Before answering this major question, it ought to be remembered that uptake will only occur once the citizen can clearly identify both the benefits of the new approach, and the points of reference in terms of his/her understanding and usual habits with regard to his/her dealings with public-sector services.
In the absence of these two elements, there is a risk of creating a climate of distrust, and leading to a substantial, costly need to offer explanatory training and guidance.

To this end, it is particularly important to ensure **the continuity** of the crucial element **of social cohesion:**

- Authority of the collective
- Trust which legitimizes and supports it

This continuity establishes itself further in enabling the citizen to recognize it and to associate it with the unifying, public character of the e-Government program.
The introduction or mixed access to commercial and non-commercial services must therefore be carried out with great precision and rolled out in phases that correspond to the time needed to learn about the services and to establish new points of reference.
To confuse different communication subjects in wanting to deliver a large number of services too hastily, for example, would be particularly counterproductive and could undo a lot of the strategy of recognition and passing-on of the system of values borne by the e-Government program.

Building up a framework around a strong value system ensuring the public's interests.

Authority and trust are the two extremes of the same spectrum which together form the basis of social cohesion. Likewise, transparency and traceability feature amongst the signs and attributes that are essential for a modern democracy promoting social cohesion:

- Indeed, in response to the trust expressed by the citizen comes the requirement for transparency that the authority must accept as being part of its contract
- In response to the power exerted by the public authorities, comes the traceability requirement, which citizens must accept as being the guarantee of the framework of trust and the fundamental component in order for them to define themselves freely and to act within the collective framework.

Authority, trust, traceability and transparency: these four components represent "untouchable" fundamental components for success in an e-Government procedure and for adhering to the modernization that it brings about - they must take the form of signs and codes (e.g. a label) that are easily recognizable and identifiable as representing the public interest that the e-Government program intends to develop:

- If the e-Government program is underway: in this case these fundamental principles should be emphasized or rebuilt to add a new dynamic to the procedure, and include it in and make it a permanent feature of the framework of chosen values based on the collective's authority.
- If the e-Government program is just beginning: these fundamental principles shall be put forward as a thought system and body of rules to be distributed. Anyone appointed as a partner to the procedure shall comply with them and can illustrate their participation in the subsequent communication and implementation guidelines - security, trust, data protection, the right to transparency, etc. to gain the trust legitimizing and responding to it.

Example: "e-Government"-certified health card (Identity secured by the State, transparency and traceability controlled by the patient, protection of data guaranteed, etc.)

The choice of partners and methods for promoting widespread use of the program are therefore essential to ensure uptake of the program and ensure its foundations are established in everyday life.

Transparency and traceability - the criteria that constitute a modern democracy?

The fear of the "Big Brother" syndrome is something everyone is conscious of, and this remains a major obstacle to implementing the effective interoperability of data. However, we need this interoperability if we are to respond in a fluid, rapid manner to the specific needs of each citizen, whose personal situations are each complex and specific, according to their different status positions with respect to the social, family, tax and economic aspects of each individual case.

How can the role of traceability be understood and re-examined?

- Traceability is present everywhere in our global and digital environment: mobile telephones and credit cards have been the main vectors for several years, without encountering much in the way of opposition.
- The issue no longer centers on avoiding traceability, but rather on mastering its unilateral and untamed character, to make its usage and set of rules socially-acceptable, within a framework of values respecting both general and individual interests.

Role of traceability in a modern democracy:

1. From the Tables of Mosaic Law and Koranic law to the International Human Rights Charter via Napoleon's 1804 Civil Code, what constitutes the very foundation of social cohesion is an invariable element that enables a society to function, with rules allowing its citizens to live side-by-side: Law.

2. While it may no longer be possible to *control* flows at the outset in order to secure them, it is important to at least be able to control them at a *later stage* in order to guarantee the continuity of the principle of responsibility, and therefore that social, economic, civil and military data, etc. may be audited and attributed.

3. In a world that is completely open, traceability is therefore the only residual guarantee of being able to ensure that national and international law works smoothly.

