A Roadmap for personal identity management

Thomas Neubauer
Vienna University of Technology
Vienna, Austria
neubauer@ifs.tuwien.ac.at

Johannes Heurix
Secure Business Austria
Vienna, Austria
heurix@sba-research.org

***Abstract*—Digital identities and secure environments are a fundamental precondition for giving life to e-government, e-health, and e-commerce. Whereas corporations are spending huge amounts on harmonizing identity management, and still fail, the average customer/citizen is left alone drowning in dozens of digital identities. This paper presents a roadmap for personal identity management. It highlights shortcomings of existing solutions, identifies major research challenges and gives an overview of steps that are necessary on the way towards an efficient solution for personal identity management. The benefits of increased usability and manageability are juxtaposed with privacy issues that potentially occur when a considerable quantity of functionality is concentrated in one single device.**

I. Introduction

Did you ever had to make an important money transaction, but you only had a public computer available, or had to buy something over the Internet or digitally sign a contract but did not have the credentials with you? Digital identities and secure environments are a fundamental precondition for giving life to e-government, e-health, and e-commerce. Whereas corporations are spending huge amounts on harmonizing identity management, and still fail, the average customer/citizen is left alone drowning in dozens of digital identities. The reasons are (i) bad usability resulting in (ii) missing trust and acceptance by its potential users, (iii) security shortcomings, (iv) missing interoperability and mobility, and (v) a lack of privacy. The existence of a variety of identities is not only unmanageable for the majority of users, in fact it is an essential security problem. The web has been embraced for a significant amount of commercial and personal communication. Governments across the world are increasingly trying to provide Internet enabled services to citizens. In order to use the Internet for carrying out sensitive operations, each party involved in a transaction or communication has to be able to confirm their identity in a trusted way [8], usually by the use of digital identities. Digital identities can be interpreted as the selective exposure of Personal Identifying Information (PII) over a network by the codification of identity names of a physical instance in a way that allows digital processing. Identity management refers to the management of digital identities or digital identity data. Identity management has been recognized as a key research theme for the coming decades (cf. [7]). Given that identity research is still in its early days, much research is geared towards conceptual investigations aimed at establishing the grounds on which further research may be build (cf. [11] for a literature review highlighting the nature of research on identity and the boundaries). This paper presents a roadmap for personal identity management with the goal to provide an easy-to-use secure authentication and signature creating device that can be used in different areas without any system changes. The paper highlights shortcomings of existing solutions, identifies major challenges and gives an overview of steps that are necessary on the way towards an efficient solution for personal identity management. The benefits of increased usability and manageability are juxtaposed with privacy issues that potentially occur when a considerable quantity of functionality is concentrated in one single device.

II. Identification of Research Challenges

In the past it has been challenging to implement efficient solutions, and those that have been implemented have been vulnerable. The management of identity raises a certain number of issues:

Lack of Trust: Trust is one of the main pillars for the acceptance, and, thus the success of new information and communication technology (ICT) applications. Building trust in the citizen and end-user was and still is heavily neglected when it comes to the use of digital identities and especially digital signatures. For example, 40% of Internet users in the European Union state that they are not using Online banking due to security concerns [1]. The concept behind digital identities (e.g., citizen and health cards) is often not understood by the users and the issuing procedure is time-consuming and complex. Existing solutions often demand the user to use anti virus programms and firewall. Studies show that most people are skeptical of the Internet as an environment for the exchange of personal data and have major doubts about personal data protection. They perceive high risks in giving personal data and fear that these will be misused in specific e-Service settings. Risk greatly hampers the take up of eID services. Electronic signatures baffle young users. To encourage the use of eID systems, the key success factors include precise information on eID systems and guarantees, and the enforcement of data protection

978-0-7695-3980-5/10 $26.00 © 2010 IEEE
DOI 10.1109/ICONS.2010.30

law. This may be accomplished through: 1) compliance with data protection and privacy principles (revision or new regulations adapted to specific user needs and requirements), 2) good communication (more specifically on the benefits that new technologies can offer) and 3) usability (allowing the user to easily cope with a system's interface).

