IDIS
DOI 10.1007/s12394-010-0075-6

Towards inclusive identity management

Lothar Fritsch · Kristin Skeide Fuglerud · Ivar Solheim

Received: 30 June 2008 / Accepted: 18 April 2010
© The Author(s) 2010. This article is published with open access at Springerlink.com

Abstract The article argues for a shift of perspective in identity management (IDM) research and development. Accessibility and usability issues affect identity management to such an extent that they demand a reframing and reformulation of basic designs and requirements of modern identity management systems. The rationale for the traditional design of identity management systems and mechanisms has been security concerns as defined in the field of security engineering. By default the highest security level has been recommended and implemented, often without taking end-user needs and accessibility issues into serious consideration. The article provides a conceptual framework for inclusive IDM, a brief overview of the regulatory status of inclusive IDM and a taxonomy of inclusive identity management methods. Several widespread IDM approaches, methods and techniques are analyzed and discussed from the perspective of inclusive design. Several important challenges are identified and some ideas for solutions addressing the challenges are proposed and discussed.

Keywords E-Inclusion · Identity management · Information security · Privacy · Authentication · Exclusion · Disabilities · Universal design · Usability

Approaching exclusive identity technology

Interaction with information systems penetrates most layers of modern society. Computing has turned into a personalized matter, where the use of information

L. Fritsch (✉) · K. S. Fuglerud · I. Solheim
Norsk Regnesentral - Norwegian Computing Center, PO Box 114 Blindern, 0314 Oslo, Norway
e-mail: Lothar.Fritsch@NR.no

K. S. Fuglerud
e-mail: Kristin.Skeide.Fuglerud@NR.no

I. Solheim
e-mail: Ivar.Solheim@NR.no

Published online: 07 October 2010

systems is based on electronic identities, and access to systems, data and applications is granted with privileges associated with electronic identities. This causes a confrontation between large parts of Europe's population with the computing, information systems and information security disciplines. As a consequence, societal requirements for e-inclusion, privacy protection, and equal rights for all citizens are formulated by disciplines and stakeholder groups that normally do not formulate technical requirements. This causes friction between system development, policy makers, and the users of such information systems. This article reviews the magnitude of this friction, and presents the need for focused, interdisciplinary research on inclusive identity management.

Rationale

The article argues for a shift of perspective in identity management (IDM) research and development. Accessibility and usability issues affect identity management in a way that demands a reformulation of the designs and requirements of modern identity management systems.

The rationale for the traditional design of identity management systems and mechanisms has been security concerns defined in the field of security engineering. By default the highest security level has been recommended and implemented, often without taking end-user needs and accessibility issues into serious consideration. An increasing number of public and private services are digitized. Many of these e-services require some kind of identification. In order to address the challenge of including all citizens in the information society it is necessary to develop identity management systems that ideally can be used by all possible users. This implies that identity management methods should be accessible for a broad range of users, with different skills, ages and various (dis)abilities—different cultures backgrounds and utilizing different devices. This calls for a shift of perspective towards the needs and capabilities of all types of users, included users with disabilities that may impede their access to identity management systems. An inclusive IDM perspective implies a need for a systematic approach towards integrating usability and accessibility concerns in the design and development of identity management systems; in this article this is called an inclusive identity management approach (IIDM).

Research agenda and frameworks

The field of inclusive IDM must take the goals, insights and concerns of various disciplines into account, especially those of universal design, security engineering and privacy/legal issues. Furthermore, we argue IIDM should define itself as an interdisciplinary and even transdisciplinary approach (Gibbons et al. 1994) that not simply aggregates established knowledge from various disciplines but can pave the way for new ideas, approaches and technical solutions.

By using Universal design (UD) of IDM-systems, all potential users with different skills, knowledge, age, gender, (dis)abilities and literacy, can be included. A central issue in the field of universal design of ICT is the role of flexible multimodal user interfaces that can meet different users' needs, abilities, situations, preferences and devices (Fuglerud 2009; Hellman 2008). The paradigm in security engineering is

often to design a single security method at a sufficient security level. However, the choice of this "one security method" will exclude many users from the use of many mainstream ICT supported products and services. The need for adaptability and flexibility in IDM can be approached by personalization which may be based on user profiles holding information about the modalities and functionalities best suiting the particular user's individual needs and preferences, use of assistive technology etc. A third field that is crucial is privacy concerns. For example, adaptive, dynamic profiling systems introduce new privacy threats. Profiling and personalization have privacy implications; user profiles may contain sensitive information about a user's disabilities. Thus, privacy requirements of universally designed systems may transcend normal privacy concerns due to profiling of disability related information about the user. Also, profiling techniques can be misused, as pointed out by Huang (2005) and Solove (2006). Hence, privacy-enhancing technology (PET), see Fritsch (2007), are called for. More research is necessary when PET and privacy-preserving IDM technology will be deployed in multimodal, user-adaptive systems.

Furthermore, we argue that IIDM can be characterized as an interdisciplinary approach, by drawing upon insights from the fields mentioned above, but also others. Figure 1 below illustrates the overall research agenda for the article.

