Towards inclusive Identity Management

Fritsch, Lothar; Fuglerud, Kristin Skeide; Solheim, Ivar
Norsk Regnesentral - Norwegian Computing Center, Gaustadtalléen 23, 0314 Oslo
E-Mail: [Lothar.Fritsch|Kristin.Skeide.Fuglerud|Ivar.Solheim] @NR.no
Tel. +47 22852500 – Fax +47 22697660

Abstract
This article will discuss identity management and profiling with respect to e-inclusion. E-inclusion is an EU commission priority within the i2010 initiative, and in particular privacy challenges in e-inclusive ICT are clearly stated in several national e-inclusion policies in Finland, Norway, Portugal, Romania and Spain in (EC 2007). Inclusive information systems adapt to users' special needs based on a profile of the users' capabilities. Identity management faces new challenges related to profiling and identification in e-inclusion:

1. Usability & accessibility issues of identity management technology
2. New challenges for personal privacy and profiling

Our article will discuss these new aspects and present new research issues for both the identity management and the e-inclusion communities.
Key words: E-Inclusion, Identity Management, Information Security, Privacy, Authentication, Exclusion, Disabilities, Universal Design, Usability

Introduction to e-inclusive information systems

It is politically recognized that being able to take part in the modern information society is a central political goal (EC 1995-2007). Therefore integration of all users, often referred to as e-inclusion, has become an important policy area. Several initiatives support e-inclusion. Examples are the European i2010 initiative on e-Inclusion (EC 2005) and the Riga Ministerial Declaration where 34 European countries expressed their strong commitment to promote an inclusive and barrier-free Information Society (EC 2006). Also, the Unites Nations' Convention on the Rights of Persons with Disabilities promotes access for persons with disabilities to new information and communications technologies and systems, including the Internet. E-Inclusion is a wide term covering both that of making ICT itself inclusive, and the use of ICT to achieve wider inclusion objectives in relation to economical, educational, socio-economic, racial, age- and class-related issues. As digital divides along economic and educational lines narrows, new divides are becoming more apparent, especially accessibility related divides for people with disabilities (Zimmerman et al. 2001). In the following we will concentrate on design issues related to accessibility, usability and security of identity management technology.

Inclusive design approaches

The terms "Universal Design" (UD) and "Design for All" (DfA) denote approaches to make mainstream products and services accessible for as broad a range of users as possible, including older people and people with disabilities.
Ronald L. Mace is known for developing the concept of universal design within the field of architecture. He demonstrated that when making something more accessible to people with disabilities, it also gets more accessible to everyone. The Center for Universal Design (CUD 1997a) at North Carolina State University was founded by Ron. L. Mace and a group at this center developed seven principles universal design (CUD 1997b):

> PRINCIPLE ONE: Equitable Use: The design is useful and marketable to people with diverse abilities.
> PRINCIPLE TWO: Flexibility in Use: The design accommodates a wide range of individual preferences and abilities.

PRINCIPLE THREE: Simple and Intuitive Use: Use of the design is easy to understand, regardless of the user's experience, knowledge, language skills, or current concentration level.
PRINCIPLE FOUR: Perceptible Information: The design communicates necessary information effectively to the user, regardless of ambient conditions or the user's sensory abilities.
PRINCIPLE FIVE: Tolerance for Error: The design minimizes hazards and the adverse consequences of accidental or unintended actions.
PRINCIPLE SIX: Low Physical Effort: The design can be used efficiently and comfortably and with a minimum of fatigue.
PRINCIPLE SEVEN: Size and Space for Approach and Use: Appropriate size and space is provided for approach, reach, manipulation, and use regardless of user's body size, posture, or mobility.

These principles are rather generic, and are adopted within a wide range of design disciplines. The European Design for All e-Accessibility Network (EDeAN) was established in 2002, in accordance with one of the specific goals of the eEurope 2002 action plan (EDeAN 2006). The goal of the EDeAN is to support all citizens' access to the information society and raise the profile of Design for All (DfA). According to EDeAN there are three main issues that must be considered in order to make products and services accessible for as many types of users as possible. These are:

1. Design of information technology, products, services and applications, which are demonstrably suitable for most of the potential users without any modification.
2. Design of products, which are easily adaptable to different users (i.e. by incorporating adaptable or customizable user interfaces).
3. Design of products which have standardized interfaces, capable of being accessed by specialized user interaction devices. (Thus, the development of specific interaction devices or so called assistive technology is outside the scope of DfA or UD, but interoperability with assistive technology is an important issue.)

Several other design approaches that encompass the goal of including people into the information society have emerged within the ICT-communities since the mid-1980's, but the main idea of most inclusive design approaches is to make mainstream products and services accessible and usable by as many users as possible. Thus, inclusive design is not about a special design for small user groups or producing assistive technology, but rather about extending the potential user groups of mainstream products and services to include disabled, elderly people and people with low ICT skills, people with low reading and writing skills etc. This is reflected in the first principle of UD and the first issue listed in DfA.
Another point we would like to highlight is the recognition of user diversity in DfA and UD - in contrast to trying to find the average user, or a typical user. Knowledge and awareness of the very different needs, preferences and abilities of different kinds of users are central in the inclusive design approaches. Therefore, flexibility and adaptability are central issues in both UD and DfA, and the development of accessible, flexible and easy-to-use mainstream ICT products and services are central goals in the design of inclusive ICT systems. It is two properties of ICT that makes this issue especially interesting and promising when it comes to universal design in ICT compared with other design disciplines:

1. The potential of adaptation of digital information is great. Information can be presented in many different ways by use of different modalities, such as text, pictures, film, audio and tactile.
2. The possibilities to make products flexible and adaptable to the single special users needs by the use of profiles and personalization.

Hereby ID management, security and privacy step forward as especially important in universal design of ICT systems.

A third important issue of inclusive design is the importance of standards and guidelines so that people, who use various technologies, including assistive technology, can use ICT products and services. The next section discusses some relevant standards and guidelines.

