National Electronic Identity Management: The Challenge of a citizen-centric Approach beyond Technical Design

Stefan Strauß
Institute of Technology Assessment (ITA)
Austrian Academy of Sciences
Vienna, Austria
sstrauss@oeaw.ac.at

Georg Aichholzer
Institute of Technology Assessment (ITA)
Austrian Academy of Sciences
Vienna, Austria
aich@oeaw.ac.at

Abstract— **National governments across Europe are currently introducing electronic identity management systems for enhancing security and gathering more unified forms of authentication for online public services. A particular challenge of security system design is to cope with the suspense between security and usability. This is strongly reflecting in identity management where this suspense becomes very apparent. Thus, for the success of identity management systems a certain focus on user centricity is demanded. This paper analyzes the system in Austria with respect to important determinants of a citizen-centric identity management approach, deduced from security usability issues, interrelated with factors for user perception as provided by the Technology Acceptance Model. The result reveals a biased picture of user centricity with an essential need for a stronger consideration of user perception and the provision of additional benefits addressing a perceivable user value.**

Keywords - electronic identity management; user centricity; security usability; e-government; Austria; TAM

I. INTRODUCTION

With the achievement of higher stages of interaction in online services and the increasing number of electronic transactions in different domains of everyday life, identity management (IDM) more and more becomes a crucial challenge in the information society as most transactions require user authentication. This is especially the case in the field of e-government, where IDM plays a particular role. The maturity of online public services allows users not just to obtain information but also to conduct transactions with public administration completely online via single sign-on (SSO). Currently, there is a rather broad scope of different concepts and technologies for authentication procedures in online services, which makes IDM a tricky task to cope with, especially for end-users. Therefore a number of countries in Europe are introducing systems for electronic identity management (e-IDMS) in order to improve security in online services and to set-up more harmonized forms of identification and the corresponding procedures. As these approaches at least aim to unify national IDM for e-government, they have a special focus on their citizens as the primary user group. Hence, user centricity is an essential factor and a certain challenge in this context.

A part of this work has been presented at the CENTRIC 2009 conference and this paper is an extended version of our contribution [1]. It upgrades the findings in [1] by emphasizing on issues regarding security usability and ties them in with user perception as a key determinant for user centricity.

Higher levels of security, efficiency and cost-effectiveness of electronic communication and transactions are the major benefits that governments expect from a national e-IDMS, for the public administration itself as well as for citizens and businesses. Lips et al. postulate that e-IDM becomes "the sine qua non of successful e-government", and highlight two perspectives that have been dominating up to now: "technical design" and "privacy advocacy" [2]. They argue for transcending the preoccupation with these essentially instrumental views towards analyzing the wider societal implications of this innovation and for paying greater attention to social design issues [3]. McKenzie et al. refer to challenges, policy dilemmas entailed by multiple goals and failures in past IDM approaches, which have spurred the debate on appropriate overall e-IDMS strategies [4]. A number of normative frameworks for e-IDMS that deal with user-centric aspects have been suggested such as the set of principles for security usability developed by Jøsang et al. [5], the Seven Laws of Identity from Cameron [6] or the findings of the PRIME project [7].

These initiatives underline the paradigm shift that IDM approaches are currently experiencing towards a stronger focus on the user. User-centric IDM is expected to provide an individual "full control of transactions involving her identity data" [8]. In terms of security systems, security usability evolved as a special research field and is an integral part of user centricity though with a strong focus on technical design issues. More recent approaches of user centricity go beyond technical design and highlight the importance of a stronger integration of further aspects: e.g., applying experiences and techniques of the field of human-computer interaction (HCI) such as psychological and social aspects of

usability in order to encourage a design perspective that comprehends the user as a part of the system [9]. However, there are several different concepts and understandings of user centricity (cf. [8] [10]) and research on national e-IDMS in terms of this aspect has been neglected. IDM approaches in e-government have some major differences compared to private sector IDM, with other determining factors to incorporate [4]; above all, governments have to care for broader aims such as social inclusion and interoperability, and at the same time governments have coercive power, which may lower incentives to be responsive to citizen concerns. As these and similar aspects have not yet received adequate attention in research on user-centric design of a national e-IDMS, this paper aims to contribute to closing this gap. On the example of the Austrian system, the peculiarities of an e-IDMS are explained with regard to security usability in order to grasp challenging aspects of citizen centricity.

The paper is structured as follows: Section II depicts the research design of the analysis. Section III elucidates general aspects of user centricity and the relation between security and usability. In Section IV, relevant determinants for user-centric IDM approaches are suggested. This is followed by an explanation of the Austrian e-IDMS and its specific design in Section V. The pursuance of user centricity in the Austrian system is analyzed in Section VI, followed by explanations for the current situation and considerations about approaches to cope with major challenges (Section VII). Finally, in Section VIII, the results of this analysis are summarized and concluded.

II. RESEARCH DESIGN

This paper analyzes national identity management from a user-centric point of view and makes a contribution to develop suitable approaches for overcoming the challenges in this domain. The analysis is based on a case-study of the national e-IDMS in Austria as a top-ranking EU-country in terms of e-government [11]. This study is part of a larger comparative research project on the introduction of national identity management systems in selected European countries. The empirical investigation (conducted in 2008) was a combination of several methods: A comprehensive literature review, an analysis of research papers, official documents, expert statements, technical reports and specifications, face-to-face interviews with key decision-makers and stakeholders at different governmental levels that were involved in the innovation process; and practical tests of the e-IDMS. For the analysis of this paper, following research questions were identified:

- What are the significant aspects of user centricity for security systems and which role do they play for identity management particularly in the context of e-government? Starting with a brief introduction of user centricity in general, we focus on key parameters relevant for user-centric national IDM.
- What are the major characteristics of the national e-IDMS in Austria and how does it incorporate user/citizen-centric parameters and the user's perception of the system? After describing specific features and peculiarities of the Austrian system we analyze them with respect to parameters relevant for user centricity.
- How balanced is the interplay between the relevant determinants for user centricity in the Austrian e-IDMS and what are major challenges for avoiding a trade-off between security and usability? Based on findings of security usability combined with considerations about user perception shed light on the current situation regarding user centricity.

Our methodological approach draws upon theoretical conceptualizations of user centricity, security usability as well as technical concepts in the field of identity management. The four basic architectural models of e-IDMS – siloed, centralized, federated and user-centric identity systems (cf. [5] [8] [12]) – show how technical IDM concepts evolved towards a user-centric architecture. Hence, we include these models in our analysis.

