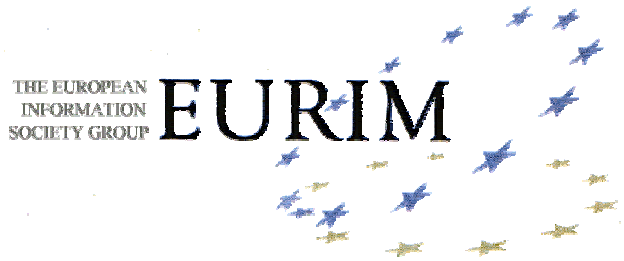
EURIM PERSONAL IDENTITY AND DATA SHARING WORKING GROUP

STATUS REPORT

April 2005



Secure Data Sharing as the Key to Efficiency in Service Delivery

Introduction

The e-Government Unit mission: "Ensuring that IT supports the business transformation of Government so that we can provide better, more efficient public services." The Prime Minister Tony Blair MP.

The e-Government mission requires the interoperation of departments' systems and processes, and methods for identifying and authenticating citizens securely across multiple channels. Should these methods fail, e-government is open to abuse by perpetrators of identity theft, the misrepresentation of personal circumstances, and significant harm to privacy and civil liberties.

Secure data sharing is a vital component in ensuring success. A '*Which?"* magazine study published in March 2005 estimates that £1.3 billion per annum is stolen in the UK by identity thieves. These criminals are experts in exploiting weaknesses in systems which rely on insecure and unreliable paper documents, and on processes that make it difficult for those involved to share data which may expose the attempted fraud.

Advances in computing, particularly in networking and security, are making it possible to reduce identity theft through secure data sharing, but new technologies often raise more questions than they answer: questions of national identity and the relationship between citizen and the state, about civil liberties, data protection and relationships with other nations and commercial organisations, about citizens owning their data and the government being free to access it in the national interest. These factors must be seen to operate in balance if secure e-government is to be delivered in an acceptable way for all stakeholders.

EURIM published a well-received status report in July 2004, entitled '*Citizen or Subject: How Far Do We Control Our Own Identities?*' designed to move the Personal Identity agenda forward. The EURIM working group has been working further on these issues and this document is a summary of our thinking to date. It re-states the benefits of secure data sharing and cites working examples. It outlines 2 complementary approaches, recommends that the eGU sponsor pilot 'quick win' projects to explore new ways of enabling secure data sharing, and suggests areas where these pilots might take place.

What is secure data sharing?

Secure data sharing is the process by which one agency is entitled to access appropriate information about an individual that has been collected by a different agency; access is by controlled and secure gateway interfaces between networks with different security controls and classification levels. This process deals with issues of trust, data quality, governance and infrastructure and the roles of information provider, information requester, trusted intermediary and the individual. At the heart of the process is the level and timing of individual consent required for the data to be shared. There are several approaches to consent ranging from none whatsoever (in some cases of national security) to a one time consent given by the individual for a specific enquiry.

© Copyright EURIM 2005. All rights reserved.

Benefits of secure data sharing.

Imagine a scenario where individuals receive the services to which they are entitled in a timely manner without the need to fill in forms, submit paper proof of address and wait for the post to arrive. In this scenario money arrives electronically in the individual's bank account rather than in a cheque mistakenly sent in the post to a previous address.

Applications for new services can use existing online credentials and previously conducted identity checks instead of repeating the same processes. Savings made through the use of electronic channels are shared with society, and where people were unaware of their entitlement to services, the systems now recognise their eligibility and offer them automatically. Individuals can also be re-assured that their details are shared with their consent whilst at the same time unauthorised attempts to use this information are detected swiftly.

These benefits can be achieved by the introduction of intermediaries to facilitate secure data sharing between service providers, following one of the two models described below. Such intermediaries can help sort out the overlapping identities and varying processes that are exploited by identity thieves. Secure data sharing introduces consistency and commonality across service provision making it harder to conceal fraud. However, data sharing opens up new vulnerabilities, including the automation of identity theft. This is being addressed by EURIM in a separate paper to which eGU may wish to contribute.

Current examples of data sharing

HMG is already benefiting from processes which share data.