The research cycle of inclusive identity management comprises three major elements:

- *Usability, accessibility and security evaluation*. Testing of concepts and solutions must be based upon approaches that integrate the usability and accessibility needs as well as security and privacy concerns in common, integrated evaluation and testing frameworks.
- *Technology R&D*. New concepts must be implemented, preferably as prototypes that can be tested out and eventually provide sustainable solutions.
- *Concepts and frameworks* drawn from a range of disciplines, such as human computer interaction (HCI) and information security design, should be combined

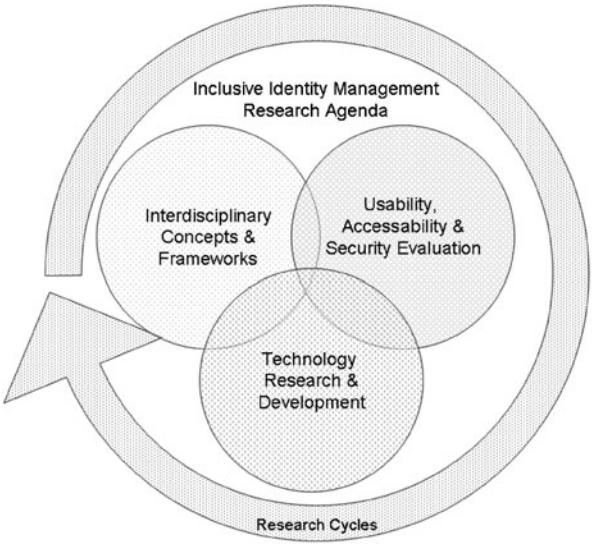

Fig. 1 Research agenda for e-inclusive identity management

into an interdisciplinary framework, e.g. into the concept of inclusive identity management (IIDM)

In order to initially describe in a more elaborate manner what characterizes IIDM as research, Gibbons' (Gibbons et al. 1994) widely known term *Mode 2 knowledge* provides a fruitful point of departure. Gibbons et al. argue that as opposed to Mode 1 research which is defined as traditional academic, investigator-driven and discipline-driven research, Mode 2 is context-driven, problem focused and interdisciplinary. In our view, the field of IIDM also requires a clearly context-driven and interdisciplinary research approach. Traditionally, this has characterized the fields of human computer interaction and universal design research (Kuutti 2007). According to Kuutti (2007) the rapid growth and increasing influence of the HCI research field, is due to its Mode 2 character and that "To some extent, HCI as a discipline has been able to bridge between university and society, and between scientific acceptability and practical relevance." (Kuutti 2007:14) In our view, the IIDM research community would benefit from following a similar course in the further development of the field. However, the field should also bear in mind Kuutti's critical comment concerning the HCI research model: "It is not the ultimate model, however: research in HCI often takes place in an incremental way, following the development of technology instead of searching for new openings. And in HCI discussion about fundamental issues and reflection upon them is largely missing—that is why I find the discussion within design research community attractive." (2007: 14).

In line with the argumentation above, we will emphasize the following elements as particularly important in characterizing IIDM as a research approach:

- Context-driven knowledge production: Problems arise and are formulated in the context of application. The research field must take into account that the IDM technology and the applications as well as users' preferences, subjective needs and competencies are all rapidly changing. What a user saw as acceptable interface some years ago may have become unacceptable several years later. In order to make a difference and have relevant impact, the research must be highly sensitive to these developments. Typically, new IIDM ideas must be developed within context defined by actual stakeholders and users facing real-life challenges.
- A pragmatic and context-driven approach to methods (e.g. both quantitative and qualitative can be applied, often in concert). Typically, flexible and time-efficient methods that provide systematic user feedback and evaluation in the whole cycle of research and development are crucial. Knowledge is socially distributed and methods must focus on collaboration and dialogue between all actors involved. The empirical examples to be presented in the article will illustrate the need for an open-minded, flexible, problem-driven, user-oriented and empirically grounded approach to methods.
- Develop IIDM ideas and prototypes iteratively. Learning and knowledge production processes are closely related. Solutions must be developed in close collaboration between developers, users (e.g. disabled persons) and other stakeholders.
- The production of knowledge does not take place primarily within the framework of a discipline, but is transdisciplinary, Theoretical and methodological frame-

works must be developed that spur new concepts and ideas, not simply aggregate old ones from different disciplines. Problems in the field must be solved by teams that comprise competencies and insights from all three main fields, and also even others, such as psychology, design research, sociology and others.

Background of inclusive identity management

This section illustrates the relevance and the foundations of a usability and accessibility perspective on identity management.

The need for inclusive identity management

There are several important societal trends that underscore the need for more accessible and user friendly IDM systems and devices. First, there is a demographic shift towards ageing in Europe (Giannakouris 2008), and in fact all over the world (Steg et al. 2006, p. 8). 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, and compensate for physical or cognitive difficulties and impairments. Figures from the U.S show that about 48.9 million Americans, or 19.4% of the population (non-institutionalized), have a disability that interferes with common activities of daily living (Stevenson and McQuivey 2003). The report by Stevenson and McQuivey (2003) contend that about 60%, of working-age adults in the U.S. are likely to benefit from the use of accessible technology. The report defines accessible technology to be technology that can be adapted or adjusted to meet individual visual, hearing, dexterity, cognitive, and speech needs (Stevenson and Kolko 2004). Second, there is an increasing political pressure towards the development of accessible solutions. Examples include the EU Riga Ministerial declaration which set the goal that all public websites should be accessible by 2010 (EC 2006), and the EU Commissions' i2010 action plan, where one of the main goals is to ensure that the benefits of the information society can be enjoyed by all (EC 2005–2010). Third, the EU has signed the UN Convention on the Rights of Persons with Disabilities including an article on universal design in ICT (EC10550 2009). Finally more countries are introducing clauses in their legislation to promote inclusive design of ICT in order to prevent discrimination and exclusion from the information society (EDeAN 2009).

Inclusive design

Several design approaches that encompass the goal of producing more inclusive products and services have emerged within ICT development communities since the mid-1980's. Examples include "universal design", "design for all", "universal usability", "accessible design", "universal access", and "sensitive inclusive design".

