E-vote 2011

SSA-U Appendix 6

Administrative provisions

Project: E-vote 2011

CONTENT

1. Project organization

1.1. Organization

The project managers will be responsible for project coordination. The customer will have the possibility to let the project manager from contractor, report directly to project steering group customer if this is appreciated.

1.2. Definition of roles

Role	Responsibility
Project manager customer	Responsible for project progress on customer side, according to agreed project plan.
Project manager contractor	Responsible for project progress on contractor side, according to agreed project plan.
Technical project manager	Responsible for development activities and coordination of these. Track iteration progress and work with the team to resolve challenges that may impede the team from delivering on the goals set for the iteration.
Subproject leader evoting contractor	Responsible for project progress for subproject evoting. Management of resources involved in deliverance of evoting.
Subproject leader adm.system contractor	Responsible for project progress for subproject adm.system. Management of resources involved in deliverance of adm.system.
Subproject leader pvoting contractor	Responsible for project progress for subproject pvoting. Management of resources involved in deliverance of pvoting.
System architect contractor	Responsible for systems architecture and systems design.
System consultant contractor	Responsible for detailed design, programming and unit testing.
Test consultant contractor	Responsible for integration test, system test and performance test.
Test manager contractor	Responsible for test strategy, test plans and progress of test activities from contractor side.
Quality manager contractor	Responsible for quality.
Usability expert contractor	Responsible for usability and accessibility from contractor side. The usability experts are capable of conducting interaction and graphical design.
Cryptographic expert	Responsible for security evoting.
Election expert evoting	Responsible for the overall solution evoting.
Election expert pvoting	Responsible for the overall solution pvoting.
Election expert adm.system	Responsible for the overall solution adm.system.

The roles of project members are defined in the table below. The team covers all project phases. The election experts will participate in the test phase as well as in the early phases of analysis and specification. Several other consultants will participate in specific phases of the project, and will be identified at a later stage.

Role	**Name**
Project core team (key personell)	
Project manager	Dag Erik Rotnebo
Quality manager	Sven Christiansen
Technical project manager	Svein Winje
Subproject leader evoting	Gabriel Dos Santos Davila
Shared rolls across the project	
Cryptographic (and security) expert	Jordi Puiggiali
Usability expert	Yngve Skråmm, Teodor Bjerrang (hired from IXD)
Test managers	
- Overall test manager	Sven Christiansen
- Manager SW factory	Gabriel Dos Santos Davila
Project members evoting	
Election expert eVoting	Onno Van Dommelen
System architects	Gerard Cervello, Sven Herzing
System consultants	Karoline König, David Alcoba, Kristo Karr, Miquel Comas, João Manuel de Vila Fernandes Orvalho
Usability expert	Michael Serisier
Test consultant	Dimitrios Kapanidis
Project members ecounting of pvotes	
Subproject leader pvoting	Hanne Melby
Election expert pvoting	Torleiv Næss
System consultant	TBD
Test consultant	Hanne Melby
Project members adm.system	
Subproject leader adm.sys.	John Sørby
Election expert adm.system	Torleiv Næss
System architect	Jan Arne Moen
System consultants	Anders Åberg, Thomas Aaeng, Lena Sæternes, Gaute Lohte, Per Hildebrand + additional consultants
Test consultant	Torleiv Næss

1.3. Contractors core team and key personnel

Role	Name
Project manager	Dag Erik Rotnebo
Quality manager	Sven Christiansen
Technical project manager	Svein Winje
Subproject leader evoting	Gabriel Dos Santos

The contractor's core team will be located in Oslo. The contractor´s office is located in Nydalsveien 28, Oslo with necessary work space and meeting facilities for the project members on contractor side.

1.4. Use of subcontractors

The following subcontractor is approved by the parties:

Name	Adress
Scytl Secure Eelectronic Voting	Tuset 20 1º7ª 08006 Barcelona Spain

1.5. Cooperation with third parties

The contractor undertakes to cooperate with third party to the extent that consider to be directly in cooperation with the contractors deliverables.

1.6. Duties of the contractor upon discharge of the Agreement

The contractor will make the following type of key personnel available for the performances of services upon discharge of the agreement:

Role
Project manager
Technical project manager

2. Principles of cooperation, project documentation and reporting

The principles of cooperation are based on the responsibility for the roles in the project organization.