Standards and guidelines

In many countries, such as, in the US, Australia, Japan and in the European Union legislative actions are put in place to require public bodies and companies to make sure that their products and services are accessible and usable by as many users as possible, including elderly people and people with disabilities. Therefore, there is an increasingly number of laws that are referring to, and requiring conformity to standards and guidelines related to DfA. Thus, many standardization initiatives are directly and indirectly stimulated by the European Commission and other national bodies (Engelen 2007). In addition, many stakeholder groups and NGO's are contributing to guidelines and standards within this field.
Since there are still relatively few official formal standards within this area, legislation in various countries do not always refer to official formal standards, but to guidelines in order to specify the details of the laws. One very well known example of this is the World Wide Web consortium and especially the Web Accessibility Initiative that has produced several guidelines on web accessibility. These guidelines are almost universally accepted as the primary reference point for web accessibility matters. However, some countries establishing legislative actions for imposing web accessibility will not refer to the WAI guidelines as the W3C cannot be considered a standardization body in the proper sense of the word (ibid.).
In Europe, there are mainly three official standardization groups CEN, CENELEC and ETSI. Their international counterparts are respectively ISO, IEC and ITU-T. Fortunately, there is some coordination of the work in the fields of Assistive Technology (AT) and Design for All (DfA). A concrete initiative was the European Commission Mandate 283 to promote the use of barrier-free design in the standardization process. This mandate stated that "it is essential that the principles of design for all, adaptive design and assistive technology are applied throughout the standardization process". The work was jointly carried out by a working group constituted by CEN/CENELEC and ISO/IEC (Engelen 2007). The working group had representatives of CEN and CENELEC, ETSI, ANEC and other consumers and manufacturers organizations. It was decided to transfer the ISO/IEC Guide 71 "Guidelines to address the needs of older persons and people with disabilities" into a European deliverable. This is how CEN/CENELEC Guide 6 came about. It is important to note that ISO/IEC Guide 71 and CEN/CENELEC Guide 6 are identical documents. Other coordination activities at European level are carried out through the ICT standards Board – ITCSB and The Design for All and Assistive Technology Standardization Co-ordination group – DATSCG. In the US several legislative actions have been undertaken, where the most important are the American with Disabilities Act (ADA) and the Federal Rehabilitation Act (Section 508). Outside observers, such as the European Union has been invited to participate in the 2007 revision of the Section 508 Guidelines.

Conformity

There exist several tools, both checklists and software, to evaluate whether an ICT product or service complies with different standards and guidelines. Pointers to additional resources such as checklists and conformity tools can often be found at the websites of the specific standards or guidelines. See for example the (W3C WAI) website and the (Section 508) website. The EIAO project, the European Internet Accessibility Project develops methodology and a demonstrator robot that can perform large scale accessibility evaluation of Internet sites. The accessibility evaluation methodology is based on the W3C WAI guidelines (EIAO 2005).

However, even if standards and guidelines are applied, several problems related to accessibility, usability and security may not be addressed. For example, there are reports of security software that may identify assistive devices such as screen readers as spyware, and thus block programs for blind and visually impaired people. (A screen reader is a software application that attempts to identify and interpret what is being displayed on the screen.) Another challenge is the widespread use of captcha's and how to eventually handle alternatives. (Captcha: Completely Automated Public Turing test to Tell Computers and Humans Apart)

Standards and accessible authentication

The CEN/CENELEC Guide 6 requires information presentation and representation in alternative formats. It states that by providing all input and all output, i.e. information and functions, in at least one alternative format, for instance visual and tactile, more people, including some with language/literacy problems, may be helped. The guide also briefly discusses alternatives to biological identification and operation:
"Where biometric forms of identification are intended, an alternative form of identification or activation should also be provided. For example, if systems require a retinal scan and a person does not have a retina, or the system requires a fingerprint and the person does not have hands or uses a prosthesis, such people are unable to operate the devices unless some alternative form of identification is substituted." (CEN/CENELEC 2002) .
A W3C note on Turing tests discusses both accessibility and security problems with so-called captcha's (May 2005). The most common use of this method is to make the user read a distorted set of characters from a bitmapped image, and enter those characters into a form. This visual verification presents huge barriers to users who are blind, visually impaired or dyslexic. Because of these accessibility barriers, the note advocates to seriously consider the use of other and alternative methods of limiting spam. Even though it mentions audio based captcha codes and other alternatives it rather hopes for better methods of identification by use of biometric technology in conjunction with single sign-on services. However, as is noted, Biometric systems will also have to take into account the fact that not all people have the same physical features (ibid.)

The need for inclusive identity management

Official figures from the USA say that about 48.9 million Americans, or 19.4 percent of the population (non-institutionalized), have a disability that interferes with common activities of daily living. The prevalence of some common types of impairments among working age adults (from 18 to 64 years) in the U.S are as follows (Stevenson et al. 2003):

- Approximately one in four (27%) have a visual difficulty or impairment.
- One in four (26%) have a dexterity difficulty or impairment.
- One in five (21%) have a hearing difficulty or impairment.
- One in five have a cognitive difficulty or impairment (20%) and
- About (4%) have a speech difficulty or impairment.

The study identified individuals who "self-identify" as having a disability or impairment as well as individuals who have difficulty with certain tasks but who do not identify themselves as having a disability or impairment. Their findings show that the majority, about 60%, of working-age adults in the U.S. are likely to benefit from the use of accessible technology (Stevenson et al. 2003). Accessible technology is technology that can be adapted or adjusted to meet individual visual, hearing, dexterity, cognitive, and speech needs (Stevenson et al. 2004). As in the U.S, the European population is ageing, and the average age of the computer users is rising. The prevalence of disabilities increases with age at a significant rate (Steg et al.

2006). This will only increase the need for accessible technology that makes it possible to do adaptations to compensate for physical or cognitive difficulties and impairments.
There is, to our knowledge, no statistics that shows to what extent different user groups have problems with using identity management and authentication mechanism. However, there are studies that suggest that such problems constitute a significant part of calls to helpdesk services. Gartner found that about 30 percent of the help desk calls were about password resets (Tari et al. 2006). Similarly, about one third of the help desk requests to an e-Government service (www.altinn.no) were related to how to log on to the service (Udjus 2007).

Are current technologies suitable for universal design of secure, e-inclusive systems?

A closer analysis of identity management systems (IMS) with respect to e-inclusion reveals a number of open issues. The discussion of these will be along the type classification in (Fidis 2005a) where identity management systems are grouped into:

Type 1: IMS for account management, implementing authentication, authorization, and accounting,

Type 2: IMS for profiling of user data by an organization, e.g. detailed log files or data warehouses which support e.g., personalized services or the analysis of customer behavior,

Type 3: IMS for user-controlled context-dependent role and pseudonym management

The following three sections will analyze authentication, profiling and role/identity management with the e-inclusion perspective.

Authentication versus e-inclusion

This section illustrates some of the challenges of e-inclusive authentication. The problems and issues herein relate to type-1 IDM systems. A taxonomy of such systems is shown in Figure 1. In order to be able to use a large number of public and private services the user must be authenticated. A very basic requirement for e-inclusion is therefore that the authentication methods can be used by as broad a range of users as possible. Common authentication methods include passwords and PINs, tokens and smart cards, and use of 3rd-party channels such as one-time codes from tokens or code generators. These methods can be difficult or impossible to use for special needs users.