Inclusive approaches to identity management are influenced by these approaches, especially by "Universal Design" (UD). UD approach aims to make products and environments usable by all people, to the greatest extent possible, without the need for adaptation or specialized design (CUD 1997). Here are the seven principles of

UD as defined by the Center for Universal Design at North Carolina State University (CUD 1997):

1. **Equitable Use**: The design is useful and marketable to people with diverse abilities.
2. **Flexibility in Use**: The design accommodates a wide range of individual preferences and abilities.
3. **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.
4. **Perceptible Information**: The design communicates necessary information effectively to the user, regardless of ambient conditions or the user's sensory abilities.
5. **Tolerance for Error**: The design minimizes hazards and the adverse consequences of accidental or unintended actions.
6. **Low Physical Effort**: The design can be used efficiently and comfortably and with a minimum of fatigue.
7. **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 generic, and are adopted within a wide range of design disciplines, from architecture and product design to design of ICT products and services.

The main idea of UD and the other inclusive design approaches is to make mainstream products and services accessible and usable by as many users as possible. These design approaches are not about a special design for small user groups (e.g. in producing assistive technology), but about extending the potential user groups of mainstream products and services to include disabled, elderly people and people with poor ICT skills, people with reading and writing difficulties etc.

The acknowledgement of user diversity, in contrast to modelling an average user, or a typical user, is important. Knowledge and awareness of the different needs, preferences and abilities of different kinds of users are central in the inclusive design approaches. Therefore, the development of accessible, flexible and easy-to-use mainstream ICT products and services are central goals in the design of inclusive ICT systems. Two properties of ICT make this issue interesting and promising compared with other design disciplines:

– The potential of adaptation and conversion 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.
– There are many possibilities to making products flexible and adaptable to the single special users needs when using profiles and personalization in adaptive systems is large.

Therefore, identity management (IDM), security and privacy step forward as important in designing inclusive ICT systems.

Another 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 and regulatory issues.

Accessibility standards and regulations

The status of accessibility standards in the field illustrates the need for new approaches. In many countries, such as the United States, Australia, Japan and the European Union, legislative actions are in place to ensure that products and services are accessible and usable by as many users as possible, including older people and people with disabilities. Thus, many standardization initiatives are directly or indirectly stimulated by the European Commission and other national bodies (Engelen 2007). In addition, many stakeholder groups and non governmental organizations (NGOs) 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 sometimes refer to less formal guidelines in order to specify the operationalisations of the laws. Well known examples are the guidelines produced by the Web Accessibility Initiative within the World Wide Web consortium (WAI 2010), such as WCAG (Web Content Accessibility Guidelines) and ARIA (Accessible Rich Internet Applications). These guidelines are almost universally accepted as the primary reference point for web accessibility matters.

Standards conformance

There are several tools, both checklists and software, aimed at evaluating 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 laws, standards or guidelines. See for example the WAI website (http://www.w3.org/WAI/) and the website of the U.S. Section 508 law (http://www.section508.gov/). Another example is the European Internet Accessibility Observatory (EIAO). The EIAO project has established a large scale accessibility benchmarking service (EIAO 2008) based on the W3C WAI guidelines.

Following accessibility guidelines and standards is necessary in order to obtain accessibility, but this does not ensure that the solution meets the unique needs and challenges of the various user groups (Lazar et al. 2007; Mikovec et al. 2009; Petrie and Kheir 2007).

Compliance with current accessibility guidelines and standards is a prerequisite for accessibility, but does *not* ensure that the user actually is able to use the solution (Babu and Singh 2009; Lazar et al. 2007)

Guidelines and standards for accessible and usable security

To our knowledge the only standards effort in the area of usable security is the W3C's Web Security Context working group (WSC 2006). This group is aware of accessibility issues, but there are limited suggestions on how to resolve them (Zurko and Johar 2008).

The CEN/CENELEC[1] (2002) document contains guidelines for standards developers to address the needs of older persons and persons with disabilities. The guidelines require 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 Braille-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, p. 14).

Need for accessible and usable IDM

There is, to our knowledge, no research that shows to what degree different user groups may have problems with IDM systems. However, there are studies suggesting that authentication problems constitute a significant part of calls to helpdesk services. For example, a survey based on users' requests to the helpdesk of the Norwegian governmental portal Altinn.no for public and commercial reporting, shows that 33% of helpdesk requests were related to user problems with log-in and authentication mechanisms (Udjus 2007; Halbach 2009). Gartner found that about 30% of the help desk calls were about password resets (Tari et al. 2006). Low usability of security mechanisms has been found to be a major source of flaw, risk and barrier to secure and proper use of IT systems (Adams and Sasse 1999; Braz and Robert 2006; Halpert 2005; Whitten and Tygar 1998; Jendricke and Gerd tom Markotten 2000; Dhamija and Dusseault 2008). Several authors have noted that image based authentication is a hindrance for vision-impaired users (Fuglerud et al. 2009; Ahn et al. 2004; Jameel et al. 2007; May 2005)

Security mechanisms in general have been found to be a major barrier for visually impaired ICT users (Fuglerud and Solheim 2008). This is probably because most of the current recommendations about usable security are based on visual representations and cues, with no indication of non-visual alternatives (Zurko and Johar 2008).

Another known problem is that security software may be in direct conflict with usability concerns: If third-party software, such as screen readers, can hook into authentication mechanisms, then malicious programs could mask as assistive technology and compromise authentication information and violate the security of the user (Jaeger 2004). The problem is that the security mechanisms block programs for the screen reader users (Jaeger 2004; Hochheiser et al. 2008). (A screen reader is

[1] CEN (the European Committee for Standardization) and CENELEC (the European Committee for Electrotechnical standardization).

a software application that attempts to identify and interpret what being displayed on the screen, often used by visually impaired or dyslectic users).

In summary, even if current standards and guidelines are applied, several problems related to accessibility and usability of security mechanisms may not be addressed. First, the solutions may not be usable even when standards are applied, and second, there are many unsolved issues regarding accessibility of various security mechanisms. Therefore more research in the area of inclusive IDM technologies is needed.