Role	Project report	Reports to	Frequency
Project member Contractor	Project progress of activities where the project member is responsible	Subproject leader	Weekly
Subproject leader contractor	Project progress of milestones where the subproject leader is responsible. Status and activities within milestones.	Project manager	Biweekly
Project manager contractor	Project progress related to approved project plan. Risk analysis	Project manager customer	Biweekly

2.1.1. Project Monitoring and Control

The main purpose of *Project Monitoring and Control* is to provide an understanding of project progress and visibility, which allows all the involved stakeholders (customer, Management Team, etc.) to see the evolution of the project and to take timely corrective actions when the project's performance deviates from the plan.

The Project Management Plan is the basis for the monitoring activities, status communication and taking corrective action. The Contractor's Project Manager primarily determines progress by comparing actual work products and task attributes, effort, cost and schedule to the Project Management Plan and Project Schedule at predefined milestones and/or periodically.

This progress, along with the main detected issues, risk log and other important information will be reflected in a *Project Status Report*. This document will be generated by the Contractor's Project Manager, and will be validated by the Customer. The periodicity of the generation of this report will be determined between the Customer and the Contractor during the Specification Phase, although we propose to generate this report bi-weekly till the delivery of the software application.

Periodic meetings between the Customer and Contractor's Project Manager will allow the coordination of the project. In these meetings the corresponding Project Status Report will be reviewed, as well as any issues requiring attention. The meetings will be on-site in the customer's premises as well as through conference calls and other remote meeting tools, such as for example Webex. Minutes of each meeting will be prepared by the Contractor's Project Manager.

Besides the project progress, two other monitoring and control tasks will be executed and reported periodically:

a) The **Risk Management** approach will identify the important risks, their impact and risk management tasks, and a risk analysis will be undertaken and documented, as explained below.
b) The **Quality Control** process will test the compliance of the project to the requirements of this quality plan and other plans governing the project..

Deliverables:
a) **Project Status Report**: contains among others an update of the project status, with the main highlights of the last reporting period, and a short list of the risk log and main issues.
b) **Meeting Minutes**: contains the details of the issues discussed in the meeting, agreed action points and attendants. Both parties will accept them once generated.
c) **Updated Project Plan** : during the project life cycle, when necessary, the Project Plan will be updated based on the evolution of its execution and change requests. Major changes must follow the change management process.

2.1.2. Escalation Process

From time to time issues may arise during the implementation of a project relative to the Contractor's or the Customer's performance, due to unplanned issues arising, or simply a change in direction.

The Contractor will provide a documented and transparent escalation process to ensure issues are dealt with rapidly when they cannot be dealt with in a prompt and expeditious manner at the project level. This escalation plan includes Contractor management responsibility where appropriate. This escalation process will be defined in the Project Management Plan, as explained above.

2.1.3. Risk Management

Risk management activities will be conducted to minimize negative risk impacts and maximize the positive (opportunity) risks identified for the project, so that project objectives are met. This will be achieved by following a structured process, defined in the *Risk Management Plan*, whilst ensuring the efforts of risk management activities are appropriate for the importance of the project to the Customer.

The purpose of the risk management plan is to describe how risk management activities will be organized and performed during the project's life cycle. Risk management activities are:
a) **Risk Management Planning.** Determine the approach to risk management.
b) **Risk identification.** Identify all known project delivery risks, system security risk, etc.
c) **Risk Analysis.** Perform an assessment of the probability of occurrence and potential impact.
d) **Risk Response Planning**. Create action plans to manage the identified risks.
e) **Risk Monitoring and Control.** Monitor, review and update risk status and plans.
f) **Risk Closeout.** Document lessons learned.

The risk management plan does not address the responses to individual risks – these are documented in the Risk Log.

The purpose of risk management planning is to minimize the negative risk impacts and maximize the positive (opportunity) risks identified. This will be achieved by identifying all known risks, performing an assessment of the probability of occurrence and potential impact, and creating action plans (mitigation plans) to manage the identified risks. This process ensures that the efforts of risk management activities are appropriate for the importance of the project to the Customer.

Risk planning is an iterative process, beginning as early as possible in the project and concluding at project close-out. The approach to and appropriateness of risk management activities should be reviewed through the project at the regular project status meetings, as defined above.

The development of the risk management plan is refined by information gathered during risk analysis and response planning activities and information recorded in the Risk Log.

