Chapter 1

eGovernment: Secure services in-context
1. From Lisbon to Barcelona: Setting the scene

I.
The Lisbon strategy, set forth by the European Union at the Lisbon Europe-
an Council (March 2000), aims at making the European Union the most
competitive and dynamic knowledge-based economy in the world, with im-
proved employment and social cohesion, by the year 2010.

As a part of this strategy, the Feria European Council (June 2000) endorsed
the eEurope-2002 Action Plan. The progress made during eEurope-2002
can be briefly summarized as follows:

- Internet penetration in homes has doubled
- Telecom framework in place
- Internet access prices have fallen
- Almost all companies and schools are connected
- Europe has world’s fastest research backbone network
- e-commerce legal framework largely in place
- More government services available on-line
- A smart-card infrastructure is emerging
- Web accessibility guidelines adopted-recommended

The Barcelona European Council called on the Commission to draw up an
eEurope-2005 Action Plan (“An information society for all”), focusing on:
“…the widespread availability and use of broadband networks throughout
the Union by 2005 and the development of Internet protocol Ipv6 …and the
security of networks and information, eGovernment, eLearning, eHealth,
and eBusiness”. eEurope-2005 is expected to build upon the success of
eEurope-2002 and maintain eEurope as the symbol of European Union po-
licy towards the Information Society.

II.
eEurope-2005 needs to be adapted with regard to three requirements:
a) eEurope-2005 should try to stimulate a positive feedback between infra-
structure upgrading and service development.
b) eEurope-2005 actions should go beyond current policies and make a real
difference.
c) eEurope-2005 needs built-in flexibility and should provide for a mid-
term review of actions to ensure a smooth phasing in the action plan.

To meet the above requirements, the eEurope Action Plan is based on two
groups of actions, which reinforce each other and build a virtuous circle.
These groups are:

{ Services – Applications – Content }
{ Broadband Infrastructure – Security }
According to eEurope-2005 Action Plan, by 2005 Europe should have:

- Modern online public services (eGovernment, eLearning eHealth).
- A dynamic business environment.

and, as an enabler for these:

- Widespread availability of broadband access, at competitive prices.
- A secure information infrastructure.

The eEurope-2005 Action Plan is structured around four interlinked lines:

- Policy Measures
- Good Practices
- Benchmarking
- Policies Coordination

III.

Initiatives regarding eGovernment exist at national, regional and local level. These are complemented by actions carried out at European level (e.g. the IDA Programme is supporting interoperability of back office processes, standardisation and provision of pan-European services, the IST Programme is financing research activities, etc.). At the Barcelona Council the creation of a one-stop European Job Mobility Information Web Site was decided. Moreover, the Barcelona Council invited the Commission to analyse the role that electronic authentication systems can play in removing obstacles to the development of eGovernment.

The key actions proposed for eGovernment services spread and enhancement, under the eEurope-2005 umbrella, are:

- Broadband Connection
- Interoperability
- Interactive Public Services
- Public Procurement
- Public Internet Access Points (PIAPs)
- Culture and Tourism

In particular, by 2004 the Member States should have ensured that basic public services are: a) interactive, b) accessible for all, and c) exploit the potential of both broadband networks and multi-platform access. The above require back-office reorganisation, which will be addressed systematically in the good practice exercise. The Member States should agree on a list of public services for which interactivity and interoperability are desirable.

IV.

The information society has a high growth potential due to the nature of the peak and emerging technologies. As peak technologies, eEurope-2005 recognizes those connected with broadband and multi-platform access.
The evolving technological environment can be viewed through a medium and a long-term point of view.