Inclusive design of IDM technologies

A closer analysis of identity management systems (IMS) with respect to e-inclusion reveals a number of important research and development issues and challenges. The discussion of these will be structured by a classification of IMS systems (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 users, e.g. detailed log file analysis or data warehouses which support personalized services or the analysis of customer behaviour,
Type 3. IMS for user-controlled context-dependent role and pseudonym management

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

Accessibility and usability challenges of authentication methods

This section illustrates some of the challenges of inclusive authentication. The problems and issues herein relate to type-1 IDM systems.

A taxonomy of such systems is shown in Fig. 2. 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 that the authentication methods can be used by as broad a range of users as possible. Common authentication methods include passwords and PINs, tokens, 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 by different user groups.

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

- **Knowledge-based authentication**: Systems based on the knowledge of a secret, e.g. passwords or PIN/TAN.
- **Token- or possession-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.
- **Biometric authentication**: The use of unique personal, physical traits as input for authentication.

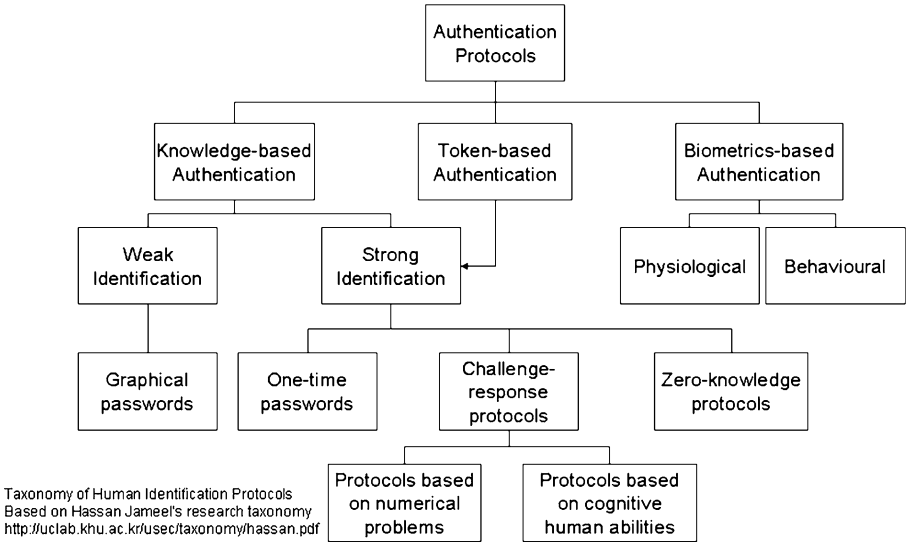

Fig. 2 Jameel's taxonomy of identification methods (Jameel 2007)

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 implementer decides upon one authentication system, and then deploys it for all users. In the e-inclusion perspective, the use of a single authentication method will exclude user groups from the authentication procedure, as for any authentication method will have 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 some user groups if not care is taken in the re-specification of the authentication mechanisms.

Some authentication methods are discussed from the views of various user groups in Table 1.

In the following we discuss some of the authentication methods and related accessibility issues in more detail.

Passwords

Procedures requiring text based passwords can lead to problems for dyslexic people (Fuglerud et al. 2009). They may have difficulties writing the password correctly, and sometimes there are a limited number of tries.

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

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

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 and 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 userwith 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	–	–	–

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.

Authentication tokens

The use of security tokens in combination with a web-site presents accessibility challenges for many users, such as people with reading disabilities. Examples of such tokens are shown in Figs. 3 and 4. 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 (shown at the top of Fig. 3), and many elderly and visually impaired people also have problems with code cards with small text size. Some blind people solve this by letting someone they trust read them the codes which they then store somewhere, either as audio, or as Braille on paper or they enter it into their computer (Fuglerud and Solheim 2008), however this introduces additional security and privacy issues.

In order to increase 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 read 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, clear contrasts and text to speech functionality which can read the code out loud through ear phones.

Fig. 3 Diverse authentication tokens used for internet banking

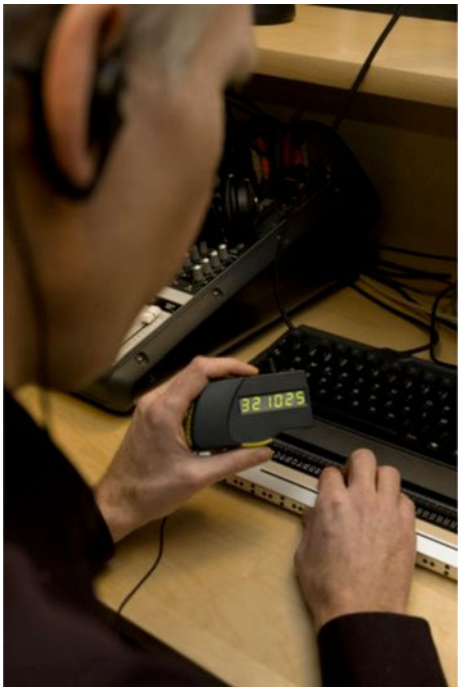

Fig. 4 Visually impaired user with an authentication token

Another solution that is accessible for blind and visually impaired users was adopted by the Norwegian bank Skandiabanken. Here the user can choose 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. They can have the one-time password read out loud to them by their mobile phone while using earplugs. In a field study of ICT barriers for blind and visually impaired people this solution was well recieved (Fuglerud and Solheim 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 because it may introduce socio-economic barriers for people without access to mobile phones (May 2005). However, in most countries mobile phones are more common than internet connections. Therefore, if people are in position to connect to internet, they are likely to have access to a mobile phone. On the other hand, the number of people with access to mobile phones with text-to-speech software may be limited in many parts of the world.

CAPTCHAs

A W3C note on Turing tests discusses both accessibility and security problems with so-called CAPTCHAs (May 2005). CAPTCHA, which stands for Completely Automated Public Turing Test to Tell Computers and Humans Apart, often refer to a small graphical representation of a word that is supposedly unreadable for software. 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 barriers to users who are blind, visually impaired or dyslexic (Fuglerud et al. 2009; Hochheiser et al. 2008).

