

4. Public Registries

Defining public registries

We define a public registry as a centralised and, in some sense, authoritative repository of information for a class of entities. This information may be of value in and of itself, but a defining feature of a public registry in our definition is its utility as the hub of an information architecture that links with other distinct databases, and by doing so, reduces the data requirements of services that build from those secondary databases. The essence, then, is one of information reuse.

This definition does not simply include any government database, though. Databases that are inherently transactional are not the target of our study. However, transactional databases will often have, or at least benefit from, a registry aspect to them. So, to take a stylised example of personal tax records, the tax collection agency will maintain both a list of tax payers and a list of annual payments made by each. Conceptually, the registry is the first list, while the transactions occur in the second. The distinction can obviously be rather grey in some cases. Further, transactions are expected to and do occur for registries: new entities get added and removed. Still, we find the distinction relevant and useful in narrowing down the types of eGovernment project that we are interested in.

From this definition, we can categorise public registries along two dimensions: the type of public registry and the scope of the public registry.

- Types of Public Registry: We may distinguish between three types of registry based on the type of “entity” about which information is stored: citizen registries⁷⁴, business registries, and asset registries. From the point of view of an analysis of “barriers to eGovernment”, this typology is potentially rather important. It is anticipated that Digital Citizen Rights are likely to be a major factor in limiting and moulding the development of public registries. However, these rights are likely to be rather different for people than they are for businesses; with the former having privacy rights that the latter very often does not. So, while inter alia technical and organisational issues are likely to be shared across registries of both types, citizen registries are likely to meet particular challenges.
- Scopes of Public Registries: Existing and proposed public registries vary a great deal in their scope. For our purposes here, we can divide registry projects up into being of European, national, or sub-national scope. European registries are meant to contain information for the entire population of relevant entities existing in Europe, or at the very least, across more than one European country. We use the sub-national scope as a catch-all for projects operating below the national level; be it regional, county, municipal, local, etc. We can further differentiate registry projects that are targeted at the full population applicable to their scope, and those that are applicable only to a subset. The distinction seems most relevant at the national level, but in principle it applies at the other levels as well.

A categorisation based on scope and the type of entity for which the registry is intended is presented in Table 1. Sub-types are provided for most boxes, and links to examples are provided for many.

⁷⁴Strictly, “citizen” is not really an expansive enough term as governments have registries on people who are not citizens – temporary residents, for example.

Table 1: European registry schemes by scope and type

Scope	Citizen	Business	Asset
European	Identity: RISER Eurodac	Company: European Business Register BRITE Project	European Patent Office Land (eg EULIS) Vehicle (eg EUCARIS)
National	Identity (Births/Deaths): Zentrales Melderegister (Austria) National Identity Register (UK) Public Services Broker (Ireland) Health (eg NPfIT: "The Spine" , UK)	Company: Companies House (UK) CVR (Denmark) CFENet (France) CFE (Portugal) Företagsregistrering (Sweden) Companies Registration Office (Ireland)	Land: HM Land Registry (UK) State Enterprise Centre of Registers (Lithuania) Centre of Registers and Infosystems (Estonia) Vehicle: WebDIV (Belgium) ACI (Italy) RDW (Netherlands) SRA (Sweden)
National Subset	Marriage Bankruptcy Child Benefit Service (Ireland) Electoral rolls Crime/Justice Criminal Records Sex Offenders Register (UK) Asylum Licensing Driving Professional status	Licensing Alcohol sale Pharmaceuticals Weapons (eg Export Control Organisation: "Goods Checker" , UK)	
Sub-National	Identity (Births/Deaths) ZMR/CRR (Austria) Electoral rolls Licensing	Company: GEWAN (Bavaria, Germany) Bremen (Germany) Catalonia (Spain) Valencia (Spain)	

It is possible to conceive of two ways in which public registries are related to the concept of "barriers to eGovernment". The first treats a public registry itself as an eGovernment project, and seeks to understand the barriers to the creation of such systems. The second stems from our understanding of public registries as being at the centre of a potential information architecture, and thus seeks to understand the ways in which they can act as barriers to the development of other eGovernment services. This is likely to be the result of incomplete and/or inaccurate information being held within the registries. As such, such problems can almost certainly be seen as the direct result of barriers of the first kind. For our purposes here, we pursue analysis of the first kind: barriers to public registries.

A brief survey of public registries

Types of Registry

In this section a review of some of the examples provided in each of the categories discussed above are explored.

Citizen Registries: The example cases listed in Table 1 provide an interesting snapshot of how the different types of registries take different forms (in terms of scope) across countries. A federal constitutional structure, as compared to a unitary one, clearly has implications for the structure of public registries and eGovernment programmes more generally. This institutional variable, together with the legal provisions that surround it, has led to an interesting solution for how to maintain a register of all citizens in Austria. There, the Zentrales Melderegister (ZMR) is effectively a distributed database. Citizens register with their local municipality, which maintains its own local registry. Updates to the local registries are then periodically propagated to a central database maintained by the federal government (ePractice, 2007a). From the seven barrier categories of the Breaking Barriers project, it is tempting to suggest that issues of this sort should be likely to lead to problems associated with “poor coordination” and potentially “leadership failures” due to the large number of organisations involved and “financial inhibitors” due to the small size of many of the municipalities needing to operate local registries. However, the apparent success of the Austrian project suggests that these barriers, if they existed, were well-tackled.

The Austrian ZMR case is also interesting in another respect. The “lack of trust” barrier – specifically with respect to privacy – was clearly perceived to be relevant to the success or failure of the project as a whole. So, while the central ZMR database assigns each individual a unique identifier number (sourcePIN), this number is almost never used directly. Instead, when citizens use their registration in interactions with agencies in different state sectors (staatlicher Tätigkeitsbereich), a sector specific identifier (ssPIN) is generated securely from the original ZMR identifier and this new ssPIN is stored in the sector-specific database. The effect is to limit the extent to which the state can cross-reference all activities of an individual, thus protecting privacy. There are, however, mechanisms for links between ssPINs for an individual to be made. Requests to the Austrian Data Protection Commission (Österreichische Datenschutzkommission), which acts as the sourcePIN Register Authority (Stammzahlenregisterbehörde), make it possible to access data for an individual across sectors (Makolm 2004).

In Ireland, a more comprehensively centralised approach to citizen registration is being pursued. However, the trade-off for the comprehensiveness could well be a weaker privacy regime. The Irish government is engaged in a project known as the Public Service Broker which is meant to sit at the centre of nearly all eGovernment services. At its heart, there lies the idea of a Personal Data Vault. This will essentially be a database record for each individual person containing all manner of personal information. Initially, the amount of information stored in the system will be at the discretion of the individual; so, those with privacy concerns or just plain ambivalence to the system's benefits are free to opt out, while those for whom the benefits strongly outweigh any perceived costs can add large amounts of information. The benefits, once a sufficient number of eGovernment services have been developed and integrated, are largely in the area of ease of data sharing and thus reductions in the amount of duplicate information that needs to be supplied to government agencies. The model for the Personal Data Vault is that each individual will have control over which actors and agencies can have access to which portions of their data. Reach, the government agency charged with the development of the Public Service Broker system, discuss building requirements for having users authorise the access of records by providing a pin to authenticate themselves. On the privacy issue, Reach states that (Reach n.d.),

Compliance with those published procedures and legislation is further subject to scrutiny by a number of statutory office holders, viz., the Comptroller and Auditor General, The Ombudsman and Information Commissioner and the Data Protection Commissioner. Finally, the Minister and his officials are answerable to the Dail and the Public Accounts Committee on all issues related to the Reach project.

Here we can see a contrast with the approach taken for the Austrian ZMR. In both systems, the state has the ability to link the activities of individuals across sectors. However, in Austria, the ability to do so is directly controlled by the Data Protection Commission, while in Ireland, the plan is to use the equivalent actor(s) in more of a “fire alarm” way. That is, those charged with ensuring privacy is upheld must discover wrong-doing in Ireland, while those same agents in Austria have technical control over the ability to compromise privacy. Taken as a whole, the state has equivalent power in both countries, but the institutional differences across the two are potentially important for the purposes of generating trust.

One service developed in Ireland to take advantage of the Public Service Broker facility is the new Child Benefit system. This is interesting in the discussion of barriers to public registries as the project can be seen both as a consumer of the Public Service Broker service, and an integral supplier of information to the registry. The dual nature of the project is clear from its stated aims, which were (ePractice, 2007b):

- Sharing of life event data among agencies
- Automatic allocation of a Personal Public Service Number to new born children
- Pro-active and automated processing of child benefit claims
- Elimination of submission of a birth certificate when claiming for child benefit

The ability to automate the process of child benefit payment is contingent on the existence of an accurate database of eligible children and parents. The effectiveness of the Public Service Broker system is likewise contingent on accuracy and completeness. Thus, the automation of birth registration with the Public Services Broker and the subsequent joining of the child benefit system to it provides reward for both citizen and state. The former sees reduced administrative burden associated with the receipt of benefits, the latter sees both reduced administrative burden and a systematically more accurate central citizen registry.

The Eurodac project providing a database of European asylum seekers' fingerprints is another prominent citizen registry. A detailed embedded case study of Eurodac is presented below.

Business Registries: Functions such as company registration show a clear tendency to be national concerns in unitary states, while being a mixture of national and sub-national in federal states. In some federal countries registration is specifically a competence of regions or municipalities. This is true of Germany and Spain, and there are several examples of eGovernment registries operating at the regional level in this sphere, for example, in Bavaria, Bremen, Catalonia, and Valencia. Decentralisation of registry provision in this way potentially increases aggregate costs as systems and processes must be duplicated. However, it may also lead to more responsive service as provider and “consumer” are “closer” in some sense.

The Bavarian business registry case offers examples of several issues of importance in such a decentralised environment. For this reason, we present GEWAN as an embedded case study below.

In order to enhance efficiency and reduce administrative burdens a number of countries have begun, or are moving towards, the use of a unique business number and single registration system for all businesses. For example, Belgium has launched the Crossroads Bank for Enterprises, an integrated business register where each registered business is attributed a unique identification number that is linked to a set of information stored in a central database. This unique identifier is maintained centrally and used as primary key to exchange information between Belgian administrations. Such an initiative eliminates the need for businesses to provide the same information to several administrations and makes possible the delivery of joined-up services to enterprises.

The Netherlands is developing a system of six Basic Registers for personal data (de Gemeentelijke Basis Administratie), all data (name, address, number of employees, company number, key activities) about companies in the New Dutch Trade Register (het Nieuwe Handelsregister), and all information about buildings (Basis Gebouwen Registratie), ground and the use of ground (Basisregistratie Kadaster), map material (Basisregistratie Topografie), and addresses (Basis

Registratie Adressen) are to be included. The Basic Business Register, or BBR for short, will contain the identification details of all companies and organisations based in the Netherlands. The unique identification of companies is necessary for the 'electronic recognition' of companies, and is essential for the exchange of information between different government organisations (multiple usage). The initial version of the BBR has been developed under the coordination of the Ministry of Economic Affairs by four national registers: the Tax Department (Belastingdienst), the Chambers of Commerce (Kamers van Koophandel), the Employee Insurance Scheme Agency (Uitvoeringsinstituut Werknemersverzekeringen), and Statistics Netherlands (Centraal Bureau voor de Statistiek).

There is also an interesting emerging European aspect to company registries. The European Business Register (EBR) (<http://www.ebr.org/>) is a European Economic Interest Group (EEIG)⁷⁵ with partners in 17 European states. It provides searchable access to company information across those states, although the level and sophistication of this access varies. While it is not de jure a central registry of European company information, it has the potential to become such a service de facto; in essence, like the distributed database system that forms the Austrian ZMR. Building on the EBR, the BRITE Project (<http://www.briteproject.net/>) is an attempt to increase the effectiveness of the EBR offering. Started in March 2006, it is a collaboration funded by the European Commission's DG Information Society & Media and coordinated by EBR which "aims to develop, implement and demonstrate an advanced, innovative interoperability model, ICT service platform and management instrument for Business Registers (BRs) to interact across the EU" (BRITE Project n.d.).

