e-Me – inclusive identity management in new social media

1.   Relevance for the Verdikt-call

The overall objective of the e-Me-project is to provide new knowledge that can significantly improve the usability and accessibility of identity management (IDM) and authentication mechanisms in new social networks without compromising privacy, security or offending legal frameworks. The e-Me-project addresses IDM challenges related to the key Verdikt-themes social networks and mobile internet systems, with a focus on accessibility and inclusion issues and challenges in the emerging research field *inclusive identity management* (IIDM) [19]. Inclusive identity management is one of the most critical issues of the new internet, seen from all perspectives: users, providers and policy makers. In order to use electronic services, user often must be authenticated and their user accounts must be managed. A basic requirement for accessible systems is therefore that IDM-methods can be used by a broad range of users, with different skills, ages, and different (dis)abilities.

The projects aims at advancing knowledge in the above-mentioned field by (1) studying the changing role of identity management in the context of increasingly pervasive social networks, which, in turn, offer a basis for (2) developing and evaluating demonstrators in specific case areas, in order to pave the way for accessible, privacy-enhancing IIDM-solutions in social networks and mobile internet systems. The two cases are (a) Social networks in *public service*, the Altinn service, and (b) *Net banking* on smart phones.

Recent developments underscore the increasing societal and commercial significance of identity, privacy and identity management issues in new social media:

- Social networks and Web 2.0 put the user in the centre of service offerings – not least in terms of user identification (authentication) and secure access authorization across multiple services.
- Social networks are rapidly transforming *from mainly* means for *informal* communication between individual persons and social groups, *towards* including also the *more formal* modes of communication and even commercial service production, in which secure and trusted IDM-solutions are crucial. (Figure 1).

Figure 1: Transformation of social networks into integrated services.

- The borders between marketing and social networking are blurred in ways that challenge privacy concerns as well as the non-commercial sharing and peer-to-peer communication culture of the traditional internet-based social networks.
- With the ever-increasing popularity of smart phones and 3G-access, IDM becomes a critical issue both for users and providers in the mobile industry. Large communication providers are "coming to realize that the key to monetizing this access is identity management", as put by Nokia Siemens Networks [41]. Accessible and user-friendly IDM-solutions will therefore be crucial because these qualities are crucial for the core business, and increasingly so.
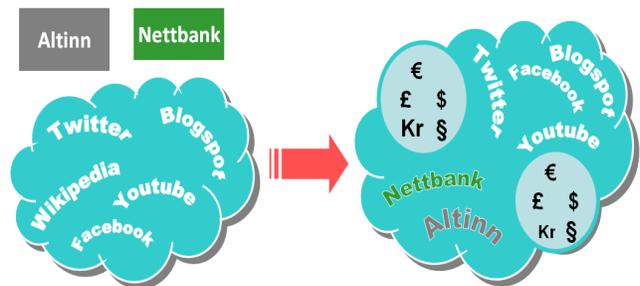
In this project the applied research focus is on the accessibility challenges for various disabled groups, which is important in its own right, but our experience is also that this focus provides valuable test environments and user experiences that shed sharp light on accessibility and usability challenges in general. Users with disabilities are continuously confronted with barriers to use everyday ICT-products and -services [10].

The first barrier is often registration and authentication. 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 2 illustrates some which can be difficult or even impossible to use for many. Studying these barriers provides insights that are relevant for all types of users.

Figure 2: Various identification and authentication mechanisms.

2.   Aspects relating to the research project

2.1   Background and status of knowledge

Social networks and Web 2.0 are making a powerful entrance to the ICT-scene. The number of users grows fast and, at the same time, identity management is becoming increasingly important and indispensible for most ICT users.

Connected to these developments, there are several main concerns which inspire and justify the e-Me-project. Generally, there is the concern of excluding large user groups (e.g. people with disabilities) from the use of social networks and Web 2.0 because of low usability and accessibility of these. Low usability of *IDM-systems* has been found to be a major source of flaw and risk [1, 7, 13, 26, 35, 55]. Moreover, research by others [30] and our team [19, 21, 22] shows that IDM systems are inaccessible to many, in particular to users with disabilities and elderly. Understanding the IDM challenges of disabled users provides a clue to understanding accessibility IDM challenges in general.

Furthermore, "virus-writers" are increasingly targeting social networking sites and other Web 2.0 technologies (e.g. Twitter and instant messaging services from Google, AOL etc.). "Virus-writers" are creating fake profiles of known people, friends or business associates hoping that people will link with them. Users are tricked into linking to the fake profiles, which can be loaded with various forms of malicious software. Myspace, Facebook, LinkedIn, and other social networking tools are becoming the target of an increasing number of phishing and criminal activity. Many users fall for these attacks, hand out personal information, and risk personal identity, privacy and data. Identity theft is also on the rise. Electronic identifiers are vulnerable to identity theft [39], identity spam and various other security challenges [37]. Personal information and user profiles are referenced with such identifiers, e.g. a social security number. Also, when deciding whether to disclose personal information users weigh the concerns of giving up information privacy against the benefits of information disclosure [36, 51]. However, they do not necessarily understand what this may add up to.