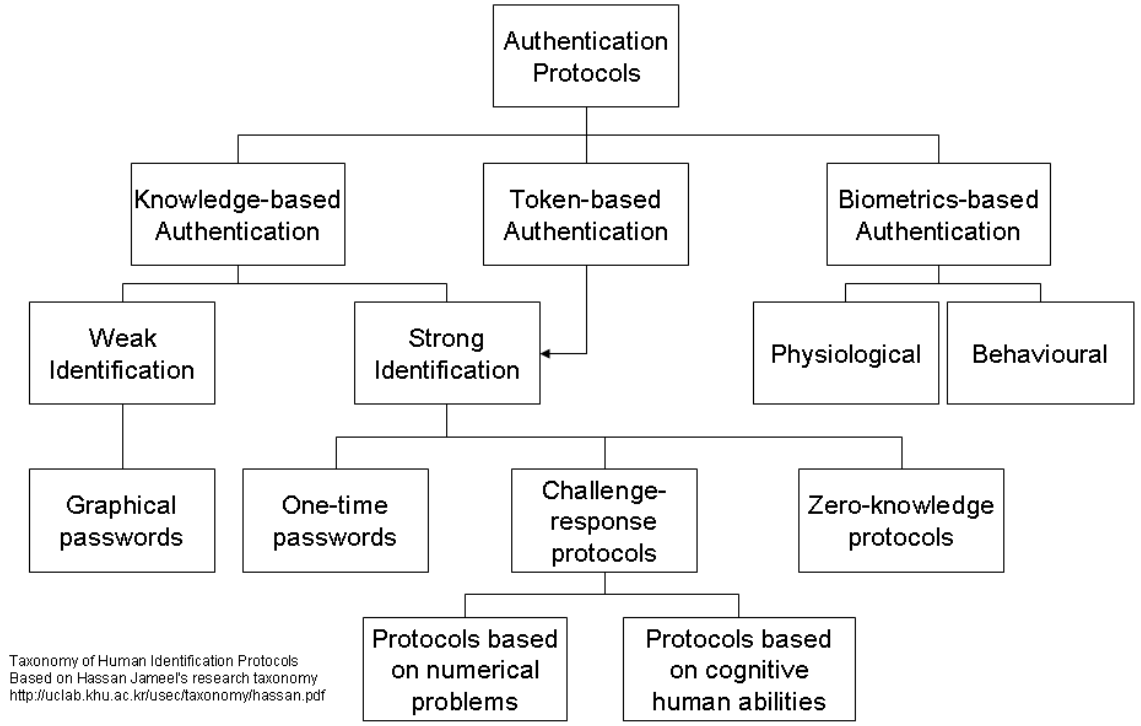

Figure 1: Jameel's taxonomy of identification methods (Jameel 2007).

The article discusses problems with authentication methods and presents examples of alternative authentication technology and requirements for these. For example, PIN-codes are typically not well suited for users with reduced memory or people that have problems with handling numbers (dyscalculia). Similarly, it turns out that logon procedures that requires passwords may lead to major problems for people with a low level of literacy or dyslexia. Another common method is visual verification of a bitmapped image (a “captcha” code, see (Ahn et al. 2004; Jameel et al. 2007; May 2005). This is a major problem for users who are visually impaired, or have a learning disability. For the various authentication methods, it is necessary to consider usability and accessibility issues. Biometrics could be a solution to many of these problems, but again, there is no single biometric method that can accommodate all users. A blind or visually impaired person may not be able to utilize visual cues necessary to perform an iris scan. An amputee may be precluded from fingerprint identification etc. Therefore, in most cases, alternative methods should be made available.

According to Jameel's taxonomy (Jameel et al. 2007), authentication methods can be divided in three categories:

1. **Knowledge-based authentication**: Systems based on the knowledge of a secret, e.g. passwords or PIN/TAN.
2. **Token- or possesion-based authentication**: Systems based on the possession of a token (a physical or electronic unique authentication resource). This could for example be a cryptographic key or certificate, a smart card, a number sequence generator.
3. **Biometric authentication**: The use of unique personal, physical traits as input for authentication.

In some systems, combinations of authentication methods are used, e.g. in so-called "two-factor authentication" where a secret and a token is needed. Usually, a security system implementation decides upon one authentication system, and then deploys it for all its users. In the e-inclusion perspective, the use of a single authentication method will exclude users

from the authentication procedure, as for any authentication method, there is a user group that has difficulties using it. The same holds for updates of authentication procedures, e.g. in online banking portals: Enhancing PIN/TAN into "mobile TAN" instantly excludes special needs users if they are not taken care of in the respecification of the authentication mechanisms. Some authentication methods are discussed from various disabled user's views in Table 1.

Method	Feature	Visually Impaired	Hearing Impaired	Physically Impaired or diseased	Cognition Impaired	Dyslexia
Passwords	Entering a password on a keyboard	-	-	Might not be able to type	Might not remember (see password overload in (Dhamija, Dusseault, 2008)), Might need longer than timeout	Might not be able to make sense of keyboards and passwords
Text Captcha	Avoiding automated signup to web services	Can't see capcha images	-	Might need long time to enter response	might not remember response in time, might not discover response	can't read response
Smart card	User a secure chip card and card readers for token authentication	Need to trust readers they can't see; Need special PIN input device	-	Might not be able to insert card into a small reader (e.g. think of Parkinson's disease, rheumatism, muscular diseases or malfunctions), might not be able to type PIN	Might forget PINs etc.	Possible problems with PIN pads and screen instructions
Number tokens	Sequence generator with or without PIN entry, display of one-time secrets	Can't read token display; display too small	-	Can't handle small tokens	Token misplaced, Token timeout too short	Can't read token display
Fingerprint scanning	Compares fingerprint pattern in memory with fingerprint on scanner	Might not trust in 3rd-party scanners they can't see	-	Not usable by paralyzed user or user with missing fingers / hands /arms	-	-
Voice Recognition	Speech or voice analysis of words spoken into a microphone	Might object to speak out their passwords in public places (cash machines, mobile devices)	Can't hear command, can't possibly speak clearly	-	-	-

Table 1: Authentication methods and their target-groups specific problems (examples)

We present some promising examples of alternative authentication methods in the sections below.

Authentication tokens with large display and audio

Figure 2: Diverse authentication tokens

The use of security tokens in combination with a web-site represents accessibility challenges for many users, especially those with reading disabilities, especially with tokens as shown in Figure 2. Some dyslectics and people with dyscalculia may have problems in reading codes from a token, especially when the number of digits or characters increases. Obviously blind people cannot read a code card (see Figure 3), and many elderly and visually impaired people also have problems with code cards with very small text size. Some blind people solves this by letting someone they trust read them the codes which they then stores somewhere, either as audio, or as text or Braille on paper or on their computer.

