Prepared for the eGovernment and CIP Operations Unit
DG Information Society and Media
European Commission

Bringing Together and Accelerating eGovernment Research in EU

INTERNATIONAL DIMENSION: Europe – North America

July 2007

eGovernment and CIP Operations Unit
DG Information Society and Media
European Commission

Executive summary

eGovernment utilises technology to accomplish reform by fostering transparency, eliminating distance and other divides, and empowering people to participate in the political processes that affect their lives. EU and U.S. governments have different strategies to build e-government. Some have created comprehensive long-term plans while others have opted to identify just a few key areas as the focus of early projects. The following paragraphs bring into light the major eGovernment developments in Europe and the U.S.

Starting with the comparison of the major source of support for eGovernment research, it is evident that in the USA the major source of research funding is at the federal level, from the USA's National Science Foundation (NSF). A similar situation characterises Europe, where the overwhelming majority of research funding comes from European Commission (EC), which with some freedom and optimism can be considered as the 'federal' centres for its 27 Member States. However, the U.S. have additional sources of eGovernment research funding from other federal agencies, eGovernment initiatives by State governments, and some industry support. In the EU, pure research funding is mainly provided by the European Commission.

In the USA many federal agencies fund eGovernment research because they have identified a number of specific issues to be addressed. By contrast, a possible interpretation of the lack of eGovernment research funding by national governments in the EU could be that many Member State governments have neither a definition nor a vision of eGovernment, and no strategic plan to transform traditional government into eGovernment.

The EU and U.S. are also different from each other in terms of the length of time their research projects are funded. EU research projects in general are funded for a longer time than those funded in the U.S. In particular, much of the funding in the U.S. is through the National Science Foundation (NSF). Through NSF, some projects are funded for as little as a few months, while other projects are funded for a couple of years. These funds are available for studies that investigate transformative research ideas; or application of new expertise or studies that may catalyse rapid and innovative advances.

In the EU, high priority is given to research actions that focus on security and flexibility of large, complex, open and interrelated infrastructures, as well as on methods for mapping and modelling the infrastructure underlying processes. eAuthentication was defined as "*the Web Based service that provides authentication to end users accessing (logging into) an Internet service*". eAuthentication is setting the standards for the identity proofing of individuals and businesses and is similar to Credit Card verification for eCommerce web sites.

In the U.S. the E-Authentication Initiative has successfully launched the E-Authentication Federation, a public-private partnership that will enable citizens, businesses and government employees to access online government services using log-in IDs issued by trusted third-parties, both within and outside the government. As this ground-breaking collaboration between government and industry continues to mature, it will further improve U.S. government's ability to deliver services to the American public and save taxpayer dollars.

Table of Contents

List of tables

1. eGovernment

eGovernment utilises technology to accomplish reform by fostering transparency, eliminating distance and other divides, and empowering people to participate in the political processes that affect their lives. EU and U.S. governments have different strategies to build e-government. Some have created comprehensive long-term plans while others have opted to identify just a few key areas as the focus of early projects. The following paragraphs bring into light the major eGovernment developments in Europe and the U.S.

1.1 Europe (EU)

In Europe the EC specifies thematic priorities for the focus of funds for eGovernment research. Implementing eGovernment through online availability of information and access to online documents was the focus in the 5th FP. This focus was shifted in FP 6, towards back-office modernisation. Nowadays, interoperability, eParticipation and electronic Identity Management are some of the major eGovernment themes funded at the European level.

The Lisbon Strategy (2000)[1] and the new i2010 initiative (2005)[2] provide the main directions for strategic policy orientation and implementation in the EU. Both those initiatives are groundbreaking for eGovernment research with the focus being on more investment and innovation, particularly in increasing the speed of innovation development and productivity. Furthermore, the i2010 initiative highlights the need to set up a single European information space promoting an inclusive European Information Society.

These strategies are reflected in research programmes funded by the EC, and in many European Member State strategies to modernise their governments by implementing eGovernment. EC research programmes related to the i2010 strategy and the eEurope 2005 Action Plan (EC 2002)[3] are e.g. the MODINIS programme (MODINIS, 2003)[4]; the Interchange of Data between Administrations (IDA, 2004); Interoperable Delivery of Pan-European eGovernment Services to Public Administrations, Business and Citizens (IDABC) programmes (IDABC, 2005)[5]; and Trans-European Networks (eTen, 2007)[6].

The Danish Technological Institute (DTI)[7] together with the European Institute of Public Administration (EIPA)[8] elaborated a key forward-looking study which resulted in a report towards the eGovernment vision for the EU in 2010[9]. This report identified *harmonisation and interoperability, trust and security*, *access for all to government services*, *knowledge management for data*, *understanding individual user needs*, *change in the public sector*, and *new government delivery models* as the major research areas of interest in Europe assessed by government stakeholders.

Accordingly, current eGovernment research was clearly focused on technology use and the exploitation of these solutions. The expected future developments emphasised that more research activities in the field of user needs and usability, socio-economic inclusion, eDemocracy, value chains, and cross-sector public services is needed. Current FP 6 projects

[1] http://www.europarl.europa.eu/summits/lis1_en.htm.

[2] European Commission (2005). i2010 - A European Information Society for growth and employment, COM (2005) 229 final. Brussels, European Commission.

[3] European Commission (2002). eEurope 2005, An information society for all: An Action Plan to be presented in view of the Sevilla European Council, COM (2002) 263 final. Brussels, European Commission.

[4] http://ec.europa.eu/information_society/eeurope/i2010/modinis/index_en.htm.

[5] http://europa.eu/scadplus/leg/en/lvb/l24147b.htm.

[6] http://europa.eu/scadplus/leg/en/lvb/l24226e.htm.

[7] www.danishtechnology.dk

[8] www.eipa.nl

[9] Millard, J., Warren, R., Leitner, C. & Shahin, J. (2006). EU: Towards the eGovernment Vision for the EU in 2010.

have a focus on wider organisational aspects of service design and delivery. Overall management of change to achieve networked governments is the primary aim. In future research, a stronger link among European and national policy requirements should be emphasised, especially a) for social cohesion and inclusion policies, and b) for economic, and cross public sector policies. The first policies were emphasised mostly by academia, the public sector and users; the latter by consultants, industry and non-Europeans.

The top ten topics of interest in eGovernment at the national level, counted by the number of their occurrences, are the following: generation and delivery of added value services, document identity management and authentication, security and trust, eInclusion and eParticipation, access via multiple channels, understanding user needs and user-centric services, (technical) interoperability, eLearning, (public) eProcurement, and quality management.

A further insight gained so far is that, currently, governments in the EU Member States barely work in cooperation with academia in order to advance the integration of innovative research with practical applications. In addition, there is a gap between the various levels of eGovernment implementation across the EU. Having a closer look at the new EU Member States, eGovernment related funding by the EC is situated under the structural programme of the EC that funds pure implementation. As a result, the eGovernment efforts of the new Member States concentrate on bridging the gap between themselves and the established countries. For this reason, specific eGovernment research is also rather neglected[10].

Codagnone and Wimmer (2007) state that overall, eGovernment research at the EU level is visionary but vaguely formulated. As shown in the research topics listed in the results recently reported within the EC-funded eGovRTD2020 project, the EU's focus is on the creation of an inclusive European information society. Recommendations given in the study by DTI and EIPA[11] are considered and transformed in the current eGovernment research programmes funded at the EU level. Thereby, the research focus is on the interface between government and citizens in order to achieve more usability and intuitive handling of public electronic services. Further high priority research topics at the EU level are knowledge management, and spurring innovation in order to achieve the Lisbon targets.

While at the EU level, a clear focus on social aspects can be recognised, national governments' eGovernment priorities spread more widely. Furthermore, results from the eGovRTD2020 study indicate foci on social aspects of national governments' activities similar to the EU foci. One reason for these diverging foci might be the gap between various levels of eGovernment implementation across Europe[12]. Northern and western EU Member States are assessed as being more advanced at implementing eGovernment than southern and eastern countries. In particular, the new EU Member States seem to heavily concentrate on progressing eGovernment implementations[13] in order to catch up with the more advanced countries. As a consequence, the lack of eGovernment research in these areas can be supported by a reasonable argument, while the reason for little or no research in western and northern Member State countries remains unclear. A few Member States have launched focused research initiatives only recently (e.g. Italy, Sweden and UK, with a focus on eParticipation).

[10] Codagnone C. and Wimmer M.A. (2007), Roadmapping eGovernment Research: Visions and Measures towards Innovative Governments in 2020, Results from the EC-funded Project eGovRTD2020.

[11] Millard, J., Warren, R., Leitner, C. & Shahin, J. (2006). EU: Towards the eGovernment Vision for the EU in 2010.