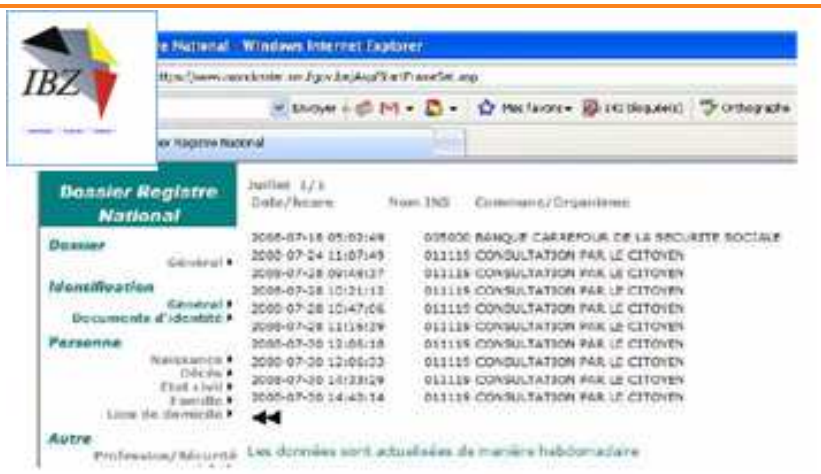
4. The switch from a context of control in which matters are closely regulated from the very outset to a completely deregulated environment controllable only at a later stage is the consequence of this opening up and globalization. It has brought about a major cultural transformation where systematic control has given way to responsibility combined with traceability. For example, no-one would consider it worthwhile re-establishing systematic customs checks in the context of today's economy.

5. Traceability is the price to pay for having a world that has opened up. Indeed, it is the greatest possible guarantee of the development of freedoms, as it enables every individual to freely exercise their enterprise and development responsibilities. This increased freedom becomes a reality if traceability is combined with a balanced idea of social cohesion, in other words: that the citizen is granted the right to access the data concerning him/her, and indeed to act on them, within conditions set by law and by the community.

6. Transparency is therefore the necessary counterpart to a "positive" traceability whereby the citizen can freely access his/her data and consult them in order to personally take action to protect them. This does not exclude the support of "Trusted Third party" public-sector bodies with the role of protecting privacy.

In the Belgian e-Government program, access to the "Mondossier", or "Myfile" application is a right offered to Belgian citizens when they are issued their e-ID Card. In the "Myfile" file, for six months a Belgian citizen can consult all transactions performed by State administrative employees who have accessed files using his/her civil register data notarized in the National Population Register - with the exception of exchanges relating to State security (Justice and National Safety).

The application comprises an on-line form enabling the citizen to request an official explanation from the government body that accessed his/her Private Data. The following information appears on the screen: date and time of consultation; the name of the person who consulted this data, if the consultation was performed via identification with an electronic card; the code of the organization that performed the consultation, as attributed by the National Institute of Statistics or by the National Register, and lastly, the name of the organization that performed the consultation.



It says a lot that for months on end this application was consulted more than any other when the Belgian e-Government program was started up. It has quickly come to be considered a new right associated with the Belgian e-ID electronic Identity card.

It has proven to be effective in ensuring uptake of the program; and Belgian citizens subsequently eagerly awaited the roll-out of public services, and then semi-public commercial services that the card could give them access to (Post offices, Transport, local services, on-line police complaints, etc.)

In short: the four foundations for fostering trust and acceptance of an e-Government program:

Authority

To what extent can I see that the service acts on behalf of the general interest, makes use of existing government services or carries an "official" status, and protects me from abuses and promises that result in me being less vigilant?

Trust

Am I able to recognize the familiar characteristics of the service I want to use? Can I recognize the signs and codes used identify the objects with which I have had physical contact? Am I guided and assisted according to my needs?

Do I have an "e-Government" label showing me that the service forms part of the Contract of Trust guaranteed by the government authorities, and which ensures that I am permanently covered in terms of legal security and the protection of my data?

If I have to pay, am I confident that the exchange is highly secure and that it does not present a risk to me? In the event of a fault, can I be sure that I shall not be debited in error? Can I check that everything has gone smoothly and am I reassured by the service at each stage? Can I go back at anytime and undo what I just did before final validation and confirmation that my transaction is complete?

Traceability

Does the service make it possible at any time to retrieve what has been done and, in the event of a dispute, demonstrate the effective responsibilities? Is it guaranteed that all exchanges can be audited and attributed to enable the service to be duly protected from misuse and attempted fraud? Is this traceability suited to my needs and is it implemented under the auspices of a Trusted Third party who ensures my privacy is protected?

Transparency

Does the service warn me about what it is recording and does it show me how to access and view the data that I have entered if I wish to do so? Does the service offer me personal access to my data and does it give me the impression I am alone in being able to access them? In the most advanced cases, may I, if my legal and tax status allows, request that all data relating to me be deleted, in accordance with the provisions offered by law to protect my privacy?