As there are a lot of different views and conceptualizations of user centricity that do not provide a commonly accepted delineation of the concept or a universal set of criteria, our approach is also informed by key dimensions of user centricity identified as predominant in the relevant literature. As the aim of our paper is to analyze user-centric aspects exceeding technical design, the methodology also orientates on Davis' [13] already classical Technology Acceptance Model (TAM), which provides a suitable framework for better understanding of user perception as it allows to grasp relevant determinants and explanations for the users willingness to get involved with a new technology. In terms of security systems and identity management, this is of special interest as the ambivalent relationship between usability and security demands for a stronger consideration of user perception in this domain.

The TAM describes the interrelation between system characteristics, perceived usefulness, perceived ease of use (i.e., usability) and attitude for usage and actual usage behavior, i.e., the intention to use. Davis defines perceived usefulness as "the degree to which a person believes that using a particular system would enhance his or her job performance". This addresses the users' perceived level of potential improvement of workflows through the usage of ICT, i.e., which benefits users expect from system usage. Perceived ease of use (usability) is defined as "the degree to which a person believes that using a particular system would be free of effort". Thus it refers to the users' expectations of the systems usability and the efforts usage implies. These two factors form the users' intention to use a technology and have impact on the individual attitude for usage of a system and thus on the resulting usage and acceptance of the system itself [14] [15].

III. ASPECTS OF USER CENTRICITY

In general, user centricity can be described as the manifestation of a certain demand for more user-orientation in technology. Placing the user and his demands in the center of technology design should provide him more control and user value. The rapid technological progress and particularly the emergence of internet services played a certain role for

the paradigm shift towards a user-centric view. The decentralized structure of the internet, distributed architectures and the increase of online service created further complexity and new user-requirements for the implementation of usable technologies and services in this context, with user centricity becoming an essential aspect. This reflects in many different domains and in particular in the field of e-government.

A. *The Suspense between Usability and Security*

In terms of security, user centricity is a particular challenge as it addresses the tense relation to usability. Zurko defined user-centered security as “security models, mechanisms, systems and software that have usability as a primary motivation or goal” [9]. The challenge is to give "end-users security controls they can understand and privacy they can control for the dynamic, pervasive computing environments of the future" [9]. This strongly reflects in the emerging field of identity management (IDM) as it is all about processing the user's personal data for identification. User-centric IDM has the central aim to give users control over their personal data and allow them to understand and manage how these data is being processed in different contexts [16].

The importance of privacy issues and an adequate consideration of principles for data protection and privacy are obvious. But the technical realization of privacy and security is a complex task and it is challenging to implement a system that is both - secure and usable. Security systems often suffer from an imbalance between usability and security. As an understated security level undermines the objectives of the system, this imbalance is in many cases at the expense of usability.

Moreover, Jøsang et al. also postulate “a very real difference” between the degree of security of a system in theory and its actual security. This underlines the potential trade-off between usability and theoretical security, as the intended protection of security systems strongly depends on the user’s understanding of the system [17]. The introduction of new security technologies such as e-IDMS brings further challenges to avoid this possible trade-off. Hence, usability “becomes a strategic issue in the establishment of user authentication methods” [18]. Generally speaking, a user-centric e-IDMS should provide privacy protection and security as well as usability. The incorporation of security usability is essential for the success of secure technologies.

B. *Principles for Security Usability*

The existence of principles for security usability indicates the demand for suitable approaches to avoid this possible trade-off. One ancient and important attempt that influenced security design was provided by the Dutch cryptographer Auguste Kerckhoff. Already in 1883, he described six principles for security systems: 1. The system must be substantially, if not mathematically, undecipherable; 2. The system must not require secrecy and can be stolen by the enemy without causing trouble; 3. It must be easy to communicate and remember the keys without requiring written notes, it must also be easy to change or modify the keys with different participants; 4. The system ought to be compatible with telegraph communication; 5. The system must be portable, and its use must not require more than one person; 6. Regarding the circumstances, in which such a system is applied, it must be easy to use and must neither require stress of mind nor the knowledge of a long series of rules.

These principles had high impact on today’s security and cryptography systems and despite of their age, some are still relevant. Jøsang et al. [17] underline the particular importance of principles 3 and 6 for today’s system design. They tied in with Kerckhoff's principles and developed principles for security usability. They distinguish between principles for security action and security conclusion. A security action is triggered, when the system demands the user to produce some information or set a security mechanism, (e.g., entering a password is a typical security action). Security conclusion means the users’ ability, to recognize the security state of the system (e.g., knowing that a connection via SSL uses encrypted data transmission). The principles are based on the conclusion, that the intended protection provided by a security system strongly depends on the user’s capability to understand, which security actions and conclusions the system requires and to react appropriately. “Security systems will only be able to provide the indented protection when people actually understand and are able to use them correctly” [17].

Another approach that deals with user-centric security is provided by Cameron’s seven laws of identity [6], which offers some important guidelines for user centricity in identity management systems. Similar to the principles of Jøsang et al., the rules for system design suggested by Cameron also focus on user understanding as a crucial factor for providing the intended level of security.

User understanding is definitely a crucial aspect for user centricity that often suffers from exaggerated security claims. Hence, some authors (cf. [19] [20] [21]) question the effectiveness of common security advice and principles in this respect. For instance, minimum requirements for password security (e.g., length, combination of signs and numbers, etc.) might be of vast importance in theory. However, as they are often not practicable and security risks are rather abstract to users, they are more of a burden for them. Most security advice are simply too complex for being useful to end-users and do not fit their demands on the system. As a result, security mechanisms foil themselves and systems are often insufficient regarding user experience.

IV. DETERMINANTS FOR A CITIZEN-CENTRIC IDM APPROACH IN E-GOVERNMENT

The previous remarks show a certain demand for a consideration of further aspects that go beyond technical design issues. As this paper deals with national IDM in the field of e-government we emphasize on identifying crucial factors for user centricity in this respect. In order to highlight how user centricity concerns the technical design of an e-IDMS, this Section starts with an overview of the basic models for identity management.

A. Evolution of Technical ID Models

There are four main types of ID models that can be distinguished: siloed, centralized, federated and user-centric systems. A siloed system is completely uncoupled from other systems with no formal connections with other IDMS. Hence, data processed within the IDMS is separated from other systems and cannot be easily linked across different domains. With respect to data protection and privacy this is a highly important aspect. However, due to this separation, a siloed system does not facilitate data sharing. Therefore it often does not fit the needs for an efficient data processing and sharing across multiple domains. Thus it allows no SSO either and users need multiple accounts when interacting with more than one system.

The *centralized approach* aims to ease this inconvenience. In centralized systems all of a person's data are stored in a repository managed by a central provider and independent from the applications using the data. This central repository is accessible to service providers, which can use it for their applications. Users are able to authenticate through one account. However, the potential threats to security and privacy are high in centralized systems as all personal data is being processed in one single unit and users are completely reliant on the central provider.

