This product is part of the RAND Corporation technical report series. Reports may include research findings on a specific topic that is limited in scope; present discussions of the methodology employed in research; provide literature reviews, survey instruments, modeling exercises, guidelines for practitioners and research professionals, and supporting documentation; or deliver preliminary findings. All RAND reports undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

TECHNICAL REPORT

Building a digital Europe

Lessons for the delivery of secure pan-European e-Government

Neil Robinson, Constantijn van Oranje-Nassau, Maarten Botterman

Prepared for the e-Government Unit of DG Information Society and Media, European Commission

RAND EUROPE

The research described in this report was prepared for the European Commission. The opinions expressed in this study are those of the authors and do not necessarily reflect the views of the European Commission.

Published 2009 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
Westbrook Centre, Milton Road, Cambridge CB4 1YG, United Kingdom
RAND URL: http://www.rand.org
RAND Europe URL: http://www.rand.org/randeurope
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Preface

This paper presents pointers on what is required to deliver a secure e-Government environment for mobile European citizens, based on the lessons learned from existing services and initiatives and identified challenges in the national and pan-European environments. The paper builds on a review of policy documents, scientific literature and an assessment of existing Pan-European eGovernment Services (PEGS; Solvit, 'Limosa', DG TAXUD, Secure Telematics (sTESTA)) and other multi-stakeholder systems developed in the private sector (Single European Payments Area; SEPA). It also draws on the presentations and discussions of a Working Conference on this theme held in Brussels in mid-November 2007 and the efforts of the SecurEgov (pan-European Secure e-Government Services) study conducted by RAND Europe for DG Information Society and Media between 2006 and 2007. This paper takes a *look forward* at what possibilities exist for regulatory intervention by the European Commission to meet some of the challenges related to the deployment of secure Pan European e-Government Services (PEGS). PEGS should provide an inclusive, seamless and cross-border service to citizens (and possibly other residents and visitors) in Europe. For the basic assessment, lessons from pan-European government-to-business (G2B) and business-to-consumer (B2C) services are also taken into account.

Thus, the paper is not meant to be an academic treatise on the various security aspects of PEGS, rather a document intended to be of direct policy benefit for the European Commission and other stakeholders in preparing the ground for the eventual implementation of PEGS.

For more information about this contact:

RAND Europe
Westbrook Centre,
Milton Road,
Cambridge
United Kingdom
CB4 1YG
+44(0)1223 353329

Contents

Summary

The security considerations identified in this paper are present in both national building blocks and actions necessary at the European level to meet those challenges of a pan-European nature. In a national context there are a number of specific security challenges that must be addressed. These include efforts to make the infrastructure as dependable as possible, abiding by privacy principles and the adoption of a risk-based approach to the management of information assets within PEGS. Some of the common aspects concerning security issues with pan-European systems include how best to deal with the different security approaches in European Union (EU) Member States.

A number of challenges at the national and European level were identified which it would be necessary to address if the deployment of PEGS were to be effective.

National challenges

First, preconditions at national level need to be met. This is a process of creating the right building blocks for the subsequent interconnection with national systems present in other Member States. These pre-conditions include: the integration of back office functionalities; adoption of relevant standards; creation of a dependable infrastructure; adoption of a risk-based approach to the management of information; proper consideration for privacy principles; and an understanding and appreciation of user needs.

European challenges

A series of specific issues are also presented which have a uniquely pan-European context. These include: different cultures between Member States; the need to take into account differing legislative frameworks; consideration of widely different legacy systems; varying approaches to security; and the absence of any dedicated management governance structure for the delivery of PEGS.

Main lessons learned

The management of the security concerns arising from the main challenges identified requires the sensible adoption of risk management techniques (stemming from acceptance that a 100% secure system is not possible), the encouragement of an atmosphere of collaboration, and empowerment of the delivery of the solution by the marketplace.

Following this, factors both inside and external to the development processes need to be dealt with proactively: organising processes of governance, project management, and multi-stakeholder involvement; also creating a culture of trust and enabling the necessary leadership. In parallel with the processes, some further elements need to be considered in

the design and substance of PEGS, namely: the use of existing standards; pragmatic and simple approaches; the level of integration (interoperability instead of harmonisation); and what steps are required to follow up on development.

Possible interventions

All these actions are placed against the background of the European Commission's role and the applicability of potential policy tools. The most appropriate form of intervention will depend on the type of service (e.g. healthcare, law enforcement, etc.), the phase of development (preparatory research, improving national building blocks, enabling infrastructures, the design of delivery mechanisms, implementation of services), and the degree of collaboration (harmonisation, centralisation, federation, or best practice exchange) appropriate to each different type of actionable activity needed to achieve the desired service.

Concrete recommendations

We identify a number of concrete actions in Chapter 5 that represent use of certain policy tools in order to support the delivery of PEGS.

The European Commission could articulate change by emphasising and communicating the need for putting in place critical national building blocks. Also, it should continue to invest and improve its platforms for best practice exchange to support the design and implementation of necessary building blocks. Helping to forge a consensus would support the identification of relevant standards. Research and development (R&D) funding in certain areas (listed in Appendix 1) would help the deployment of PEGS in those areas where knowledge is lacking and where this knowledge cannot be obtained by 'doing' activities, such as would be the case with a pilot. The final form of intervention might be consideration of passing or revising legislation in certain areas (e.g. revision of the Privacy Directive).

The way forward

In the remainder of Chapter 6 we suggest a multi-stage approach using real-life experience gathered from two distinct kinds of pilots and further research to progress this agenda. The first pilot, building upon the lessons learned from the November conference, would be a directed pilot with clear objectives and mandate, a well-organised governance structure and sustained commitment from the participants. Mechanisms for monitoring the effectiveness of governance, decision-making and project management would be built into this pilot to maximise the opportunities created from such a 'learning environment'. To make the outputs of the directed pilot as relevant as possible for policymakers, it would be built upon adaptive decision-making principles that allow continuous feedback loops and policy development. The second, more informal, pilot would be a 'sandbox' allowing discovery of new ways of using applications and methods of interaction and delivery of secure PEGS. Aside from the pilots, activity is proposed along three streams of development:

1. further sharing of practice experience of current pan-European e-Government applications and international business experiences;
2. an assessment of the need for different levels of intervention at pan-European level (e.g. harmonisation of legislation or further support programmes); and

3. a benchmarking exercise of the information assurance maturity of the Member States, as a way to expose the complex risks that would need to be assessed and managed prior to PEGS deployment.

Acknowledgments

The authors would like to thank Lorenzo Valeri and Jennifer Rubin for their thoughtful and insightful comments on this paper.

CHAPTER 1 Introduction

This paper is structured in the following way. Chapter 2 deals with the building blocks that need to be in place in a national context, i.e. what things need to be done well within Member States prior to participation in any PEGS. Chapter 3 lists some of the most pressing and unique trans-border challenges that are particularly relevant to PEGS. Chapter 4 deals with the lessons that have been learned. Chapters 5 and 6 outlines the range of policy interventions open to the European Commission, then outlines a way forward, indicating how an approach using two pilots might help to create as many opportunities for progress as possible.