4.5. Choosing service operators and partners to promote the widespread use of the program

The choice of partners to promote the widespread use of an e-Government program is based directly on the uptake schamtic described in the previous chapter

In terms of timing, the process of promoting the widespread use of an e-Government program and the search for partners forms part of a cycle that can now be set out clearly:

Phase 1 - Launch and building of foundations:

1. Definition of the program and communication of the **Charter** describing the authorities' will for modernization and transformation,
2. Construction of the system and the **legal framework** of trust extended across all modern communication and local community-based resources (physical, digital, wireless, audio, video, etc.) to respond both to the needs of citizens and government authority effectiveness,
3. Construction of **founding documents** and ensuring their reliability (civil register - identity cards) and methods of legal validation (date and signatures) for certificates and individuals interacting using digital channels, complying with international standards for secure documents and distribution of the first Identity documents,
4. **Communication** on the Charter of values representing the status and modernized social cohesion, as a constant point of reference for uptake of the program,
5. Delivery of the **first flagship governmental services** providing real benefits to citizens or companies,
6. Delivery of **other governmental documents**, interoperating securely, for new e-Government domains (Social security card - complementary health insurance card (direct payment), health card, resident permit, driving licence, etc.).

Phase 2 – Distribution, extension and generalization:

1. Building, at the same time, of the entire **back office for public information interoperability** and for the shared workflow ensuring optimization of administrative processing,
2. Distribution of an integration package and an **e-Government label** enabling the certification of services serving the general interest as respecting the Charter and applicable to any e-Government program,
3. Extension to local authorities and delivery of **local e-Government services**, emphasizing the citizen nature of the program and the capacity of documents issued to provide numerous benefits within local, day-to-day life (personal services, access to local mediation services, etc.),
4. Extension of the program to a **broad network of "collective" partners**, semi-public (electricity, water, gas, transport, medicine, culture, leisure) or private-sector (Banks, Telecoms) entities - each being certified as compliant with the common framework of values of trust, security and quality of service or at the point of need. Each partner can incorporate public elements of the e-Government program in the documents that it distributes according to the conditions imposed by the public-sector program framework,
5. International **interoperability** of documents and exchanges, recognition of documents supplied by the international community.

Communication, with a view to strengthening the collective value system borne by this program, shall accompany every stage. Basically, the ultimate goal is very simply to comprehensively and collectively transpose all of society's social and economic bodies into a modern, competitive framework enabling growth, services, well-being and human development.
It is therefore clear to see that the most resistance is likely to stem from our cultural baggage, which over time can reach across a complete generation, without letting up. The Smart card was born in 1979. The first social security smart cards appeared in the late 1990s. The first e-ID cards appeared between 2000 and 2003. Today, health cards are the latest smart cards to see the light of day; perseverance is important.

Partners for developing the modern ties reinforcing social cohesion

1. The choice of partners for the program shall take into account that the State is looking for a distribution network that will ensure that success of its program.. The role of government authorities in this sense is not so much to deliver services but to build an infrastructure that can act as a catalyst, both to new types of use for the community, enabling every citizen to become more involved socially and economically in their local area, and, moreover, create a new ethos in the provision of public-sector services.
2. This is the meaning behind the English expression, "Citizencentric Government".
3. But to avoid apathy during the transformation and in order to set a good example, government authorities must concentrate their efforts on launching sufficient e-Services to ensure a critical mass of flows to then produce the virtuous spiral for all other government and economic players.
4. The launch of portals of services to citizens and companies meets this necessity, in addition to the clear improvement that this brings about both for the administrative functioning and for the citizen.
5. It is when it looks to launch this virtuous spiral that the distribution network starts to really take form. The e-Government program network is built using the conventional channels of a genuine marketing initiative (according to the 4Ps theory: Product – Price – Place – Promotion) where, the product having been defined by the State as a public-sector service provider, it is now a case of ensuring the most widespread use possible.
6. The countries that have approached this point from the marketing perspective set out above are those that are today displaying the highest rate of success.
7. This is how the example of the partnership with the Bank in Austria or Portugal should be interpreted. There, they receive a mandate and certification as partners of the national e-Government program, testifying to the quality with which these private-sector operators work together and communicate, via their services, the trust and authority of the State in its will to strengthen social cohesion. Evidently, this is a promotional initiative which offers these private-sector operators clear advantages in terms of building loyalty among their own customers.
8. In these examples, the citizen, the appointed operator (Bank, Telecoms, etc.) and the state work within the same framework of trust and authority that unites them; this is the principle of social cohesion.

These boutiques represent the link that Portugal has chosen in order to design its global procedure to modernize social cohesion: to experience in person an integrated approach to administration, new and completely rebuilt around the citizen, before presenting the result on the internet via a portal of integrated services.

