Data protection and multi-application smart cards - the use of intelligent servers to ensure interoperability and data flow requirements

Dinant, Jean-Marc; Keuleers, Ewout

Published in:
Computer Law and Security Report

Publication date:
2005

Document Version
Publisher's PDF, also known as Version of record

Computer Law & Security Report (2005) 21, 146–152

Computer Law
&
Security Report

DATA PROTECTION IMPLICATIONS OF SMART CARD SCHEMES

Data protection and multi-application smart cards – the use of intelligent servers to ensure interoperability and data flow requirements

Ewout Keuleers, Jean-Marc Dinant

CRID – University of Namur, Belgium

Abstract This is the third part of a paper, commenced in CLSR in 2003–2004, that looked at the data protection implications of multi-application smart cards. Technical solutions were then canvassed to demonstrate that any privacy concerns could be overcome. In this final part, the authors look at the use of the card over communications networks and EU regulation of the data protection implications.

A. Introduction

Multi-application smart cards are becoming more and more common. In order to take benefit from the opportunities offered by multi-application smart card schemes, e.g., the generation of value-added information or services, authorities at different tiers are underway implementing local and national smart card schemes. However, from a privacy point of view, the use of such ''universal'' cards, incorporating various applications, is not without concerns. Although cross-profiling is not unlawful by definition and an analysis of the collected data can be legitimate, it is clear that such technologies can also be used for other purposes. To avoid the creation of George Orwell's 1984 *Big Brother*, the implementation and exploitation of multi-application smart card schemes must respond to some basic preliminary requirements.

In the first part of this paper,[1] we dealt with the privacy principles regarding the use of global unique identifiers for the cross-profiling of personal data of smart card holders. In addition to the role of each actor concerned, notably the application providers and smart card manufacturer, we commented on the legal constraints to develop

E-mail addresses: ewout.keuleers@fundp.ac.be, ictlaw@gmail.com (E. Keuleers), jmdinant@fundp.ac.be (J.-M. Dinant).

[1] Ewout Keuleers and Jean-Marc Dinant, ''Data protection: multi-application smart cards: the use of global unique identifiers for cross-profiling purposes'', [2003] 19 CLSR 480.

0267-3649/$ - see front matter
doi:10.1016/j.clsr.2005.02.001

less privacy-killing technologies. Hereafter,[2] some technical solutions were proposed to demonstrate that multi-application smart card technology can be reconciled with the principles of personal data protection legislation. In this respect three technical solutions were analysed and criticized. While the first two solutions relate to the role and functioning of the scheme's application providers, the third solution consists out of the development of less privacy-infringing smart card technology in relation to the use of unique identifiers.

In this third and final part, we will asses the flow of personal data over the multi-application smart card's communication networks, interconnecting the different application providers. In this analysis, the use of so-called intelligent servers to increase the multi-application smart card's interoperability and the role of the communication provider will be central.

B. *SmartHub*: privacy and intelligent servers

The implementation of so-called 'intelligent servers' in a multi-application smart card scheme (MSC) is a valuable contribution to the overall success of such a scheme. The scheme's open architecture will make it possible to integrate additional applications in the existing configuration, without many technical constraints. In addition, an intelligent server, for instance SmartCities' *SmartHub*, guarantees the interoperability between the different application providers of a local smart card scheme and the interoperability between different (local) schemes.[3]

The objective of SmartCities,[4] *SmartHub* is to design a centrally managed high-performance engine, for data movement and interface management across multi-application smart card scheme applications, to complete the open architecture developed by the existing SmartCities project.[5] To illustrate the added value of *SmartHub*, the following illustration can be given.

In order to avoid a card holder having to register each time he intends to make use of a new scheme service, e.g., swimming pool, library, etc. the concerned application provider can use the holder's smart card to identify the card holder and to retrieve personal data from the centrally managed data base.[6] Therefore, frequently used data — for instance name, surname, address, phone number, date of birth, etc., will only have to be asked once and will be stored and kept up to date in the central data base. Therefore, the centrally managed personal data do not have to be asked for over and over and can be sent whenever and wherever needed. The centrally placed *SmartHub* assures the interoperability between the different application providers and the central data base of the MSC scheme, and thus the proper data flow in the MSC scheme.

Before assessing the privacy constraints on the development and implementation of *SmartHub*, a distinction should be made between the legality of the MSC scheme as such and *SmartHub*'s role in this configuration.[7] On the one hand, one should consider to what extent Directive 95/46/EC allows the central management and processing of personal data, notably the free data flow between the scheme's application providers.[8] On the other hand, the integration of *SmartHub* in a multi-application smart card scheme brings forward the following two issues.