Missing Interoperability/Mobility: We refer to interoperability as the ability of using identity information from one identity management system in another (cf. [3], [4]). Interoperability is "the ability of information and communication technology systems and of the business processes they support to exchange data and to enable sharing information and knowledge". It means the ability of different organizations to effectively communicate and cooperate in order to enable service provision. As such, interoperability may either expand, e.g., regarding usability, or limit, e.g., regarding security, the benefits of identity management to citizens, businesses or governments [26], [15]. Interoperable identity management systems raise considerable concerns for privacy and data protection. Interoperability problems and ease of use obstacles have left small and medium enterprises (SMEs) wishing to introduce cross-border signature solutions in the market in a very difficult situation. On a European-wide scale there are currently no products available solving the above-described limitations for a successful European electronic signature application that combines different national licensing schemes, certification services and national signature creation applications together with a user-friendly, portable secure signature-creation device.

Lack of Security:

- Identity theft: A variety of authors provide examples and case studies on identity theft and identity-related crime (cf. [17], [12], [19]). Nentwich et al. [21] show how an attacker can hijack an authenticated session that is established with an e-government web application.
- Code Execution: According to Nentwich et al. an attacker could (i) observe the complete traffic between the host and the smart card, e.g., by replacing the device driver for the smart card reader with a malicious version, (ii) modify the code of certain local applications, either by changing their static program image on disk or by altering the process image while the program is running, (iii) extend the code of a running process, e.g., with the help of the software package detours, and (iv) alter the code and memory of all local processes, if he gains control of the operating system. These shortcomings allow the attacker to alter the data to be signed anywhere between local applications and the card reader's device driver and to gain complete control over the program's input and output.
- Smart Cards: The side channel attack based on time measurement [25], for example, makes use of the fact that one can record different execution times for different values of a key. With the aid of statistical analysis, it is possible to extract the hidden private key. Power analysis [20], which depends on different power consumption for different operations, is another approach that can lead to more information about the chip and stored secrets. Of course, research is not only looking at possible attacks but also at feasible countermeasures, such as equal execution times for different branches when looking at time-based analysis. The aforementioned attacks have the potential to reveal secret information, such as the user's private key and PIN code. However, they require physical access to the card or the card reader device.
- Hardware: The main goal of the trusted computing initiative (as launched by the Trusted Computing Group - TCG) is the creation of a secure execution environment for personal computers. To this end, hardware support in the form of trusted platform modules (TPM) is integrated with the computers' motherboards. Based on a TPM, a secure boot chain from the hardware over the operating system to the applications can be created. For example, a trusted boot loader allows only a trusted operating system to be loaded, or the integrity of the operating system is verified at boot-time. Then, this operating system makes sure that only certified applications are started. This ensures that only unmodified applications (as certified by the software vendor) are executed, making it much more difficult for an attacker to alter programs such as the secure viewer. Also, there were a number of recent proposals [14], [27] that claim to provide a trusted execution environment without any additional hardware. Some of these techniques, however, have already been broken (cf. [28]).
- Digital Signature: In 1999, the European parliament and the council issued Directive 1999/93/EC, introducing the legal framework for the electronic signature in the European community. The goal of this directive was to support e-commerce and to facilitate the adoption of e-government in the member states. To this end, the concept of an advanced digital signature was conceived that should be treated legally equivalent to a handwritten signature. To qualify as equivalent to a handwritten signature, a digital signature must be based on a qualified certificate and must be created by a secure signature-creation device. However, Nentwich et al. [21] demonstrate how the content of a digitally signed mail can be manipulated and show how a secure viewer application can be tricked into signing a different document than the one displayed to the user. Shankar et al. [28] demonstrated the typical problem of a Trojan horse, capturing the secret PIN when it is entered directly on the computer and not via a card reader keypad. The authors also showed an attack

against a secure viewer. The threat of a Man-in-the-Middle also exists when using a SSL connection. The optional client authentication with digital signatures (instead of the insecure alternative using PIN/TAN) that exists in the SSL protocol could solve the problem but (i) it demands an external reader, and (ii) the concept of digital signatures is too complex for most users.

- Secure Viewer: The major challenges of signature creation on untrusted platforms are discussed in [23], [9]. Semantic problems of what has been signed are analyzed in [13], [24]. Solutions (e.g., [18], [2], [30], [29]) are proposed for the application area of e-government where secure viewers are needed for applying electronic signatures.

