The 3rd High-Level Forum on City Informatization in the Asia-Pacific Region
(CIAPR III –Shanghai 2002)

Delivering Services and Public-Private Partnership in E-government

(with a final warning about digital divide, digital opportunity and the danger of a new colonialism)

by Franco BASSANINI
Senator, Republic of Italy
Former 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)

We can think to 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.

Access to services is at the heart of e-government because it is primarily about creating access through the means that are most convenient for people. Moreover, e-government enables a new paradigm of service delivery to citizens and to businesses.

E-government also means, as it has been said, that **we need to reinvent 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.**

Access to Services and Digital Divide

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 it is rather a long term goal.

Nevertheless, we cannot accept the fact 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 allow the electronic supply of services and information to citizens to which they would have been able to access, however, in some other way. Besides that, 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.**

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.**

In Italy, the government in conjunction with the representative organizations of commerce, has prepared and financed (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 costs.

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.

This means that we need to implement a **service integration model**, where services and content 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 you **need 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.

Public-Private Partnership

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**. It also means that an architectural and organizational back-office/front-office model needs to be devised. 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.

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?

To answer these questions we should also be prepared to answer a more fundamental question: **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.**

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 (and also commercial shops, or lottery collection offices) 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.

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.

The Issue of Authentication

The integrated service model raises some other relevant issues: for instance, the **citizen's identification for access** and the **unique citizen's identifier**. If providing government electronic services to citizens is the centerpiece of all e-government strategies, the **issue of authentication** is perhaps the main problem of an advanced e-government policy.

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**.

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. **And 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**.

Clearly, many e-government services do not require strict authentication. Many other e-government services 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** (passwords can be stolen, or guessed), the burden and the complexity for the user is the need to register with **many different service providers and** to handle **many different passwords or personal identification numbers.** Moreover, passwords and personal codes **do not allow a sure association with the personal identity of the citizen.**

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.

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 Cards for Authentication

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. Therefore, 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 fact, 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 needed for the delivery of a variety of services such as social security or healthcare or tax collection.

Of course, 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 – must be allowed to develop their electronic services without assuming that a smart card of any kind is available. Even if it is, they must prepare, obviously, to serve citizens or residents who will not be in possession of such a card for a long time.

Nevertheless, in many European countries it begins to be acknowledged that without the level of identification and authentication made possible by the smart service cards, the delivery of most services would be inappropriate, if not impossible. Therefore, **the deployment of e-government strategies** through the development of electronic services' delivery to citizens seems to be associated to the **massive deployment of smart cards**. The key players here are not only public administrations but also **financial service providers**.

Service Cards and Identity Cards

Some countries in Europe have faced the problem of providing citizens with a strong authentication means by planning the delivery of 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 unique 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 necessarily 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: ID Cards and Digital Signature Cards

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. When they come into the world, they receive from the National Tax Service a personal identity code, created by using an algorithm in order to warrant the sure association of each code with an individual and with his personal data.

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.

In fact, the Italian 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 electronic documents carrying full legal value** (requests, applications, agreements or contracts, drawn up between private persons and/or companies or public administrations).

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.

The Italian Case: the Role of the (Private) Certification Authorities

Following the Italian Law (First Bassanini Law, 1997) the registered CAs are private companies supplying public services with notarial powers, and with the task of certifying the univocal correspondence between the personal identity of a citizen and the digital certificates issued to him.

In Italy, 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 and must 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 the simultaneous use of different kinds of smart cards, is about to be available 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 system provided by the Italian law, therefore, allows the implementation of open, flexible and distributed electronic systems, and permits to keep separate the needs of police and national security from the needs of delivering online services. Moreover, the Italian system favours the public-private partnership: indeed, it gives 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.

The unique Citizens' Identifier

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. On the other hand, a unique 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 unique 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 a valid authentication mechanism 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.

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 purposes seems to be more achievable.

E-government for Development: from Digital Divide to Digital Opportunity for All

I would like to conclude my introduction to this panel with some brief remarks about the issue of e-government for development. Using the words of the ***DOT Force Report 2001***, the heart of the matter is: how to ***"bridge the digital divide and harness the power of information and communication technologies (ICT) and global networks to assure opportunity, empowerment and inclusion for all****…ICT offer enormous opportunities to narrow social and economic inequalities and support sustainable local wealth creation, and thus help to achieve the broader development goals that the international community has set. ICT cannot of course act as a panacea for all development problems, but by dramatically improving communication and exchange of information, they can create powerful social and economic networks, which in turn provide the basis for major advances in development"*.