The delivery of pan European e-Government services has the potential to make a significant contribution toward European integration and the emergence of a common European administrative space, further empowering European citizens to move about freely and work in any European country, regardless of domicile and without prejudice to status. A common administrative space would permit the seamless delivery of government services including taxation, healthcare, social security, work and residence permits, identification, etc. to citizens, regardless of location. Pan European e-Government also promises to help drive economic competitiveness and progress towards the Lisbon goals by supporting the free flow of people, goods and services (especially the implementation of the Services Directive), also by reducing administrative burdens and improving the effectiveness and efficiency of the European public sector.

CHAPTER 2

Governments must lead by example

Prior to engaging upon any interaction with PEGS initiatives, public administrations in the Member States should strive to 'lead by example' in the achievement of their own e-Government agendas. This chapter does not aim to provide a recipe for implementing 'secure e-Government' in a national or Member State context, rather it aims to identify and summarise those relevant building blocks that must be in place in each Member State prior to the implementation of PEGS.

These building blocks have a certain logic to them, although each country has approached them in different ways. Some have begun with the important task of the integration of back office functionalities, which seems like an appropriate place to start. Figure 1 illustrates a possible best approach on the experiences of some Member States.

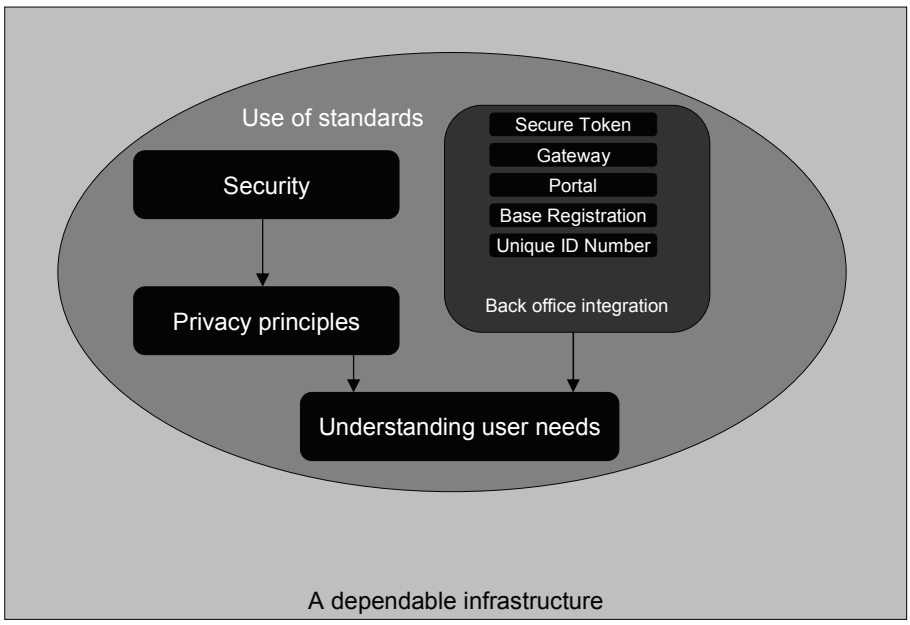

Figure 1. Steps for introduction of national-level building blocks for PEGS

2.1 Back-office integration

The first building block is back-office integration. Some administrations already have sophisticated programmes in place to rationalise and share information between government departments, but other countries are still developing their strategies. A common approach to identity is a key part of this integration as it enables achievement of the goal of 'single authentic sources of data in key registries that are unique, correct, and interoperable'.

The concept of the '24/7 virtual government' is becoming the standard for service delivery by governments. Very often this has been enabled by tools first used in the private sector, such as customer relationship management (CRM). This is a way to organise common business practices (e.g. marketing, accounts, etc.) around the customer or end-user. Despite the conceptual simplicity of such strategies, many acknowledge that it is relatively difficult to achieve such objectives in the public sector. In some instances, putting the citizen first via the opportunities that technology offers may involve radical reorganisation of the very architecture of government, rather than a simplistic 'digitisation' of cumbersome and outdated processes.

However, back-office integration is not just about the structure of data; it also must take into account systems and interoperability. This is particularly the case given the different channels of service delivery ranging from self-service via the web, to a government agent acting on behalf of a citizen, to a border control post with a terminal linked to a customs or immigration system. Back-office integration also permits proactive service delivery and the completion of forms in advance. If back-office data can be shared in a seamless fashion within a Member State, the benefits of PEGS can be realised far more effectively. Although the joining-up of similar services in a European context, without regard for national coherence, is possible, the chances of confusion are much greater if this is done first between countries rather than internally in a Member State. Examples might be in the area of unemployment benefit and taxation, where it makes sense for the taxation authority to check whether a citizen is claiming unemployment benefit in the country where they pay taxes, prior to any application for social security benefits in a new Member State.

2.2 Use of standards

The use of standards can help to facilitate interoperability and accessibility. Examples of this abound in the current e-Government climate and are focused on the area of electronic identity management (eIDM). These include the International Civil Aviation Organisation (ICAO) Machine Readable Travel Document (MTRD) standard, around which many governments are building national smart card systems. Similarly, in the financial services sector, the EMV Smart Card standard has become popular for card platforms offered by many financial institutions. In addition, the use of standards can help to address the issue of the proliferation of identities, allowing one human individual to seamlessly and easily manage identities relating to different institutions (e.g. government, financial institutions, employers, etc.) and different roles (employee, citizen, customer), which in some cases have specific requirements (e.g. an authorised representative of a large organisation; a medical doctor). As it is not going to be possible to ask Member States to re-engineer systems already in development, the use of standards tailored for the European context will be

critical to achieve interoperability. These standards need to guarantee interoperability at the semantic level (i.e. level of meaning), even if the technologies themselves are based on different technical standards.

2.3 Dependable infrastructure

Within a Member State a dependable infrastructure is required for the delivery of e-Government. This means that the information infrastructure which supports the storage, transmission and management of data used in any e-Government applications must be robust in the face of attack (from both the electronic sphere and the physical space, which may have consequences in the information infrastructure). Also, it must be resilient, including properties of 'graceful degradation'[1] degrading – no single attack must be capable of bringing the entire infrastructure to its knees; rather, the service must degrade gradually over time, with enough opportunity for alternatives to be found.

Having a dependable infrastructure may not necessarily mean a separate infrastructure from public networks either – there are procedures, techniques and tools (e.g. Domain Name System Security (DNSSEC), Internet Protocol Security in Internet Protocol version 6 (IPSEC in IPv6)) that would permit a comparative level of technological assurance to a privately-run secure network. Engineering a network with such properties of resiliency has the benefit of meeting two objectives: first, that dependency is created so that government can rely upon an alternative (manual or even paper-based if necessary) system; second, it maximises the channels available to the citizen, helping to address the problem of the digital divide (as many will still want or have to use face-to-face or manual forms of interaction with government). Finally, measures needed to provide for the dependability of this infrastructure are continually evolving and are doing so at a rapid pace as we move into the ubiquitous Information Society. Clearly, the requirement for each Member State to have a dependable infrastructure is important, but such infrastructures must be dependable in the context of their connection to others in other Member States.