**Medium term:** The residential environment of the citizen is a smart home. In order for the citizen to take full advantage of new information services, it will be necessary to distribute and make them accessible once they have crossed the threshold of the home. Regarding the institutional environment, the common practices will include teleworking, videoconferencing, and wide B2B, G2G and C2G marketplaces, whereas there will be three prerequisites for connectivity:

a) **Telecommunications delivery infrastructure.** The next generation broadband infrastructure will offer speeds over 10 Mbps. Such a move from narrow band to broadband Internet access would have a profound effect on Internet usage, resulting in higher levels of connectivity and enabling new sorts of services. The high data transmission rates of new 3rd generation (3G) phones will, in certain cases, support data rates up to 2 Mbps. The emergence of short-range radio-based machine-to-machine communication systems, such as Bluetooth, would allow PCs, laptops, mobile phones, PDA and domestic appliances to be connected to each other at distances between 10-100 metres and at speeds of up to 1-2 Mbps.

b) **User hardware.** As PC penetration levels are very high, the emphasis will shift towards replacement sales. The use of “thin clients”, devices with limited intelligence that operate using applications based elsewhere, will increase. Europe’s rapid uptake of digital mobile phones will be very fast, in contrast with the slow adoption of PC and Internet. The market of PDA will keep on increasing rapidly, suffering by serious compatibility issues.

c) **User software.** The predominance of Microsoft operating systems is likely to continue in the short- to medium-term future. Linux, the second most popular operating system (in terms of number of copies shipped-placed) will spread rapidly but remain a far cry from the estimated more than 100M users of Windows. Netscape’s and Microsoft’s Internet browsers will continue to dominate the market. eServices and Internet security software will become essential. Digital rights and digital contents management software will be brought to the centre of attention.

**Long term:** The distinction between the home and the outside world will be blurring. Services will be provided wherever the citizen-consumer requires them. With such an evolution in mind, Ambient Intelligence (AmI) is proposed as a key visionary concept by the Information Society Technologies Advisory Group (ISTAG) (the reference to this concept does not necessarily mean that we share it). AmI stems from the convergence of Ubiquitous Computing and Communication and Intelligent User-Friendly Interfaces.

By the onset of such a convergence, the citizen will be surrounded by intelligent interfaces, supported by computing and network technology which will be everywhere and which will be embedded in everyday objects. AmI is aware of the human presence, it implies seamless environment of computing, advance networking technology and specific interfaces. AmI responds
intelligently to indications of desire, it is unobtrusive, often invisible, and not involving the citizen into complex learning processes.

The key enabling technologies for this long term visionary-picture, as drafted by ISTAG (June 2000), are the following:

- **Embedded Intelligence**
- **Micro-electronics and Opto-electronics**
- **Middleware and Distributed Systems**
- **Trust and Confidence Enabling Tools**
- **IP Mobile and Wireless**
- **Cross-media Content**
- **Multi-domain Network Management**
- **Multi-modal and Adaptive Interfaces**
- **Multi-lingual Dialogue Mode**
- **Converging Core and Access Networks**

V.

Standardisation is a basic tool to enable and ensure access to services and to support their portability, interoperability and compatibility. Standards can be categorised as horizontal and vertical. Horizontal standards are mostly non-sectoral with a generic use (e.g. those governing electrical safety). On the other hand, vertical standards are usually sector-based (e.g. those regulating interoperability among telecommunication networks). In the area of eGovernment, horizontal standards are the most appropriate ones.

Nowadays, the technical specification work, related to vertical services, is moving from official standards bodies to fora, consortia, and other specification providers. This is considered to be a process led by business demand. Currently, there are three global official standards bodies, i.e. the International Telecommunication Union (ITU), the International Electrotechnical Committee (IEC) and the International Standards Organization (ISO). In addition to them there is the ISO/IEC Joint Technical Committee (JTC1). In addition to the global bodies there are several other national and international bodies and a huge and growing number of fora and consortia (e.g. IETF, IEEE, CEN, etc.).
2. Secure Information Infrastructure

I. EU Strategy

The European Union has launched a comprehensive strategy framework and actions on security and privacy issues. Main parts of this strategy are:

- The Commission Communication on Network Security
- The Commission Communication on Cybercrime
- The Data Protection Directive regarding electronic communications
- The Proposal for a Council Framework Decision on attacks against information systems

A number of relevant initiatives have been launched (e.g. cyber security task force, awareness campaigns, promotion of good practices, improved exchange of information mechanisms, etc.). Their results will provide the basis for the work towards a secure information infrastructure. Furthermore, work on the creation of a secure European smart card infrastructure should continue and the roll out of applications should be intensified.