At a time when e-Government 2.0 can be considered as representing the quintessence of Web services, it is good to be able to **draw on lessons from the Portuguese experience:**

- **Continuity** - we rely on what does not change for the transformation to be a success - uptake is built up around the continuity of the fundamental frameworks. And if the points of reference have to be changed, guidance will need to be offered, and it will be important to ensure positive feedback in order to foster peoples' trust.
  Any changes made must be attractive, and this comes after the intial phase which will determine whether citizens choose to accept or to reject the changes.

- **Provide something tangible** – to encourage uptake before then implementing in a virtual environment, especially for an environment where the internet and digital technology have not reached the deployment critical mass.

Citizens' Boutiques in Portugal: Constructing citizen 2.0 before putting it on line!

Anabela Pedroso, President of the Agency for the modernization of public services in Portugal

"e-Government is too conceptual !
Concrete reference points are needed first to build trust. The citizen shops (Lojas do Cidadao) are a new general interest concept."

"We need to prove to citizens that a paperless approach brings real benefits and added comfort. The citizen boutiques enable us to demonstrate what a one-stop shop looks like: Learning and trust begin with face-to-face contact. At least 5 years are needed for a real cultural change to take place. Face-to-face contact is even more justified for proximity services, which must not be neglected as it is where the most tangible success is played. It is then all the simpler to transpose into e-Services the reality that citizens are familiar with - the points of reference are thus acquired and the necessary learning has taken place. They are able to recognize the signs and codes, which they then find on-line. »

Modernizing social cohesion requires a global approach covering all aspects of citizens' life.

This is the reality that the citizen boutiques wished to embody. They offer all Portuguese citizens a concrete experience of what it means to have integrated public-sector services: an experience that is very real that has formed part of their everyday life for several years already.

Citizens can expect this same level of integration when connecting to the country's e-Government services.

The “citizen boutiques” come under the responsibility of the Institute for the management of citizen shops, an administratively and financially independent public-sector institute. Inter-ministerial in its mode of action, it comes under the authority of the Ministry of Finance.

What is innovative about this public experience is that it has redesigned according to a perfect, state-of-the-art marketing initiative. Its real ingenuity lies in having been rebuilt around its citizens, the requirements they express, their need for trust, the image they would like to have of the public domain, with absolute humility on the part of the Agency for the modernization of public-sector services, who patiently built up this unprecedented success.

The attention to detail offered by these new sites goes as far as **incorporating citizens' pleasure** and emphasising the citizen in his relationship with public-sector services. With the new "boutiques" located in shopping centers, information panels located on every floor provide information on the queuing times at different counters, offering citizens the choice of doing some shopping or relaxing at a café until their turn comes at the counter they are waiting for.

Another example of the attention to detail is to have dared to embark on a purely semantic front-office approach for the service, with the paths to follow marked out and with all-integrating terminals - "I've lost my wallet", "I'd like to take my retirement", "I'd like to create my own business in an hour", etc. The aim of these counters is to mask the complexity of the inter-operability of the services in the background.

From tax services, the interior ministry, the civil register, welfare services, services for making medical appointments, adult education and training services, postal services, railways, electricity, gas, telephone, public television channels, solicitors, lawyers, accountants and registrars to an industrial property office, the efforts of 90 different points of service are combined. Also included are municipal services, immigration services and services to assist individuals in precarious situations.

The service is incorporated and the Entrepreneur point of service enables anyone wishing to make the leap into business to receive the advice and assistance they need in order to meet the challenge of creating their own company in less than an hour - registration of trademark, status, register, registry recording and social security and subsidy files, all included. In the citizen supermarket below, more than 200 companies were created in January 2008, the month of our visit. This new center was already receiving more than 4,000 visits per day 20 days after opening. The main center in Lisbon receives up to 12,000 visits per day.

The citizen boutiques bring all public services together in one place, with an optimum level of integration and inter-operability. With it receiving visitors Monday to Saturday and its level of service, it looks much more like a trendy shopping arcade than an administrative center.

The Lisbon offices cover up to 10,000m2 per center, some over two floors connected by escalators, making them feel surprisingly like a luxury boutique.

Pathways marked out by domain, and counters for ministries, town halls and post offices, electricity and gas (shown here), all brought together in the same place, sharing the same back office.

This center located in Lisbon's suburbs, set up in a vast shopping mall, has received more than 4,000 visits per day since opening in January 2008.

Since this project began seven years ago, more than 60,000,000 administrative acts have been recorded in the 10 centers opened to date.