Lack of Privacy: The FIDIS research project defined a typology of three kinds of identity management systems [5]: IdMS for accounting, IdMS profiling and User-controlled IdMS. Type one and type two are usually used by large organizations or enterprises and are marked by centralized management. Type three is instead controlled by the user and decentralized so that the personal data is typically managed by the user. Type one and two focus on reliability and data integrity, type three brings forth mechanisms with respect for privacy, mainly the integration of privacy enhancing technologies (PETs) (cf. [11]). The ongoing moves toward the surveillance society suggest that individuals are seriously at a disadvantage in controlling the effects of surveillance whether consequences are intended or not [32], [11]. The management of identity raises a certain number of issues, such as privacy issues that may lead to the implementation of a surveillance society [31], or risk related to the stealing of identity (identity theft). People are concerned about threats to privacy when using online services but are not concerned about the amount of information available on them online (the so called privacy paradox). Major risks associated with profiling activities are heavily connected with shifts in power structures. Profiling enables those with power (businesses, governments, employers) to enhance that power, by making even more precise decisions that benefit themselves rather than the other party (cf. [11]). Changes to power structures in relation to the use of identity systems emerge as an important theme deserving research attention (cf. [6], [22]).

III. Roadmap Definition

This section gives an overview of the research roadmap for personal identity management and defines some major research challenges.

Trusted Device: One research focus is the usage of trusted devices (e.g., of biometric USB tokens). The EU Directive 1999/93 of the European Parliament on electronic signatures contains requirements for secure signature-creation devices, which are needed to produce qualified electronic signatures. Annex III of the Directive covers requirements for secure signature-creation devices to ensure the functionality of electronic signatures. It does not cover the entire system environment in which such devices operate nor does it contain requirements for electronic signature products as such. Today smart cards are generally considered the most appropriate devices to create electronic signatures with a high degree of usability and security, especially needed for qualified electronic signatures. However, smart cards have proven to have severe security shortcomings (cf. section II). Trusted devices, such as USB tokens or mobile devices with appropriate co-processors, offer a promising alternative to smart cards since they are well suited as secure signature-creation devices because they (i) are computers of their own and under sole control of the signatory, (ii) cover the signing and viewing function, secure storage of certificates, the related user verification, key generation and the allocation and format of resources required for the execution of those functions and related cryptographic token information for a discussion on the necessity of those requirements, (iii) are compatible with all public key infrastructures and certification authorities that deliver electronic certificates compliant with the X.509 standard, and (iv) make the need for additional hardware (card reader) and software installed on the client (driver software, signature software) obsolete. The chip technology used in tokens is subject to Moore's law as is every other area of information technology. This led to major improvements in the performance and capacity of token processors. Tokens have become an open computing platform, several years after mainstream computers (cf. [10]). Since the smart card is the most widely-used security tool for signature-creation, the biometric USB token as alternative must comply with very high security specifications so that security requirements defined in Annex III of the Directive 1999/93/EC of the European Parliament on electronic signatures are met and trusted environment for creation of qualified electronic signatures is applied.

Privacy Enhancements: Public single-sign-on solutions, such as OpenID, are hardly protected, smartcard based signature solutions and client based solutions (e.g., used for e-government) are vulnerable. The major focus of this roadmap is to guarantee security and privacy in the following way: Moves toward the surveillance society and profiling activities must be prevented. We will evaluate current privacy enhancing technologies (e.g., pseudonymization) for its applicability to be used in combination with identity management systems. Attacks such as replacing the device driver, modifying the code of certain local applications and extending the code of a running process are prevented by using a trusted code execution environment. Regarding attacks on digital signatures, a security token can prevent manipulations of digitally signed documents and the secure viewer application. Trojan horse attacks on the client are also prevented by our solutions, but our research effort will focus