[12] See IDABC's eGovernment observatory. eGovernment facts sheets by country, available at http://ec.europa.eu/idabc/en/chapter/383

[13] See IDABC's eGovernment observatory. eGovernment facts sheets by strategy, available at http://ec.europa.eu/idabc/en/chapter/419

1.2 United States of America (USA)

In the USA, the National Science Foundation (NSF)[14] is the major source of support for eGovernment research in the United States. The National Science Foundation (NSF) is an independent federal agency created by Congress in 1950 "to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defence…" With an annual budget of about $5.91 billion, NSF is the funding source for approximately 20 percent of all federally supported basic research conducted by America's colleges and universities. In many fields such as mathematics, computer science and the social sciences, NSF is the major source of federal backing. Under the term "Digital Government Research" NSF has supported more than 200 investigations since the 1990s.

The focus of digital government research lies at the intersections of computer and information sciences, related social, political, and behavioural sciences, and the problems and missions of government agencies. Digital government research studies the use of information and technology to support and improve public policies and government operations, engage citizens, and provide government services while addressing technical, social, and organisational perspectives.

Multidisciplinary approaches are encouraged and partnerships with government agencies are a required element for most projects. The digital government programme partners with other programmes at NSF (such as Information Technology Research and Digital Libraries programmes) to share funding for proposals that meet the requirements of more than one programme. In addition, some federal agencies, such as the Library of Congress, share in the funding of digital government research that addresses that agency's research needs. NSF funds digital government research that covers a variety of public sector topics including Communication, Digital divide, Education, Government records, libraries, and archives, Government statistics and surveys, international problems and comparative studies, intra and intergovernmental relations, Law and regulation, Natural resources management, Organisational and institutional analysis, Political processes, preparedness and national security, Privacy, Public management and administration, and Service delivery.

The digital government programme at NSF welcomes research that involves many different methods and approaches to information technology, use, and management, including any appropriate combination of frameworks and methods that suit the questions to be studied, such as data sharing and integration, digital libraries and archives, geographic information systems, human computer interaction, information architecture and management. The research programme at NSF sets forth general themes but leaves the focus and the structure of the investigations up to the researchers. Ultimately, the goal is to generate knowledge for both research and practical purposes. Workshop grants help to identify key issues within the domains of government that could benefit from formal research partnerships between universities and government agencies at the national, state, and local levels.

Examples of such workshops include:

- Towards the Digital Government of the 21st Century[15]
- Some Assembly Required: Building a Digital Government for the 21st Century[16]
- Information, Institutions and Governance[17]
- Responding to the Unexpected[18]

[14] http://www.nsf.gov

[15] Schorr, H. & Stolfo, S. J. (2002). Towards the Digital Government of the 21st Century. DG.O 2002. Los Angeles, CA, USA.

[16] Dawes, S. S., Bloniarz, P. A., Kelly, K. L. & Fletcher, P. D. (1999). Some Assembly Required: Building a Digital Government for the 21st Century. NSF Grant 99-181.

[17] Fountain, J. E. (2003). Information, Institutions and Governance: Advancing a Basic Social Science Research Program for Digital Government University of Massachusetts at Amherst - Department of Political Science.

[18] Arens, Y. & Rosenbloom, P. (2002). Responding to the Unexpected. Report of the Workshop Held in New York City, February 27-March 1. New York City.

• It's About Time - Research Challenges In Digital Archiving And Long-Term Preservation[19]

Consequently, digital government research grants cover a variety of public sector topics including communication, digital divide, education, government records, libraries, and archives, government statistics and surveys, international problems and comparative studies, intra- and intergovernmental relations, law and regulation, natural resources management, organisational and institutional analysis, political processes, preparedness and national security, privacy, public management and administration, and service delivery. Thus, much of the digital government research that has emerged from the USA focuses not only on technical perspectives but also a large amount of work has been done learning about the social implications of eGovernment.

Two recent initiatives funded by NSF seek to build a community of international digital government researchers: "Building A Sustainable International Digital Government Research Community", a project carried out by the Centre for Technology in Government, strives to create a framework for creating a sustainable global community of practice among digital government researchers and sponsors. The newly formed Digital Government Society of North America is an organisation of professionals and scholars who share an interest in furthering the development of democratic digital government (DGS, 2007)[20].

2. ICT related research programmes and strategies

Across the continents a similar focus in eGovernment research emerges: *identity management and authentication, interoperability, cyber security, and information management*. The programmes and strategies detailed below address core eGovernment and digital government issues.

2.1 Europe

In the EU the continued focus is creating trust and security by national and international ICT research. Of particular interest are authentication and identification for interaction purposes. Biometrical identification is strongly promoted by governments in order to generate more user acceptance of, and participation in electronic public services. Consequently, EU Member States recognise a need to intensify research in the field of permanent document identity and identifiers. Therefore, identity management within the virtual world becomes more and more important.

Within the EU, regional differences exist, for example, the Baltic States do not have such a strong focus on trust and security, identity management and authentication as other countries have. Future research into these matters and the resulting eGovernment applications will need to take these regional differences into consideration.

As a consequence of the new public management movement, seamless data exchange becomes a central requirement for improved harmonisation and interoperability. Thus, standardisation needs basic infrastructure technologies and domain specific technologies. Especially in respect to the approach of a single access portal, semantic interoperability is required to support avatars and intelligent agents, which will lead users through complicated processes and which will route them to the back-office.

In line with the Lisbon strategy and the i2010 targets, many existing strategies identify accessibility and broadband availability as crucial factors within the public sector. More than ever, "access for all" to government services requires socio-economic research to better understand the needs of certain target groups with different skills and knowledge (e.g. the elderly, immigrants). Making information more accessible via indexing and structuring data e.g. through semantic web or data mining have been identified as important topics to be investigated. Likewise, multi-channel accessibility is at the centre of many strategies, and in

[19] Hedstrom, M., Dawes, S. S., Fleischhauer, C., Gray, J., Lynch, C., McCrary, V., Moore, R., Thibodeau, K. & Waters, D. (2002). It's About Time - Research Challenges In Digital Archiving And Long-Term Preservation.

[20] http://www.dgsociety.org/

particular access through mobile devices is often mentioned in relation to multi-channel access.

2.2 United States of America (USA)

Although NSF funds a majority of the research in the United States, the US Department of Commerce, National Institute of Standards and Technology (NIST)[21] also sponsors digital government research. NIST's Information Technology Laboratory conducts IT-research that contributes to national and industry standards for such topics as computer security, personal identity, digital information access, software development, and networking. Also, research sponsored by the branches of the Armed Forces as well as by the US Department of Defence conduct and support a wide variety of research programmes aimed at improving national defence.

The US Department of Homeland Security (DHS)[22] sponsors technology research focused on the ability to detect and deter attacks on information systems and critical infrastructures. This research programme supports university-based centres of excellence and examines issues related to security systems and to the security-related elements of the Internet, data bases, information systems, and telecommunications networks. One example of an NSF funded initiative that looks at how federal statistics are used in collaborative eGovernment research is Collaborative Research: Quality Graphics for Federal Statistical Summaries (dgQG, 2002)[23]. This effort focuses on developing and assessing quality graphics for federal statistical summaries considering perceptual and cognitive factors in reading, interacting with and interpreting statistical graphs, maps and metadata.

The Federal Government is the largest single producer, collector, consumer, and disseminator of information in the United States. In fiscal year 2006, the Federal Government continued to use industry leading information technology to more effectively manage and deliver government information and services. As a result, Federal programs operate more transparently and effectively. Greater access to government information benefits our country by sustaining an informed citizenry, aiding government decision makers, and supporting our economy - fundamental to a healthy democracy.

The Administration's electronic government (E-Government) promotes increased access to government information, improves services to the citizen with efficient and effective Federal programs, and helps agencies achieve their goals. E-Government helps agencies share information between Federal agencies, States, and local and Tribal governments to monitor the performance and results of Federal programs.

The cost-effective use of information technology to provide consistent access to and dissemination of government information is essential to promote a more citizen-centred government. Agencies manage web-based technologies to help citizens obtain government information and services. In addition, agencies use information technology to communicate with the public and gather feedback to determine whether Federal programs are achieving results and meeting user needs.

To ensure agencies apply E-Government principles and utilise information technology to the fullest potential, agencies measure results to verify progress and planned performance improvement. As a result, agencies better manage their information resources including their investments in information technology. The Office of Management and Budget (OMB)[24] works with agencies to systematically track and measure whether resources used by programs help achieve intended goals through the President's Management Agenda Scorecard each quarter.

