



Electronic Voting Software

Security Target

EAL 4+

Source Code, High Level Architecture Documentation and Common Criteria Documentation Copyright (C) 2010-2011 and ownership belongs to The Norwegian Ministry of Local Government and Regional Development and Scytl Secure Electronic Voting SA  (“Licensor”)

The Norwegian Ministry of Local Government and Regional Development has the right to use, modify (whether by itself or by the use of contractors) and copy the software for the sole purposes of performing Norwegian Public Sector Elections, including to install and run the code on the necessary number of locations centrally and in any number of counties and municipalities, and to allow access to the solution from anywhere in the world by persons who have the right to participate in Norwegian national or local elections. This also applies to elections to the Longyearbyen Community Council at Svalbard and any possible future public elections in Norway arranged by the Election Authorities.

Patents, relevant to the software, are licensed by Scytl Secure Electronic Voting SA to the Norwegian Ministry of Local Government and Regional Development for the purposes set out above.

Scytl Secure Electronic Voting SA (or whom it appoints) has the right, inside and outside of Norway to use, copy, modify and enhance the materials, as well as a right of licensing and transfer, internally and externally, either by itself or with the assistance of a third party, as part of the further development and customization of its own standard solutions or delivered together with its own standard solutions.

The Norwegian Ministry of Local Government and Regional Development and Scytl Secure Electronic Voting SA hereby grant to you (any third party) the right to copy, modify, inspect, compile, debug and run the software for the sole purpose of testing, reviewing or evaluating the code or the system solely for non-commercial purposes. Any other use of the source code (or parts of it) for any other purpose (including but not limited to any commercial purposes) by any third party is subject to Scytl Secure Electronic Voting SA’s prior written approval.

**Document HIstory**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Comments** |
| 0.2 | 2010-04-10 | Scytl R&D | Created Document. |
| 0.7 | 2010-05-10 | Scytl R&D | Draft version for review |
| 0.8 | 2010-05-12 | Scytl R&D | Completed version |
| 0.9 | 2010-05-20 | Scytl R&D | Version with development feedback. |
| 1.0 | 2010-05-25 | Scytl R&D | Reviewed version |
| 1.1 | 2010-12-03 | Scytl R&D | Reviewed version to include recent software changes. |
| 1.2 | 2011-06-03 | Scytl | Added disclaimer, and copyright and next version target |

**DISCLAIMER:** This document is a work in progress and some important information in it is obsolete, inaccurate or is missing. Because of this the document content is not yet published. Regular updates will be made to the document. This disclaimer will be also updated to reflect the state of the document.

**NEXT VERSION TARGET DATE:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Comments** |
| 1.3 | 20.06.2011 | Scytl |  |

**Quality Assurance:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **QA responsible** | **Comments** |
| 1.1 | 22.03.2011 | Markus Harboe |  |

Approval

|  |  |  |  |
| --- | --- | --- | --- |
| **Approved by** | **Role** | **Sign** | **Date** |
| Svein Endresen | Project Manager |  | 22.03.2011 |
| Svein Winje | Technical Architect |  | 22.03.2011 |
| Dan Sørensen | Customer |  |  |

[1 E-Voting TOE 5](#_Toc262581219)

[1.1 Security Target and TOE Identification 5](#_Toc262581220)

[1.1.1 ST Reference 5](#_Toc262581221)

[1.1.2 TOE Reference 5](#_Toc262581222)

[1.2 TOE Overview 6](#_Toc262581223)

[1.2.1 TOE Environment 7](#_Toc262581224)

[1.3 TOE Description 8](#_Toc262581225)

[1.3.1 Evaluated Components of the TOE 8](#_Toc262581226)

[1.4 TOE Boundaries 11](#_Toc262581227)

[1.4.1 Physical Boundary 11](#_Toc262581228)

[1.4.2 Logical Boundary 11](#_Toc262581229)

[2 Conformance Claim 13](#_Toc262581230)

[3 Security Problem Definition 14](#_Toc262581231)

[3.1 Secure Usage Assumptions 14](#_Toc262581232)

[3.2 Threats 14](#_Toc262581233)

[3.3 Organizational Security Policies (OSP) 18](#_Toc262581234)

[4 Security Objectives 19](#_Toc262581235)

[4.1 Security Objectives for the TOE 19](#_Toc262581236)

[4.2 Security Objectives for the Operational Environment 21](#_Toc262581237)

[4.3 Security Objective Rationale for the TOE 22](#_Toc262581238)

[4.3.1 Mapping of Security Objectives to threats and organizational security policies 22](#_Toc262581239)

[4.3.2 Justification of Security Objectives to threats and OSPs 23](#_Toc262581240)

[4.4 Security Objective Rationale for the Operational Environment 28](#_Toc262581241)

[4.4.1 Justification of Operational Environment Security Objectives and assumptions 28](#_Toc262581242)

[5 Security Requirements 29](#_Toc262581243)

[5.1 TOE Security Functional Requirements 29](#_Toc262581244)

[5.1.1 Class FAU: Security Audit 29](#_Toc262581245)

[5.1.2 Class FCO: Communication 30](#_Toc262581246)

[5.1.3 Class FCS: Cryptographic Support 31](#_Toc262581247)

[5.1.4 Class FDP: User Data Protection 32](#_Toc262581248)

[5.1.5 Class FIA: Identification and Authentication 46](#_Toc262581249)

[5.1.6 Class FMT: Security Management 48](#_Toc262581250)

[5.1.7 Class FPR: Privacy 51](#_Toc262581251)

[5.1.8 Class FPT: Protection of the TSF 51](#_Toc262581252)

[5.1.9 Class FTA: TOE access 54](#_Toc262581253)

[5.1.10 Class FTP: Trusted path/channels 55](#_Toc262581254)

[5.2 Security Functional Requirements dependencies 56](#_Toc262581255)

[5.2.1 Justification why dependencies are not met 57](#_Toc262581256)

[5.3 Mapping of TOE Security Requirements to Objectives 58](#_Toc262581257)

[5.4 Justification of TOE Security Requirements to Objectives 60](#_Toc262581258)

[5.5 Security Assurance Requirements 65](#_Toc262581259)

[5.5.1 Rationale for Security Assurance Requirements 66](#_Toc262581260)

[6 TOE Summary Specification 66](#_Toc262581261)

[6.1 TOE Security Functions Rationale 66](#_Toc262581262)

[**6.1.1** **Security audit** 68](#_Toc262581263)

[**6.1.2** **Identification and authorization** 68](#_Toc262581264)

[**6.1.3** **Process Accuracy** 69](#_Toc262581265)

[**6.1.4** **Cryptographic support** 69](#_Toc262581266)

[**6.1.5** **Service Availability** 70](#_Toc262581267)