- Housing Benefit administration sometimes involves a degree of data sharing across organisational boundaries where a national benefit is delivered by local authorities through private sector service providers, e.g. Vertex-Ealing Borough Council-DWP-Treasury. Secure data sharing has reduced problems with fraud and administration, and led to significant savings.
- Project Semaphore, part of e-Borders, depends on secure data sharing between airlines, other carriers, and key border control, law enforcement and intelligence agencies. Project Semaphore will identify people who have boarded transport destined for the UK, check them automatically against databases of individuals who pose a security risk, and keep a simple electronic record of entry into the country. The system will also enable authorities to record people leaving the UK, helping to identify those who overstay. It will play an important part in safe-guarding against terrorism, serious and organised crime and illegal immigration. At the same time, it will allow legitimate passengers to travel more efficiently and securely both into and out of the UK.
- The Inland Revenue and the Department of Work and Pensions are sharing information in order to calculate tax credits more accurately.
- Government Gateway, of which more below.

These, however, are isolated examples and the widespread benefits mentioned will accrue only when secure data sharing becomes part of the foundations of an integrated public service infrastructure rather than a worthy afterthought. EURIM recognises that government departments need help in justifying the investment required to implement secure data sharing infrastructure, since it involves agencies other than their own (and higher priorities have been placed on the performance of individual departments' own internal objectives). Secure data sharing pilot projects will help prove the case; the question is which approach to pilot for which application?

Models for secure data sharing

Although there are a variety of legacy models in different parts of the public sector, there are two main models for secure data sharing. The first has been used for many years by banks and credit card companies, and we term it the 'financial services model'. The second is only possible now that the majority of the population enjoys network access, and we term it the 'federated' model. Looking at each in more detail:….

© Copyright EURIM 2005. All rights reserved.

The *Financial Services* Model.

In this approach, service providers (such as banks and credit card issuers) contribute data to a central store facilitated through the initial consent given by the consumer. This data is hosted by a Credit Reference Agency (CRA) as the trusted intermediary, and may be complemented with personal data acquired from other sources by the CRA. Here, the individual gives consent for their data to be shared when they apply for the service. This consent is wide ranging and lasts for the duration of the relationship with the service provider.

This model has a shared 'pot' of information. The data held is dynamic with regular updates received from the subscribers. A virtual single consumer view is established as a result of each specific request. The content of the single view will be based upon the level of contribution from the subscriber and type of transaction to which the request relates. The data is used to assess the identity and entitlement risks associated with a product or service. Individuals can be notified of accesses to their data, have sight of the data shared and are able to challenge and rectify incorrect data.

The model is well understood, having been developed over the last twenty years or so by companies such as Experian. The credit reference industry has a proven infrastructure which employs powerful analytical tools and databases to establish trends and assess risk. Although the experience of financial services organisations is that processing documents is costly, with no proof that it prevents identity fraud taking place, CRAs can support the corroboration of document attributes back to source. The current system can vouch for the individual's identity in terms of their financial dealings, and CRAs can also provide details that would contribute towards the assessment of an individual's entitlement to benefits e.g. identifying instances of multiple occupancy where the person claims to be living alone. However, there is no ability to vouch that someone does own a particular National Insurance Number (NINO) or Passport Number, since this information is held under different identity relationships between that individual and the State.

Models for secure data sharing in this way are sometimes referred to as 'Circle of Trust', in which subscribers, consumers and the CRA are members of the circle. It is clear the financial services model could be applied in the public sector, utilising the existing infrastructure. Indeed, some departments, such as the Rural Payments Agency in Defra, appear to have made use of such services over the past few years.

The *Federated Model.*

This model is practical now that the majority of the population enjoys Internet access. The technology as a whole has benefited from extensive standards work across the IT industry, with initiatives being led by OASIS, the W3C, the Liberty Alliance, and IETF amongst others.

Here, the individual is assumed to have an on-line relationship with each service provider, and uses a trusted intermediary to facilitate a single sign-on service, and to exercise direct control over the flow of personal information between service providers. Government Gateway is an early example of federation in the UK, and there are other similar initiatives underway in local government.