2.4 Security

A risk-based approach to the management of information assets within public administrations is a crucial building block for governments prior to their roll-out of PEGS. While common understanding is that information security can be reduced down to the implementation of technical measures (such as firewalls, intrusion detection systems and so forth), in actual fact it requires managerial effort including, but not limited to, policies and procedures, management buy-in, leadership and continuous monitoring, audit and compliance. Understanding and taking on board the doctrine of information assurance instead of the more focused and technical concept of information security supports the achievement of confidentiality, availability and integrity requirements, and helps to support the message that 'security' and 'assurance' are not end states but processes. Clearly, given the types of information likely to be transferred around a PEGS, security is a critical

[1] Graceful degradation is the term for the ability of a system to withstand large scale damage or disruption over time rather than immediately succumbing to the effects of damage

part. Demonstrating the seriousness with which security is being taken is not only essential to help build citizen trust, but also contributes to trust between participating Member States.

2.5 Abiding by privacy principles

European governments as data custodians must abide by the data protection principles embodied in the current European Data Protection Framework. Adherence to these principles may be affected by a number of factors, for example, the effectiveness of any data protection ombudsman or supervisor, the competence of data custodians and the surrounding context or environment. Furthermore, the presence of outdated residual data will serve to complicate matters and may offer opportunities for error. Thus the requirement to 'clean up' databases, by removing obsolete data, must be met.

Another critical issue in ensuring privacy is not breached when deploying e-Government services (and hence PEGS) is 'mission creep' (i.e. the expansion of the mandate of any PEGS to fulfil other out-of-scope requirements), which may occur with acquiescence to law enforcement demands. Given the large amounts of data in circulation (much of it related to identity), it would be natural that representatives from the law enforcement and intelligence communities will want to have access to such data. Attempts to use or interrogate data sets made available by PEGS would be pushing the boundaries of the spirit or letter of the Data Protection Directive 94/46/EC and should be resisted as much as possible. Therefore, the implementation of PEGS must be acutely aware of mission creep and expansion of requirements driven by law enforcement needs.

This building block is relevant to PEGS because, like security, any deficiencies in Member States' adherence to privacy principles will result in a corresponding 'race to the bottom', as privacy protection becomes only as strong as that of the Member state with the weakest protections or the lowest common denominator. Such a race to the bottom can seriously undermine user trust, and thus the uptake of PEGS in general. Some of this challenge can be addressed by creating more transparency, allowing the data subject to know who uses the data and for what purpose, and to have the possibility to correct erroneous data. Also, a wider use of the right to consent is an important part of any data protection approach, as is an effective remedy in the case of privacy breaches.

2.6 Understanding user needs

e-Government must be citizen-centred and available through a variety of channels to the mobile European citizen in order to maximise opportunities for interaction. Data from the Federal Public Service of Information Technology and Communication (FEDICT) in Belgium indicated that only 10% of Internet users in Belgium use online forms to interact with the public sector and fewer than half of Belgian Internet users have ever sent an email to public administrations. These should include current common channels such as web and digital TV, also mobile and other forms of human–computer interaction not yet considered but on the horizon (e.g. via the Ambient Intelligent Environment). The lesson is that the provision of e-Government must be inclusive – unlike businesses, governments cannot forget about (or even must prioritise) a minority of their user community that is costly to reach – and thus it must consider the use of all possible delivery channels.

According to indicative research undertaken by the Belgian information and communication technology (ICT) agency FEDICT, there are a number of key user needs for e-Government:

- a 24/7 electronic counter (with the ability to make and receive payments and follow through all stages of a transaction);
- a central website with all forms available online;
- opportunities for the empowered management of personal data (e.g. via a digital safe);
- proactive forms of service delivery that are respectful of privacy;
- short overviews of procedures, steps and time-limits for interactions with the public sector; and
- pre-completion of forms and the proactive distribution of grants and benefits.

In an ideal world, citizens should not have to enter the same information repeatedly to qualify for benefits, and yet be able to count on their data to be treated with respect to privacy. User-centric e-Government takes a proactive approach. This means that, for example, a person who is eligible to receive benefits or rebates simply does so automatically. In a utopian example, the administration has all the required information needed to:

1. make an assessment of eligibility in advance;
2. confirm amounts and details with the relevant ministry; and
3. automatically pay into the citizen's bank account via authorised interaction with the financial institution following confirmation and notification to the citizen.

In one sense then, 'the best e-Government is no government' or at least a minimal level of interaction with agreed consent from the citizen.[2]

This raises an important tension that would need to be carefully managed, namely that European privacy requirements dictate that personal information (PI) or sensitive personal information (SPI) is only collected for the purpose for which it is intended. Data from UNISYS indicates that European citizens are very concerned about breaches of privacy: according to the UNISYS Security Index, misuse of personal information is a concern for 81% of respondents and 50% are significantly worried. Yet taking a proactive stance to the delivery of e-Government may contradict this. This might require reorganisation of information usage in order to enable administrations to collect data at one gateway, and then use it where necessary to deliver eligible and required services without the user filling in more forms (whether on paper or online) to confirm their eligibility.

Understanding of the user and their needs is an important prerequisite for PEGS because only with an adequate idea of the cultural and user requirements for each country and the highly mobile trans-European user, will such applications be broad enough to cater for all

[2] Data from FEDICT in Belgium indicated that two-thirds of Belgium Internet users and 80% of Belgian citizens expressed a preference for the pre-population of all forms required for interaction with the public sector.

sections of the likely user base. It also helps to make an effective cost–benefit analysis, when developing PEGS, to estimate who will use the services and with what frequency, and thus what strain will be put on the system as a whole and on certain public authorities in particular.

CHAPTER 3 The unique trans-border challenges of PEGS

Aside from meeting the challenges outlined in Chapter 2, which are particular to Member State level, a number of transborder challenges exist which impact security levels and must be dealt with in order to deploy secure PEGS successfully.

3.1 Different cultures

The EU is a mix of widely different cultures spanning 27 different Member States, each with particular national habits and expectations. There are also regional variations that may serve to affect the deployment of PEGS, for example, in the preferences for forms of regulatory intervention. In addition, there may be country-specific considerations around the use of personal data to take into consideration. This is particularly the case with new Member States in Central Europe, which may have cultural or social barriers to the management of personal data necessary for e-Government to take place. Although these cannot be easily and quickly reconciled, a first step to addressing them is identifying them and making them explicit, so that any solution can take such differences into account.

3.2 Different legislations

Despite the presence of a number of pan-European legislative directives, there is still a wide variety of legislation in place concerning some of the issues that PEGS covers. For example, although the Data Protection Directive has been transposed into the national laws of Member States, there remain differences in the details of its transposition. Also, EU law allows the coexistence of national laws that deal with overlapping or adjacent areas. Such a patchwork of national rules complicates overall compliance.

3.3 Consideration of legacy systems

Across the Member States there are a broad range of e-Government systems in varying stages of deployment. These range from stove-piped systems in one or two areas (e.g. driving licence renewal, application forms) to highly sophisticated environments with gateways, eXtensible Mark-up Language (XML)-enabled interoperability and electronic identification (as is the case in Austria, Belgium and, to a lesser extent, Estonia).

3.4 Different security approaches

One critical factor for PEGS is the requirement for interoperability or comparability of security levels and approaches. Although when using certain networks (e.g. sTESTA) each participant must be certified according to a common standard that they meet security requirements, this is not possible with the open nature of any PEGS. Other ways would

need to be found to achieve equality of security, so that what constitutes a certain level in one country may be understood similarly in another.