4.6 A few more key factors…

Political and legal aspects

Political leaders and governments are responsible for expressing public will, and they are in charge of carrying e-Government projects forward. To do so, they need to know how to adapt the legislations in force. The legal framework needs to be designed at the same time as the range of services. The legal framework is traditionally slow to develop and often requires parliamentary approval. It is important to plan the lead-times and deadlines sufficiently early.
Local government authorities can act as experimental 'laboratories", but the national framework is essential in order to obtain homogeneous, interoperable construction of social cohesion as a whole.

Economic aspects

e-Government is a long-term society-based procedure requiring large-scale financial investment. The political justification will be made easier if services enabling quick returns are developed.
Several examples can be cited of quick wins" in terms of savings: Direct payment by complementary health insurers for social security cover - food aid in very poor countries - social services - Smart card travel documents that can be used in the digital environment, on-line police complaints, etc.

The on-line tax service is often a success if it considerably reduces the declaration workload, but it does not occur sufficiently frequently and its central theme is too far-removed from social cohesion concerns and those of citizens' everyday life. However, with it facilitating financial entries and making them reliable, this can offer an excellent political justification for building the entire back office, onto which other services can then be added.

It should not be forgotten that in such a long-term procedure, the dividend is political before it is financial.
A motorway is never cost-efficient on the day it opens! It is built as part of town and country planning.
The same applies to e-Government, where the scope is society-based planning

Technological aspects

e-Government is a powerful catalyst for the development of NTICs, which can deliver a definite financial ROI. in the Keynesian sense of the term: Trust frameworks, exchange standards facilitate companies' competitiveness and the modernization of public-sector organizations. This transformation is also the source of major innovation that filters down into the GDP and into the dynamism of an economy.

Socio-cultural aspects and other factors of uptake

e-Government applications must place the citizen at the heart of the system in order to obtain an optimum success rate. The citizen's view of modern society leads to a reversing of the flows, now led by demand. As a result, citizens read their social contract as the possibility to be themselves, "different and unique", in all forms of the social ties that link them to the community (Parent, Teacher to their children, entrepreneur, employee, individual on a social level, individual on a citizen level, individual looking to find their own personal cultural or harmonic development, etc.).

But the very globalization that offers every individual infinite access to all desires and all knowledge has introduced the destabilizing element of solitude, where individuals search for new points of reference to enable them to create tribes, villages and social groups, the primary biological need of homo sapiens.

Strengthening social cohesion also means respecting the very root of what creates the cultural bond within a group. This helps understand the move in Saudi Arabia to enable e-Government to facilitate access to prayer times and the prayer calendar. Because in Saudi Arabia, this subject represents a community-wide element.

More than ever, modern man is in need of local, community-based services, the most vulnerable in society need them more than anyone else. The e-Government program must not overlook this need. This is also a major factor for uptake.

e-Gov 2.0: The keys to success

Choosing and building the pathway to success
Best practices and operating procedures

CONCLUSION: When the State becomes a service provider

The reversal of our relationship with the concept of the public interest tends to lead us to consider Public Authorities as a service provider to whom we have entrusted the task of managing our rights and protecting us from any risks, who in short has a tacit contractual obligation to meet our individual needs.

Nevertheless, the attachment to public-sector services remains strong, as we consider them to be impartial and therefore more ethical than private-sector services.

It is therefore not surprising that e-Government has been most successful in areas where public authorities have wholeheartedly embraced this cultural transformation, presenting themselves to the public as a service provider that has taken on board the changes in outlook, giving citizens a say in how this transformation manifests itself.

Those who have best “marketed” this cultural shift and positioned the public authorities as a service provider that is capable of driving and promoting change, rather than reluctantly enduring it, have achieved the most spectacular uptake rates. This is only the case if this positioning has been accompanied educational efforts.

In short, and herein lies the ambiguity of modernization and its communication, the promoters of an e-Government 2.0 program should ideally:

- Demonstrate their capacity to provide a service that is as efficient, inventive and pioneering as private-sector service providers, in particular by using the best methods and tools from the private sector (NTIC, Marketing, Customer Relations, Payment, Access, etc.)
- Maintain, but also emphasize, an image of their authority, ethics, symbols and value system which create a sense of community and the will to live side by side; in short, to act out their role of guaranteeing social cohesion.

This helps us understand why, in the vast majority of countries, e-Government has been experienced as a national challenge where citizens are encouraged to develop a real feeling of pride by participating in the modernization process. The close attention that various countries, particularly in Europe, anxiously pay to the annual rankings that assess their progress and their use of any favourable results to support their argument is quite emblematic.

