e-Government and e-Governance:
Citizens and Cities in a Global Society
GCD Conference and Mayors' Summit 2002 ■ Bologna, Italy > 24 / 25 October 2002

Enhancing the Public-Private Dialogue and Partnership in E-Government

Key-note Speech

by Franco BASSANINI
Senator, Former Italian Cabinet Minister for Public Administration and Regional Affairs
Member of the UN High-Level Advisory Panel for ICT
Member of the Executive Board of the Ecole Nationale d'Administration (ENA), Paris

E-**government** enables a new paradigm of public services delivery to citizens and to businesses. In fact, we can think of e-government as a means of **empowering people by changing the way people access to public services, by promoting transparency and accountability in governmental action and by supporting the processes of knowledge acquisition**.

E-government also means **reinventing government** by implementing new organizational, architectural and operational models of administration,

which are made possible by the appropriate use of information and communication technology.

These new models need to be enabled by new legislation and specific regulatory actions, that in many countries must precede, not follow, the deployment of new technologies. For instance in the area of service delivery and in dealing with personal data online, special attention must be given to allow only entitled persons to access services that imply modification of sensible personal data, to ensure **security and privacy protection requirements** and to regulate the way we keep track and record of each transaction that is carried out.

The new Model: the Life Events Approach and the Challenge of Administration Integration

First of all, we need to implement a **service integration model**, where services and contents are presented according to user's requirements. The adoption of a **life events approach** is a fairly standard practice in e-government today. This approach shall overcome the old administrative way of interacting with government - the one often referred to as **single agency transaction model** - where the citizen needs to know which administration is delivering what service and to interact directly with that administration.

This new interaction paradigm has the potential and the capability of **hiding from the user the organizational and administrative complexity** of the public administration. This idea is in principle very attractive. However, its implementation may not at all be easy and will clearly require different solutions in different countries.

The new model has many political, institutional, administrative, organizational and technical implications and raises many general questions.

To overcome the single agency transaction approach we need to face the **challenge of administration integration**. This means that all administrations need to interoperate among them in a **peer-to-peer relationship**. This however also means that we have to overcome the traditional relationship pattern between administrative *back-offices* and *front-offices.*

By definition all public administrations play some back-office role, by implementing administrative procedures that only involve data in their possession. But, in the present service delivery model, they typically play a front-office role as well. A new architectural and organizational back-office/front-office model needs now to be devised. **To provide integrated**

access, the front-office needs to be separated from the back-office, even if they belong to the same administration. Moreover, **it may no longer be true that administrations need to deal with both tasks.**

One of the political issues of reinventing government is indeed to choose **which entity should be responsible for the front office procedures** needed to implement the new paradigm organised around life events. Should this be the task of **central** government or of **local** administration? And are we sure that in some cases the **private sector** could not do the job better?

Public-private partnership in e-Government

To answer these questions we must previously deal with two a fundamental issues. Which are, in the new society empowered by information and communication technology, the tasks that should be carried out by public administrations, and hence to remain within the public sector? And**, which are the tasks that can be transferred to the private sector?**

This leads to discussing partnership. **Reinventing government also means reinventing partnership**. Partnership is not at all about outsourcing, or joint capital investment with the private sector or, more recently, about project financing. Partnership with the private sector can better be achieved by **implementing policies that create the demand of services** and the **conditions for an adequate return of investment** in implementing and deploying tasks up to now traditionally performed by the government and in offering services up to now exclusively supplied by the public sector.

Existing institutions, both within government and external to it, should be drawn into partnership with government in order to facilitate access to services, in particular in implementing the new front-office-life-event based paradigm. **Particularly when it is virtual, i.e. a portal, the front-office is a task that might be carried out by the private sector on a competitive basis.**

Government could also take advantage of the already existing **infrastructure of the private sector** particularly to **improve accessibility.** In many countries post offices or financial services and ATM are in better reach than any local or central government office. These all present valuable resources that are currently delivering isolated services, an amazing backbone upon which it is possible to draw. Once a safe authentication tool (electronic identification card, service card, electronic signature card) has become widespread, nothing can prevent **the existing network from being exploited** (think of post offices, tobacco shops, Bancomat, etc.) **in order to have access to public services.**

The project started during the last legislature in Italy for using commercial businesses as a network of electronic terminals of the public service system and of public utilities, especially in urban and rural areas, responded to this logic. In conjunction with the representative organizations of commerce, the Government prepared and decided to finance (25 mil.$) a plan for transforming many private commercial structures (tobacconists, bars, restaurants, food retailers …) into terminals for the electronic delivery of services to citizens. Each citizen who is not equipped for access at either home or work will be able to use these terminals to communicate with the administrations, if necessary using an electronic ID or an electronic signature card for recognition. The merchant will act as a substitute for the front line public servant, hence lessening the public administration's personnel's costs.