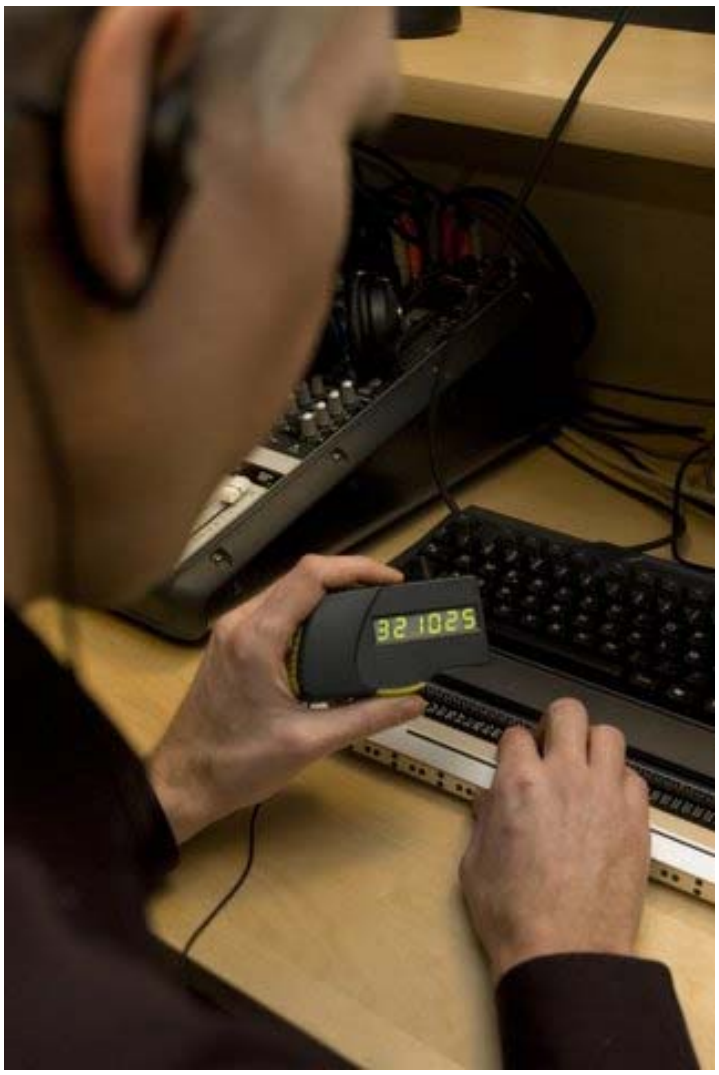

Figure 3: Visually impaired user with an authentication token

In order to increase the security, many Internet banks are replacing code cards with a hardware token that generates a onetime authentication code. Again, the text size represents a challenge to many users. Another challenge is the display time which may be too short, especially if the user needs to use a magnifying glass in order to interpret the code, or if the user is dyslectic and needs longer time to be sure about the sequence. However, there is a potential in making code calculators more accessible. For example the bank DnB NOR in Norway offer their visually impaired customers a hardware token with large display with clear contrasts and text to speech functionality which can read the code out load through earplugs.

Another solution that can be accessible for blind and visually impaired users is adopted by the Norwegian bank Skandiabanken. Here the user can select to have a one time password sent to their mobile phone via a Short Message Service (SMS-message). In Norway, an increasing number of blind and visually impaired people have text-to-speech functionality installed on their mobile phone. Thereby they can have the one-time password read out load to them by their mobile phone while using earplugs. In a field study of ICT barriers of blind and visually impaired people this solution was therefore considered positively (Fuglerud et al. 2008). Google introduced a similar SMS-based security measure for account creation because of its architectural constraints with real costs. The aim was to decrease the feasibility of exploiting the web resource. The solution has been criticized however, because it may introduce socioeconomic barriers for people without access to mobile phones (May 2005). This may still be a very valid objection in many parts of the world, and especially the number of people with access to mobile phones with text-to-speech software may be limited.

Audio based capthca codes

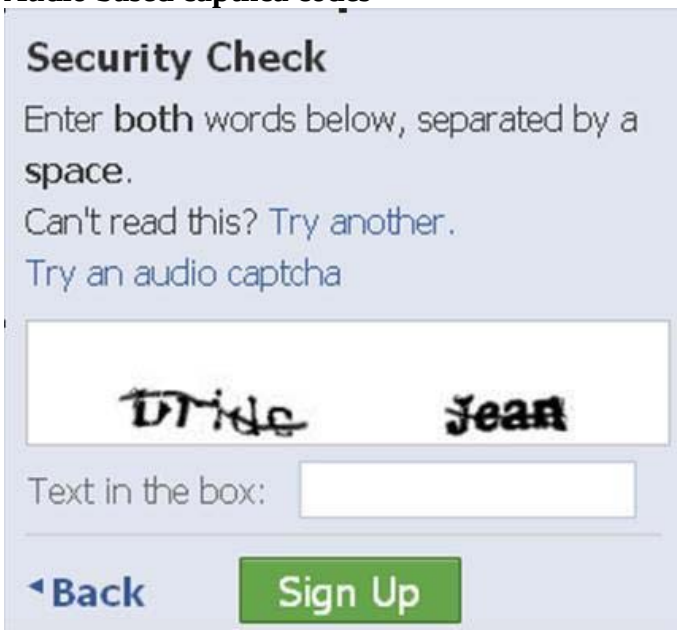

Figure 4: From the registration process at www.facebook.com

There exists solution that provides audio based captcha codes rather than visual based capthca codes. This is an option in the registration process e.g. at Facebook.com, shown in Figure 4.

Image based authentication

Schmidt et. al (2004) reports on a study of users using an image based authentication method. The idea of this approach is to offer people with poor reading and writing skills the opportunity to select and remember images instead of a password based on numbers and/or letters. The user had to select one image out of 24 images, three times. The sequence of three images that the user selected would be their password. The security achieved by selecting three images from three sets of 24 images would be similar to a 4 digit PIN. The study showed that the login time was significantly reduced with the image based authentication method. The study also found that many of the participants were able to remember their image based pictures after several weeks without problems. Whereas most of them had difficulties in remembering a password or a PIN code after several weeks.

Biometrics Pro & Contra

Biometric authentication such as fingerprint scanning, retina scanning or voice recognition systems can be considered easy for users with cognitive problems. There is no need to remember secrets, or to operate authentication tokens, handle PIN codes or follow unintuitive "mobile TAN" procedures on mobile phones. Authentication is done just by pressing a finger to a scanner.