The *federated model* represents a sort of mixture between the siloed and the centralized approach. Here, a central identity provider (IdP) manages data relevant for identification of a person and providers of services and claims (SP) can use these data. The federation allows linking up previously unlinked identifiers and SPs base their applications on one single authentication mostly without creating or maintaining user accounts on their own. Users only authenticate via one single account, which can be used for multiple services. Hence, a federated system offers more user convenience and reduces privacy threats of the centralized model as the IdP normally does not hold all personal data. However, as the IdP knows, which identifiers belong to a specific person, he has the ability to abuse this knowledge and breach the user's privacy. Thus the functionality of a federated system strongly depends on the reliability of the IdP and the creation of a trustworthy infrastructure.

To diminish the users' dependence of a central IdP in a federated system, the *user-centric model* evolved. It has a certain focus on the person interacting with the system and offers her more control. There is no central IdP, users can choose between different SPs as well as IdPs. As identity providers dot not belong to a federation they are expected to act in the users' interest rather than in those of the SPs. Due to this freedom of choice, which parties to trust and which information to reveal in a particular transaction, a person is more independent and can gain advanced reliability in a user-centric system. However, this extent of control also brings greater demands on the users' skills to handle this [5] [8] [12].

B. (Preliminary) Parameters

The relevance of user centricity for the success of e-government is evident. Already in 2004, the mid-term review of the EU action plan eEurope 2005 attested a need for a "move to a demand-driven approach that emphasizes service delivery, end-user value for all and functionality" [22]. As citizens build a major subset of users in e-government, this paper focuses on citizen centricity in the context of electronic IDM and the term "user" mainly refers to the citizen. IDM in e-government is different from IDM in private sector. This difference demands for the consideration of other aspects. So as to realize a user/citizen-centric e-government approach, Blakemore and Undheim appeal for "a clearer focus on technologies that use citizen-relevant channels to deliver citizen/public value, rather than just to deliver efficiency gains and cost savings" [23]. Governments have to ensure equal access to public services for all citizens. This implies the multi-channel principle, i.e., to offer alternative channels to government services (online as well as offline). Online public services should be usable with familiar technologies in order to "maximize inclusion and utility, and to avoid unnecessary demands (skills, device purchase etc.) on citizens" [23].

In [1] we identified three major factors for citizen centricity in national IDM:

Equality of access: In e-government, IDM has to consider issues on a broader scope such as social inclusion, affordability, consistency, interoperability and the availability of public services for the whole population. Inclusiveness and providing non-exclusive access to public services via traditional as well as online channels to all citizens is a central requirement. Public services have to be accessible without e-ID as well and without any disadvantages in order to avoid a digital divide. The e-ID should reduce, not enlarge the distance between the citizens and public administration.

Privacy protection: The consideration of data protection and privacy aspects as a core issue is of vast importance for IDM. Governments have the substantial duty to protect the citizen's privacy and support them in controlling their personal data. Hence, a major requirement on a user-centric e-IDMS is its contribution to empowering users in managing their ID in a self-determined way. One crucial property "that must be satisfied in order to ensure privacy protection" is the unlinkability of personal data [24]. This means to avoid the use of unique identifiers, which are a threat to privacy because they can be used for „privacy-destroying linkage and aggregation of identity information across data contexts" [25]. Thus, different identifiers for every sector should be used, e.g., in the form of local pseudonyms [25]. Data processing in the e-IDMS has to be transparent to users so that they are able to comprehend how their personal data is being processed within the system.

Citizen convenience: Improving convenience for users is a central issue for IDM, as it determines how the system responds to the citizens' demands. This affects e-government in particular as public services should be usable for every citizen. The e-ID should support SSO and ease the users' need to handle multiple accounts and the corresponding procedures. At the same time the e-ID should provide citizens' a suitable and convenient way to deploy their e-ID

in different contexts without the need for handling multiple login data and procedures.

An additional factor in line with these parameters is *trust.* It is strongly interrelated with the other factors and particularly connected to the possible trade-off between security and usability. One might say trust is in between the poles of this possible trade-off: Security and trust are interdependent and determine each other in some respects. Lacking usability foils security and as a consequence also lowers trust in the system. When security mechanisms empty into high complexity, users are then not able to understand and consider them appropriately. One important aim of national IDM is to increase the amount of trust in e-government. "Concepts of trust and identity have become intimately bound, and go beyond a purely technical focus" [26]. Government organizations require citizens to trust in them "in order to be legitimate and efficient" [27]. Applying a reliable environment for public service usage is an essential precondition for citizens' trust in e-government. The e-IDMS should establish a solid fundament for trustworthy interactions between citizens and government with the assurance, that his personal data is treated correctly and not against his privacy [27].

V. DEVELOPMENT OF THE AUSTRIAN E-IDMS AND SPECIFIC DESIGN CHARACTERISTICS

First initiatives for a national e-IDMS already began in the early 90ies with plans to set up a smart card system in the field of social and health insurance administration. The European Directive (1999/93/EC of December 13 1999 on a Community Framework) for electronic signatures triggered further impulses at a European level. Austria was (among other EU-member states) directly involved in designing the signature and hence one of the first countries in Europe to implement a national e-IDMS for e-government services. In October 2000, the idea of a smart card for unique identification of citizens in a certain role – the so-called "Citizen Card" (in German called "Buergerkarte") was born and announced as an integral part of Austria's national conversion of the eEurope initiative "information society for all". Shortly afterwards the government approved a resolution for the implementation of a smart card based system to support e-government services [28]. First prototypes of Citizen Cards were released during a pilot scheme and available from 2002 until 2005.

As the system architecture for the Citizen Card (CC) follows a technology-neutral approach the concept is not bound to one specific card. Although plans during the development process aimed to use the electronic health insurance card (today known as "e-Card") as primary device for the CC concept. Together with the ATM card, the e-Card became one of the major carrier devices to carry the CC-function.

A. Major system characteristics

The Citizen Card as centerpiece of the Austrian e-IDMS has some specific characteristics. First of all, it strives for technology-neutrality and multiple tokens as it is not a physical card but a virtual concept that can be implemented on various different hardware components (e.g., smart cards, cell phones, USB devices) [29] . Due to their broad range of use, smart cards are currently the preferred carrier devices with e-Cards and ATM cards as main tokens. These cards are wide-spread among the Austrian population. Every citizen (8.3 million) has an e-Card and about 80% of the Austrians hold an ATM card. These cards have the "sleeping" CC-function integrated, which means that they are prepared for the e-ID but the function needs initial activation. Ministerial IDs, staff IDs of the Chamber of Commerce and student IDs are some of the further possible carrier devices. The Citizen Card fulfills two basic functions in online transactions with public administration: it allows to verify the card holder's identity and to authenticate his/her request by providing an electronic signature, which is stored on the card. A peculiarity of the e-IDMS is its ID model and the technical privacy concept: the system is based on a complex techno-organizational infrastructure with an ID model that is grounded on unique identifiers in the Central Register of Residents (CRR), whereas sector specific identifiers (ssPINs) are derived from. The amount of data stored on the card depends on the specific carrier device. But every Citizen Card contains at least the card holder's full name, date of birth, the source-PIN as unique identifier (for details see next Section) and the cryptographic public keys needed for the e-signature and content-encryption. The private key is stored in a separate hardware unite on the cards' chip. For protection of these data, up to three different PIN-codes that are only known by the card holder are applied. The first one is for general access protection of the device, the second one for using the e-signature and the optional third for the additional feature of an integrated data box for storing electronic documents such as a birth certificate [29] [30].