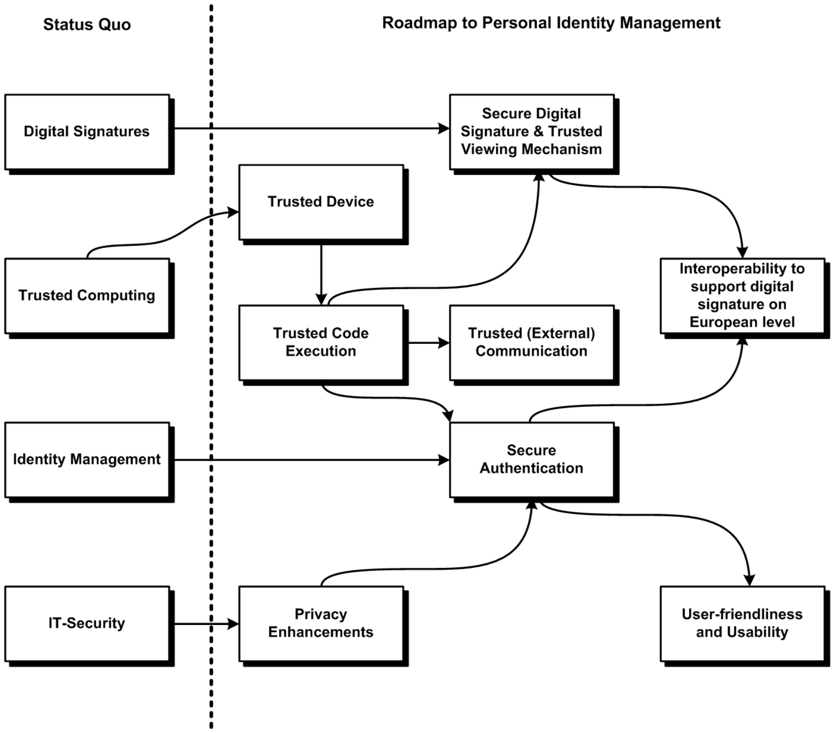
Status Quo
Roadmap to Personal Identity Management
Digital Signatures
Secure Digital Signature & Trusted Viewing Mechanism
Trusted Device
Trusted Computing
Interoperability to support digital signature on European level
Trusted Code Execution
Trusted (External) Communication
Identity Management
Secure Authentication
IT-Security
Privacy Enhancements
User-friendliness and Usability

Figure 1. Roadmap

on identifying potential malware (e.g., Trojan horse) attacks directly affecting the processing chip of the token. Identity theft (e.g., Man-in-the-Middle attacks) will be mitigated by relying on client authentication with digital signatures instead of the insecure alternative using PIN/TAN.

Trusted Code Execution Environment: The trusted code execution environment demands a trusted device as basis in order to allow to run applications even in insecure environments (e.g., PC, Cybercafé). It uses the token's processor to execute program logic. Additionally, the token's cryptographic processor can be used for supporting the execution of cryptographic operations that are demanded by the program logic.

Secure Authentication: The secure authentication unit allows a secure login procedure in different areas of application. The system provides the user with a management cockpit to effectively control and properly verify his various identities and roles. Authentication information is based on knowledge, ownership or characteristic that is controlled through this component. The successful authentication is prerequisite for the use of other components existing on the security token. Authentication is the second step of a two-step process; the first is identification. The proposed security token solution relies on strong authentication that enforces two-factor authentication or multi-factor authentication using some combination of a password, token, public key certificate or biometric device.

Secure Digital Signature and Trusted Viewing Mechanism: Users should feel confident that the security of their security device (e.g., token) is legally recognized as a secure signature-creation device. From the perspective of the Directive 1999/93/EC the recognition can be the result of a conformity and evaluation assessment by a designated independent certification body. Therefore, the key issue to produce qualified electronic signatures is a successful conformity assessment and evaluation of the secure signature-creation device to be developed. One aim must be to obtain a certification using the common methodology for IT security evaluation as secure signature-creation device for qualified electronic signatures in accordance with the European Directive 1999/93/EC and at least one national signature act. The secure signature-creation unit must allow to sign and verify documents. Existing signature applications are vulnerable because the program code is executed on the PC. The signature application should only be executed in the trusted code execution environment on the trusted device. The application of a secure digital signature demands the use of a trusted viewer in order to guarantee that the user only signs the data he wants to sign. By integrating the trusted viewer on the token, the user gets a "really" trusted viewer for the first time. The trusted viewer can either work with a small display integrated on the token or alternatively in combination with a mobile device. In the latter case the mobile phone works as trusted viewer, where the user has to verify the document he wants to sign. As the trusted viewer is a typical vulnerability in the signature process, at least the following security issues must be addressed: (a) modification of data to be signed, (b) capturing the PIN, (c) signing different data than intended, (d) execution of arbitrary code on the signature creation application, (e) interfering with the communication between signature creation application and signature creation device, and (f) modification of the signed data to be verified.