Asset Registries: The issue of vehicle registration is also relevant at the European level. Across the European Union tackling car theft, registration fraud, and cross-border traffic enforcement can be problematic as member states can have difficulties in quickly and conveniently accessing car registration information in other countries. Indeed, as this is considered a priority for the European Union, project REGNET began in 2006 as part of the IDABC programme to provide an electronic network to enable exchange of vehicle registration data between member states⁷⁶. Outside the European Commission there have been a small number of initiatives in this area. Probably the most significant and well known is the European Car and Driving License Information System (EUCARIS) (<http://www.eucaris.net/>) that was set up in 1994. EUCARIS enables countries to share their car registration and driving license data. It is a commercial venture that has been developed by governmental authorities and is intended to be used by government authorities responsible for the registration of motor vehicles, issuing vehicle documents and driving licences; and government organisations responsible for tracing stolen vehicles, theft and fraud prevention, as well as prosecuting authorities, the police and customs and excise. Countries can decide whether or not to join EUCARIS for a fee. In 2006 participating countries included, Great Britain, Germany, Luxembourg, Latvia and the Netherlands.

EUCARIS does not have a centralised database; the system allows people to search other countries registers but cannot alter them in any way. It has been set up to work within the existing regulatory, legal, technical and cultural landscape. Thus, those that have developed and implemented EUCARIS have had to address a number of issues that are of relevance to the current study. These include: privacy and data protection; identification and authentication; interoperability and differences in administrative law and other practices in each country. For example, different countries hold different types of data and some do not have a centralised registration database. These issues can also be linked to Public Administration Transparency and Re-use of Public Sector Information. Also, the issue of Intellectual Property Rights may also be of relevance here, in terms of who owns and developed the EUCARIS software. These issues will be discussed further below.

The EUCARIS case provides an example of an early eGovernment service that was developed in a relatively "low tech" way to address existing constraints to eGovernment. Such a study, in conjunction with a close dialogue with key stakeholders within the REGNET project could be particularly valuable as REGNET aims to optimise the process of sharing registration information;

⁷⁵ c.f. <http://www.europa.eu/scadplus/leg/en/lvb/l26015.htm> (accessed 2006/12/04).

⁷⁶ See Synergy, Issue 4, October 2005 <http://europa.eu.int/idabc/en/document/5005/5584> And the IDABC Work programme 2005 – 2009, November 2005 <http://europa.eu.int/idabc/en/document/5101/3>. (both accessed 2007/01/25).

and endeavours to address many of the problems encountered by EUCARIS through, for example, tackling data harmonisation and enabling exchange between all member states.

Land registries provide another interesting example of emergent eGovernment.⁷⁷ A recent survey found that 86% of land registries in Europe and North America are “wholly or partly computerised” (HM Land Registry 2005: 10). From Table 1, the HM Land Registry (UK) (<http://www.landreg.gov.uk/>) is notable as they have developed several web-based services. There is a service for professionals (Land Registry Direct) (<http://www.landreg.gov.uk/direct/>), one for the general public to search the registry (Land Register Online) (<http://www.landregisteronline.gov.uk>) and an under-development, and somewhat delayed, online conveyancing service (Chain Matrix)⁷⁸. As might be expected with this latter type of service, there were legal issues.⁷⁹

In a revealing example of the technical and organisational issues that can underlie public registries, Peeva (2001) provides an outline of the decisions that Bulgaria confronted in its attempts to comply with its Kyoto Protocol commitments. Faced with the need to record land-use and land-use change in the country, Peeva’s analysis sets out how the preferred registry design, both technically and institutionally, varies with the nature of the registry that is chosen. The level of expected transactions and the nature of the organisations that will engage in them is found to lead to different preferred policies.

Comparing the registry types: Business-related registries are currently more developed in an eGovernment sense than citizen-related ones. The apparent relative success of company registries can be seen in the large number of national and European projects in Table 1 that apply to this area. There is some variation in the mechanisms used for encryption and authentication of data, even in the more successful national schemes. Still, there appears to be a tendency to move towards web-based systems, as exemplified by Companies House (UK) rolling out such a system (the “WebFiling” system) after initially developing an email-based system (the “Software Filing” system). It is plausible that the initial divergence in authentication mechanisms is a result of the differing degrees of centralised direction across state sectors that this issue received in different countries. So, in countries such as Estonia (Centre of Registers and Infosystems, see below) and Austria (Bundesrechenzentrum [BRZ]⁸⁰), programs led by central government were put into place for the management of registry systems. This included authentication and encryption, and thus provided them with the opportunity to avoid the need for different sectors to “reinvent the wheel” in these respects.

Institutional forms of registry provision

The institutional form of registry provision is an interesting area to explore. Ostensibly, the Estonian example is an obvious one of a centralised approach. There, the Centre of Registers and Infosystems (Registrite ja Infosüsteemide Keskus) was setup under the auspices of the Ministry of Justice and has a very broad range of registries within its remit.⁸¹ In many other countries, such functions fall under the control of a rather disparate array of governmental and non-governmental departments and agencies. An obvious line of inquiry is to investigate whether the centralisation of registry services in this way produces benefits – in the form of reduced “organisational culture”, “human resource”, or “funding” barriers – or whether the potential downsides that it introduces – in the form of “poor coordination” between registry provider and “client” organisation, and lack of domain-specific expertise – overwhelm the upsides. For this reason, we selected Estonia as one of our embedded cases. However, our field research revealed that this outward impression does not completely hold up to closer scrutiny, with a more standard decentralised structure in place in reality. The case is nonetheless very revealing about several important issues (see section below).

⁷⁷ For a more extensive discussion of eGovernment projects related to land registries c.f. Panayiotou (2003).

⁷⁸ <http://www.landreg.gov.uk/e-conveyancing/chainmatrix/> (accessed 2006/12/05).

⁷⁹ HM Land Registry note the following (HM Land Registry n.d.), The Land Registration Act 2002 contains the legislative provisions to enable the implementation of eConveyancing services. Secondary legislation in the form of rules now needs to be drafted and passed by Parliament to give effect to those legislative provisions.

⁸⁰ <http://en.brz.gv.at/> (accessed 2006/12/05).

⁸¹ http://www.eer.ee/index_eng.phtml (accessed 2006/12/04).

At the opposite end of the scale from centralised state provision of registry services, there are some instances of privately-run registries (albeit with public sanction and cooperation). The role of the Automobili Club d'Italia (ACI) in “managing [on behalf of the Italian Government] the Car Public Registry [... which] includes managing the taxes and payments services, vehicle ownership and the end-of-vehicle-life data for many Italian regions” (IBM n.d.) is a prime example. Again, little information about this project is currently available. However, such a structure obviously leads to questions whether such an institutional form leads to greater or lesser problems in the provision of registry services. Does an element of private sector discipline yield more customer-focused results, or does a profit motive of sorts inhibit development? Does the monopoly position of the registry provider remove the relative financial discipline normally associated with the private sector, especially where it knows that the state cannot afford for it to fail? More generally, are there lessons that can be drawn by comparing the ACI case with the Estonian central registry agency approach?

The embedded case studies

The sections above on the scope of public registries are suggestive of ways in which barriers to public registry schemes may vary across cases. We may suspect that smaller (lower) scope schemes, being concerned with more manageable bureaucracies and, perhaps, with more malleable organizational cultures will suffer less from issues surrounding coordination and remapping of internal processes. Consequently, registry schemes at, say, the level of the city or region may be more successful than those at the national and transnational level in those regards. By contrast, issues of funding and (relatedly) human resources may well be more problematic for smaller scope schemes that have smaller governments and correspondingly smaller budgets behind them. An inability to benefit from economies of scale would probably exacerbate these funding issues.

It is conceivable that the extent to which legal barriers come into play also varies by the scope of the scheme. If legal restrictions tend to be applied at the national level, then those schemes that operate at that level may benefit from stronger backing from a national government that has the opportunity to change the law. By contrast, regional level schemes are less likely to be able to achieve any required legal reforms (to the extent that they must be passed at the national level). Equivalent reasoning may also apply with respect to European level schemes that are reliant on national legal changes or implementation. The EUCARIS and Eurodac projects, which have failed to achieve fully pan-EU coverage, may be examples of this. It should be noted that this line of reasoning speaks only to the relative ability to overcome barriers, not to the relative occurrence of such barriers across different schemes.

Some working hypotheses are then:

- Organisational barriers increase as the associated level of government gets higher.
- Resource barriers decrease as the associated level of government gets higher.
- Legal barriers are more likely to be overcome by schemes that operate at the national level.

Based on the discussion set out above, we selected three embedded case studies. The aim was to pursue some of the issues that became apparent from our preliminary research and categorisations. To this end, we selected cases at three different levels – sub-national (GEWAN), national (Estonia), and European (Eurodac). These cases were also chosen so as to cut across the other dimension that we identified – that related to the type of entity about which information is stored. Thus, we have a company register (GEWAN), a “citizen”⁸² register (Eurodac), and a project that is, in part, an asset register (Estonia). As noted above, a further attraction of the Estonian case

⁸² Perhaps “person registry” would be a more appropriate name for this category given that the information being stored is about asylum-seekers, not citizens.

was its apparently different institutional structure in the sense of having a centralised agency providing large portions of the national registry requirements.

Case Study: GEWAN: Web-based Business Registration in Bavaria

Leo van der Wees

Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, Netherlands

Definition of the case study

GEWAN (GEWerbeAnzeigen im Netz)⁸³ is a fully web-based business registration eService currently being used in Bavaria, Germany. The GEWAN database at its centre is employed by the founders of companies and agencies, municipalities and District Administrator offices in the State to exchange data through the Internet. This supports four main services: registration; dissemination; information; and statistics. It includes an electronic notification service, for example to inform the Tax Office that a company has been founded and will have to pay taxes.

Setting of the GEWAN case study

The high rate of growth of new companies in the State of Bavaria was one of the motivations for initiating the GEWAN project in 1998. Registering new companies can help their success by offering them relevant support, but the registration process had involved substantial paper work and human effort. The Bavarian State Office for Statistics and Data conceived and developed the idea of creating a central company registration database to help reduce this costs and effort, while improving the quality of the registration data and the analyses and services related to this information.

This State Office remains the most important player in the project, as it manages its operation and development. It is supervised by the Bavarian Minister of the Interior, but there is no indication of his direct involvement in this project. Other key players include the Gemeinde (cities) and Landratsämter (district administrations). GEWAN is also supported by business experts in the region (e.g. in helping to determine which information should be processed through its database) and representatives responsible for the protection of personal data.

The State Office for Statistics and Data previously handled all company data now incorporated into the GEWAN database. The new eService has meant the access and registration opportunities offered by the Office are now also available through the use of the Internet. This easier and cheaper registration is expected to support more people in attempting to start a business.

There are similar registration systems on the Internet, such as those used by the Dutch Chamber of Commerce⁸⁴ which provides comparable services.

Milestones in the development of GEWAN

1998: Bavarian Office for Statistics and Data originates the idea of a digital company registration service

1999: The Office for Statistics and Data begins testing software it has developed for the new Internet-based registration service.

2000: In December, a pilot project (GEWAN 3.0) begins operating, in only the city of Gaißach.

⁸³ For further details on GEWAN, see Bayerisches Landesamt für Statistik und Datenverarbeitung (2005; 2006). Information about this case (in German only) is also available through the GEWAN Gewerbeportal (<https://gewan.bayern.de>). And a description of GEWAN is also available on the EU's Good Practice database for eGovernment (<http://www.epractice.eu/cases/329>).

⁸⁴ The form for searching this Dutch company registration database can be found at: <http://www.kvk.nl/handelsregister/zoekenframeset.asp?url=https://server.db.kvk.nl/wwwsrvu/html/zoek.htm> (registration is required for full access).

2001: In April, GEWAN moves from being a pilot project to integration as a web eService.

2001: In December, Gaißach becomes the first municipality to be officially connected to GEWAN

2002: In March, the GEWAN system is completely updated.

2004: In February, Regensburg becomes the first county (Landkreis) for which the office for the district (Landkreisamt) and all its municipalities are connected to GEWAN.

2007: The latest system update (to version 4.0.1) was undertaken in March, by when more than 1000 municipalities and over 50 Landkreisamt offices were connected to GEWAN. More than 70% of the business registrations are being disseminated electronically to the relevant institutions appointed by law.

Challenges and potential barriers faced

The risk of technical obstacles was minimized by developing GEWAN in close cooperation between software experts and the people who were expected to use the system. The software development was also facilitated because such an Internet-based registration and exchange system is not new, so it wasn't necessary to create a completely new technologically-advanced system. In addition, effective operation would be to all stakeholders' benefit, which provided an all-round incentive to make the system work well.

