It's Okay To Be A Dog On The Internet – Privacy And Trust In e-Government

Mike Richards
Computing Research Centre
The Open University
Walton Hall, MK7 6AA,
Milton Keynes, UK
M.Richards@open.ac.uk
http://crc.open.ac.uk

Karim Adam
Computing Research Centre
The Open University
Walton Hall, MK7 6AA,
Milton Keynes, UK
K.A.Adam@open.ac.uk
http://crc.open.ac.uk

Blaine A. Price
Computing Research Centre
The Open University
Walton Hall, MK7 6AA,
Milton Keynes, UK
B.A.Price@open.ac.uk
http://crc.open.ac.uk

Abstract : *E-government should not be considered as a single service, or even a small range of services; instead it can comprise an almost limitless range of activities. We believe that it is necessary to impose order on these diverse services before the full potential of e-government can be realized. We propose a simple classification of potential e-government services based on the privacy requirements of the service. We also believe that many e-government services have direct parallels with commercial services and that these private services should form both the inspiration and realization of e-government.*

Keywords: e-government, privacy, e-commerce, trusted-third parties.

1. Introduction

There is no doubt governments generate increasing amounts of information that they will want to communicate with their citizens (G2C). Equally significant is the ease with which citizens access such information (C2G). E-government provides a platform where content can be *intelligently processed and integrated* (Abie et al., 2004).Privacy is just as crucial to the successful deployment of e-government as it has been to the flourishing e-commerce sector.

2. Using e-government

We have chosen to consider e-government from the related perspectives of privacy and authentication with respect to a mobile user's location.

2.1. Concepts

Information privacy is defined as *"the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"*(Westin, 1967). This information might be a name, address or government-issued identifier such as a National Insurance number. Using the European Data Protection Directive (Directive 95/46/EC, 1995) as a starting point, we suggest that any interaction should only result in the minimum impact on an individual's privacy. We recognize that certain activities require the release of greater amounts of personal information than others, whilst some activities result in no impact whatsoever.

Authentication is the process of confirming that an individual is who they claim to be. Where privacy concerns are minor or non-existent, authentication is less of a concern or indeed entirely unnecessary; correspondingly, where privacy is important, authentication becomes crucial.

2.2 Authenticating e-government users

A number of well-established authentication systems exist that allow remote users to access restricted systems, many of these use cryptographic information that is unique to an individual or to a computer.

Strong authentication is possible through a system known as Public Key Infrastructure (PKI); built upon public key (asymmetric) cryptography whereby individual users each possess a unique pair of mutually-related encryption keys. One key, the private key, is retained by the user at all times; the second, the public key, is freely available to everyone. Pivotally, material encrypted with a public key can only be decrypted with the corresponding private key (and *vice versa*). It is immaterial that a copy of Bob's public key are held by untrustworthy Eve, she cannot use it to read data encrypted by Alice using another copy of Bob's public key.

Public key cryptography offering very high levels of protection has been widely available for many years but has never achieved wide-scale acceptance by individual users; despite public key cryptographic plug-ins for applications such as email, only a tiny fraction of such traffic is encrypted. Studies have shown (Whitten & Tygar, 1999) that standard security applications are too complicated for general use and the process of performing a secure exchange distracts from the primary task of exchanging data. For users to embrace encryption, and through it, enjoy the benefits of secure, authenticated communication, the encryption process must be invisible.

Perhaps the most widespread deployment of cryptography is the Global System for Mobile Communications (GSM) used by most mobile telephony services. Telephones on such networks enjoy reasonable levels of security using the symmetric cryptographic algorithms A5/1 and A5/2. Both forms of encryption are relatively weak, but GSM users can be assured that their communications are relatively secure from eavesdropping and that callers are correctly identified (authenticated). It is important to note that the user remains unaware of the encryption process and is not expected to intervene in the process of creating the encrypted link.

