FIDIS

Future of Identity in the Information Society

Title:	D4.12: A qualitative comparative analysis of citizens' perception of eIDs and interoperability
Author:	WP4
Editors:	Ruth Halperin, James Backhouse (LSE, UK)
Reviewers:	Els Kindt, KUL, Wainer Lusoli, JRC
Identifier:	D4.12
Type:	[report]
Version:	1.0
Date:	Sunday, 28 June 2009
Status:	[final]
Class:	[Public]
File:	D4.12.fidis_deliverable.wp4.final.doc

Summary

This report investigates citizens' perceptions towards the adoption of interoperable electronic identity systems in the EU context. It focuses on empirical data collected from UK and German citizens during the course of the FIDIS project and analyses it in order to obtain a deeper understanding of the way that citizens perceive the risks being incurred by the move towards eGovernment systems in particular. Using qualitative, grounded theory methods the analysis derived five discrete risk areas that are felt to pertain in this regard: systems and technology, competence of authorities, integrity of authorities, the control of personal data, and the power balance between citizen and state. There follows an analysis and discussion of the findings developing the themes of social risks and some implications for state policy in this area.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Information Society Technologies

Copyright Notice:

PLEASE NOTE: This document may change without notice – Updated versions of this document can be found at the FIDIS NoE website at www.fidis.net.

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz (ICPP)	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University[1]	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne (MU)	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science (LSE)	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Centre Technique de la Gendarmerie Nationale (CTGN)	France
19. Netherlands Forensic Institute (NFI)[2]	Netherlands
20. Virtual Identity and Privacy Research Center (VIP)[3]	Switzerland
21. Europäisches Microsoft Innovations Center GmbH (EMIC)	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

[1] Legal name: Stichting Katholieke Universiteit Brabant
[2] Legal name: Ministerie Van Justitie
[3] Legal name: Berner Fachhochschule

Versions

Version	*Date*	*Description (Editor)*
0.1	22.03.2009	• Initial release (Ruth Halperin)
0.2	30.03.2009	• Closing chapters (James Backhouse)
0.3	10.04.2009	• Revised final draft (Ruth Halperin)
0.4	15.04.2009	• Version ready for internal review (Ruth Halperin)
0.5	30.04.2009	• Comments from reviewers (Els Kindt, Wainer Lusoli)
0.6	22.06.2009	• Revised version following review (Ruth Halperin)
1.0	25.06.2009	• Final version for submission (James Backhouse)

Table of Contents

1 Executive Summary

This report investigates citizens' perceptions of the information risks implicit in the spread of electronic identities. It focuses on data collected from UK and German citizens during the course of the FIDIS project and analyses it in order to obtain a deeper understanding of the way that citizens perceive the risks being incurred by the move towards eGovernment systems in particular. The study is not quantitative but qualitative and using grounded theory methods it derives 5 discrete risks that are felt to pertain in this regard: systems and technology, competence of authorities, integrity of authorities, the control of personal data, and the power balance between citizen and state. There follows an analysis and discussion of the findings developing the themes of social risks and some implications for state policy in this area.

Systems and technology are seen to be risks insofar as the reliability and dependability of the information systems that electronic identities require are seen as still wanting in some respects, with expectations of failures at crucial moments.

Beyond the information systems lie the management and administrative systems that state departments operate and here too citizens feel that there are information risks owing to the doubts about the performance of these bodies. Recent data losses in the UK and the USA have served to redouble concerns about the **competence levels** in staff and bureaucratic processes.

Citizens have reserves also about the **integrity of government** in respect of maintaining protection for their data, in short there is a lack of trust that information privacy principles will be applied to their data at all times. The notion of 'function creep' emerged repeatedly to refer to this risk.

Control of data is also seen as problematic in that citizens have felt that their control over their personal information is inadequate for a properly privacy-respecting regime. The feeling is that opportunities to request consent for how data is shared are not being offered to citizens.

More generally with the move towards identity based eGovernment systems a risk of **an over-powerful** state is being perceived. These new systems are felt to put an inordinate amount of power into the hands of the digital state, with inadequate remedies available to citizens in the event of contingencies occurring.

The discussion ranges across issues of the need for trust to be won back by state agencies if the digital state agenda is to be successful to questions of how the balance of efficient interoperable systems and appropriate consent opportunities may be decided. The authors accept that an efficient administration needs to countenance new purposes for existing data but must nevertheless offer ways of consent being requested. Finding the right threshold that triggers a request is going to be critical. Too many requests for consent may be just as bad as too few or none at all. The discussion ends in a question about whether there is a need for a digital social contract between state and citizen to determine boundaries around many of these questions that have only emerged alongside the digital state itself.

2 Introduction

> ***I am concerned that one day I shall present my ID card, only to be told that the state no longer recognizes my existence. "The card is never wrong, sir". Meanwhile, organized crime will have no difficulty in exploiting ID cards at everyone else's expense*** *(an anonymous UK citizen)*

The research reported in this deliverable was set out to perform a qualitative analysis of citizens' perception on interoperable Identity Management Systems (IdMS) in the EU, public sector. The study draws from empirical data collected from UK and Germany, and presents a grounded analytical framework depicting an array of perceptions pertaining to electronic identity (eID).

3 Background

This study is a continuation of the research undertaken by FIDIS WP4 in 2006 exploring attitudes of citizens towards eID. In this context a survey was launched entitled "A survey on citizens trust in ID authority and systems"[4]. This web-based closed questionnaire produced a significant response for the quantitative analysis contained in the research deliverables 4.4 and 4.5 cited below as well as in the recently published FIDIS book (Backhouse and Halperin, 2009[5]). The data set that forms the basis for the empirical study in the present deliverable derives from the qualitative part of the research that used an open-ended question at the end of the survey questionnaire, which invited respondents to comment freely on the issues forming the subject of the survey. This generated a wealth of statements made by respondents in the form of free text. In particular, high response rate in both UK and Germany lend itself to rigorous content analysis. We took it as both an opportunity and a necessity to offer an analysis of this unique data set, which goes beyond indicating whether citizens were 'for' or 'against' eID, to uncovering underlying reasoning and perceptions.

[4] Report available at: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp4-del4.4.survey.pdf

[5] Backhouse, J., & Halperin, R. (2009). Approaching Interoperability for Identity Management Systems. In K. Rannenberg, D. Royer, A. Deuker (Eds.), *Identity in the Information Society: Challenges and Opportunities* (pp. 245-268) Berlin Heidelberg: Springer.

4 Motivation

As the move towards eGovernment gathers pace in Europe, the impact of the digitalisation of many citizen-state interactions is beginning to challenge accepted wisdom on what digital citizenship consists of, what its risks are, and how they might be managed in the new digital era.

Although much has been written about the need for the greater efficiency that eGovernment is presumed to bring about, the main perspective taken has been from the state's point of view (Cf. Nixon and Koutrakou, 2007). Electronic delivery of governmental services, such as tax and benefits, has been seen universally as advantageous. Little is known about the views of the citizen on these new developments and yet gradually the idea is just beginning to sink in that public consent and acceptance of new IdMS will be useful if not vital. A research programme currently underway in the UK "Ensuring Privacy and Consent in Identity Management Infrastructures"[6] has drawn attention to the role of the citizen in ushering in successful new IdMS. How citizens perceive ID schemes emerged as a key concern[7]:

> *If they [citizens] did not have confidence in a scheme, take up would be slow, motivations of some to undermine it strong, and the net result would be an ineffective scheme. Hence, research to uncover the precise nature of citizen fears with an aim of developing at the very least a communication programme or hopefully a dialogue with citizens should be a high priority. Research should focus on those currently most affected by ID programmes, since their fears will be most advanced.*

In the midst of much discourse about the functionality of such systems, often ignored is the necessity for considering the perceptions and concerns of the citizen about new technology that deploys identity management in the context of eGovernment. The term "citizen-centric" (cf. Lips, 2007) has been developed[8] to refer to this aspect of the emerging systems, an aspect that may vitally affect whether or not such systems win public acceptance. The eventual institutionalisation of eGovernment systems will almost certainly require that they prove to be amenable and acceptable – i.e. citizen-centric. Time and again large-scale systems prove to be eventual failures as the result of resistance from end-users during the phase of implementation (Bauer, 1997).

[6] http://www.epsrc.ac.uk/Events/DigitalIdentities
[7] http://www.kablenet.com/KE.nsf/EventsSummaryView/0CFE397AFD0FF888802572E50050D62B?OpenDocument
[8] http://www.digitalchallenge.gov.uk/links-and-resources/research/study-on-organisational-change-for-citizen-centric-egovernment

Notwithstanding this, there is almost complete lack of EU evidence on eID services perceptions (Lusoli and Miltgen, 2009)[9]. A perceptible gap in research exists therefore with respect to citizens' perceptions of new IdMS, which deserve attention and consideration. Citizens are the ultimate sponsors and ought to be the beneficiaries of any government identity scheme. Furthermore, citizens' perceptions hold important implications for any future attempts at implementing new IDMs, for they may well be translated into subsequent behaviours, namely, resistance to use, misuse, or non-use.