As a consequence, secure and trusted IDM solutions are crucial. Therefore, it is unavoidable to include systems and devices for identification and authentication to social networks and Web 2.0. Here, we meet the usability and accessibility challenge. For example, login procedures requiring passwords can lead to problems for dyslexic people. Similarly, image authentication such as captcha-code [2, 34, 40] is a barrier for vision-impaired users. In addition, assistive technologies and measures for ICT-related security may arrive in direct conflict with each other: If third-party software, such as Braille or audio screen readers, can hook into authentication mechanisms, then malicious programs could mask as assistive technology and compromise authentication information and thus violate the security of the user [33].

User-controlled identity management tools are suggested as a response to the need to handle an ever increasing number of identities in new digital services [19]. Some approaches and prototypes of user-controlled identity management exist [9, 35], but usability experts warns about exposing the user to such high degrees of complexity, while users seek to get things done with the least possible effort [13]. Such complexity might confuse even users without disabilities [47] An inclusive IDM approach must take into consideration that users have very different physical and mental capabilities, and that these change over time [27].

By universal design (UD), all potential users with different skills, knowledge, age, gender, (dis)abilities and literacy, can be included. A central issue in universal design of ICTs is flexible multimodal user interfaces (UI) that can meet different users' needs, abilities, situations, preferences and devices [20, 28, 29, 31, 48, 50]. Systems that can adapt to users needs and preferences are called for. However, adaptive, dynamic profiling systems introduce new privacy threats. As [38] argues, profiling and personalization have privacy implications; user profiles contain sensitive information about a user's preferences and (dis)abilities. Universally designed systems' privacy requirements transcend normal privacy concerns, due to profiling of possible sensitive and disability-related information about the users. This could be misused, as pointed out by [32] and [54]. Hence, there is a need for research about privacy-enhancing technology (PET) [18] and privacy-preserving IDM-technologies that can be deployed in universally designed ICTs.

Social networks, web 2.0, dynamic profiling and personalization also raise legal questions regarding privacy and regulation, and question how systems should be designed and function in order to comply with the Data Protection Act [5, 46]. It is important that e-Me has law experts as partners that will explore legal and privacy issues and also safeguard full compliance with relevant legal regulations.

To include all users in the different arenas of the e-society, we must add usability and accessibility to IDM-systems, i.e. to develop IIDM. This challenge is about to become increasingly important when social media and Web 2.0 expand to include sensitive information and formal transactions. The e-Me-project's ambition is to make scientific contributions to the intersection of the above-mentioned areas.

2.2   Approaches, hypotheses and choice of method

In short, the objective of the e-Me-project is to provide new knowledge that significantly improves the usability and accessibility of IDM-systems and authentication mechanisms in new social networks without compromising privacy, security and legal frameworks. The e-Me-project aims at developing prototypes to explore borderlines between public, commercial and private information and to show how inclusive and universally designed IDM solutions can be realised. In order to manage this work, we have developed three guiding research **hypotheses**: These are: (H1) For different security and privacy levels, it will be possible to select a small, but sufficient number of complementary authentication mechanisms that will cover the needs of most users (ideally all). (H2) The use of multimodal user interface element can remarkably increase the accessibility and usability of ICT-based authentication and IIDM-solutions. (H3) It is possible to personalize and adapt the user interface of IIDM-systems to each user's preferences and needs without compromising legal frameworks or the users' privacy.

In order to meet the objectives and goals of the project, the hypotheses have to be combined with realistic research challenges. In order to achieve user-controlled IIDM in the context of converging Web 2.0 and social networks, following challenges will be addressed in the e-Me-project's multidisciplinary "heart":

Challenge 1: User-centred approaches to IIDM
(1.1) Development of appropriate methods for user-centred requirements specification, and usability and accessibility evaluation in the field of IIDM and social media. (1.2) Development and application of IIDM-demonstrators as a design language for interaction between users and scientists. (1.3) Assessment of usability and accessibility of technical IIDM-solutions vs. principles of universal design.

Challenge 2: Profiling and privacy
(2.1) Development of frameworks promoting personalization (user models and user profiles) of social media and IIDM for users with and without disabilities. (2.2) Exploring how universally designed and multimodal approaches to IIDM may enhance the participation in and usefulness of social networks. (2.3) Analysis of the potential and risks of the developed IIDM-technologies.

Challenge 3: Legal issues in IIDM
(3.1) Mapping and analysis of possible challenges in existing legislation related to the development of requirements for IIDM. Emphasis will be on data protection and information security regulations. (3.2) Formal studies regarding how IIDM-related login and authentication procedures may be designed and function in harmony with legal requirements.

The knowledge needed to answers to these challenges is not achievable by just bringing pieces of knowledge produced by different disciplines together, but by integrating them [23]. The e-Me research group comprises broad expertise which can be grouped into three main research fields, security/privacy, legal and human-computer interaction (HCI) research. Researchers within these disciplines may have quite different views and perceptions of knowledge production and what methods and approaches to use [42]. A mixture of quantitative and qualitative/interpretative methodologies as deemed appropriate by the different disciplines is selected as described below. In order to lay the ground for fruitful collaboration, the research group will discuss the underlying assumptions in each discipline. The research in e-Me will be centred around development of demonstrators within two cases. A common framework for sharing and analyzing the results within the interdisciplinary group will be established and will be regularly evaluated and discussed throughout the project.