As we bring our overview to a close, in the "e-Government family" we should not forget to consider the increasing demand in terms of e-Democracy: This self-assertion and rapid transformation from "passive consumer" to "active consumer" brings about a second cultural transformation which leads to participatory management and transparency in the democratic process.

The world of ideas and civic participation is in turn, driven by public demand. E-democracy is in its infancy and will rapidly become a key cultural and societal trend. the most common example at present is electronic voting. However, Estonia’s interactive Council of Ministers on the Internet is no longer an isolated case. The town of Issy les Moulineaux in France uses the same system, as do many other towns.

e-ID: from Identity to Electronic Identification - the key to Social Cohesion?

Identification is used to authenticate our identity when we access Public-sector Services - and enables the management of the authorizations granted to us, according to who we are, what our role is and what mandates and rights we have, to obtain the benefits of our request.

Digital identification opens the door to access our rights and is the key to our personal filing cabinet where we store the files we have entrusted to the State in its role as Public Notary.

Thus we can see that its reliability is key to the trust that will be placed in the entire e-Government system.

This is why the basis of any procedure must begin with ensuring the reliability of the Civil Register - The founding document upon which identification security is to be based.

Unified identification - Unique identification - and Multi-service documents

Some states have preferred multi-service and multi-identifier identification documents. When communication between identifiers is essential for the service that we require, we need to be able to trace communications in a transparent manner to make sure there is no abuse. Three governance systems for Identification and protection of flows are therefore observed:

- A **unique identification system** where a national organization for privacy protection acts as a Trusted Third-party and data exchange operator, protecting citizens from interoperability abuses within the information domains (Belgium).
- A **multiple, unified identification system**, in line with the model proposed by Liberty Alliance, where a unique secret acting as a link between identifiers by information domain is held by the citizen and/or a public privacy-protection organization providing a National Service validating identifiers and enabling monitored interoperability amongst identifiers (Austria).
- A **partitioned identification system** - where, by its construction, identifiers may only be connected by the citizen personally. The document, by way of convenience, may accommodate several identifiers in the form of a "portfolio" of identifiers, avoiding the need for the citizen to carry a large number of secure documents (Portugal).

Traceability and transparency - the fundamental elements of the modern Social Contract?

It is no accident that citizen data access websites such as "Myfile" (Belgium) are so successful, as they show all the uses made of personal data by government bodies. Transparency is the necessary counterbalance to traceability that is an automatic consequence of an open, deregulated environment. The balance between transparency and traceability enables a contractual approach to be envisaged between the "Customer", i.e. the Citizen, and the "Operator", i.e. the State. In response to the traceability imposed by the "Operator" State authority comes the transparency demanded by the consumer, this being essential to citizens' trust and backing.

e-ID, a key to the uptake of e-Government

As e-ID is a central element in building trust and protecting citizens with respect to the digital management of their files, it is hardly surprising that e-Government is most successful in countries that have organized widespread use of an electronic identification system **guaranteed by the State.**

e-Government: the Front Office of a "service-oriented" State

If we were given the almost impossible task of defining it in just a few words, we would say that it is the Front Office of the Operator managing the **"Public Authority-Citizen"** relationship, whose ultimate aim is to contribute to the **optimum efficiency** of the positive relationship between these two parties.

If we were to bring together all the e-Government best practices observed to make up the ideal site**, particular attention would be paid to:**

For the Individual/Citizen

- Organizing access to and layout of the site according to users' needs, with an access by end-use and by rights field. The State's back office has its own structure, but this must be hidden from now on. When we order a car, the manufacturer does not tell us about the difficulty involved in swapping parts from one production center to another. This is normal. It is the same for government bodies.
- Organize and facilitate learning. For example, in Estonia, e-Government is currently included in the civic education of young people.
- Promoting the service, facilitating information-gathering and knowledge acquisition, organizing communication in the same way as modern private-sector service providers manage their Customer Relations.
- Coordinate and pool information to ensure accessibility and responsiveness, and meet the demand for real-time services which is currently becoming widespread. **Offer the possibility of face-to-face communication as well as electronic services in the interests of promoting.** e-Inclusion and solidarity with the most disadvantaged.