Similarly, most Web browsers permit secure transactions such as the transmission of credit card details over the World-Wide Web. They support a limited form of authentication in as much as each computer in the transaction is authenticated before the exchange of private information takes place. However, once again, it is significant that all of the cryptographic exchanges take place without user intervention; indeed to all intents and purposes, the process is entirely transparent.

We propose that widespread acceptance of authenticated e-government services will only come about when authentication systems can be made as transparent as those used in existing mobile telephone systems. PKI offers high levels of security and authentication and can be used by personal mobile devices or interactive television 'set-top boxes'. However, at present, PKI is insufficiently intuitive for widespread adoption by 'technophobic' users.

3. Accessing e-government

The dazzling range of potential e-government services comprise such a diverse collection of activities that it is very difficult to talk about an ‘e-government solution’. Rather, we can classify e-government activities into broad categories sharing sufficient similarities as to suggest common solutions.

We propose that e-government services can be broken down into three broad categories based on their privacy and authentication requirements.

3.1. Anonymous not authenticated

Many interactions with government are simple requests for public information such as health advice, bus timetables, statute, consumer advice and so on. None of these documents contain personal information and are not intended to be customized to individual users. Traditionally, government has produced vast quantities of paperwork at enormous expense and to limited effect. These documents are ideally suited to computerization and delivery over the Internet and it is here where unqualified successes in the field of e-government can be found.

In the UK, Her Majesty's Stationery Office (HMSO, soon to be the Office of Public Sector Information) makes a vast amount of legislation and other public sector information available free of charge. Another UK site, www.directgov.gov.uk provides anonymous access to a wide variety of government information from finding a local school to obtaining a driving license. Releasing this information does not require that the requestor authenticates themselves. Indeed by statute many documents must be made available to anyone who requests them. Requests for this type of information can be performed on an anonymous basis without any need for authentication.

3.2. Authenticated

Certain types of government information are unique to an individual or organization; we might think of a person's tax record, health information or their criminal history. This information cannot be allowed to leak into the wider world and a great deal of legislation exists to prevent the abuse of personal data. Japan and most Western countries have implemented strong privacy laws based on OECD Guidelines (OECD, 1980).

Any e-government solution providing this type of service must restrict access to authorized users; users must be authenticated in some manner. Authentication involves the disclosure of some measure of personal information constituting an infringement on the user's privacy. The precise level of disclosure and the type of information will vary from government to government and activity to activity.

3.3. Anonymous authenticated

There is a category of interaction where the user must be authenticated as eligible to receive a service from government, but where the government must not know their identity. The most obvious example of such an interaction is voting in an anonymous ballot. It is reasonable to ask voters to prove their identity (authentication) before casting a vote, but their electronic equivalent of a ballot paper should not be traceable to that individual (anonymous).

Voting slips in a traditional paper-based election should not contain any link back to an individual voter. An electronic election should attempt as far as possible to replicate this process.

3.4. Using location as a form of authentication

Certain services are only accessible or relevant within a given area. For instance, Alice is walking through an unfamiliar city and wants to know where the closest metro station to her current location; Bob might want to know how to apply for a parking permit in his home town and Chloe wishes to know when the next bus will arrive at her current stop.

No further authentication is required at this time since very little personal information is being exchanged. Instead, the required information is drawn from a much larger pool and tailored to the user's location.

Location information can be provided by an individual using any one of a number of wireless technologies – registration with WiFi or Bluetooth cells; through the GPRS mobile telephone system or via GPS. There are advantages and disadvantages with each technology and it is entirely likely that any system will have to use a number of technologies in order to provide accurate location-based authentication.

4. Using privacy requirements to design e-government

Approaching e-government from the view of privacy shows that we are not presented with a *tabula rasa* – instead we are fortunate that many privacy concerns have been addressed by existing commercial applications. It is not necessary to reinvent the wheel, we can not only learn from e-commerce, but possibly use their infrastructure to provide government services.

4.1. Privacy implications for anonymous not authenticated services

Here, there are almost no privacy implications; the person making the request is protected from intrusion since the service is universally accessible. Users can be reassured that they are viewing a source of genuine information if all e-government sites were issued with a digital certificate of authentication viewable through a Web browser or mail program.