The risk identification activity will:

a) **Commence at the Project planning stage**, be repeated at intervals as defined by the project and conclude at Project Closeout.

b) **Identify a comprehensive list of potential risk** events that have a negative (threat) or positive (opportunity) impact.

c) **The identification of risks** will be based on several sources, including:

   1. Examining each element of the project work breakdown structure.
   2. Comparing current project with previous similar experiences.
   3. Reviewing all the requirements stated in tender and contract.
   4. Interviews with the Customer stakeholders.

Analyzed risks will be prioritized to identify the top ten risks with threats and opportunities. When selecting the top ten risks, consideration will be given to those risks with overall rating of "HIGH" as well as risks that are important to the Customer or other stakeholders. The remaining risks that will not be the focus of immediate risk management effort will be reconsidered at monthly intervals.

Risk Response plans (Risk mitigation plans) will be developed for both threats and opportunities for each of the top 10 risks selected from the prioritization process.

The Risk Log and Risk Mitigation Plans will be reviewed as agreed with the Customer.

Deliverables:

a) **Risk Management Plan**: This document describes how risk management activities will be organized and performed during the project's life cycle.

b) **Risk Log**: This document contains the details of all the risks identified, especially of the ones with higher impact. This document will contain the following for each specific risk identified:
   1. The risk owner who is the person responsible for managing the response plan.
   2. The risk response strategy that will be used.
   3. The description of the mitigation or contingency plan.
   4. Any stakeholders impacted by the risk.
   5. The cost of the risk response.

c) **Risk Mitigation plans:** This document, one for each of the high priority risks detected, describes the risk details, planned mitigation actions and possible contingency plan(s).

2.2. Quality assurance

Quality assurance methods and preparation of quality plan, are described in Appendix 4, section 4.

3. Security

3.1. Elaboration of Requirement GR2.1

DNV

KOPI

DET NORSKE VERITAS

MANAGEMENT SYSTEM CERTIFICATE

Sertifikat nr. 2002-OSL-AIS-0002

Med dette sertifiseres at
LEDELSESSYSTEMET
ved

ErgoGroup AS
IKT-driftstjenester

adresse:
Nydalsveien 28, 0402 Oslo

er funnet å være i overensstemmelse med følgende standard for informasjonssikkerhet
ISO/IEC 27001 : 2005

Dette sertifikatet er gyldig for følgende produkter eller tjenester:
Tjenesteutvikling.
Salgsstøtte.
Integrasjon og drift av kommunikasjons- og servicetjenester.
Programutvikling, applikasjonsdrift, lagring av data, brukerstøtte og driftsovervåking.
Konsulenttjenester knyttet til ovennevnte områder.
Dette i henhold til siste versjon av Statement of Applicability.

Første sertifikat gyldig fra:
2002-05-08

Sertifikatet med vedlegg er gyldig til:
2009-12-05

Jan Roald Brembo
Revisjonsleder

NORWEGIAN ACCREDITATION
ISMS 001

Sted og dato:
Høvik, 2007-01-12

For akkreditert enhet:
Det Norske Veritas Certification AS

Anne Feiring
Ledelsens representant

Brudd på forutsetningene for sertifikatet, slik det fremgår av vedlegget, kan gjøre sertifikatet ugyldig.

DET NORSKE VERITAS CERTIFICATION AS, Veritasveien 1, N-1322 Høvik, Tel.: +47 67 57 99 00, Fax: +47 67 57 99 11
AQN-23no 2002-04-23

At the time this certificate was issued, ErgoGroup was split up in several 100% owned companies. Later all companies have been merged into ErgoGroup AS, and all certificates applies to the merged company. Yearly auditing is performed for the contractor.

3.2. Elaboration of Requirement GR2.2

Details of the practices implemented in this area are explained in Section 4 of "SSA-U Appendix 5 - Testing and Approval" and section 2 above.

Our SSDLC methodology is based on the following main activities:

Security Risk Identification and Management Activities

Project security risks
Project security risks are managed as part of the risk management activities (project monitor and control). A risk assessment and a risk management plan are created as part of the Initial project phase, and maintained throughout the project.

Security analysis and risk assessment is performed by compiling all the security related information and their relationships. This allows the generation of reports that can be used for risk management reports or audit purposes

Project security risks cover in addition the surrounding security environment: security policy, secure assets, physical security, business continuity, secure handling of information, and related topics. Risk management in this area is based on ISO 27001 standard guidelines.