From the beginning, it seemed that GEWAN would bring only advantages for all the main stakeholders (e.g. in saving time, money and effort). There were not even significant objections against it from those accustomed to the traditional system, as the old paper-based approach was not functioning properly.

Information security and privacy issues were the main potential barriers identified at the outset. The building-in of safeguards in these areas was therefore prioritized.

Adoption and implementation of GEWAN

To help avoid subsequent problems, the Office for Statistics and Data ran an initial pilot project within several areas for one year, after first allowing computer experts to test the pilot intensively. In the period of pilot operation, security was enhanced, the project began doing useful work and the GEWAN project team started to offer seminars to the people who would use the system. This helped to increase familiarization with the new eService. After the pilot, the system was adjusted to cope with more registrations. Initial opinions on the project are not known, but since the number of applications in the first five years of operation was substantial, the early perceptions of GEWAN seem to have been generally positive.

The State Office for Statistics and Data continues to update the system regularly⁸⁵, and organizes seminars and lectures to teach people how to use the system. The regular updating copes adequately with any software-related problems that arise, which has further helped to avoid major technical obstacles to the system's general operation. A set of manuals is available at the GEWAN site to enable people to operate the system without additional help.

Project design

The key legal factor to be addressed in the project was the protection of the sensitive company and personal data held in the GEWAN database. This aspect was therefore prioritized in the system's design and implementation, including the incorporation of the latest data security methods when the system is regularly updated. Special care is also taken with the dissemination of company information to third parties. For example, no sensitive data is disseminated, in order to prevent this

⁸⁵ Recent information on updates and on the development of GEWAN can be found at <https://gewan.bayern.de/> (click on Aktuelles in the top menu).

type of information coming into the hands of unauthorized persons; and only those parties with which its registered companies are obliged to work (e.g. Tax Collectors Office) are sent any related information directly from GEWAN.

As it was designed for the registration of company data, it was essential that plans for this system had to ensure it could process effectively the substantial number of registrations expected. One of the aims of the pilot was to test that this would be possible when GEWAN was introduced.

Registered companies and authorized operators have a separate menu from which to login into the GEWAN database to access four main eServices:

- **Registration:** Municipalities can acquire and register data on companies. A key objective of GEWAN is to improve the quality of this data, which is achieved by simultaneously checking information as it is entered into the system to ensure its correctness and completeness. In addition, the system ensures that those involved in more than one business need to register their general details only once. As soon as it is entered into the system, a check is made to ensure this data has not been entered previously. All registration data is made available immediately after it is entered for inspection by the Landkreisamt, which can adjust the information at any time.
- **Dissemination:** After the business registration has been checked and approved by the Landkreisamt, it is sent via the Internet to those institutions appointed by law to receive the data. This saves time and money because the data no longer has to be sent by post. Registrations refused by the Landkreisamt are immediately returned to the applicant. The data will be reprocessed and an explanation for the refusal attached by the Landkreisamt
- **Information service:** GEWAN also offers support for consultants by giving them access to its extensive information system. Its database can be explored easily by entering the date or place of registration, or other search criteria. If the system retrieves several results, they are presented in a clearly structured manner to provide an overview of companies and persons related to one or more companies. In addition, various specific overviews can be produced (e.g. general information about a company; historical data related to a company; or information about the persons working for an enterprise).
- **Statistics:** GEWAN decodes/translates the data entered into the system on economic activities as indicated by European regulations. This offers opportunities both to create various useful local lists (e.g. all restaurants in a municipality) and to undertake comparisons within the EU. Such lists can be sorted and printed easily.

Project impacts

GEWAN has surpassed its initial goal of improving the performance of the registration process because of the faster handling of information (e.g. quicker and easier of registrations of companies and access to, and analysis of, that data). In addition, its database has been useful for enhancing other functions, such as policy processes and statistical analyses.

Exact numbers relating to the system's performance aren't available, but we believe the increase in efficiency certainly weighs up well against the investment made for this project. The precautions taken regarding the protection of company and personal data seem to have avoided significant obstacles in this respect. The data at our disposal does not mention any changes of laws that would have facilitated the execution of the project and subsequent operation of the resulting system.

The benefits delivered by GEWAN for all stakeholders meant the success of the project was important to all. As a result, there weren't many political or other objections to the development. Impacts on specific stakeholders include:

- The State Office for Statistics and Data had to previously catalogue various data, including company registrations. With GEWAN, it could do this at less costs and much more easily compared to the considerable time, effort and money needed to process paper-based data.

- Businesses enjoy the biggest benefits of GEWAN. When someone wants to start a company, registration is much faster than before and the administrative burden a lot lower.
- Citizens generally notice the project only when they are looking for a company to perform a certain task for them. Plans exist to make a small part of the GEWAN database accessible to the public so that consumers can check the kind of company with which they are doing business.
- The government has a better picture of the development of companies to assist its policy and decision making by, at the click of a mouse, having access to GEWAN's large database with company information. For example, it could compare pollution statistics with data from GEWAN to check how the level of actual pollution corresponds with the related goals registered for particular companies.
- Because of GEWAN, the persons (e.g. notary offices, city offices) who register new companies have taken on new roles as operators of eServices, such as taking care of the input. The State Office for Statistics and Data has also added the maintenance of the database to its registration responsibilities.

Factors affecting this case of significance to wider eGovernment initiatives

Seven Barrier Categories

The Breaking Barriers Project, funded by the EC, identified and explored the key barriers to eGovernment in Europe. The project team proposed seven key barrier categories of obstacles to eGovernment progression. The categories are intentionally broad and tied to a multitude of more specific barriers relevant at different governance, institutional and jurisdictional levels. This categorization is particularly valuable when discussing the barriers relevant to this case which may have relevance for other eGovernment initiatives. In summary the barriers are: leadership failures, financial inhibitors, digital divides and choices, poor coordination, workplace and organizational inflexibility, lack of trust and poor technical design⁸⁶.

The following are the main issues that arose during the implementation of GEWAN of relevance to the seven barrier categories identified by the Breaking the Barriers to eGovernment project (no new barriers were detected in this case study outside these categories).

Leadership failures: The substantial experience and good reputation in processing data of the Bavarian State Office for Statistics and Data made it the logical leader of this project, and it has performed this role well.

Financial inhibitors: Financial inhibitors seem not to have played a role in this project, particularly because it produced clear savings to the State Office for Statistics and Data compared to its previous paper-based handling of company data.

Digital divides and choices: Learning how to use the system can cause a problem in its effectiveness. For example, some people still have to learn how to work with it effectively (e.g. start-up companies when first encountering the system). This can create an 'ICT threshold' to be overcome by less technology-minded companies and individuals, while at the same time offering advantages to those who master its use. To overcome a possible threshold education on how to use the system is taken care of by GEWAN.⁸⁷

Poor coordination: Coordination of its technical design and approaches to disseminating company data is a high priority for this project because many parties play a role in the system's development and use. It seems that GEWAN has been effective in this coordination, as indicated by its substantial and growing user base of over 1000 organizations.

⁸⁶ For more details about the Breaking Barriers to eGovernment project please see <http://www.egovbarriers.org>

⁸⁷ See: <https://gewan.bayern.de/> (under Schulung).

Lack of trust: Although there are always likely to be some people who will continue to trust paper registration more than electronic media, the success of GEWAN in attracting so many participants is building trust in a web-based approach and reducing the degree to which companies hesitate before using this eService.

Poor technical design: The wide use of the GEWAN system indicates that it works well and has a reasonable technical design. Any technical shortcomings are corrected by regular updates and patches⁸⁸. And since an Internet-based registration and exchange system is not new, so it wasn't necessary to create a completely new technologically-advanced system. As a result the chances for a poor technical design were limited.

Relative influence of eGovernment challenges

The GEWAN project has been quite successful. There were not many barriers which have caused significant problems. Therefore we would stress the factors which lead to this success and which could be kept in mind for other eGovernment projects as well:

The GEWAN project has been very successful in Bavaria. There were not many barriers which have caused significant problems, but they had to overcome resistance to the use of new technology and to the uncertainty about the advantages of a central system. Nevertheless we would like to stress the factors which lead to this success and which could be kept in mind for other eGovernment projects as well:

- Political, administrative and organizational (40%): People working for the Bavarian statistics office and companies willing to register have faced administrative barriers for years. The procedure to register companies was too lengthy, too much of a hassle, therefore, the idea to develop a system to smoothen the procedure for the registration was accepted without significant objections by any party. Also politicians were in favor of the system because the system gives them easier access to data which could be of importance for political and economical decisions.
- Legal (5%): Privacy protection was an issue, mainly because the data protection authorities requested a detailed concept in order to provide access to data only to those users that were legally entitled. Maybe because the Bavarian statistics office was an important stakeholder in the project, the way which was dealt with personal data was being trusted. This might be different in other regions of Germany and in other member states.
- Financial (5%): Finance had a relatively low influence in this case because it was clear beforehand that the result of the system would save the Bavarian statistics office and start-ups willing to register time and money.
- Social and economic (40%): The main idea behind the project was to eliminate administrative barriers for starting companies, and to eliminate several manual administrative steps following the initial registration.
- Technological issues (10%): Technological issues were an issue in the early years as Internet bandwidth was low and access wasn't given in many locations. Also, there was a lack of trust in the concept of central data storage via an Internet network. One of the main issues was to protect the data in the database and the data being transported to the users of the data.

Conclusions

As far as we can assess, the project has been successful in undertaking its planned function, with many registrations during its years of use. However, there are no detailed assessments yet. The expertise of the State Office for Statistics and Data in this area seems to be a key reason for the

⁸⁸ See: <https://gewan.bayern.de/> (under Aktuelles).

reasonably smooth progress of the project in achieving its aims. From the start, experts in this Office were aware of the main problems that could surface with this kind of project, and thus were able to plan how to avoid and minimize their occurrence. This highlights a key lesson: that understanding where barriers could lie is an important management tool.

The technical barriers were simply not there because the concept was not new. At the start of GEWAN already many Internet registration services were being used. Also quite a long test period – almost 3 years – avoided technical and user interface problems to arise.

The ICT-threshold has been kept low because GEWAN has been offering courses how to use the system from the beginning.

The result justifies the resources spent not only because the system met its goals, but also because it has extra advantages like the easy exchange of data with tax services, better and cheaper statistical services, and company information service for consumers.

There are also good prospects for implementing it in other German States, as the ease of use and benefits delivered by GEWAN appeal widely to government, companies and company subscribing offices (e.g. notary offices). Thus, the impact of GEWAN is definitely sustainable and practice is being shared.

References

Bayerisches Landesamt für Statistik und Datenverarbeitung (2006), Gewerbeanzeigen im Netz (Gründagentur, Gemeinde, Landratamt)

Bayerisches Landesamt für Statistik und Datenverarbeitung (2005), Projekt GEWAN
Verfahrensbeschreibung nach Art. 26 Abs. 3 Satz 1 BayDSG

Interviews: Hansjörg Zitzmann, representative Office for Statistics and Data.

Case study: Eurodac: Fingerprint Identification of Asylum Applicants in Europe

Dr Sjaak Nouwt

Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, Netherlands

Definition of the Case Study

The European dactylographic⁸⁹ (Eurodac) identification project⁹⁰ has established a supranational system for fingerprint identification of asylum applicants and illegal immigrants in Europe, including a database that shows where an asylum applicant entered the European Union. The Member State identified by Eurodac as being where the asylum application was first made is held responsible for examining that asylum application, and asylum seekers who have moved elsewhere can, as stated in the Dublin Convention, be returned to it. Eurodac includes all EU Member States that signed the Schengen accord, which removed their internal border controls⁹¹, as well as the non-EU countries Norway and Iceland.⁹²

In addition to applicants requesting asylum, the database managed by the Eurodac Central Unit also registers the fingerprints of illegal residents and other persons (known as a 'third-country nationals') who are not a national of one of its participating States and who irregularly cross the external border of Member States.

The intention is to use this system to help prevent asylum applicants applying in more than one State, say by changing their name or by throwing away their travel and identity papers. This is not a novel form of eService. For example, incomers to the US must have personal biometric data, such as fingerprints, checked before they are allowed to enter the country. This gives the US government a detailed picture of the kinds of people travelling into the country. The Eurodac database is comparable, except that it only determines which country should examine the application of an asylum seeker.

Setting of the Eurodac case study

Eurodac's Central Unit maintains the system's database. It is managed by the European Commission with the aim of promoting cooperation between Member States to achieve Eurodac's goal of gaining a better understanding of the location and movements of third-country nationals within the EU and crossing its borders. This requires the Central Unit to maintain an accessible database to provide the information needed by the Member States.