9 Available: http://ftp.jrc.es/EURdoc/JRC50089.pdf.

5 Structure of this report

In this brief introduction we have presented the rationale underlying this research, highlighting the pertinent need for studying issues related to interoperable IdMS as perceived by EU citizens. The remainder of this report is structured as follows. The next section introduces the methodology used in the study. We explain the choice of a qualitative interpretivist approach to guide this study, describe how we collected the data and used grounded research method for data analysis. Then follows the main part of this report, presenting and demonstrating the findings of this research. The empirically grounded framework that emerged from the analysis uncovers the diverse set of perceptions held by German and UK citizens as regards eID and interoperability. This is followed by a discussion of some key implications arising from the analysis.

6 Methodology

The methodology adopted in this study draws from grounded theory (Glaser and Strauss, 1967; Martin and Turner, 1986) as it offers a research method that seeks to develop accounts that are grounded in data. This generative approach seemed particularly useful here, given that no systematic research on this topic has been published to date. In particular, we adopted the analytical technique of open coding (Strauss and Corbin, 1990) as explained further below. This method provides for an exploratory and context-based research into the phenomenon at hand.

The inductive and contextual characteristics of the methodology suggested by grounded theory fit with the interpretive orientation of this research. The focus here is on developing a context-based description, with an aim of generating an account of citizens' perceptions regarding public sector IdMS.

6.1 Data collection

The data for this study was collected using a web survey method. The survey was designed in two parts, one consisting of a closed questionnaire[10] and a second part, aiming at obtaining qualitative data, consisting of an open-ended question that invited respondents to comment freely on the subject of electronic identity in the public sector, government context. This technique generated a wealth of data – statements made by respondents in the form of free text.

The web survey used in the study was translated into eight different European languages in order to maximize the diversity of respondents. The first stage in preparing the data for this study therefore involved translation of all data into English so as to allow a standardised analysis. Once the translation was completed, with the help of FIDIS partners in the different countries, the process of content analysis began.

Statements made by respondents varied in terms of length and their level of elaboration, for example, few respondent stated: *'1984'* whereas one other explained in more detail:

> *It's an absolute necessity to pare the amount of centrally stored electronic data to the absolute minimum. Especially cross-comparison of different data bases must be permitted by law, just as access to this data by companies/business. Additionally, it must not be possible to read out electronic data stored on regular ID cards by radio frequency or any other contactless method, because every encoding, encryption or access protection will be cracked, which is just a question of time. Business/companies, banks and insurances have economical interests to get access to this data, so that access must be permitted by law.*

[10] Results can be found at http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp4-del4.4.survey.pdf

Whilst the dataset obtained for this study provided a rich and revealing source about citizen perceptions, some limitations associated with the chosen method of data collection are nevertheless evident because web surveys are self-selected samples. We could have opted for in-depth interviews but this method has its own drawbacks. Interviews would not have provided large, diverse and anonymous responses derived through the web survey. Another issue with a web survey is the potential response bias. It may be argued that those with strong opinions on IdMS were most eager to respond. Given these considerations, our findings cannot be said to represent the population in general as no controlled sampling was applied. However, this does not undermine the validity of the data nor lessen the importance of the findings that emerged from the analysis. The study was not designed to provide statistical generalisability (Yin, 1984), however, it may properly lay claim to analytical generalisability, in particular, to the common type of generalising from data to descriptions (Lee and Baskerville, 2003).

In contrast to the quantitative survey providing results from eight EU countries, the national representation of the data used in this study was limited to two countries only, namely, Germany and UK. While the response rate in those countries lent itself to rigorous content analysis, the number of responses from other countries was to small to allow inclusion. The overall number of qualitative responses from UK citizens was N=377 and in Germany N=360.

6.2 Data analysis

Making sense of the large body of unstructured text generated from the web survey required the creation of a grounded analysis framework. Content analysis of the text gradually led to the creation of a framework of underlying reasoning or beliefs that characterised the range of responses and attitudes. This technique uses a form of content analysis where the data are read and categorized into concepts that emerge from the data themselves rather than imposed from outside (Agar, 1980). This method of open coding (Strauss and Corbin, 1990) relies on an analytical technique of identifying possible categories and their properties and dimensions. As the data are examined, concepts are organized by recurring themes. These themes become prime candidates for a set of stable and common categories, which link a number of associated concepts. This is known as axial coding (Strauss and Corbin, 1990) and relies on a synthetic technique of making connections between sub-categories to construct a more comprehensive scheme. The goal is to determine a set of categories and concepts that covered as much of the data as possible (Orlikowski, 1993). This iterative examination yielded a set of broad categories and associated concepts that describe the range of perceptions held by citizens. In the next section we introduce the refined categories by turn, illustrating each one with the data from which it emerged.

7 Findings

The grounded analysis of the data set gradually gave expression to a number of high-level constructs that were slowly narrowed down into a manageable handful of framework elements. As the analysis proceeded, the categories were refined into an ever-smaller number of these elements. The framework needed to be simple but high-level in order to capture as wide range as possible of citizens' perception within that smaller set of constructs. We now present a high-level introduction to the framework that was refined in this manner.

Grounded framework overview

One dimension that emerged was termed ***systems and technology*** *(7.1)*. Although technology was seen to be more dependable than in the past there were fears about the robustness of identity management systems in particular. The theme of system and technology emerged from the analysis of both the UK and German data. Citizens perceptions categorised here are those referring directly to IT components of IdMS. Four subcategories were identified under Systems and Technology. The first subcategory is comprised of *general assessments of IT in IdMS (7.1.1)*, reflecting general concern over technological limitations. The two subcategories that follow focus instead on specific technologies namely: *biometrics (7.1.2)* and *RFID (7.1.3)*. *Central database (7.1.4)* is the fourth and final subcategory located under the technology theme. Security issues related to central database architecture for IdMS was cited as the major reason why citizens should fear the large-scale deployment of interoperable electronic IDs.

The theme of ***public authority competence*** (7.2) emerged from the data analysis in both countries. It refers to citizens' perceptions regarding the ability of the state and its departments to secure and manage personal data. Three subcategories were identified under the competence theme. First are *general perceptions (7.2.1)* regarding the competence, or rather, incompetence of public administration. The remaining two subcategories are more closely related to technology use in public sector, one questions *technical proficiency* (7.2.2) in public authority and the other focus on perceived *success/failure* of large-scale IT project implemented by public authority (7.2.3).

Alongside competence, the ***integrity of public authorities (7.3)*** ranked high with both German and UK citizens, concerned about questions of truthfulness and fairness from the institutions of the state in respect of their handling of personal data. Trust is the key issue brought fourth in the perceptions of citizens associated with the theme of public authority integrity. These perceptions were further sorted into two subcategories suggested by the grounded analysis: the first subcategory refers to *general distrust* in public authorities (7.3.1). It ranges from moderate expressions of *mistrust* to the view of governments as *corrupt*. The second subcategory addresses the interoperability issue of sharing personal information, that is consequent on trust in authorities. Concern from *mission creep (7.3.2)* was expressed in general terms (7.3.2.1), in reference to *multiple* 'third parties' (7.3.2.2) and in reference to specific third parties or uses, namely: *commercial (7.3.2.2.1)* and *law enforcement (7.3.2.2.2)*.

A major theme that emerged from the analysis captures citizens' perceptions concerning ***control over personal information*** (7.4). Few respondents addressed the issue of *data integrity* in this context (7.4.1), which made up one subcategory in the analysis. Another issue addressed by the second subcategory was that of *transparency* afforded to citizens (7.4.2). Finally, the most crucial issue represented in the third subcategory of the control theme concerns *disclosure by consent (7.4.3)*.

The last theme comprising of the framework is ***citizen-state power balance*** (7.5). This theme represents citizens' perceptions concerning changes to power relations that interoperable IdMS might bring about. Expressions of fear from a detrimental shift in citizen-state power balance varied in the use of metaphors and of tone. To captures these variations, expressions were classified into a set of data-driven subcategories: *Surveillance society of glassy citizens (7.5.1); Criminalisation of civil society (7.5.2), Imperil freedom and civil liberties (7.5.3);* and, *Totalitarian regime (7.5.4) with the two subsets Nazism/Fascism/Dictatorship (7.5.4.1), and, Big brotherism (7.5.4.2)*.

As outlined above, five high level categories constitute the grounded framework depicting perceptions of citizens towards eID and interoperability. These consisted of: Systems and Technology, Public authority competence, Public authority integrity, Control over personal data, and, Citizen-State Power Balance.

In the sections that follow we present each category in turn, providing illustrations from the data analysed. Statements made by respondents are presented in full without editing to content or format. This is in line with the research aim of placing central stage the perception of citizens, giving them ample expression. Extensive use of data inserts in the presentation of the framework also accords with the grounded theory approach chosen for conducting this study.

The chapter closes with the findings related to expressions of how citizens might ultimately act in the light of their perceptions. These expressions were categorised under a theme entitled ***recalcitrant citizen*** (7.6).