B. Techno-organizational infrastructure and ID model

The Austrian e-IDMS is based on a complex techno-organizational infrastructure. This set-up can be explained regarding the CC's two main functions – identification and e-signature. For the creation and provision of the e-signature, a Public key infrastructure (PKI) was established. The PKI consists of one or more Certificate Authorities (CAs) that issues all services relevant for the e-signature and Registration Authorities (RAs), where card holders can apply for an e-signature. (Currently, the institution a.trust is the only CA in Austria that applies qualified certificates required for the e-ID). This CA coordinates several RAs (i.e., banks, post offices, etc.), which usually provide the full activation of a Citizen Card including the integration of the ID model [29] [30].

The core infrastructure component for the ID model is the Central Register of Residents (CRR). This register is a national database, which contains data of all Austrian residents. The primary key for every data-record is the CRR-number, a 12-digit number, which acts as unique identifier for a specific person. The CC's whole ID model is based upon the CRR-No. but not directly used to respect privacy protection. Hence only a strong encryption of the CRR-No. – the so-called source-PIN – is stored in the card to identify the card holder and the law prohibits storing it outside the card.

The source-PIN is created during card activation and used for generating sector-specific PINs (ssPIN). An ssPIN is based on an irreversible cryptographic function, which prevents to recreate its original elements (i.e., the source-PIN). Currently, there exist ssPINs for 26 sectors (e.g., tax, education, health, etc.). An ssPIN is used for unique identification of a person within the specific belong sector. Storage of an ssPIN is regulated by the law and only allowed within the sector it belongs to or is allowed to use it [30]. The Figure below gives an overview of the interrelations between the major infrastructure components.

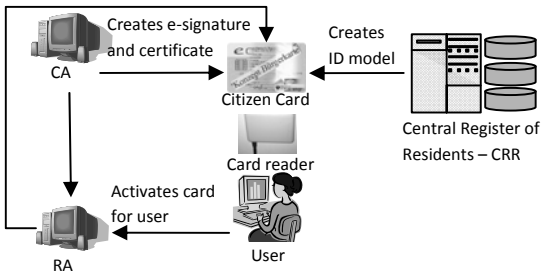

Figure 1: Techno-organizational infrastructure

C. *Requirements and user interaction with the e-IDMS*

Using the CC in online services requires the initial activation of the function. RAs carry out the corresponding procedures for the card holder. Until recently, this was only possible by visiting an office. Now the whole activation process can be carried out online as well with the precondition that the e-Card is the carrier device. For the handling of the CC, a PC with internet connection, a card reader and special software – the so-called Citizen Card environment (CCE) – are required. The CCE is available in different variants, including productions completely free of charge. In 2009, an online-variant of the software has been introduced. The activation for ATM cards costs 12 € once, and the certificate for the e-signature is 15.60 € per year.

A typical user session with CC usually proceeds as follows: most public online services are available via SSO on the Austrian e-government portal help.gv.at. After choosing a service, the user is prompted to authenticate by putting his card into the card reader and entering a PIN-code. This grants the service access to the user's ID data on the card in order to generate a confirmation for accessing the service (typically, it looks like this: "I, John Doe, born on January 1st 1973, confirm that I am using this service. Date, time: January 12, 2010, 9:32:12"). This confirmation has to be signed by the user by entering his signature-PIN. Then, depending on the current service, some forms have to be filled out with personal data (e.g., income data for tax declaration). When submitting, the user is prompted again to sign another confirmation in order to affirm his service request and the correctness of his data. During submission, the service requests creation of the ssPIN in the back office, by reading the source-PIN out of the card and combining it with the unique number of the current sector the service belongs to (e.g., tax). After service completion the data is being further processed in the back office applications of the appropriate authority. It depends on the administrative procedure, whether data processing is completely automated or includes further treatment by the administration office [29] [30].

VI. THE BIASED PICTURE OF A CITIZEN-CENTRIC VIEW ON THE AUSTRIAN E-IDMS

This Section analyzes the realization of relevant determinants for citizen centricity (as described in Section IV) in the Austrian system and then strives for explanations of the biased picture that the analysis and the following delineations draw.

A. *Mapping of the e-IDMS against typical ID models*

A tentative attribution of the Austrian system to the four basic ID models as described in Section IV.A is revealed by the Table below:

TABLE I. MAPPING OF THE E-IDMS

	Siloed	**Centra-lized**	**Fede-rated**	**User-centric**
Method of authentication			X	
Location of Identity Information		X	X	(X)
Method of linking accounts/learning if they belong to the same person			X	(X)
Trust Characteristics (who is dependent on whom, for what)		(X)	X	
Convenience			X	(X)
Vulnerabilities	(X)	X	X	

As the basic models represent rather simplified "ideal-types", this mapping cannot be stringent, but still it gives an initial clue about the system with regard to citizen centricity.

The user authenticates with the Citizen Card to each service via SSO, whereas the CRR is the central identity provider and supplies the ID data to service providers. Hence, the method of authentication correlates with the federated model. Regarding location of identity information, the e-IDMS is mainly a mixture of centralized, federated and user-centric model: all relevant ID information is centrally stored in the CRR that service providers can integrate in their separate accounts but identity verification usually requires the CC. Linking of data across different domains is prevented by the ssPINs and the corresponding legal regulations, i.e., it is only allowed to link data within the same sector or by offices permitted to process the data. But the identity provider knows in which services a user deploys his e-ID and the CRR contains more personal data than generally needed for every service. Thus, users have to trust that the federal identity provider and the service providers

use their data properly and with respect to privacy. Due to its powerful role, the user is somewhat constrained by the federal identity provider. As service utilization with e-ID requires the CC as a separate device and PIN-codes, users gain more control. However at the same time they are also confronted with increased requirements to handle the e-ID. As SPs have to request the federal IdP for the creation of ssPINs, they are not completely liberated from the burden of credential management. Altogether, the Austrian e-IDMS mainly follows a federated approach, whereas some of its features strive for a user-centric system design.

B. Provision for citizen centricity

The e-IDMS incorporates a citizen-centric approach and the consideration of relevant aspects reflects in several ways. Regarding *equality of access*, different approaches have been employed to avoid social exclusion and exclusiveness of the e-IDMS; some of them especially during the rollout phase also in order to broaden penetration and stimulate usage of the system: to reduce financial burden, online transactions with the e-ID were free of charge until the end of 2006. Since 2008, there are no costs when using the e-Card as CC. The technology-neutral concept allows using several different devices as carrier for the e-ID. Due to the possibility to integrate the e-ID into different systems, it provides openness and interoperability at least to some extent. The e-ID is not compulsory and citizens are free to decide whether to use it or not. Austria provides a broad scope of different e-government services and of course, services are still available in traditional offline forms. Online services do not per se require the e-ID and can be used with common authentication methods (i.e., username/password) as well. Just a few services require the e-ID and only in cases, where the transaction should be processed completely online without any media friction. In this respect, the e-ID could also be noticed as enabler of an additional access-channel. Due to the availability of multiple tokens, citizens also have some choice, which carrier device to use as Citizen Card. As there are no costs for using the e-Card, neither for activation nor for usage, most people are expected to prefer this device.

For the consideration of *privacy*, the e-IDMS is based on a sophisticated ID model, which strives for a balance of security and data protection. As persistent static identifiers allow data linking across different domains, they enable potential privacy threats, i.e., identity fraud or infringement of personal information [4]. Hence, the Austrian e-IDMS is based on a complex ID model, which avoids the direct processing of a unique identifier (as described in Section V). The use of the ssPINs aims to prevent illegal linkage of personal data. These identifiers are different for a defined number of domains (currently 26), and legal regulations limit the use of an ssPIN to the domain it origins from or is allowed to use it. Moreover, it is also prohibited to persistently store the source-PIN (as basis-number for an ssPIN) outside the Citizen Card. This technical sector separation corresponds to the deployment of different pseudonyms. As the e-IDMS applies an electronic token in form of a hardware device, users receive at least some control over their personal data. The combination of knowledge (the PIN-code) and possession (the card) improves security of the authentication procedure compared to usual concepts, which are based on username/password.

The system contributes to enhance *citizen convenience* as it provides a comprehensive approach to harmonize authentication procedures. Most Austrian e-government services are available at the e-government portal help.gv.at and citizens can use their CC to authenticate at this single entry-point via SSO. With the CC as one device to authenticate in different services, identity management is alleviated as citizens do not have to handle several user accounts and credentials. The openness of the concept to different carrier devices gives users the possibility to choose their preferred token for the CC-function. The possibility of activating the e-Card completely online offers a convenient way to enable it as carrier medium. Beside the two main carrier cards (e-Cards, ATM cards) there was also a CC available on a cell phone without needing a smart card or card reader. A legal provision allowed this so-called “Citizen Card light”, which had less security requirements. As the legal regulation was only temporarily, the “Citizen Card light” was only available until the end of 2007. In November 2009, an improved version of the CC on a cell phone has been announced and is available since 2010 [31]. An additional online version of the CCE is available since 2009, which is completely browser-based and thus reduces efforts as users do not have to install additional software components.

The techno-organizational infrastructure of the e-IDMS contributes to create a circle of *trust*. The involved parties (CA, RA, IdP, SPs) have to fulfill certain requirements, which are legally defined (e.g., in legal regulations for e-signature, privacy, administrative procedures, etc.). The Data protection commission serves as a custodian over the lawful appliance of the e-IDMS. The Ministry of the Interior administrates the CRR and acts as central identity provider on behalf of the DPC. Service providers have to register their applications and to request for deploying their services with the CC. Due to the privacy aware system implementation and the increased amount of control, the e-IDMS seems to be grounded on a reliable fundament that is capable of enhancing citizens’ trust in e-government.

C. Current usage and acceptance of the system

With the two main carrier devices – e-Card and ATM cards – the penetration of potential CC is high as these cards are wide-spread in Austria and already prepared for the CC-function. There is also a number of services available that can be used with the CC at all three administrative levels (federal, provincial, municipal) at the Austrian e-government portal. However, there is no significant increase in card activation and usage although the Citizen Card is obtainable for several years already. The optimistic goals for the number of card activations had to be adjusted downwards several times. E.g., the intended number of 200,000 active CCs by the end of 2005 was not achieved. In 2006, only about 60,000 activated cards were in use and a substantial part of these are bulk activations by public organizations [1]

[32]. According to recent estimates of the Federal Chancellery, about 120,000 were circulating by May 2009 [33].

A look at the usage levels of three exemplarily online services reveals some peculiarities [1]:

TABLE II. USAGE OF SERVICES IN 2007

Transactions	Total	Total - online	Citizen Card
Tax declarations	Approx. 4,000.000	1,846.922 (46%)	12.801 (0.7%)
Student grants*)	66.933	53 (0.1%)	53 (0.1%)
Retirement pay account **)	35.974	10.485 (29.1%)	10.485 (29.1%)

*) Data refer to academic year 2007/08. **) Data refer to 2008.

There are some remarkable differences in usage of these services. The number of transactions for tax declaration is of particular interest as it is considerably higher compared to the other services. It is the most successful e-government application in Austria; the amount of citizens transmitting their tax declaration online is close to 50%. However, the vast majority prefers common authentication based on username and password. Less than 1% uses the CC for this service. As online processing of the two other services requires authentication with CC, the number of online transactions equals the number of transactions with Citizen Card. The comparatively higher amount of citizens using the online service for retirement pay account queries is explainable by the significantly higher number of potential users (students only represent a small share of the population) as well as strong advertising and PR actions taken for e-health and social services during the roll out of the e-Card, which received increased public attention.

D. Explaining the current situation

The usage level is only progressing very slowly and a remarkable increase as expected by the main stakeholders has not occurred yet. Despite of the important considerations of citizen centricity in the Austrian system, the overall situation draws a rather biased picture.

In order to identify explanations for this situation it is expedient to take up a more general view on the e-IDMS as a security system, as this allows gaining a better understanding of relevant determinants. From this point of view, the e-ID represents a certain security mechanism for citizens when interacting with public administration. Users are mostly considered to be the soft spot of a security system that often neglect the proper use of security mechanisms. This negligence is often stated as irrational or ascribed to the users' lack of understanding the security mechanism. However, a closer look shows that users act "entirely rational" when rejecting security advice, as [21] argues: "A main part of the problem with security advice is that we hugely exaggerate benefits". Additionally, the cost of user effort is often ignored [21]. Security systems and the corresponding requirements overwhelm users and offer them "a poor cost-benefit tradeoff". Therefore, security mechanisms are often rejected by users as the high requirements made of users do not match the predicted benefits. Users are confronted with a real effort to handle a security system while at the same time this effort should prevent from threats that are rather theoretical [20] [21]. Applications with an exclusive focus on security mostly offer "a small perceived advantage in exchange for dealing with an extraordinary complex interface" [19].

These remarks can also be transferred to the situation of the Austrian system. The high complexity of the e-IDMS plays a certain role for the user experience and thus is a major vulnerability of the system, which has been a central point of criticism and entails further controversial aspects. Although the sophisticated ID model was designed to prevent data linkage and protect the citizens' privacy, the effectiveness of this solution is questioned. As online service process many personal data, illegal data linkage is still feasible over these data, despite of the deployment of ssPINs. The complex coherences of the system cause a lack of transparency, which does not allow users to comprehend how their e-ID and the related data are being processed within the system. This also limits the users' amount of control over their personal data. Essential requirements for preventing the e-ID to become an instrument of surveillance are effective controls of the maintenance of fundamental privacy principles (e.g., commensurability, data minimization, purpose limitation of data processing, etc.). Due to the high overall complexity and opacity of the system, this controllability of a proper data processing in account with privacy is rather hard to ensure. Lacking transparency and high complexity can also be expected to lower the citizens' level of trust in the e-IDMS. Overall, the e-IDMS and especially the CC are perceived as too complex with several flaws regarding citizen centricity. Benefits and convenience are rather low compared to the high requirements made of users [32] [34].

These propositions address several serious aspects, which indicate the suspense between usability and security in the Austrian system in several contexts. There is some certain evidence for this assessment. Two studies revealed some interesting indications for the situation: In the "eUser" study of 2005, 27% of the Austrian Internet users described the need for a special end-user device for identification (i.e., the CC) as a burden for using online public services. Costs were estimated as too high compared to the expected benefits of the CC [35]. According to another study from 2006, 33% of the respondents mentioned to have no intention to obtain a CC at all. The reasons stated for this correspond to the propositions above: There is no or not enough need for the CC (46%), lack of information about usage (37%), the CC is not trustworthy enough (22%). Furthermore, 38% of the respondents that stated to be card holders mentioned to never have used their CC [36].

When considering the high requirements for usage (card activation, card reader, installation of special software), it is not very unlikely that handling of the e-ID is perceived as burden. Several problems and obstacles in practical use also appear from entries in the online support-forum for CC

users.[1] Practical tests conducted for this research confirmed the non-trivial and partly complicated handling of the e-ID. Indeed, the number of security actions and conclusions (cf. [16]) demanded from the user often seems to be over exaggerated and beyond a standard users understanding of a common system.

Beside the problem of high complexity, from a user's perspective, the system does not seem to offer enough benefits and incentives. The marginal rate of contacts for a citizen with public administration (only approx. 1.7 contacts per year) and the existence of common and fairly effective authentication methods are important aspects in this context [1]. This, combined with the exaggerated efforts of using the e-ID may considerably account for a weak benefit/cost ratio (whereas costs do not primarily address financial expense, but a disproportional effort). Thus, the e-IDMS provides only a low user value.

It has to be noted that major stakeholders are aware of this situation and since the mentioned studies have been conducted, several measures were set to improve citizen centricity and increase diffusion. The measures mainly address the reduction of costs and usability problems: e.g., no charges for the e-Card, promotion of cost-reduced notebooks with integrated card reader and pre-installed software, an additional online version of the CCE and the re-launched option of a cell phone based CC. To increase penetration and usage, several promotion campaigns mainly target teenagers and students. However, at present it is uncertain whether these actions are adequate to cope with the current situation and increase the level of usage.

VII. IMPROVING USER CENTRICITY BY (RE-)FOCUSING ON THE USER VALUE

The previous Section has shown that, although the Austrian system seems to consider several citizen-centric aspects the actual situation is not satisfying regarding usage and acceptance. This leads to the TAM as its aim is to identify relevant determinants for acceptance or rejection of a technology. A classification of the current situation to the two factors of the TAM, usefulness and ease of use, confirms the biased picture depicted and offers further explanations. The benefits a user expects from the system are addressed by the factor perceived usefulness. The ease of use addresses the costs and efforts that system usage entails. Now it has been pointed out that these efforts are perceived as rather high because citizens are confronted with additional requirements (i.e., card activation, card reader, special software) and the overall complexity of the system is perceived as too high.

At a first glance, the reduction of complexity might come into mind as necessary approach for easing the situation and improving citizen centricity. Reducing complexity certainly is important to lower current burdens to usage. But does this also stimulate usage? At least in the Austrian case this effect did not occur: stakeholders took several measures in this regard to alleviate handling of the e-ID. However, it is currently not foreseeable whether these actions will be effective. Moreover, the scope of action for reducing complexity might be limited with respect to the intended security level. Plus, a deviation from the sophisticated ID model of the Austrian e-IDMS cannot be expected to be performed easily without enormous efforts and problems regarding privacy protection.

In this regard, a rather interesting aspect is pointed out by Gutmann and Grigg: users do accept "a little more complexity (…) for a fair offering in value" [18]. Davis [13] argued similar, whereby "(…) users are often willing to cope with some difficulty of use in a system that provides critically needed functionality". This implies a stronger focus on finding a balance between acceptable complexity and user value. It might seem obvious that system usage is strongly interdependent with the benefits users can expect. But as already underlined in the previous Section, this determining issue seems to be neglected especially in terms of security and identity management systems. Hence, "cost and benefits have to be those the users care about, not those we think the user ought to care about" [20]. Costs are not just meant in a monetary sense here but subsume all the efforts that users are confronted with. When the transaction costs incurred by switching from familiar forms of identification to the e-ID are high and the expected benefits due to this switching are low then usage is expected to be low either.

In accord with the TAM it thus strongly depends on the perceived usefulness of the e-IDMS, whether users are willing to accept a certain degree of complexity. The difficulty of usage can surely contribute a lot to "discourage adoption of an otherwise useful system", but "no amount of ease of use can compensate for a system that does not perform a useful function" [13].

The analysis has already shown that the system does not seem to offer enough benefits and incentives. Whilst the scope of available services is relatively broad, at the same time, the average frequency of citizen contacts per year is relatively low. Hence the incentives to access these services via CC are marginal and the usefulness is perceived as too low either.

When considering the recent measures of major stakeholders, it is salient that the ease of use, respectively the usability of the e-IDMS seems to receive more attention than usefulness. Hence there is a certain demand for increasing benefits and creating a "real" user value, which implies, that service provision plays a crucial role for user centricity in the e-IDMS. From a user's point of view, current services with e-ID do not considerably differ from common e-government services except of the authentication method. An important step forward might be finding out, which additional benefit of the e-ID citizens would really appreciate. For instance services, that offer new possibilities for interaction with public administration and that legitimate the sophisticated concept behind the system. At its current state, the e-IDMS seems to be less suitable as an instrument for standard-users than for users with special demands. For instance, the number of citizens with a frequent use for the e-signature and document encryption yet seems rather marginal. This might be different in businesses with a certain demand for this application and the security level provided by the e-ID.

[1] http://tinyurl.com/c9kuvn

Major stakeholders also rated the business sector as crucial for further diffusion.

A certain additional value for citizens could be to enhance transparency of government actions: e.g., to grant users access to administrative documents that pertain to themselves and to provide information about current administrative proceedings in terms of freedom of information, of course with respect to privacy and data protection issues. Here, trust as an important aspect comes in again. Freedom of information laws appears "to have contributed to citizens showing higher levels of comfort about how their information will be handled" [4]. Or in other words: when citizens are able to comprehend how their personal data is being processed in public administration, this contributes to increase trustworthiness in government, which represents an important incentive. From a privacy perspective, transparency is essential as surveillance can only be effectively controlled and prevented when information about purpose of e-ID usage and processing are definitely regulated and accessible for citizens [34]. Applications for e-ID in terms of freedom of information would also be conducive to improve effectiveness of privacy as it contributes to improve an individuals' control over his e-ID respectively his personal data.

VIII. CONCLUSION

The analysis of the Austrian e-IDMS regarding its incorporation of citizen centricity reveals a biased picture: although the system includes important citizen-centric factors and several measures were set to reduce complexity and alleviate handling of the e-ID, the level of usage and acceptance of the system does not meet the expectations of major stakeholders. This ambivalent result highlights that the intentions behind the e-IDMS regarding end-users do not seem to match the users' perceptions of the system. The implementation of the Austrian system was dominated by strong focus on security. This entailed a high overall complexity, which is a particular burden for acceptance and usage. However, measures to reduce this complexity have not lead to the intended effects yet. In this respect, the e-IDMS indeed reflects the depicted suspense between security and usability. The crucial challenge for security systems in general and e-IDMS in particular is to find suitable approaches for avoiding this suspense. First and foremost this implies a stronger focus on providing a "real" user value. This seemingly rather obvious finding addresses the necessity for a paradigm shift in system design to compensate the mismatch between design philosophy behind the system and the usability needs regarding security usability from a user's view.

An important step towards finding suitable approaches for easing this situation is to emphasize on user perception as determinant of vast importance for user centricity. The deployment of the TAM allowed to conclude that this necessary focus is currently rather neglected in the e-IDMS. The measures taken mainly address the ease of usage (i.e., increase usability) whilst the usefulness of the system (i.e., the expected benefits) is left behind. Hence, there is a certain demand for further efforts to improve usefulness, which mainly concerns service provision and the creation of additional user value. Whilst the e-ID in its current state inter alia suffers from the end-users irregular demand, businesses might have a more frequent need.

The Austrian case-study provided a useful example about the importance of considering further aspects in system design that go beyond technical issues in order to gain an expedient level of user centricity. These aspects refer to complex interrelations among multiple scopes especially in terms of e-government. The major challenge in this regard is to balance multiple goals, i.e., to provide a certain level of security, protect the citizens' privacy and offer both usable and useful features from a citizen's perspective. Necessary adaptations do not just address the technical design of the system but might also include further actions to take, i.e., reconfigurations of policy frameworks and legal regulations for e-ID usage. Furthermore, governments neither are nor should they be in a position to simply introduce additional services as this is a matter of checks and balances. Hence, a focus on improving transparency for citizens could contribute to experience user value. An additional benefit citizens could appreciate might be to facilitate access to government information and administrative proceedings that concern them. This institutionalization of freedom of information would also contribute to improve trust in (e-) government. As the e-IDMS represents an innovation, a rather tentative increase in acceptance and usage does not seem surprising. However, when this technology should establish itself in a mid-term perspective, this requires by all means the composition of further measures in order to strive for a more balanced provision of citizen centricity with respect to its multiple determinants.

REFERENCES

[1] G. Aichholzer and S. Strauß, "The Citizen's Role in National Electronic Identity Management. A Case-study on Austria", Proc. of the Second International Conference on Advances in Human-Oriented and Personalized Mechanisms, Technologies, and Services (CENTRIC 09), IEEE Computer Society, 2009, pp. 45-50, doi: doi.ieeecomputersociety.org/10.1109/CENTRIC.2009.13

[2] M. Lips, J. Taylor, and J. Organ, "Identity management as public innovation. Looking beyond ID cards and authentication systems", in ICT and public innovation: assessing the modernisation of public administration, V. Bekkers, H. van Duivenboden, and M. Thaens, Eds., Amsterdam: IOS Press, 2006, pp. 204-216.

[3] M. Lips, J. Taylor, and J. Organ, "Electronic government towards new forms of authentication, citizenship and governance", Paper to Oxford Internet Institute conference: Safety and Security in a Networked World, October 8-10, Oxford University, 2005.

[4] R. McKenzie, M. Crompton, and C. Wallis, "Use Cases for Identity Management in E-Government", in IEEE Security and Privacy vol. 6 (2), March-April 2008, pp. 51-57.

[5] A. Josang, M. AlZomai, and S. Suriadi, "Usability and Privacy in Identity Management Architectures", Proc. of the fifth Australasian symposium on ACSW frontiers - Volume 68, Australian Computer Society, 2007, pp. 143-152.

[6] K. Cameron, "The laws of identity", 2005, http://tinyurl.com/2226ry.

[7] J. S. Pettersson, S. Fischer-Hübner, N. Danielsson, J. Nilsson, M. Bergmann, S. Clauss, T. Kriegelstein, and H. Krasemann, "Making PRIME usable", Proc. of the 2005 Symposium on Usable Privacy and Security (SOUPS '05), vol. 93, New York: ACM Press, 2005, pp. 53-64. doi: doi.acm.org/10.1145/1073001.1073007

[8] A. Bhargav-Spantzel, J. Camenisch, T. Gross, and D. Sommer, "User Centricity: A taxonomy and open issues", Journal of Computer Security vol. 15 (5), October 2007, pp. 493-527.

[9] M. E. Zurko, "User-Centered Security: Stepping Up to the Grand Challenge", Proc. of the 1st Annual Computer Security Applications Conference (ACSAC 05), IEEE Computer Society, 2005, pp. 187-202, doi:doi.ieeecomputersociety.org/10.1109/CSAC.2005.60

[10] T. M. Eap, M. Hatala, and D. Gasevic, "Enabling User Control with Personal Identity Management", Proc. of the IEEE International Conference on Services Computing (SCC 07), IEEE Press, 2007, pp. 60-67, doi: doi.ieeecomputersociety.org/10.1109/SCC.2007.56

[11] Cap Gemini Ernst and Young, "Online Availability of Public Services: How is Europe Progressing? Web based Survey on Electronic Public Services. Report of the Sixth Measurement", 2006, http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/online_availability_2006.pdf

[12] M. Donohue and A. Carblanc, "The role of digital identity management in the internet economy: a primer for policymakers", No. DSTI/ICCP/REG(2008)10/REV1: Organisation for Economic Co-operation and Development (OECD), 2009.

[13] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology", MIS Quarterly, 13, September 1989, pp. 319-339.

[14] L. Leong, "Theoretical models in IS research and the technology acceptance model (TAM)", in Technologies & Methodologies For Evaluating information Technology in Business, C. K. Davis, ed., Hershey, PA: IGI Publishing, 2003, pp. 1-31.

[15] Y. Malhotra and D. F. Galletta, "Extending the Technology Acceptance Model to Account for Social Influence: Theoretical Bases and Empirical Validation", Proc. of the Thirty-Second Annual Hawaii International Conference on System Sciences (HICSS 99), Washington, DC: IEEE Computer Society, 1999, pp. 6-14.

[16] M. Hansen, H. Krasemann, M. Rost, and R. Genghini, 2003, "Datenschutzaspekte von Identitätsmanagementsystemen. Recht und Praxis in Europa", Datenschutz und Datensicherheit 27 (9), 2003, pp. 551-555, https://www.datenschutzzentrum.de/projekte/idmanage/DUD-27-9.pdf

[17] A. Jøsang, B. AlFayyadh, T. Grandison, M. AlZomai, and J. McNamara, "Security Usability Principles for Vulnerability Analysis and Risk Assessment", Proc. of the 23rd Annual Computer Security Applications Conference, 2007, pp. 269-278, doi: 10.1109/ACSAC.2007.14

[18] C. Braz and J.-M. Robert, "Security and Usablity: The Case of the User Authentication Methods", Proc. of the 18th International Conference of the Association Francophone d'Interaction Homme-Machine (IHM 06); Vol. 133, 2006, pp. 199-203, http://doi.acm.org/10.1145/1132736.1132768

[19] P. Gutmann and I. Grigg, "Security Usability", IEEE Security and Privacy 3 (4), 2005, pp. 56-58, http://www2.computer.org/portal/web/csdl/abs/mags/sp/2005/04/j4056abs.htm

[20] B. Schneier, "Balancing Security and Usability in Authentication", February 2009, http://www.schneier.com/blog/archives/2009/02/balancing_secur.html

[21] C. Herley, "So Long And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users", Proc. of the 2009 New Security Paradigms Workshop (NSPW 09), September 2009, pp. 133-144, http://research.microsoft.com/en-us/um/people/cormac/papers/2009/solongandnothanks.pdf

[22] EU-Commission, "eEurope 2005 Mid-term Review", 18.02.2004, Bruessels: Commission of the European Communities, 2004, http://ec.europa.eu/information_society/eeurope/2005/doc/all_about/acte_en_version_finale.pdf

[23] M. Blakemore and A. T. Undheim, "A Handbook for Citizen-centric eGovernment", 2007, http://www.ccegov.eu/downloads/Handbook_Final_031207.pdf

[24] FIDIS, "D13.6: Privacy modelling and identity", Deliverable-Report., Future of Identity in the Information Society, 2007, http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp13-del13.6_Privacy_modelling_and_identity.pdf

[25] M. Rundle, B. Blakley, J. Broberg, A. Nadalin, D. Olds, M. Ruddy, M. T. M. Guimarares, and P. Trevithick, At a crossroads: "Personhood" and digital identity in the information society, No. JT03241547, 29.02.2008: Organisation for Economic Co-operation and Development (OECD), 2008, http://www.oecd.org/dataoecd/31/6/40204773.doc.

[26] F. Wilson, "Think Paper 11: Trust and Identity in Interactive Services: Technical and Societal Challenges", 2007, http://www.ccegov.eu/Downloads/Paper%2011%20-%20Trust%20and%20identity%20in%20interactive.pdf

[27] P. Chadwick, "Managing identity, privacy and the public trust, Institute of Public Administration Austrialia series: The art of the long view. The role of Government: Taking responsibility or sharing it?", 2006, http://www.privacy.vic.gov.au/privacy/web.nsf/download/D9010341D53F4684CA2571790011A65E/$FILE/Managing%20iden

tity,%20privacy%20and%20the%20public%20trust%20%28IPAA%29%2016%20May%202006.pdf

[28] A. Hollosi, H. Leitold, and R. Posch, "Die Bürgerkarte: Basis und Infrastruktur für sicheres e-Government", in Tagungsband der Arbeitskonferenz Enterprise Security - Unternehmensweite IT-Sicherheit, P. Horster, ed., Paderborn, Germany: IT-Verlag, March 2002, pp. 1-12.

[29] G. Karlinger, D. Konrad and R. Posch, "Weissuch Bürgerkarte", Version May 2002, http://www.buergerkarte.at/regain/file/D:/webs/at.buergerkarte.downloads/WeissbuchBuergerkarte.20020515.pdf?index=main

[30] Austrian Federal Chancellery,"Administration on the Net - The ABC guide of eGovernment in Austria", No. New edition 7/2008, Vienna: Austrian Federal Chancellery, 2008, http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=19394

[31] Heise Online, "Österreich führt Handy-Signatur im E-Government ein", press release of June 07 2010, http://www.heise.de/newsticker/meldung/Oesterreich-fuehrt-Handy-Signatur-im-E-Government-ein-1016339.html

[32] ARGE-Daten - Österreichische Gesellschaft für Datenschutz (Austrian Society for Pricacy), "Was wurde aus der Bürgerkarte", press release of October 5 2006, http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=50759zjj

[33] ORF Futurezone, "E-Voting: Blackbox statt Wahlkabine", press release of May 17 2009, http://futurezone.orf.at/stories/1603378/

[34] S. Priglinger, "Auswirkungen der EU-DL Richtlinie auf die E-Gov-Welt", in Datenschutzrecht und E-Government, D. Jahnel, ed., Graz, 2008, pp. 267-283.

[35] eUser study, "Public online services and user orientation - country brief Austria", 2005, http://tinyurl.com/cj3hus

[36] Fessel GfK - Institut für Marktforschung Ges.m.b.H. (Institute for market research),"Online Studie 6 Monitoring E-Government", 2006, http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=21828

[37] C. N. M. Pounder, "Nine principles for assessing whether privacy is protected in a surveillance society", Identity in the information society (IDIS) vol. 1 (1), 2008, pp. 1-22.

Al URLs last visited on 30.06.2010