The problem of certification has been around for many years and has been a challenge to the deployment of security standards such as Common Criteria. The difficulty with achieving comparability of security in PEGS is in finding common ground due to different security practices, infrastructures and cultural attitudes to security. Furthermore, the situation is complicated by uncertainties about the broad range of different security contexts that a framework would need to take into account. Getting agreement on which security levels can be associated with what services also complicates any attempt to work towards an applicable security framework. Finally, although a commercial model of security based on standardisation (where those that can comply with requirements are permitted to join an authorised circle) may be the most rigorous, politically this would be difficult to implement due to concerns about denying access to PEGS for citizens from non-compliant countries.

Clearly, designing a security certification framework that can deal with such uncertainties is challenging. However, other work – most notably the Interchange of Data Between Administrations, Businesses and Citizens (IDABC) programme of the European Commission – has been looking at these issues in the context of creating a trusted intermediary between public key infrastructure authorities in the Member States. The remaining legal and technical challenges from the 2005 IDABC operational Bridge Gateway Certification Authority (BGCA) feasibility study continue to be explored after the dissemination of final recommendations[3] following the pilot study.

Unlike the operational BGCA project, which focuses only on the area of public key infrastructure, the timelex/Siemens study into electronic identity (eID) interoperability for PEGS is looking at the broader question of the interoperability of eID as a whole (rather than in one specific means of delivery). The timelex/Siemens study conducted for IDABC into eID interoperability for PEGS is exploring another approach as a solution to this challenge.[4] This study aims to define a universally applicable multi-level authentication model after a review of eIDM interoperability across a range of Member States and Accession Countries. So far, four tiers have been defined, ranging from minimal to high assurance. The resulting model will allow application owners to determine what tier of authentication is required and, for those providing eIDM solutions in a national context, to what foreign services a particular solution will be expected to provide access.

Due to the need to provide a comparative level of authentication across disparate environments, the applicability of a public key infrastructure solution may be seen: with an appropriately certified Certification Authority, different standards compliant software (such as may be present in the Member States' own e-Government deployments) can be included in a broad certificate chain. However, the lack of uptake of this complex and

[3] IDABC Documentation on Bridge / Gateway Certification Authority available at http://ec.europa.eu/idabc/en/document/3235/5585 (visited 01 January 2009)

[4] IDABC eID Interoperability for PEGS study available at: http://ec.europa.eu/idabc/en/document/6484/5644 (visited 01 January 2009)

costly architecture may preclude is deployment in this setting, not to mention the minimal security requirements for some forms of PEGS.[5]

Flowing from the comparability of security will be measures to provide for the interoperability of trust – that is, mechanisms to transfer trust between systems that have used different criteria in assessing trustworthiness. This will be harder to achieve, as there are several elements to trust, not least appearing to be trustworthy. Furthermore, trust has both a human and a technical face. The human face of trust is the perception that end-users have of interacting with a system (or a person), whereas technical trust can be achieved via the use of authentication and non-repudiation techniques and even more sophisticated matching, filtering or ranking schemes.

The role of national security authorities in managing, and being the ultimate arbiters for making sense of and correlating, these different security approaches will be paramount. National security authorities in each Member State may need to act as a security gateway, ensuring where possible that modes of interconnection meet national requirements, on the one side, and PEGS requirements, on the other.

Another consideration to be addressed in the wider context of security is how the interdependencies caused by interconnection of infrastructures across Member States affect overall system resilience. Achieving more understanding of how dependability is affected in a system of systems approach in the context of PEGS is a further prerequisite, so that areas of critical dependency can be identified and taken into consideration in the development of security requirements.

Finally, any system is only as secure as its weakest link; therefore care must be taken in the certification and accreditation of participants in order to ensure that the security posture is not unduly compromised (and if this looks likely, then a process is in place to deal with such challenges).

3.5 No applicable project management structure

Finally, the process of developing transborder PEGS does not fall under any direct EU competence, which means that the COM has no formal mandate to act and that there is no applicable project management or governance structure. At present, a large scale pilot (LSP) is being designed by a self-organising group of Members States to develop a European eIDM framework.

[5] The Netherlands applies a layered system of security levels and estimates that ~80% of public e-Services are thought to require only the lowest security level.

CHAPTER 4 Lessons learned in the provision of trans-border services

Given the peculiar and unique features of delivering PEGS outlined in Chapter 2, the November Working Conference identified a number of lessons learnt for the trans-border provision of services from other pan European systems or initiatives such as sTESTA, DG TAXUD and SEPA.

One of the key lessons was that in the delivery of any trans-European service where security plays an important role, the challenges were not concerned with technical controls on security or the security technology itself, rather with the organisation of the service and associated system, its legal footing, mandates and structure for governance and decision-making processes. The relevance of this lesson to the EU context is in regard to the complexity and difficulty of addressing these elements at EU level. Comparatively more resources will have to be expended on attaining agreement on the structure of any organisation charged with delivering PEGS, or putting in place a solid legal footing, for example, than merely deploying a specific security or authentication technology.

The November Working Conference illustrated an atmosphere of willingness to collaborate and cooperate between both the public and private sectors toward the delivery of PEGS. Any PEGS will include private-sector partners (as it would be impracticable and highly expensive for European governments to choose to deliver such PEGS by themselves). Involving the private sector in the execution and design of PEGS solutions would probably increase pragmatism in the delivery of a workable solution using commonly accepted standards (tailored to a European context). The public sector can learn from the private sector in the way in which different solutions are found to the same sorts of problem (e.g. in regard to inefficiencies in governance).

Leaving the market to deliver a solution using the most appropriate technology was seen as an ideal approach when it comes to meeting information security requirements. The use of a 'rulebook'-based approach – where the 'how' of the delivery of security is left open but the rules are specified in a framework – was seen as a very important lesson having wider application. In the pan-European context this is important, as it may permit the development of a 'federation of solutions' more tailored to prevailing local conditions and norms than a comprehensive 'one size fits all' approach. Having said this, it should be very clear that while the operation of security can be outsourced, its responsibility cannot – those charged with implementing PEGS must be aware of this fact. In any case, the degree to which it is possible to outsource security will be subject to political considerations.

PEGS solutions have to be built from scratch, taking on board existing experience and national building blocks. Building on a learning curve was an important lesson. When delivering systems of such complexity, it is important to use prior experience as much as possible, as there may be others who will have encountered the same or similar issues and resolved them. Another benefit from this approach is that legacy systems can be built upon, particularly where they are shown to be demonstrably successful. However, it was mentioned explicitly that any attempt to copy a best-in-breed solution for all is politically and practically unfeasible, due to the legacy issue.

In the face of security challenges it must be acknowledged that 100% security is neither an achievable nor a desirable objective. Instead, the use of considered risk management approaches is of critical importance. Although this can manifest itself in different ways, it is important to realise that risks should not be simply ignored or avoided, but managed, mitigated, accepted or outsourced. The management of risks means prioritisation of resources against those judged to be most important and the establishment of appropriate technical controls on those risks (e.g. business continuity measures) or use of other means (e.g. insurance). The relevance of this lesson to PEGS is that risk management must be applied consistently; therefore, a common understanding of what constitutes the most pressing risks (across the EU 27) should be reached, prior to the application of resources. There may be a role for a pan-European body, such as the European Network Information Security Agency (ENISA) or the European Commission, to own this process, in order to ensure that national interests are effectively incorporated without allowing these to block or wholly derail the process. ENISA is a particularly appropriate candidate, due to its role as an independent expert authority capable of providing advice to the EU on matters in this field.