In the first place, one should consider the application of the general data protection principles contained in Directive 95/46/EC. Secondly and considering the fact that personal data will be communicated over a network, one has to consider the principles of Directive 2002/58/EC on privacy in electronic communications networks.[9] In relation to the latter Directive, the focus will be on the proper nature of the smart card communications network, connecting the different applications and actors. If this is a private network, this Directive is not applicable. If, on the contrary, the network is considered a public one, the principles laid down in this Directive become applicable.

C. Application of Directive 95/46/EC

Recital 47 of Directive 95/46/EC states that: ''*where a message containing personal data is*

[2] Jean-Marc Dinant and Ewout Keuleers, ''Data protection: multi-application smart cards: the use of global unique identifiers for cross-profiling purposes, towards a privacy enhancing smart card engineering'', [2004] 20 CLSR 22.

[3] Cf., *infra* on public networks and pan-European smart card schemes.

[4] www.smartcities.gov.uk.

[5] SmartHub Business White Paper, Black Sea Consulting, August 2002.

[6] This central database has to be distinguished from the central data warehouse. SmartCities' Data warehouse contains the anonymous data used to make global cross-profiles of the card holders.

[7] In this regard, we refer to the first two parts of this contribution on data sharing and the use of global unique identifiers (GUI).

[8] Cf., articles 6 and 7 of Directive 95/46/EC.

[9] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, *Official Journal L 201, 31/07/2002 P. 0037 — 0047*.

	Application Provider	*SmartHub*
Content of the message	Controller	
Additional data are generated (*e.g.*,traffic data)		• Controller for the created data; and • Processor, transmitting the message on behalf of the application provider
No additional data are generated		• Processor, transmitting the message on behalf of the application provider

Figure 1 SmartHub: data controller or processor?

transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service''.

In this regard, the following conclusions can be made.[10] In the first place, the application providers present in a multi-application smart card scheme are and remain controllers for the data contained in the communicated message or content. We underline that it is possible that a number of persons are jointly considered controllers within the meaning of Directive 95/46/EC. In the second place, communication providers such as *SmartHub* will only be considered data controllers in respect of the additional personal data created to provide their service[11] such as, for instance, traffic data. In this hypothesis, it will be *SmartHub*'s responsibility to comply with data protection legislation and, e.g., to inform the data subjects of the kind of personal data being processed and for what purposes.[12] Eventually, if no additional data necessary for the provision of the service are generated, *SmartHub* will be storing and transmitting personal data on behalf of the application providers, i.e., the data controllers. In this view, *SmartHub* can be qualified data processor Fig 1.

Nevertheless and irrespective of the qualification of processor and/or controller, both the data controllers and processors must adopt appropriate technical and organizational measures to protect personal data against unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.[13]

D. Application of Directive 2002/58/EC

Article 3 of Directive 2002/58/EC states that: ''*this Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community*''.

In order to determine whether this Directive is applicable or not, the following two questions have to be answered:

- Is the service provided an electronic communications service?
- Is the service concerned provided over a public network?

1. An electronic communications service

By virtue of the Framework Directive for electronic communications,[14] an ''electronic communications service'' is defined as: ''*a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic*

[10] Also see Cécile de Terwange and Sophie Louveaux, ''Data protection and Online Networks'', *Computer Law & Security Report*, [1997] 13 CLSR 237.

[11] See also recital 26 of Directive 2002/58/EC.

[12] Cf. article 6.2 of Directive 95/46/EC and article 10 of Directive 1995/46/EC.

[13] Article 17 of Directive 95/46/EC.

[14] Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services.

communications networks and services; it does not include information society services[15] *which do not consist wholly or mainly in the conveyance of signals on electronic communications networks*''.

As indicated before, this definition underscores that the regulation of the content as such must be differentiated from the regulation of the transmission. In principle, *SmartHub* assures the data flow and interoperability between different application providers and therefore enables a message to be delivered, this irrespective of the communication protocols used. In this light, it is evident that the service provided for consists of the communication of a message, this irrespective of its content.[16]

2. An electronic communications service provided over a public network

Although the latter Directive does not contain a definition of ''*public network*'', explicit reference is made to the definition given in Directive 2002/21/EC.[17] According to this definition, a public network can be considered as: ''*an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services*''.[18] In the light of this definition, one can be skeptic: a public network is a network used to provide a public service. Therefore, a second question needs to be answered: what is a ''*publicly available electronic communications service?*''

The answer hereto can be found in Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and service. Although the universal service obligations are limited to certain basic communication services, a definition of a concept similar to the one of ''*publicly available electronic communications services*'' can be found. In accordance with article 2 (c) a publicly available telephone service means: ''*a service available to the public for originating and receiving national and international calls and access to emergency services through a number or numbers in a national or international telephone numbering plan*''.