⁸⁹ The study of fingerprints as a means of identification.

⁹⁰ See: <http://europa.eu/scadplus/leg/en/lvb/l33081.htm> for a summary of Eurodac legislations. For more detailed legislative and other background, see the European Commission's websites: 'Towards a Common European Asylum System'. (http://ec.europa.eu/justice_home/doc_centre/asylum/doc_asylum_intro_en.htm); 'Attributing Responsibility for Examining an Asylum Application in the European Union'. (http://ec.europa.eu/justice_home/doc_centre/asylum/criteria/doc_asylum_criteria_en.htm); and 'Eurodac - a European Union-wide Electronic System for the Identification of Asylum-

seekers' (http://ec.europa.eu/justice_home/doc_centre/asylum/identification/doc_asylum_identification_en.htm).
⁹¹ This excludes the UK and Ireland, who did not sign the Schengen 'accord' or 'acquis'. This abolished the internal borders of the signatory states and created a single external border where immigration checks for the Schengen area are carried out in accordance with a single set of rules, allowing free movement within it (see: <http://europa.eu/scadplus/leg/en/lvb/l33020.htm>).

⁹² Norway and Iceland are members of the European Economic Area (EEA), which has been maintained to enable three of its members who are outside the EU (Norway, Iceland and Liechtenstein) to participate in the Internal Market while not assuming the full responsibilities of EU membership. This allows participation in EU-related programmes such as Eurodac.

The key stakeholders that Eurodac seeks to satisfy are the government institutions responsible for the registration and identification of third-country nationals in its participating States. However, the Eurodac database is not directly accessible by these national authorities. Instead, the Central Unit can only inform one of its States whether or not the fingerprints of a person are in its database and identify to which Member State it has forwarded these records.

Eurodac is monitored by the European Data Protection Supervisor (EDPS), who ensures the rights of data subjects are not violated by the processing or use of the data held by the Central Unit.

Milestones in the development of Eurodac

This case study looks at the entire development of the Eurodac project, from the conception of the idea in the Dublin Convention of 1990, to its implementation through the European Council Regulation in 2003 and on to assessments of its implications in practice. The following are significant milestones leading to the creation of Eurodac and its subsequent development.

1951: Signing of the United Nations' Geneva Convention relating to the status of refugees.⁹³

1990: Signing of the Dublin Convention⁹⁴ relating to the State responsible for examining applications for asylum lodged in one of EU's Member States.

1991: Discussions on the technical feasibility of a supranational biometric identification system in Europe begin.

1996: Political discussions start considering a supranational identification system.

1997: Dublin Convention comes into force.

1998: European Union Treaty of Amsterdam⁹⁵, which specifically requests Member States to establish criteria and mechanisms for determining which State is responsible for considering an application for asylum.

2000: Signing of the European Council's Regulation 2725/2000 of 11 December establishing Eurodac.⁹⁶

2003: Signing of European Council Regulation Dublin II⁹⁷, introducing some changes to the original convention (e.g. restricting a Member State's responsibility for an asylum-seeker who has illegally entered into EU territory to twelve months, after which, if it is impossible to determine through which Member State the asylum seeker entered the EU, responsibility switches to the State where that person has stayed illegally for over five months).

2003: Eurodac operations begin on the 15th of January.

2004–2007: Evaluations of Eurodac (see European Commission 2004; 2005; 2006; 2007).

⁹³ See: http://www.unhcr.ch/html/menu3/b/o_c_ref.htm

⁹⁴ See: European Commission (1997) for details of its provisions.

⁹⁵ Treaty of Amsterdam (amending the Treaty on European Union, the Treaties Establishing the European Communities and Related Acts), Official Journal of the European Union C 340, 10 November 1997, <http://europa.eu.int/eur-lex/en/treaties/dat/amsterdam.html>.

⁹⁶ European Council Regulation (EC) No 2725/2000 of 11 December 2000 concerning the establishment of Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention (http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32000R2725&model=guichett). See: also Council Regulation (EC) No 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002R0407&model=guichett

⁹⁷ European Council Regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, http://eur-lex.europa.eu/LexUriServ/site/en/oj/2003/l_050/l_05020030225en00010010.pdf

Challenges and potential barriers faced

To be successful, Eurodac needs to record the number of asylum requests, the person behind the request and an indication of the place where the request for asylum took place. The project looked to the provisions of the Dublin Convention to help identify ways of clarifying and addressing the complex issues likely to emerge when implementing this new system.

Eurodac's expectation at its outset was that the countries involved would be successful in acquiring fingerprint data. The main technological problems foreseen related to sending this data to the Central Unit, where it could be shared with other States in the initiative. Additional implementation challenges were posed in the form of judicial and coordination issues concerning privacy and the differences in regulations between participating countries.

The sensitive nature of the identity-revealing data to be kept in the Eurodac database makes privacy a significant challenge, as it might make Member States somewhat reluctant to share all of their data. Regulations regarding such data vary greatly across Eurodac's participating States, which could create obstacles to the effective cooperation that is vital to the success of this project.

The transfer of identity data has always been a sensitive subject, particularly when it is shared across areas as large as that covered by Eurodac. The collection of fingerprints can be considered a privacy infringement because of its connection with criminal investigations. For example, a recent inquiry into asylum applications centres (COA) in the Netherlands established that asylum seekers are still uncomfortable with the obligation to allow their fingerprints being taken.⁹⁸ Another key Eurodac data collection issue is the significant distance that has to be travelled before the information reaches the Central Unit, which could pose a problem in keeping Eurodac up-to-date. Such obstacles can be addressed using digital network solutions such as e-mail and direct data transfer. However, these methods need to be protected from external interference to safeguard the sensitive data. For this reason, Eurodac contains only fingerprints and identification numbers, but no further personal information such as name, address, etc.

Another problematic area requiring much attention is the role of 'transit countries'⁹⁹, the Member States on the external borders of the EU where asylum seekers first enter the Union and to where they can be returned by other countries because they are where the asylum request was first lodged. Such countries are faced with significant financial and administrative burdens in dealing with these applicants, while often seeing little benefit in return for participating in Eurodac. Gaining the commitment of these transit countries to providing comprehensive, timely and accurate data is therefore crucial to the success of the system.

The Eurodac Central Unit collects fingerprint data from asylum seekers, irregular border-crossers and "illegal" residents over the age of fourteen. Some transit (border) countries, like Greece and Italy, undermined the Dublin II and Eurodac regime by transmitting only very few fingerprint data from irregular border-crossers very late to the Central Unit of Eurodac (Aus 2006). In 2004, Greece waited on average more than 29 days before transmitting its data. As a result, the would-be refugee had four weeks to lodge a potentially successful application for asylum in another Member State. This type of behaviour by transit countries can be explained by a game theory, called the Rambo-situation (Aus 2006:13). In this, a transit country, such as Greece, is seen as an 'upper-lying' (Rambo-like) state, while destination countries, like Germany and the Netherlands, are 'lower-lying' states (underdogs). It is very difficult for the underdog to convince Rambo of the need to participate in the Eurodac regime.

There are at least two ways of persuading 'Rambo' transit countries to cooperate (Aus 2006: p.13). Firstly, disadvantaged 'underdog' destination countries can try to improve their lot by making 'threats' and seek to decrease the utility of defection for transit countries. Second, the disadvantaged countries can make 'promises' and try to increase the utility of cooperation for transit countries. The aim is to create "collective action" (Holzinger, 2003) that achieves and distributes some gain through coordination or cooperation by the joint actions of a number of 'players' in the

⁹⁸ NRC (newspaper), 6 February 2007.

⁹⁹ For example, a large number of asylum seekers enter the EU via transit countries in southern Europe, such as Greece, Italy, Spain and Portugal,

game. Difficulties in achieving the goals of collective actions can be caused by the strategic constellations of the actors (Member States). This results in 'collective action problems', like distribution, defection, coordination, disagreement and instability difficulties. These problems can be resolved, for example by altruism, norms, focal points, correlated strategies, collective decision-making, external power and sanctioning. 'Political' solutions, like decision-making or enforcement, can resolve all types of problems. 'Motivational' solutions can solve some of the problems, and 'rational expectation' solutions can solve some types and help to solve others (Holzinger 2003).

The way the budget for Eurodac would be established and developed was not clear when the project began. However, the technical feasibility study preceded the political assessments of the project's desirability and appropriateness. Discussions on technical requirements started in December 1991, but it was only in 1996 that the political discussions began (Aus 2006). The underlying computerized system to be used for the automated registration of fingerprints in Eurodac already existed when the project began to be implemented. Nevertheless, the use of biometrics in such a system was still relatively novel in 2000, when Eurodac was considered to represent the first application of biometric identification technology within a supranational political entity (Aus 2006).

Adoption and implementation of Eurodac

The Geneva and Dublin Conventions, to which Eurodac participating countries are signatories, makes the State where an asylum claim is lodged responsible for examining the application. To apply the Dublin Convention, it is necessary to establish the identity of applicants for asylum and of persons apprehended in connection with the unlawful crossing of the EU's external borders. Each Member State should also be allowed to check whether a third country national found illegally on its territory has applied for asylum in another Member State.

Member States decided to use fingerprints to meet these objectives as they constitute an important element in establishing the exact identity of a person. Eurodac emerged from the resultant need to collect, store and communicate fingerprint data efficiently and reliably to enable the data to be assessed and compared. However, as will be explained below, transit countries do not always fully comply with the relevant Eurodac regulations because of the high workload and extra administrative and financial burdens they impose.

As stated above, Member States were aware that the collected data should be protected by privacy regulations, so that the data would not fall in to unauthorized hands. When Eurodac was implemented, Member States realized that they had to take this challenge into account.

The main players in Eurodac are the European Commission, which initiated and manages the project, and the EU Member States, which are covered by its database (plus Norway and Iceland). The Commission also established and manages the Central Unit that controls the Eurodac database. The Member States are responsible for the data delivery. This has involved establishing internal organizational structures that enable interworking between peripheral (border) offices where much data is collected from individuals crossing borders, and the relevant National Central Office coordinating data collection in that State. To ensure the reliability of the project and its systems, Member States agreed that there should be an annual evaluation of it (see European Commission 2004; 2005; 2006; 2007).

As indicated by the timeline above, the Eurodac project did not come about overnight. There were also some start-up problems. One of the early difficulties was that the structure of the Community changed after Eurodac had emerged following the Dublin Convention in 1990. This restructuring involved new countries with varying needs seeking accession to the EU. This led to the project being put on hold until the EU structure settled down again.

Project Design

Policy Decisions

Key decisions affecting the project and systems design arose from the European Council Regulation in 2000 setting up Eurodac, which defined the scope of its responsibilities. Discussions

on the inclusion of Norway and Iceland and negotiations on the participation of Denmark¹⁰⁰ were also important influences on the design.

A vital design requirement was to protect the fingerprint data from being accessed by those without the authority to do so. To address this, the European Commission formulated a Council Regulation in 1999, which was later amended by the European Parliament.¹⁰¹ This requires Eurodac data to be masked and deleted after the asylum applicant has been: legalized; issued with a residence permit; left the territory of the Member State; or acquired the citizenship of one of any Member State.

No great obstacles arose with regard to the legislative aspects in the development and operation of Eurodac. However, there was an explicit emphasis during negotiations to establish Eurodac that its database could be used to implement only the relevant regulations relating to the Dublin Convention, and not for other purposes. For instance, Eurodac may not be used for “the functioning of other international instruments” or “starting criminal investigations against asylum seekers”.¹⁰²

The Commission also continues to insist that the system’s search function should be used only for transactions foreseen by Article 18 Paragraph 2 of the Eurodac Regulation 2725/2000 of 11 December 2000, which reflects data protection rules safeguarding the rights of the data subject to access his/her own data. These provisions offer the ability to conduct “special searches”: access by the data subject to view any communication of the data relating to him/her recorded in the central database and of the Member State that transmitted them to the Central Unit. Such special searches take place only when requested by the person whose data are stored in the central database.