Scientific work close to users is central from an HCI perspective. User requirements are to be acquired, user-centric demonstrator development will be conducted, and extensive user-tests will be executed – all with accessibility and usability in mind. Usability and accessibility studies in the requirements specification
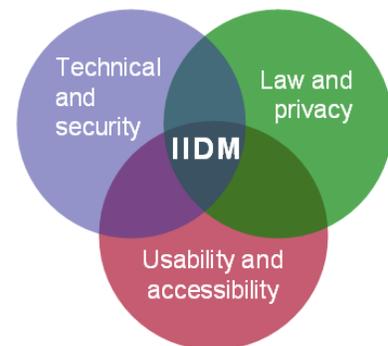
phase of IIDM rely on several qualitative methods [4, 6, 24, 56] with profound user involvement. These methods will give detailed information about diverse users' needs and requirements of accessible IIDM from a diversity of users. Through several previous research projects, we have established close cooperation with three NGOs. They will help us to get into contact with users who can challenge the established solutions, namely users with a variety of disabilities (cf. Chapter 2.3.4). These NGOs will be involved throughout the project.

The methodological approach within the area of security research is composed of privacy risk assessment [22] and multilateral security analysis [38]. Within the area of law and privacy, legal studies will be performed, such as mapping and analysis of legal issues related to privacy and other areas of legislation. In order to define a base-line, a structured survey (questionnaire) among public bodies and private companies offering Web 2.0 and social network services will be conducted, focusing on security, privacy and ethical issues.

Finally, in order to demonstrate possible new solutions according to the hypotheses H1-H3, we will build IIDM-demonstrators and conduct field trials and testing in our usability laboratories. Two cases frame the demonstrators:

Case 1: *Internet banking*, in collaboration with Encap and Storebrand bank. The company Encap is an innovative provider of authentication technologies for mobile phones, used by Storebrand Bank, among others. Web 2.0 providers may provide potential access to a broad variety of new services, but the IDM mechanisms are often a bottleneck and high threshold for many users. In this case we will experiment with IIDM mechanisms and organisation that may provide improved access, user control and more personalized banking services in social network settings on a mobile platform. Researchers in the e-Me project have in a previous, recent project [21] studied and evaluated the Encap's and Storebrand Bank's IDM-solutions and the e-Me experiments will benefit from this work.

Case 2: *Front end public service*: Brønnøysund (BRREG) is the major Norwegian government provider of public computerised registers. In the e-Me context BRREG is aiming at exploring how the agency can utilize Web 2.0/social networks as a means for improving public service quality and public access. Experiments will be set up aiming, in the context of the comprehensive, national Altinn-system, to explore how social networks can be applied in novel ways by BRREG executive officers in developing new and personalized approaches to IDM, with impacts on the overall service production. Researchers in the e-Me project have in a previous, recent project [25] evaluated the existing solutions, but also developed and implemented alternative, more accessible IDM (log-in) procedures to Altinn. This is beneficial for the planning of the e-Me experiments.

Building [27] and experimenting [4,33] with first paper demonstrators [53], and then programmed demonstrators which evolve through several iterations using a model of rapid prototyping and frequent evaluations.

2.3 The project plan, management, organization and collaboration

2.3.1 The structure of the project

The e-Me-project will be conducted as a set of 6 clearly defined modules. The partners' roles in the modules are presented in the table on p. 6. Below, a description of each module:

Module 1: Inclusive Identity Management: user challenges and accessibility conditions
Goals: To identify user challenges and needs, and asses the status of accessibility in IDM-technology and frameworks. The main research activities will be:

- *User studies*: Comprehensive user studies, quantitative and qualitative, of disabled users' experience and challenges facing IDM systems and authentication mechanism in social media. What are the actual accessibility problems? What is the magnitude of the problem? How do the problems affect their access to ICT and the information society in general? Both personal interviews and questionnaires will be carried out. Questionnaires will be sent to members in the participating user organizations. Explorative interviews with approximately 30 disabled persons from various groups will be carried out. We will collaborate with the user organization in recruiting test users. The user groups will comprise primarily dyslectics, frail elderly and visually impaired people.

- *Defining typical user profiles.* Based on user studies, a set of realistic user profiles will be produced. They will represent persons with accessibility problems related to individual characteristics within the three areas of motor, sensory and cognitive (dis)abilities.

The *main products* of the module will be: (1) in-depth knowledge about IDM and accessibility and usability challenges, (2) user-generated requirements for inclusive IDM, and (3) user profiles emerging from the user studies.