[21] www.nist.gov

[22] www.dhs.gov

[23] http://www.geovista.psu.edu/grants/dg-qg/intro.html

[24] www.whitehouse.gov/omb

As described throughout this report, Federal agencies are improving the dissemination of and access to government information for the public. Agency E-Government initiatives described in this report promote greater access to government information and are supported by enduring processes completed by agencies to effectively disseminate government information.

2.2.1 Improving Public Access to Government Information

Government information is information created, collected, processed, disseminated, or disposed of both by or for the Federal Government, and is an agency and public resource which has both value and associated costs. The magnitude of government information and breadth of the Federal Government's program activities requires agencies to strategically manage their information resources. Information resources management is a practice used by agencies to achieve their missions and program goals.

Programs designed to disseminate and provide the public access to government information are fundamental to sound information resources management and essential for agencies to meet their program goals. The Federal Government continues to improve the methods by which government information is disseminated and made available to the public. Use of up-to-date technical methodologies, Federal agency public websites, consultation with the public, and effective Freedom of Information Act (FOIA)[25] operations not only improve access to and dissemination of government information, they help agencies to maximise the usefulness of the information while minimising the costs for the American taxpayer.

2.2.2 Helping the Public Locate Government Information

Federal agency public websites and portals are valuable information dissemination products promoting a more citizen-centred government. These sites provide access to government information and are a means for delivering services to and communicating with the public. Federal agency public websites not only increase access to government information and services, they also allow citizens to participate and become more involved in their government.

OMB's (Office of Management and Budget) Memorandum M-06-02, "Improving Public Access to and Dissemination of Government Information and Using the Federal Enterprise Architecture Data Reference Model," promotes greater access to government information through active dissemination and identifies procedures to organise and categorise information and make it searchable across agencies[26].

Agencies continue to apply this policy in order to improve the public's access to government information. To meet this requirement, agencies updated and published their information resources management strategic plans describing how their information resources activities help accomplish the agency's mission[27]. Agency plans also describe how the respective agency ensures the activities are integrated with organisational planning, budget, procurement, financial management, human resources management and program decisions.

Agencies continue to make progress to assist the public in locating government information by publishing their information directly to the Internet. This procedure makes government information freely available to increasingly sophisticated search engines so the public can quickly search and retrieve requested information. Agencies also communicate directly with the public to understand their needs and obtain feedback about the quality of their Federal agency public websites. Several agencies have used this feedback to redesign their agency's public website and make it a more effective and accessible information dissemination product.

---

[25] www.usdoj.gov/04foia

[26] OMB Memorandum M-06-02 can be found at: http://www.whitehouse.gov/omb/memoranda/fy2006/m06-02.pdf .

[27] E.g. The Defence Department's E-Government Act Report is located at: http://www.dod.mil/cio-nii/docs/DoDFY2006EGovernmentReport.pdf.

2.2.3 The Federal Internet Portal

As the official portal to government information, www.usa.gov provides a centralised location where the public can locate government information and services. Among many other features, USA.gov provides effective search functions, a site index and site maps, a link to agency inventories, schedules and priorities of government information, and active dissemination through up-to-date technologies including Really Simple Syndication (RSS) feeds. USA.gov continues to provide links to Spanish-language government information resources. In 2006, USA.gov's search functions were expanded to include authoritative news and image searches of government information. USA.gov in April 2007 completed an online tutorial of its search functions to complement its services and further aid the public in locating government information[28].

USA.gov and the President's USA Services E-Government Initiative established call centres and created a website of information to support the Department of Veterans Affairs and United States Department of Agriculture's responses to breaches of personally identifiable information[29]. Veterans and other citizens were able to call the centres and access the website to learn more about the breach incidents, who to contact, and the steps to mitigate and prevent future breaches.

USA.gov also sponsors an interagency "web content" working group. The working group regularly conducts training for Federal employees, including tips for agencies for making agency websites more effective and relevant to popular search engines (e.g., Google, MSN and Yahoo). Additionally, a web content working group maintains Webcontent.gov, conducts interagency meetings to assist agencies in managing their websites, and exchanges best practices among other agencies.

2.2.4 Improving Agency Disclosure of Information

The Freedom of Information Act (FOIA), as amended, remains a longstanding means by which the public can access government information. Executive Order 13392, "Improving Agency Disclosure of Information," established a citizen-centred and results-oriented framework for agencies to improve their FOIA operations[30]. The Executive Order required agencies to designate a chief FOIA officer and FOIA public liaison, establish FOIA requester service centres, conduct a review of FOIA operations, and create FOIA improvement plans. These measures are designed to make FOIA operations more results oriented[31].

On June 14, 2006, agencies completed reports summarising their reviews of FOIA operations and provided their agency's FOIA improvement plan[32]. Agencies continue to work with the Department of Justice (DOJ)[33] and OMB (Office of Management and Budget) to successfully implement their FOIA improvement plans, and on October 16, 2006, the Attorney General reported to the President on FOIA implementation including Executive Order 13392[34].

Agencies reported the use of up-to-date information technology and proactive disclosure of information prior to receipt of a FOIA request as two promising practices for improving access to requested records and disseminating information more quickly, resulting in more cost-effective FOIA operations. For example:

---

[28] Completion of the tutorial addresses a requirement of Section 213 of the E-Government Act.

[29] The website can be found at: http://www.firstgov.gov/dataincidents.shtml .

[30] The text of Executive Order 13392 can be found at: http://www.whitehouse.gov/news/releases/2005/12/20051214-4.html .

[31] See Section 1(c) of EO 13392.

[32] A listing of all agency FOIA improvement plans can be found at: http://www.usdoj.gov/oip/agency_improvement.html.

[33] www.usdoj.gov

[34] The Attorney General's Report to the President pursuant to Executive Order 13392 can be found at: http://www.usdoj.gov/oip/ag_report_to_president_13392.pdf .

- The Small Business Administration implemented an information technology application to automate requests, track and locate requested records, and disseminate records to requesters and the public;

- The Department of Labour is developing procedures for identifying and proactively disclosing information; and

- The Department of Defence is redesigning and standardising agency websites to make it easier for the public to access information.

2.2.5 Financial Accountability and Transparency

On September 26, 2006, the President signed the Federal Funding Accountability and Transparency Act of 2006, Pub. L. No. 109-282, to improve the quality and accessibility of information about Federal spending[35]. The Act requires OMB (Office of Management and Budget) to oversee development of a website through which the public can readily access information about grants and contracts provided by Federal government agencies[36]. Development of this website will complement other websites currently providing the public Federal program performance information (e.g., www.USA.gov, www.Results.gov and www.ExpectMore.gov).

The Federal government currently has some information on Federal expenditures available through various databases and reports, including the Federal Procurement Data System, the Federal Assistance Awards Data System, and the Consolidated Federal Funds Report system. OMB is working with agencies through an interagency task force to ensure the milestones for developing and maintaining the site are achieved in accordance with plans and statute.

2.2.6 Organisations Complementing Federal Agency Information Dissemination Programs

Agencies take advantage of many channels to effectively disseminate their information to the public, including Federal and non-federal governments, libraries and the private sector[37]. By taking advantage of the skills and resources of these entities, agencies provide the public with multiple sources for accessing information and manage their information resources in a more cost-effective manner. In addition, agency partnerships with other dissemination entities increase public access to government information through the increased availability of information technology products and services.

There are many dissemination channels available for agencies including popular commercial search engines (e.g., MSN, Google, and Yahoo search engine services), USA.gov, and many others[38]. Community technology centres, public libraries, research rooms at the National Archives and Records Administration (NARA)[39], and Federal Depository Libraries managed by the Government Printing Office increase public access to government information through complementing existing agency dissemination programs. The information technology

[35] The text of the Federal Funding Accountability and Transparency Act can be found at: http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=109_cong_public_laws&docid=f:publ282.109.pdf.

[36] More information on the development of this website can be found at: http://www.federalspending.gov .

[37] This section includes information on compliance with Section 213 of the E-Government Act.

[38] To learn more about organizations complementing Federal information dissemination, see: OMB's April 15, 2005 report, "Organizations Complementing Federal Agency Information Dissemination Programs." The report can be found at: http://www.whitehouse.gov/omb/inforeg/section_213_report_04-2005.pdf .

[39] www.archives.gov

resources of these organisations combined with the assistance of organisation staff and volunteers provide increased access to government information.

Agencies are establishing innovative partnerships with non-profit and private sector dissemination entities to improve access to and dissemination of government information. For example:

- NARA recently announced an agreement with iArchives (see: www.iarchives.com) to digitise and provide access to selected records;

- The National Aeronautics and Space Administration (NASA)[40] is in discussion with several private organisations to digitise and make available to the public their information holdings; and

- The Centres for Medicaid and Medicare Services[41], a part of the Department of Health and Human Services, partnered with Walgreen's and public libraries to produce, distribute and help the public understand information about the Medicare Prescription Drug Card.