Nevertheless, this answer cannot be satisfactory as it is circular: a public network is used to provide a public service, i.e., a service available to the public. In order to assess the private versus the public character of a network or a service, and in the absence of any other regulatory provision, one may consider the former regulatory framework for telecommunication services.[19]

3. Closed user group and private networks

For many years a ''*public service*'' was considered to be everything that exceeds the scope of a private, corporate network or a closed user group. The latter concepts are defined in a Communication of October 1995 on the implementation of Directive 90/388/EEC on competition in the markets for telecommunications services.

The Communication states that: ''*the term 'for the public' is not defined in the Directive and must be understood in its common sense: a service for the public is a service available to all members of the public on the same basis. Particular examples of services which should not be considered 'for the public', and thus should not be made subject to special or exclusive right, are those provided over corporate networks and/or to closed user groups. Corporate networks and closed user groups (CUGs) cover a number of telecommunications services, both voice and data. They are fundamental to the Services Directive particularly because they fall outside the scope of the voice service which Member State may reserve to their telecommunications organizations*''.

In the first place, ''*corporate networks*'' are defined as those networks generally established by a single organization encompassing distinct legal entities, such as a company and its subsidiaries or its branches in other Member States, incorporated under the relevant domestic company law. Secondly, a ''*Closed User Group*'' (CUG) is defined as a grouping of entities, not necessarily bound by economic links, but which can be identified as being (i) part of a group on the basis of a (ii) lasting professional relationship among themselves, or with another entity of the group, and whose internal communications needs result from (iii) the common interest underlying this relationship. In general, the link between the members of the group is a common business activity.

[15] Information society services are defined by Directive 98/34/EC, as modified by Directive 98/48/EC.

[16] In this regard, reference could be made to the definition of electronic communications network, as defined in article 2 (a) of Directive 2002/21/EC.

[17] Cf., article 2 of Directive 2002/58/EC.

[18] Article 2 (d) of Directive 2002/21/EC.

[19] It must be stressed that the concepts used were introduced before the 1999 'Telecom' Review and the adoption of the Directives in the field of electronic communications. In this light, one should consider whether the concepts of CUG and a network as defined in this Communication are still relevant or accurate.

Although most EDI applications, e.g., fund transfers in the financial sector, airline ticket reservation systems, information transfers between universities involved in a common research project, can be considered private services, this is not always the case in a multi-application smart card scheme.

On the one hand, only selected and authorized application providers may integrate their application in an open smart card architecture. For this reason, the network could be considered as private, i.e., only the ''certified'' application providers may provide their services to the smart card holder. On the other hand, the service, i.e., a multi-application smart card, is available to the public as such or to all members of a certain community. In this light, the application of the notion of CUG is not always so evident. In its opinion on the proposal of Directive COM (2000) 385,[20] Group 29 stressed that personal data processed for the use of closed/private networks would fall solely under the general Directive 95/46/EC. Furthermore, it stated that this was regrettable because private networks were gaining an increasing importance in every day life. This was evident in the increase in communication between individuals, such as in the workplace, and the growth of specific risks to privacy that such networks created e.g. monitoring of employee behaviour by means of traffic data or lack of confidentiality of communications.

In the SmartCities Project, both the Southampton City Council and the University of Southampton have issued their own smart card. While everybody can apply for the City Council's card, the University's smart card is only issued to its students and staff. To the extent that the University community could be considered a CUG, the service provided is a private service and Directive 2002/58/EC is not applicable. In contrast, the smart card issued by the City Council is available to the public, this irrespective of one's residence or nationality. Accordingly, the service provided for has to be considered a public service, subject to Directive 2002/58/EC.

Furthermore, it should be underlined that *SmartHub*'s underlying technology can guarantee the interoperability between local smart card schemes and, therefore, become an important factor in the establishment of pan-European smart card schemes and networks. In this hypothesis, the network of networks will reach out to most of the European citizens, to the extent that the application of the concept of Closed User Group will become very abstract. If *SmartHub* provides its electronic service on public networks, the principles and privacy guarantees of Directive 2002/58/EC have to be considered. In view of the proper nature of the delivered service, i.e., transmission and delivery of messages containing personal data, the most important requirements relate to (i) the secure and confidential character of the service[21] and (ii) the processing of traffic data and location data.