Some solutions provide a screen-reader-friendly annotated audio based CAPTCHA code rather than visual ones. This is an option in the registration process e.g. at Facebook.com, shown in Fig. 5.

Audio CAPTCHAs typically presents users to a stream of spoken digits, which the user then must type into the form. These audio streams often have background noise and a variety of voices in order to make it hard for speech recognition software to interpret the digits. This also makes it hard for the user to interpret the audio digits. Even so, the audio alternative is certainly better for blind people, but is not accessible for hearing impaired people. Also, the distorted speech and background noise represents usability problems for other groups (Hochheiser et al. 2008).

There are also image based alternatives which involves identification of image content, but none of them are not very common (Hochheiser et al. 2008). While an image based alternative might be better for reading impaired, it is not for the visually impaired. Because of the accessibility barriers using CAPTCHAs, the W3C note advocates to consider the use of other and alternative methods of limiting spam (May 2005). They suggest that use of biometric technology in conjunction with single sign-on services may be more accessible. However biometric systems will also have to take into account that not all people have the same physical capabilities.

Biometrics

Biometric authentication such as fingerprint scanning, retina scanning or voice recognition systems might be considered feasible 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

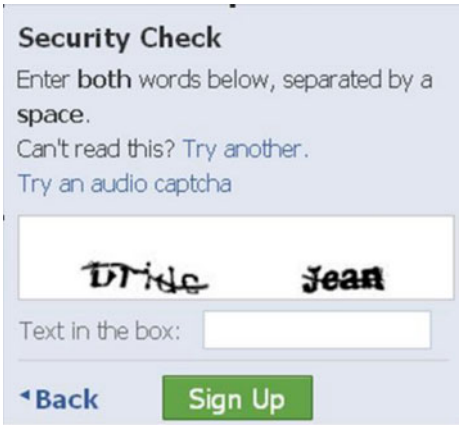

Fig. 5 Facebook offers both text based and audio based CAPTCHAs. (www.facebook.com)

proximity. Elderly users suffering from conditions like Parkinson's disease might not be able to keep the finger still long enough for a successful scan. Finally, there are people with no fingers. A blind person might have major objections in providing electronic signatures authenticated by a fingerprint when they cannot see the system or information 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.

Summary of challenges for inclusive authentication

There are several problems with authentication methods and some examples of alternative authentication technology have been presented above. Common authentication methods include passwords and PINs, tokens, biometry, smart cards, and 3rd-party channels such as one-time codes from tokens or code generators.

Figure 6 below roughly illustrates accessibility challenges of such mechanisms for various user groups. OK means that the method is accessible, NO means that it is not or less accessible.

The figure shows, for example, that authentication procedures that require passwords may lead to major problems for people with poor literacy and/or dyslectic people. Physically impaired people may have problems in entering strong passwords which require special key-combinations. Text CAPTCHAs are less accessible for many groups of disabled people. As described earlier, visual CAPTCHAs are a major problem for users who are visually impaired, or have a learning disability. Number tokens such as PIN-codes are not well suited for users with reduced memory or people who are dyslectic or have problems with handling numbers (dyscalculie). If the numbers are represented visually they will represent problems to visually impaired people. For each of the various authentication methods, it is necessary to consider usability and accessibility issues for the various user groups. Biometrics could be a solution for many of these problems, 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. Even if some alternatives exist it is a challenge in how to handle the alternatives. An inclusive IDM approach takes into consideration that users have different physical and mental capabilities, and that

Method	Feature	Visually impaired	Hearing impaired	Physically impaired	Cognitively impaired	Dyslexia
Passwords	Text token	OK	OK	no	no	no
Text captchas	Disturbed text	no	OK	no	no	no
Smartcards	Small card with chip; card reader	no	OK	no	no	no
Number tokens	Challenge - response	no	OK	no	no	no
Fingerprint scanning	Small scanner	no	OK	no	OK	OK
Voice recognition	Microphone on computer system	OK	no	OK	OK	OK

Fig. 6 Accessibility challenges and authentication mechanisms

these change over time. This calls for universally designed IDM solutions that can provide alternative authentication mechanisms to specific types of users in a usable and accessible manner. In order to present each user with a suitable interface, some kind of profiling may be utilized. This is discussed in the next section.

Profiling & privacy risks

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

Profiling

Profiling has been defined as "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 (e.g. use of data mining techniques to establish general, abstract profiles of a group), and personalized profiling which is focused on in this article.

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 and Wall 2004).

The use of profiling techniques poses a challenge to existing anonymisation techniques, which mostly aim at avoiding profiles (Fritsch 2007). However, in the area of e-inclusion, profiling might have positive effects on system usability, as we discuss in the section below.

Personalized profiles and individual needs

E-inclusive systems may process personalized user profiles that model disabilities, cognitive requirements and personal preferences. 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 is a collection of the user preferences and data. This particular approach to personalization resonates well with the Universal Design principles mentioned in 2.2. For example, UD principle 2 states that the system should accommodate a wide range of individual preferences and abilities, and the UD principle 3 and 4 are about how the system should be easy to understand and that information should be communicated effectively, regardless of the user's experience abilities. The UD principles aim to support the development of systems that can be accessed and utilized by all users regardless of the user's cognitive, physical or sensory characteristics. Thus pursuing a Universal Design approach might mean

developing solutions that are 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 users on request, rather than an enforced design feature.