7.1 Systems and Technology

> ***I look forward to the day on which the database will be hacked. And it will be hacked! (Germany)***
>
> ***If I could be assured that the technology matches the demands being placed upon it, I would be less concerned about using it. As it stands at present, there can be no such assurance…* (UK)**

System and technology is a theme that emerged from the analysis of both the UK and German data. Citizens perceptions categorised here are those referring directly to IT aspects related to IdMS. Four subcategories were identified under Systems and Technology. The first subcategory is comprised of general assessments of IT in IdMS, reflecting general concern over technological limitations. The two subcategories that follow focus instead on specific technologies namely: biometrics and RFID. Central database is the fourth and final subcategory located under the technology theme. As will be discussed later on, security issues related to central database architecture for IdMS came prominent in the perception of citizens.

7.1.1 General assessments of IT in IDMS

> *Electronic ID provides many benefits and are (probably) technically realizable but doubts remain about the integrity of the IT system…*(UK)
>
> *I am concerned about the reliability of the technology used (UK)*
>
> *I do not believe such a (safe) technology exists, nor that it can be proven to exist without many years of use in a less critical mission application*. (UK)
>
> *Computing data can be readout and decrypted afterwards by everybody. The question is how fast this works but not whether it works at all! (Germany)*
>
> *There are no secure computer systems. Due to the large number of people that have a right to access, the danger of abuse of data is too big to process them in the planed way. (Germany)*

it can be stressed enough that data never are secure! They rely on systems, that you have not developed yourself. .. what do you do, if in 5 years analysis you will find out, that there is a backdoor, by which the data is systematically tapped?(Germany)

… The security of the data on servers (no system is really safe when there is an attack by hackers!) (Germany)

7.1.2 Biometrics

Currently, the error rates for biometrics are too high to allow practical application in high-volume fast throughput application areas. (UK)

In my judgement the capturing and processing of biometric traits infringes dignity of man. E. g. fingerprints can be forged, see http://www.ccc.de/biometrie/fingerabdruck_kopieren?language=en. The systems for the processing and storage of biometric data generally should be deemed as insecure (computer bugs, security holes, lacking or weak encryption of the stored data etc.) (Germany)

I am generally against the storage of biometric data. Fingerprints can very well be faked. With other technologies this is only a question of time. …The EU is claiming too much power. (Germany)

7.1.3 RFID

The idea[of a EU eID] is good, but… - not if there is an RFID-Chip on it … This IS going to be abused, if not by the authorities themselves, then by criminals within these organisations. (Germany)

I do consider it problematic for one if data can be accessed without contact via RFID. (Several attacker cases are known that render a key to access data as well unnecessary), as well as the additional data that is stored on this ID-card. (Germany)

It has to be assumed that extremely unsecure and from a data protection point of view totally insufficient technologies – such as RFID that unfortunately is already used in German Passports - will be deployed for this identity card. That is one of the reasons why such an EU identity card has absolutely to be rejected. . (Germany)

Already the electronic passport hasn't been a good idea but an electronic identity card (for which the citizen probably will have to pay a high price again!!!) is absolutely wrong! If data collection shall become easier then one could rely on barcode and DataMatrix. – they offer possibilities that are similar comfortable but it is nearly impossible to read them out without being noticed. Ps: I work in the ID-area and hence I have sufficient knowledge about RFID to identify security holes and risks – something I deny 99% of the politicians!!! . (Germany)

I am worried about the privacy dangers of RFID in electronic ID cards, and about the lack of platform independency and open standards. (UK)

7.1.4 Central Database

the idea of a centralized ID databases is foolish in the extreme. It will be a honeypot for criminals, and lead to less security rather than more. Identity in the digital world is important, but centralized systems are not the way to provide. Federated, distributed systems are much safer, and work just as well. (UK)

Sorry, I just don't want all my data stored in the one place. (UK)

Such a system does not need to be centralized (as the British Government is currently suggesting to do). My main issue is with the "One Big Database" which will accumulate on every person in the UK, which is not being talked about - issues such as terrorism and benefits fraud are used to divert discussion away from this issue instead. (UK)

Concentrating a large amount of personal ID information in one space when chip copy or chip substitution cannot be prevented has to be regarded as a high security risk rather than a security gain. (UK)

A central storage of date has to be refrained from. This should be ruled by the constitution to put a limit to governmental control-systems. (Germany)

Why store the data in a central database? A standardized identity card is sufficient (Germany)

I am against the centralisation of data. Request to all competent authorities: Read the Book "Mastercode" by Scott McBrian". Central datapools are too dangerous, because nobody can really handle the medium personal computer and "security" is an universal key to surveillance and access to this data. . (Germany)

I have strong doubts. ... A centralised database with personal data frightens me a lot! (Germany)

A central storage of all data of the EU-citizens is too attractive for theft of data. (Germany)

I dislike an electronic data storage unit that communicates its data to everybody who tries to retrieve it. The problem is the electronic data storage unit and not the question whether only one country can read out the data or not. (Germany)

*Actually I object more to the existence of the central-but-universally-accessible database, *especially* as long as the EU is split into disparate jurisdictions, than to the existence of interoperable documents. (Germany)*

Although technology was seen to be more dependable than in the past there were fears about the robustness of identity management systems in particular. Biometrics and wireless technology, vulnerable open standards that interoperability often requires and mainly centralised database – all were mentioned as examples of reasons why citizens should fear the large-scale deployment of interoperable electronic IDs.

7.2 Public authority competence

> ***I'd love to believe that the ID authorities will be technically competent and ID fraud will become a thing of the past. But I just can't, and the potential problems here are very serious.* (UK)**
>
> ***Theoretically the electronic identity card is a smasher; unfortunately politicians tend to be technically insufficient at implementation causing significantly more harm than potential benefits to the citizens. (Germany)***

The theme of public authority competence emerged from the data analysis in both countries. It refers to citizens' perceptions regarding the ability of the state and its departments to secure and manage personal data. Three subcategories were identified under the competence theme. First are general perceptions regarding the competence, or rather, incompetence, of public administration. The remaining two subcategories are more closely related to technology use in public sector, one questions technical proficiency in public authority and the other focus on perceived success/failure of large-scale IT project implemented by public authority.

7.2.1 General competence of public authority

> *I believe the authorities will attempt to be honest and secure but ultimately will be unsuccessful in maintaining the confidentiality of my data.* (UK)
>
> *Electronic ID provides many benefits but…doubts remain over the competence of those who manage them. (UK)*
>
> *I feel the authorities will fail to deliver a secure, working system. It will be a monumental waste.* (UK)

7.2.2 IT proficiency in public authority

Citizens perceive the government to be lagging behind in IT adoption and expertise, in such a way that undermines the potential advantages of interoperable IdMS:

> *In general the simplification of administrative processes is positive. But… the thing is, the authorities by no means have the necessary IT-knowledge and the overview in this field, to make the appropriate decisions or to use the electronic systems properly. If you look at the systems/software/standards of education the authorities are currently using (old, proprietary systems etc), you will see, that they are not state of the art regarding these matters. (Germany)*

> *Often authorities are the last ones that take up technical improvements (encryption etc.) - for data security that is a true problem. (Germany)*

> *… In general I approve electronic identity cards, but I don't believe that authorities will wangle that in a secure way. (Germany)*

> *A unified European ID-card would be good….but the ability of governmental authorities to handle personal data is by no means provided in Germany. (Germany)*

> *The governmental staff lacks the necessary skills to appropriately handle the data. (Germany)*

> *Most UK senior civil servants and Ministers do not understand IT and believe it is "beneath them" to educate themselves.(UK)*

> *I don't take the people at the authorities for incapable but if you see how little they know about IT-security I don't believe that they will be able to protect my data sufficiently*. (UK)

7.2.3 Success and failure of past IT projects

In the UK, reference was made to past unsuccessful government IT projects and the outlook of many was pessimistic:

In these responses there is conveyed also the notion of the second order risk that the significant sums being expended would prove to be a waste of money for the taxpayer who is ultimately underwriting these projects; another related facet of the incompetence charge lies in the perceived inability of the government to manage large-scale IT projects properly:

> *…we also already have all the evidence we need to know that massive governmental IT projects are massive disasters, since every single one in the past twenty years has been* (UK)

> *My concern is the ability of Government organisations to effectively implement, maintain and operate this system based on many displays of total ineptitude in delivering large IT transformational change programmes in the past. The fact that I cannot think of a single example of a successful Government programme of this kind is deeply concerning…* (UK)

> *Unfortunately the authorities have show in the past their incompetence in realising or advertising for bids of IT-projects. See Elster [Note: German system for making electronic tax declarations] No authentication.(Germany)*

7. 3. Public authority integrity

The main problem is not the data that is stored on the ID-card, but the lack of trust in the authorities that handle the data. It maybe quite handy to have all data available electronically. The disadvantages outnumber the advantages however: the stored data will wet the appetite of the politicians, even if this was excluded in the process (e.g. Autobahn-toll in Germany). (Germany)

I deeply mistrust my government, other EC governments and private business to hold information about me. (UK)

Public authority integrity is a key theme that emerged from the data-driven analysis in both Germany and the UK. Trust is the key issue brought fourth in the perceptions of citizens associated with this theme. These perceptions were further sorted into two subcategories suggested by the grounded analysis: the first subcategory refers to general distrust in public authorities. It ranges from moderate expressions of mistrust to the view of governments as corrupt. The second subcategory addresses the interoperability issue of sharing personal information, that is consequent on trust in authorities. Concern from mission creep is expressed in general terms, in reference to multiple 'third parties' and in reference to specific third parties or uses, namely: commercial and law enforcement.