II. Security research

The priorities of the research activities on security under the Sixth Framework Programme will be: a) trustworthy networks, b) trustworthy information infrastructures, with an emphasis on emerging technologies (broadband, wireless architectures, ambient intelligence), and c) identification of vulnerabilities and their inter-dependencies in infrastructure.

The research activities should also support standardization, with a view to wider use of open standards and open source software. Research should, also, take into account the human factor in security (e.g. baseline security standards, user-friendliness of security systems, etc.).

III. Key actions for security

The key actions proposed for a secure information infrastructure, under the eEurope-2005 umbrella, are:

- **Cyber Security Task Force** (CSTF): The CSTF should become a center of competence on security issues and questions.
- **Security Culture**: Such a culture should be developed so that secure information and communication products are designed and implemented (“built-in” security), and so that the awareness of security risks is raised.
- **Secure Communication between Public Services**: Examination of the possibilities to establish a secure communications environment for the exchange of government information.

IV. The threat to Privacy

The successive generations of IT applications and the environment for online activity have raised concerns about how personal data are being used.
Governments and international bodies (e.g. Council of Europe, Organization for Economic Co-operation and Development, etc.) have, often timely, responded to these concerns with guidelines and legislative measures aimed at avoiding abuses, either in fulfilment of their mission to safeguard the basic human rights of citizens, or to encourage a favourable climate for e-services by ensuring that citizens will have sufficient confidence in the new electronic environment, in order to be able to participate in it. On the other hand, the EU has put in force two Directives on this domain: the Data Protection Directive and the Telecommunications Data Protection Directive. Other more pro-active approaches to safeguard privacy (e.g. USA) include self-regulatory mechanisms, which legitimise the commercial activities while suffering by weak enforcement possibilities. On the other hand, self-regulation can be adopted in the setting of standards for privacy practice.

<table>
<thead>
<tr>
<th>Genetic Society</th>
</tr>
</thead>
<tbody>
<tr>
<td>As N. Negroponte pointed out, the Information Society is genetic in its nature, i.e. each generation becomes progressively more “digital” than its previous. In this context, an increasingly wide range of human characteristics (identity, behaviour, biological features, etc.) finds themselves reflected in an electronic equivalent. The increasing weight of the electronic expression of those characteristics will lead to new indicators of privacy. Current determinants of privacy (name, address, etc.) are eventually replaced by virtual characteristics, expressed in terms of a host of personal data. Recent reports (Future Bottlenecks in the Information Society, JRC/IPTS, June 2001) show that the privacy concerns are expected to be a serious bottleneck to the take-up of electronic services.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PET and PIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>The emerging technology, with an impact on privacy, is PET (Privacy-Enhancing Technologies) and PIT (Privacy-Invasive Technologies). PET may be used to improve the security of personal data; they aim at the development of information systems capable of providing a high level of personalised services, whilst requiring that the collection of personally identifiable data be kept to a minimum. On the other hand, PIT (Privacy-Invasive Technologies) pose severe threats by using new programming paradigms (e.g. Java, XTM, Active X, etc.) that permit remote servers to run applications on a client’s PC, via the web browser. In eGovernment applications concerns are raised because of the possible use of a “digital” or “virtual” identity.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Benefit and threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>The very strong market driver of personalized eCommerce products and services may be both, a benefit to citizens’ well being and a threat to their privacy. As one can demonstrate through an isomorphism exercise the same holds true for eGovernment, eHealth, etc. services. Due to the strong political and ethical component associated with privacy, the European parliament may take an even more active role in the development of future policies in this area, and thus affect the development of eGovernment initiatives, policies and applications.</td>
</tr>
</tbody>
</table>
3. **Electronic Signatures and Public Key Infrastructure: State-of-the-recent-past**

### Recent past in-context

In the course of the Belgian Presidency of the European Union (late 2001), a report was presented on the issue of electronic identification of citizens and organizations in the EU Member States (J.-M. Eymeri, *The Electronic Identification of Citizens and Organizations in the European Union: State of Affairs*, European Institute of Public Administration, 37th meeting of the Directors-General of the Member States of the EU, Bruges, 26-27 November 2001). This report described and commented upon the state-of-the-art on this issue within EU. Today, this report represents the state-of-the-recent-past on the issue; for the shake of completeness, its main findings will be briefly referred to in the sequel.