Module 2: Privacy, security and legal frameworks
Goals: To Propose IIDM solutions in 100% compliance with relevant regulations.
The main research activities:
- *Mapping of relevant legal sources*, general analysis of regulations and other sources, analysis regarding concrete IIDM solutions in particular pursuant to i) the Data Protection Act and ii) specialised legislation regulating areas with high influence on peoples' welfare and participation in society (e-Government, banking etc.
- *Security in inclusive IDM.* Description of state-of-the art in the field of inclusive IDM from a technical security point of view, identify research challenges in the cross section between accessibility and security, and suggest how these challenges shall be addressed in the e-Me modelling work and demonstrator development.
- *Gap analysis*: We will analyse the relation between accessibility laws, and standards on the one hand and the realities of IDM, standards and regulations on the other hand. The analysis will engage all research fields and disciplines.

The main products of this module are analysis of various fundamental legal and security aspects that are crucial as prerequisites for further work in the project, and for the understanding of the societal and technological context of inclusive IDM in general.

Module 3: Modelling inclusive and personalized IIDM technologies in new social networks
Goals: To develop, define and validate functional and technical requirements for universally designed and inclusive interfaces to identity managements systems in social media.
On the basis of the results from Module 1 and Module 2 the following research activities will be carried out:
- Definition of functional and technical requirements for demonstrators of universally designed and accessible multimodal interfaces for authentication that can be accessed and used by all, also by disabled persons.
- Identification and description of usability requirements to accessible inclusive IDM solutions and interfaces.
- Definition of requirements for adaptation mechanisms for personalization and customization based on user profiles.
- Recommendations of usable solutions and approaches of multimodal inclusive IDM solutions for various user groups. Guidelines and contributions to standards in the field of identify management and computer security.

The *main product* of Module 3 will be research frameworks and functional and technical requirements for implementation of demonstrators of accessible, multimodal interfaces to IDM systems.

Module 4: Demonstrator development and evaluation
Goals: To develop demonstrators for the case environments that are applied in exploring and testing the initial hypotheses of the project.
Demonstrator development: In this module a test environment will be established, aiming at developing two dedicated test demonstrators for the two case environments. A portfolio of user-centred methods will be applied, such as personas, user scenarios, paper-prototyping, technical rapid prototyping, usability testing, accessibility testing etc. The demonstrators will be meticulously designed to meet:
- The requirements for a realistic testing of the initial hypotheses of the project.
- The accessibility and usability requirements from Module 2.
- The requirements for adaptation mechanism for personalization and customization based on user profiles.

- The functional and accessibility requirements of the case environment.

Evaluation and testing: There will be a mix of various methods in the evaluation of the demonstrators. Due to the exploratory character of the project, the testing will apply methods in accordance with this. The main method will be end-user-testing and field trials in naturalistic settings, but also laboratory tests of specific aspects and features will be carried out.

The *main outcome* of Module 4 will be new and empirically substantiated knowledge about design of and mechanisms for inclusive and user-controlled IDM in Web 2.0/social networks settings.

Module 5: Networking and outreach

Goals: The main goal of this module is to contribute significantly in the development of the emerging research field of IIDM (inclusive Identity management). An additional goal is increasing public awareness.

The project has defined the goals for publication : 25 scientific, peer-reviewed publications, whereof 10 in academic journals and 15 at international conferences including talks. 10 popular scientific articles in national, professionally targeted journals. 30 national conference/seminar presentations. 1 PhD-dissertation. Web-site. The dissemination plan is described in detail in the electronic application form.

Module 6: Project management (se also Chapter 2.3.3)

Goals: High-quality project scientifically. Timely goal-achievement. Orderly economy and project administration. Project management is described in detail in the next chapter below the table.

Main roles and responsibilities

Module: Partner:	1. IIDM & user challenges	2. Privacy, security & legal frameworks	3. Modelling IIDM	4. Demonstrators & evaluations	5. Networking & outreach	6. Project management
NR	ApR-I	ApR-S	ApR-I	UC, SWD-W, SWD-M, L	AP	PM
Karde	ApR-I		ApR-I	UC	AP, Pdiss	PM
Tellu		ApR-S	ApR-S	SWD-M, L	Pdiss	
Encap		ApR-S	ApR-I	SWD-M	Pdiss	
Informatics	AcR-I		ApR-I		AP	
Computers and Law	AcR-L	AcR-L, AcR-S	AcR-L, AcR-S		AP	
BRREG	Cit-C	ApR-L	Cit-C	Cit-C	Pdiss	
Storebrand	Cus-C	AcR-L	Cus-C	Cus-C	Pdiss	
Seniornett	ApR-I			UC	Pdiss	
Blindeforbund	ApR-I			UC	Pdiss	
Dysleksiforbundet	ApR-I			UC	Pdiss	

Color code:
- **main activity**
- **support activity**

PM = Project Management
AP = Academic Publications
ApR-I = Applied Reseach e-Inclusion
AcR-I = Academic Research e-Inclusion
ApR-S = Applied Reseach Security and Privacy
AcR-S = Academic Research Security and Privacy
AcR-L = Academic Research Law

PDiss = Popular scientific Dissemination
UC = User Contact
Cit-C = Citizen Case (publig electronic services case)
Cus-C = Customer Case (banking case)
SWD-M = Software Development Mobile platform
SWD-W = Software Development Web platform
L = Laboratory facilities