However, biometric authentication might have large disadvantages in field use. Fingerprint scanning is clearly not suitable for paralyzed users who cannot defend themselves against having their finger scanned by a malicious intruder in their proximity. Elderly users suffering e.g. from Parkinson's disease might not be able to keep the finger still long enough for a successful scan. Finally, there are special-needs user with no fingers. A blind person might have major objections in providing electronic signatures authenticated by a fingerprint while they cannot see the system they give their fingerprint to. Voice recognition systems are vulnerable to lingual titubation, background noise, throat infections and serious privacy issues when used around other people.

Concluding, it can be assumed that there is not one biometric authentication solution that will be e-inclusive.

Open issues

E-inclusive authentication methods have yet to be specified. As discussed above, e-inclusive systems very likely need adaptive security measures with several channels. Additionally, changes in the user interface and usage procedures might not be made fast to prevent user exclusion. Many authentication methods are not suitable for special needs users, and must be adapted. This holds for server-side authentication functions as well as for tokens or other technology on the user side. The principal research challenges are:

- **Creation of a taxonomy of authentication usability with respect to e-inclusion**: The elaboration of usability and security levels of authentication methods as sketched in table 1 needs to be elaborated into a taxonomy of usable authentication methods.
- **Development of adaptive, multi-channel and multi-modal authentication strategies**: A single authentication method will always exclude some users. Development work should be put into the design of authentication methods that contain several channels, modalities and adaption options for various user needs.
- **Development of usability measuring methods for authentication methods**: Standardized ways of evaluation of authentication usability would speed up testing, certification and evaluation of e-inclusive authentication methods. Such metrics should measure security levels as well as usability levels.

Special needs profiling, adaptive inclusive systems & privacy risks

This section relates to IMS type 2: Identity management systems for profiling of user data by an organization, e.g. detailed log files or data warehouses which support e.g., personalized services or the analysis of customer.

Profiling

We depart from the following definition of profiling: Profiling is “The process of constructing profiles (correlated data), that identify and represent either a person or a group/category/cluster” (FIDIS D7.2: Descriptive analysis and inventory of profiling practices”)(Fidis 2005b, p. 33).
There are in principle two types of profiling: group profiling, typically (e.g use of data mining techniques to establish general, abstract profiles of a group) and personalized profiling which is focused in this paper.
On the general level, it is likely that that profiling technologies will have a profound impact on access to and participation in the Information Society, as profiles 'could possibly be used against individuals without their knowledge, thus shaping their access to facilities, goods and services, also potentially restricting their movement and invading personal space. In fact, this would regulate their access to, and participation in, the European Information Society' (Levi et al. 2004).

Personalized profiles and special needs

E-inclusive systems may process personalized special-needs user profiles that model disabilities, cognitive requirements and personal weaknesses. Personalization means that systems can be adapted to meet the individual user needs. Personalization includes the technologies, techniques and design features that are employed to configure system interfaces to meet the interaction needs of an individual end-user by personal choice whereby the end-user requests a particular design feature. At the core of personalized services is the user profile or personal profile, which gathers the user preferences and data. This particular

approach to personalization resonates well with the Universal Design' principles mentioned above. These aim to support systems that can be accessed and utilized by all users regardless of the user's cognitive, physical or sensory characteristics. However, pursuing a Universal Design approach does not mean that solutions are not adapted or personalized to the needs of the specific user. For example, an experienced ICT user may want to skip what she finds as tedious and unnecessary instruction whereas the novice may find such help useful. A solution to this may be that personalization is adopted as a design approach that is available to all user' on request, rather than an enforced design feature.

Personalized profiles are particularly valuable for people with special needs as they often have needs that are not satisfied by simply implementing standardized accessibility guidelines and solutions, typically directed towards an average user with a desktop computer. (Cremers et al. 2004). Importantly, as indicated before, this is not a tiny minority but rather the majority of computer users. Most current accessibility guidelines are of this kind, but they do not take into account that people with special needs often will require targeted, specific type of support. Personalized support aiming to meet these specific needs is important. Adaptive systems that utilize profiles may be able to better support the user with special needs by: (see also FIDIS D7.2: Descriptive analysis and inventory of profiling practices" p 33)

- Filtering out the irrelevant information (reducing cognitive load), by delivering this information at the right time (just in time); For example: for various disabled groups, it is often crucially important that the relevant information is as brief, accurate and relevant as possible.
- Choosing a form of delivery that maximizes its impact on this user (taking into account the cognitive style of the user); For example: the user interface is designed according to the medical and/or cognitive profile of the user with special needs, e.g. interfaces for blind people or for people with dyslexia.
- By proposing very contextualized help (the system is aware of the task in which the user is currently engaged into). For example: for the cognitively disabled user it is helpful with contextualized help, e.g. to provide relevant online support in writing processes.

In order to succeed in supporting the person with special needs, a use model must be developed and often also a cognitive profile defined. As noted in the FIDIS project, there are actually few examples of projects and products, even R&D prototypes that provide adaptive, personalized, cognitive profiles for people with special needs. One recent example is the DIADEM project that the authors participate in. The DIADEM project (http://www.project-diadem.eu/) aims at providing an adaptable web browser interface in order to enable people who suffer a reduction of cognitive skills, to remain active and independent members of society. This will be achieved by developing an expert system that monitors the user, adapting and personalizing the computer interface to enable people to interact with web based forms. This system will be located on the user's PC and will ensure that the many services available over the Internet are open and accessible to as many people as possible, whilst providing privacy and security. The user interface is dynamically adjusted to the needs of the user based on input data from the user herself.

Challenges and concerns

Profiling (group profiling and personalized profiling) can in several way be valuable for people with special needs, but there are also several challenges and concerns related to privacy and ethics.

- Stigmatization and exclusion: extensive use of group profiling can be used to exclude rather than include people with special needs; or profiles could be used for economic exploitation e.g. in price discrimination or impulse shopping

- Personalized profiles require extensive use of personal data that are sensitive
- Extensive use of personalized profiles may lead to process of proliferation of personal data that come out of control
- Personalized, cognitive profiles may require sensitive medical data about persons (e.g. cognitively disabled) that are not aware that their data are used and are not likely to stand up for their right for privacy or medical privacy

Open issues

- **Development of a framework of privacy and security risks and consequences of special-needs profiling in ICT infrastructures**: Risk assessment and consequences of privacy incidents in ICT are not well researched (Fritsch et al. 2008). Specific privacy and security risks for disabled persons who are profiled in ICT systems have not been assessed yet. However, with the recent vandalism incident targeted at a forum for epilepsy patients, some of the risks of poor security and identity management became obvious (Poulsen 2008). Risk modeling for profiling of disabilities should be researched.
- **Research and development of privacy-respecting adaption and personalization mechanisms - information systems without profiles**: As most of the contemporary profiling mechanisms use explicitly gathered and database-stored profiles, or gather personal information during the use of the systems by the users, there is a clear need to research into information systems for e-inclusion and adaption that minimize the need for stored personal disability profiles.
- **Control techniques for profile data, their flow in ICT systems and their usage by systems**: Often, profiling information is provided voluntarily by users of context-aware services. However, such an opt-in approach is not appropriate in the case of adaptive systems for disabilities, as the disabled users don't have an opt-out option on the services they depend upon. Such systems should be built in ways that strictly control information storage, information flow, information access and usage in such infrastructures. How this goal is reached is a topic for future research.
- **Research and resolution of medical privacy issues on systems with disability profiles**: Accumulation of disability profiles creates a profile of medical conditions. It is yet uncertain whether such information would turn the e-inclusive information infrastructure as a whole into a medical information system that is subject to medical privacy rules and regulations. How much this holds, and how this can be managed should be researched.