The Eurodac information system

The Eurodac Central Unit was set up in the European Commission via a Restricted Call for Tender (DG JAI A2/2000/A2), which resulted in a contract being signed between the Commission and the successful tenderer in March 2001. The Call for Tender was to implement an automated fingerprint information system (AFIS) that was capable of handling 7,500 transactions per day (500 transactions per hour) with an availability of 99.9%. It needed to deliver greater than 99.9% certainty of accuracy for all returned submissions, with a probability of less than 0.5% of missing a match where a match should happen. Another requirement was that the database had to be capable of storing up to 800,000 full ten-print images per year. In addition, the contract included the delivery of a reference client that could emulate a Member State to prove that the AFIS was capable of handling transactions from a Member State for all data types.

System Management Tools have been implemented to help the Central Unit monitor the activities of the AFIS and produce statistics to match the regulatory statistical requirements. The Monitoring System also had to include a logging capability to track the activities of the Central Unit. In addition, a Business Continuity System (BCS) was established as a backup if the Central Unit becomes unavailable. The BCS also has testing capabilities to allow Member States or Accession Countries¹⁰³ to test any new solutions being implemented at a National Access Point, in order to prevent problems arising with the ‘live’ Central Unit.

The network infrastructure that links the Central Unit to the National Access Points is provided through the Trans-European Services for Telematics between Administrations (TESTA II) network, a Generic Service of the European Commission’s Interchange of Data between Administrations (IDA) programme¹⁰⁴. This is an encrypted private network for public administrations, offering a

¹⁰⁰ European Council Decision (EC) No 2006/188/EC of 21 February 2006 on the conclusion of the Agreement between the European Community and the Kingdom of Denmark extending to Denmark the provisions of Council Regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national and Council Regulation (EC) No 2725/2000 concerning the establishment of Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006D0188:EN:HTML>

¹⁰¹ See European Commission (1999) and European Parliament (1999).

¹⁰² Legal Service of the Council, Advice 18 March 1993, 5546/93, JUR 25.

¹⁰³ Countries applying for membership of the EU before their application is approved.

¹⁰⁴ See: <http://europa.eu/scadplus/leg/en/lvb/l24147a.htm>

secure telecommunications infrastructure based on IP networking, similar to the Internet. Security is an important element of all data transmission and this is ensured by using the TESTA network and the use of Public Key Infrastructure (PKI) services, also provided through the Generic Services of the IDA Programme.

Impacts of Eurodac

In the various annual evaluations by the European Commission (2004; 2005; 2006; 2007), the general conclusion has been that the Central Unit has produced very satisfactory results in terms of speed, output, security and cost-effectiveness. There are, however, concerns about excessive delay in the transmission of data from several countries to the Central Unit and the low quality of this data. These problems have been addressed in cooperation with the responsible Member States.

Despite these reservations, the evaluations have found that Eurodac has generally met its broad original policy goals of supporting the application of the Dublin Regulation and establishing mechanisms and criteria to determine which Member State is responsible for examining an asylum application lodged in a Member State. For example, the annual evaluation reports show that in 2004 only 17,287 people were found to have lodged a double application, but in the subsequent two years 31,307 and 31,636 third-country nationals lodged a double application. It has also assisted in monitoring and helping to reduce the 'asylum shopping phenomena', where asylum seekers move around between countries to find a point of access. In addition, Eurodac has facilitated the harmonization of Member States' asylum policies and fostered stronger co-operation among its participating States on asylum matters.

The Eurodac system's focus on exchanging electronic data about asylum applicants has also forced the States involved to adapt their old processes to the new technology in order to achieve gains in increased speed, accuracy of information flow and security in government processes. This has resulted in the peripheral (border) offices in several countries being provided with the electronic equipment needed to capture relevant data quickly for transmission to the relevant National Central Office and, from there, to the Eurodac Central Unit. This has significantly improved the quality and speed of the overall process. Moreover, because of the sensitive nature of the information, security was also improved.

Eurodac also meant a change in policy processes. The benefits resulting from this include the harmonization of Member States' asylum policies and a convergence towards a Common European Asylum Policy.¹⁰⁵

Factors affecting this case of significance to wider eGovernment initiatives

The seven barrier categories

The Breaking Barriers Project, funded by the EC, identified and explored the key barriers to eGovernment in Europe. The project team proposed seven key barrier categories of obstacles to eGovernment progression. The categories are intentionally broad and tied to a multitude of more specific barriers relevant at different governance, institutional and jurisdictional levels. This categorization is particularly valuable when discussing the barriers relevant to this case which may have relevance for other eGovernment initiatives. In summary the barriers are: leadership failures, financial inhibitors, digital divides and choices, poor coordination, workplace and organizational inflexibility, lack of trust and poor technical design¹⁰⁶.

¹⁰⁵ For more details of the EU policy towards a Common European Asylum System, see: http://ec.europa.eu/justice_home/fsj/asylum/fsj_asylum_intro_en.htm

¹⁰⁶ For more details about the Breaking Barriers to eGovernment project please see <http://www.egovbarriers.org>

The following are the main issues that arose during the implementation of Eurodac and that are of relevance to the seven barrier categories identified by this Breaking Barriers to eGovernment project (no new barriers were detected in this case study outside these categories):

Leadership failures: No significant leadership failures occurred, as all participating States saw Eurodac as a necessary and logical result of the Dublin Convention. Moreover, it was in each State's interest to make this project work because it would give them a clearer picture of the facts of illegal immigration and asylum seeking across Europe, and how arising problems could be solved at European and Member State levels. Eurodac has greatly benefited from the way participating States cooperated to make the project work. This attitude made it possible for States to register third-country nationals, giving them a better picture of their location and movement in their country and across Europe. Without this political leadership, the project would never have even begun. The management of Eurodac's Central Unit by the European Commission also proved to be the appropriate level of authority.

Financial inhibitors: The four annual reports on Eurodac (European Commission 2004; 2005; 2006; 2007) discuss the cost effectiveness of Eurodac. The costs of Eurodac are spread between an EU-level contribution and each participating State, which carries most of the costs. This has been one factor in problems that have arisen with the transit countries who perceive they have an unfair share of the financial burden. As it is reported in each Annual Report (2004-2007) on the activities of the Eurodac Central Unit, the Community generated savings for national budgets by using common available communication infrastructures. The fourth annual report (11 September 2007) analyses that savings for the Member States have been generated because the Community covered the costs for the communication and security services for the exchange of data between the Central and the National Units.¹⁰⁷ This is a result of using the common available infrastructures, like the aforementioned TESTA network. Furthermore, the fourth annual report shows that, after four years of operations, the total amount of € 7,8 million was spent on all externalised activities specific to Eurodac. In 2006, the costs for maintaining and operating the Central Unit were € 244.240,73.

Digital divides and choices: The main problems arising here are related to differences between Member States with regard to the knowledge these countries have about the technology being used and their further development. These differences could also be relevant for the workplace and organizational Inflexibility barrier category.

Poor coordination: This has been one of the most difficult barriers for Eurodac to overcome as there are many differences in regulation between the various Member States in their handling of asylum applications and immigration. The project's focus on the identification of persons and the encoding, storage and management of related data on a computer database makes coordination across States a particularly sensitive issue. Although fast communication and high quality data are essential to the correct functioning of Eurodac, some countries are somewhat reluctant to send the fingerprint data in time. As a result, the information could be outdated, leading to a third-country national entering country X by the time the Central Unit receives the relevant data from country Y, where the person also requested asylum. The negative overall impact on transit countries of the use of Eurodac means they may have little or no interest in bearing the administrative burdens of asylum requests. As Aus (2006) has commented: "The unilateral political and administrative benefits of not being held responsible for processing the asylum requests of tens or even hundreds of thousands of irregular border-crossers each year are apparently valued higher than the costs of sustained non-compliance with Community law".

Workplace and organizational inflexibility: The cultural differences between the various parties in the project have sometimes formed an obstacle to the transmission of the fast and accurate data communication that is essential to efficient administrative and the organizational adaptation necessary to make optimum use of the Eurodac system. For instance, the significant growth in

¹⁰⁷ European Commission (2007), Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2006. Commission Staff Working Paper SEC(2007) 1184, Brussels: European Commission, 11 September 2007, p. 5
http://ec.europa.eu/justice_home/doc_centre/asylum/identification/doc/sec_2007_1184_en.pdf

administrative workload in transit countries due to conforming with Eurodac regulations can have negative impacts on the staff processing the paperwork. Another problem is that there are still a lot of rejections caused by low quality fingerprint data because of poor training of operational staff.

Lack of trust: To help overcome obstacles resulting from concerns about the misuse of sensitive personal identification data, it has been important to Eurodac's operation to be transparent in meeting best practice in data protection standards, such as through monitoring by the EDPS. It is also important that Eurodac provides a systematic notification of the deletion or protection (masking) of information in its database when that is being used at crucial stages in an asylum seeker's progression, such as acceptance as a refugee or eventual naturalization as a citizen of a country.

Poor technical design: AFIS is a typical fingerprinting tool used widely for police and justice activities and Eurodac benefits from being able to base its technical capability on these well tried and understood tools and techniques. In general, Eurodac software development was able to draw on much existing experience collecting, managing and communicating fingerprint data to help it avoid significant technical design problems.

Legal factors

There are several legal issues related to Eurodac that centre on the protection of the privacy-sensitive data it holds and manages:

- Protecting the privacy rights of third-country nationals: One key concern relates to Eurodac's core functions of systematic collection, central storage and transnational exchange of biometric data. This constitutes a violation of the rights of the third-country national concerned under the European Convention on Human Rights (ECHR).¹⁰⁸ The ECHR's case law sheds light on the exceptional circumstances under which such practices may be justifiably undertaken for the maintenance of law and order, internal security, etc. For instance, national authorities are allowed, in special circumstances, to submit "special searches", that we mentioned above.
- Data deletion: Concerns exist about the deletion of data in accordance with Eurodac's rules. Technical and practical difficulties hinder the systematic notification to delete or mask data in Eurodac because of the naturalization of an asylum applicant or when the asylum applicant is recognized as a refugee.
- National level: It has been very difficult, perhaps impossible, for the Commission, Central Unit or EDPS to control which national authorities gain access to personal information registered in Eurodac. One major reason for this is that Eurodac holds data in the personal and politically sensitive area of asylum seeking, including political refugees fearing prosecution from the countries they come from.
- European level: Legal concerns at a European level about Eurodac.

Legal concerns at a European level about Eurodac include (1) Plans for interoperability with the Visa Information System (VIS)¹⁰⁹ and Schengen Information System (SIS II)¹¹⁰ and (2) the implications of a proposal in December 2006 by the German Presidency of the EU to make Eurodac accessible for police and law enforcement authorities. This stated that a proposal was being

¹⁰⁸ This relates to Article 8(1) of the ECHR giving everyone the right to respect for a private and family life, home and correspondence (see: <http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/EnglishAnglais.pdf>).

¹⁰⁹ VIS consists of: the Central Visa Information System (CS-VIS); and an interface in each Member State, the National Interface (NI-VIS) which provides the connection to the relevant central national authority of the respective Member State, as well as the communication infrastructure between CS-VIS the NI-VIS interfaces (see: <http://ec.europa.eu/idabc/en/document/2186/330>).

¹¹⁰ The Schengen Information System (SIS) is an information system that allows the competent authorities in the Member States to obtain information regarding certain categories of persons and property (see: <http://europa.eu/scadplus/leg/en/lvb/l33183.htm>).

prepared “for a Council decision concerning access to Eurodac by Member States’ police and law enforcement authorities for the purposes of preventing, detecting or investigating criminal offences, in particular terrorist offences.”¹¹¹ This justified extending Eurodac’s use by stating: ‘Frequently, asylum-seekers and foreigners who are staying in the EU unlawfully are involved in the preparation of terrorist crimes, as was shown not least in the investigations of suspects in the Madrid bombings and those of terrorist organizations in Germany and other Members States...’.¹¹² Although this specific German proposal might be withdrawn, this phrase directly linking third-country nationals (both legally and illegally resident within the EU) to acts of terrorism is worrying, as it could imply EU measures or policies in the field of Freedom, Security, and Justice are based on the general presumption that migrants within the EU are to be treated as suspected terrorists. Such a policy would run against the generally accepted principles in EU law of non-discrimination and equality. It could also have a negative impact for the position of migrants and their further integration into the society of EU Member States. The invitation by the JHA Council has resulted in a note by the Standing Committee of Experts on International Immigration, Refugee, and Criminal Law (Commissie Meijers) to Vice President Franco Frattini of the European Commission,¹¹³ and a letter to Mr. Jacques Verraes, Directorate D: Internal Security and Criminal Justice of the European Commission.¹¹⁴ The Standing Committee strongly advises against the intended legislation to amend the Eurodac regulation because it would be unlawful and thus would risk to be annulled by the Court of Justice.