As to the security and confidentiality requirements, recital 20 of Directive 2002/58/EC states that service providers should take appropriate measures to safeguard the security of their services, if necessary in conjunction with the provider of the network, and inform subscribers of any special risks of a breach of the security of the network. Such risks may especially occur for electronic communications services over an open network such as the Internet or analogue mobile telephony. Furthermore, the adopted security measures must be appraised in the light of article 17 of Directive 95/46/EC.

In relation to traffic data, i.e., data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof,[22] a particular regime has been inscribed in article 6 of Directive 2002/58/EC.[23] In application of this article, traffic data relating to subscribers and users, processed and stored by the provider of a public communications network or publicly available electronic communications service, must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. In this regard, it has to be underlined that the completion of the transmission of a communication depends on the type of electronic communications service that is provided. For instance, for a voice telephone call the transmission will be completed as soon as either of the users terminates the connection. For electronic mail the transmission is completed as soon as the addressee collects the message, typically from the server of his service provider.[24]

[20] Article 29 WP, Opinion 7/2000 on the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, 12 July 2000, COM (2000) 385.

[21] Articles 4 and 5 of Directive 2002/58/EC. See also recitals 20 and 21 of Directive 2002/58/EC.

[22] Article 2 (b) of Directive 2002/58/EC.

[23] Article 9 of Directive 2002/58/EC deals with location data other than traffic data.

[24] Recital 27 of Directive 2002/58/EC. See also recital 22 of Directive 2002/58/EC on automatic, intermediate, and transient storage.

	Directive 2002/58/EC	Directive 95/46/EC
Security	Article 4	Article 17
Confidentiality	Article 5	Article 17
Traffic data	Article 6	Article 6 and recital 26

Figure 2 Requirements under Directive 95/46/EC and Directive 2002/58/EC.

Although traffic data may not be stored for longer than necessary[25] or must be made anonymous,[26] a three-fold exception has been foreseen: in the first place, traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.[27] Secondly, traffic data may be processed for marketing electronic communications services or for the provision of value-added services, provided that the subscriber or user to whom the data relate has given his or her consent.[28] Thirdly, Member States may adopt legislative measures providing for the retention of data for a limited period justified on the grounds of national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system.[29]

Although Directive 2002/58/EC leaves it to the individual Member States to define traffic data and to determine the conditions of data retention,[30] it is recommended that this be done in close cooperation and consultation between the 25 Member States. In particular, reference has to be made to the initiatives of the European institutions in the field of cyber crime. Under the Belgian presidency, the European Council presented a proposal for a Framework Decision on the retention of traffic data and on access to this data in connection with criminal investigations and prosecutions.[31] One of the objectives of this Framework Decision is to provide for a common understanding of the concept of traffic data and to harmonize the conditions under which traffic data may or must be retained.[32]

4. Conclusion

In light of the foregoing it is clear that the distinction between private and public networks is not easy to make. Furthermore, how can one defend that a public group of users, e.g., the City Card holders, do benefit from Directive 2002/58/EC, while a private group, e.g., the University Card holders, using the same card and services, are denied the same level of protection. For these reasons, the adoption of a more pragmatic viewpoint can be defended.

Directive 2002/58/EC is not applicable to private networks. Therefore, if one can be sufficiently sure that the service or message stays within the private network, for instance the University's intranet, the requirements imposed by the latter directive can be left in the sidelines. However, from the moment the service exceeds the private scope, e.g., leaves the University network, the Directive becomes applicable. In these circumstances it is submitted that the service is provided over a public network, unless otherwise demonstrated.

Furthermore, the Directive 2002/58/EC deals with principles already covered by the general data protection Directive 95/46/EC. The requirements in the field of security and confidentiality of electronic communications,[33] can be derived from articles 16 and 17 of Directive 95/46/EC,[34] applicable to all networks irrespective of their private or public character. Indeed, recital 10 of Directive 2002/58/EC confirms that Directive 95/46/EC applies in particular to all matters concerning the protection of fundamental rights and freedoms and it also applies to non-public communications services.

[25] Cf., article 6.1 of Directive 95/46/EC.

[26] Cf., recital 26 of Directive 95/46/EC, according to which anonymous data are not subject to data protection legislation.

[27] In this regard, reference has to be made to article 6.1 (e) of Directive 95/46/EC according to which personal data may no longer be stored or processed than is necessary for the purposes for which the data were collected.

[28] Article 6.3 of Directive 2002/58/EC.

[29] Articles 6 and 15 of Directive 2002/58/EC. See also recital 11 of Directive 2002/58/EC. In this regard, reference should be made to the CTOSE project, which stands for Cyber Tools On-Line Search for Evidence. www.ctose.org.

[30] It should be noted that the Member States had to transpose Directive 2002/58/EC before 31 October 2003. In the United Kingdom, this directive was transposed by the Privacy and Electronic Communications (EC Directive) Regulations 2003.