7.3.1 Distrust in public authority

…Unfortunately I have no faith anymore in public institutions... (Germany)

Trusting a bunch of civil servants to safeguard personal information, or to interpret it correctly is stupid beyond belief. (UK)

Possibly later on a law will be passed, that allows for the use of this data for other purposes. Since the data is already there, there is no chance of not disclosing it. (Germany)

In general that is a good idea to reduce bureaucracy and simplify paperwork with authorities. But… I do have strong doubts with respect to data protection, since I do not have sufficient trust in the authorities in charge. (Germany)

I believe that the current personnel of the authorities (employment office, social assistance office, etc.) isn't trustworthy enough to treat personal data in a confidential

manner. Shall it be an identity card in the form of a chip card that stores everything? I can't imagine anything about the whole project.

I personally do not believe that the authorities use my personal data thoughtfully, because I have had negative experiences. My personal data are very important for me and authorities have already too much insight in my private sphere. (Germany)

I think that the mania of the authorities to collect personal data has been raised to an intolerable level during the passed years due to political pressure. Regardless of the media used for the ID (paper or electronic) my trust in the authorities responsible for the collection and storage of personal data is decreasing due to my fears regarding a wrong understanding of safety by the politicians. (Germany)

You ask for my faith in the EU and its institutions? If I had faith in them, the responsible people were quite successful in purging every little bit of it. . (Germany)

I am concerned about the current government, as well as the prospect of others due to the way in which politics is heading. I have lost trust in this and other governments and am simply not happy about the introduction of ID cards in the UK. Any reassurances this government - and other politicians - gives upon this and other matters have stopped resonating with me. I do not believe any of it anymore. I am a dissatisfied 'citizen', yet at the same time highly educated and not prone to such things.(UK)

States cannot be trusted to restrict their use of citizenship data to what they promised in different circumstances .(UK)

ID cards are a good idea but…I do not trust the UK Government to securely treat my information.(UK)

Democratic governments cannot be trusted to keep promises because the electorate, rightly, demands changes. Identity is a service to the citizen which is dependent on trust so government cannot provide it. However, it can regulate those who provide that service, as they regulate professionals such as medicine and law.(UK)

Used a national ID card for ~20 years outside of EU and have absolutely no confidence in any government being able to hold my data securely (UK).

Governments cannot be trusted to maintain identity information on the citizen's behalf, and once such information is under the control of governments, its abuse will necessarily follow - either by government itself, or by criminals who infiltrate government systems.(UK)

We already have all the evidence we need to know that businesses and authorities will take absolutely no care of our personal data whatsoever; barely a day passes without another news item about massive ID thefts. (UK)

[the] government do not have the slightest regard to any promises or guarantees of secrecy or data security they may have made. (UK)

Perceiving public authorities as corrupt

I regard authorities as corrupt. (Germany)

*Corrupt, characterless politic * destroyed trust* no data revealing. (Germany)*

To make this absolutely clear: I AM ABSOLUTELY OPPOSED TO ANY KIND OF DATA RETENTION PLANED BY YOU OR THE EU! The reason being: I NOWADAYS ABSOLUTELY DISTRUST POLITICS AND ECONOMY. They have proven to be only interested in power and money too often. I consider present politicians generally corrupt. I consider our current economical system hostile towards humanity (Germany).

It is therefore no surprise that they are keenly supported by the EU, a corrupt, self-serving and thoroughly undemocratic organisation. (UK)

just another form of disgusting state control by treasonous, corrupt authoritarians. (UK)

I would not trust lower level officials to obey rules from the top - they don't now with eg driving licence data (even when not actively corrupt, which does happen) (UK)

7.3.2 Function Creep

7.3.2.1 General concern from function creep

Personally, my worry is that the data being available would lead to it being used; i.e. "everything looks like a nail when you have a hammer".(UK)

I am concerned about "mission creep" for such a database once it exists (UK)

The idea of a European ID is in general to be supported, but I see a big risk, that the personal data will not only be used according to the purpose binding. Such a huge

collection of personal data holds potential for misuse and lacks in the security mechanisms have fatal effects. (Germany)

As practical the central collection of data about individuals may be and as much authorities and institutions may try to protect my data, no protection is perfect and I don't believe that my data are used only by one authority but that they are passed on in case of doubt if it seems to be "useful" (one should think only of the incredible surveillance that the US practise in their "war against terror", I really doubt that it has been enforced by legitimate means. (Germany)

Data which were collected once will be used for any purpose (see toll collect). The privacy commissioner will not have any power. (Germany)

Does a unified European ID-Card necessarily have to be electronic (RFID)? To my knowledge these two goals do not have a compulsory interconnection. A central database makes me feel unwell: heterogeneous regulation on data protection; abuse, also by governments. Who grants that personal information provided for a certain purpose is not, simply by changing the law, abused for different uses (eg: German Autobahn toll)? (Germany)

7.3.2.2 multiple concerns from function creep

… Many governments have always abused systems when they wanted, if they were abusable, even if the approach was good and helpful. This can be observed for example with the Australian model for college fees. It may have taken twelve years and a change in government until the fees were raised more and more to fill the holes in the budget, but it happened in the end. Similar things are going to happen with surveillance and panic of the masses. As long as a politician is able to make the people believe that by dragnet observation and total surveillance the "axis of evil" can be fought against or the danger of terror can be reduced (even if all research points the opposite direction) a surveillance system will be abused. There is no win in security, because a) there are enough "Terrorists" in the European countries, that hold their passports legally and b) because those that don't can obtain a passport by illegal means. Conclusion: Electronic IDs can make things easier. But the risk of abuse by politics - not by the administration - is too high to compensate for the gains in simplification. (Germany)

My basic fear is that collected data will be used afterwards by politicians/authorities/enterprises etc. for other purposes than the originally declared ones. See the deployment of the toll system for – alleged – law enforcement purposes. Or – how it unfortunately but definitely will happen – concerning the telecommunications data retention of connection and communication data. The accumulation of data always raises greediness of - amongst others - interior

politicians and law enforcement authorities. Here I don't want to share my stance on nowadays interior security mania at all. Enterprises also try to make money out of the collected data anytime as long as there doesn't result any risk from that. (Germany)

I am afraid that personal biometric data are combined with different databases and will be used for other purposes than the one originally determined (fraud-resistance). These "other" uses are for example - criminal prosecution, marketing, health-insurance. . (Germany)

7.3.2.3 Passing personal information to private sector

NO connection of my ID-card-Data with any companies, non governmental structures!! The potential for abuse in this field is enormous, because private companies have different aims. (Germany)

…. Particularly if they (public authorities) are in financial straits they might sell the data. (Germany)

I have a severe lack of faith in the ability and willingness of the authorities to protect personal data from being passed on to businesses. (UK)

I am very concerned about the misuse of ID information especially considering links between government and industry. (UK)

…To hand data over to companies to me is a nightmare, because they are not subject to any control. Data that are collected, will also be abused, be it by states or by companies. (Germany)

7.3.2.4 Law enforcement, 'war against terror'

I don't have the confidence that authorities can resist the temptation to use all available info to solve their acute problems eg 'terrorism' or crime. (UK)

*.. I do have the necessary insight and experience, to be more than worried. Amongst other things the introduction of the so called "Anti-Terror-Security placebos", that have been lying around in the drawers of the lawmakers, the European governments have gambled away my trust * Purpose binding of the collected data are not worth anything, as soon as the data is collected they will be used sooner or later) * I am not afraid of terrorists, but a lot more of those who protect our constitution*

*("Verfassungsschützer" German term for secret service); attacks against the western-liberal basic order are accoutring meanwhile on a daily basis, but they are not executed by islamistic circles * Further keywords: data retention directive (and how it came along), obsession (literally: "horniness") for biometrics, electronic eavesdropping, TKÜV (a German legislation, regulating the access to telecommunication by the authorities) and surveillance interfaces, BND (secret service) – scandal, dragnet investigation, assignment of armed forces for internal security, highway-toll-data (Germany recently implemented a highway toll system, that uses sophisticated surveillance technologies, allowing for tracking), increase of video-surveillance, love for RFID, CIA-flights, facilitation of electronic voting and the refuse to give access to its mechanisms to the public etc. Last not least: Ministers for Internal affairs and ministers for justice, whose only problem with the measures mentioned above seems to be, that they now and then are rejected by the supreme court – or with data protection authorities, whose criticism they object by questioning their competence and their right to take a stand with regard to these issues. Now, why exactly should I still trust the authorities? (Germany)*