OMB continues to encourage strategic partnerships, including those mentioned above, to support the principles of E-Government by maximising the usefulness of government information while minimising the cost to agencies and the public.

2.2.7 Public Access to Electronic Federal Records

The Federal Government is creating and collecting information faster today than ever before. As a result, agencies are working to capture enormous quantities of records and ensure they are accessible for future use by agencies and the public. Effective management of government records ensures adequate documentation of the policies and transactions of the Federal Government, allows the Federal Government to review and improve its programs, and helps the public obtain information about Federal programs and activities. To achieve these benefits, agencies systematically manage all their records regardless of form and medium (e.g., paper and electronic form) throughout the information life cycle.

To promote more effective records management, NARA issued "Guidance for Implementing Section 207(e) of the E-Government Act of 2002."[42] NARA's guidance highlights agency responsibilities to identify and schedule their electronic records and to transfer to NARA electronic records requiring permanent retention. Agency responsibilities for identifying and scheduling electronic records can be separated into two categories: developing records schedules for all records in existing electronic information systems and establishing procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving new electronic information systems or enhancements to existing systems. Additionally, OMB requires agencies to document and verify whether records produced by each major information technology investment are appropriately scheduled with NARA's approval as part of their capital planning and investment control[43].

In their 2006 E-Government Act Reports, agencies were instructed to describe how they were fulfilling their responsibilities under Section 207(e) using NARA's guidance. All 24 Chief Financial Officer Act agencies are working to implement NARA's guidance and many agencies are actively engaged with NARA to prioritise existing systems and schedule records.

---

[40] www.nasa.gov

[41] http://www.cms.hhs.gov/

[42] NARA's Guidance for Implementing Section 207(e) of the E-Government Act of 2002," can be found at: http://www.archives.gov/records-mgmt/bulletins/2006/2006-02.html.

[43] OMB Circular A-11, Section 300 can be found at: http://www.whitehouse.gov/omb/circulars/a11/current_year/s300.pdf.

OMB and NARA continue to work with agencies fulfilling their responsibilities under Section 207(e) using NARA's December 2005 guidance and other applicable records management policies. In addition, NARA will sponsor a forum in 2007 to highlight the importance of a collaborative relationship between an agency Chief Information Officer (CIO) and the agency's Records Officers. In addition, agencies are using guidance documents to help them comply with other existing records management responsibilities highlighted by NARA's December 2005 guidance. For example, agencies are using the Records Management Profile, included in the Federal Enterprise Architecture, to incorporate statutory records management requirements and sound records management principles into agency work processes and information systems[44].

2.2.8 Access to Federally Funded Research and Development

Dissemination of and access to information about federally funded research and development (R&D) stimulates the exchange of new scientific information and technologies, and provides opportunities for understanding and applying knowledge towards the production of useful materials[45]. Federal agency R&D activities are an essential component of many agency missions resulting in a broad variety of federally funded R&D. Many Federal agency public websites disseminate and provide access to Federal R&D information, and as a result, agencies can better:

- coordinate Federal R&D activities;
- collaborate among those agencies conducting R&D;
- transfer technology among Federal agencies and the public; and
- access information about R&D activities.

As reported in previous U.S. E-Government Act reports, the Federal Government currently funds two primary research and development information repositories: RaDiUS[46] and Science.gov[47]. RaDiUS provides the public and agencies with information about federally funded R&D activities. Science.gov provides links to science websites and scientific databases so citizens can access the results of Federal research.

Most Federal agencies are supplying information or are otherwise represented in RaDiUS. In addition, more than 12 Federal agencies contribute to Science.gov. Some agencies, such as NASA, provide greater access to R&D information by directly linking their R&D databases to Science.gov.

Agencies reported on their use of RaDiUS and Science.gov as part of this year's annual agency E-Government Act reports. Several agencies link individual agency sources of R&D information to the Government-wide repositories.

To increase public access to R&D information, agencies disseminate information through multiple channels, including public libraries and their own Federal agency public website. Other examples include:

- The Department of Commerce's National Oceanic and Atmospheric Administration disseminates R&D information from satellite imagery at: http://www.orbit.nesdis.noaa.gov;

[44] The Federal Enterprise Architecture (FEA) Records Management Profile, version 1.0 can be found at: http://www.archives.gov/records-mgmt/policy/rm-profile.html .

[45] This section includes information on compliance with Section 207 of the E-Government Act.

[46] https://radius.rand.org

[47] www.science.gov

- The Department of Defence's Research and Engineering component operates a centralised public web portal for public access to R&D information at: https://rdte.osd.mil ;

- The Department of Education disseminates R&D information, including the results of research and statistics at: http://www.ed.gov/rschstat/landing.jhtml ;

- The Department of Energy's Project Summary Database is a searchable database of ongoing R&D projects at: http://www.osti.gov/fedrnd/ ;

- The Environmental Protection Agency's Science Inventory is a searchable, agency-wide catalogue of more than 900 science activities at: http://www.epa.gov/si ;

- The National Aeronautics and Space Administration's Technical Report Server disseminates R&D information about current and historical technical literature at: http://ntrs.nasa.gov/search.jsp ;

- The Nuclear Regulatory Commission disseminates the results of R&D reports at: http://www.nrc.gov/reading-rm/doc-collections/nuregs/ ;

- The National Science Foundation provides information on R&D awards at: http://www.nsf.gov/awardsearch/ ; and

- The Small Business Administration's TECH-Net website disseminates technical information about and for small businesses at: http://tech-net.sba.gov/index.cfm .

3. Comparing eGovernment research in the U.S. and Europe

The following table provides an overview of how eGovernment research is funded by governmental institutions in the EU and the U.S. When comparing the EU and U.S. in terms of their research initiatives in eGovernment, one also has to bear in mind that the EU consists of a Federation of independent Member States, while the U.S. have a different structure of federation. The following table presents the main indicators for eGovernment research funding and compares funding practices in the EU and the U.S.

Starting with the comparison of the major source of support for eGovernment research, Table 1 shows that in the USA the major source of research funding is at the federal level, from the USA's National Science Foundation (NSF). A similar situation characterises Europe, where the overwhelming majority of research funding comes from European Commission (EC), which with some freedom and optimism can be considered as the 'federal' centres for its 27 Member States. However, the U.S. have additional sources of eGovernment research funding from other federal agencies, eGovernment initiatives by State governments, and some industry support. In the EU, pure research funding is mainly provided by the European Commission.

Table 1 EU/US research Funding

Criterion of comparison	EU	USA
Major source of support	European Commission Community Research & Development Information Service (CORDIS)	The US National Science Foundation (NSF)
Project participants (related to major source of support)	Ministries, Universities, Research centres Private consulting companies Special agencies	University-based researchers Non-profit professional associations
Additional sources of support	Pure eGovernment research is mainly funded at the EU level National governments fund mainly implementation projects	Federal agencies
Conditions of success for projects	Meet programme thematic priorities Different types of organisations International Consortium of EU Member States	Multidisciplinary approaches Partnerships with government agencies (theory and practice)
Funded projects range in size from	Total of € 3 625 million for funding Information Society Technologies over the duration of FP6	Less than € 14 840 to large projects that exceed € 1 400 000
Length of funding	A year to 4-5 years	A few months to up to 5 years
Characteristic of research agenda	Directive, i.e. it does specify thematic priorities, and outcomes	Not directive, i.e. it does not specify questions, methods, or outcomes

Source: eGovRTD2020

Taking into account the high-level strategic objectives defined by the EU in its own key eGovernment implementation priorities, its Member States are mostly focusing on implementing existing ICT-solutions and applications to eGovernment implementation projects or programmes. In most cases, no research aspects are involved in these implementation projects as most countries in the EU do not have specific programmes for eGovernment related research. Consequently, if no focused eGovernment research is funded at the EC level, there could be a substantial lack of eGovernment research in the EU for the next half decade.

Table 1 also depicts the requirements research projects have to meet in order to get funded in the different regions. In the EU, research projects have to meet the thematic priorities of the programme they are applying for. Also, an international project consortium is mandatory for EU-level funding, consisting of partners from at least two different EU Member States, as well as from different typologies of organisations (academia, industry, public sector). By comparison, the USA requires a multidisciplinary approach and the cooperation and collaboration of theory and practice, i.e. partnerships between government agencies and university-based researchers, which has also been an implicit requirement in EC-funded projects for several framework programmes.

In the USA many federal agencies fund eGovernment research because they have identified a number of specific issues to be addressed. By contrast, a possible interpretation of the lack of eGovernment research funding by national governments in the EU could be that many Member State governments have neither a definition nor a vision of eGovernment, and no

strategic plan to transform traditional government into eGovernment. This point may benefit from further considerations.