Personalized profiles might be particularly valuable for e.g. novices, elderly, visually impaired or people with cognitive disabilities, as they often have needs that are not satisfied by simply implementing standardized accessibility guidelines and solutions. As indicated before, this is not a tiny minority but rather the majority of computer users. Current accessibility guidelines are typically directed towards an average user with a desktop computer (Cremers and Neerincx 2004). They do not take into account that people have various devices and often will require targeted, specific type of support. Personalized and adaptive systems that utilize profiles may be able to better support each individual users needs by:

- **Filtering out the irrelevant information** (reducing cognitive load), by delivering this information at the right time (just in time); For example: for various groups such as novices, elderly and cognitively disabled 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 the user** (taking into account the physical, sensory and cognitive characteristics of the user); For example: a user interface designed to meet requirements of dyslectic, language impaired or foreigners, could utilize explaining symbols and illustrations, while a system designed for blind people must be usable with screen readers (meaning that it must be usable in a text only mode without symbols and illustrations).
- By proposing **strongly 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.[2]

In order to succeed in supporting various user groups, use models must be developed and often also a profile for each group should be defined (novices, elderly, children, physically, sensory or cognitively disabled etc.). As noted in the FIDIS project, there are actually few examples of projects and products, even R&D prototypes that provide adaptive, personalized, profiles for people with disabilities. 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

[2] See also FIDIS D7.2: Descriptive analysis and inventory of profiling practices" p 33.

the needs of the user based on input data from the user herself in combination with analysis of the user's interaction pattern.

Identity management with respect to individual 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 for a service or for 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 disabled 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 (Fuglerud et al. 2009).

While some explicit modelling of disabilities, special input or output equipment must be configured to systems, disabled users may prefer not to be discovered as disabled. 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 malicious people might render such for a unusable. Here, too much anonymity might hurt the purpose of the service (Herring et al. 2002). Various new topics in handling identities of different user groups, such as disabled 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 "Erreichbarkeits-manager" (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 and Gerd Tom Markotten (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. anonymising 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 and Van Herreweghen (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.

Discussion

Our aim in this article is advocacy of universal design of identity management technology. Based on the traditional development of information technology, we illustrated the shortfalls of technologies for access control, authorization, authentication, profiling and user-controlled identity management with respect to the inclusion of various user groups, such as disabled. The topical area blends three major communities: Information technology (including identity management and information security), accessibility (focused on usability and interoperability with

assistive technology) and policy makers (promoting the e-society, pursuing standards and laws concerning e-inclusion, equal opportunities, and subsequently motivating market players to implement them).

With respect to the policy implemented in the European Union, the i2010 Policy Support Program provided a targeted initiative for the advancement of e-inclusion in Europe. However, its explicit focus on web accessibility and web-based applications channelled EU support into the application of W3C's WAI guidelines. In today's ICT world of e-government, e-learning, mobile phones, vending machines, RFID ambients and ICT based media distribution and consume, the system access points for users by far leave the perimeter of web based applications. However, the common denominator in these ICT based environments is the identity management problem area. All systems need to handle and process electronic identities of various security degrees. For many such applications, no participation is possible without using electronic identifiers. The lack of IDM schemes that show sufficient flexibility to accommodate the needs of various user groups and support of various technologies (such as different end-user terminals with or without assistive technology), will exclude many citizens from the information society.

Research and innovation in this area is a challenging task. Inclusive identity management requires collaboration of various disciplines with diverse scientific traditions, unique methods of practice, and non-overlapping expectations about what constitutes a research result. Technical and engineering communities with their respective approaches of design and implementation of a single solution collide with the ethnography-based focus of accessibility research and e-inclusion research stakeholders. In addition, the socio-economic interests (cost of ownership, deployment cycles, and size of customer bases) are complicating the real-world deployment of accessibility solutions. An interdisciplinary research framework spanning all involved disciplines, their traditions, metrics and innovation strategies must be defined to involve a variety of approaches, ranging from ad-hoc-prototyping to long-term research based on metrics for accessibility, usability and information security.

The following section summarizes some of the particular challenges of the three types of identity management systems.

Further research challenges

Several research and development challenges arise from the material presented in this article.

First, accessible and usable authentication methods for everybody have yet to be specified. There is a need for taxonomy and metrics of inclusive authentication: The outline of accessibility and security levels of authentication methods as sketched in Table 1 needs to be elaborated into a taxonomy of authentication methods from the e-inclusion perspective. Also, standardized ways of evaluating authentication with regard to usability and accessibility would speed up testing, certification and evaluation of authentication methods with regard to e-inclusion. Such metrics should measure security levels as well as accessibility and usability levels. Furthermore, as discussed above, e-inclusive systems very likely need adaptive security measures with several channels. A single authentication method will always exclude some user groups. Development work

should be put into the design of authentication methods that contain several channels, modalities and adaption options for various user needs. Additionally, changes in the user interface and usage procedures may not be made too fast to prevent user exclusion. Many authentication methods should be personalised and adapted in order to meet the individual needs of each user. This holds for server-side authentication functions as well as for tokens or other technology on the user side.

Second, issues pertaining to profiling are important from an interdisciplinary IDM research perspective. Some issues are in common with general profiling. Profiling (group profiling and personalized profiling) can in several ways be valuable for people with disabilities. However, it is clear that extensive use of group profiling can be used to exclude rather than include people with disabilities; or profiles could be used for economic exploitation e.g. in price discrimination or impulse shopping. Also, personalized profiles require use of personal data that are sensitive. Furthermore, extensive use of personalized profiles may lead to process of proliferation of personal data that come out of control. Finally, personalized, cognitive profiles may require sensitive medical data (e.g. type of cognitive disability) about persons that are not aware that their data are used and are not likely to stand up for their right for privacy or medical or disability related privacy. 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 for research of information systems for e-inclusion and adaption that minimize the need for storing personal (dis)ability profiles.

Third, IDM with respect to individual needs, this is the type 3 IMS. The idea of user-controlled identity management systems raises a number of issues, but in identifying research challenges, two aspects seem crucial: 1. the notion of adaptive, user-profiling information systems, and 2. the usability and accessibility of user-controlled identity management.