Identity Management with respect to special needs

This section relates to IMS type 3, which are user-controlled context-dependent role and pseudonym management systems. In (Fidis 2005a, p. 14) such IMS are characterized as follows: *The data managed are mainly personal data. Privacy protection therefore is a driving force for the development of IMS of this type and a relevant unique selling proposition (USP). To implement certain functions, such as use of trusted pseudonyms or authentication (e.g. via credentials), in some cases the implementation of centralized third party services is necessary. In addition, the communication partner of the user, who is contacted via the managed identity, in many cases is an organization.*
In other words, type 3 IMS enable the user to choose how identifiable he or she wants to be against a service or against other users. Such identity management has some important implications:

- users should be enabled to participate anonymously or pseudonymously

- users decide which of their personal attributes shall be revealed in which context
- users might like to keep track about what has been revealed
- to engage in e-commerce, forms of payment that support IDM with type 3 IMS can be necessary, e.g. anonymous payment mechanisms.

Why would special needs users care, with their difficulties in accessing plain services with simpler IDM mechanisms? There is evidence that such users might have interests in determining when and who should get knowledge about their identity and disability status. While some explicit modeling of disabilities, special input or output equipment and such must be configured to systems, at the same time the special-needs users prefer not to be discovered as special-needs users. This enables them to engage in "normal" interactions on virtual platforms, where the disabilities are not visible(Zubal-Ruggeri 2007).
However, in some cases, "trolling" – the invasion of special-interest forums by curious or malicious people might render such fora unusable. Here, too much anonymity might hurt the purpose of the service (Herring et al. 2002).
Various new topics in handling identities of special-needs users come into focus. Users might choose not to reveal disabilities to look like other users of an online service, while in other contexts they prefer adaptive systems or special interest groups where disabilities are identifiable.
To support user-controlled identity management, some research prototypes have been implemented. They are briefly discussed below.

Reachability manager

An early effort in user-controlled identity management was the "Erreichbarkeitsmanager" (Reachability manager) project (Reichenbach et al. 1997). The protected information here was the reachability status of the owner of a mobile phone. Phone owners could configure their reachability dependent on many caller attributes, profiles and credentials. The purpose of the system was the user-controlled reachability for selected callers in various situations. The implemented prototype used mobile phones and Apple Newton personal digital assistants as the trial infrastructure. Some surveys along the project gave positive feedback from professional users. However, no special consideration for usability & e-inclusion issues was made at the time.

iManager

In Jendricke et al (2000) iManager is presented as a type 3 identity management system with a user-friendly interface. Its underlying model identifies several states of observability and confidentiality for user actions. A rules database combines such required states through usage policies with various security mechanisms, e.g. anonymizing services and credential management. Configuration through end-users is performed mainly through a policy-driven approach.
iManager was implemented prototypically in Java at Albert-Ludwigs-University in Freiburg, Germany,

IDEMIX

Camenisch et al.(2002) describes a radically new approach towards type 3 identity management. IBM Research developed a family of protocols based on zero-knowledge-proofs and other advanced cryptographic techniques supporting the concept of "anonymous credentials". Such credentials are pieces of data that can be used to show identity-related information such as age, possession of driver's licenses etc. without revealing other identifying information. With an infrastructure based on IDEMIX, digital tokens for many kinds of authentication, registration or service adaption could be used in anonymous ways. IDEMIX is currently being integrated into the Eclipse Higgins open source software development system (http://wiki.eclipse.org/Idemix_Provider).
However, IDEMIX offers many usage options, and thus requires users to manage a growing complexity. The integration of IDEMIX into a user-friendly management interface, e.g. similar to iManager, still needs to be done. As IDEMIX handles many cryptographic secrets

and related security information, cognitive models for all users must be found to safely deploy IDEMIX to the public.

Open issues

Concerning e-inclusive, adaptive information systems, can user-controlled identity management be implemented, and does it help users with special needs? How can disability-related identity information be hidden in e-inclusive systems? How can disability-related identity information be used for system adaption, authentication and other purposes in secure & anonymous ways? Are identity management systems of type 3 usable and e-inclusive? How do disabled users wish to manage their identities? What metaphors and interfaces are needed to enable all users to manage their on-line identities? The discussion needs to focus on two aspects:

1. **Adaptive, user-profiling information systems**: Adaptive information systems need knowledge about users to adapt. A braille terminal will always request information in plain text, while a cognitively challenged person will always be observable within a session as having a higher error rate and slower response rate than the average user. To provide e-inclusive, adaptive systems with such information, it cannot be effectively removed from the systems. A common strategy in such situations is the effort to anonymize sessions while interacting with information systems. Various technologies and concepts supporting the separation of sessions and identity have been developed in the area of Privacy-enhancing technologies (PET). Such systems include the concept of secure anonymous channels that connect important parts of the infrastructure, where the access to the channel implicitly expresses group affiliation (Koelsch et al. 2005) with a specific prototype described in (Zibuschka et al. 2007). While this works on an individual level, some special needs users could be grouped into larger segments of needs. For synchronous, anonymous access to services through groups, where the whole group creates the anonymity set, a solution for map-oriented location-based services has been presented in (Kohlweiss et al, 2007). Such an infrastructure can be deployed for groups of special needs users as well. The concept of location camouflaging in (Fritsch 2008) suggests hiding the real user transaction in a cloud of artificial, simulated accesses to obscure the real person's identity. However, the deployment of such techniques to various e-inclusion target groups has yet to be done.
2. **User-controlled identity management**: Although some approaches and prototypes of type 3 IMS exist, the major critique from the usability experts warns about exposing the user to high degrees of complexity, while users seek to get things done with the least possible effort (Dhamija et al. 2008). Such complexity might confuse even users without disabilities, as (Pettersson et al. 2005) found that users of various interfaces to privacy management get confused between pseudonyms and the real world even on user-friendlier interfaces.