The U.S. fund eGovernment research across multiple disciplines. On the contrary, most eGovernment research projects at the EU-level focus on ICT, and national level eGovernment funding mainly gives emphasis to the implementation of ICT in the public sector, without any core research. However, recently, this has started to change in European Member States such as Germany, Italy, Sweden, and UK.

The EU and U.S. are also different from each other in terms of the length of time their research projects are funded. EU research projects in general are funded for a longer time than those funded in the U.S. In particular, much of the funding in the U.S. is through the National Science Foundation (NSF). Through NSF, some projects are funded for as little as a few months, while other projects are funded for a couple of years. Two funding streams that yield shorter-term initiatives are the Small Grants for Exploratory Research (SGER)[48] and Workshop Grants. SGER grants, usually smaller in amount as well as shorter in length, are often pursued to explore an idea that may result in the development of a larger study and proposal. These funds are available for studies that investigate transformative research ideas; or application of new expertise or studies that may catalyse rapid and innovative advances.

NSF's Workshop grants help identify key issues within the domains of government that could benefit from formal research partnerships between universities and government agencies at the national, state, and local levels. Because NSF funds such a large portion of eGovernment research in the USA, many long term research initiatives have emerged from discussions at NSF funded workshops.

Furthermore, the NSF scheme provides funding for new projects on an annual basis, there is no Framework Programme such as FP6 and FP7 in the EU. In the USA, the NSF presents broad funding themes for digital government under their Computer & Information Science and Engineering programme but does not set forth direct questions or methods. Each year the focus shifts to address emerging topic areas. Thus, in the USA, research is solicited under broad theme areas but questions, methods and outcomes are left to the research teams.

4. eAuthentication

The eAuthentication was defined as "*the Web Based service that provides authentication to end users accessing (logging into) an Internet service*". E-Authentication is setting the standards for the identity proofing of individuals and businesses, based on risk of online services used. The eAuthentication is similar to Credit Card verification for eCommerce web sites. The verification is done by a dedicated service that receives the input and returns success or failure indications.

Public trust in the security of information exchanged over the Internet plays a vital role in the E-Gov transformation. E-Authentication makes that trust possible.

eAuthentication worldwide initiatives focus on meeting the authentication business needs of the E-Gov initiatives, building the necessary infrastructure to support common, unified processes and systems for government-wide use. This will help build the trust that must be an inherent part of every online exchange between citizens and the Government.

4.1 eAuthentication in the EU

In computer security, authentication is the process by which a computer, computer program, or another user attempts to confirm that the computer, computer program, or user from whom the second party has received some communication is, or is not, the claimed first party. A

[48] www.nsf.gov/od/lpa/news/publicat/nsf0203/cross/ocpa.html

blind credential, in contrast, does not establish identity at all, but only a narrow right or status of the user or program[49].

In the EU, high priority is given to research actions that focus on security and flexibility of large, complex, open and interrelated infrastructures[50], as well as on methods for mapping and modelling the infrastructure underlying processes. This is related to secure platforms[51], networks and software ensuring interoperability and competition, and cryptographic techniques. Furthermore, methods for network security inspections, forensics and tracings have to develop, above all new methods for acquisition of highly charged data with tools not based on the operating system. Especially attention in regard to eSecurity is given to research of identification and authentication[52] matters with focus on biometrics[53].

Besides, research activities also concentrating on guaranteeing reliability and security of software-intensive systems. Furthermore, innovative identity management[54] systems shall empower the user and include technologies that authorise users to handle their identification themselves or choose to leave it to the service provider. For identity management across heterogeneous systems, authentication and some minimum standards are essential. Legal, technical and organisational barriers must be identified before the electronic identity is applicable. Besides, security industry should switch emphasis from “managing ownership for users” to “empowering users” to manage their own data.

The strategy of a secure information strategy published in the i2010 strategy for the Information Society requires improvements of eSecurity, particularly for the Internet[55]. Therefore, research shall address risk management, identity management and privacy enhancing, certification and standardisation, regulation and general policy strategies, authentication, trusted computing, network security, as well as technologies to support law enforcement activities[56].

Much of the literature on IDM (ID Management) describes authentication from a fairly narrow viewpoint, of confirming a person’s identity with respect to some set of electronic credentials, typically password or PKI certificate, obtained by formal registration with a registration authority, in order to gain access to an IT system. In GUIDE authentication (including just identification) is defined more generally as the process of confirming the identity of an individual entity, by whatever means necessary to establish the validity of the claimed identity, according to a given level of trust or assurance, either implicit or explicit, in a given context.

This definition leaves it open as to what method and what data is used in the process, or indeed whether or not it is an automated electronic process or a manual process. Some examples are:

---

[49] http://en.wikipedia.org/wiki/Authentication

[50] Dachs, Bernhard; Georg Zahradnik (2005), R&D Priorities of Europe’s leading Public Research Organisations in the Field of ICT, in: Challenges and opportunities for IST research in Europe. http://fistera.jrc.es/pages/books/content%20Challenges%20book/challenges%20book.htm

[51] Esterle, Alain (2005), ICTsecurity stakes and identity management, in: IST at the service of a changing Europe by 2020: Learning from world views. FISTERA final conference. http://fistera.jrc.es/pages/books/content%20FFC%20book/ffc%20book.htm

[52] European Commission (2004): Working paper on eGovernment beyond 2005. An overview of policy issues. http://europa.eu.int/information_society/activities/egovernment_research/doc/working_paper_beyond_2005.pdf

[53] European Commission (2006): International High Level Research Seminar on “TRUST IN THE NET”, Vienna, Austria, 9 February 2006. Main Recommendations.

[54] Mahroum, Sami; Bernhard Dachs, Matthias Weber (2005), The European Dimension of Foresight and the Priority Setting in IST, in: Challenges and opportunities for IST research in Europe. http://fistera.jrc.es/pages/books/content%20Challenges%20book/challenges%20book.htm

[55] Paltridge, Sam; Sheridan Roberts, Brigitte van Beuzekom (2005): Scoping study for the measurement of trust in the online environment. OECD. http://www.oecd.org/dataoecd/26/15/35792806.pdf

[56] European Commission (2006): International High Level Research Seminar on “TRUST IN THE NET”, Vienna, Austria, 9 February 2006. Main Recommendations.

- Checking the age of a young person for the purchase of alcohol, where a visual check of an identity card may be sufficient.

- Accessing an informational web site, where a name attribute may be sufficient.

- Accessing ones tax records on-line, where a PKI certificate may be necessary.

Each has different levels of risk attached, but commensurate with the application context in question. The more severe the likely consequences are, the more confidence in a claimed identity will be required to engage in a transaction.

Guide is concerned with the following main classifications of authentication mechanism[57]:

- **Identification** – (or Knowledge based authentication) involving knowledge of one or more identity attributes, not necessarily secret. The attributes involved can be unique identifiers for the individual in some context. E.g. a National Identity number, a passport number, social security number, etc.

- **Credential Based Authentication** – (or Shared Secret), typically involving username/password or certificate/PIN pairs, or shared secrets like 'favourite film'.

- **Biometric Based Authentication** – Verification of a person's physical biometrics

- **Token Based Authentication** – a special case involving a hardware token (smart card or SecureID) containing any of the above identity data.

A range of different levels of 'strength of authentication' are achieved both within each type (e.g. certificate is stronger than password) and by using different types in combination, often called n-factor authentication. For example 3-factor authentication is also commonly described as:

Something an individual **has** – A hardware token
Something an individual **knows** – A PIN number
Something an individual **is** – A biometric

4.2 U.S.A.: E-Authentication Initiative Launches the E-Authentication Federation

The E-Authentication Initiative has successfully launched the E-Authentication Federation[58], a public-private partnership that will enable citizens, businesses and government employees to access online government services using log-in IDs issued by trusted third-parties, both within and outside the government. As this ground-breaking collaboration between government and industry continues to mature, it will further improve U.S. government's ability to deliver services to the American public and save taxpayer dollars.

As of September 7, 2006, 17 Federal agencies have joined the E-Authentication Federation as Relying Party members, signalling their intent to make select systems available through the use of trusted third party log-in IDs. Of the 17 agencies that have joined the Federation, 14 have already launched E-Authentication-enabled online services.

The Federation also includes six Credential Service Provider members, which issue, manage and verify the login IDs upon which the online services rely to admit end users to their sites. Federation member Credential Service Providers consist of both government agencies and commercial entities, including financial services companies. Financial services companies are able to participate in the Federation under the authority of the Department of Treasury[59],

[57] Guide D 1.2.1.B
[58] http://www.cio.gov/eauthentication/

[59] www.ustreas.gov

which is able to authorise certain companies as designated financial agents (DFA) of the government.

