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

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.