I am not in favour. Besides it is NEVER transparent, what authorities, but also companies actually do with the data. Solely the introduction of fingerprints on an eID does discomfort me. In a lot of cases you can wee, that *if a technology is once introduced, it will one day be used for criminal prosecution and the like by the authorities, even if that was excluded at the time of introduction. STRICTLY AGAINST IT!!!! .(Germany)*

*as long as there are data available there will be votes for using them for other purposes. See toll collect system in Germany or the US "war against terror" *lol*. Who relies on authorities and assigns technological expertise to them bears the blame himself…(*Germany)

EU-authorities have – inter alia with the transmission of flight passenger data to the US – already shown clearly that data protection doesn't play an important rule. Why should I now rely on the same institutions? .(Germany)

our Government will hand over our data to the CIA or any other organisation they care to without telling us. (UK)

7.4 Control over personal data

The only person who cares enough about my identity information to be allowed to control it is me (UK)

In the case of the ID at least the stored personal data have to be under the control of the owner. (Germany)

A major theme that emerged from the analysis captures citizens' perceptions concerning control over personal information. Few respondents addressed the issue of data integrity in this context, which made up one subcategory in the analysis. Another issue addressed by the second subcategory was that of transparency afforded to citizens. Finally, the most crucial issue represented in the third subcategory of the control theme concerns disclosure by consent.

7.4.1 Data integrity / accuracy of data

data sometimes become obsolete and in some cases I don't have the possibility to update them – because I don't know, where all over the world data about me are available. (Germany)

If there are wrong entries one is economically dead. This deeply intrudes into personal rights and is a good example how a good invention at the same time can lead to bad consequence, if mistakes are made. Therefore it is important to have the possibility to look at the data and to correct wrong data free of charge. (Germany)

As a citizen I have virtually no say in what the government does: or a quick and easy way to control it…I don't want them managing my own data. (UK)

will I be able to see or correct the information that will be held about me.(UK)

7.4.2 Transparency

The way of the EU as well as national authorities handled the passenger data after the attacks of 9/11 shows very clearly, why I will NOT want to see my personal data to be stored electronically, be it national or on EU-level. Without further objection the request of the USA to provide most intimate data of EU-citizens was met. Nobody knows what they do with this data and what they are used for. (Germany)

ALL data that are collected about me should be made available to me, so that I am able to recognize who has collected what data about me. (Germany)

TRANSPARENCY is important for acceptance: Which of my personal data are stored where and by whom respectively? (Germany)

7. 4.3 Disclosure by consent

I would support a de-centralized (e.g. on-chip) database, where accesses need my active authorization. (Germany)

I am in favour of a Europe-wide standardised electronic digital identity card. I require more transparency for the handling of my personal data. Data should only be passed on to third parties after a call back has taken place. (Germany)

In general I consider the idea of a unified EU-ID-card reasonable. It would be nice, when this occasion could be used to also introduce an E-card, that could be freely extensible, so I could one card for everything, eg. ID-card, drivers-license, EC/Creditcard, Paybackcard, Digital signature, electronic wallet. But it has to be made sure, that everybody can determine themselves, which information is transmitted, especially to enterprises. (Germany)

If my data finally are exchanged without my knowledge I am not able to reconstruct who possesses what data about me at all. The problem consists on the one hand of the fact that I possibly do not want, that A knows the data that I passed to B. (Germany)

… If you give me the full control of access and availability of the personal data I am happy, that means authorities are allowed to store personal data but I am the only one who can grant other authorities/firms/services access to them. If I have 100% control I would accept that emergency data (contact person, insurances or medical emergency data: blood group, allergies, organ donor data etc) will be stored on this ID card. A European standardisation would in this case be very helpful across Europe in emergency situations. (Germany)

.. it has to be ensured that the owner of the ID will be asked than ever the data will be fetched. (Germany)

it is important that the citizens are given full control on what happens with his or her data, since they are now being collected nearly everywhere. It goes without questions that they are necessary for today's administrative and business processes. (Germany)

In general I think the idea of unique EU-wide IDs is desirably. I am worrying about the electronic readability. Especially if I have no control about which data will be stored on the ID. (Germany)

I would like to know, whether there are plans to store the personal data on a citizen within his sphere. This could, for example be done by using a wirelessly readable ID-Card, that only can be accessed in close range of the reader. Any access would therefore need consent of the citizen, thus every citizen would still control his personal data. (Germany)

The transfer of personal data may only be carried out with full and unambiguous consent, and not by the usual means of opt-out. (Germany)

*If asked whether I might give my consent for *specified* personal data to be shared with x *for a particular purpose*, my answer would be "yes". (UK)*

Requiring informed consent is an essential step in minimizing perceived risks to privacy and identity.(UK)

The key point is that individuals need to be in control of use of their personal data - it must only be with their informed consent. So if asked whether I am happy for my data to be shared with x, my answer is "no".(UK).

Data sharing between countries should be an "opt in" scheme, not "opt out", and people should be informed fully of the implications of either choice".(UK).

Another issue is that of Governments gradually expanding the scope of their powers to share personal data "in the public interest", but without seeking informed consent. ".(UK).

7. 5 Citizen-state power balance

***While I have no great problems with the idea of a proof of identity (e.g. Passport), the ID schemes proposed will shift the balance of control of identity from the Citizen to the State* (UK)**

The storage of [personal] data is an instrument for power of the Community (EC) against its citizens, which lacks an equivalent antelope, thus ignoring the principles of a constitutional state. …(Germany).

The theme of citizen-state power balance represents citizens' perceptions concerning changes to power relations that interoperable IdMS might bring about. Expressions of fear from a detrimental shift in citizen-state power balance varied in the use of metaphors and of tone. To captures these variations, comments were classified into a set of data-driven subcategories: Surveillance society of glassy citizens; Criminalisation of civil society, Imperil civil liberties; Totalitarian regime

7. 5.1 Surveillance Society of Glassy Citizens

I don't want the "glassy citizen"!!! Nobody needs total surveillance. (Germany).

Whether one would like to have this identity card or not, I don't want to have it, but I am – as I was concerning the passport – forced to reveal personal data (such as the fingerprint). Therewith borders will not be more secure, terrorism will not be defeated, but instead the citizen – i. e. me – will become more and more glassy. But then I could go naked on the street as well. (Germany).

I don't support a glassy citizen. Through the implementation of an electronic identity card and the exchange of data between enterprises and authorities as well as between authorities and authorities privacy vanishes completely. A surveillance Europe isn't desirable. (Germany).

What is the whole drama good for? I don't believe that an electronic identity card contributes to more security; rather it will animate even more enterprises etc. to collect data ("Zeit" published an interesting dossier dealing with this topic at the end of 2004 – "The glassy human"). In this context it is tried via telling scare stories to collect more data than necessary about every single person and – without us being able to comprehend it – to transfer more data than necessary. So – how does the single citizen benefit from that? (Germany).

The whole thing is only good for creating a totally transparent citizen, that is controllable everywhere and by everybody. Politics is only working for industry. In the future the law will be increasingly interpreted in favour of industry. The data will not be secure. Money rules the world. Therefore the collected data will someday by somebody be sold. Include more countries like turkey or Romania in the EU. Total chaos is near. Poverty of the people is near, except for politicians and industry. Reduction of EU-politics by at least 50% as well as the number of EU-politicians! (Germany).

Electronic identity cards do not offer any benefits except of the one that they create nearly unlimited opportunities for surveillance and governmental control. Even if law at first limits these opportunities so far it always has shown finally that abuse is practised if there are possibilities of abuse. That hasn't necessarily to be done with ill intent but due to fear, foolishness or just because you can do it. Therefore this is already the first step into this direction and it is the most dangerous of all (Germany).

I have the substantive impression, that all the methods with electronic ID-cards (no matter what kind they may be, they could also be eg. Credit cards), are targeted specifically to record and analyze individuals and all their actions. It is in a way fascinating to see that only a very little amount of proposals is even considering to verify the right to conduct such an action, none anyhow do go as far as looking at the person doing so, neither do the systems delete (or better to not even collect it) the respective data after it is needed or to reduce it in a way, that a mapping ist not possible anymore (Germany).

I am opposed to total surveillance and control. We are already controlled by media and economy. Where is this going to lead us, if all data is exchanged globally? Huge databases with statistics and analyses can produced to steer the behavior of the "blind". (a citizen that is concerned about the future.) (Germany).

reminds me of the movie „Public Enemy No. 1"… Total control over everybody and everything. If a mistake happens I just will disappear globally… Cool (Germany).

It's not about easy access for citizens to authorities. Because we already have an easy access: open door, show ID and that's it. The reason for ID cards is to establish surveillance measures and - as you elaborate in the beginning - a central data base with the personal data of all EU-citizens. And this is communicated to me as advantage for the citizens. How stupid do you think we are? (Germany).

7. 5.2 Criminalisation of civil society

A EU-ID-card would result in legal and illegal abuse as you can see with the new EU-Data retention. Without reason all citizens are criminalised. (Germany).