Trusted (External) Communication: the trusted device must guarantee a secure communication with external entities. (i) The Public Key Infrastructure (PKI) is demanded for disposing a unique public key pair certified by a trusted body, the Certification Authority, which delivers a digital certificate [8]. The public key is made publicly available, the private key is kept on the token. The private key allows its respective owner to prove his identity and use it for authentication and signature purposes. (ii) Other kind of communication can be, for example, the establishment of a VPN connection from the token to the external entity in order to communicate with a server system. The VPN maintains an authenticated, encrypted tunnel for securely passing data traffic over the network (typically, the Internet), in order to provide the intended confidentiality (blocking snooping and thus packet sniffing), sender authentication (blocking identity spoofing), and message integrity (blocking message alteration) to achieve privacy.

Interoperability to support digital signature on European level: The challenge regarding interoperability is based on the lack of technical interoperability standards on a European level. This has led to many isolated national secure signature-creation devices and technical specifications, where certificates from only one certification authority can be used for one application. Therefore it is imperative to bridge the cross-national limitations with an interoperability software layer that links signature software through application interfaces. This area of research and development is concerned with software interoperability as there is no signature application standard on a European level. A concept for cross-border usage of signature creation devices for creation and verification of qualified electronic signatures will be provided. Each qualified certificate issued by a certification service provider comes with signature software.

User-friendliness and Usability: User-friendliness and usability are some major pillars needed for the acceptance of a security solution by the user. The research challenge is to develop a practical solution of a European electronic signature-creation device for qualified electronic signatures on a European-wide scale, so that there will be no need to the user for further software installations. No sensitive data is sent outside the USB token. Special attention should be drawn on two main research and development areas: (i) software to enable cross-border interoperability in order to sign and verify accordingly and (ii) integration of software into a trusted device as secure signature-creation device. This unique combination has several advantages such as mobility, ease of use and effectiveness so that each user can generate and verify qualified electronic signatures on a cross-border European level without installation of hardware and software. There is no need to remember the PIN code.

IV. Conclusion

This paper presented a research roadmap for personal identity management. Based on recent literature, this paper identified shortcomings of existing approaches especially regarding security and privacy and open research challenges. The focus of the evaluation was on the user side. The user should benefit from not having to install hardware devices (e.g., card reader) or software (e.g., driver, signature applications) and from having a security environment to go, that can also be used in insecure environments. Moreover, the solution will definitely foster the use of secure signature-creation devices as it makes it easy to sign and verify documents anywhere in Europe by the use of a single device. However, the benefits of increased usability and manageability have to be juxtaposed with privacy issues that potentially occur when a considerable quantity of functionality is concentrated in one single device. The proposed research challenges serve as an enabler for realizing the full benefits, e.g., of public applications, such as e-government, e-health, etc. However, first and foremost it provides private persons with a trusted device that allows them a more efficient and especially more secure life in the Internet.

V. Acknowledgments

This work was supported by grants of the Austrian Government's FIT-IT Research Initiative on Trust in IT Systems under the contract 816158 and was performed at the research center Secure Business Austria funded by the Federal Ministry of Economy, Family and Youth of the Republic of Austria and the City of Vienna.

References

[1] Forrester Consumer Technographics Q2 2004 European study.

[2] A. Alsaid and C. J. Mitchell. Dynamic content attacks on digital signatures. *Information Management & Computer Security*, 13(4):328–336, 2005.

[3] J. Backhouse. Interoperability of identity and identity management systems. *Data Protection and Data Security*, 30(9):568–570, 2006.

[4] J. Backhouse and R. Halperin. Approaching interoperability for identity management systems. In K. Rannenberg,. D. Royer, A. Deuker, *The Future of Identity in the Information Society*, Springer, 2009.

[5] M. Bauer, M. Meintz, and M. Hansen, editors. *Prototypes and concepts of identity management systems*. FIDIS Deliverable 3.1. Available at: Fidis.net, 2005.

[6] G. Crossman. *Digital identity management*, chapter The ID problem, pp. 175-83. Hampshire: Gower, 2007.

[7] P. Dunleavy, H. M. S. Bastow, and J. Tinkler. *Digital era governance*. Oxford University Press, 2006.

[8] G. Forget and A. Stervinou. The virtual smart card. *Card Technology Today*, 19(7-8):12, 2007.