Solution security risks
Solution security risks are managed as part of the Software Development Lifecycle, to ensure that the solution complies with the security objectives demanded by the Customer, and that software engineering activities take into account secure software development practices.

Risk management at this level is based on using ISO/IEC 15408 (Common Criteria) guidelines as reference. Other guidelines, e.g., OWASP, are used as reference for managing general security risks of the software engineering process.

Secure software development practices are more generic and are based on existing guidelines: SEI Secure Design patterns and OWASP Secure Development Guides.

For the specific security requirements that must be fulfilled by the solution, the following approach will be used for this project (aligned with Common Criteria):

- Definition of the security objectives of the solution: Identification of the security objectives to be fulfill by the final solution
- Security compliance: Identification of the security functions implemented in the solution and how do they achieve the security objectives.
- Risk analysis of the solution: Identification of the different assets, attacker roles, threats, countermeasures implemented by the security functions and their threat mitigation.

As a result of this activity, security requirements are specified and integrated with other non functional requirements into the requirements management process. These requirements will be tracked using the requirements traceability features of the Continuous Integration system

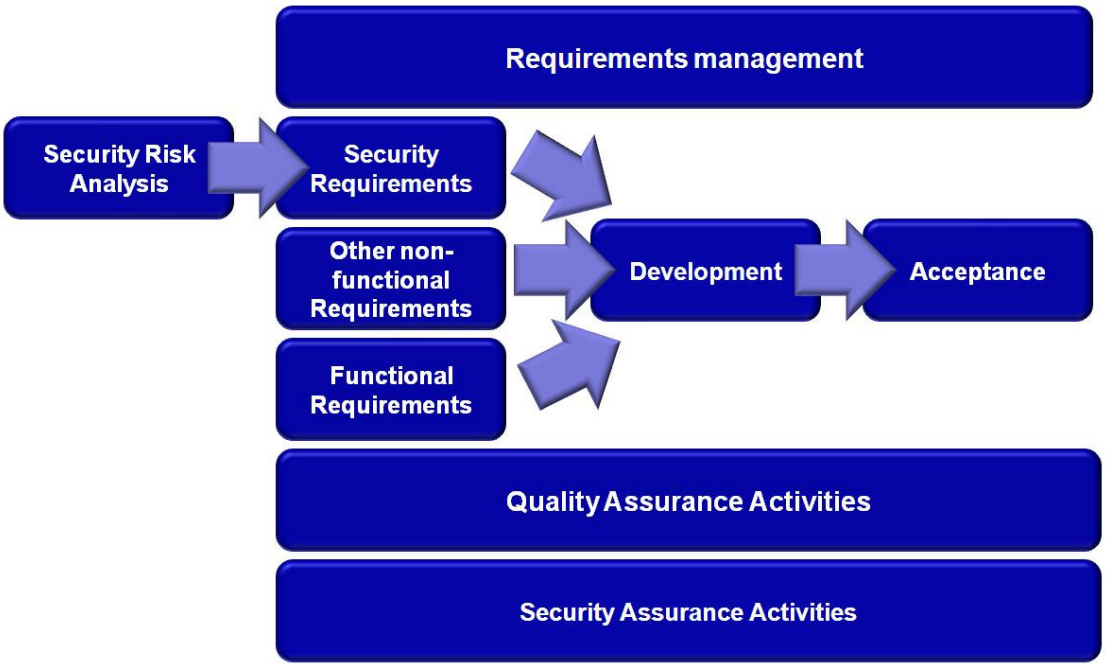


Figure 1 - Security Analysis and Requirements

Security Engineering Activities

Security at the software design level is based on the security risk assessment results obtained from the Risk Identification and Management Activities. These results are used for:

- Defining the Security Architecture of the Solution: The solution architecture is designed using also the security objectives and security functionalities as reference.
- Defining the security requirements that must be implemented in the solution: security functionalities are used for defining the security requirements to be implemented in the solution. These requirements are introduced as non-functional requirements and will be tracked and tested the same way as the other functional requirements.
- Defining the detailed specifications of special security functionalities: some security functionalities require the use or implementation of special cryptographic primitives or advanced algorithms. In this case, a detailed description is provided to ensure the proper implementation.