There are five core arguments why the intended legislative measures would be unlawful:¹¹⁵

- Access to Eurodac data for law enforcement authorities would be irreconcilable with the present purpose limitation of the Eurodac regulation
- There is no legal basis in the EC Treaty for extending the purpose with security purposes
- The purpose extension would be incompatible with obligations under international treaties ratified by all Member States and with relevant principles of Community Law, the observance of which the Court of Justice ensures
- Data protection authorities lack sufficient means to protect the rights of asylum seekers
- The proposal will affect the integrity of Eurodac.

Relative influence of eGovernment challenges

On a 100% scale, the following are approximate relative levels of influence on Eurodac of some key factors that could affect eGovernment projects:

- Political factors (35%): The main political obstacles came from some objections in transit countries. The negative overall impact on them of the use of Eurodac means they may have little or no interest in bearing the administrative burdens of asylum requests. As Aus (2006) has commented: “The unilateral political and administrative benefits of not being held responsible for processing the asylum requests of tens or even hundreds of thousands of irregular border-crossers each year are apparently valued higher than the costs of sustained non-compliance with Community law”.

¹¹¹ European Council Document 16982/06, 20 December 2006,

<http://www.statewatch.org/news/2007/jan/eurodac-16982-06.pdf>

¹¹² European Council Document 17102/06, 22 December 2006, p. 6.

<http://www.statewatch.org/news/2006/dec/eu-german-pres-policing-agenda.pdf>

¹¹³ Standing Committee of Experts on International Immigration, Refugee, and Criminal Law, ‘Note on the proposal of the JHA Council to give law enforcement authorities access to Eurodac’. Utrecht, the Netherlands, 18 September 2007, CM0712-IV.

¹¹⁴ Standing Committee of Experts on International Immigration, Refugee, and Criminal Law. ‘Letter regarding the Proposal to give law enforcement authorities access to Eurodac’. Utrecht, the Netherlands, 6 November 2007, CM0714.

¹¹⁵ See also the website of the Standing Committee:

<http://www.commissie-meijers.nl/commissiemeijers/pagina.asp?pagkey=37264>

- Legal factors (40%): This is related mainly to the protection of privacy rights of third-country nationals, the non-deletion of data in accordance with Eurodac's rules, the lack of control over national authorities who gain access to personal information in Eurodac, plans for the interoperability of Eurodac with the Visa Information System (VIS) and the Schengen Information System (SIS II), and the linking of third-country nationals to acts of terrorism, as a result of the expected proposal to make Eurodac accessible for the police and other law enforcement authorities.
- Financial (10%): The fourth annual report (11 September 2007) analyses that savings for the Member States have been generated because the Community covered the costs for the communication and security services for the exchange of data between the Central and the National Units.¹¹⁶ This is a result of using the common available infrastructures, like the aforementioned TESTA network. However, there is a financial discussion because transit countries perceive that they have an unfair share of financial burden.
- Social and economic issues (10%): Burden-sharing and variable administrative resources and reception capacities could be significant activities in meeting the concerns of transit countries. For example, sharing the economic burden of administrative procedures and capacities for the reception of refugees between all countries could help to promote cooperation and compliance by the transit countries.
- Technological issues (5%): AFIS is a typical fingerprinting tool used widely for police and justice activities and Eurodac benefits from being able to base its technical capability on these well tried and understood tools and techniques.

Conclusions

The original expectations about areas where the project was likely to be successful were generally met, such as in political leadership and technical performance and security measures. However, there are some obstacles that proved to be problematic because they reflect different interests, regulations and mentalities of participating countries. For instance political and economic consideration among transit countries have proved to be a constraint, as they have led to such countries seeing Eurodac as a burden, not a benefit.

Privacy, communication, legal adaptation and coordination have been the key words in this project. The privacy of third-country nationals remains a major unresolved issue. The States participating in Eurodac must ensure that this sensitive data does not fall into unauthorized hands. To do this, they have to take the necessary measures (e.g. adaptation of privacy regulations and improving computer system security). However, if something like the 2006 German proposal mentioned above (in the subsection Legal factors) is ever implemented, it would give law enforcement authorities across Europe access to Eurodac. This could be an infringement of the 'purpose limitation' principle in data protection regulations, and could strengthen the idea that immigrants or asylum applicants should be considered as possible terrorists or criminals. Legal issues concerning privacy remain a major barrier yet to be fully overcome in relation to third-country nationals.

Effective communication between participating States and the Central Unit is essential to the successful functioning of Eurodac. This will mean coordination of the various data to meet the needs of Member States also becomes more effective. Problems concerning coordination and workplace inflexibility also continue, often because of great variations in the workings, institutions and cultures of different Member State.

¹¹⁶ European Commission (2007), Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2006. Commission Staff Working Paper SEC(2007) 1184, Brussels: European Commission, 11 September 2007, p. 5
http://ec.europa.eu/justice_home/doc_centre/asylum/identification/doc/sec_2007_1184_en.pdf

References

- Aus, J. (2006), Eurodac: A Solution Looking for a Problem? European Integration online Papers (EIoP), Vol 10 (2006), 21 July. <http://www.arena.uio.no/publications/>
- European Commission (1997), Convention Determining the State Responsible for Examining Applications for Asylum Lodged in One of the Member States of the European Communities – Dublin Convention, Official Journal of the European Union C 310, 19 August, pp. 0001 – 0012, [http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=41997A0819\(01\)&model=guichett](http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=41997A0819(01)&model=guichett)
- European Commission (1999), Proposal for a Council Regulation (EC) concerning the establishment of 'Eurodac' for the comparison of the fingerprints of applicants for asylum and certain other aliens, Brussels: European Commission, May 26, COM(1999) 260 final, http://ec.europa.eu/justice_home/doc_centre/asylum/identification/printer/doc_asylum_identification_en.htm
- European Commission (2004), First Annual Report to the Council and the European Parliament on the Activities of the Eurodac Central Unit, Commission Staff Working Paper SEC(2004) 557, Brussels: European Commission, 5 May 2004 http://www.libertysecurity.org/IMG/pdf/first_annual_report_eurodac_2004.pdf
- European Commission (2005), Second Annual Report on the Activities of the Eurodac Central Unit, Commission Staff Working Paper SEC(2005) 839, Brussels: European Commission, 20 June 2005 http://ec.europa.eu/justice_home/doc_centre/asylum/identification/doc/sec_2005_839_en.pdf
- European Commission (2006), Third Annual Report to the Council and the European Parliament on the activities of the Eurodac Central Unit, Commission Staff Working Paper SEC(2006) 1170, Brussels: European Commission, 15 September 2006 http://ec.europa.eu/justice_home/doc_centre/asylum/identification/doc/sec_2006_1170_en.pdf
- European Commission (2007), Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2006. Commission Staff Working Paper SEC(2007) 1184, Brussels: European Commission, 11 September 2007 http://ec.europa.eu/justice_home/doc_centre/asylum/identification/doc/sec_2007_1184_en.pdf
- European Parliament (1999), Report on the proposal for a Council regulation concerning the establishment of 'Eurodac' for the comparison of the fingerprints of applicants for asylum and certain other aliens, Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, Rapporteur: Hubert Pirker, November 11, A5-0059/1999 final, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-1999-0059+0+DOC+PDF+V0//EN&language=EN>
- Holzinger, K. (2003), The Problems of Collective Action: A New Approach. Preprint aus der Max-Planck-Projektgruppe Recht der Gemeinschaftsgüter, Bonn 2003/2, http://www.coll.mpg.de/pdf_dat/2003_2.pdf
- Other sources of information relevant to Eurodac*
- Aus, J. (2006), Eurodac: A Solution Looking for a Problem? Working Paper No. 9 May 2006 <http://www.arena.uio.no/publications/>
- Aus, J. (2006), Logics of decision-making on community asylum policy. Working Paper No. 3, February, <http://www.arena.uio.no/publications/>

European Parliament A-series, Commission-report fifth Parliamentary period, A5-0219/2000,
<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2000-0219+0+DOC+PDF+V0//EN&language=EN>

European Parliament A-series, Commission-report fifth Parliamentary period, A5-0059/1999,
<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-1999-0059+0+DOC+PDF+V0//EN&language=EN>

Standing Committee of Experts on International Immigration, Refugee and Criminal law,
<http://www.commissie-meijers.nl/commissiemeijers/pagina.asp?pagkey=37264>

Interviewees: Mrs. Evelien Brouwer (Centre for Migration Law, Radboud University Nijmegen, the Netherlands, now working for the Institute for Constitutional and Administrative Law, Utrecht University, the Netherlands), Employee (European Commission, DG Justice, Freedom and Security, Unit B2: Immigration and Asylum, Brussels, Belgium), Mr. Jonathan Aus (ARENA - Centre for European Studies, University of Oslo, Norway).

Case study: X-Road: An Interoperability Framework for eAccess to Registers in Estonia

Chris Parker

Gov 3 Ltd, an eGovernment Consultancy, UK

Definition of the case study

The X-Road project¹¹⁷ was launched in 2001 with the main objective of guaranteeing the delivery of a web-based service to enable citizens, businesses and government servants to access nearly one hundred governmental databases and registers. The institutions responsible for the larger registers had previously started to develop web services for citizens, but the results of these earlier projects varied greatly. This led to similar services having significant differences (e.g. in user interfaces; agreements between the database user and the authority responsible for the register; and authentication services). All these problems encouraged the project leaders to develop a new general solution, which was carried out by the X-Road project within the Estonian Interoperability Architecture guidelines¹¹⁸.

In the context of the EU, which Estonia joined in 2004, a key objective was to implement the free movement of information across national borders to support the free movement of goods, people, etc within the Union. Good examples of this potential are the possibility of linking Estonian eServices with pan-European developments such the Schengen Information System¹¹⁹ and EUCARIS¹²⁰ European car registration centre.

The user groups targeted by X-Road's eServices are:

- Citizens¹²¹: Giving access to the personalized data recorded by state institutions in different databases, with about 70 registers connected to the common architecture in April 2007.
- Businesses: The management of businesses can obtain a list of available eServices customized for their needs.
- Government institutions: Probably the most active group of X-Road users.

Setting of the X-Road case study

Implications of the Estonian Database Act

According to the Estonian Databases Act¹²², which came into force in April 1997, state registers in the country operate under different ministries. There are more than 200 different official registers. About a hundred are considered to be the most important, including the registers covering: Population; Business; Land; and Cars. Most registers work under the relevant ministries, boards, inspectorates and municipal governments. However, there are a few ministries where the technical and organizational environments for some registers are centralized (e.g. the Centre of Registers

¹¹⁷ For information about project X-Road (in English) see: <http://www.ria.ee/27309>

¹¹⁸ See: <http://www.riso.ee/en/information-policy/interoperability>

¹¹⁹ The Schengen Information System contributes to the implementation of provisions on the free movement of persons within the EU and in judicial cooperation in criminal matters and police cooperation (see: <http://europa.eu/scadplus/leg/en/lvb/l33183.htm>).

¹²⁰ See: www.eucaris.net

¹²¹ The citizens' portal (entrance to the X-Road environment) is at: www.eesti.ee

¹²² For details of the Act (in English), see: <http://www.riso.ee/en/node/40>

and Infosystems in the Ministry of Justice¹²³). Several state registers are also outsourced to private companies.

The centralization of registers is not possible and reasonable for several reasons. Each ministry is relatively independent in their decision making processes and work principles. Cross-government cooperation is complicated, which is a particularly strong obstacle in this kind of ePublic Service. In addition, 'info-political' considerations are against centralization, such as special personal data protection principles that make centralization more complex. Centralization of some databases in a few ministries were driven only by pragmatic considerations, and so cannot be considered as typifying general considerations about systems based on the centralization of registers.

The Databases Act defines a general (or basic) categorization for national registers (e.g. relating to Population; Legal Persons; Immovable Property, State Assets). In addition to the general national registers, there are also State registers (databases established by the Government to meet a law or international agreement and which are necessary to perform the functions of one or several ministries); other state agency databases; and local government databases. These register categorizations have been based of a process of establishment (by Law, by Act of Ministry or Local Government etc.), which takes account of the relevant Scandinavian practice in this field.

At the start of 2007, the categorization was changed and the new Law (Public Information Act) does not emphasize the establishment process and the status of registers but rather the importance of basic data rather than the Basic Register as such. This indicates that the same organizational, legislative and technical barriers are relevant for most state databases, not just basic registers. This case study is therefore of wider relevance than only the kinds of registers connected within X-Road.