Gateway was conceived as a single-sign-on service that would allow an individual to use one credential for authentication to many different public sector service providers. An individual starts by setting up an account with Gateway, using either username and password or a digital certificate for authentication. Then, working from Gateway, he can access a service provider account by entering – in consecutive sessions – the provider's customer reference number and an activation code received by post. Thereafter he can access that service provider account, and others for which he has registered in a similar way, simply by authenticating to Gateway.

Although Gateway is currently provided by Government, the service exists largely for the benefit of the individual, and is quite clearly under the individual's direct control: an individual can, for example, delete a Gateway account, add relationships to it, or create a second account at will. Moreover, Gateway avoids the privacy issues that would arise if an individual's relationships and identities were all merged into one. Instead, Gateway recognises that an individual has distinct and private relationships with different public sector entities, and gives him a tool to help manage these relationships.

However, federation is still a new approach, and the tools within Gateway remain quite limited. Apart from secure messaging, and one or two transaction options, the only functionality is single-sign-on. There is a clear need for a permissioning tool that would allow the individual to grant a service provider access to

© Copyright EURIM 2005. All rights reserved.

personal information held either in the account itself, or by other service providers - using a channel that runs through through his account. Such a tool would enable the individual to carry out a wide range of multi-domain transactions, including: (i) transactions that currently require documentary proof, typically of identity, age, or concessionary status; (ii) the creation of one-to-many records, such as a validated CV; (iii) change of contact details to many service providers in one transaction; and (iv) various mail redirection and permissoned marketing applications.

In parallel with this growth in functionality, there may be a case for reviewing the organisational and business models for Gateway. Since the service exists primarily to help individuals transact with organisations, there is no fundamental reason why it should be hosted by the Cabinet Office. In time, it could be offered by an organisation with the declared aim of working as the individual's trusted agent. Indeed, there could be several such organisations, perhaps called identity brokers, each possibly sponsored by an existing issuer of secure authentication tokens, such as banks, telcos, or local authorities (some of whom issue smart cards).

For such a model to be viable, service providers would need to pay the individual, or the broker acting on the individual's behalf, for authentication and shared data. Then, with the help of the public sector to drive critical mass, it may become possible for an individual to use his broker account for dealing not only with the public sector, but also with private sector organisations, such as utility companies and on-line commerce sites.

The federated model – with its reliance on identity brokers – has both strengths and weaknesses. On the negative side are the facts that it is not yet proven, and requires that individuals have network access. But on the positive side, federation can be seen as logical development of existing work on Gateway, that both enables new applications, and enhances privacy in a person-centric way that gives the individual precise control over who sees what and when. In addition to the existing single-sign-on functionality, there would seem to be immediate potential for developing the use of federation in the education sector, looking at applications such as lifelong learner record.

Conclusion

Secure data sharing has a vital role to play in the e-Government agenda and is a foundation of integrated government rather than a 'nice to have'. However, it can appear to be difficult to justify because the benefits are not widely understood and the concept is not immediately apparent to departments, which have higher priorities. We have seen that it is already delivering benefits, but there may be cases now where lack of data sharing is actually frustrating implementation of policy. For example, it would be of value to share use of the NINO in order to prevent illegal working, implement anti money laundering provisions and monitor ISA applications.

The government's effectiveness and efficiency measures may be achieved through use of secure data sharing to support the Child Support Agency and to streamline processes by checking cases online rather than on paper. It could certainly reduce waste by stopping the capture and storage of data that can never be corroborated. The rules for secure data sharing demand clear guidelines on who gets to see what and when. There are two broad approaches, one based on a consent-driven subscriber model, the other based on federated data and granular consent. Both have merit and need to be explored in real scenarios.

In order to help inform the case for widespread secure data sharing, understand the interdepartmental complexity and test the appropriateness of the models, we suggest 'quick win' projects in the near term. Our first thoughts are that the financial services model could usefully be applied by the UK Passport Verification Service and DVLA to corroborate passport and driving licence details respectively, sharing of the NINO, and that either the financial services model or the federated model could be used for the construction of lifelong learner records and other education applications. Our study has reached a stage where we would like to open dialogue to expand on our work to date and choose appropriate areas for further study.

This EURIM group believes that sponsorship of early win projects for secure data sharing will deliver wide far reaching benefits for the CIO council and provide leadership opportunities for the e-Government unit.

© Copyright EURIM 2005. All rights reserved.