Conclusion and Outlook

The focus of this paper has been the need for inclusive identity management mechanisms such that this will benefit everyone, including people with disabilities and special needs. A fundamental challenge for inclusive identity management is the change of perspective concerning the information security technologies involved. While security engineering usually targets the highest security level for a particular authentication method, or for particular security goals, inclusive systems must provide several alternatives to users. Additionally, the capabilities of humans change over time, implying a life cycle of usable security techniques that will be used consecutively in a user's life.

We have pointed out several open research issues for each of three types of identity management systems; authentication, profiling and user controlled and context-dependent IMS systems. The open issues are not only technology related, but spans over several disciplines. This includes mainstreaming inclusive design in the development usable and accessible multimodal authentication mechanisms in different channels, careful considering of profiling and privacy matters, the need for standardization and interoperability with assistive technologies and the need for viable models and incentives to system providers. Research, design and testing of identity management systems and their security features, such as authentication techniques, is a fundamental research challenge. Without sufficient solutions in this area, many users may be excluded from the participation in the electronic society right from the login screen.

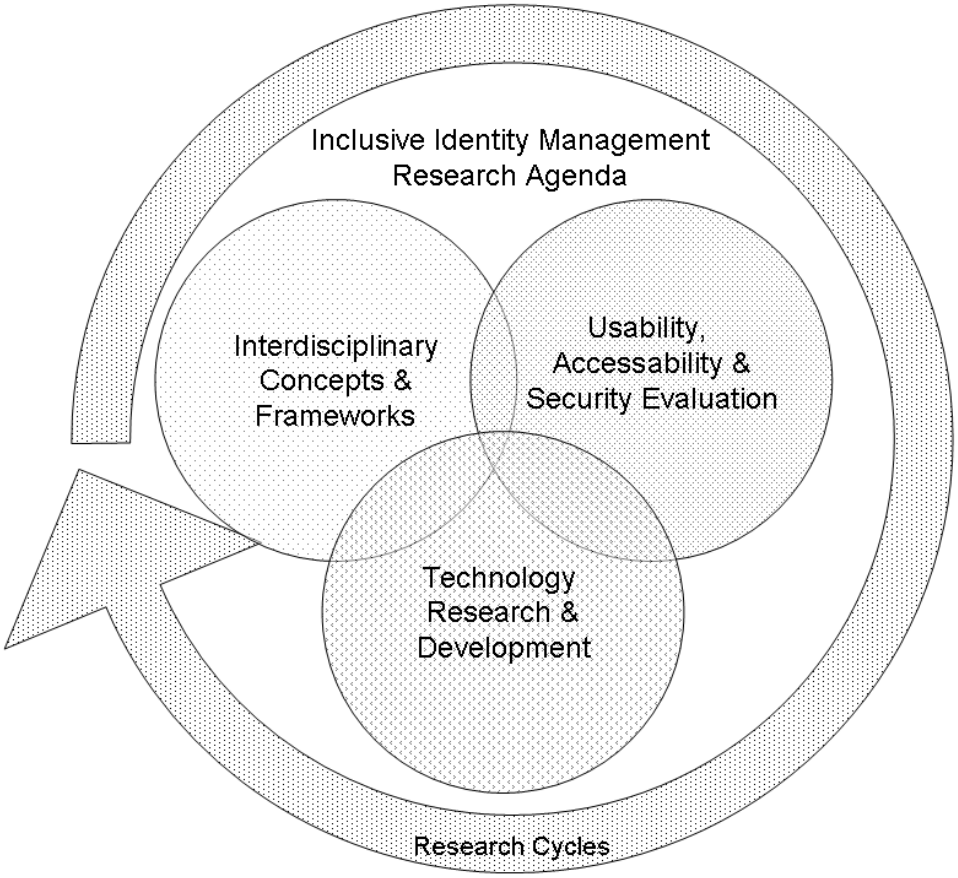

Figure 5: Research Agenda for e-inclusive Identity Management

We have shown that this is a complex field that involves work in different areas. We think this fosters an interdisciplinary effort, and that it is of particular importance to ensure that the needs of users with disabilities and special needs and other stakeholder are taken into account by the involvement of these groups in future research activities within this area. We sketched the research agenda fort his effort in Figure 5.

Acknowledgements

This work was based on research within the project "UNIMOD - Universal design in multi modal interfaces", partly funded by the Norwegian Research Council, and on work within the European Union IST FP6 Diadem project sponsored by the European Commission.

References

ADA. *Americans with Disabilities Act. ADA Home page*. Accessed 20. May 2008. URL: http://www.ada.gov/.

Ahn, L. v.; Blum, M. & Langford, J. (2004). Telling humans and computers apart automatically. *Commun. ACM*, 47 (2): 56-60, 2004.

Camenisch, J. & van Herreweghen, E. (2002). Design and Implementation of the Idemix Anonymous Credential System. *Research Report RZ 3419.* Zürich.

CEN/CENELEC. (2002). CEN/CENELEC Guide 6. Guidelines for standards developers to address the needs of older persons and persons with disabilities. *Edition 1, January 2002*. January 2002.

Cremers, A. H. M. & Neerincx, M. A. (2004, June 28-29). *Personalisation Meets Accessibility: Towards the Design of Individual User Interfaces for All*. User-Centered Interaction Paradigms for Universal Access in the Information Society, UI4All 2004, Vienna, Austria. Springer-Verlag Berlin Heidelberg. pp. 119-124.

CUD. (1997a). *Center for Universal Design*. Accessed 10 January 2006. URL: http://www.design.ncsu.edu/cud/.

CUD. (1997b). *Principles of Universal Design,* The Center for Universal Design, North Caroline State University. Accessed 10 January 2006. URL: http://www.design.ncsu.edu:8120/cud/univ_design/princ_overview.htm

Dhamija, R. & Dusseault, L. (2008). The Seven Flaws of Identity Management: Usability and Security Challenges. 6 (2): pp. 24-29.

EC. (1995-2007). *Inclusion, better public services and quality of life*. Europe's Information Society Portal, The European Commission. Accessed April 2007. URL: http://ec.europa.eu/information_society/eeurope/i2010/inclusion/index_en.htm.

EC. (2005). i2010 - A European Information Society for growth and employment. *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and The Committee of the Regions*, Report no 229 final, Commission of the European Communities. 01.06.2005. 12 pages.

EC. (2006). *Internet for all: EU ministers commit to an inclusive and barrier-free information society*. Press Releases. Reference: IP/06/769, European Commission. Accessed 11th of October 2007. URL: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/769&format=HTML&aged=0&language=EN&guiLanguage=en.

EC. (2007). i2010 e-Inclusion Subgroups National Reports. Portugal, European Commission, Information Society and Media Directorate-General, ICT for Inclusion 3 December 2007. 175 pages.

EDeAN. (2006). *European Design for All e-Accessibility Network*. Accessed 15 Nov. 2007. URL: www.edean.org.