I'm concerned about the increasing data collection activities of the state and the EU respectively. The collection of single data may not be bad yet but if you combine data from several data bases this leads to pictures that could be misinterpreted easily: Islam researchers are denied entry because they ordered the "wrong" books at Amazon. Students get into the focus of dragnet investigations totally groundless. Respectable citizens are filmed in cities at every turn. Politicians claim that you can prevent assaults with that but this isn't true, as is proved by London… This list could be continued therefore I beg you: Stop the data collection excesses! (Germany).

Not the data like name and date of birth are problematic, but the problem ist that more and more data are being collected. We aren't criminals but citizens!! (Germany).

Personal data will not be passed on Fingerprint=Criminal Citizen=Criminal??? (Germany).

I don't believe that while introducing electronic identity cards the desires / needs of the population are taken into consideration. The only purpose is to obtain an EU-wide database in order to be able to – under the pretence of counter-terrorism - easier access personal data of the population - dragnet investigation etc. (Germany).*

It is as if all citizens are considered to be potential criminals. (UK)

A lot of people think if you're not a criminal then there's nothing to fear from identity cards, I however disagree. The idea of having a citizen number and everything being known about me from that is repugnant. (UK)

7. 5.3 Imperil freedom and civil liberties

The states and the EU seem to consider their citizens as "enemies", that have to be surveilled, controlled, harassed and restricted in their rights (Germany).

The current behaviour of the government, to revoke citizen's rights and to establish a European Police State is very problematic. I also will not accept fingerprints or

genetic data in my ID-card, because I passively leave these date behind thus I will be traceable. Other than that I generally support the idea of an electronic passport, because I am very enthusiastic about technology and I do see chances and advantages. (Germany).

I am very doubtful about any surveillance… The freedom of mankind is the most precious asset and has its foundation in the constitution. RESIST THE BEGINNINGS! (Germany).

Electronic Ids of any kind are absolutely unnecessary. They only support the protection of paranoid regimes against their citizens. They are not compatible with fundamental [civil] rights. (Germany).

It's all about establishing control! The one who fall of the system or who offers resistance against the system - even in a peaceful manner - can be pressured by legal means thanks to your ID-cards. ***This has nothing to do with freedom - but with protection of the government against the citizens.*** *Yes I know! Times become even worse! Therefore the ordinary politicians have to protect themselves against the ordinary citizens! At least if the citizens realise that the lobby groups of the firms govern the politicians and not the citizens themselves as it should be in a democracy. And pleas don't tell me, that I am a „paranoid geek", because I am unfortunately neither paranoid nor a geek. I am just a citizen of age, observing the world, who realised how important democracy is for peace and how week our democracy is. How innocent do you think the citizens are? We are patient - because we believe in the goodness of the people - even in case of company bosses or politicians. But we are not stupid and we do not let us be messed around. (Germany).*

A discussion what outcome is expected from search measures because they enable the state to totally control individuals but they don't bring any benefits – even not security technology benefits- for the individual at all. – Questions concerning the voluntariness of the planned measures (example Switzerland). –The potential for abuse in case of further restriction of civil base rights as currently can be experienced in Great Britain and Germany - …(Germany).

I am against each kind of ID and would like if the IDs would be immediately disestablished. IDs are a symbol of anti-freedom. (Germany).

Please don't flush privacy and freedom down the corporate and military toilets. Please don't (UK)

The EU has to finally act in favor of the people and to support citizen's rights, instead in the name of a alleged fight against terror and in favor of the industry they weaken or give up the rights of every individual with pseudo-arguments. This especially goes for the dissemination of data to countries outside of the EU. . (Germany).

Only a free Europe of citizens' rights will win the trust of the people in the long term. (Germany).

While I'm very much your average person and therefore not someone one would expect the authorities to be interested in, I feel very sensitive the increasing encroachment of the state(s) - the reduction of liberty, freedom of speech on the basis increased terrorism. The ID card is one additional nail in the coffin - if I chose to go on a protest march would this be put on one's card (or could someone in "authority" examining your ID card use it to interrogate some database) and therefore be stigmatised as a "troublemaker" - what recourse would I have to see if such things were flagged. Would one be able to apply to one authority who could then tell you each and every time your ID card had been used or information contained about you in the associated database been interrogated and by whom. But that in itself is one person having too much information about you.- (UK)

ID cards and the NIR in the UK and elsewhere are an infringement of our civil liberty and lessen our freedom. It makes the State and big business more powerful over the citizen to the detriment of the citizen. We are in danger of becoming subservient to the State and will be tracked, monitored and controlled for all our lives with very little personal freedom or privacy (UK)

ID cards are an infringement of civil liberties and lessen the freedom of law-abiding citizens. (UK)

I believe that the very concept of an ID card is alien to a common law democracy like the UK. (UK)

Any approach or means to safeguard our security and democratic way of life is highly questionable if by its nature it asks of us to forfeit the very things it alleges to protect, i.e. personal freedom and civil liberties. (UK)

…I strongly believe that the right to privacy is slowly being eroded to a point where privacy is no longer achievable. An electronic ID which combines personal data with biometric data will further this erosion. A European ID card bears the risk of it becoming a requirement for purposes where its use is in no way mandated. (UK)

Whatever the advantages of ID cards (pan-European health information being primary) they have to be rejected on libertarian grounds. (UK)

Maintaining data on citizens without consent is a violation of rights to privacy and could potentially be abused by the states, if this is in the name of 'security' it is even

more tragic as Europe has always been threatened by political violence and saw no need for such draconian measures. The governments have enough checks on us, and enough intelligence at their disposal. (UK)

It would more than pleasantly surprise me if this once the result were rather in accordance with human rights, especially privacy - than, as so often before, based on economic profit, structural simplicity (for the government) or political haggling between EU countries: things that so often have shaped the "people's union" before. After all, there always remains one question, even after the data is in whatever way safely in the hands of governmental institutions with no external intrusions or modifications possible: Quis custodiet ipsos custodes? And this EU-citizen's trust in "our guardians" has become, after dozens of decisions against citizens' interest, a steady decline in the upholding of human rights, and after governmental institutions more and more prone to severe overreactions against their own (nominal) sovereign, influenced by lobbying and fear of allegedly ubiquitous terrorists, very small indeed...(UK)

7.5.4 Totalitarian regime

7.5.4.1 Nazism/Fascism/Dictatorship

What's all this good for? The fascistic EU-dictatorship somehow or other implements the permanent total surveillance of all citizens whether we approve it or not. And the collected data are also passed on to big enterprises - finally the biggest concentration camp of all time, the EU, belongs to them. (Germany).

Such systems/approaches have been implemented in Germany between 1933 and 1945 with deadly outcome for some parts of the citizens (Germany).

The abuse done by corporations is less problematic than the one by governments. For example have you ever imagined, what happens, if tomorrow another "Hitler" is rising? And if he then has access to all these data? No? Then think again, and do not simply ignore this scenario (Germany).

Both ends are ideologies of killers and people who would support and ID programme (communists and Nazis). For the record, I consider myself a Classical (Free-Market) Liberal. (UK)

ID cards are for Nazi Germany and Soviet Russia and other Police States and Dictatorships. They are completely incompatible with a free, democratic society. (UK)

The idea of a general ID Card for all citizens is very wrong and a manipulative way of certain people in power seizing the rights of its citizens. It is a modern form of dictatorship and basically not a fair system. (UK)

The UK ID card proposals and the associated register (which is really the problem, very cleverly disguised) represent a further descent towards totalitarianism and are nothing more than an instrument of population control and surveillance. They must and will be stopped.(UK)

the people running a UK ID card system would continue to be selected from the present two authoritarian principal authoritarian political parties (UK)

I oppose all governmental initiatives to intervene in matters of personal privacy. The role of government is the provision of essential public services and social safety nets; it must not micro manage the lives of citizens. I strongly oppose the tendency of governments to authoritarianism and over regulation.(UK)

these big databases could be used to control citizens if a dictatorship was in power(UK)

Citizens that are not trusted by the state have no freedom. Therefore an ID society is the first step towards dictatorship. (UK)

ID cards are the biggest threat to personal liberty that Europeans are facing since 1930-40s fascism. It is the first step towards a European police state, worse than anything ever seen in the East during the Cold War.(UK)

7.5.4.2 Big brotherism

Big brother is watching you is approaching and nobody wants to recognize that. The purpose of collecting data is – in any case – to control people – the only question is who uses these data for what purpose. By means of data one easily can „create" fringe groups and discriminate, persecute or try to exterminate them but also grant certain privileges to them. That doesn't only happen in left or right dictatorships but also in democratic republics. Potentates always use all available – legal and illegal – instruments in order to discriminate other people. According to the particular form of government this is more or less difficult but it is always possible. For me there always comes up the question what authorities want to do with all the data and for what purpose other countries and enterprises shall obtain my data. A brief example – you have a vehicle insurance and are asked whether you park your car on a rented

parking place or on the street. Actuarial that doesn't matter because the insurance rate remains the same. For what purpose are those data collected from ALL drivers then? That sure enough is – so far – an unimportant question, but these data also could be used for other purposes e. g. how many people can afford a parking place, how many public parking places are lacking in the particular community and where are they lacking. So far that would make sense although already this would be an abuse of data, because nobody gave his consent for using the data for that purpose. But now the community is able to deploy its employees more efficiently in areas lacking of public parking places to issue parking tickets to vehicles that are parked illegally. A profitable source of income for the state that requires only little effort but that is definitely illegal. But nobody asks for that, and if one does anyhow it is looked for a scapegoat. Of course the scapegoat could be found in another data group e. g. a black German-Russian who is gay. How to find him? Of course with your data base, BIG BROTHER. Not only Adolf Hitler and the GDR took advantage of databases. (Germany).