[31] www.statewatch.org/news/2002/aug/05datafd.htm. See also the data retention website of the Electronic Privacy Information Center, EPIC.www.epic.org/privacy/intl/data_retention.html.

[32] Also see the Public consultation and workshop on traffic data retention, European Commission, 16 June 2004. See also Pascal Reynaud, ''*Sombre avenir pour les données de trafic*…'', www.droit.be, 9 September 2004.

[33] Articles 4 and 5 of Directive 2002/58/EC.

[34] Section III of Directive 95/46/EC on confidentiality and security of processing.

If this is so then *SmartHub*, whether providing services on a public or a private network, must take adequate measures to guarantee the secure and confidential nature of the personal data processed and it may not store card data longer than is necessary (Fig. 2).

E. Multi-application SC schemes: conclusions and recommendations

The use of new technologies, such as the development and implementation of multi-application smart card schemes, is not without concerns for one's fundamental rights. More and more citizens, throughout the European Union, will be confronted with such schemes and the underlying privacy issues — notably the use of global unique identifiers for cross-profiling purposes. Nevertheless, it should be emphasized that data protection legislation should not impede its development and that the opportunities offered by these schemes can be reconciled with data protection and privacy principles. All parties involved — industry, policymakers and citizens — should be aware of the associated privacy concerns. On the one hand, the industry should take into account that it is in their proper interest to develop privacy-compliant products, while on the other the confidence consumers have in privacy-compliant products can be strengthened.

Smart card manufacturers need to adopt appropriate technical measures to prevent the unique identifier embedded in the smart card from being accessed by all the scheme providers and therefore becoming a global unique tracking identifier. This may be done by using a crypto random function encrypting the smart card serial number (SSN) with random noise.[35]

Application providers, in their role of data controllers, have an overall liability with regard to the legal obligations imposed by Directive 95/46/EC. They have to take technical and organizational measures to prevent their personal data being processed by other entities. In this respect, they should not use the same identifier as other applications of the same scheme.

The European Commission, by virtue of its competences derived from Directive 1999/5/EC, may take an initiative. Indeed, the latter Directive grants the European Commission the competence to decide that an apparatus shall be so constructed that it incorporates safeguards to ensure that the personal data and privacy of the user or the subscriber are protected.[36] Furthermore, similar provisions have been inscribed in Directive 2002/58/EC on privacy and electronic communications. According to its recital 46 and article 14, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data. Recital 26 states more explicitly that: ''*it may therefore be necessary to adopt measures requiring manufacturers of certain types of equipment used for electronic communications services, e.g., smart card manufacturers, to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected*''.

Since telecommunication terminals may be used — and are commonly used — for legitimate but incompatible purposes by distinct data controllers, the presence of a global unique identifier raises the major risk of purpose re-routing. In addition, it may enable illegal and privacy-invading global cross-profiling activities. Similar to what has been done for mobile cell phones, the European Commission has to make the suppression of the general availability of a GUI a mandatory requirement before putting such telecommunication terminals on the European market. This is now a matter of urgency as more and more telecommunication terminals are transmitting such a GUI (Ethernet Card, RFID's,[37] Smart Card, etc.) to a growing amount of third parties.

Acknowledgements

The authors would like to thank Professor Yves Poullet, Mrs M. Verónica Perez Asinari and Mr Pierre-Yves Potelle for their valuable comments and suggestions.

Ewout Keuleers and **Jean-Marc Dinant**, CRID — University of Namur Belgium. Ewout Keuleers is a researcher at the Centre for Computer and Law (CRID) and an attorney at the Bar of Brussels; ewout.keuleers@fundp.ac.be or ictlaw@gmail.com. Jean-Marc Dinant has a Masters Degree in computer sciences and is about to present his PhD on Personal Data Security on the Internet. He was CRID's coordinator for the SmartCities Project. www.smartcities.gov.uk; jmdinant@fundp.ac.be. CRID is a research center for Computer and Law at the University of Namur (Belgium). www.crid.be.

[35] Cf., Part 2 of this paper, Jean-Marc Dinant and Ewout Keuleers, '' Data protection : multi-application smart cards : the use of global unique identifiers for cross-profiling purposes — Part 2 : towards a privacy enhancing smart card engineering'', [2004] 20 CLSR 22.

[36] Cf. article 3.3 (c) of Directive 99/5/EC.

[37] Ewout Keuleers and Etienne Wéry, ''Gillette incorpore un identifiant unique dans ses rasoirs : rasez-vous, vous êtes fliqué !'', www.droit-technologie.org , 3 September 2003.