4.2. Privacy implications for authenticated services

As already noted, such applications require some release of personal information. The type of information varies from service to service. The payment of a fine or the purchase of a public transport pass requires payment in exactly the same manner as an online shop. Such an e-government service would need to process online payments and dispatch confirmation and/or physical products to the user. It is clear that existing e-commerce sites have solved these problems. Internet protocols such as HTTPS ensure that it is possible to send secure payment details over an inherently insecure network. Individual corporate policies offer additional security for users; these include only dispatching goods to the physical address where a credit card is registered, phone-back to confirm identity and printed and e-mail receipts for every transaction.

For certain services it is not necessary that the person interacting with e-government is the person who will use a government service; a parent might buy a ticket for a child, whilst a particularly loving partner might pay their fellow's parking ticket. E-government need only be concerned that the payment is made, not necessarily the origins of the payment. Illegitimate use can be controlled by existing legislation regarding the use of personal data, banking transactions and credit cards.

Some services require a still higher level of authentication; the UK's Self Assessment system for personal Income Tax allows users to access their personal tax records, and to claim state benefits and file tax returns online. A standard commercial system (without authentication) is used to make payments.

4.3. Privacy implications for anonymous authenticated

This aspect of e-government poses particular challenges for designers. A service can only be provided after some measure of authentication, but the service provider must be unaware of who is accessing the service.

In 2004, four Geneva suburbs trialed Internet voting in a national referendum (E-VOTING, 2004). Each of the 22,000 voters was given a card carrying a unique sixteen character code and a second, four-character security code hidden under a scratch-off panel. Authentication was performed online by entering both codes along with the voter's date and place of birth. Despite the seemingly impressive authentication process, the method is not foolproof – there is no reason why one person could not use another's voter card provided they knew some relatively trivial personal information.

We propose that an anonymous authenticated service would comprise two completely different components; the first would be an authentication server; which would release a single 'token' code once the authentication process has been completed. This token could then be used in the second component – the service provider. The token would constitute the only data passed between the two

components. This is a kind of privacy proxy which we describe in more detail in our work on user control of privacy in ubiquitous computing (Price et al., 2005).

The exchange of secure tokens is not unreasonable; we foresee a system where individuals possess private/public keys that can be used to encrypt, decrypt and sign data. After authentication, a user would be emailed a token encrypted using their public key. The user could then decrypt the token and use it on the secure service provider.

5. Ensuring trust in e-government

> *'You may be deceived if you trust too much, but you will live in torment if you do not trust enough.'*
> Frank Crane, American clergyman and journalist, (1861 – 1928).

Trust is precious and it is the cornerstone of providing personalized e-government services (Decman, 2003). Individuals must trust that the government is not abusing their privacy, whilst the government must be reassured that only sanctioned individuals are using public services. A government might be entitled to say 'trust us', but then again, so is the citizen.

5.1 Implementing a trust architecture for e-government

We are concerned that at present individuals are expected to place too much trust in the good faith of government without having recourse when that trust is abused. Recently, (April 2005), the British electoral system was found to permit widespread fraud through the misuse of postal ballots. The results of elections may be in doubt because of criminal activity yet there is little recourse for those affected.

We hold that it is entirely reasonable to outsource trust to a third body, independent of government but tightly controlled by statute. All requests for personal information from e-government services would be directed to the trusted third party who would be responsible for releasing only the information needed, maintaining the security of the data and informing citizens that their data has been used.
Outsourcing of trust is already commonplace in the commercial sector. Online businesses rely on trust providers for the digital certificates needed to conduct secure transactions. Similarly, retailers are beginning to aggregate their online operations with several retailers sharing a common trust architecture; for instance, two major UK retailers, W.H. Smith and Marks and Spencer both use Amazon's e-commerce infrastructure to deliver their own goods and services.