As we know, new IT developments can be the cause of new "moats", new inequalities, new exclusions: the digital divide. **But when wisely applied, ICTs can represent the decisive card to win the fundamental game: that of guaranteeing equal opportunities to all women and all men.** Equal opportunities in the diffusion of knowledge. In the quality of life. In the exercise of liberty and of rights, that are the essence of human dignity. And also in the

promotion of growth – cultural, economic and social. Therefore a great opportunity for filling in moats and much more important fractures: hunger, disease, illiteracy, exclusion of women and exploitation of children.

Today, technology can realise within months what a short time ago would have taken years. This possibility is not only open to the industrialised countries. **Through a coordinated, systematic and massive employment of ICTs, it is possible to trigger off widespread and sound processes of growth and development, self-propelled and self-managed by the same developing or least developed countries. The development of e-government could be the starting point and the driving power for achieving this goal.**

In fact, we cannot look at e-government simply as the application of business efficiency in public administration. The spread of ICTs and the realisation of effective plans for e-government strengthen the capacity of governments to set policies and to improve the quality and transparency of decisions, reinforce the legitimacy and accountability of governments, favour widespread access to knowledge, allow the implementation of distance learning programmes, of tele-medical services and of technical and commercial assistance for business. The developed countries measure the overwhelming impact of these innovations in re-engineering their administrations. But also developing countries like China, Mongolia, Bangladesh, South Africa, Bolivia or Senegal have had significant experiences in this area.

The digital divide can be overcome, in a few years, if at least two fundamental conditions are present: basic literacy and an efficient electrical network. Of course, also a TLC network and mass computer literacy are needed. But to set up a phone network is, in fact, a **much cheaper and faster operation** than the realisation of all the other "classical" infra-structural networks: 100km of fibre optic cable with a capacity of 100 Terabit per second costs a thousand times less than 100km of motorway; ICTs are not expensive, they don't consume great quantities of energy, and they respect the environment. Mass computer literacy also has **reasonable costs and time requirements**, as long as we start from a situation of good basic training. This is demonstrated by the rapid progress achieved by countries like India, Brazil and Egypt, as well as by some developed but late starter countries, like Italy.

The New Frontier of International Cooperation: a Warning

It is obviously necessary to guarantee **favourable environmental conditions**: a clear, simple regulatory scenario open to investments and competition; political stability and democratic trust; organic and consistent plans

for human empowerment, for the modernisation of the administration and for the development of e-government. **But it is not necessary to adopt the specific institutional and technical models or solutions chosen by the more advanced countries or by one among them.**

It seems to me that on the basis of these considerations it is possible to outline a new frame of reference, **a new frontier of international cooperation**; but at the same time I feel the need to raise a **warning.**

Of course top priorities for international cooperation policies and investments in least developed countries need to address basic needs first, like food availability and healthcare. But then a clear strategy for development must be promoted, stressing the role of the ICTs as propellant power. Therefore, it seems to me that the **new priorities of international cooperation should be the investments in five sectors: basic literacy extended to all people, electrification, telecommunication infrastructure, computer literacy, digitalization of the public administration.**

These are the decisive priorities to overcome situations of underdevelopment and inequality and to make possible the deployment of the information society and the application of ICTs to government operations, which in turn can become a key factor and a further enabler for development.

Eventually we need to provide funds and to address the issue of access in financing and the one of partnership. Unfortunately, some areas of the private sector and some governments seem to have recently established a sort of inappropriate connection. By this, I mean a connection between their investments and their cooperation with the developing and the least developed countries in the ICT sector, on one hand, and the adoption by the same countries of specific models of governance or of specific patterns of social and political organization and/or specific technical solutions (like specific budget, tax or land register systems), on the other hand.

This approach, which is present in some cooperation initiatives, may actually lead some developed countries to impose a new form of colonialism to the developing and the least developed countries. This is a risk and a danger that we must absolutely avoid, beginning by giving wholly and exclusively **to the United Nations** (and not to the G8) the role and the responsibility of co-ordinating and promoting the international cooperation in this field. Moreover, we must firmly hold by the statement of the Dot Force Report 2001: *"The need for clear strategies to manage the complexity of the challenge of creating digital opportunities for all points to a fundamental fact:* ***the most important****, and in many cases most difficult,* ***decisions and actions will have to be taken by nations and communities***

***themselves**, to create the environment, mobilize the consensus, and **set the priorities that will shape each nation's path to digital opportunity**. At the same time, the international community in its various guises - governments, private sector, non-profit sector, international organizations - can and must play a critical role, mobilizing resources, building partnerships, increasing coordination, extending markets, sharing innovations"*.

ICTs and e-government can be and must be used as a new, powerful tool and as a leverage for boosting autonomous and self determined processes of development and empowerment. Self determined by each country and by the people of each nation of the world. ICTs should not become the Trojan horse of a new colonialism.