2.3.2 Project management

Project manager will be Dr. Riitta Hellman with long experience form large research projects. (CV attached). Her background from universities, applied research institutes and consulting within universal design and usability will enable her to manage the research work, publishing activities and project administration appropriately. She will distribute the joint budget, monitor the scientific progress and production of results, ensure that the work is of high scientific quality, and take care of all reporting obligations. She will administer and chair the steering committee and the international expert panel. She is responsible of the dissemination planning, and together with the joint academic partners, she will participate in supervising the publication process. Overall quality assurance is the responsibility of hers. Her responsibilities also cover ethical and gender issues. ● All 6 **modules** will be assigned a **module coordinator** to. Module coordinators are responsible of cooperation towards other project modules, and they may accomplish tasks on request from project manager. ● **International expert panel**, comprised of experts from related fields will have no executive role in the project, but will provide an independent assessment of the projects scientific plans and production. The panel will connect the project to international milieus of relevant expertise. (Member list attached.) ● **Steering committee** will be the main decision making body of the project as it comprises a technical representative from the project partners. Each project partner will also

be required to produce progress reports to steering committee. ● **Project participants** are responsible for specific tasks and deliverables within the modules they are assigned, and for undertaking the work in a timely and thorough manner, relying on the newest scientific knowledge in the research field.

2.3.3 International collaboration

The e-Me project will actively participate in the EU's Information Society events for e-Inclusion, e-Government and e-Participation. We will particularly keep an eye on Inclusive e-Government. Within all 3 areas, the EU's expert workshops will be attended. Further, we will submit papers to the yearly eChallenges-conference (http://www.echallenges.org/e2009/) and the SOUPS (Symposium On Usable Privacy and Security) conference (http://cups.cs.cmu.edu/soups/2010/). In addition, e-Me aims at organizing a workshop on inclusive identity management at the SOUPS- conference. One explicit goal of the attendance at these international events is to further develop the international academic contacts within the field. The e-Me-project will support collaborative international paper-writing by hiring guest researchers to stay at NR, and for e-Me researchers to visit a foreign institution. The project has a budget for collaborative paper-writing each year. The main purpose of this is to produce high quality articles in quality conferences and journals. Regarding the scientific plans, methodologies and approaches, the project will consult the expert panel of internationally renowned researchers in relevant areas, such as usability/security (Dr. Lorrie Faith Cranor, who is also general chair in the SOUPS steering committee), accessibility (dr. John Gill), in consumer research (dr. Petteri Repo), and privacy/security (dr. Simone Fischer-Hübner). (Key personnel competences attached). The expert panel will meet ca. once a year. The meetings will, if possible, be co-located with relevant conferences. In addition, we will ourselves make use of social networking order to make the most of the international contacts.

2.3.4 User representation

Three **user organizations** (NGOs) provide e-Me with their unique experience and competence of user needs, and they connect e-Me with test users. **Seniornett** promotes the participation of the elderly in the e-Society. It organizes local senior clubs that are motivating and teaching elderly to use ICT. It is member of ICT50+, an EU-project on adults and ICT. **Norwegian Dyslexia Association** (NDA) is a national organization for persons with functional disabilities related to reading and writing. NDA promotes the interests of the dyslectics in education, work, media and research. **The Norwegian Association of the Blind and Partially Sighted** (NABP) works to achieve equal opportunities and status in society for people with visual impairment, and provides a multitude of special products and services.

2.3.5 Project partners and expertise

The project consortium is designed to provide a focused, high-quality environment for the envisaged interdisciplinary research work. ● **Norsk Regnesentral** (NR) is a research institute in the areas of ICT-security and universal design. NR has long experience in HCI-related issues from national and international projects. NR has a *Visiting Researcher Agreement* with ICT-innovation companies Karde AS and Tellu AS. **Karde AS** is an SME working with ICT and innovation issues (including R&D-project management) through national and international R&D-projects. One area of expertise is ICTs for disabled users. **Tellu AS** is an SME specializing in R&D on mobile services and accessible HCI for mobile applications. Both NR and Tellu AS have *laboratory facilities* which, with additional equipment (allocated in the budget), can be used for demonstrator development and user testing of IIDMs. ● **Institute of informatics** (Ifi) – University of Oslo is the oldest and largest informatics department in Norway with approximately 1500 B.Sc/ M.Sc students and 150 Ph.D-students. Ifi has research groups with expertise on universal design, security and mobile ICTs. The main research areas of the **Norwegian Research Centre for Computers and Law** (NRCCL/AFIN) – University of Oslo are data protection and information security, media law and internet governance, e-Government, legal technology and electronic commerce. Its research on privacy issues and information security is interdisciplinary with emphasis on law. ● The **Storebrand Group** is a company within pensions, life and health insurance, banking and asset management. Storebrand's internet bank is e-Me's *CASE 1*. **Encap AS** provides e-Me with its mobile bank ID-technology for test purposes. Encap won the European Mobile Authentication Technology Innovation Award of the year 2008. The solution is approved as a mobile OTP-mechanism for BankID. The **Brønnøysund Register Centre** (BRREG) is a government body under the Norwegian Ministry of Trade and Industry, and consists of several different national computerised registers. Parts of BRREG's work on Altinn II comprise e-Me's *CASE 2.* ● In addition 3 NGOs as presented in Chapter 2.3.4 on user representation. (Letters of intent and list of key personnel competencies attached).