Why must an EU-citizen register his residence, why does he need the authorisation of authorities for every bagatelle, and why shall he now be forced to possess an electronic identity card, whereas the US obviously manage without all of that and even – without the whole inflated red tape – benefit from fewer people being unemployed, more economic dynamic, and more individual commitment. The dimension and the pace, with that the EU – according to the sample of Orwell's "1984" – develops to an authoritarian, fascistic police state that controls all spheres of human life completely is to an extremely high degree alarming. Just the fact that EU-policy maker – i. e. council and commission – are not even a bit democratically legitimated (because multiple indirect allocation of positions hardly has something to do with democracy) speaks volumes. The EU primarily should pay attention to defending civil liberties against the permanently increasing authoritarian and anti-democratic greediness of its member states. But the idea of a "union for the citizens" today is more away than ever. Instead of that the EU has degenerated to a precursor concerning the installation of an unprecedented police state-alike control- and surveillance-instrument. People have already recognized that and have clearly opposed to the EU-constitution even though the enemies of democracy in the council and the commission strongly believed in the ratification of the constitution. This EU-constitution would be the next step towards an Orwell-like totalitarianism. The political leadership of the EU obviously is unable to learn from history and hasn't recognised yet that the human pursuit of freedom and self determination – that nowadays comprises also and to a high degree the informational self determination – can be suppressed only for a certain period of time. "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." – Benjamin Franklin (1706 – 1790) (Germany).

Welcome to 1984 ...:-((Germany).

Stop 1984... (Germany).

1984 (UK)

The current discussion about the electronic identity card, the electronic health card and the exchange of passenger data (even if that has been cancelled by the European Court of Justice) reminds me too much of the introduction of a Big Brother state. Other so-called Anti-Terror laws – like the case of the bank secret – widely overshoot the mark, too. That is something I can do without easily. (Germany)

As my responses indicate, I am not positive about this scheme for EU-wide identity cards. I think that it will just promote Big Brotherism while doing very little to nab genuine terrorists, crooks, etc., the smartest of whom will always be able to outwit such a system. (UK)

Hopefully the EU will stop playing Big Brother, especially council and commission, and start to listen to voters more than to lobbyists. The general collection of telco data of 450 million innocents is the worst thing of legislation I have heard of in a long time, but electronic IDs is not much better. (UK)

will vote for whatever political party will oppose such Orwellian measures. (UK)

7.6 Recalcitrant citizens

What emerges beyond just the perceptions of the risks associated with the deployment of IdMS is the expression of citizens' commitment to follow up with actions. The language smacks of resorting to civil disobedience in order to resist government eID schemes.

> *I will trick them [governments] and tell them lies, whenever this is unavoidable. They do not leave a different way of handling this. Fight the EU. Freedom for humanity. No power to economy.(Germany)*

> *I will refuse with all means to give more than my contact data (name, birth day/place, address) to be stored on electronic IDs! (Germany)*

> *I will refuse to release any biometric data. I will not have a passport with biometric data issued. (Germany)*

> *I will never carry an ID card – the state is my servant, not my master, and I do not need a license to exist.(UK)*

> *the data transferred by airlines to the USA has altered my plans travel to North America because of the invasive nature of the information given to them. I will therefore never be prepared to register for an ID card, whatever the penalty*. (UK)

The use of powerful verbs such as "fight" and "resist" gave the impression that citizens would be prepared go to some lengths in their opposition:

> *I will resist it at every turn* (UK)

> *I will **fight** vigorously to oppose their introduction here*. (UK)

> *I will fight to preserve my liberty against this disgraceful fascist onslaught* (UK)

> *People I talk to are going to sabotage or resist this nonsense*. (UK)

Even more extreme were these responses. Of course such expressions of sentiment are relatively easy to pronounce but what action ensues remains to be seen.

If necessary I will emigrate! (Germany).

I would sooner renounce my citizenship than submit to the British government's evil scheme (UK)

I will never, never, NEVER have my fingerprints, retina scans or DNA profile taken from me and put on a Government Database. I would rather die than have that happen.. (UK)

I will therefore never be prepared to register for an ID card, whatever the penalty. (UK)

If put into use, I would be inclined to move to another continent. (UK)

I will fight vigorously to oppose their introduction here. (UK)

"Are you prepared to go to jail, rather than be forced to carry an ID card?". My answer would be Yes. (UK)

I would rather go to prison than participate in the UK ID card scheme even though I am a Labour Party supporter in general, pay my taxes, and have never been in trouble for the law for so much as a parking fine. (UK)

I would rather go to prison than give my personal details to an ID database register. (UK)

People I talk to are going to sabotage or resist this nonsense. Don't forget we stopped Hitler and he was once king of the hill. Remember Towton Moor. (UK)

I'm in the UK and very much against the introduction of ID cards and the NIR and plan on doing my best to avoid getting on the NIR. (UK)

My identity should be something I control and own. The current moves by governments to manage ID amount to attempted theft of my identity. I will fight strongly to protect this. (UK)

8 Discussion

The data that has been collected and the findings presented provide the basis for a number of different themes all worthy of discussion and development. Following the logic of the findings template of analysis these would include minimally – technology and systems, authority competence, authority integrity, control over personal data and finally citizen-state power balance. Indeed, it is worth pointing out the intrinsic coherence of this progression, which commences with the technological artefacts themselves and comes to rest with the high-level concepts of political power and resistance, while the thread of logic that connects them all is evident for all to see. We felt it advisable however to focus on the upper levels of abstraction and in particular the last three constructs of integrity, control over personal data, and citizen-state power balance.

The question of public authorities integrity lies at the heart of a trust relationship between the digital citizen and the digital state and its operatives. By integrity, we imply the expectation that that the party entrusted with citizen data will discharge their custodianship without resorting to unethical behaviour, such as sharing it with third parties unforeseen at the outset of the relationship. In large public administrative systems power and responsibility have to be delegated - by the state, by the citizenry, for the purposes of facilitating the provision of services and the performing of state functions. However it is highly detrimental to the reputation of the state and to its status in the eyes of its citizens if public servants are regarded as corrupt and willing to make available information to unauthorised third parties. The perception of untrustworthiness of the personnel in the public authorities came from both UK and German respondents: *I have lost trust in this and other governments (UK)* and *Unfortunately I have no faith anymore in public institutions (Germany)*. The parallelism in the two countries' responses is almost uncanny, especially considering that the particular context of the UK ID card debate could not apply in Germany during data collection.

The record of failures was even more embarrassing after this data collection than the period subsequent to it. Indeed so bad was the situation that the UK Government introduced a White Paper[11] setting out the management standard for the safe handling of citizen data. This standard is now rapidly becoming a de facto data-handling standard in the private sector of the UK as well.

The issue of function creep is a vexing one. The existence of data collected for one purpose but later desirable for another purpose – that may well be beneficial to the digital citizen – creates a dilemma. Limiting the use of data to the original purpose may seem an excellent principle, so that extension of purpose would require further consent from the citizen, but in practice the fast-moving world of public service provision may make that further consent difficult to obtain in the short run. If there were a fund of pre-existing trust upon which the digital state could draw, then it might be a different proposition. The problem is that this fund of trust is missing. German respondents mentioned the fear of German autobahn toll data

[11] http://whitepapers.silicon.com/0,39024759,60559201p,00.htm

being made available for law enforcement purposes and the case of the London Transport oyster card data being also used in this way is well known. Fears were voiced in respect of personal biometric data being used for criminal prosecution, marketing and health insurance. The quotation from a UK respondent: *States cannot be trusted to restrict their use of citizenship data to what they promised in different circumstances* is paralleled almost exactly by the German respondent: *Possibly later on a law will be passed, that allows for the use of this data for other purposes*. Whether this state of affairs is due to the unreliable character of administrators more generally, or perhaps instead a function of the demands of government in an information society is a question that citizens must reflect on.

Notions of privacy that sprang from an earlier, less frenetic, paper-based reality, may not be compatible with the digital state. Expectations of high quality delivery of electronic services may conflict with personal privacy expectations that date from a past that is fast disappearing from memory. Is the function creep indeed something that is intrinsic to a fast-changing world? If so then perhaps a compromise needs to be discovered between all or nothing.