From the software engineering point of view, general guidelines are used to ensure that there are not risks related to errors or bugs in the implementation.

- Specific security training to software engineers

- Security requirements implemented and traced as any other requirement
- Implementation of a continuous Integration system that prevents issues in the source code remain undetected
- Use of specific source code security static analysis tools as part of our standard Continuous Integration system
- Usage of well know and widely used open source cryptography libraries
- Software design based on Secure Design principles, SEI Secure Design patterns and OWASP Secure Development Guides.

Security Assurance Activities
Besides the usage of automated tools in the Continuous Integration system, the source code and binaries are subject to specific security assurance activities such as:

- Code reviews by the security experts that designed the secure function
- Penetration tests, where applicable
- Source code security audits
- Security status monitoring of external tools and libraries

3.3. Quality assurance of documentation related to Common Criteria (CC)

Documentation required to achieve CC EAL4 will be provided for all components directly related to evoting, including counting and returning of members. All election system components not directly related to evoting will be documented for CC EAL2.

Certification documentation will be planned as part of project initiation, and the documentation will evolve throughout the project to reach level 2/4 (as applicable). The documentation process will be fully transparent to the customer and will be made available for the customer's security experts.

If necessary, ErgoGroup can include expertise from subsidiaries that have experience with CC certification, for instance BuyPass AS.

4. Accessibility and usability

Elaboration of Requirement M1

User centered design, an overview
"User centered design" contains a set of tools for analysis, design, prototyping, evaluation and testing.
The fundamental principle is close user involvement throughout the project, using workshops, focus groups, field studies, interviews, usability tests etc.

The advantage of frequent usability testing using prototypes at early stages of the project is that we can detect defects in the user interface early. Correcting mistakes in a low-fi prototype is far less expensive than modifying code.

The methodology can be divided into six main stages/activities:

- Analysis and planning
- Information architecture
- Interaction and functional design
- Graphic design
- Implementation
- Deployment

Stages and activities
This a general outline of the methodology with more details about activities and deliverables. All the different tools and activities are not used in all projects. Every project is unique, and the methodology can be more seen upon as a toolbox than a script that has to be followed to the letter in every project.
The main forum for all these activities is the workshop. User centered design is a joint venture between the customer, representatives for the end users (if different from the customer) and the development team.

1. Analysis and planning

User need analysis

- Defining personas, user groups and needs: What types of users will use the system, what are their common traits, where do they differ, what are their needs?
- Defining level of accessibility: What are the requirements concerning accessibility? Are there large user groups with disabilities?
- Defining context: In what context will the system be used? What are the users' goal and motivation? Where will it be used – noisy workplace, at home, school etc.

Content analysis

- Is there an existing system? What do we need to preserve? What works well in the old system and what does not work?
- Evaluate existing works processes. Can they be improved or made more effective?

Develop user scenarios (personas, user stories, use cases)

It is important to develop and document typical tasks (scenarios) that the users will perform. We will use these scenarios later in the implementation phase to test whether or not the system will support the behavior described in the scenario.

Defining design goals

What kind of user interface behavior does the end user expect and need from a particular scenario? In one scenario the end user is a professional performing the same tasks every day and having quick and easy access to information and functionality needed to perform their tasks is the most important aspect of the user interface. Another scenario might cover a set of tasks that is performed rarely, and the end-user require clarity and guidance through a process. Holding their hand, so to speak. The user experience in these to extremes will be design very differently and are not interchangeable.

Defining targets for usability requirements

How can we determine that we have achieved good usability? Is it a matter of personal opinion from the project manager? We believe that the only way to measure usability is to get feedback from the users through statistics, usability tests and field studies. In order for us to have something to test, we must define concrete goals and targets for what is good (enough) user experience covering different scenarios. For example: "In order for scenario x to pass, 70% of end users in the target groups must complete the operation in 3 minutes and 90% within 5 minutes". "Today 40% present of the users say that they are satisfied with the current system. 6 months after release of the new system 90% of the users must be satisfied with the new system". Defining a set of measurable realistic targets can reduce disagreements and conflict between the customer and the developer by eliminating personal opinion and adding a more empirical approach to design and usability.
Deliverables: Report containing goals, targets, user groups, personas, use cases, flowcharts and other findings from the analysis phase.