The E-Authentication Federation is growing rapidly, and over the course of the next year, the E-Authentication Initiative expects to add several high-volume online services and Credential Service Providers that will greatly increase E-Authentication's value to Federal agencies and the American public.

The E-Authentication Federation achieved significant growth with the addition of 15 new relying party systems. This expansion more than doubles the total of operational relying parties in the Federation, bringing that number to 31 systems. The newest members of the Federation include the Department of Health and Human Services National Select Agent Registry[60]; U.S. Department of Agriculture HSPD-12 Maps[61] (Appendix I); Department of Transportation COMPASS[62]; Department of Justice E-Trace[63], and Small Business Administration Global Login System[64], which provides E-Authentication-enabled login service to 12 distinct SBA applications.

The Office of Management and Budget has directed agencies to reduce their contributions to the E-Authentication initiative by half for fiscal 2007, signalling another change in direction for a project many believed was the key to making e-government less about consolidating Web sites and more about transactions. Last year, the General Services Administration[65], which runs E-Authentication, collected about $10.5 million to run the program office. For 2007, OMB told agencies to contribute less for two main reasons: Because of Homeland Security Presidential Directive-12 (Appendix II), the administration no longer considers E-Authentication as necessary for internal agency applications as it once did, and officials want to move it to a fee-for-service model by 2008.

HSPD-12 requires agencies to issue smart identification cards to employees and contractors. Each card includes a digital certificate, which could be used for physical and logical access. Agencies are spending millions of dollars setting up the infrastructure to handle HSPD-12 cards. This is the second refocusing of E-Authentication. In 2003, OMB abandoned the idea of a centralised gateway and went with a federated approach. Since March 2006, the number of e-authentication transactions has increased from less than 2,000 per month to more than 18,000 per month[66].

Along with the E-Authentication funding directive, OMB also detailed some other changes to e-government and the Lines of Business Consolidation efforts. OMB has yet to name the Security LOB shared-services providers, but likely will decide on the six agencies that submitted business cases when the president's 2008 budget request comes out in early February. The six agencies that want to be shared-services providers are the departments of Homeland Security and Justice, Treasury's Bureau of Public Debt, the Agency for International Development, the Environmental Protection Agency and the Office of Personnel Management.

The General Services Administration estimates that agencies have about 600 applications that would benefit from E-Authentication services. Right now, about 14 do. So GSA and the government have a long way to go before they fully enjoy the benefits of a single-sign-on environment. Officials from GSA and the Office of Management and Budget are working with agencies to figure out how and in what order the other 586 applications will start using Security Assertion Management Language or a digital certificate[67].

---

[60] www.hhs.gov

[61] www.usda.gov

[62] http://www.mrutc.org/compass/index.htm

[63] www.usdoj.gov

[64] www.sba.gov

[65] www.gsa.gov

[66] http://www.gcn.com/print/26_01/42893-1.html

[67] http://www.gcn.com/print/25_28/42001-1.html

4.3 Public Key Infrastructure (PKI)

Public-key infrastructure is a complex technology that is a burden for agencies to implement. PKI is a powerful authentication technology that can enable a wide array of agency applications and services. By anticipating PKI and implementing the technology properly, an agency can create the foundation for many useful applications.

With PKI, a third-party entity vouches for the bona fides of two interacting parties. Those parties might be a bank and its card-carrying customer, or an agency and its smart card-carrying employee. The vouching is in the form of digital certificates — actually large numbers — issued by a certificate authority to the trusted parties.

Although PKI certificates from different vendors are generally equivalent, agencies have many options to consider before choosing a provider. Agencies might be looking for a supplier of smart cards. They may need hardware, such as card readers, or software, such as personnel tracking systems, to work with PKI.

Consulting services can help integrate PKI with existing systems. Indeed, combinations of consultants with different expertise could be necessary to implement different agency applications and services. Technical support and maintenance services are always important considerations.

Because PKI is associated with secure and possibly vital agency applications, it's important to determine the disaster-recovery features that different vendors offer. Bullet-proof PKI applications are not going to help you if the certificate authority goes down. Agencies might also prefer vendors that are geographically close to you or, alternatively, far away from you. The former might be a benefit if you need assistance. The latter might help ensure survivability if there's a regional disaster.

"Management has to organise itself and lead," said Dr. Peter Alterman, assistant chief information officer for electronic authentication at the National Institutes of Health. Alterman is chairman of the Organisation for the Advancement of Structured Information Standards' Federal PKI Policy Authority and a member of the OASIS IDtrust Steering Committee. As with any new implementation, there will be resistance to change[68]. In addition, although a PKI digital certificate might just be numbers, the infrastructure itself — hardware, software, services — is not cheap. "The actual PKI technology is trivial compared to the budget and management issues," Alterman said.

An agency also needs to decide who will be administering the PKI system — the agency itself or an outside entity. "IT needs to ask whether they really want to take on the physical security responsibility," Alterman said. This could involve coordinating information technology, human resources and building security to a greater extent than usual. The trade-off is better security for greater responsibility. Shifting responsibility for physical security to another entity could simplify management — or not — but might also affect overall security.

4.3.1 PKI possibilities

Vijay Takanti vice president of security services at Exostar said recently that "PKI is like an electrical outlet. Once you have it, you can plug all kinds of apps into it."

In the U.S. there are many state and local agencies that federal agencies have to work with on an ongoing basis or in an emergency situation. The Homeland Security Department[69] might partner with state and local law enforcement; federal health agencies could exchange information with hospitals or public health authorities; money might flow between federal, state and local agencies. It would be convenient to be able to identify trusted people,

[68] http://www.gcn.com/print/26_12/44367-1.html

[69] www.dhs.gov

exchange confidential information and allow secure transactions. Unfortunately, state and local agencies can't use shared-service providers. So even though these groups have to work together, they can't use the same PKI system.

However, they can still use PKI to solve their problems. Providers such as CertiPath[70] offer bridge services for just this purpose. CertiPath, jointly owned by ARINC[71], Exostar[72] and SITA[73], cross-certifies entities to a common standard, while CertiPath is directly cross-certified with the Federal Bridge Certificate Authority[74].

Interagency cooperation is just one bonus of PKI technology. "Agencies need to consider making changes to their ways of doing business," Alterman said. In particular, agencies need to think about ways to re-engineer their business processes to take advantage of PKI. Prime candidates for PKI include:

- Interagency communication and cooperation.
- Risk-associated activities, such as identity cards.
- Confidentiality and privacy concerns.
- Financial transactions.

PKI's potential in securing e-mail is one use agencies find attractive. The Defence Department[75] and the United Kingdom's Ministry of Defence[76] already have such systems. PKI certificates encrypt e-mail on the sending end and decrypt it on the receiving end. The process is transparent to users and makes for a new level of secure communications.

Encryption is an obvious application of PKI, but not enough agencies appreciate what PKI-encrypted files can accomplish. An encrypted file is not only unreadable by outsiders but also essentially stamped as belonging to your agency. Establishing such ownership credentials is valuable.

Digitally signing a file is similar but doesn't involve encryption. A digitally signed file ensures that its ownership is incontestable. The file is also tamper-resistant: People can read it but not alter it. This is very important for agencies that need to circulate agreements or other documents they don't want marred by deliberate or inadvertent changes.

As these examples show, agencies need to approach PKI applications as a two-step process. First, they must identify the PKI-based applications that interest them. Then they need to figure out the integration implications for each of these applications.

It's possible, for example that the agency applications of interest only run on a particular operating system. The agency must ensure that the corresponding PKI software will run on the same operating system. Most PKI providers support Windows and other operating systems, including Novell NetWare, Linux and Mac OS. Some operating systems support PKI themselves.

Finally, because each agency probably has its own PKI solution provider, interoperability between providers is important. This is simplest if the providers use non-proprietary technology. Some engineering of the infrastructure may be required for applications and PKI to interoperate well.

---

[70] www.certipath.com

[71] www.arinc.com

[72] www.exostar.com

[73] www.sita.aero

[74] www.cio.gov/fbca

[75] http://www.defenselink.mil/

[76] www.mod.uk

4.3.2 PKI in EU

A recent report from the European Commission reveals that, although eSignatures are now legally recognised in all Member States, their take-up is still too slow – particularly with regard to cross-border interoperability. The Commission's report on the operation of its 1999 Directive on a Community framework for electronic signatures reveals that all 25 Member States have now transposed EU eSignature rules into their national legislation. Despite this, the adoption and use of electronic signatures is still far too low and is hindering the potential growth of trade in goods and services via the internet. In particular, the market for "qualified" (with sophisticated technical protection) eSignatures has been much slower to take off than expected.