Also, the issue is related to citizen records' accuracy. Administering the digital state raises the issue of how to maintain accuracy of personal information when circumstances are changing fast. Change of address, occupation, marital status, health status and so forth are all inevitably features of modern life and all require recording somewhere in the public authorities' records. The issue is who will do this? Wholesale and constant data input to maintain the appropriate level of accuracy needed to run the digital state with efficiency and justice will certainly require the involvement of the digital citizen, at least in respect of data input to governmental and agency databases at the many points of entry that are springing up. Hence some control by the citizen over personal information may be necessary and with it must come the transparency that allows the citizen to see what is currently recorded, and perhaps with which other agencies their data are being shared.

While there might seem to be merit in constantly requesting the citizen to approve of new purposes being adopted for their personal data, some might be inconvenienced by being repeatedly asked for their approval. Governments and citizens will probably want discretion to be exercised in order to minimise nuisance caused by continuous requests for consent. The problem once more rests on the low level of trust that many citizens repose in their governments with regard to their use of personal information. On the basis of these findings, the winning back of citizen trust in public authorities' handling of such assets must be a major objective of European governments.

With profiling such a major feature in the use of large-scale databases, the danger is that citizens on the basis of medical emergency, insurance or other data, might be unknowingly sorted into a category that is treated differently from others, perhaps not offered benefits or services for which they might be in reality eligible, or alternatively, unwittingly chosen for checks and vetting on the basis of spurious similarities between their behaviour and that of criminals and malefactors. The 1986 constitutional ruling in Germany regarding "informational self-determination" underpins the robust responses from German respondents on this issue.

As the value grows of stored citizens' personal information, in a context of more and more information-driven activities for both public and private sector, the power in the hands of the custodians increases concomitantly. Research into the phenomenon (Clegg, 1989) suggests that power is only evidenced when there is resistance, or else there is no need to deploy power. Increasingly European citizens are facing a choice of either accepting the growing agenda for state control of citizen data, with data sharing and interoperability a key driver behind many of the latest systems in eHealth, eGovernment and law enforcement, or of resisting this development. Currently the resistance is coming from privacy lobby groups such as Privacy International and other civil liberties groups. There is as yet no widespread revolt against these developments despite widespread dissent. The views expressed in this study indicate that there exist numbers of citizens who are extremely wary of what is happening and who feel strongly about the incursions into their privacy that attend the introduction of electronic IDs and similar mechanisms. Similar views were expressed by both United Kingdom and German respondents. That is, no substantive differences were observed between the two countries in terms of their citizens' perceptions as similar themes emerged in both UK and Germany.

One vexing issue is the number of times that the owner of the data might be consulted for their consent with regard to sharing it with other users and purposes. The systems perspective might lean on the side of trying to reduce the number of consent requests, stressing that outline policy permission could be granted with only "exceptional" matters needing consultation. The critical policy decision however is how to define what is exceptional in terms of change of purpose. Administrators would fear that requests for consent would be missed, deliberately ignored, or refused and there is a big question of how to deal with the digital divide, with those citizens who are not connected to the web and may never be so in the foreseeable future. A choice may have to be made as to whether the discretion for the citizen is about opting in or opting out. Opting in meaning that the default position is that the citizen's consent is not assumed to exist unless actively expressed. Opting out meaning that the default position is that the citizen is assumed to consent unless actively stating otherwise. The experience in private enterprise, and this is the driving force for "citizen-centric" information systems suggests more administrative actions and decisions will be formed on the basis of profiling citizens' personal data and transactions, hence the decision to share information will have more impact.

The state will always reserve to itself powers to allow it to exercise special rights in extreme circumstances, for example, national defence, terrorism and arguably organised crime. Most citizens expect that identity information will be made available to the authorities in such contexts. But should this state of affairs be the norm? What powers do citizens have to balance the exceptional power of the state? Should there be further empowerment of Information or Identity Commissioners in order to defend the ordinary citizen's interest. The deployment of Privacy Enhancing Technologies (PETs) would offer a route to inscribe citizens' rights into identity management technology, but the widespread take-up of PETs is still some way into the future.

Technology concerned with the management of personal identities constitutes the first step in a thread of logic, of entailed circumstances, that binds personal information risk to the developing digital state. Deploying that technology to drive the digital state means putting vital clues to personal identity into the hands of state agencies and their employees. Information systems are always social systems. Given that information systems risks include malfunction caused by employee error or incompetence and loss of confidentiality, both integrity and competence become further steps in the logic of securing personal information. Incompetence and wilful loss of integrity both jeopardise citizens' privacy, security and well-being. Finally even with the proper functioning of the technology, observance of integrity and correct application of procedure and policy, there still remains the issue of what should be the powers of the state and those of its citizens. Perhaps the time is approaching when a clearer and more equitable demarcation of powers in this area needs to be established – a digital bill of rights perhaps?

9 Conclusion

This study has collected a large number of opinions from both UK and German respondents on the question of electronic identities and their interoperability. It has shown that there are clear issues strongly felt in both countries – the comparison of the two countries points to strong similarity, rather than difference, in the perception of citizens. The analysis determined five key areas of concern: technology, competence, integrity, control and power. Overall the message comes that governments need to win back the trust of the citizens if the digital state is to develop in a harmonious fashion. One important way to establish that trust is for the state to demonstrate proper concern for the personal data in its custody. In the UK there are signs, such as the Data Handling Procedures developments for example, that at last the proper management of data security is beginning to be seen as a priority. However more needs to be done to clarify the policy issues around what constitutes a change of purpose and under what conditions a new purpose requires new consent from the citizen. There may indeed be a case for a far reaching review of how the state handles citizen data, where the lines should be drawn in terms of powers, and what redress the citizen has when these lines are transgressed. The evidence here is that the sharing and management of identity information is a strongly felt issue that will not be readily forgotten or set aside.

10Publications related with this deliverable

Backhouse, J., & Halperin, R. (2008). *Security and Privacy Perception of eID: A Grounded Research* Paper presented at the European Conference on Information Systems (ECIS), Galway, Ireland.

Backhouse, J. (2008). Risk perception and identity management in the digital state. Paper presented at The Vigilant Society Symposium, Lisbon, Portugal

Backhouse, J., & Halperin, R. (2009). Approaching Interoperability for Identity Management Systems. In K. Rannenberg, D. Royer, A. Deuker (Eds.), *Identity in the Information Society: Challenges and Opportunities* (pp. 245-268) Berlin Heidelberg: Springer

Halperin R., & Backhouse J., (2009). Interoperable eIDs: Game Over for Digital Citizens? Paper presented at the Identity in the Information Society Workshop (IDIS09), London, UK

Halperin R., & Backhouse J., (Forthcoming 2010). Citizen Centric or Government Centric? Perceptions of Risk in New Identity Management Systems. In: C. Reddick (Ed.) *Politics, Democracy and E-Government: Participation and Service Delivery*. Hershey, PA: IGI Global

11 References

Agar, M. H. (1980). *The Professional Stranger: An informal introduction to ethnography*. New York, NY: Academic Press.

Backhouse, J., & Halperin, R. (Eds.). (2007). *EU Citizen's trust in future ID systems and authorities*: FIDIS Deliverable 4.4/4.5 Available at fidis.net.

Backhouse, J., & Halperin, R. (2009). Approaching Interoperability for Identity Management Systems. In K. Rannenberg (Ed.), *Identity in the Information Society: Challenges and Opportunities* (pp. 245-268) Berlin Heidelberg: Springer.

Bauer , M. (Ed.). (1997). *Resistance to New Technology: nuclear power, information technology and biotechnology*. Cambridge: Cambridge University Press.

Clegg, S. R. (1989). *Frameworks of Power*. London: Sage.

Glaser, B. G., & Strauss, A. L. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research*. New York, NY: Aldine.

Lee, A. S., & Baskerville, R. L. (2003). Generalizing Generalizibility in Information Systems Research. *Information Systems Research, 14*(3), 221-243.

Lips, A. M. B. (2007). E-Government Under Construction: Challenging Traditional Conceptions of Citizenship. In P. Nixon & V. Koutrakou (Eds.), *E-Government in Europe Rebooting the State* (pp. 33-47). London: Routledge.

Lusoli, W., & Miltgen, C. (2009). Young People and Emerging Digital Services. An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks (JRC Scientific and Technical Reports EUR 23765 EN).

Martin, P. Y., & Turner, B. A. (1986). Grounded Theory and Organizational Research. *The Journal of Applied Behavioral Science, 22*(2), 141-157.

Nixon, P. & Koutrakou, V. (2007) (Eds.), *E-Government in Europe Rebooting the* London: Routledge.

Orlikowski, W. (1993). CASE tools are organizational change: Investigating Incremental and Radical Changes in Systems Development. *MIS Quarterly, 17*(3), 309-340.

Strauss, A., & Corbin, J. (1990). *Basics of Qualitative Research: Grounded Theory, Procedures, and Techniques*. Newbury Park, CA Sage.

Yin, R. K. (1984). *Case Study Research: Design and Methods*. Thousand Oaks, CA: Sage.