As with many large-scale public sector projects involving technology, there are a number of lessons to be learned for the actual process of management of the project, governance of decision-making and operation of the actual services once they are implemented. In projects involving a broad and diverse group of stakeholders, a clear road map with milestones and timeline is essential and must be followed. Also, the use of a separate dedicated project secretariat was considered important (which has the added benefit of helping to manage the version control of project documentation), as was robust project management skills. In addition, the influx of budget that PEGS may bring could have unintended knock-on effects on public servants, who are used to managing projects with scant resource. Furthermore, the organisations most affected (and with most to gain) from implementation should retain control of the strategic direction of any implementation. Yet another element of the project management lesson was establishing good communication between all the stakeholders (notwithstanding the importance of properly identifying everyone with an interest in PEGS implementation) and those organisations in control of the direction of the process. Finally, a decision-making process may take consensus as a desirable principle, but voting must be considered also. Consensus is time-consuming and often leads to broad compromises, which are likely to deliver frameworks that leave too much discretion to individual Member States, leading to new barriers to standards and interoperability.

CHAPTER 5 Approaches and policy actions

Having seen the building blocks that should be taken into account for the delivery of secure PEGS, a map can be outlined which describes the various steps or activities and the interaction and interrelationship between these different steps and associated factors. The classes of activity to be undertaken include:

- the creation of essential preconditions which can be directly influenced by organisation;
- the exogenous and endogenous factors that should be taken into account when trying to deliver PEGS;
- organisation of the development process itself;
- a summary overview of the critical steps in the process;
- important elements belonging to each service under development; and
- what follow-up is required after the development phase.

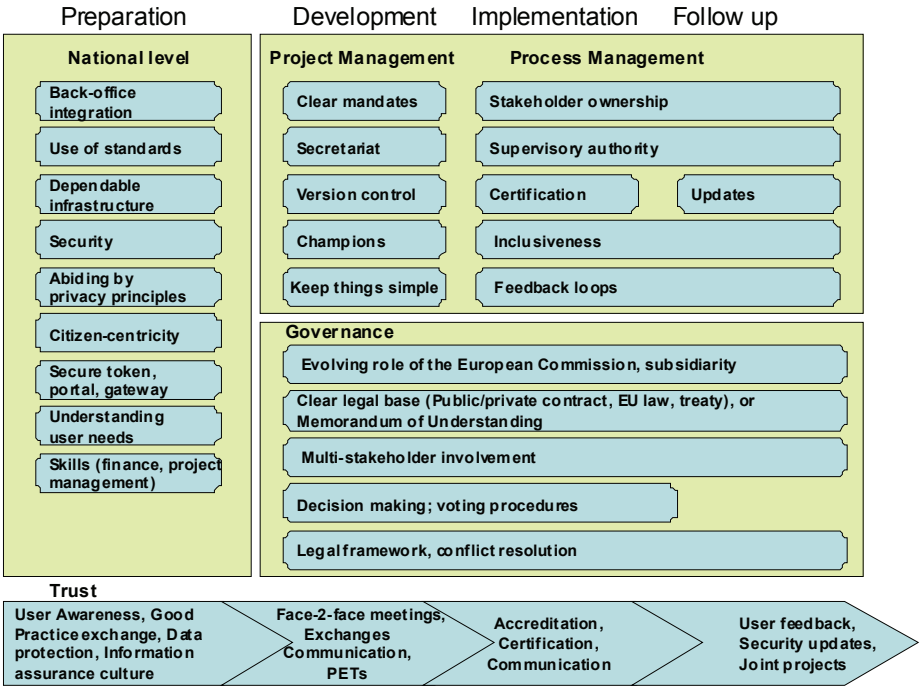

Figure 2. Interaction between elements to deliver secure Pan European e-Government Services

The following points represent a logic frame of the architecture of the various elements that affect or drive the stages illustrated in Figure 2.

- Critical process steps. These are steps that each stakeholder would need to take within their own Member State context prior to attempting to deliver any ambitious PEGS agenda. These would include establishment of the building blocks outlined in Chapter 1, but also other activities that would need to be undertaken at a pan-European level, for example, the creation of trust among all stakeholders (Member States, European institutions).
- Essential preconditions that can be directly influenced – these conditions can be influenced or optimised by structural design of an appropriate organisation and include establishment of a mandate, unambiguous governance mechanisms (e.g. voting mechanisms), identification of the role of the European Commission, etc.
- Critical characteristics belonging to each service under development. As has been seen from a number of the systems presented at the November Working Conference, each particular pan-European system has a number of common characteristics. These include such properties as:
    - the use of existing standards (perhaps tailored to a European context);
    - maintaining user-centricity (keeping user needs at the forefront of service design);
    - keeping simplicity in the architecture;
    - not getting bogged down in defining the detail of security (e.g. using a rulebook approach); and
    - building in privacy requirements from the outset.

- Exogenous and endogenous factors. Such factors may need to be dealt with or taken into account in implementing the steps or processes needed to move from building blocks present in a national or Member State context to PEGS delivery. Factors outside the process such as current environment, habits, culture, legacy systems, changing political agendas, etc. may affect the speed or impetus of progress. Other exogenous factors of importance include the threat environment, pace of technological change and market for relevant technologies (e.g. biometrics). A key question in this area is the time at which these different factors should be addressed – early in the process, or at the later stages. Endogenous factors (i.e. those that are internal to the process) might include security factors and user community take-up (not taking too long, as per SEPA).
- Organisation of the development process itself. This is an important facet and includes activities such as:
    - the creation of appropriate project management mechanisms, e.g. an independent agency or secretariat;
    - the creation of an achievable and realistic road map with an external audit validation mechanism which can act as a motivating influence to ensuring commitment to deadlines set out in such a document; and

    - the identification of champions that are willing to lead the way, or evangelists at the Member State and European level who are willing to spread the word about the initiative and encourage active participation.

- Follow-up after the development phase. Follow-up actions will be required in order to exploit the development phase, build upon successes, consolidate progress and awareness and adjust the architecture (where possible) based on user feedback. Examples of such activities include:
    - education and awareness for those leading implementation in each Member State to manage budgets appropriately (leaving enough left over for dissemination);
    - marketing and awareness campaigns (necessary to reinforce the benefits of PEGS to citizens and counter any likely bad publicity);
    - publicity and other dissemination efforts; and
    - embedding the output of the development phase in national activities to make PEGS endemic and an automatic part of the delivery of e-Government at Member State level.

In order to achieve the steps needed to deliver PEGS, collaboration between all the important stakeholders is required. The multidisciplinary nature of PEGS, requiring interaction from the public and private sector, European Commission and citizenry in general, lends itself to a hierarchy of collaboration mechanisms. This might be described as legal harmonisation at the highest level (where the European Commission and other European institutions are driving the process), with centralisation of certain tasks as a subset, federation in the middle (the ideal level for large companies and national governments to interact), and best practice exchange, which is best suited to forms of lower-level collaboration between individual programmes or initiatives; also to support the building-block phase in national Member States.