Milestones in the development of X-Road

X-Road pilot projects started in 2000 and the first operational model began in December 2001. The initial test focused on queries from different Police databases, which ensured special attention was given to guaranteeing the rules of personal data protection for citizens. The mass use of services was launched at the end of 2002, by when Estonian digital ID-cards were available. By April 2007, X-Road offered several hundred eServices for different user groups.

The X-Road development was initiated in the Department of State Information Systems in the Ministry of Economic Affairs and Communications¹²⁴. The development was subsequently transferred to the Estonian Informatics Centre¹²⁵. The project is continuously developing because of the changes in technology, new needs of partnering organizations, etc. The main development work has been undertaken by the private sector, with some support from ICT specialists in public institutions.

One of the main driving forces was the lack of money in state budgets. The very different technical and organizational environments involved would have made it extremely expensive and complicated to build multiple front offices, user identification mechanisms and a large number of interfaces between state registers.

Challenges and potential barriers faced

The main potential barriers foreseen when planning the project were organizational and legislative. For instance, one of the info-political issues addressed was the difficulty of trying to make the register integration process compulsory. Some attempts to do this using legislation had not worked;

¹²³ Other examples of register centralization are some databases of the Ministry of Agriculture's Registers and Information Board and in the Estonian Motor Vehicle Registration Centre in the Ministry of Economic Affairs and Communications.

¹²⁴ By the Estonian Government of Republic Act, this Ministry is responsible for the general coordination of state information systems in Government. Six people work in this department in April 2007. See www.riso.ee for more details of its activities.

¹²⁵ Six people were permanently engaged with this application in April 2007 (see www.ria.ee for more details of its activities).

neither had separate agreements between ministries on how they would join their registers to a single eService environment.

The X-Road concept was innovative. The basic idea was to avoid destroying the existing situation in back-offices dealing with registers, while better integrating the way that users engaged with them. This was thought to be important because the state registers operate under different ministries and their organizational, fiscal and technical environments and models are different. A focus mainly on the data exchange architecture would allow different ministries and separate registers to have their own technical platforms where required, but within a consistent and coordinated architectural framework. Although a few registers could retain separate front-offices, most were expected to connect to the single X-Road 'middleware' and offer eServices through it. This is what has occurred.

The sensitive nature of much information in the registers included within X-Road led to the development and implementation of a personal data protection concept which allows everyone to check their own data and to know who is using this information. This was designed to help build trust among users, while fulfilling the public authorities' legal regulations.

Adoption and implementation of X-Road

Key players and their roles in the project's creation and implementation

The key players¹²⁶ behind X-Road included: the Department of State Information Systems (RISO)¹²⁷, specialists from the Estonian Informatics Centre that works under the Ministry of Economic Affairs and Communications; IT managers from other public institutions; private businesses; and universities. RISO is responsible for general coordination, initialization of the project, main visions and ICT architecture design; the Informatics Centre for implementation, including leading the practical integration process; the IT managers and administrators of main ministries for dealing with issues relating to the registers issues; and the main development work on X-Road and individual registers was done by private companies (e.g. AS Cell Networks and AS Cybernetica). There are no financial commitments between the public sector partners.

The major decision-makers who actively influenced the projected design were: RISO's ICT systems architect and its Head of Department; the project manager from X-Road Centre in the Informatics Centre; and system designers from Cell Networks and Cybernetica. An example of a state institution X-Road partner is the Centre of Registers and Infosystems under the Ministry of Justice¹²⁸, which includes the Business Register, Titlebook Register (part of the real estate information system), Ships Register and Marital Property Register. It was created at the beginning of 2006 during the organizational process that merged the registers in the Ministry of Justice.

Addressing initial problems

The initial understanding was that it would be easy to implement the required eServices as soon as the technical platform was operational. The general understanding among different stakeholders today is that the establishment of the basic platform was only the beginning of a complicated eService implementation process, where the main real problems are non-technological.

At the time of project's launch, legal regulations regarding access to registers via X-Road were too complicated. This was solved by introducing more flexible technical, organizational and legislative approaches. Another incorrect initial decision was the expectation that most of the development work on local database interfaces would be done by the same company that had undertaken the main X-Road development. As soon as more developers (both from private and public sectors) were trained, the efficiency of operational access increased. There was also a recognition that more

¹²⁶ This case study is based on interviews with experts from some of the main stakeholders in public institutions. A main author of this study was also involved from the start in X-Road's strategic planning and development.

¹²⁷ At the start of the project this was known as the department of State Chancellery.

¹²⁸ See: www.eer.ee

technical competence should be built into the back-office support. Other initial problems in the process of implementation included: encouraging partners to connect their systems; helping them with technical issues; offering appropriate hardware and software to assist the integration process; and preparing and approving regulations at Government level.

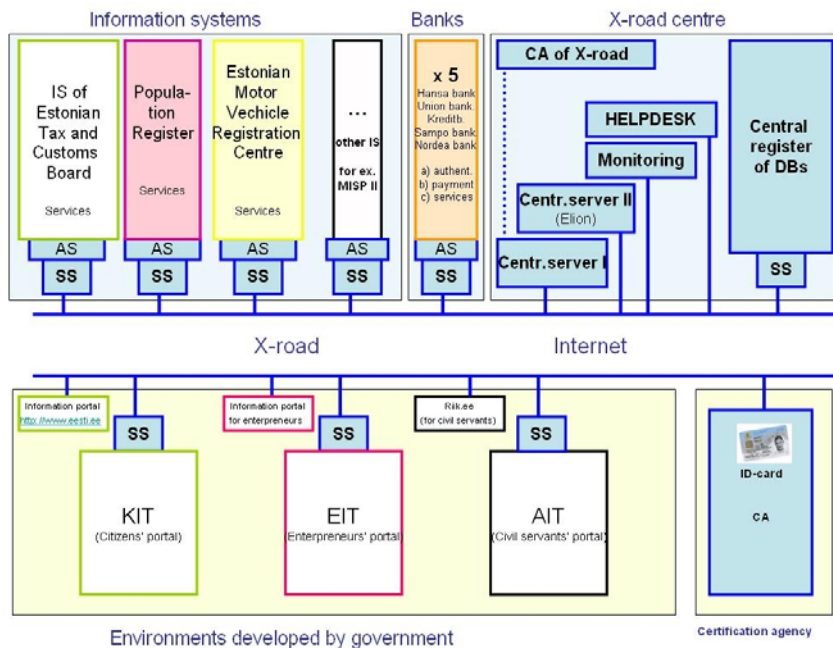
The rate at which registers joined X-Road was slower than expected after the technology was tested and first became available. This was due mainly to organizational obstacles. The general finance model of some registers was also an obstacle in the initial phase of the project. For example, the Population register used a different model to others, which meant it would lose part of its budgeted income after integration with X-Road. This caused the institutions affected to oppose participation. The problem was resolved after a revision to the relevant paragraph in the Population Register Law.

Technologies used to implement the project

X-Road harmonized the register environment within the Estonian Interoperability Architecture¹²⁹. Like other similar national interoperability framework principles adopted by EU countries, this is not a legal regulation or direct eGovernment standard, but forms 'strong recommendations', focused mainly on the public sector. However, as with X-Road, such interoperability frameworks are increasingly incorporating private sector ICT systems.

The schema of the system configuration in Figure 1 shows that all the information systems involved are connected to the X-Road security servers via adapter servers (AS), which converts messages in X-Road XML format to special database query languages (mainly SQL) and from query answers back to XML. The data transfer protocol used in April 2007 was SOAP, together with older XML Remote Procedure Call (RPC) protocols where appropriate.

Figure 1



The X-Road Centre is at the heart of a broader eGovernment environment because all the central servers (e.g. doing central monitoring and certification) of this wider network are connected and located here. The Centre has specialist staff who manage eGovernment hardware, software,

¹²⁹ See: <http://www.riso.ee/en/information-policy/interoperability>

Internet connections, etc. Its management group also organizes relevant courses and seminars and coordinates activities with the EU and other external bodies.

The undertaking of research and development projects by the X-Road Centre is likely to increase. For instance, A new central register of databases added to the Centre at the beginning of 2005 includes not only the description of all Estonian public sector registers and databases, but also collects descriptions of all government eServices in the WSDL (Web Service Description Language) format. This enables the development of different automatic tools by using the library of eServices to automatically generate new ones on the basis of the stored service descriptions.

Project Design

Key design decisions included:

- implementation of the interoperability framework as a foundation building block for public eServices in Estonia;
- use of the open systems concept;
- the guaranteed neutrality of technical platforms;
- a cost model in which the end-user of eServices should not pay for the service;
- development of a single mechanism for authentication and authorization of users; and
- a data-security model that enables everyone to know how his/her data is used by government.

Impacts of X-Road

Overview of outcomes

There is no available detailed study of the impacts of the X-Road project. However, it seems that its aims and visions have been broadly reached. Compared to the original goals, the expectation of its early growth were too optimistic, primarily because of unforeseen difficulties that meant the integration and take-up process took much more time and effort than planned. The main problems were not in the technology but with organizational, legal, financial and motivational aspects.

The main impacts in organizational, legislative and technological terms were in developing a model of cooperation between different state registers that allows fast, inexpensive and very flexible development of different eServices in a secure way that guarantees data protection. Users seem to be generally satisfied, as indicated by its increasing usage profile, rising steadily from 590,337 in 2003 to almost 3 million in 2006, involving more than 12% of the Estonian population in accessing X-Road eServices via different portals. In addition to citizens, about 400 organizations are connected to this environment and around 23,000 entrepreneurs access its business portal.

Uses of this integrated registers system have had strong impacts to the processes in the partner organizations, as well as in the different user organizations. These arise not only in the direct handling of registry tasks, but even more importantly in how the approach adopted has opened opportunities to take a fresh look at the organization and its processes and practices. It was in this way that the implementation of X-Road prepared the ground for administrative reforms and changes in the organizations. Several developments and organizational changes in the Informatics Centre arose from its role as the X-Road Centre in the system's set-up period. And a number of forms of innovative cooperation have been implemented between partnering organizations, which have had indirect impacts to the work of these organizations.

Success factors and factors required a rethink

The main success factors were finding appropriate motivational models for engaging different stakeholders. For instance, the institutions responsible for state registers were attracted by:

- the simple and easy process of integration through the X-Road middleware
- saving money when using shared services (e.g. a single front office; single ID-card based authorization and authentication of users; and special data protection measures)
- technical support and helpdesk advice during the implementation process.

The prime motivations for citizens to access registers using the X-Road environment is that is free, has a simple user interface, employs a unified authentication mechanism and offers a long unified list of the integrated eServices available.

On the technology side, some relatively minor issues needed to be revised during the project. For example, the SOAP data transfer protocol standard was not available and not planned for when X-Road was first conceived. During interviews for this study with government stakeholders, a view was strongly expressed for ensuring basic knowledge about the technology is transferred more effectively to the implementing agency. It was felt the know-how had remained too strongly with the private companies who developed the software for X-Road, particularly in the project's early phase.

As already explained, the rules for accessing and integrating registers had to be made more flexible after initial problems were experienced. Coupled with strong 'idea selling' efforts, this helped to speed the project's progress significantly. The assumption that the different register organizations could leave all technical integration work to one developer was overcome by the special short training courses for the registers' back-office developers, after which the pace of integration increased to a satisfactory level.

Special 'selling' also had to be done to raise awareness of X-Road among senior decision makers.

Legislative changes

The Database Act, Public Information Act and related ministry-level sub-acts formed the overall regulatory environment for the registers system. Some rules of integration of the system and general descriptions of responsibilities and principles of supporting systems were also provided. In addition, principles established in the Personal Data Protection Law also had a significant influence on the development and implementation of the register integration projects. The main problems and discussion in this area were about permission to use a single electronic identification (eID) and the degree to which cross usage of data between different registers should be allowed.

Modifications were made to relevant legal acts during the implementation process. The X-Road project implementation could therefore be seen as helping to create a new legal environment for the registers. Special integration agreements were established to help manage the partners' organizational aspects through an agreed set of common rules.