2.3.6 Fellowships

E-Me's *doctoral* fellowship is allocated at the Institute of informatics (University of Oslo). The *postdoctoral* fellowship is allocated at Norwegian Research Centre for Computers and Law (NRCCL/AFIN, University of Oslo).

2.4 Budget

The project will span over 4 years: 2010-2013, with a total budget of 20,1 mill. NOK. PhD and post doctoral fellowships are included in the budget. The size of the budget reflects the complexity of the problem area, the combination of theoretical and applied research work, development and testing of case demonstrators in laboratories, the interdisciplinary approach to the envisaged scientific work, and finally the broad international collaboration.
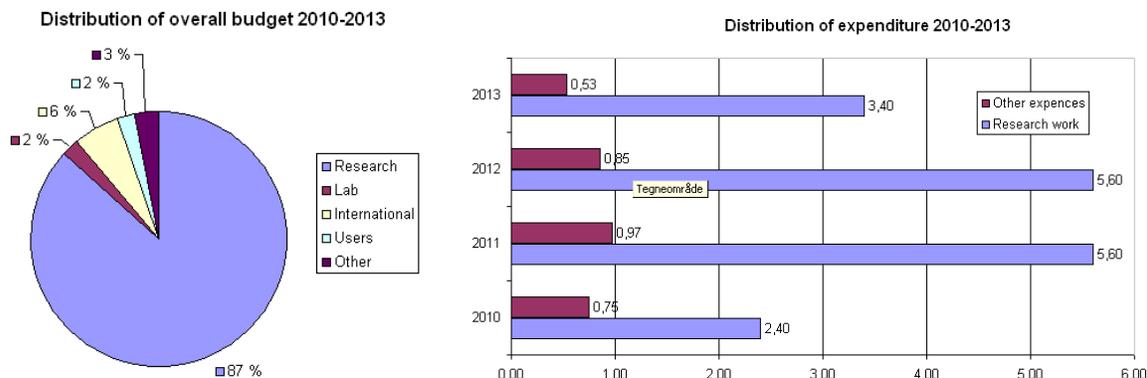
3. Perspectives and compliance with strategies

3.1 Compliance with strategies

NR's long term goal since 2000 has been to achieve international reputation within accessibility research. The primary prerequisite for this has been to conduct a considerable amount of fundamental research of our own origin. The recent projects UNIMOD (Verdikt) and DIADEM (EU) are examples of this. The second one is that the research group working with e-Inclusion and e-Accessibility will develop into a clearly international research unit for scientists on both postgraduate and postdoctoral level. Several researchers with international background have joined NR during the last years. The third one has been that the research carried out by our research group also has a clear relevance to practical use. We anticipate that all these three premises have been well advised with respect to the research objectives and tasks chosen for the e-Me project.

3.2 Relevance to society

As shown in Chapters 1 and 2, this project addresses one of today's most important societal challenges: inclusion of all in the continuously evolving information society. People with disabilities in Europe continue to be confronted with many barriers to use of the everyday ICT products and services [10]. Weak or missing accessibility to electronic services is a key obstacle. Thus, one of the most important policy areas of this decade within ICT-trends has become e-Accessibility and e-Inclusion, both in EU [15, 16],[14] and the USA [52]. The Norwegian government aims at ensuring that all technological solutions involving ICT in the public sector shall be based on universal design [44], promotes accessibility and e-Inclusion [49] anti-discrimination and rights for the disabled [3]. In the field of procurement, the Norwegian legislation has been changed to correspond to the EU Directive. According to this legislation, universal design must be considered in each procurement process. [8]. Thus, the E-Me-proposal is highly relevant for key societal challenges, and perfectly compliant with national and international policies, priorities and laws.

3.3 Environmental perspectives

Prototyping in the e-Me-project will not have noticeable environmental impacts.

3.4 Ethical aspects

The critical ethical aspects in e-Me are connected to the **fieldwork** and the possible misuse of identity management technologies. All fieldwork, such as requirements specifications through user tests, focus groups or personal interviews, will be carried out in compliance with the ethical guidelines for research in

science and technology, provided by the National Committee for Research Ethics in Science and Technology (NENT) [43], guidelines from the Norwegian Data Inspectorate concerning handling of personal data [11] and use of personal data within research projects [12]. Any handling of personal data in the E-Me project will comply with the Norwegian Personal Data Act [46]. E-Me aims at **developing IDM-technologies** that support users in their freedom to stay in control over their privacy. Provision of IIDM-services is based on a wide processing of personal data which may have an impact on the right to privacy and on the freedom of movement in an anonymous way. IIDM-technologies investigated and developed in e-Me may have a an ambiguous potential [45] or [17] in terms of ethics and privacy.

3.5 Gender equality and gender perspectives

E-Me promotes gender equality by the **management and staffing** of the project. The project manager will be female. IDM needs of both age and gender groups will be assessed by e-Me. The volunteer **test users** from participating organisations will be recruited gender-equally.