For government bodies

- Drastically reduce unnecessary bureaucracy, undertake necessary reengineering work, ensure interoperability of processes and migrate from a paper-based culture to an electronic culture: …this may represent something of a revolution, but it is a necessary transition.
- Prioritize the need for transparency, whose effect on uptake and success is proven and undeniable.
- Providing citizens/consumers with a positive image of their day-to-day life in all domains and instilling as much as possible the feeling that their relationship with public-sector management is built around them, by them and for them.
- Maintaining points of reference acquired, particularly those relating to the fundamental principles of Social Cohesion at local level, to encourage faster uptake and ensure the continuity of the principle of the Authority as an integral part of any relationship between Individual citizens and the Community. These points of reference are an important factor in ensuring continuing trust, which will encourage citizens' acceptance of the calculated risks taken in modifying the methods and means to create a modernized public service
- Emphasizing the protection of individuals' privacy and personal data, which is essential to obtain their trust and ensure the success of e-Government. The use of e-ID, essential if this challenge is to be met, must be designed with this approach in mind.
- Building up a secure cross-functional, shared framework common to all public services so as to create fluidity in the processing of administrative information and to be able to meet the real needs of citizens in an unburdensome manner, keeping the complexity hidden from them as much as possible. This way the service provided can offer real performance.
- Bringing together banks, or telecoms operators in certain countries, as partners for public-sector payment and including them in the Circle of Trust as vectors for the promotion of e-Government accelerates the implementation process.
- Using as many local and community-based applications as possible to promote almost daily use of e-Government will also boost uptake. Cooperation between States and Local Authorities provides a clear, positive view of Local Authorities' contribution to the national effort to promote e-Government.
- Lastly, with regard to the dematerialization of legal acts, compliance with legal provisions and the legal validity of paperless procedures must be emphasized so that this secondary, but potentially difficult question is not at the heart of the debate.

Above: 2nd generation Citizen Boutique - "I've lost my personal documents" counter and night counters (open until the shopping center closes at 10p.m.).

e-ID is a shared key to access all services, including on-line services.

Only the type and form of benefits for the customer need to remain central. The rest is a question of equipment and logistics.

Epilogue: e-Gov 2.0, the code word for referring simply to "Modern Social Cohesion"?

It is no accident that we are witnessing the emergence of e-Government 2.0 at a time in our history when deregulation is commonplace, barriers are coming down, and the world has become open, infinite and full of unlikely outcomes. Uncertainty now forms the underlying structure of the new socio-economic balance and will be central in society's attempts to achieve harmony in the future.

It is something of a revolution, and we have no measure of its scale, nor of the extent to which the vast majority of our contemporaries struggle to grasp its particular set of rules.

When faced with such a transformation, there is a natural tendency to have a greater need to find one's bearings, to belong to a group, or indeed several groups, to stimulate the need for community-based services in order to counteract the rather overly virtual, inhuman nature of the "global" environment and electronic abstraction.

We've kept things well on track: e-Gov 2.0 and "Citizen Centric" of course represent legitimate requests from users of public-sector services, but far beyond that, these are first and foremost a demand for points of reference, meaning, and a secure order, in which a clear and modern framework is established to set out or provide a reminder of what the citizen's relationship is with respect to the community.

e-Gov 2.0 is the rather modest name applied to an essential procedure for the transformation, or even the reconstruction, of the "Social Contract" and the ensuing new socio-economic balance.

e-Gov 2.0 is therefore first and foremost a political initiative that expresses the public will to rethink the social pact and to experience it fully together, collectively and individually.

It is hardly surprising then, that this reconstruction has seen its greatest success where this procedure was presented from the start as expressing an overall, consistent political will, uniting the collective and the individual, national alongside local, differences alongside points in common; in short, to weave the complete web that enables a society to move forward, to act as a guiding light and promote a shared culture.

e-Gov 2.0 has the extraordinary strength that it re-examines the very basics of the democratic process and the ways in which the corresponding duties and rights are expressed. To see its rapid extension at the start of this new century opens up unprecedented perspectives for the generalization of democratic frameworks, which go hand in hand with the current worldwide trend, still very much in its infancy, of promoting collective values such as citizens' responsibilities and the promotion of sustainability and fairness.

In short:

Whilst, as part of its modernization, the State or Government Authority needs to put citizens' day-to-day life at the heart of the transformation, it also needs to reassert the bond of trust that remains specific to it, and ensure this is easily-recognizable, immaterial and sustained.

The demands of citizens, meanwhile, are ultimately fairly basic: they simply want an efficient, transparent and protective state!

When we wanted to analyze the success of a newly launched web portal, citizens were telling us:

"This virtual world is a reflection of daily life at its most positive. It is my world: it is not intelligent but it is genuine, sincere and is close at hand, available and reassuring".

Evika Karmagioli, VP, e-Gov2U, Greece, 2008

Bibliography

BLAKEMORE, M. & LLOYD, P. *Trust and Transparency: pre-requisites for effective eGovernment* (2007).