5.2. Benefits for the individual

The citizen would know a third party by its reputation from the commercial environment where it has been providing services to a wide range of organizations. They would be confident that the trusted third party is bound by legislation such as the Data Protection Act 1998 and the Freedom of Information Act 2000. The pieces of legislation would allow individual users to access personal records held by the third party. We propose that an individual should be able to see a comprehensive history of every access to their record (barring those withheld on security grounds) free of charge, rendering transparent their every interaction with government; such openness can only increase individual trust in good government.

One side-benefit of such a service is that the trusted third party could offer every citizen a personal digital certificate. Such certificates could be used to authenticate themselves to other Internet services or to digitally sign email messages.

5.3. Benefits for the government

Companies such as Thawte and Verisign have already constructed a trust infrastructure for commercial applications. Their infrastructure is widely deployed, universally supported in software and hardware,

thoroughly tested and implicitly trusted by all those who engage in e-commerce. Turning trust over to such bodies allows the rapid introduction of authenticated services without the government having to build or maintain a trust infrastructure; whilst competition between providers should increase the quality of service and drive down costs for the end user.

Building on internationally accepted standards permits the roll-out of e-government services on a supra-national scale – facilitating the provision of services in any country where the individual has rights to government services; an obvious example would be the ability of an EU citizen to access e-government services in any of the member states as easily as they would in their home country.

5.4. Benefits for industry

A trust infrastructure would prove to be a lucrative source of income for any company that chose to provide authentication services. It is entirely possible that existing mobile networks will form the foundation for mobile e-government; this is potentially a new market for mobile network operators who are currently engaged in a search for 'the next big thing'.

A business that is part of a successful trust infrastructure would be able to use their experience to secure further private contracts with other businesses. Similarly, companies taking part in the construction and operation of a trust infrastructure would be able to increase public awareness of their brand.

6. Conclusions

We believe that dividing e-government services along privacy lines is a worthwhile exercise. It reveals that many services can be provided without impinging upon privacy and that these services can be rolled out with great speed using existing technology. Governments are beginning to recognize that privacy concerns need to be integrated as services are developed. Countries such as Canada, the United States, Australia, and New Zealand require Privacy Impact Assessments for any new e-government service.

Those services that require some measure of authentication bear great similarity to well-established e-commerce solutions and may in fact be identical apart from the type of service provided. It is entirely possible that the existing e-commerce infrastructure could be reused by e-government providers, minimizing both cost and the time taken to build such services.

We believe that those services that require both authentication and anonymity are the most difficult to construct and will not be realizable in the immediate future.

The provision of privacy services is already well established in the commercial environment and it seems entirely reasonable to use this hard-won experience to build the privacy architecture needed for e-government. Indeed we consider the provision of privacy protection by trusted third parties to be not only desirable, but essential, on both financial and democratic grounds.

References

Abie, H., Foyn, B., Bing, J., Blobel, B., Pharow, P., Delgado, J., Karnouskos, S., Pitkanen, O., & Tzovaras, D. (2004). The need for a digital rights management framework for the next generation of e-government services. *Electronic Government, 1*(1).

Decman, M. (2003). *Trust in E-Government: Digital Signatures without Time Stamping?* Paper presented at the EGOV 2003, 256-259.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995), 95/46/EC. Available from: http://europa.eu.int/comm/internal_market/privacy/law_en.htm

E-VOTING. (2004). *E-Voting*. Site officiel de l'Etat de Genève. Retrieved 15 March, 2005, available from: http://www.geneve.ch/evoting/english/presentation_projet.asp

OECD. (1980). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available from: http://www1.oecd.org/publications/e-book/9302011E.PDF

Price, B. A., Adam, K., & Nuseibeh, B. (2005). Keeping Ubiquitous Computing to Yourself: a practical model for user control of privacy. *International Journal of Human-Computer Studies*, (to appear).

Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum.

Whitten, A., & Tygar, J. D. (1999). *Why Johnny can't encrypt: A usability evaluation of PGP 5.0.* Paper presented at the 8th USENIX Security Symposium, Washington, D.C., 169-184.