4. Communication with users and dissemination

4.1 Communication with users

E-Me will involve users in all phases. The project will use **social media** for external communication with users through participating **NGOs**. E-Me will open www.e-me.no (complying with current accessibility standards) for information on e-Me, its scientific activities, products (papers and demonstrators) and events. E-Me will use its **expert panel** and **focus groups** as a mechanism for external communication and outreach.

4.2 Dissemination plan

Dissemination plans and activities are presented in detail in the electronic grant application form.

References

1. Adams, A. and M.A. Sasse, *Users are not the enemy: Why users compromize computer security mechanisms and how to take remedial mesasure.* Communications of the ACM, 1999. **42**(12): p. 41-46.
2. Ahn, L.v., M. Blum, and J. Langford, *Telling humans and computers apart automatically.* Commun. ACM, 2004. **47**(2): p. 56-60.
3. AID. *Norge undertegner FN-konvensjon om rettighetene til personer med nedsatt funksjonsevne*. Pressemelding 2007 30.03.2007; nr.:32:[
4. Albinsson, L., *Using Cartoons to Engage Stakeholders in Innovation and Design of IT Artefacts*, in *Wonderground, Design Research Society International Conference*. 2006: Lisbon, Portugal.
5. Alsenoy, B.V., et al., *Social networks and web 2.0: are users also bound by data protection regulations?* Identity in the Information Society (IDIS), 2009, special issue on Social Web and Identity 2009.
6. Beyer, H. and K. Holtzblatt, *Contextual design: defining customer-centered systems*. 1998: Morgan Kaufmann Publishers Inc. 472.
7. Braz, C. and J.-M. Robert, *Security and usability: the case of the user authentication methods*, in *Proceedings of the 18th International Conferenceof the Association Francophone d'Interaction Homme-Machine*. 2006, ACM: Montreal, Canada.
8. Brynn, R. *Universell utforming i offentlige anskaffelser*. 2006 2007-04-03;
9. Camenisch, J. and E. van Herreweghen, *Design and Implementation of the Idemix Anonymous Credential System*, in *Research Report RZ 3419*. 2002: Zürich.
10. Cullen, K. and et al, *MeAC - Assessment of the Status of eAccessibility in Europe*, in *Main Report October 2007*. 2007.
11. Datatilsynet (2005a) Veileder: Bruk av personopplysninger i forsking. DEL I Meldeplikt eller konsesjonsplikt?, p. 8.
12. Datatilsynet (2005b) Veileder: Bruk av personopplysninger i forsking. DEL II Hvilke regler gjelder for forskning?, p. 19.
13. Dhamija, R. and L. Dusseault, *The Seven Flaws of Identity Management: Usability and Security Challenges.* Security & Privacy, IEEE, 2008. **6**(2): p. 24-29.
14. EC. *Public Procurement*. 2004-2006;
15. EC. *i2010 - A European Information Society for growth and employment*. 2005; 12].
16. EC (2007) *Communication "European i2010 initiative on e-Inclusion - to be part of the information society"*. Europe's Informatin Society. Thematic portal,
17. Figge, S., *Situation-dependent services - a challenge for mobile network operators.* Journal of Business Research, 2004. **57**(12): p. 1416-1422.
18. Fritsch, L., *State of the Arth of Privacy-enhancing Technology (PET) - Deliverable D.2.1 of the PET Web project*, in *the PETweb project*. 2007, Norsk Regnesentral Oslo, Norway.
19. Fritsch, L., K.S. Fuglerud, and I. Solheim, *Towards inclusive identity management*, in *Identity in the Information Society Workshop*. 2008, Pre-Proceedings of the 1st IDIS workshop 2008: Arona, Italy.
20. Fuglerud, K.S., *Universal design in ICT services*, in *Inclusive Buildings, products & services: Challenges in universal design*, T. Vavik, Editor. 2009: Trondheim, Norway. p. 244-267.
21. Fuglerud, K.S., et al., *Universal design of IT-based solutions for registration and authentication.*, in *DART/02/09*. 2009, Norwegian Computing Center: Oslo. p. 60.
22. Fuglerud, K.S. and I. Solheim, *Synshemmedes IKT-barrierer. (Eng: ICT-barriers for the visually impaired)*, in *Report number: 1016*. 2008, Norwegian Computing Center: Oslo, Regjeringskvartalet, Akersgt 59, auditorie R5,. p. 91.

23. Gibbons, M., et al., *The New Production of Knowledge : The Dynamics of Science and Research in Contemporary Societies.* 1994, London SAGE Publications.

24. Godet, M., A. Gerber, and K. Radford, *Creating Futures: Scenario Planning as a Strategic Management Tool.* 2006: Economica. 346.

25. Halbach, T., *Dokumentasjon av UNIMOD-innloggingsprototypen (Eng: documentation of the UNIMOD login prototype)*, NR-Rapport, Editor. 2009, Norsk Regnesentral. p. 40.

26. Halpert, B.J. *Authentication Interface Evaluation and Design for Mobile Devices*. in *Information Security Curriculum Development (InfoSecCD)Conference '05*. 2005. Kennesaw, GA, USA.