2. Information architecture

Information architecture describes the structure of the system and is an important tool especially in designing websites containing large amounts of information. The structure must satisfy the various user groups' needs perception of a logical structure. A public-facing website should not necessarily present the user with a menu structure and navigation aids describing the internal structure of the organization when that is not known or event interesting for the user. We want to achieve an intuitive information architecture enduring a best possible flow of information. The users must feel comfortable

1. knowing where they are in the system
2. knowing what that they can find or do there
3. knowing how to get from where you are to something else

Deliverables: Sitemap describing the organization of the pages in the system.

3. Interaction and functional design

Interaction design concerns how users move between and within pages in a system. To describe data flow to and from the user we use various types of notation, UML activity diagrams, BPML or whatever the customer is most comfortable with.

Functional design

Working in parallel with interaction design is function design which describes the basic lay-out and content of a page. Even though this is not precise design one have in mind the constraints of the project concerning screen

resolution, type of tasks to be performed, what type of users and other factors that decide how the page should function. It is important throughout the process take accessibility issues into account. You will get a much more accessible system if you build accessibility into the system from the bottom instead of trying to fix it as an afterthought in the last stages of a project. We can use these functional sketches as basis for user testing to uncover potential problems at an early stage.
Deliverables: Functional design, process descriptions, diagrams.

4. Graphical design
Graphical design has as its primary goal to convey a visual profile/ identity and aid the user in performing task, make them feel comfortable using the system and help sending the message the system is supposed to send: "Secure and trustworthy", "young and hip" etc. The design will of course be the object of user testing to ensure that it works according to plan.
Deliverables: Set of complete pages and a design guideline describing how graphic elements should be used on other pages in the future.

5. Implementation
We now have a graphic design, interaction design, functional design and information architecture. The development team can now plan how to implement these pages and how their functionality affect the back-end system. The pages are then implemented in cooperation between a user interface programmer and the usability expert. The solution will be incrementally tested both with regard to functionality, technical stability, usability and accessibility.

6. Deployment
The project is not fished even if the system is released. Even after extensive user testing before deployment, you need to ensure that the software works as intended for the end user. We will therefore conduct studies and tests in order to uncover problems and defects in the system. This can be done conducting field studies, log analysis, surveys or user testing.

Elaboration of Requirement M2

The overall goal of user tests is to ensure best possible user experience for all users. That also includes users with disabilities often using different kind of assistive devices to be able to use the computer. Even though we test the system for accessibility throughout the development process using tools like Wave web accessibility evaluation tool from AIM[1] and Web Accessibility Toolbar[2]. For a more detailed description see elaboration of requirement M3.

Elaboration of Requirement M3

User testing /usability testing
One of the corner stones of user centered design is user testing. User testing is a way to evaluate the usability of a system. The test is performed by observing and analyzing end users while they solve identical problems under identical conditions. The goal is to identify user patterns exposing faults, defects, challenges and areas of improvement of the tested system.

[1] http://wave.webaim.org/
[2] http://www.paciellogroup.com/resources/index.html

Different alternatives
There are different ways of conducting usability test depending on where you are in the project and how big and complicated the project is. The goal is to ensure a high quality, yet cost effective test.

Paper based demonstrator
A paper based test is a low-fi approach to user testing. It consists of printout of pages either rough sketches or more elaborate designs. This type of test is usually conducted early in the process. The weakness of the test lies in the absence of technology that will be used in the finished solution. The accessibility of the system cannot be tested in this manner. There are, however some advantages:

- We will not get system errors that often plague early prototypes and technical proofs of concept.
- The user is less likely to be concerned with insignificant details of the solution. They think of the test just as a test and no a final product.

Screen based demonstrator
If you need to test complex interaction and look and feel you probably want to develop a prototype where the user can interact with the system to perform certain tasks as if it is a finished product. There is, however, no real back-end system. It is just a simulation.
The weakness of this type of test is if the user chooses to interact with the system in unpredictable ways, (which in a finished system might be a correct alternative option) the demonstrator might respond in ways not expected by the user or more likely not respond at all. This can aggravate the reader and disrupt the testing process.

Full scale prototype
When the parts of the software are ready for system testing, we can also perform a usability test using the live system. We can now see how users respond to the system proper. We can now uncover other aspects of the user experience as e.g. response time. This type of test also allows for accessibility tests with disabled users, usually with sight impairments.