Digital Divide and Access to Services

By providing on-line service delivery we do not necessarily imply that every person needs to be able to get access personally from office or home, by using a personal computer or any of the other possible channels, like mobile phones. In many areas of the world this achievement is not among the present priorities of governments, but rather a long-term goal.

Nevertheless, **we cannot accept the issue that in the short term we will improve access to services only for people who have personal access to PCs and are literate enough to use the Internet directly to transact.**

In addition, it is well known that ICTs don't just enable the electronic supply of services and information to citizens to which they would have been able to access, however, in some other way. Moreover, ICTs also offer new possibilities**, new forms of citizenship**: the possibility of accessing more rapidly not only information and public services, but also new opportunities of dialogue and participation. **A fundamental instrument of democratic participation cannot be reserved just for the few: access should be available to all.**

In fact, for reasons that we all know, the vast majority of people all over the world will be constrained for a long time or will prefer to access services through intermediaries and, hence, will have to move to places where they can find the appropriate facilities and the needed help to get the service they require. **Network terminals** in all the front offices of the **public administration should help overcome the digital divide**. But that is not enough. So, we must provide the conditions required for **the establishment and the development of other (private) intermediaries.**

Access to Services and Private Intermediaries

The question of who those intermediaries are cannot be answered in general; rather it could have different solutions in different countries. But these solutions must clearly be in the reach of people and do not necessarily need to be public administrations. Also **the use of intermediaries in the form of single-person agencies or small businesses acting as physical contact points for access to government services could be a key component of an access strategy**.

For instance, the rapid development of the telematic taxation system in Italy was made possible by the mobilisation of private intermediaries (banks, trade-unions, business unions and business consultants).

In any case, services will have to be provided online either to be accessed directly by end-users or indirectly through intermediaries. However, services that are not organized in a way which is relevant to people will limit the achievement of the broader objectives of access: we will actually increase divides rather than using information technology to reduce them.

The apparently marginal issue of the role played in the passage to e-government by the present intermediaries between citizens and the public administrations must be faced within the above outlook.

In fact, nowadays citizens and enterprises that need to obtain services or fulfil obligations turn to multifarious subjects that help them with these transactions. This is due partly to the complexity of the policies of the sector, partly to the outsourcing of certification tasks, which would otherwise weigh on the general taxation, and for an important part to the inefficiency and inaccessibility of the administrations themselves.

The present Intermediaries: Risks, Opportunities, Resistances

There is a vast services sector, whether it be that of notaries, surveyors, tax-experts, employment consultants or merely agencies supplying certificates and the like, for which a part at least of the added value produced would be substantially swept away by an increase in accessibility and by the interconnection of the database.

Here the risk is that the interests concerned could mobilise to hinder the reform and modernisation process of the administrative system in various ways, not all obvious to public opinion, as already occurred with the simplification policies, even by means of underground alliances with the bureaucratic apparatuses most reluctant to renew themselves.

The problem must thus be faced seriously - both at national and local level - by aiming at **exploiting the opportunities and reducing the risks of a massive and systematic employment of private intermediaries.** Several initiatives may be devised to avoid the risks and to exploit the opportunities.

There is no doubt, for instance, that generally speaking a decisive policy of liberalisation of the access to professions - which seems to be required by the European integration - would be a powerful indirect factor to overcome some of the problems mentioned above.

At a nearer level, a constructive relationship with professional orders and with categories concerned could be developed. This relationship should be based on the capacity to give an **understanding of the advantages** the most modern and advanced part of the present intermediaries could obtain. By this, I mean the possibility of increasing the added value of transactions and the opportunities thus offered to **widen the service range provided to customers**. This is especially true as regards services to enterprises where the outsourcing of a series of administrative activities would allow one to restrain costs and improve productivity.

The modernisation of the sector (let us think of the birth of the early professional associations) should facilitate this transaction and establish the bases for efficacious partnerships. A rise in the public demand for administrative services (for instance, salary management) could represent an important factor in this direction.

Moreover, an important role could be played by the development of the **associative world** and of the **non-profit sector** in the field of the electronic delivery of public services to citizens (as already happened in many others sectors). The specialisation in intermediation as regards the e-government could remove several obstacles in the path to the full exploitation of potentials deriving from the integration of services: This could be very important for the more disadvantaged sectors of the population, which otherwise risk being excluded.