"A reliable system of electronic signatures that works across intra-EU borders is vital to safe electronic commerce and the efficient electronic delivery of public services to businesses and citizens," noted Information Society and Media Commissioner Viviane Reding. "Much work still needs to be done, in particular to make signatures work across borders."

It is expected, however, that the public sector will play a key role in driving future demand. A number of applications in the pipeline, including the use of electronic ID cards and eSignatures to provide on-line access to public services, should lead the way to wider adoption. Development of eSignature applications could also be stimulated by the demand created by electronic public procurement systems and ID management, as will be stressed in the Commission's eGovernment Action Plan, to be adopted soon.

The Commission will continue to encourage the development of eSignature services and applications and to monitor market and technological developments over the coming year. More specifically, it will support further standardisation work aimed at interoperability of different eSignature technologies, within and across borders. It will also prepare a report examining whether further regulatory measures may be needed to promote wider use[77].

Recently, a UniCERT public key infrastructure (PKI) certification solution from Cybertrust[78] has been selected to ensure the secure transfer of information between European local governments and external sources, as part of the EU's Interoperable Delivery of European eGovernment Services to Public Administrations, Businesses and Citizens (IDABC) programme[79].

Following an EU tender, Postecom[80], a subsidiary of the Italian Post Office, was awarded the contract for the provision of certification services to the IDABC programme – in particular certification authority services, and services relating to the continuation and improvement of the IDA public key infrastructure, which today delivers various certification services (based on X509 certificates) mostly to closed user groups and applications.

Postecom has recently announced its decision to use UniCERT, the Cybertrust PKI software that issues digital certificates compliant with the European Directive 1999/93/CE, to deliver the PKI certification platform.

PKI digital certification secures applications, communications and transactions, allowing for privacy, integrity and authenticity of the document and of the author's identity. "Cybertrust's involvement in this important eGovernment project will allow Postecom to develop a high-quality, innovative PKI system that will secure data and increase efficiency in local government communications," explained Roberto Palumbo, Postecom business unit manager[81].

[77] http://europa.eu.int/idabc/en/document/5436/194

[78] www.cybertrust.com/solutions/identity_management/digital_certificates

[79] http://ec.europa.eu/idabc/en/document/5838/194

[80] http://www.postecom.it/

[81] http://www.cbronline.com/article_news.asp?guid=99B213F3-6BA7-4BF0-8C99-F4E73CB6F450

4.3.3 PKI use at U.S. DOD (Department Of Defence)

In a sweeping move to improve computer security, the military in the U.S. required all personnel to use public-key infrastructure (PKI) technologies to log on to the Non-secure IP Router Network (NIPRNET)[82], the military's unclassified network. The Joint Task Force for Global Network Operations (JTF-GNO)[83], the organisation that oversees the operation and protection of military networks, issued guidance to military services and agencies on configuring systems and providing training for the PKI implementation. The initiative requires the use of Common Access Cards, digital signatures, e-mail encryption, and Web server soft certificates for desktop and notebook computers and servers that connect to NIPRNET, according to the JTF-GNO Communications Tasking Order 06-02, Tasks for Phase 1 of the Accelerated PKI Implementation.

JTF-GNO's guidelines include target dates for implementing PKI and instructions on the use of passwords for those computers and servers that do not make the deadline. They also require significant awareness and system configuration training for all DOD systems administrators. "Compliance with this [task order] will enhance the security of DOD information systems and establish deadlines for training, verification, installation and progress reporting," said Tim Madden, a spokesman for JTF-GNO[84].

In response to the order, the Army started implementing PKI in January 2006 and plans to have 10,000 workers at Army headquarters using it. Spyware or keystroke-tracking software can steal user names, passwords and personal identification numbers, but they cannot steal Common Access Cards that use electronic information and digital PKI certificates to verify users' identities, said Lt. Gen. Steven Boutelle, the Army's chief information officer, in a January 25, 2006 Army statement. "One of the greatest vulnerabilities of our networks is posed by weak user names and passwords," Boutelle said. The Army has borne the brunt of the attacks.

TKC Integration Services (TKCIS)[85] won a contract in 2005 worth more than $1 million to oversee the installation of PKI throughout the Army. The Alaska Native Corporation[86] chose Tumbleweed Communications' Tumbleweed Validation Authority[87] product to verify whether a user's PKI digital certificate is valid, said Joel Lipkin, senior vice president of TKCIS' General Services Administration and Systems Integration Division[88].

Later on last year (2006), the Air Force, Army and Navy have successfully implemented the initial public-key infrastructure technology mandated by the Defence Information Systems Agency, and required under Homeland Security Presidential Directive-12 (Appendix I). But officials report that the process has not been trouble-free nor are the challenges over.

Navy officials said that virtually all of its personnel now log on to networks using the Common Access Card and a personal identification number, while Air Force officials report usage of "at

---

[82] http://www.disa.mil/main/prodsol/data.html

[83] http://www.jtfgno.mil/

[84] http://www.fcw.com/article92280-02-13-06-Print

[85] www.tkcis.com

[86] www.alaskans.com/alaskanative

[87] www.tumbleweed.com

[88] http://www.fcw.com/article92280-02-13-06-Print

least 95 percent." The Army, meanwhile, said more than 80 percent of its personnel now can log on to its unclassified network using a CAC and personal identification number.

Air Force Lt. Gen. Charles Croom, director of the Defence Information Systems Agency, set a July 31 2006 deadline for full PKI implementation for user authentication, digital signatures and encryption on all of its desktop and notebook PCs, and servers. DOD has struggled to implement PKI for years because the services did not have the infrastructure to manage the public keys[89].

Before Croom's memo, DOD issued Defence Directive 8500, requiring that e-mail be digitally signed and that online applications and networks use encryption certificates for user authentication. The services never fully met Directive 8500, in part because they had few applications that accepted PKI certificates.

But through the wider use of the CAC, that infrastructure slowly is being put into place to make it easier to use digital certificates. Army CIO Lt. Gen. Stephen Boutelle said he was the first in the Army to get a Common Access Card. Thereafter, the program was expanded to his G/6 staff and the Army staff as a whole. "We all had to learn how to get on with dial-up, Cisco [virtual private network], Citrix, DSL and wireless cards," he said. "There are nuances to each." The transition has not been painless. Some personnel were upset that others could not read their encrypted e-mail. "People have learned that security is not necessarily convenient," Boutelle said. "Once they understood we were serious, they realised they had to remember their PIN and bring their card to work." (Government Computer News, 14/08/06).

4.4 US Federal E-Authentication and Higher Education

The United States federal government has been working on an E-Authentication project[90] actively since 2003 in response to the E-Government Act of 2002[91]. Movement has been slow, but there are many federal agencies[92] now leveraging this infrastructure in a federated manner. For more details about the initiative, there is the publicly available Burton Group Report on the Federal E-Authentication Initiative[93]. Since then, there has been work to bridge both Liberty Alliance[94] and Shibboleth-based federations[95] with the e-Government services. Involvement also extends to the Post Secondary Electronic Standards Council (PESC)[96] who is working with all these organisations to assure higher education is appropriately represented. Certainly NSF Fastlane[97] and Federal Student Aid (FAFSA)[98] seem like the most obvious first candidates to work with higher education institutions.

With all the activity surrounding the federal government deploying these services in a federated method, institutions should definitely be getting their internal infrastructure in place to support and interoperate with one of the major federations (InCommon, eGovernment, etc).

[89] http://www.gcn.com/print/25_24/41654-1.html

[90] http://www.cio.gov/eauthentication/

[91] http://www.whitehouse.gov/omb/egov/g-4-act.html

[92] http://www.cio.gov/eauthentication/documents/FederationMemberList.pdf

[93] http://www.cio.gov/eauthentication/documents/BurtonGroupEAreport.pdf

[94] http://www.projectliberty.org/index.php/liberty/strategic_initiatives/egovernment

[95] https://spaces.internet2.edu/display/SHIB/EAuthenticationDeployment

[96] http://www.pesc.org/events/links.asp

[97] https://www.fastlane.nsf.gov/jsp/homepage/proposals.jsp

[98] http://www.ed.gov/about/offices/list/fsa/index.html

4.5 The future of authentication

4.5.1 Organic photonics

Nanoident Technologies[99] specialises in printable organic semiconductors that can produce thin, flexible, inexpensive and integrated circuit devices in large formats. The company recently announced the launch of a new biometrics division and the introduction of a Photonic Solutions Platform. Conductive organic materials could make the technology small enough and inexpensive enough so that biometrics could be integrated into small devices such as handhelds and smart cards. The printable circuits are built up in layers using ink-jet printers and are not limited to wafer size, as traditional silicon chips are. The new biometric platform incorporates photo emitters and detectors with read-outs for authentication. Nanoident's first biometric offering will be an optical fingerprint detector.