The use of a (single) identification number of citizens and organisations, either private or public, and the creation of an electronic identity card are merely ways to achieve the protection of:

- electronic communication,
- electronic financial transactions,
- electronic exchanges of personal data,
- access to public databases where personal data are stored.

### EU: Pathway to identification

Given the high importance of the above processes - and based on the existing and emerging technologies - the EU adopted a generic pathway towards the electronic identification of persons and organizations and the authentication of the documents they produce. The pathway refers to at the EU and the Member State level and makes use of two mainly technical means:

**Electronic Signature**

**Public Key Infrastructure (PKI)**

### Asymmetric Cryptosystems

Briefly, electronic signing requires an identity and a signature certificate to be issued - to the person concerned - by a certification authority. The certificate inextricably links the personal data to two digital cryptographic keys, which are used by an *asymmetric cryptosystem*. The two keys are called *private key* and *public key*, respectively. By using the two keys, an electronic signature can be affixed and received. The public key is communicated to persons with whom the author of the electronic document exchanges a document on line. It enables the person who receives the document to decode a message encoded by the sender (with the private key which only the sender knows). The private key is used by the author of a document to put his signature on the document. The public key allows the receiver of the document to verify the authenticity of the signature. The PKI ensures the interconnection between:

- Citizens or organizations.
b) Registration Authorities (RA) in charge of receiving and dealing with their requests for certificates.

c) Certification Authorities (CA) in charge of allocating key pairs.

d) Bodies managing central directories and controlling the system.

The relevant regulatory framework is based on the EU Directive 99/93 ("Community framework for electronic signatures"). Although today all Member States have adopted this Directive, only a few added that the decrees implementing the law are (or not, as the case may be) in force. Moreover, in several countries these decrees were adopted with some delay, so that considerable amount of work needs to be done in the field of electronic identification. Regarding the state of progress of PKI development in the various Member States, the most advanced countries, where the PKI is already operational, have built systems with very similar patterns.

IV.

The role of the Registration Authorities (RA), which are responsible for dealing with citizens, and which collect requests for certificates or electronic identity cards, is usually decentralised to public bodies (e.g. public institutions and municipalities in Belgium, administrations and public agencies in Denmark, etc.).

V.

Regarding the role of the Certification Authority (CA), which is responsible for issuing certificates and pairs of keys, two main solutions have been explored so far. In several countries (Belgium, Denmark, the Netherlands, Sweden, Finland, United Kingdom), the task of providing certification services has been contracted out, through official public procurement, to private organisations set up for that purpose. In a few other countries, contracting out plays a less important role (e.g. in Spain, the services of issuing electronic certificates and keys are provided by the public administration; in Italy, public administrations themselves can act as certification authorities and issue electronic certificates). A second group of countries (Greece, France, Ireland, Luxembourg, Austria) pose different degrees of technical advancement; nevertheless, they have something in common, which is the type of PKI these countries intend to develop and the role to be given to the various actors remain the subject of an on-going debate.

VI.

In some countries (e.g. Germany, Spain) the progress in the use of electronic signatures depends heavily on practical factors, such as the availability of the software and hardware equipment on the civil servants’ computers. Since the cost of such equipment is considerable, this leads to delays in the spread of PKI. In Finland, an advanced country in this field (electronic identity card and PKI are in use since 2000), progress is still slow in practice, mainly because e-mail software is hardly suitable for the use of electronic certificates and electronic signatures.
VII.

Another issue refers to the role and degree of the administration’s control over the network of organisations involved in a PKI infrastructure. In many countries, decisions - in principle regarding this politically sensitive issue - have not yet been definitively adopted. Several countries have decided to entrust with supervisory powers an existing authority (e.g. in Belgium, the National Register of the Ministry of the Interior plays a central role in the system; in Germany, the authorities responsible for regulating the postal and telecommunication services (RegTP) control the certification providers; in Denmark, the National Telecom Agency is responsible for auditing certification authorities). In other countries, the supervision of PKI actors lies with a public authority (e.g. in Italy, this is the Authority for IT in Public Administration). In the Netherlands, a central government authority, along with a number of domain policy authorities, will regulate and monitor PKI. In Sweden, on the other hand, the state control over the organisations in charge of PKI takes place through contracts.