27. Hansen, M., A. Pfitzmann, and S. Steinbrecher, *Identity Management throughout one's whole life*, in *Information Security Technical Report 13/2*. 2008. p. 83 - 94.

28. Hellman, R. *Accessible Electronic Services on Digital TV*. in *The first International Conference on Technology for Participation and Accessible eGovernment Services*. 2007. Kristiansand, Norway.

29. Hellman, R. *Universal Design and Mobile Devices*. in *Universal Access in HCI, Part I, HCII 2007*. 2007.

30. Hochheiser, H., J. Feng, and J. Lazar, *Challenges in Universally Usable Privacy and Security*, in *Symposium On Usable Privacy and Security (SOUPS) 2008, .* 2008: Pittsburgh, PA, USA.

31. Honkala, M. and M. Pohja, *Multimodal interaction with xforms*, in *Proceedings of the 6th international conference on Web engineering*. 2006, ACM: Palo Alto, California, USA.

32. Huang, M., *Unequal Pricing in the Information Economy: Implications for Consumer Welfare.* Journal of Business Ethics, 2005. **56**(4): p. 305-315.

33. Jaeger, P.T., *Beyond Section 508: The spectrum of legal requirements for accessible e-government Web sites in the United States.* Journal of Government Information, 2004. **Volume 30**(Issue 4): p. 518-533

34. Jameel, H., et al., *Human Identification through Image Evaluation using Secret Predicates*, in *To be published in Topics in Cryptology CT-RSA 2007, The Cryptographers Track at the RSA Conference 2007*. 2007: San Francisco, CA, USA.

35. Jendricke, U. and D. Gerd tom Markotten, *Usability meets security - The Identity-Manager as your Personal Security Assistant for the Internet.* Proceedings of the 16th Annual Computer Security Applications Conference, 2000.

36. Kai-Lung, H., C.Y.T. Bernard, and G. Chyan-Yee, *Online information disclosure: Motivators and measurements*. 2006, ACM. p. 415-441.

37. Klingsheim, A. and K. Hole, *Personal Information Leakage: A Study of Online Systems in Norway* 2008, Department of Informatics,University of Bergen: Bergen.

38. Kobsa, A., *Privacy-enhanced personalization.* Commun. ACM, 2007. **50**(8): p. 24-33.

39. Levy, S. and B. Stone, *Grand Theft Identity*, in *Newsweek* 2005. p. 38-45.

40. May, M., *Inaccessibility of CAPTCHA. Alternatives to Visual Turing Tests on the Web*, W3C, Editor. 2005, W3C Working Group Note, work in progress.

41. Meyer, P. (2009) *The changing face of identity management*. Nokia Siemens Netwok Unite,

42. Myers Michael D. Section Editor (living version). *Qualitative Research in Information Systems*. Originally published in MISQ Discovery, June 1997 [electronic article] 2009 31. Aug 2009;

43. NENT (2005) Forskningsetiske retningslinjer for naturvitenskapelig og teknologisk forskning, The National Committees for Research Ethics in Science and Technology in Norway, p. 15.

44. NOU 2005: 8 Equality and accessibility.(Eds, A. Syse, et al.), Justis- og politidepartementet.

45. Nowak, G.J. and J. Phelps, *Direct marketing and the use of individual-level consumer information: Determining how and when 'privacy' matters.* Jounal of Direct Marketing, 1997. **11**(4): p. 94-108.

46. Personopplysningsloven, *LOV 2000-04-14 nr 31: Lov om behandling av personopplysninger (personopplysningsloven).* 2001, Justis- og politidepartementet,.

47. Pettersson, J.S., et al., *Making PRIME usable*, in *Proceedings of the 2005 symposium on usable privacy and security*. 2005, ACM: Pittsburgh, Pennsylvania.

48. Reeves, L.M., et al., *Guidelines for multimodal user interface design.* 2004. **47**(1): p. 57-59.

49. Report No. 17. (2006-2007) Information Society for All(Ed, FAD), Ministry of Government: Administration and reform, p. 180.

50. Sarter, N.B., *Multimodal information presentation: Design guidance and research challenges.* International Journal of Industrial Ergonomics, 2006. **36**(5): p. 439-445.

51. Schrammel, J., C. Köffel, and M. Tscheligi. *Information disclosure in different types of communities*. in *Fourth International Conference on Communities and Technologies*. 2009. Pennsylvania, USA,.

52. Section 508. *Section 508*. 2007 June 2007;

53. Snyder, C., *Paper Prototyping: the fast and easy way to design and refine user interfaces*. Interactive Technologies. 2003: Elsevier.

54. Solove, D., *A taxonomy of privacy.* GWU Law School Public Law Research Paper No.129, University of Pennsylvania Law Review, 2006. **154**(3): p. 477.

55. Whitten, A. and J.D. Tygar, *Usability of Security: A case study*. 1998, Carnegie Melon University, Pittsburgh, PA 15213, USA. p. 39.

56. Zimmermann, G. and G. Vanderheiden, *Accessible design and testing in the application development process: considerations for an integrated approach.* Universal Access in the Information Society, 2007.