S. PAUGAM, CNRS, EHESS - Le Lien Social - Collection : Que sais je ? PUF - Avril 2008

R. LAUFER, M. ORILLARD, *La Confiance en Question* – Ed. L'Harmattan – Collection Logiques Sociales 2000

G. LE CARDINAL, J-F. GUYONNET, B. POUZOULLIC, *La Dynamique de la Confiance* – Ed . DUNOD – 1997

François DUBET, Danilo MARTUCCELLI, *Dans Quelle Société Vivons Nous* – Ed. SEUIL – Collection l'Epreuve des Faits 1998

Wainer MUSOLI, Caroline MILTGEN – *JCR European Commission, Institute for Prospective and Technical Studies - Young people and emerging digital services – An exploratory survey of motivations, perceptions and acceptance of risks, March 2009*

Professeur Hubert ALLEMAND- Médecin-conseil national Assurance Maladie - Caisse Nationale *Prévention des risques médicamenteux : l'Assurance Maladie s'engage pour prévenir la iatrogénie. - Juillet 2006*

European Regional Development Fund (EU) - *Citizen first for e-Inclusion, December 2008.*

Agnès BRADIER , Deputy Head of the e-Government UNIT, EC - DG Infso & Media , *Le Gouvernement Electronique : Une Priorité Européenne* – Ed. de l'ENA – Revue Française d'Administration Publique N°110, 2004, pp 337-348

Peter VANVELTHOVEN, State Secretary for State Computerization, Belgium, and Jan de Prest - *Note de Politique Générale 2007*, Belgium computerization ICT General Policy 2007

Danilo MARTUCCELLI, *Grammaire de l'Individu* – Ed. Gallimard 2002 – Folio Essais

Viviane REDING, EC Member in charge of Information Society & Media, *E-Government 2010: Citizens and Business first* Ed EUROSPACE S.R.L. 2006

Youval ECHED, Etienne VEYRET, Eric BILLIAERT, Gemalto & YeMA Consultants – *e-Government 2.0: identification, security and trust, Exploring European Avenues – September 2007*

The Gemalto review – *article on e-stonia – published February 2009*

Youval ECHED – YeMA Consultants, *Un internet de confiance pour l'administration électronique,* Ed. Cahiers Stratégiques de l'AFNOR - ENJEUX N°241 – février 2004, pp 40 – 43

OECD 2008 – eGovernment studies – Belgium – October 2008 on www.fedict.be

OECD iGovernment Working papers series and Richard HEEKS, *Benchmarking eGovernment: Improving the National and International Measurement, Evaluation and Comparison* – Ed. University of Manchester Institute for Development Policy and Management, 2006

Agence Wallonne de Télécommunication, Atelier de Sensibilisation à la sécurité en Région wallonne - 12 février 2007

European Project MODINIS, *Status of Identity Management in European eGovernment Initiatives Report IIR 1,* EC DG Infso et Media - 6 June 2006

EC DG INFSO & MEDIA, Ralf CIMANDER (Ifib Germany), **Andreas AARMMA** (SK, Estonia), *eGovernment, Interoperability at Local and Regional Level, e-Id in Estonia,* Good Practice Case, 2006

EU i2010& ECOTEC consulting, A Handbook for Citizen-centric eGovernment - December 2007

EC DG INFSO & MEDIA, *eGovernment Factsheets, country profiles from www.epractice.eu*

Cap Gemini Consulting October 2008: The increasing role of citizens in service delivery

Politech Institute 2007 - Fostering Public Sector Performance in Europe

Gemalto

Gemalto (Euronext NL 0000400653 GTO) is the world leader in digital security with 2008 annual revenues of €1.68 billion, and 10,000 employees operating out of 75 offices, research and service centers in 40 countries.

Gemalto is at the heart of our evolving digital society. The freedom to communicate, travel, shop, bank, entertain, and work—anytime, anywhere—has become an integral part of what people want and expect, in ways that are convenient, enjoyable and secure.

Gemalto delivers on the growing demands of billions of people worldwide for mobile connectivity, identity and data protection, credit card safety, health and transportation services, e-Government and national security. We do this by supplying to governments, wireless operators, banks and enterprises a wide range of secure personal devices, such as subscriber identification modules (SIM) in mobile phones, smart banking cards, electronic passports, and USB tokens for online identity protection. To complete the solution we also provide software, systems and services to help our customers achieve their goals.

As the use of Gemalto's software and secure devices increases with the number of people interacting in the digital and wireless world, the company is poised to thrive over the coming years.

For more information: communications.publicsector@gemalto.com and www.gemalto.com.

gemalto
security to be free