Services could be placed then in different categories, depending upon the degree of integration required – for example, cultural services might be highly localised in comparison to PEGS for customs, which would have to be highly harmonised at the EU level. Some also may be better off being rolled out among specific groups of Member States, given the utility of service to a certain prevalent sector or geographical space, but also possibly based on cultural convergence (for example, the approach to privacy).

CHAPTER 6 European Commission intervention and policy tools

The final step necessary for the European Commission is the identification of appropriate policy tools in order to support the delivery of PEGS, dependent upon the particular characteristics of each level of integration. A list of different types of available policy tools or forms of regulatory intervention might be as follows (by increasing weight of 'regulatory burden').

- Provide leadership. The articulation of change by the European Commission would be one useful form of intervention, particularly in regard to describing the required national building blocks and supporting the implementation of these in Member States prior to the deployment of PEGS. Such discussions could occur in a number of existing pan-European forums such as the eGovernment Subgroup or within the context of IDABC. *In any case, the continued presence of European Commission representatives at major forums such as the Poorvoo Group, presenting a consistent and robust agenda for change, will be helpful. Furthermore, the collection, sifting and classifying of data on the national building blocks (and the ownership of this information via a reputable body or agency such as ENISA) will support the European Commission's platform.*
- Provide a platform for best practice exchange, such as ePractice, which really delivers the support that national case owners need to design and implement the necessary building blocks. Within ePractice, special attention may be given to those actors looking for developing cross-border and/or pan-European applications. *ePractice should strive to improve continuously the good practice exchange mechanism, by:*

    - *helping the transformation of existing services into more modular formats;*
    - *facilitating training and testing;*
    - *collaboratively drafting an evolving 'cookbook' based around specific challenges;*
    - *increasing awareness among stakeholders;*
    - *building relationships and trust; and*
    - *actively using the private actors involved in the systems and software design to sell and market effective solutions.*

- Help to forge a consensus that can support the identification of appropriate standards tailored to a European context (e.g. standards taking into account the peculiarities of the European Privacy Framework). *This might be achieved by the European Commission emphasising its public support to industry fora e.g. the Organisation for the Advancement of Structured Information Standards (OASIS) or the World Wide Web Consortium (W3C) with the Platform for Privacy Preferences.*
- Provide seed money for research into a number of issues identified which may help in the deployment and implementation of PEGS. Examples can be found at Appendix 1 (public funding or funding by public interest sources). Research and Technology Development (RTD) is useful for areas where the generation of new knowledge is necessary and where this knowledge cannot be acquired by just 'doing', as would occur in a pilot environment. *This may take place via the inclusion of such topics in Framework 7 Programmes, but the justification of the inclusion of particular research topics in the Framework Programme would need to be carefully considered, alongside other instruments such as commercially tendered studies (Directorate General Information Society and Media (DG INFSO), IDABC, ENISA and inclusion in Competitiveness and Innovation Program for ICT (CIP ICT PSP) pilots and thematic networks).*
- Pass legislation. For example, in revision of the Data Protection Framework to protect better against abuses of privacy resulting from 'mission creep' by stakeholders not directly associated with the delivery of PEGS, and instituting better *ex-ante* legal measures for the improvement of security. In addition, such a revision may address the need for cleaning up databases by removing obsolete data. *Concrete examples might be:*

    - *the push for greater emphasis on responsibilities for privacy in the review of the Electronic Communication Framework;*
    - *drafting proposals for legislative efforts on the back of the Strategy for Secure Information Society (e.g. via the creation of breach notification laws); or*
    - *greater emphasis on inclusion of consideration of privacy in the legal aspects of impact assessments.*

The use of these tools would have to be geared towards the services and would be dependent upon the type of services (e.g. law enforcement or healthcare) and level of integration (harmonisation; federation or best practice). For example, for the European Commission to support the delivery of PEGS for customs, it might be more likely that interventions such as the imposition of new regulations might be more appropriate, since having a harmonised PEGS for taxation would contribute toward wider EU objectives for growth, etc. For those PEGS linking with private-sector systems, some of the more regulatory 'lighter touch' tools might be more appropriate in order to provide a positive environment for private sector participation. For healthcare, for example, the chosen intervention might be along the lines of market stimulation – inspiring or engaging the insurance industry. In yet other areas, R&D would be the most obvious approach.

6.1 The way forward

Sooner or later the deployment of some form of test implementation or pilot will be necessary in order to progress PEGS from exploration to actual implementation. Defining what PEGS fall within the scope of a pilot will require further analysis and the development of selection criteria. Clearly, the identification of such criteria is a candidate for further work. In any case, interoperability will be a key part of the selection criteria for a PEGS pilot. A possible way forward based on the concept of development in practice and learning could be found in adjusting the two types of pilots that the European Commission supports under its CIP ICT PSP.[6]

1. *A directed pilot focused on the delivery of PEGS by a set of countries and people that are politically and personally committed to make it work. This will be a two-stage process. First, in the design stages, the pilot will need to observe practices as they are developed within the current eIDM large-scale pilot and how it has taken into account the lessons learned from the November Working Conference. This would be a form of monitoring exercise, using management instruments already in place between the European Commission and participants in the current eIDM large-scale pilot. The second phase would be the implementation of the pilot. The aim of the directed pilot is to identify what real issues come up in practice when truly working together in a pan-European environment, including legal issues, interoperability issues (e.g. not only at a technical level but also at a level of culture or semantics), etc.*

This pilot should be undertaken by a set of countries familiar with the delivery of e-Government and which are already at an advanced stage of deployment of some, if not all, e-Government services (and have perhaps initiated preliminary bilateral links to other countries). This pilot will have a focused timeline, structure and objectives. Candidate countries for the directed pilot would bring in demonstrable experience in e-Government and stakeholders would need to be able to demonstrate a degree of political and personal commitment. In its implementation stage the directed pilot should try to take on board and adopt the lessons learned which were identified in the previous chapters, and would attempt to implement strong governance, requiring participants to agree upon and adhere to identified timetables, milestones and a road map.

The pilot would need to establish mechanisms for measuring or monitoring the effectiveness of project management, governance and decision-making processes. Consideration of adaptive decision-making principles, which permit continuous feedback loops and policy improvements, would need to be built into governance structures with the directed pilot. The European Commission's role – aside from contracting party and initiator of the pilot - would be to act as an independent authority, helping to support progress against a road map, and making sure (as was seen with SEPA) that participants stick to their commitments. The factor of time (speed of the process, keeping momentum and adherence to timescales) will be important in developing the directed pilot and monitoring its success and follow-up. Other responsibilities for the European Commission might include helping to ensure the fairness of governance processes (e.g. by making sure

[6] More detail on the pilots can be found at Appendix 2: Understanding the 'Two-track pilot' model.

all stakeholders are involved), dissemination of outputs to EU Member States with less mature e-Government programmes, and making sure that, to the extent possible, a 'level playing field' exists following the result of the pilot and that fair competition is not compromised.

2. *Pilot B is more application-driven. This 'sandbox' environment would have a more exploratory rationale, which would encourage the development of a broad range of approaches to delivery of PEGS applications depending upon the specific characteristics of services (education, health, border control, immigration, etc.).*

Participation would be limited to a smaller number of pioneer countries, aimed at making the application itself work on a smaller scale before expanding. Participation would be based on conformance to a minimum interoperability level (set deliberately low to encourage participation), based on globally adopted standards revised for the European context. Lessons learned about the delivery of particular applications should be fed back into directed pilots.