Factors affecting this case of significance to wider eGovernment initiatives

The Seven Barrier Categories

The Breaking Barriers Project, funded by the EC, identified and explored the key barriers to eGovernment in Europe. The project team proposed seven key barrier categories of obstacles to eGovernment progression. The categories are intentionally broad and tied to a multitude of more specific barriers relevant at different governance, institutional and jurisdictional levels. This categorization is particularly valuable when discussing the barriers relevant to this case which may have relevance for other eGovernment initiatives. In summary the barriers are: leadership failures,

financial inhibitors, digital divides and choices, poor coordination, workplace and organizational inflexibility, lack of trust and poor technical design¹³⁰

The following are the main issues that arose during the implementation of X-Road of relevance to the seven barrier categories identified by the Breaking the Barriers to eGovernment project (no new barriers were detected in this case study outside these categories):

Leadership failures: Top managers were not very seriously engaged, except IT managers. Project management and leadership problems in the launch period were resolved by recruiting a new implementation manager. The value of effective 'selling' of this kind large cross-government project, including to senior managers, was highlighted by the X-Road experience.

Financial inhibitors: Financial issues were not barriers in this case. A stable state budget financing mechanism was functioning and requirements were met within the planned budget, which may have been one reason why the project was not highlighted on senior management's radar.

Digital divides and choices: Careful planning and design of user interfaces, security and privacy processes to boost trust and other user-related issues helped to avoid the emergence of any specific digital divide obstacles in this case.

Poor coordination: The general relevant coordination mechanisms and organizational aspects were achieved within central government ICT services. Coordination between IT managers of public organizations was not the barrier, but some coordination problems arose between general managers of partnering public organizations.

Workplace and organizational inflexibility: This was the main barrier in this project, particularly where internal motivational factors in public sector organizations did not support the kind of changes and innovation represented by the X-Road initiative. As money saving was not a major motivating incentive for public institutions, the main driving forces were probably: the simplicity of integration; provision of help-desk and support from the Informatics Centre; and pressure from related legislation.

Lack of trust: This factor had a minor influence on the success of the project in terms of trust doubts between the partnering organizations, which possibly influenced progress on the integration effort and the take-up speed. The user identification mechanisms were designed to take account of all data security needs, which seem to have help build trust among users.

Poor technical design: The technical design avoided significant obstacles by following the available best practice. Solutions were piloted and applications tested completely before going live. Although some technical aspects required discussions between different partner organizations (because of the need to integrate different ICT platforms), this did not result in any major technical complications. Additional development work for solving any technical problems that arose in partnering organizations was adequately financed and carried out.

Relative influence of eGovernment challenges

On a 100% scale, the following are approximate relative levels of influence on X-Road of some key factors that could affect eGovernment projects:

- **Political, administrative and organizational (40%):** Administrative barriers, existing work practices and lack of motivation for changes were among the main influence here, but direct political influences less so. Also, IT managers were hesitant in the launch period. A main argument was about not allowing other developers into their own technical environments, which was solved after the institution's own technical staff were offered training and started undertaking this development work themselves.
- **Legal (30%):** This is related mainly to personal data protection, public information regulations, digital signature rules and database regulations.

¹³⁰ For more details about the Breaking Barriers to eGovernment project please see <http://www.egovbarriers.org>

- Financial (5%): Finance had a relatively low influence in this case because of the project's stable budget planning mechanism, with relatively minor efforts needed to find appropriate levels of finances. The main financial discussion concluded that the adopted strategy for integration of registers would cost much less than alternative methods considered.
- Social (10%): This related primarily to take-up of the X-Road eServices developed. In some ways, too fast a take-up of services can pose as many problems as too slow a rate. Broader info-political considerations are needed to overcome these problems, such as those related to privacy.
- Technological issues (15%): The most significant technical effort focused on the creation and testing of the basic architectural and system concepts and techniques during the pilot project.

Conclusions

The X-Road concept has proved to be a good one and has been generally successful, after the project's initial problems. It is important to emphasize the role in this achievement of motivational models that address the need to take account of risk, organizational, legislative and psychological barriers of stakeholders in such a public-sector area. After the complicated and at times difficult initial implementation period, stakeholders began to appreciate the value of the innovation and were happy to cooperate. But the process itself was not very easy. The main barrier was not the technology but the difficult organizational and legislative environment of the public sector in which the project was enacted. Fiscal and technical barriers have been less important, and in most cases were solved without significant complications.

Estonia had some advantages in the implementation process. Its legal system was still in the phase of development and the implementing ministry had the power in practice to create necessary regulations. Stable general ICT coordination institutional structures and expert personnel helped to support the development and implementation, including strategy, action and resource planning. A positive driving force came from the generally supportive attitude of citizens toward new innovative services.

The X-Road system has provided a high quality exchange layer that facilitates quick and effective communication between government databases and provides a wide range of services to improve efficiency and decision-making in both public and private institutions. The system provides so many cost and efficiency savings that it easily justifies the investment in it. Other countries would benefit from the implementation of systems similar to X-Road system, which can be the basis for delivering a productive and comprehensive means of communication between government databases.

Sources

Interview with Riho Oks, Development Advisor to the Director of Informatics Centre. Riho Oks was involved directly with the implementation process of X-Road project being responsible on integration process of registers from different public institutions

Interview with Ahto Kalja X-Road project manager. Estonian Informatics Centre. Ahto Kalja was one of the main architects of the project and working not only with technical issues but also with organizational and legislative topics.

Interview with Uno Vallner, Head of IT Architecture Unit, Department of State Information Systems, Ministry of Economic Affairs and Communications. Uno Vallner was one of the initiators and visioners of the project

Interview with Marko Lehes, Director of Centre of Registers and Information Systems, Ministry of Justice

Conclusion

What are the broad conclusions that we can draw from the three embedded cases? The first conclusion is that, despite their common technical goals of acting as registries, each project experienced rather different barriers. As we hypothesised, the registries that were not related to personally identifying information appeared to face fewer barriers associated with the “lack of trust” category, and equally faced fewer legal hurdles. Thus, for the company register, GEWAN, the only relevant barriers were found to be “digital divides” and some limited “leadership failures”. It is notable that GEWAN appears not to have been impeded by “poor coordination”. Part of the reason for selecting it as an embedded case was that the project necessarily involves a large number of administrative actors operating at different levels of government.

Moving on to the Estonian case, slightly more serious barriers were discovered. They were found to primarily revolve around “organizational inflexibility” and to some extent around “lack of trust”. As the x-Road project included aspects of citizen registries, it is unsurprising that the privacy aspect of “lack of trust” was more apparent than it was for GEWAN. The discovery of problems with “organizational inflexibility” is more interesting. Part of the reason for choosing the Estonian case was to investigate whether a more centralised system of registry provision is a successful model. The x-Road project suggests that there are costs and benefits to such a structure. It appears that when centralised systems are dependent on the cooperation of other departments and agencies in a technical sense, then great care must be taken to ensure that the necessary changes in development patterns are made across all organizations concerned. Thus, the finding is one that touches on the “poor coordination” category. The solution to the barrier turned out to be using a better understanding of the desires of the diversity of organisations associated with the project.

For Eurodac, the main barriers were found to be far more extensive. They were “financial inhibitors”, “poor coordination”, and “organizational inflexibility”. Given the personally identifying nature of the information stored, it is interesting that “lack of trust” did not feature more prominently as a barrier. In fact, the findings of our research suggest that this possible barrier was acknowledged and dealt with at a fairly early stage by limiting the data held in the registry to only fingerprints – with no associated identifying information. While there is cause for concern that specification creep will undo this strategic decision in the future, for now privacy issues appear to be of low consequence.

The barriers that were unearthed are of note as they stem from the pan-European nature of the project. Engaging in collaborative eGovernment projects across countries with varying degrees of experience and capacity with communication technologies would seem to be an activity that requires careful planning. Different levels of experience with eGovernment systems is likely to be linked to different organisational structures in each country. In turn, these different structures are likely to require different mechanisms to reconfigure them for effective use of new IT systems.

We found that the importance of “financial inhibitors” is itself an indicator of a cross-cutting underlying issue – the political aspects of the project. Fundamentally, Eurodac suffers from an imperfect alignment of incentives to participate in the project across the member states. Those countries that act more as gateways than as destinations have less to gain from the system. This leads to reduced incentives both to commit financial resources and to act diligently in the administration of Eurodac. While the particular pattern of interests in this case is a result of the policy area concerned, this would appear likely to be a problem that is likely to appear in other similar pan-European eGovernment endeavours.

The Eurodac case also revealed that, despite harmonisation attempts, the differing legal regimes across states have made for some difficulties in the uniform operation of the service. It is in this area that privacy issues have had their biggest effect. However, the main impediment here seems to be the differing laws rather than the privacy in and of itself.

The final point to make on the barrier categories is that, in general, “poor technical design” is not a problem. This would seem to be because the operation of registries is, now, a fairly standard, well-tested service. Administrations have a lot of experience of running large databases in many contexts; and technology seems to be the most straightforward factor to resolve in the cases reviewed here.

One last question remains. How did the hypotheses that we offered above fair in our empirical research? On the first – that organisational barriers increase as the associated level of government gets higher – the evidence would seem to support it. The sub-national project (GEWAN) appeared to suffer little from barriers of this sort, while the national Estonian, and pan-European projects were found to have progressively larger problems in this area. The results are less conclusive for the second and third hypotheses; respectively, that resource barriers decrease as the associated level of government gets higher, and that legal barriers are more likely to be overcome by schemes that operate at the national level. While financial inhibitors were only found to be of importance for Eurodac, this is the result of underlying political issues rather than an actual lack of financial resources for the participating countries. In the case of X-road having adequate finances and planning and budgeting appropriately were noted but as the project was delivered within budget was not a major issue. Legal aspects were also found to be of limited relevance for the sub-national project we studied, but it seems likely that this was the result of it being concerned with company information rather than personally identifying data. In support of the hypothesis the national level X-road project illustrated the benefits of being able to develop the most appropriate legal frameworks to facilitate the initiative.

To conclude, this case study has shown that, despite ostensibly similar technological goals, public registries face very different levels and types of barriers. The nature of the data that they store is of prime importance, but the institutional and political context also has a strong bearing on the difficulties that are likely to be faced. It seems unlikely that there is a single best model that can be used to implement public registry projects as it is important to adapt these considerations to the specific context.

References

- BRITE Project. No date. BRITE Objectives. <http://www.briteproject.net/modules/wfchannel/index.php?pagenum=3> (accessed 2006/12/04)
- ePractice 2007a. Civil Registration in Austria. <http://www.epractice.eu/cases/1910> (accessed 2007/01/12)
- ePractice 2007b. eEnabled Child Benefit Service in Ireland. <http://www.epractice.eu/cases/1909> (accessed: 2007/01/12)
- HM Land Registry. No date. eConveyancing: The Story So Far. <http://www.landregistry.gov.uk/e-conveyancing/storysofar/> (accessed 2006/12/04)
- HM Land Registry. 2005. Inventory of Land Administration Systems in Europe and North America (4th Edition). URL: <http://www.landregistry.gov.uk/assets/library/documents/inventory.pdf> (accessed 2006/12/03)
- IBM. No date. To serve the Italian passion for motoring. URL: <http://www-306.ibm.com/software/success/cssdb.nsf/CS/KHAL-62ESK3?OpenDocument&Site> (accessed 2006/12/04)
- IDABC eGovernment Observatory. 2005. eGovernment in the Member States of the European Union. URL: <http://europa.eu.int/idabc/en/document/4370/254> (accessed 2006/12/04)
- Makolm, Josef. 2004. "Registers as Part of Back Office Integration: The Austrian Experience", Lecture Notes in Computer Science 3183/2004. URL: <http://www.springerlink.com/content/dy4d3a8ct4g7nww1/> (accessed 2006/12/04)
- National Audit Office. 2002. Better Public Services through eGovernment: Case Studies in support to Better Public Services through eGovernment.

Panayiotou, Panayiotis Andrea. 2003. "Electronic governance for the Lands and Surveys Department in Cyprus", *Property Management* 21 (5), pp. 337-354. URL: <http://proquest.umi.com/pqdlink?did=537524621&Fmt=7&clientId=15810&RQT=309&VName=PQD> (accessed 2007/01/25)

Peeva, Valya. 2001. *Development of a National Registry in Bulgaria: Options and Recommendations*. Center for Energy Efficiency EnEffect: Sofia, Bulgaria. URL: <http://www.oecd.org/dataoecd/5/39/2467284.pdf> (accessed 2007/01/25)

Reach. No date. Reach FAQs. <http://www.reach.ie/faqs.htm#privacyissues> (accessed 2006/12/04)