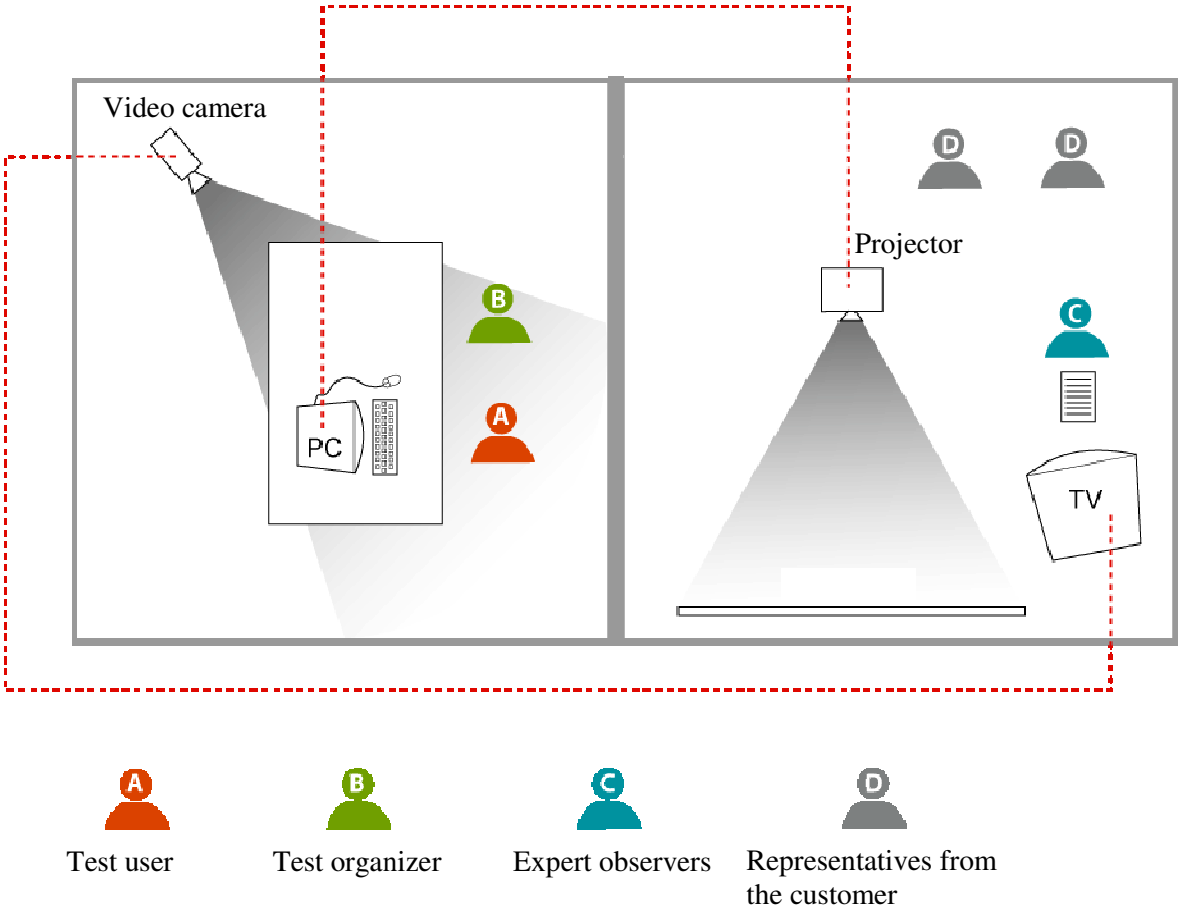
The weakness with this type of test as with the screen based demonstrator, is that it often will contain errors which can disrupt the test.

On-line demonstrator
The complete system must also be tested preferably in its production environment. This type of test is also used in testing existing systems prior to redesign.

Execution
The test is conducted using two adjoining rooms (see illustration below). In the observation room observers follow the test in real-time via video and take notes. In the other room are the tester, the test organizer and one observer taking notes.

A full scale usability test normally consists of:

- 1 test organizer
- 1-2 expert observers
- 1-2 representatives from the customer
- 5-8 test users



Elaboration of Requirement M4

We welcome usability, accessibility and other forms of testing from external consultants approved by the ministry.

Elaboration of Requirement M5

Please refer Appendix 4, section 2 on our implementation methodology and how usability and accessibility requirements are build into the development process itself.