But, Klaus Schroeter CEO of the Austrian company Nanoident Technologies AG said that "fingerprints alone are not a very secure method…we have developed a new multimodal biometric centre, that detects underlying tissue structures as well. It increases the recognition accuracy from about 97 percent for prints alone to about 99 percent". Schroeter said the first application of the fingerprint-only technology probably would be in European cell phones that will appear by the end of the year. Smart-card applications will come when interfaces in the chips are created for the platform. The multifactor platform will be available later[100].

The price of the technology will play a big part in its acceptance, Schroeter said. A 32K card today sells for around $5. "A $10 sensor wouldn't fit into that market," he said. But with a printable sensor starting at less than $1, it becomes feasible.

4.5.2 Palm scanning

Fujitsu Computer Products of America Inc.[101] is coming out with a new version of its PalmSecure scanner featuring a smaller form factor with improved speed and accuracy. The Sunnyvale, Calif., company introduced PalmSecure in 2005. It uses a proprietary algorithm to recognise vein structures within a palm implementing technology that is perceived hygienic and more accurate than fingerprints, although not as accurate as an iris scan.

The first version had a standalone reader about 2.5 inches square that connects with a device by a USB port. "It was a little bulky for a laptop or PC log-in," said business development manager Hiroko Naito. It was better suited for embedding in larger devices such as automatic teller machines. The new version has a higher-performance camera, improved recognition algorithms and the size has been reduced by 25 percent. "It takes a little more time to do the matching," than on a typical fingerprint reader, "but it is more sophisticated and more accurate," Naito said. The company claims false-positive and false-negative rates of less than one-millionth of a percent. It also has almost no failures to enrol, Naito said. The device uses near-infrared light to detect blood flow in a palm held above the sensor and matches vein patterns. The technique is more robust than fingerprint detection, she said. "Asian females are a nightmare for fingerprints," Naito said, because they tend to have thin ridges, lower body temperatures and drier hands. Medical environments, where users are often washing hands and using moisturisers, also can be difficult for fingerprints[102].

[99] www.nanoident.com

[100] http://www.gcn.com/print/25_22/41472-1.html

[101] www.fujitsu.com

[102] http://www.gcn.com/print/25_22/41472-1.html

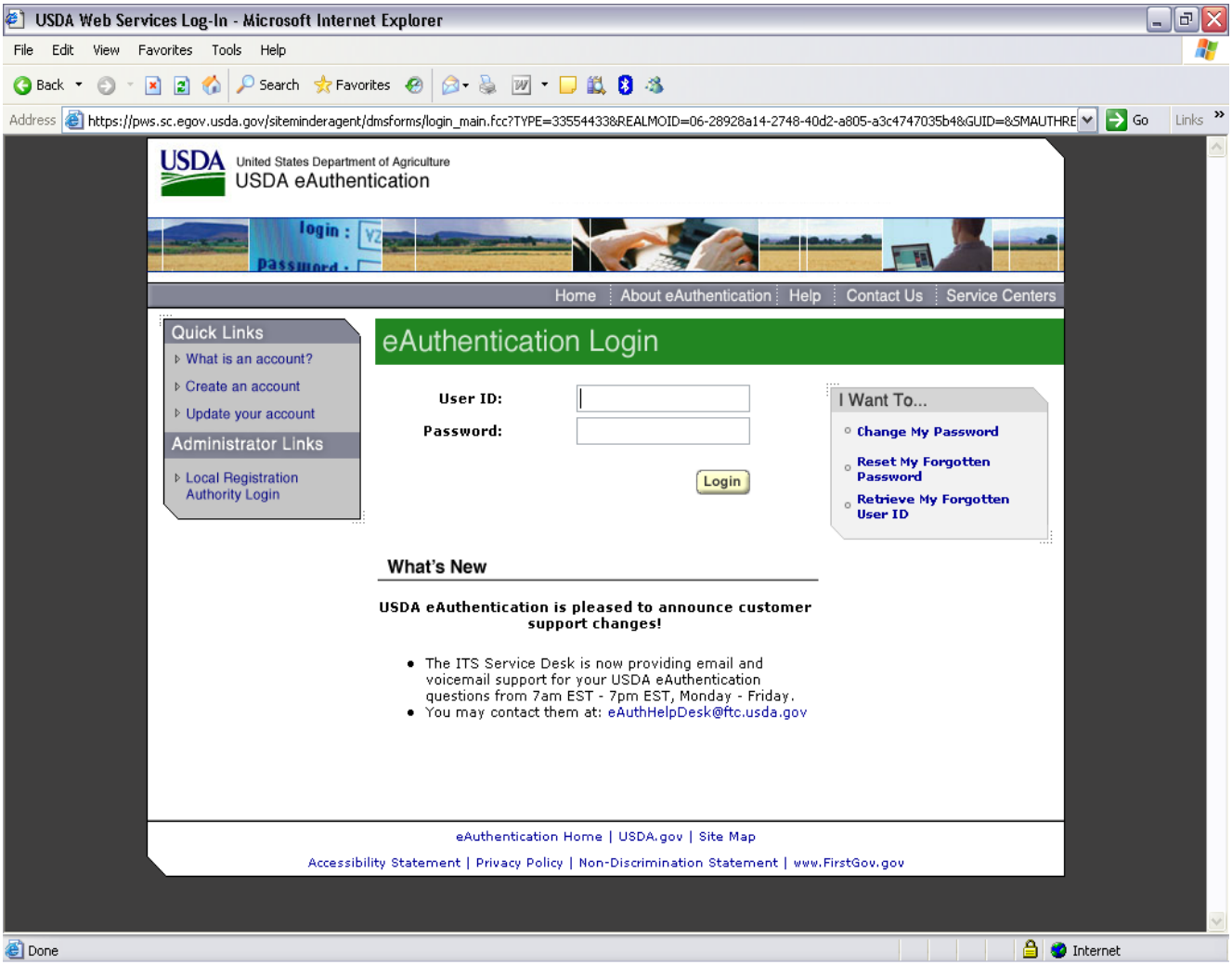
APPENDIX I

The US Department of Agriculture eAuthentication system

To log into the system, someone needs to access the following URL:

https://indianocean.sc.egov.usda.gov/GSM/index.jsp

The following eAuthentication screen appears:



The Internal Control Administrator is the person (assigned by the user organisation) who is responsible for setting up points of contact and assigning system permissions to other users in the organisation that wishes to use the system. Therefore, this person is the first to log into the system. The ICA cannot carry out any other tasks within the system (such as entering, reviewing or submitting applications).

The ICA is required to fill out a form and submit it electronically via the GSM Online System. Operations Division staff reviews the submission and approve the ICA. After the ICA is approved, that person can begin assigning GSM Online System permissions to users within their organization. Once a point of contact is created and assigned system permissions, the user can access the system.

APPENDIX II

Homeland Security Presidential Directive/Hspd-12[103]

Office of the Press Secretary
August 27, 2004

Subject: *Policy for a Common Identification Standard for Federal Employees and Contractors*

(1) Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

(2) To implement the policy set forth in paragraph (1), the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the "Standard") not later than 6 months after the date of this directive in consultation with the Secretary of State, the Secretary of Defence, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The Secretary of Commerce shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.

(3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).

(4) Not later than 4 months following promulgation of the Standard, the heads of executive departments and agencies shall have a program in place to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the Standard. As promptly as possible, but in no case later than 8 months after the date of promulgation of the Standard, the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. Departments and agencies shall implement this directive in a manner consistent with ongoing Government-wide activities, policies and guidance issued by OMB, which shall ensure compliance.

(5) Not later than 6 months following promulgation of the Standard, the heads of executive departments and agencies shall identify to the Assistant to the President for Homeland Security and the Director of OMB those Federally controlled facilities, Federally controlled information systems, and other Federal applications that are important for security and for which use of the Standard in circumstances not covered by this directive should be considered. Not later than 7 months following the promulgation of the Standard, the Assistant to the President for Homeland Security and the Director of OMB shall make recommendations to the President concerning possible use of the Standard for such additional Federal applications.

[103] http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

(6) This directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans.

(7) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.

(8) The Assistant to the President for Homeland Security shall report to me not later than 7 months after the promulgation of the Standard on progress made to implement this directive, and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

GEORGE W. BUSH

Prepared by:

Lead contractor:
European Dynamics

http://www.eurodyn.com

Contract No.:

Contract No. 30-CE-0043035/00-16

European Commission
Information Society and Media Directorate-General
eGovernment and CIP Operations Unit

Tel (32-2) 299 02 45
Fax (32-2) 299 41 14

E-mail infso-egovernment@ec.europa.eu
Website http://ec.europa.eu/egovernment