Adaptive information systems need knowledge about users in order to adapt. A Braille terminal will always request information in plain text, while a cognitively challenged person may be observable within a session as having a higher error rate and slower response rate than the average user. To provide inclusive, adaptive systems with such information, it cannot be effectively removed from the systems. A common strategy in such situations is the effort to anonymise 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, users could be grouped into larger segments of needs or type of disability. 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 different (dis)ability groups 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 end user groups has yet to be done.

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 and Dusseault 2008). Such complexity might confuse even users without disabilities. For example, Petterson 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

The article has argued for a change of perspective in identity management (IDM) research and development. Societal and technological changes spur rapid growth and expansion of the use of electronic identity management systems. All citizens, also disabled persons, are required to use the systems. The article shows that accessibility and usability issues affect identity management in a way and to an extent that demands a reframing and reformulation of basic designs and requirements of modern identity management systems. The traditional design of identity management systems and mechanisms has focused exclusively on security concerns as defined in the field of security engineering. By default, the highest security level has been recommended and implemented, often without taking end-user needs and accessibility issues into serious consideration.

The article has provided a conceptual framework for inclusive IDM, a brief overview of the regulatory status of inclusive IDM. An overview and taxonomy of authentication methods with respect to accessibility and usability was presented. We assert that there is no single authentication method that can be used by all users, and that alternative methods are needed in order to include various end-user groups with different skills, different age and various (dis)abilities. A number of widespread IDM approaches, methods and techniques are analyzed and discussed from the perspective of e-inclusion.

Several important challenges—in particular related to inclusive authentication methods, profiling and adaptive IDM supporting each individuals needs, are identified and some ideas for solutions addressing the challenges are proposed and discussed.

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.

Open Access This article is distributed under the terms of the Creative Commons Attribution Noncommercial License which permits any noncommercial use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.

References

Adams A, Sasse MA. Users are not the enemy: why users compromize computer security mechanisms and how to take remedial measure. Commun ACM. 1999;42(12):41–6.

Ahn LV, Blum M, Langford J. Telling humans and computers apart automatically. Commun ACM. 2004;47(2):56–60.

Babu R, Singh R. Understanding blind users' accessibility and usability problems in an online task. Fifteenth Americas Conference on Information Systems. San Francisco, California, USA; 2009.
Braz C, Robert J-M. Security and usability: the case of the user authentication methods. Proceedings of the 18th International Conference of the Association Francophone d'Interaction Homme-Machine. Montreal, Canada, ACM; 2006.
Camenisch J, Van Herreweghen E. Design and implementation of the idemix anonymous credential system. Zürich; 2002.
Cen/Cenelec. CEN/CENELEC Guide 6. Guidelines for standards developers to address the needs of older persons and persons with disabilities. 2002, January.
Cremers AHM, Neerincx MA. Personalisation meets accessibility: towards the design of individual user interfaces for all. In: Stary C, Stephanidis C, editors. User-centered interaction paradigms for universal access in the information society, UI4All 2004. Vienna: Springer-Verlag; 2004.
Cud. Principles of universal design, the center for universal design, North Caroline State University. 1997. http://www.design.ncsu.edu:8120/cud/univ_design/princ_overview.htm. Accessed: 10 January 2009.
Dhamija R. Dusseault L. The seven flaws of identity management: usability and security challenges. 2008. p. 24–29.
Ec. Social inclusion, better public services and quality of life, The European Commission. 2005–2010. http://ec.europa.eu/information_society/eeurope/i2010/inclusion/index_en.htm. Accessed: April 2008.
Ec. June 2006—Riga Ministerial Conference—"ICT for an inclusive society", European Union. 2006. http://ec.europa.eu/information_society/activities/einclusion/events/riga_2006/index_en.htm. Accessed: April 2008.
EC10550. Information note 10550/09 - SOC 380 from The Commission to COUNCIL (Employment, Social Policy, Health and Consumer Affairs): Report from the High Level Group on Disability on the implementation of the UN Convention on the Rights of Persons with Disabilities- Information from the Commission. Brussels, 4 June 2009
Edean. Legislation & standards, European design for all e-accessibility network. 2009. http://www.education.edean.org/index.php?row=1&filters=f6. Accessed: 14. Dec. 2009.
Eiao. European internet accessibility observatory. 2008. http://www.eiao.net/. Accessed: Dec 2008.
Engelen J. Report on standardisation and DfA. Leuven: Kath Univ; 2007.
Fidis. FIDIS deliverable D3.1: structured overview on prototypes and concepts of identity management systems (15. September 2005). 2005a. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf.
Fidis. FIDIS deliverable D7.2: descriptive analysis and inventory of profiling practices. 2005b.
Fritsch L. State of the Arth of Privacy-enhancing Technology (PET)—deliverable D.2.1 of the PET Web project (Report: 1013, 22-nov-2007). Oslo: Norsk Regnesentral; 2007.
Fritsch L. Profiling and location-based services. In: Hildebrandt M, Gutwirth S, editors. Profiling the European Citizen - Cross-Disciplinary Perspectives. Dordrecht: Springer Netherlands; 2008. p. 147–160.
Fuglerud KS. Universal design in ICT services. In: Vavik T, editors. Inclusive buildings, products & services: challenges in universal design. Trondheim, Norway; 2009. p. 244–67.
Fuglerud KS, Solheim I. Synshemmedes IKT-barrierer. (Eng: ICT-barriers for the visually impaired) (March 06, 2008) Oslo: Norwegian Computing Center, s. 91. 2008. http://www.nr.no/pages/dart/project_flyer_synshemmedes_ikt_barrierer.
Fuglerud KS, et al. Universal design of IT-based solutions for registration and authentication. (Jan. 31, 2009) Oslo: Norwegian Computing Center; 2009, s. 60, http://publ.nr.no/4975.
Giannakouris K. Population and social conditions: ageing characterises the demographic perspectives of the European societies eurostat. 2008.
Gibbons M, et al. The new production of knowledge: the dynamics of science and research in contemporary societies. London: Sage; 1994.
Halbach T. Dokumentasjon av UNIMOD-innloggingsprototypen (Eng: documentation of the UNIMOD login prototype) (April 28, 2009) Norsk Regnesentral, s. 40, 2009.
Halpert BJ. Authentication interface evaluation and design for mobile devices. Information Security Curriculum Development (InfoSecCD)Conference '05. Kennesaw, GA, USA., September 23–24. 2005.
Hellman R. Accessibility of eServices on mobile phones. IADIS International Conference e-Society 2008. Algarve, Portugal. 2008. 9–12 April 2008.
Herring S, et al. Searching for safety online: managing "trolling" in a feminist forum. Inf Soc. 2002;18 (5):371–84.
Hochheiser H, Feng J, Lazar J. Challenges in universally usable privacy and security. Symposium On Usable Privacy and Security (SOUPS) 2008. Pittsburgh, PA, USA; 2008.