EIAO. (2005). *European Internet Accessibility Observatory*. Accessed Jan 2006. URL: http://www.eiao.net/

Engelen, J. (2007). Report on standardisation and DfA. *CEC Deliverable Number D2.2a*, Kath. Univ. Leuven. December 31, 2007.

Fidis. (2005a). FIDIS Deliverable D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems. 15. September 2005. URL: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf.

Fidis. (2005b). FIDIS Deliverable D7.2: Descriptive analysis and inventory of profiling practices. 2005b.

Fritsch, L. (2008). Profiling and Location-Based Services. In, pp. 147-160. Dordrecht, Springer Netherlands. URL: http://www.springer.com/new+&+forthcoming+titles+(default)/book/978-1-4020-6913-0

Fritsch, L. & Abie, H. (2008). A Road Map to the Management of Privacy Risks in Information Systems. In Gesellschaft f, I. (ed.) vol. 128, pp. 1-15. Bonn, Gesellschaft für Informatik.

Fuglerud, K. S. & Solheim, I. (2008). Synshemmedes IKT-barrierer. Resultater fra undersøkelse om IKT-bruk blant synshemmede. *Report number: 1016*. Oslo, Norwegian Computing Center. March 06, 2008. 91 pages.

Herring, S.; Job-Sluder, K.; Scheckler, R. & Barab, S. (2002). Searching for Safety Online: Managing "Trolling" in a Feminist Forum. *The Information Society*, 18 (5): 371 - 384, 2002. URL: http://www.informaworld.com/10.1080/01972240290108186

Jameel, H. (2007). Taxonomy of Human Identification Protocols. Korea,, U-security Research Group, Ubiquitous Computing Laboratory, Kyung Hee University. Accessed 21 May 2008. URL: http://uclab.khu.ac.kr/usec/taxonomy/hassan.pdf.

Jameel, H.; Shaikh, R. A.; Lee, H. & Lee, S. (2007, February 5-9). *Human Identification through Image Evaluation using Secret Predicates*. To be published in Topics in Cryptology CT-RSA 2007, The Cryptographers Track at the RSA Conference 2007, San Francisco, CA, USA. URL: http://uclab.khu.ac.kr/usec/publication/hassan_rsa.pdf.

Jendricke, U. & Gerd tom Markotten, D. (2000). *Usability meets security -The Identity-Manager as your Personal Security Assistant for the Internet*, New Orleans, Lousiana, USA. URL: http://www.acsac.org/2000/papers/90.pdf

Koelsch, T.; Fritsch, L.; Kohlweiss, M. & Kesdogan, D. (2005). Privacy for Profitable Location Based Services. In vol. 3450, pp. 164-179. Boppard, Springer.

Levi, M. & Wall, D. S. (2004). Technologies, Security, and Privacy in the Post-9/11 European Information Society. *Journal of Law and Society*, 31: 194-220, 2004. URL: http://www.ingentaconnect.com/content/bpl/jols/2004/00000031/00000002/art00002 http://dx.doi.org/10.1111/j.1467-6478.2004.00287.x

May, M. (2005). Inaccessibility of CAPTCHA. Alternatives to Visual Turing Tests on the Web. In W3C (ed.), W3C Working Group Note, work in progress. 23 November 2005. Accessed 12. May 2008. URL: http://www.w3.org/TR/turingtest/.

Pettersson, J. S.; Fischer-Hübner, S.; Danielsson, N.; Nilsson, J.; Bergmann, M.; Clauss, S.; Kriegelstein, T. & Krasemann, H. (2005). *Making PRIME usable*. Proceedings of the 2005 symposium on usable privacy and security, Pittsburgh, Pennsylvania. ACM.

Poulsen, K. (2008, 28. Mars). Hackers Assault Epilepsy Patients via Computer. *WIRED News*. Accessed 20 May 2008. URL: http://www.wired.com/politics/security/news/2008/03/epilepsy#.

Reichenbach, M.; Damker, H.; Federrath, H. & Rannenberg, K. (1997). Individual Management of Personal Reachability in Mobile Communication. In, pp. 164-174. London, Chapman & Hall.

Schmidt, A.; Kölbl, T.; Wagner, S. & Straßmeier, W. (2004, June 28-29, 2004,). *Enabling Access to Computers for People with Poor Reading Skills*. 8th ERCIM Workshop on User Interfaces for All, Vienna, Austria. Springer-Verlag Berlin Heidelberg. pp. 96–115.

Section 508. *Section 508*. Accessed 14. June 2007. URL: http://www.section508.gov/.

Steg, H.; Strese, H.; Loroff, C.; Hull, J. & Schmidt, S. (2006). Europe Is Facing a Demographic Challenge Ambient Assisted Living Offers Solutions. In AAL (ed.). *European Commission (Contract No. 004217)*, VDI,VDE,IT. March 2006.

Stevenson, B. & Kolko, J. (2004). Accessible technology in computing - examining awareness, use and future potential, A Research Study Commissioned by Microsoft Corporation and Conducted by Forrester Research inc. 58 pages. URL: http://www.microsoft.com/enable/download/default.aspx#research.

Stevenson, B. & McQuivey, J. L. (2003). The wide range of abilities and its impact on computer technology, A Research Study Commissioned by Microsoft Corporation and Conducted by Forrester Research inc. 24 pages. URL: http://www.microsoft.com/enable/research/default.aspx

Tari, F.; Ozok, A. A. & Holden, S. H. (2006, July 12-14). *A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords*. Symposium On Usable Privacy and Security (SOUPS), Pittsburgh, PA, USA.

Udjus, L. (2007). "Gjør døren høy - gjør porten vid". Offentlige elektroniske tjenester for alle. *Stat og styring*, 2007 (3).

W3C WAI. *Web Accessibility Initiative (WAI)*. Accessed 14. June 2007. URL: http://www.w3.org/WAI/.

Zibuschka, J.; Fritsch, L.; Radmacher, M.; Scherner, T. & Rannenberg, K. (2007). *Privacy-Friendly LBS: A Prototype-supported Case Study*, Keystone, Colorado, USA.

Zimmerman, D.; Roll, M. & Yohon, T. (2001, 10/24/2001 - 10/27/2001). *Making Web sites and technologies accessible*. Professional Communication Conference, IPCC 2001, Sante Fe, NM, USA. IEEE International. pp. 87-93. URL: http://ieeexplore.ieee.org/Xplore/login.jsp?url=/iel5/7661/20931/00971553.pdf?tp=&isnumber=20931&arnumber=971553.

Zubal-Ruggeri, R. (2007). Making Links, Making Connections: Internet Resources for Self-Advocates and People With Developmental Disabilities *Intellectual and developmental disabilities*, 45 (3): 209-215. June 2007, 2007.