3. *Share the practice experience of current pan-European government applications (2nd Generation Schengen Information System (SIS II)/Visa Information system (VIS)/European Dactylographic Comparison System (EURODAC), etc.) and international business experiences (UNISYS, IBM, etc.) (possibly organised around the directed pilot), and develop standards, or gather experience with the use of existing (open) standards.*

Sharing experiences often permits the identification of common challenges and best practice among previously disparate stakeholders. One approach to help support the ongoing success of PEGS as progress continues from R&D to demonstration and implementation would be the establishment of a more formalised system to identify best practice among current pan-European e-Government applications. The current ePractices platform is an ideal candidate for this approach. These might range from trans-European systems such as the Second-Generation SIS II, VIS and the Biometric Matching System (BMS) to those from other European portfolios such as DG TAXUD, Solvit, EURES, and trans-European networks (eTEN) applications such as NETC@RDS and Riser, or in specific domains (e.g. Safer Internet or Pan-European Game Information (PEGI) self-regulatory system) and those outside of the European Commission's area of responsibility (e.g. NATO systems or common European financial systems). Generating an atmosphere to solicit from private sector or non-EU schemes would require an innovative approach, perhaps via the use of a circle or closed forum where such best practice should be shared in a trusted environment.

In addition, it would be valuable to identify other experiences from the private sector. Although the underlying drivers for the development of consistent regional initiatives with the private sector are different to e-Government (reduction in costs, achievement of efficiencies, greater emphasis on economic incentives), there are still some applicable lessons to be learned (e.g. the need to design an effective project management structure, the necessity for governance mechanisms, the need to keep strategic control of the process in the hands of the primary user community, etc.).

4. *Need to assess the need for different levels of intervention at pan-European level: e.g. harmonisation of legislation or legislative action, further support programmes? To be considered and implemented at the moment that it becomes necessary (monitoring, rather than regulating, until more experience can be identified from the directed pilot).*

Finally, given the importance of legislation and legislative action at EU level, a watching brief will need to be kept up on the need for harmonisation of legislation at the European level. Whether this is to do with specific challenges unique to PEGS (e.g. the creation of a legislative framework for the provision of appropriate mechanisms to deal with the security challenges posed by PEGS), or an overarching framework, will have to be decided. The experience gained from undertaking the directed pilot will be crucial in the identification of areas ready for regulatory intervention and appropriate timescale. A critical element here will be the European Commission's actual competence to take action and effectively ensure the principle of subsidiarity.

5. *Conduct a large-scale benchmarking exercise of the information assurance (IA)[7] maturity of EU Member States: not to apportion blame, rather to identify where levels and understanding of trust diverge in order to inform properly any security requirements for PEGS.*

A broad macro-level IA benchmarking exercise would support the identification of different levels of trust in the Member States. Because such a benchmark considers IA (rather than technically-orientated information security), it could take into account the peculiar national and cultural characteristics of each country to provide a normalised understanding of strengths and challenges at the Member State level. As has been seen earlier in this paper, meeting the security concerns of PEGS requires risk management. However, due to the complexity and absence of transparency around the types of risk that may be encountered, risk assessment and management is fraught with difficulty. A macro-level IA benchmark or review would be a first step in understanding these complexities and expose the nature of risks likely to occur via the interconnection of Member State systems (e.g. differing levels of maturity in two countries in the same area may raise cause for concern). Although benchmarking at the national level has methodological challenges associated with it in terms of comparability and understanding of the national context (not to mention availability of data), the comprehensive accessibility of other tools to normalise results (e.g. GDP data or statistics on the use or take up of e-Government) will permit valid comparison.

[7] http://www.iaac.org.uk: 'Information Assurance (IA) can be defined as: "a management process, the purpose of which is to ensure that the critical information within an organisation and the systems and networks that manage it are reliable, secure and private, and that measures and processes are in place to counter malicious electronic based attacks. IA encompasses other disciplines such as information security management, risk management and business continuity management."'

APPENDICES

Appendix A: Possible R&D areas

This list sums up a number of open points or queries raised by the different pan-European systems presented at the November Working Conference, combined with gaps for further necessary research identified following primary research by the SecurEgov study.

Addressing these gaps may be possible via Framework Programme 7 research or small studies indicating where the European Commission might be able to support other forms of intervention, in order to provide answers to these questions. For those areas of research dealing with the legal framework, studies or research financed from the Policy Support Programme might be more appropriate. Research into some of the more technical areas will be better performed by industry.

Following on from the background paper into the *State of Research into Secure Pan-European e-Government Services*, we structure the identified research topics into four themes.

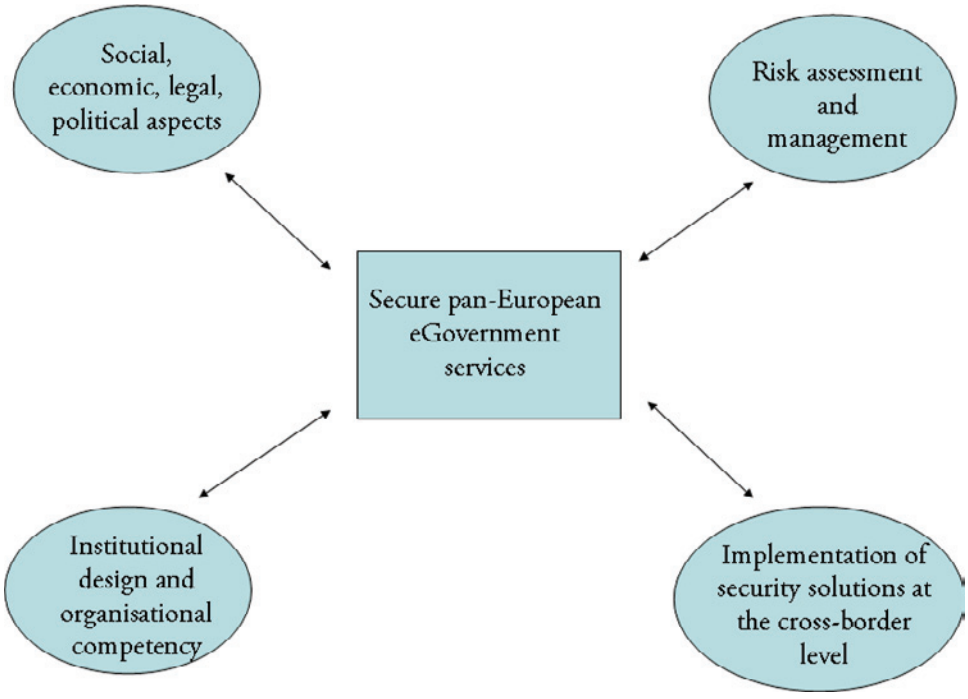

Figure 3: R&D areas for Pan-European SecurEgov

(Source: RAND Europe)

Institutional design and organisational competency

- What are cost-effective ways to clean out (and keep clean) outdated data without increasing the administrative burden?
- What should be the role of the European Commission in managing convergence of technical and organisational solutions, while respecting the principles of subsidiarity, in order to achieve the roll-out of PEGS?
- What is the role of national security authorities as the accreditation bodies for PEGS security?
- How can an efficient framework be developed to open up and interconnect Member States' back offices so that this does not need to be done on a case-by-case basis (as with the Belgian example)?
- What constitutes good practice for the development of systematic interfaces across different government departments (a tool of citizen-centric PEGS)?

