



## EUROPE

THE ARTS  
CHILD POLICY  
CIVIL JUSTICE  
EDUCATION  
ENERGY AND ENVIRONMENT  
HEALTH AND HEALTH CARE  
INTERNATIONAL AFFAIRS  
NATIONAL SECURITY  
POPULATION AND AGING  
PUBLIC SAFETY  
SCIENCE AND TECHNOLOGY  
SUBSTANCE ABUSE  
TERRORISM AND  
HOMELAND SECURITY  
TRANSPORTATION AND  
INFRASTRUCTURE  
WORKFORCE AND WORKPLACE

This PDF document was made available from [www.rand.org](http://www.rand.org) as a public service of the RAND Corporation.

[Jump down to document](#) ▼

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

### Support RAND

[Browse Books & Publications](#)

[Make a charitable contribution](#)

### For More Information

Visit RAND at [www.rand.org](http://www.rand.org)

Explore [RAND Europe](#)

View [document details](#)

### Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Unauthorized posting of RAND PDFs to a non-RAND Web site is prohibited. RAND PDFs are protected under copyright law. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please see [RAND Permissions](#).

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.

# 2015: A connected and diversified Europe

eIDM Vision Paper

Constantijn van Oranje-Nassau, Neil Robinson,  
Maarten Botterman

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

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.

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

**RAND**® is a registered trademark.

© Copyright 2009 European Commission

All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from 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](mailto:order@rand.org)

# Summary

---

Europe in 2015 may be largely interconnected with pan-European eGovernment services (PEGS) being delivered to citizens based on a full scale common European electronic Identity Management (eIDM) system; providing seamless identification and authentication of individuals. However, it is just as likely that Europeans and their governments resist such coordination of efforts and interoperability of systems; thus opting for a very minimalist approach to eIDM; where a common identifier may support a very specific and limited set of basic applications. In between these two alternative futures we identify a scenario that is largely services driven and foreshadows a fragmented eIDM environment with different coalitions of countries and stakeholders, clustered around the utility that each service represents.

The landscape in 2015 will be largely determined by a number of factors:

- Outcomes of the large scale pilot
- Levels of identity
- Ambitions: Quality of service
- Prevalence of trust

With key drivers being: further European Integration, the implementation of the Services Directive, the stated ambitions on administrative burden reduction, and parallel private sector developments

There is no clear incentive for national public authorities for developing pan-European services for citizens, let alone a full scale European eIDM framework. However there are other developments and trends that will push or pull further cross border or even pan-European collaboration in these areas. As these do not all work in the same direction it is likely that a diversified supply of cross-border and pan-European services will emerge. Likely applications will be found in health care and in support of worker mobility. A possible third area could be education. In parallel, the exchange of ID information will increase in the field of law enforcement and specific niche applications for business sectors. The financial sector is also likely to go ahead and develop its own platform.

PEGS hold the potential to provide a new impetus to European integration and they may preempt the emergence of a pan-European Administrative space. The current inertia of public authorities to invest in cross border eIDM models, as well as to adjust legal legacy systems and coordinate organisational processes, still present a formidable barrier. Thus leadership is required and needs to be accompanied by effective governance of the process, with a firm hold on the principle of subsidiarity. The success of any European eIDM depends largely on trust. Trust

between Public Authorities (PAs) and trust of the citizens in administrations across the EU to defend their interests and rights and to deliver concrete benefits.

A European eIDM framework is also expected to yield economic benefits, the assumption being that businesses will use such an overarching identification system to develop new services. There is however substantial hesitation from the business community to proceed. The general attitude is characterised as 'wait and see', and for business to invest in any public eIDM system there clearly needs to be sufficient critical mass of users/consumers. To get the private sector on board earlier in the process the PAs involved would need to work with existing standards, draw in the business community to understand their needs, and to involve it in the development of the system. In particular, care should be taken not to re-invent the wheel and use or reference existing common standards.

Once effective solutions and good examples at local, national and regional level emerge political commitment to actual implementation is expected to grow. The current focus on the Large Scale Pilot is too limited to effectively develop a common eIDM system for Europe; given the various other platforms and avenues that could be explored and which are in fact being developed already. Any common solution would require strong leadership, in order to ensure a co-ordinated approach based on addressing the real needs of users, and facilitate a European application that is simple, secure, resilient, robust and effective. The most likely feasible and possibly desirable option is to aim for one common European Identifier; one number based on existing national ID numbers, without authentication at the EU level.

This raises the issue of what security level would be required for accepting non-nationals to the system. Either a common EU system is developed with accepted standards for a given set of applications or any Pan European (PE) application would most likely require the highest security level, which may still be Public Key Infrastructure (PKI) in 2015. Much also depends on trust between public authorities. Even the safest systems are worth little if the process of eID enrolment is fraught with inaccuracy and fraud. It will be difficult to achieve this high level of trust among citizens of the EU 27 (or maybe 30 by 2015). Thus accompanying measures and guarantees are required that provide assurance of fraud free enrolment. In addition serious sanctions for inaccuracies and incompetence need to be in place, as well as guarantees for liability and damages.

Citizens need to trust that their information is safe and that neither government nor unauthorised third parties have access to this data. If this cannot be guaranteed or if the perception of abuse prevails – through actual breaches or false perceptions – the system will fail because of a lack of users. It should also be envisaged that the system decouples the electronic Identity (eID) from the personal data, which would allow usage of the (non-personalised) data for socio-economic and health research purposes.

The expected lacklustre demand could be partially overcome if other actors would have access to the PE eIDM backbone to support the development of their services, thus creating a multiplier and a network effect which would increase the overall value of the system. Public spending could be applied to stimulate take up by the private sector. Also public policy can help creating more transparency. The plethora of standards, models, specifications, meta-languages and frameworks risks drowning practitioners in the total number of alternative and possibly incompatible approaches, leading to a loss of opportunity and effectively doubling the amount of work. It would be desirable to set up a PE "knowledge centre" on identity management, and "virtual

middleware” that would support the various different systems across Europe to interconnect by indicating or referencing which technical middleware would be appropriate to allow different eIDM systems to interconnect.