However, the greatest boost to overcoming the obstacles the intermediaries put in the path to e-government cannot but come from the **implementation of the demand for bureaucratic cost reduction** both by citizens and enterprises alike. Here **consumers' associations** play a primary role, but **local administrations** too can and must actively boost this demand (as successfully done, for example, as regards self-certification).

This is the decisive ground on which the administrative reform is based. Whoever thinks that it can be piloted **on the basis of the sole offer** risks

underrating the political and social difficulties that, both outside and inside the administration, stand in the path of a full exploitation of the ICT.

The Issue of Authentication

The integrated service model raises some other relevant issues: for instance, the **citizen's identification for access** and the **single citizen's identifier**.

The issue of authentication is generally a matter of concern about security and private data protection. These are of course not only technical issues, but have also **significant political implications**. For instance, we need to answer among others the question of whether authentication for access is implemented in a centralised way or can be better dealt with by using a distributed model.

One of the most frequently discussed subjects when it comes to e-government, particularly in Europe, is the development and deployment of **smart cards for authentication**. In principle, these cards can hold either personal citizen information, electronic keys for digital signature, possibly biometrics information such as retina scans or fingerprints as well as information relevant to the delivery of a variety of services such as social security or healthcare.

Providing government electronic services to citizens is the centerpiece of all e-government strategies and in some cases it has been associated to the massive deployment of smart cards. In many countries it has been assumed that without the level of identification and authentication made possible by a national smart ID card, the delivery of most services would be inappropriate, if not impossible. No matter which channel is considered for service delivery, **the question of how much authentication is required to make sure that the right person gets the right service, is to date an unresolved issue that needs to be addressed.**

To avoid that service cards become more a constraint than an enabler to the provision of online services, government agencies and departments - both central and local - should develop their electronic services **without** assuming that a smart card of any kind is available. Even if it is, they must prepare to serve citizens or residents who will **not** be in possession of such a card.

Clearly, many e-government services do not require strict authentication and do work well with **passwords, personal identification numbers** and other software authentication systems. Although no significant problems have been reported so far with the use of these systems, this will prove

impractical in the long run. Apart from security issues, the burden and the complexity for the user is the need to register with many different service providers and to handle many different passwords and personal identification numbers.

For all those most-delicate services concerning **access and changes to sensible personal data** and for the most-vulnerable transactions such as **payments and fund transfers** there is **the need to provide a more acceptable and safer solution.** The key players here are not only public administrations but also financial service providers.

This provision is more than a technical security requirement, it is actually the enforcement of basic rights and citizen's privacy protection requirements. **Although private data protection depends on local regulations, the problem of ensuring that only the entitled person can access or modify sensible data needs to be addressed in all countries.**

Smart Service Cards and Identity Cards

Smart card technology can be used to develop "service cards" that provide the strict authentication required for these services and the high level of security made possible by electronic keys stored on the card.

Some countries in Europe have faced the problem of providing citizens with a strong authentication means with the quite inappropriate solution of delivering national ID cards, i.e. identification documents, such as passports or driving licences that also can clearly benefit from the adoption of smart card technology.

The main purpose of ID cards, issued by the central government or by other public authorities, such as those related to policing and national security, is to allow recognition. Unfortunately, in many countries, and according to many cultures, it is not acceptable to oblige citizens to carry an identification document and to provide proof of their identity. Consequently, it is inappropriate to consider the government issued ID card as the sole service card available worldwide.

From a more global perspective, we need to **find a solution for enabling every person all over the world, be they citizens or residents, to access services online without been obliged to carry an identification document.** When a service card is required, it should not have the same characteristics of an identification document. It should be like a credit or debit card with no personal identification on it; and, most importantly, it should not be delivered by government authorities.

The Italian Case: the smart ID Card

The Italian case is worth analysing as a possible reference model. Italian citizens have been obliged for quite a long time to carry a paper national identification document. In order to improve the level of national security and the electronic delivery of services, in 1998, with the so-called Third Bassanini Law, the Italian government planned the substitution of the existing paper document with a smart-card-based identity document usable also as a smart service card. The distribution of ID smart cards to citizens is presently being piloted.

This project is now facing technical constraints - such as the availability of a robust public-key infrastructure able to support millions of users - and the concern about privacy voiced by various parties on the fact that the authentication procedure to access any service is under the control of the central national security department. Moreover, the deployment of this program will take a long time and will require a significant investment.