VIII.

An important issue is the authentication and protection of electronic exchanges within the public sector (e.g. Belgium focuses on the development of FedPKI, which aims to provide all civil servants with an electronic certificate, referring to them not as individuals but as civil servants working for a certain institution and qualified by a certain mandate to sign certain documents and take certain decisions). In Germany there are pilot applications underway (e.g. Media@Komm, Sphinx) for protecting the electronic communications within the administration and promoting the widespread use of qualified electronic signatures. Spain is running a programme aiming at providing all civil servants with an electronic card enabling them to identify themselves and sign electronic documents digitally. In Italy, civil servants have been provided with smart cards with digital signing functionalities. In the Netherlands, the government chose to first create PKI within the public administration, and only then to extend the system within the Citizen-Government (C-G) and Government-Business (G-B) contexts. In Denmark, the tax administration created a digital signature system, allowing tax auditors to exchange data securely. In Sweden, there is limited progress, due to the fragmentation of the public sector into autonomous agencies. Overall, the Member States seem eager to protect intra/inter-administrative communications by exploiting PKI and electronic signatures.

IX.

Another important open issue is the specification of a set of concrete criteria for a qualified electronic signature as referred to in the EU Directive. Other uncertainties hold true regarding the differences between the certification authorities accreditation schemes in various countries. Because of the legal contradictions, the providers of the certification services should build up a portfolio of national accreditations in order to be able to operate throughout the EU. A possible solution to this issue could lie with the concept of homogenous accreditation systems.
### 4. Scope and objectives of the report

<table>
<thead>
<tr>
<th>Secure Infrastructure</th>
<th>This report deals with and focuses on the following interlinked objectives and key-items of eEurope-2005:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Objective:</strong></td>
<td><strong>Secure Information Infrastructure</strong></td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Secure communications between public services</td>
</tr>
<tr>
<td><strong>Means:</strong></td>
<td>Electronic signatures</td>
</tr>
<tr>
<td></td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td><strong>Action line:</strong></td>
<td>Good practices</td>
</tr>
<tr>
<td><strong>Req’mnt:</strong></td>
<td>Positive feedback between infrastructure-service development</td>
</tr>
<tr>
<td><strong>Concerns:</strong></td>
<td>Privacy</td>
</tr>
</tbody>
</table>

In other words, eEurope-2005 aims at developing a secure information infrastructure as an enabler of modern online public services. One of the proposed actions, towards this end, is the establishment of secure communications between public services. Two of the most powerful technological means for establishing such a secure communication is the electronic signatures and the Public Key Infrastructure (PKI).

To this end, the report suggests a set of appropriate good practices for the exploitation of electronic signatures and PKI for the provision of secure online services by the public sector.

<table>
<thead>
<tr>
<th>Public services</th>
<th>Objective: <strong>Modern online public services</strong> <em>(eGovernment)</em></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action:</strong></td>
<td>Interactive public services</td>
</tr>
<tr>
<td></td>
<td>Public Internet Access Points (PIAP)</td>
</tr>
<tr>
<td><strong>Means:</strong></td>
<td><em>(eGovernment)</em> applications</td>
</tr>
<tr>
<td><strong>Action line:</strong></td>
<td>Policy measure</td>
</tr>
<tr>
<td><strong>Req’mnt:</strong></td>
<td>To go beyond current policies and make a real difference</td>
</tr>
<tr>
<td><strong>Concerns:</strong></td>
<td>Privacy</td>
</tr>
</tbody>
</table>

In other words, eEurope-2005 should result in the provision of modern online *(eGovernment, eLearning and eHealth)* services. All basic services should be provided for by the public sector, online, interactively, and - inter alia - through Public Internet Access Points. These services should be provided via *(eGovernment)* information systems and applications, respecting privacy of the citizens.

To this end, the report reviews legislation with an eye towards strengthening interoperability, creating awareness and safeguarding privacy, in the context of developing interactive *(eGovernment)* information systems and applications, and offering public services to the citizens.
Bibliography

4. European Commission, Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions.