Identity Management Systems:
Gateway and Guardian for Virtual Residences

Marit Hansen[1], Peter Berlich[2]

EMTEL Conference: New Media, Technology and Everyday Life in Europe Conference
London, April 23rd - 26th, 2003

Abstract

Information and Communication Technologies (ICT) expand traditional ways of social interaction and thereby feed back on the society that created them. Users have to navigate their enhanced social context and in doing so legitimately strive to apply familiar concepts such as the notion of residence or the intuitive handling of roles.

We introduce the concepts of Virtual Residence and Identity Management Systems and elaborate on their interrelation: Firstly, Privacy-Enhancing Identity Management Systems can implement important features of the Virtual Residence. Secondly, the user may benefit from the residence metaphor being employed as an appropriate interface for Identity Management Systems.

We find that the proposed Virtual Residence serves to support the context awareness of users and Identity Management Systems, as well as to enforce certain context-based behaviour. Identity Management Systems, on the other hand, serve to implement rule-based behaviour and can form the underlying and required identity-managing infrastructure of a Virtual Residence.

An outlook completes the paper.

Keywords: *Virtual Residence, Identity Management, Privacy, Multilateral Security*

1. Introduction

Quantitative leaps in technology can result in a qualitative evolution. Latest since the industrial revolution, society has been challenged with coping with the side effects of technology, sometimes surpassing the designed and anticipated effects by orders of magnitude and resulting in unmanaged change. The rationalisation of manufacturing through automation beginning in the mid of the 18th century leading up to new social and political arrangements, can be seen as an example. The

[1] Marit Hansen, Independent Centre for Privacy Protection, Kiel, Germany, marit.hansen@t-online.de.
[2] Peter Berlich, Baden, Switzerland, peter@berlich.de.

"computer revolution" starting in the mid of the 20th century, started in an effort to further rationalise and mechanise human work, led to the generation of a global network of information in the late 20th century that is in principle available to every citizen of an industrialised country.

The consequences of the sudden introduction of "virtual personae", shadowing and emulating humans in all their various aspects and roles, are only now being understood let alone managed. Concepts of roles and identities need to be expanded and adapted in order to take into account the higher order effects introduced by the possibility of instantaneous communication and full transparency.

Individuals need to cope with the expanding concept of their own identity. We suppose that the majority of the population will do so by expanding their traditional concept of **managing** their **identity** and taking a trial and error approach. It is a challenge for economics, politics, law and science and it is a task in the self-interest of businesses and nations to support them.

The concept of Virtual Residence [Beslay/Punie 2002] has entered the discourse of identity. Building on the established concepts of Privacy-Enhancing Identity Management Systems (beginning with [Chaum 1985]), this text is aimed at exploring and refining the model of Virtual Residence from the angle of Identity Management, bridging the concepts and discussing them in the perspective of further streams in current research and their impact on society.

2. Critical discussion of terms and definitions

2.1 Identity Management

Identity and **roles** form the basis of human interaction. Not taking into account physical aspects for the purpose of this discussion, identity is traditionally defined as the conjunction of an internal instance ("I") and an external instance ("Me"), both of which are determined and generated out of their existence within and interaction with a physical and social, external world [IMS Study 2003]. A role is a representation of an individual's identity within a given social context, responding to formal and informal expectations. Identity is constituent of a manifold of partial identities [Clauß/Köhntopp 2001]. These partial identities are themselves instantiations of roles.

Identity Management (and analogously role management) is the natural human behaviour of generating, managing and choosing roles according to a found social context. These roles are often mandated by socio-cultural norms and possibly refined by each individual ("role making"). In each context people spontaneously choose an appropriate role ("role taking"), exhibiting a natural capability of resolving any apparent role conflicts in their behaviour. They have a gradually learned, intuitive understanding of what information to divulge and how to react to information received, depending on their communication partner, situation and their own as well as their partners' role within a presupposed socio-cultural reference frame.

Identity Management Systems (IMS) support the user in handling his or her (digital) identities and roles in the on-line world. IMS offer certain functionality, e.g., creation and management of pseudonyms, authentication (e.g. single sign-on), authenticity (e.g. digital signatures), reachability (defining who may contact oneself, possibly assigning them higher or lower priorities [Damker/Pordesch/Reichenbach 1999]) or release of data in line with the user's preferences in the act of role-taking. In the context of this discussion, IMS shall only denote systems under which the user partakes in the control over his or her digital identity.[3]

[3] The term IMS has also been used for systems, which process the user's data profiles on behalf of a third party, and commonly in a central repository, such as a database. The subtle difference here is one of generating vs. aggregating an external representation of the user's identity or "self". In order to enable more than trivial applications, such IMS should provide the possibility to use more than only one digital identity.

Privacy-Enhancing Identity Management Systems (PE-IMS) are designed to (re-)establish users' control over their digital identity: They support users' awareness of the current context with regard to their privacy, enabling an informed choice whether and when to divulge which information and facilitating an appropriate degree of anonymity. They employ a presupposed individual right to informational self-determination, under which everybody has the right to know who knows what about himself or herself.[4] First concepts were introduced by David Chaum in 1985 [Chaum 1985], but so far have not been implemented in practice.[5]

2.2 Virtual Residence

The concept of **Virtual Residence** [Beslay/Punie 2002] is an approach towards translating and extending the intuitive and commonly accepted concept of boundaries between private and public spaces, e.g., legal rules, socio-cultural norms and habits and people's awareness, from the off-line world into the on-line world. In doing so, this concept tries to overcome the principal difficulties of dealing with an automated aspect of identity by focusing on the boundaries of identity rather than its assumed core properties, abandoning the question of constituency ("How is this individual *different* from the rest of the world?") in favour of perimeter ("How is this individual *separate* from the rest of the world?").

In addressing concerns over security and privacy, the Virtual Residence is seen as an equivalent to "domicile" or "residence" in the off-line world. Thereby it should foster trust and confidence among users: "For people to feel at home in an online private space, it needs to be able to represent their multiple identities, respect their privacy and establish an acceptable level of security." [Beslay/Punie 2002] Especially in the context of new ICT applications such as ambient intelligence[6], the question arises how those technologies shall be "domesticated". Beslay and Punie in their proposed approach postulate the applicability of canonically generalised social codes and values in the on-line world. They point out the necessity of developing a set of rules by means of extrapolation from the off-line world.

While intuitively, the concept of Virtual Residence is easily appealing, its actual definition oscillates between the "virtual" as a representation of the "real" (physical and probably as well personal) and a virtual space in its own right. Similarly, the term "residence" could comprise not only a pure storing place and point of contact, but also a digital hide where one can (presumably safely) store and manipulate digital assets including, but not limited to constituents of one's own identity.[7]

An ad-hoc concept of identity in analogy to identity in the off-line world, then, may be too narrow for a successful translation of terms. If we consider the sum of all digital assets as what makes up the digital identity, then the Virtual Residence may be considered a representation of digital identity rather than

[4] The right to information privacy is a fundamental human right. In the European Context an important baseline is the "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data". In its Considerations, paragraph 2, is stated: "[...] data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals".

[5] The reason for this lack of implementation may lie in technical shortcomings, such as an error-prone level of complexity and a general lack of technical transparency and the possibility of security gaps. However, there may also be more fundamental reasons, such as a mechanical system's general inability to **recognise** their environment instead of just taking a necessarily incomplete **inventory** of it and the resulting dependence on the user's judgement, which renders key conceptual benefits, such as automated recognition of social context, unachievable as a matter of principle.

[6] Ambient Intelligence builds on three recent key technologies: Ubiquitous Computing, Ubiquitous Communication and Intelligent User Interfaces. It emphasises on greater user-friendliness, more efficient services support, user-empowerment, and support for human interactions. (ISTAG. Scenarios for Ambient Intelligence in 2010. Final Report, Feb 2001, EC 2001; available at: http://www.cordis.lu/ist/istag.htm.)

[7] As also predicted by David Siegel [Siegel 1999], who envisions for each person a "Universal Personal (Web) Site", which holds the owner's every digital asset and is "a complete filing and tracking system that helps him manage everything in his life", in other words an inventory of also the owner's non-digital assets, wants and needs.

vice versa. The Virtual Residence point of view may result in a more practice oriented handling of identity, making its key interfaces more accessible. However it remains to be shown whether by resorting to a phenomenological concept, we can reduce the fundamental challenge of managing identity per se.

Within the concept of Virtual Residence, the thrust of a definition of identity shifts towards the definition of boundaries. These boundaries will share some key properties:

- They need to be flexible and osmotic, controlling the flow of information and empowering the user to establish tight, higher-order borders along these boundaries.
- They can be vertical (separating aspects of identity, e.g., publicly visible aspects from hidden aspects or desired personality facets from repressed ones) or horizontal (separating different partial identities or individuals).
- They should be able to represent (i.e. map) all boundaries socially relevant in the off-line world, physical (spatial) ones as well as those intrinsic to a determined social system.

From this short list, one can already deduce some of the key challenges the concept of Virtual Residence is faced with, namely its dependence on social conventions and a consequential lack of universality for any given implementation. This is not surprising given individual boundaries depend on the respective social context.

On the other hand, a natural advantage of the Virtual Residence concept lies in the fact that it can be canonically extended to represent social groups instead of individuals.[8]

3. Relation Virtual Residence vs. Identity Management Systems

In the following, we shall focus on two different views of the relation between Virtual Residences and Identity Management Systems: Firstly we shall explain how IMS can be used to implement core concepts of the Virtual Residence, secondly we shall examine how the Virtual Residence idea might function as a mental model and interface for IMS. Related research streams are pointed out.

3.1 Identity Management Systems for Virtual Residences

The concept of Virtual Residences emulates people's desire for private space[9] not only in the off-line, but equivalently in the on-line world. Adapting the notion of such an on-line private residence means generalising the concept of boundaries and enabling its technical implementation. Traditional residences possess and consist of various kinds of boundaries, especially real, physical boundaries, giving a feeling of protection, and virtual, mental boundaries, dividing private and (more) public spaces.

Virtual “identity boundaries” limit access to personal information, constituting the observed (or at least observable) identity. These identity domains form the subject's partial identities from various observers’ perspectives. (Re-)Moving identity boundaries is a natural and everyday act in many transactions. It does however imply irreversibly aggregating information so that entropy and correspondingly the observers' overall knowledge of the subject increase and the subject’s control over this information decreases. Information, once disclosed, cannot be reclaimed.[10]

In deciding which information to reveal in which context, people are already applying an intuitive

[8] This gives rise to a representation of virtual personae not emanating from identifiable individuals, but from communities, legal entities, etc.
[9] Perhaps also territory.
[10] This aspect of the probabilistic nature of information is a fundamental issue with all so-called Information Rights Management systems.

understanding of identity boundaries and identity domains in the off-line world. In the on-line world the notion of context is far more complex because of reduced or unavailable authenticity, anonymity and transparency. In contrast to the off-line world, building informative user profiles simultaneously for a huge number of people is possible with a much lower effort due to massive data trails, proliferated automation, digital format and mostly weak security.

According to the principle of multilateral security [Rannenberg/Pfitzmann/Müller 1996; 1999], only minimal trust in other parties should be required, whereby control over privacy should be kept in the user's private space. Therefore, it is not sufficient to control the amount of personal data being disclosed, but they should be unlinkable so that unauthorised parties cannot profile or even identify users by collecting and aggregating data trails with a reasonable effort[11]. PE-IMS enable this by use of different pseudonyms for different situations and user-controlled re-use of pseudonyms, e.g., for the purpose of building a reputation. This concept of user-controlled linkage[12] or linkability[13] is typically implemented by cryptographic means, such as convertible credentials.[14]

The manifold domains of personal information emanating out of IMS constitute the representation of the Virtual Residence. PE-IMS support users in asserting their privacy rights and empower them to assume their self-responsibility:

- PE-IMS are gateways for all forms of digital communication between the private and public space, controlling the flow of information between the user and the communication partners concerning disclosure of personal data. Conversely, if a PE-IMS can be circumvented[15], the result will be a reduced degree of actual Identity Management [Köhntopp/Pfitzmann 2001]. In order to mitigate this risk, PE-IMS can either implement a rather coarse notion of the various identities, one that is unlikely to be at odds with off-line user practice, or be made aware of any interaction, even those it cannot control.[16]

- PE-IMS can serve as guardians for and between the user's different identity domains. Their main objective is user-controlled linkage and linkability of personal data [IMS Study 2003]. The core building block of IMS is the use of different kinds of pseudonyms. As laid out elsewhere [Pfitzmann/Köhntopp 2001; 2003], important classes of pseudonyms depend both on the role, which the user is acting in, and on the communication partner. The user should be aware what re-use of pseudonyms, i.e. linkability from an observer's perspective, would mean to his or her informational self-determination. PE-IMS support the user by methods for context detection and logging transaction data which are relevant for Identity Management so that he or she can estimate the knowledge of the communication partner about the user's personal information from prior transactions and act accordingly. Considering this information the user may decide not to re-use specific pseudonyms, but to generate new ones.

  The possibility of transferring attributes from one pseudonym to another can be provided by so-called convertible credentials [Chaum 1985]. A user could pseudonymously obtain such a

[11] I.e. within assumed limitations on time and effort. All security is, of course, subject to economical feasibility on the side of the attacker as well as the defender.

[12] Linkage sees the linking of information from the user's perspective, whereby the user is enabled to choose the degree of linkage of different transactions, pseudonyms, properties, or other information [Hansen/Rost 2003].

[13] Linkability means looking from an observer's or attacker's perspective which might e.g. observe all digital communication links, but does not have the power to break strong cryptography [Pfitzmann/Köhntopp 2001; 2003; Hansen/Rost 2003].

[14] It should be noted that prevention of linkability could conflict with requirements for managing information across social spheres, e.g. legal requirements. Even PE-IMS should provide mechanisms for fine-grained tailoring of linkability according to the socio-cultural consensus, especially to legally codified rules.

[15] Typically, circumvention can easily happen by utilisation of out-of-band channels such as verbal conversation.

[16] The former and not the latter approach appears to be the more practical one. However, even in a context of ambient intelligence, technology should be designed in a way to co-operate with IMS rather than providing seamless, but from a privacy point of view unmanageable integration of services.

credential from a dedicated organisation. When asserting the possession of a credential to any communication partner, the first pseudonym needn't be revealed. In order to achieve this, a credential can be converted into a credential for the currently used pseudonym. Therefore the use of different credentials is as unlinkable as can be (depending on the granularity of the kinds of credentials and their distribution throughout the users).

Not all functionality can be implemented by client-side IMS technology [Köhntopp/Pfitzmann 2001]. The communication partner may have to support certain processes, e.g., by allowing anonymous or pseudonymous use of services and defining the requirements for specific properties of pseudonyms, if desired. A Public Key Infrastructure (PKI) supports use of digital pseudonyms, which can authenticate the pseudonym holder. Third parties may also be integrated as trustees, e.g., being an Identity Broker with the ability to reveal the identity of a pseudonym holder in order to provide means for investigation or prosecution, or acting as a Liability Broker of the pseudonym holder to clear a debt or settle a claim [Pfitzmann/Köhntopp 2001; 2003].

An IMS can only be a reliable guardian for the user's different identity domains if specific privacy and security requirements are met. The IMS itself, managing a large amount of sensitive personal data, has to be trustworthy. The communication network has to be trustworthy as well, in the particular sense that it must not enable tracking a user and aggregating his or her different identities, which means to implement anonymity against observers. Technologies capable of fulfilling these privacy and security requirements exist, but are not state-of-the-art [IMS Study 2003]. There is a natural risk of IMS proliferating and gaining critical mass which are driven by special interests that might be contrary to the established criteria of Privacy-Enhancing Technologies[17]. Whereas PE-IMS can act as a guardian for the user's Virtual Residence, current IMS are deficient in protecting the user's privacy and establishing an acceptable level of security [IMS Study 2003].

The spaces and spheres within a Virtual Residence have a natural limit in complexity through the spaces and concepts they emulate as a user interface. Potentially they may therefore be insufficient to represent the complex mapping of all identity aspects performed in "conventional" IMS. Thus, either the identity structure of a user needs be or will be simplified by himself or herself or a more complex mapping needs to be created transcending the means of a pure representation of familiar physical spaces.

It is desirable that the user has full control over which implicit social information are being related within the set-up of the Virtual Residence, as can be derived from the European Convention of Human Rights and Fundamental Freedoms. This capability appears to be a key benefit but also one of the most difficult to achieve, as the user – other than in the "real" residence or world – has a very limited or even no way of obtaining feedback about the reception of the social signals he or she is sending. IMS could facilitate this kind of feedback (preferably in a standardised, or at the very least in human-readable form) or – failing that – allow for providing for a standard set (or several such sets, representing different cultures) of social codes.

Not all boundaries of the Virtual Residence may be known from the start, as that requires knowledge of and control over even indirect interfaces. The dimensions of a Virtual Residence will evolve from a diffuse set of boundaries towards a better-defined perimeter. The simplifications and explications inevitable for use in digital worlds simultaneously represent shortcomings that the complex set of social interactions it tries to accommodate and emulate may not easily allow for.[18]

[17] E.g. they don't empower the user to control effectively the flow of his or her personal data.

[18] Cf. the learning curve newbie users in newsgroups have to go through in order to learn the limitations put on e.g. the use of irony.

3.2 Virtual Residence for Identity Management Systems

Leveraging its postulated rule setting properties, Virtual Residence can serve as an interface metaphor in order to hide the inner workings of an IMS while providing a usable mechanism for managing its functionality, in much the same way a desktop serves a metaphor for the inner structure and workings of a computer system. In order to represent the abstract properties of a Virtual Residence, spatial boundaries may be shown to the user, e.g., by mimicking real residences. As with IMS, not only "look & feel" has to match the user's expectations and capabilities, but the detection of context is paramount in order to support the user in choosing his or her partial identity, i.e. creating or re-using a pseudonym and properties and applying the correct set of rules deciding on the conditions for disclosure of personal data or reachability. This role triggering is highly context-dependent. If desired, role taking can be automated or governed by default assumptions. In ambiguous situations, the set of partial identities the user can choose from can be narrowed down or at least ordered by presumed suitability.[19]

3.2.1 Spatial representations of Virtual Residence

Multimedial representations of a residence in an IMS enable the user to choose a location, which denotes the current context or role. Two mental models basing on spatial boundaries between different domains are a "Virtual Apartment" and a "Virtual City".[20]

Interface "Virtual Apartment"

To start with, a virtual apartment will have a door, which controls access from the outside world. A virtual visitor, establishing a communication with the user, may first have to ring; the state of the door may show how far he or she is allowed to come in, i.e. the door may be open or closed (or "half open", e.g., opening only the upper half of it so that a visitor can be talked to, but is not invited to enter the apartment).

A generic virtual apartment may comprise typical rooms such as a living room, a working room, a sleeping room, a kitchen, a bathroom and one or more hobby rooms. The visitor could be "taken into a specific room" which would define the situation; e.g., the boss or a colleague could be invited into the working room, automatically establishing the working context by opening the right files, putting other data into the background.

But even without a visitor, the user may decide on the room, which he or she is currently "in", i.e., which describes best the current context. This may be relevant for following transactions where the user wants to be addressed in a certain role. Additionally it may not only provide a role-specific personalisation of services, but also may determine reachability preferences. E.g., in a working (room) context, the boss or colleagues will have the benefit of the right of priority, or in a sleeping room the user shall not be disturbed except in the case of emergency.

[19] Considering the classification of pseudonyms according [Pfitzmann/Köhntopp 2001; 2003], there is a difference between relationship pseudonyms and role pseudonyms which has to be taken into account when designing a user interface: The communication partner normally can be exactly specified (by choosing a name from an address book or interpreting the communication address), whereas the role a person is acting in often is somewhat fuzzy. In many cases the context is approximately clear, e.g. differentiating between a private and a professional role, which could be easily chosen by a user. But within those role contexts there regularly exist sub-roles, e.g. in professional life whether one is member in a collaborating team, a staff leader, a subordinate to another person, whether one acts within one's office, deals with single customers or is representing the office in public. Thus, it will be natural to build hierarchies of roles to help the user in refining chosen basic roles.

[20] Note that representations of these models could be implemented as user interface of Identity Management Systems. Even with mainly text-oriented digital communication it is not necessary to stick to command- or menu-based user interfaces. What may seem to be at least unusual for standard user interfaces, is already state-of-the-art in interactive computer games. To offer similar user interfaces may only be a matter of time. Even if there is not real 3D support as in Virtual Reality demonstrations, a stripped version showing 2D maps and clicking icons instead of wandering through an animated 3D world may enhance former concepts of user interfaces.

The user may design his or her own virtual apartment according to personal preferences. The choice of room and possibly configuration of doors, windows and blinds as well may define not only the context, but also may determine the relationship to communication partners.

It is an interesting question whether a visitor sees in his or her IMS the same virtual apartment as the visited person: As with current web pages, there may be a preferred representation designed by the resident of a virtual apartment. This default representation can be modified according to the communication partner's preferences for his personal viewing or be replaced by a neutral default configuration. The personal representation of the resident may also be intentionally withheld in the interest of his or her privacy. Adequate representation will be relevant in a trans-cultural context where the selection of apartment rooms and the context they represent may differ.

Interface "Virtual City"

A great deal of life is not restricted to one's own apartment, but happens outside. In our understanding, IMS will be less relevant for personal relations than in a communication between users and organisations respectively their representatives. These organisations are not located within the apartment, but have their own buildings (and residences) in a city. Therefore it makes sense to expand the metaphor of a virtual apartment to a virtual city, which could be visualised by a map or by a 3D animation. It may even be a city simulation analogous to "SimCity"[21].

Whereas the apartment paradigm focuses more on roles of the user and less on communication partners unless they are visitors, the virtual city offers choice of communication partners and, derived from that context, selection of an appropriate role.

The generic virtual city may consist of various buildings or places denoting situations and communication partners, e.g. representing:

- Governmental authorities (such as town hall, tax authority, real estate register);
- Stores;
- Workplaces (such as offices);
- Schools;
- Doctors;
- Pharmacies;
- Insurance companies;
- Lawyers or notaries;
- Counselling groups;
- Privacy commissioners for getting support on privacy questions including the IMS;
- Leisure areas (such as sporting areas, parks, cinemas, gambling points);
- Friends' homes.

In analogy to the virtual apartment, default reachability requirements can be linked to specific locations. User may build their own "personalised" virtual cities. Representation forms configured by the organisations themselves and designed according to their Corporate Identity may determine the display of virtual organisational buildings. Even travelling between virtual cities could be supported. When visiting other people, the context may also include specific socio-cultural or legal requirements but also

[21] http://simcity.ea.com/.

helping in language support, time zones etc.

3.2.2 Context Detection

Along with the residence representation, from which the context and role the user is acting in could be derived, other criteria may be relevant or could support the determination of context: The user can explicitly choose the context, sensor output can be evaluated, or meta information can be used to characterise the context. In addition to spatial representation, in particular the communication partner influences the context and thereby the user's role.

User-determined context

For establishing a connection, the communication partner could be explicitly chosen from an address book on the user's side or his or her network address could be typed in. Of course potential communication partners can be represented arbitrarily textually or by icons, photos, avatars or stick figures. This representation may be equipped with further attributes, such as a uniform, in order to explicate its function and thereby supporting the determination of context. The user himself or herself could be present in this virtual world by his or her own virtual persona.

Context detection by sensors

A possibility with some parallels to the virtual apartment or virtual city is context detection by interpreting the output of sensors which may even be placed ubiquitously, e.g., a smart home with sensors almost all over the place where a user may act in. Those sensors could also suit for biometric interpretation of the user himself or herself, e.g., the context may be derived according to speech (speech recognition, language, tone) or posture. The sensors may also evaluate the environment such as other people being near, analysing e.g. their biometrics or other information sent out from them or their IMS about themselves or the context.

Context description by meta information

The development of a "Virtual Residence User Interface" and the distribution of capable and instructive sensors as well as the interpretation of their information require a substantial investment. This effort can be alleviated by definition of an "Identity Management Protocol Set" [Hansen/Rost 2003], which describes the context in form of meta tags in a specific (presumably XML-based) language. Such an Identity Management Protocol Set should describe

- Basic requirements for Identity Management
  including the required configuration of privacy and security mechanisms and the possible integration of third parties for specific services;
- Degree and type of linkability
  including the tagging of transaction beginnings and endings; the requirements and degrees of freedom concerning the choice of the pseudonym's type, its re-use and attributes; tasks of possibly integrated third parties, e.g., in assigning the pseudonym; policies and preferences with respect to processing of the user's personal data;
- Information about role triggering,
  i.e. addressing one or a few possible roles and the related communication schemes the user might choose from;
- Possible integration of privacy information
  which help the user in estimating the level of privacy and which may be provided by third parties such as privacy commissioners or peers.

The set of metaphors used within the Virtual Residence (rooms within a house, houses within a city,

etc.) need to be practically universally standardised or at least understandable. Possibly, the concept of spheres and rooms is too coarse and is better represented by variable parameters (e.g., trust, social proximity, wealth, social status, rank, etc.), not all of which need to be disclosed to the discussion partner. This model may however be too complex and unnecessary for standardised social situations (e.g., trade, friendship, love). These standardised situations to a very large extent determine the user's expectations and actions[22] and even his or her legal rights.[23]

The Virtual Residence has the potential to substitute certain parameters of social interaction with regards to the social interpretation of interaction (e.g., whether a one-to-one communication is public or private). Additionally a set of non-pre-structured or spontaneous social scenarios or settings (cf. certain chat rooms) could complement the Virtual Residence.

3.3 Related research streams

It is instructive to note that various research streams work on topics valuable for providing usable Privacy-Enhancing IMS, especially context detection. As it is beyond the scope of this paper to expand on the current work in other fields, we will only give references:

- Context-dependent personalisation is being analysed in several projects: The objective of "VHE: Virtual Home Environment"[24] is to "enable the user to access a variety of services in UMTS [...] networks that are tailored to his individual needs. Additionally, services should be dynamically adjusted to the user's location to provide location-based information".
- "I-centric communications" are an "approach to design communication systems that adapt themselves to the individual communication space and individual environment and situation. In this context 'I' means I, or individual, 'Centric' means adaptable to I requirements and a certain user environment" [Arbanowski/van der Meer/Popescu-Zeletin 2000].
- This concept is enhanced towards "Ambient Awareness", meaning functionality provided by an I-centric system to sense and exchange the situation in which the individual is in at a certain moment in time [van Kranenburg et al. 2002].
- Already since 1997 research groups working on wearable and ubiquitous computing proposed methods for context awareness relying on sensors (e.g. [Abowd et al. 1997; Abowd et al. 1999; Brown et al. 2000; Gellersen/Schmidt/Beigl 2002; Michahelles/Samulowitz 2002], thus representing a different kind of context than the described social context relevant for choosing partial identities. It is noticeable that information on location alone is not regarded as sufficient for describing this kind of context [Schmidt/Beigl/Gellersen 1999]. One important outcome of the research in this field is the context toolkit [Salber/Dey/Abowd 1999].
- The objective of the European Project TEA – Technology for Enabling Awareness, conducted in 1999 and 2000, was to "develop an awareness-enabling add-on component for mainstream mobile computing and communication devices, such as PDAs, laptops, and mobile phones". Context awareness is characterised as follows: "The notion of context awareness for devices itself can be split up into three components: activity, environment and self. The activity describes the task the user is performing at the moment, or more generally what his or her behaviour is. This aspect of context is focused on the user of the device, and his or her habits. The environment describes what the status is of the physical and social surroundings of the user. The current location, the activities in the environment and other extern properties like for

[22] Cf. Eliza experiment [Weizenbaum 1966].
[23] Could the user expect communication to be kept in confidence or was it clear that a communication was public – in other words, can he or she assert a right to privacy with respect to the event and the content of the communication?
[24] http://www.isst.fhg.de/english/projekte/2002/VHE.html.

instance temperature or humidity belong to this axis. Finally, the self-component contains the status of the device itself. This third point of view on context awareness has not been researched as much as the other two, but is a very interesting one in the scope of cognitive sciences." [TEA 2000]

- In research on usability "Attentive User Interfaces" are proposed which are sensitive to the user's attention [Vertegaal 2003]. As the focus of attention may be relevant to the context, it would be interesting to combine those interfaces with IMS, especially when it comes to ubiquitous computing. Another approach is taken in the project "Virtual Human" which develops avatars as personal interaction agents for users.[25]

4. Conclusion and outlook

Virtual Residence and Identity Management build on common core concepts: Firstly, Privacy-Enhancing Identity Management Systems are needed to implement important parts of Virtual Residence by managing multiple identities while guaranteeing a high level of privacy and security. Secondly, the traditional paradigm of Virtual Residence could function as an approach to interface design of Identity Management Systems, which supports the users' understanding about their current role and the specific context they are in. Thus, it could help the users in choosing the appropriate partial identity and privacy configuration.

However, it has yet to be proven that PE-IMS will be able to sustain critical mass in the market. Experience of the last few years has given little indication that Privacy-Enhancing Technologies (PET) were to emerge spontaneously in the free market. Although there are some initiatives to foster PET[26], society may not be able to leverage its potential in order to implement PE-IMS.[27] Current state-of-the-art of IMS do not meet commonly accepted privacy and security requirements for PE-IMS.

The terms IMS and Virtual Residence should not be treated as disjunctive representations of structure but seen as complementary representations.[28] They are probably only hierarchical in the sense that Virtual Residence presents the user with an interface for IMS and a front-end for other services such as access to personal or shared information and access to certain, personalised or personal applications such as an e-mail client.

New technologies such as Identity Management Systems will have to keep in touch with familiar concepts such as the residence paradigm to be accepted by users. On the other hand such new ICT offer possibilities, which go beyond traditional concepts, e.g. the convertible credentials which do not have an equivalent in the off-line world.

People will have to actively manage their privacy in role making and role taking. This requires aware and informed users, capable and empowered to make informed decisions, meaning that both technologies exist which enable choices and users are educated to handle them appropriately. Society will have to face the challenge how privacy can be maintained effectively and in a user-friendly way while taking into account diverse legal requirements and social interests. IMS will be people's privacy guardian.

[25] http://www.virtual-human.org/.
[26] E.g. by direct funding or privacy seal programmes
[27] E.g. by accepting that all personal user data is processed by providers of IMS which may comprise of commercial enterprises with a key market position.
[28] Such as folders and directory structure both representing a virtual hierarchy.

5. References

[Abowd et al. 1997]
Gregory D. Abowd, Anind K. Dey, Robert Orr, Jason Brotherton: Context-Awareness in Wearable and Ubiquitous Computing; Technical Report, GIT-GVU97-11, Graphics, Visualization, and Usability Center, College of Computing, Georgia Institute of Technology; Poster in the Proceedings of the 1st International Symposium on Wearable Computing (ISWC '97), October 13-14, 1997; 179-180; http://www.cc.gatech.edu/fce/pubs/iswc97/wear-poster.html.

[Abowd et al. 1999]
Gregory D. Abowd, Anind K. Dey, Peter J. Brown, Nigel Davies. Mark Smith, Pete Steggles: Towards a better understanding of context and context-awareness (panel statements); in: H.-W. Gellersen (Ed.): Proc. of the First International Symposium on Handheld and Ubiquitous Computing; HUC'99, Karlsruhe, Germany, 27-29 Sept., 1999; Springer, Berlin 1999; 304-307.

[Arbanowski/van der Meer/Popescu-Zeletin 2000]
Stefan Arbanowski, Sven van der Meer, Radu Popescu-Zeletin: I-centric Services in the Area of Telecommunication – 'The I-Talk Service'; Proc. of the 6th IFIP TC6/WG6.7 Conference on Intelligence in Networks; SmartNet 2000; Vienna, Austria, September 18-22, 2000; 499-508.

[Berlich 2001]
Peter Berlich: Das Internet als innerer Ort – "Das Digitale Kloster"; Proceedings Symposium "Digitaler Diskurs"; Migros-Kulturprozent; ARC Romainmôtier 21.1.1999 – 24.1.1999; in: B. Suter, M. Böhler (Eds.): Hyperfiction; Stroemfeld Basel/Frankfurt a. M. 1999; http://update.ch/beluga/digital/99/berlich/digikloster.html.

[Beslay/Punie 2002]
Laurent Beslay, Yves Punie: The Virtual Residence: Identity, Privacy and Security in: The IPTS Report 67 (September 2002); JRC Seville, 2002; 17-23; http://www.jrc.es/pages/iptsreport/vol67/english/IPT3E676.html.

[Brown et al. 2000]
Peter Brown, Winslow Burleson, Mik Lamming, Odd-Wiking Rahlff, Guy Romano, Jean Scholtz, Dave Snowdon: "Context-Awareness: Some Compelling Applications"; Proceedings of the CHI2000 Workshop "The What, Who, Where, When, Why and How of Context-Awareness"; ACM Conference on Human Factors in Computing Systems, CHI2000; The Hague, Netherlands, April 1-6, 2000; http://www.dcs.ex.ac.uk/~pjbrown/papers/acm.html.

[Chaum 1985]
David Chaum: Security Without Identification: Transaction Systems to Make Big Brother Obsolete; in: Communications of the ACM, Vol. 28 No. 10, October 1985; 1030-1044.

[Clauß et al. 2002]
Sebastian Clauß, Andreas Pfitzmann, Marit Hansen, Els Van Herreweghen: Privacy-Enhancing Identity Management; in: The IPTS Report 67 (September 2002); JRC Seville, 2002; 8-16; http://www.jrc.es/pages/iptsreport/vol67/english/IPT2E676.html.

[Clauß/Köhntopp 2001]
Sebastian Clauß, Marit Köhntopp: Identity Management and Its Support of Multilateral Security; in: Computer Networks 37 (2001); Special Issue on Electronic Business Systems; Elsevier, North-Holland 2001; 205-219; http://www.elsevier.com/gej-ng/10/15/22/67/33/34/article.pdf.

[Damker/Pordesch/Reichenbach 1999]
Herbert Damker, Ulrich Pordesch, Martin Reichenbach: Personal Reachability and Security Management – Negotiation of Multilateral Security; in: Günter Müller, Kai Rannenberg (Eds.): Multilateral Security in Communications. Vol. 3, Addison-Wesley, München 1999; 95-111.

[Gellersen/Schmidt/Beigl 2002]
Hans-W. Gellersen, Albrecht Schmidt, Michael Beigl: Multi-Sensor Context-Awareness in Mobile Devices and Smart Artefacts; in: Journal on Mobile Networks and Applications; Special Issue on Mobility of Systems, Users, Data and Computing in Mobile Networks and Applications (MONET); 7(5), Imrich Chlamtac (Ed.); Oct. 2002; 341-351; Draft: http://www.comp.lancs.ac.uk/~hwg/publ/monet.pdf.

[Hansen/Rost 2003]
Marit Hansen, Martin Rost: Nutzerkontrollierte Verkettung – Pseudonyme, Credentials, Protokolle für Identitätsmanagement; in: Datenschutz und Datensicherheit (DuD) 27/5 (2003); Vieweg, Wiesbaden; 293-296.

[IMS Study 2003]
Identity Management Systems (IMS): Identification and Comparison Study; Study commissioned by the Institute for Prospective Technological Studies, JRC Seville; to be published in 2003.

[Köhntopp/Pfitzmann 2001]
Marit Köhntopp, Andreas Pfitzmann: Informationelle Selbstbestimmung durch Identitätsmanagement (Informational Self-Determination by Identity Management); in: it+ti Informationstechnik und Technische Informatik, Schwerpunktthema "IT-Sicherheit" 5/2001; Oldenbourg Wissenschaftsverlag, München, September 2001; 227-235.

[van Kranenburg et al. 2002]
Herma van Kranenburg (Ed.), Stefan Arbanowski, Erwin Postmann, Johan Hjelm, Johan de Heer, Fritz Hohl, Stefan Gessler, Heikki Ailistoo, Anthony Tarlano, Wolfgang Kellerer, Francois Carrez: Ambient Awareness in wireless information and communication services; White Paper Wireless World Research Forum Working Group 2, December 2002.

[Michahelles/Samulowitz 2002]
Florian Michahelles, Michael Samulowitz: Smart CAPs for Smart Its – Context Detection for Mobile Users; in: Personal and Ubiquitous Computing, Vol. 6, Issue 4 (2002), Springer, London, September 2002; 269-275.

[Pfitzmann/Köhntopp 2001; 2003]
Andreas Pfitzmann, Marit Köhntopp: Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology; Draft v0.14, 2003-05-27; v0.8 in: Hannes Federrath (Ed.): Designing Privacy Enhancing Technologies; Proc. Workshop on Design Issues in Anonymity and Unobservability; LNCS 2009; 2001; 1-9; v0.10 as Open Paper for Discussion on the Information Hiding Workshop 2001 Holiday Inn University Center, Pittsburgh, PA, April 25-27, 2001; http://www.koehntopp.de/marit/pub/anon/.

[Rannenberg/Pfitzmann/Müller 1996; 1999]
Kai Rannenberg, Andreas Pfitzmann, Günter Müller: Sicherheit, insbesondere mehrseitige Sicherheit; in: it+ti 4/1996, 7; revised as: IT Security and Multilateral Security; in: Günter Müller, Kai Rannenberg (Eds.): Multilateral Security in Communications; Vol. 3: Technology, Infrastructure, Economy; Addison-Wesley, München 1999; 21-29.

[Salber/Dey/Abowd 1999]
Daniel Salber, Anind K. Dey, Gregory D. Abowd: The context toolkit: aiding the development of context-enabled applications, Proc. of CHI'99, Pittsburgh, PA, ACM Press, 1999.

[Schmidt/Beigl/Gellersen 1999]
Albrecht Schmidt, Michael Beigl, Hans-W. Gellersen: There is more to Context than Location; in: Computers and Graphics (Proc. of the Intl. Workshop on Interactive Applications of Mobile Computing (IMC98), Rostock, Germany, November 1998); Vol. 23, No. 6, 1999; 893-901.

[Siegel 1999]
David Siegel: Futurize your Enterprise – Business Strategy in the Age of the E-Customer; John Wiley & Sons, Inc., New York 1999.

[TEA 2000]
Technology for Enabling Awareness (TEA) Project, 2000: http://www.teco.edu/tea/tea_pub.html.

[Vertegaal 2003]
Roel Vertegaal: Attentive User Interfaces; in: Communications of the ACM; March 2003/Vol. 35, No. 3; 31-33.

[Weizenbaum 1966]
Joseph Weizenbaum: "ELIZA – A Computer Program for the Study of Natural Language Communication between Man and Machine", Communications of the Association for Computing Machinery 9 (1966); 36-45.