[9] D. Fox. Zu einem prinzipiellen Problem digitaler Signaturen. *DuD Datenschutz und Datensicherheit*, 22(7):386–388, 1998.

[10] P. Girard and J.-L. Giraud. Software attacks on smart cards. *Information Security Technical Report*, 8(1):55–66, 2003.

[11] R. Halperin and J. Backhouse. A roadmap for research on identity in the information society. *Identity in the information society journal*, 1(1), 2008.

[12] R. Holtfreter and K. Holtfreter. Gauging the effectiveness of US identity theft legislation. *Journal Financial Crime*, 13(1):56-64, 2006.

[13] A. Josang, D. Povey, and A. Ho. What you see is not always what you sign. In *Proceedings of 2002 Annual Technical Conference of the Australian UNIX and Open Systems User Group*, 2002.

[14] R. Kennell and L. Jamieson. Establishing the genuinity of remote computer systems. In *12th Usenix Security Symposium*, 2003.

[15] T. Kinder. Mrs miller moves house: the interoperability of local public services in Europe. *J Eur Soc Policy*, 13(2):141-157, 2003.

[16] B. Koops. Counter-profiling by ”weak” parties. In *Implications of profiling practices on democracy and rule of law*. M. Hildebrandt and S. Gutwirth and P. De Hert, 2006. FIDIS Deliverable D7.4.

[17] B. Koops and R. Leenes. Identity theft, identity fraud and/or identity-related crime. *Data Protection and Data Security*, 30(9):553–559, 2006.

[18] H. Langweg. Malware attacks on electronic signatures revisited. In J. Dittmann, editor, *Sicherheit 2006. Konferenzband der 3. Jahrestagung Fachbereich Sicherheit der Gesellschaft für Informatik*, pages 244–255, 2006.

[19] D. Marron. Alter reality: governing the risk of identity theft. *British Journal of Criminology*, 48:20-38, 2008.

[20] T. Messerges, E. Dabbish, and R. Sloan. Examining smart-card security under the threat of power analysis attacks. *IEEE Transactions on Computers*, 51(5), 2002.

[21] F. Nentwich, E. Kirda, and C. Kruegel. Practical security aspects of digital signature systems. Technical report, Secure Systems Lab, Technical University Vienna, 2006.

[22] B. Otjacques and F. Feltz. Interoperability of e-government information systems: issues of identification and data sharing. *J Manage Inf Syst.*, 23(4):29-51, 2007.

[23] U. Pordesch. Risiken elektronischer Signaturverfahren. *DuD Datenschutz und Datensicherheit*, 17(10):561–569, 1993.

[24] U. Pordesch. Der fehlende Nachweis der Präsentation signierter Daten. *DuD Datenschutz und Datensicherheit*, 24(2):89–95, 2000.

[25] W. Schindler. A timing attack against RSA with the chinese remainder theorem. In *International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, 2000.

[26] H. Scholl. Interoperability in e-government: more than just smart middleware. In *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, page 123. IEEE, 2005.

[27] A. Seshadri, M. Luk, E. Shi, A. Perrig, L. van Doorn, and P. Khosla. Pioneer: Verifying code integrity and enforcing untampered code execution on legacy systems. In *ACM Symposium on Operating System Principles (SOSP)*, 2005.

[28] U. Shankar, M. Chew, and D. Tygar. Side effects are not sufficient to authenticate software. In *13th Usenix Security Symposium*, 2004.

[29] A. Spalka, A. B. Cremers, and H. Langweg. The fairy tale of ’what you see is what you sign’ - Trojan horse attacks on software for digital signatures. In S. Fischer-Hübner, D. Olejar, and K. Rannenberg, editors, *Proceedings of the IFIP WG 9.6/11.7 Working Conference.*, pp. 75–86, 2001.

[30] A. Spalka, A. B. Cremers, and H. Langweg. Trojan horse attacks on software for electronic signatures. *Informatica, Special Issue ”Security and Protection”*, 26:191–204, 2002.

[31] J. Taylor, M. Lips, and J. Organ. Identification practices in government: citizen surveillance and the quest for public service improvement. *Identity in the Information Society*, Springer, 2009.

[32] D. Wood. *A report on the surveillance society*. Information Commissioner Office, 2006.