Once available to all Italian citizens, the **smart ID card will clearly also be used as a national service card**, but it will be only **one possible means of enabling users to access electronic services, coexisting with many others**.

 As a matter of fact, cross-border mobility in Europe will require e-government services to be made available not only to citizens, but also to residents, temporary workers and tourists and only a few of the service users will carry Italian government-issued ID cards.

Services requiring strong authentication will be delivered not only by public administrations but also **by private service providers**, particularly providers of financial services. When a smart card is needed to access those services, it would be more logical to expect the government to rely on infrastructures and standards developed, and agreed upon, by the private sector rather than the other way around.

The Italian Case: the electronic Signature Cards and the Role of the (Private) Certification Authorities

The Italian very advanced regulation on **electronic signature** (based upon the so called First Bassanini Law of 1997) has assigned to the private sector the complex task of developing privately managed Public Key Infrastructures. As a consequence, the **private sector** has developed all the infrastructure services needed to deliver signature cards.

Private Certification Authorities (CA) registered according to the Italian law, can therefore **deliver digital keys and certificates used to electronically sign documents carrying full legal value.** Following the Italian Law, the registered CAs are **private companies** supplying public services with notaries powers, and with the task of certifying the univocal correspondence between the personal identity of a citizen and the digital certificates issued to him.

It is not a surprise that the vast majority of the 14-registered CAs in Italy belong to the financial sector. It is in fact the financial sector that would have the most justifiable and urgent reasons to strengthen security and authentication.

All citizens and residents can personally obtain signature cards from one of the registered Certification Authorities, just as they obtain credit cards from banks.

A **signature card is not an ID card**, since it does not necessarily carry any picture or other visual identification and since it is not issued by government authorities. Nevertheless, it provides a strong and legally valid electronic authentication mechanism.

Moreover, the registered CA, electronically connected with the National Tax Service, can, if requested, **store the personal fiscal code of the citizen in his smart signature card:** in practice, the CA verifies, before the issue of each card, the personal identity number given by the Tax Service to the citizen and stores it in the digital certificates registered in his card.

Therefore, **all digital certificates produced by the registered CAs,** according to the procedure provided by the law for awarding the digital signature, are certainly associated with the personal identity of each citizen and represent **a sure electronic mean for his electronic identification.**

In fact, signature cards can be considered a proof of identity exactly in the same way as the personal signature is considered a proof of identity. **Therefore, they can be accepted as service cards by all administrations as well as by the private service providers**.

A new Open Source (*General Public Licence*) software, enabling to **use simultaneously all kinds of smart cards**, is about to be available in Italy, for private companies and public administrations. So it will be possible to use the signature cards as service cards; and, consequently, it will be possible to use the signature cards' network for solving the problem of authentication for the delivery of electronic services to citizens.

The single Citizens' Identifier

It is worth noting how many private- and public-sector cards are already in use in Europe. From credit cards to electronic purses, from Subscriber Identity Module (SIM) cards for GSM phones to healthcare, social security or driving license cards. It is unrealistic to assume that these different cards will integrate into a single, government-sponsored scheme for ID cards. An agreed common scheme, which is limited to signature and authentication purpose, seems to be more achievable.

In fact, in many countries the idea of **a single code identifying citizens, to be used as a key to access personal data** stored in the data bases of all administrations, **is perfectly acceptable.** On the contrary, in other countries, there is **a strong resistance to the idea of a single citizens' identifier.** But a single identification code represents **the only possible way to deliver integrated services.**

All countries will eventually have to accept the idea of providing, throughout a regulated identification process carried out by the private or by the public sector, electronic signature keys and certificates to all citizens. This is in practice a different and new form of assigning a single identifier to citizens, which is introduced in their best interest to allow them to take full advantage of the information society, with the purpose of **ensuring secure access to personal data and transactions** and to provide the best available mechanism for privacy protection.

The Italian regulation provides for both an ID card and a signature card as valid authentication mechanisms to access online services. While the ID card concept might not be acceptable worldwide**, the signature card, particularly if delivered by the private sector, might prove acceptable in all countries and in different legal cultures.**

The system provided by the Italian law, therefore, allows for the implementation of open, flexible and distributed electronic systems, and permits to **keep the needs of police and national security separate from the needs of delivering online services.**

Moreover, the Italian system **favours the public-private partnership**. In fact, it gives to private companies the task of registration, authentication and certification, through the issue of signature cards valuable also as service smart cards, thus allowing public administrations to concentrate on the administration's true core business, i.e. the delivery of services and utilities to citizens.