Implementation of security solutions

- How can appropriate levels of service over public networks for mission-critical or high-availability networks used for PEGS (e.g. via IPv6) be obtained, and is it possible to use high-availability service-level agreements over public networks?
- Can further applied research into trust-enhancing technologies (e.g. BT plc or Hewlett Packard Labs Trustguide research) take place?

Social, legal and political aspects

- How can revision of the EU Data Protection Framework take place to deal appropriately with law enforcement access to (residual) data held in PEGS?
- Can ways to integrate security into data protection rules and prevention of abuse instead of dealing with the consequences *ex-post* (e.g. perhaps a security directive) be identified?
- How can statistics on the digital divide be improved?
- What constitutes an appropriate combination of expert control and personal consent over how personally sensitive data is used?

Risk assessment and management

- How can security or trust levels (perhaps the reverse – measuring in-security) be measured and can appropriate parameters to measure trust or security and the value of both be discovered?
- How can security requirements be defined, when these will evolve, and what is the appropriate way of managing this change?
- What gaps exist between legal, semantic and trust interoperability?

Appendix B: Understanding the two track pilot model

A paper by Professor Roger Jowell of City University prepared for the Government's Chief Social Science Researcher's Office in 2003 recommended that 'closely monitored pilots' should accompany the full-scale introduction of new policies and delivery mechanisms.[8]

Pilots should be undertaken only if a number of conditions are met:

- if a new policy and its delivery mechanisms are already cast in stone, then a pilot is redundant;
- pilots must be allowed to run their course;
- the pilot must take into account realistic timescales of the time it takes the actual policy to bed in;
- pilots should be preceded by systematic gathering of data from the UK and abroad; and
- the precise purpose of a pilot should be made clear in advance.

An earlier report from the UK Cabinet Office Performance and Innovation Unit in 2000 identified two types of pilots:[9]

- impact pilots – tests of the likely effects of new policies; these pilots are concerned with assessing whether a new policy intervention will actually work; and
- process pilots – these are designed to explore the practicalities of implementing a policy in a particular way or route; the assessment of what methods of delivery work best or are most cost-effective.

It is in this spirit that we propose that, prior to the full roll-out of PEGS, a two-track pilot is developed. Both the directed pilot and the 'sandbox' are forms of process pilots, designed to explore the day-to-day practicalities of implementing secure PEGS.

---

[8] R. Jowell (2003) *Trying It Out: The Role of Pilots in Policy-making. Report of a Review of Government Pilots*. Government Chief Social Researcher's Office, Cabinet Office Strategy Unit. London: HMSO, p. 8.

[9] Performance and Innovation Unit (2000) *Adding It Up: Improving Analysis and Modelling in Central Government*. London: The Cabinet Office.

Directed pilot The directed pilot will be a structured form of test of the deployment of PEGS. It will involve a small number (no more than six or seven Member States) which have already demonstrated competency in bilateral or multilateral initiatives (e.g. in the eIDM large-scale pilot). Such countries must demonstrate significant progress in e-Government (e.g. meeting an initial threshold for the number and take-up of national e-Government applications), and demonstrable maturity in e-Government deployment, etc. The directed pilot would include a monitoring function, possibly performed by the European Commission. Key performance indicators and measures of success would be laid out in advance of the pilot commencing, in order to make clear at what point the pilot might be judged a success. Also, the design of the pilots would take into account a number of other considerations highlighted by the Jowell Report, mainly:

- identification of adequate budget;
- the mix of government versus private sector involvement;
- the duration of the pilot (including the tendering process);
- the use of methods and correct application of methods to the aim of the pilot; and
- the use of qualitative and quantitative elements.

The operation of this pilot would have pertinent lessons identified from the November Working Conference uppermost; namely that those most affected by the pilot would be in the driving seat of strategic direction; there would be rigorous governance mechanisms in place with appropriate project management, a realistic timescale and achievable objectives. Particularly, in contrast with the current eIDM large-scale pilot, great focus would have to be placed on project management techniques in order to assure consistent delivery. In order to support the progress of the pilot a firm legal base would need to be established and the management and monitoring function given enough mandate to act (e.g. by casting the deciding vote) in decision-making to avoid stalling progress.

Sandbox pilot In contrast, the sandbox pilot would be based on a 'join-in' environment. This would be achieved by the publication of a number of standards (including security and interoperability) to which participants would have to ensure their systems could conform. These standards might be devised and owned by an externally competent body such as ENISA. Participants then would be able to interact in a bilateral, multilateral or pan-European manner. A feedback loop would be provided by an external observatory or monitoring function, but unlike that of the directed pilot, this would have no 'teeth' or mandate to force decisions, rather it would be there simply to report the findings of the interaction between Member States. Thus reporting and monitoring functions would be softer and more on the basis of identification of good practice, or where interactions went well or poorly between Member States. The collection and dissemination of the results of these interactions and experimental tests would be via a specific study or piece of research that could be conducted at the end of the pilot.

In order to provide feedback from the sandbox pilot to the directed pilot, the European Commission would need to be kept informed as to how identified lessons from one are impacting upon the progress of the other. As it is expected that the European Commission would play a significant role in the directed pilot (in terms of acting as an external management authority, as was the case with SEPA), it is reasonable to expect that the

observatory function of the sandbox pilot would report regularly to the European Commission, perhaps at three or six-monthly intervals (depending on the duration of the pilot).

Finally, a critically important issue to understand is that, due to the fact that pilots are highly monitored and observed (being precursors to fully developed policy implementations), there is a risk that the act of monitoring and evaluating them may change their outcomes. Because a pilot (which has been under close evaluation) has been successful does not mean to say that the full-blown policy implementation will be similarly successful. All too often, assumptions are made that this will be the case, to great financial and sometimes ministerial or governmental cost.

Appendix C: Glossary

B2C	business-to-consumer
BGCA	Bridge Gateway Certification Authority
BMS	Biometric Matching System
CIP ICT PSP Programme	Competitiveness and Innovation Programme for ICT Policy Support
DG TAXUD	DG Taxation
DNSSEC	Domain Name System Security
eID	electronic identity
eIDM	electronic identity management
EMV	Standard for smart payment cards
ENISA	European Network Information Security Agency
eTEN	Trans-European Networks
EURODAC	European Dactylographic System
FEDICT	Service Public Fédéral Technologie de l'information et de la Communication (Federal Public Service of Information Technology and Communication)
G2B	government-to-business
ICAO	International Civil Aviation Organisation
ICT	Information and Communication Technology
IDABC	Interchange of Data between Administrations, Businesses and Citizens
IPSEC	Internet Protocol Security
IPv6	Internet Protocol version 6
MRTD	Machine Readable Travel Document
NATO	North Atlantic Treaty Organisation
OASIS	Organisation for the Advancement of Structured Information Standards
PEGI	Pan-European Game Information

PEGS	Pan-European e-Government Services
PI	personal information
SEPA	Single European Payments Area
SIS II	Second-Generation Schengen Information System
SPI	sensitive personal information
sTESTA	Secure Telematics
VIS	Visa Information System
W3C	World Wide Web Consortium
XML	eXtensible Mark-up Language