Huang M-H. Unequal pricing in the information economy: implications for consumer welfare. J Bus Ethics. 2005;56(4):305–15.
Jaeger PT. Beyond Section 508: the spectrum of legal requirements for accessible e-government web sites in the United States. J Gov Inf. 2004;30(4):518–33.
Jameel H. Taxonomy of human identification protocols Korea: U-security Research Group, Ubiquitous Computing Laboratory, Kyung Hee University. 2007. http://uclab.khu.ac.kr/usec/taxonomy/hassan.pdf.
Jameel H, et al. 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; 2007.
Jendricke U, Gerd Tom Markotten D. Usability meets security—the identity-manager as your personal security assistant for the internet. New Orleans, Lousiana, USA; 2000.
Koelsch T, et al. Privacy for profitable location based services. Vol. 3450. Boppard, Springer; 2005. p. 164–79.
Kohlweiss M, Gedrojc B, Fritsch L, Preneel B. Efficient oblivious augmented maps: location-based services with a payment broker. In: Borisov N, Golle P, editors. Privacy enhancing technologies, 7th International Symposium, PET 2007 (LNCS 4776), vol. 4776. Berlin: Springer; 2007. p. 77–94.
Kuutti K. Design research, disciplines, and new production of knowledge. International association of societies of design research. Emerging trends in design research. Hong Kong; 2007, 12–15 November.
Lazar J, et al. What frustrates screen reader users on the web: a study of 100 blind users. Taylor & Francis; 2007. p. 247–69.
Levi M, Wall DS. Technologies, security, and privacy in the Post-9/11 European information society. J Law Soc. 2004;31:194–220.
May M. Inaccessibility of CAPTCHA. Alternatives to visual turing tests on the web (23 November 2005) W3C Working Group Note, work in progress. 2005. http://www.w3.org/TR/turingtest/.
Mikovec Z, Vystrcil J, Slavik P. Web toolkits accessibility study SIGACCESS. 2009(94):3–8.
Petrie H, Kheir O. The relationship between accessibility and usability of websites. Proceedings of the SIGCHI conference on human factors in computing systems. San Jose: ACM; 2007.
Pettersson JS, et al. Making PRIME usable. Proceedings of the 2005 symposium on usable privacy and security. Pittsburgh: ACM; 2005.
Reichenbach M, et al. Individual management of personal reachability in mobile communication. London: Chapman & Hall; 1997. p. 164–74.
Schmidt A, et al. Enabling access to computers for people with poor reading skills. In: Stary C, Stephanidis C, editors. 8th ERCIM workshop on user interfaces for all. Vienna, Austria, Springer-Verlag Berlin Heidelberg; 2004, June 28–29.
Solove D. A taxonomy of privacy: GWU Law School Public Law Research Paper No.129. Univ PA Law Rev. 2006;154(3):477.
Steg H, et al. Europe is facing a demographic challenge ambient assisted living offers solutions (March 2006) VDI,VDE,IT; 2006.
Stevenson B, Kolko J. Accessible technology in computing—examining awareness, use and future potential. A Research Study Commissioned by Microsoft Corporation and Conducted by Forrester Research inc, s. 58. 2004. http://www.microsoft.com/enable/download/default.aspx#research.
Stevenson B, Mcquivey JL. The wide range of abilities and its impact on computer technology. A Research Study Commissioned by Microsoft Corporation and Conducted by Forrester Research inc, s. 24. 2003. http://www.microsoft.com/enable/research/default.aspx.
Tari F, Ozok AA, Holden SH. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. Symposium On Usable Privacy and Security (SOUPS). Pittsburgh, PA, USA; 2006.
Udjus L. "Gjør døren høy—gjør porten vid". Offentlige elektroniske tjenester for alle. (Eng: "Make the door high—the gate wide". Public electronic services for all.), Stat og styring. 2007.
Whitten A, Tygar JD. Usability of security: a case study (Report: CMU-CS-98-155, December 18) Carnegie Melon University, Pittsburgh, PA 15213, USA, s. 39. 1998.
Wsc. Web security context Working Group home page. 2006. Last updated: 14. Oct. 2009, http://www.w3.org/2006/WSC/. Accessed: 14. Dec. 2009.
Zibuschka J, et al. Privacy-friendly LBS: a prototype-supported case study. Colorado: Keystone; 2007.
Zubal-Ruggeri R. Making links, making connections: internet resources for self-advocates and people with developmental disabilities. Intellect Dev Disabil. 2007;45(3):209–15.
Zurko ME, Johar K. Standards, usable security, and accessibility: can we constrain the problem any further? Symposium On Usable Privacy and Security (SOUPS) 2008. Pittsburgh, PA, USA; 2008.