scytl

Secure Electronic Voting

The Council of Europe’s Standards on e-Voting

Pnyx Compliance with the Council of Europe’s Security & Audit Standards on e-Voting

December 2004

The Council of Europe’s Standards on e-Voting

Pnyx Compliance with the Council of Europe’s Security & Audit Standards on e-Voting

Scytl secure electronic voting

The cryptographic mechanisms and protocols described in this document are protected by international patent applications

http://www.scytl.com

TABLE OF CONTENTS

Introduction

On September 30, 2004, the Committee of Ministers of the Council of Europe adopted the Recommendation Rec(2004)11 on “legal, operational and technical standards for e-voting”. This Recommendation is the result of a thorough study conducted during the last two years by a Multidisciplinary Ad Hoc Group of Specialists on legal, operational and technical standards for e-enabled voting (IP1-S-EE), under the auspices of the Integrated Project “Making Democratic Institutions Work”.

The Recommendation states a number of factors that clearly justify the advancement on the study, experimentation and adoption of e-voting throughout Europe in public elections and referendums:

> *“Recognising that as new information and communication technologies are increasingly being used in day to day life, member states need to take account of these developments in their democratic practice;*
>
> *Noting that participation in elections and referendums at local, regional and national levels in some member states is characterised by low, and in some cases steadily decreasing, turnouts;*
>
> *Noting that some member states are already using, or are considering using e-voting for a number of purposes, including:*
>
> *- enabling voters to cast their vote from a place other than the polling station in their voting district;*
>
> *- facilitating the casting of the vote by the voter;*
>
> *- facilitating the participation in elections and referendums of all those who are entitled to vote, and particularly of citizens residing or staying abroad;*

> *- widening access to the voting process for voters with disabilities or those having other difficulties in being physically present at a polling station and using the devices available there;*
>
> *- increasing voter turnout by providing additional voting channels;*
>
> *- bringing voting in line with new developments in society and the increasing use of new technologies as a medium for communication and civic engagement in pursuit of democracy;*
>
> *- reducing, over time, the overall cost to the electoral authorities of conducting an election or referendum;*
>
> *- delivering voting results reliably and more quickly; and*
>
> *- providing the electorate with a better service, by offering a variety of voting channels."*

The Recommendation therefore promotes the adoption of e-voting by member states. Still, the IP1-S-EE Group is fully aware of the potential risks that could pose a careless introduction of e-voting. As a consequence, the Recommendation sets out elevate prerequisite objectives to ensure public confidence and to ensure an accurate and sound introduction of e-voting:

> *"Aware of concerns about certain security and reliability problems possibly inherent in specific e-voting systems;*
>
> *Conscious, therefore, that only those e-voting systems which are secure, reliable, efficient, technically robust, open to independent verification and easily accessible to voters will build the public confidence which is a pre-requisite for holding e-voting;"*

Scytl, the leading company in secure e-voting technology, has developed Pnyx, a security solution for e-voting that derives from over 10 years of research and development and is protected by international patent applications. Pnyx is a set of software modules that are integrated into electronic voting platforms to guarantee the same level of trust, privacy and security that you get in conventional paper-based electoral systems. Pnyx has been awarded the prestigious 2005 IST Prize by the European Commission and it has been successfully integrated into several electronic voting platforms in Europe, including one of the only two permanent Internet voting platforms for binding elections and consultations in the world.

The purpose of this document is to analyze Pnyx compliance with the security and audit standards set in the Council of Europe's Recommendation Rec(2004)11. Appendix III of the Recommendation includes a total of 23 security standards (from standard 77 through standard 99) and 11 audit standards (from standard 100 through standard 110). This document is organized following the same structure as Sections D (Security) and E (Audit) of Appendix III of the Recommendation and includes each one of the security and audit standards with a brief explanation on how Pnyx complies with them.

Security Standards

I. General requirements

“77. Technical and organisational measures shall be taken to ensure that no data will be permanently lost in the event of a breakdown or a fault affecting the e-voting system.”

- Pnyx has been designed to be deployed in fault tolerant environments.
- The cryptographic protocol protects the integrity and secrecy of the votes. Votes can be backed up without compromising the election integrity and the voters’ privacy.
- The integrity and authenticity of the votes can be checked before retrieving them from any backup.

“78. The e-voting system shall maintain the privacy of individuals. Confidentiality of voters’ registers stored in or communicated by the e-voting system shall be maintained.”

- Votes are sealed (i.e., encrypted) before they are cast.
- Only a pre-determined number of electoral authority members are able to decrypt the votes. If this pre-determined number of electoral authority members is not reached (even if it is only by one person), the members present do not have any information to decrypt the votes.
- The decryption of the votes takes place in an isolated environment (unplugged from any network), physically protected and extensively audited.
- A mixing protocol ensures that after the votes are decrypted, no technician or electoral authority can correlate the clear-text votes with the corresponding voters (or the IP address from which the votes were cast).

"79. The e-voting system shall perform regular checks to ensure that its components operate in accordance with its technical specifications and that its services are available."

- All the actions executed by Pnyx are registered in a tamperproof log.
- The authenticity and integrity of the platform components (e.g., executable programs) is protected by means of digital signatures.
- All the critical information is digitally signed and its integrity is checked before being accepted by any platform component.

"80. The e-voting system shall restrict access to its services, depending on the user identity or the user role, to those services explicitly assigned to this user or role. User authentication shall be effective before any action can be carried out."

- Pnyx uses cryptographic techniques, such as digital certificates and strong authentication, to control the access to its services.
- To execute critical operations, such as the opening of the digital urn, Pnyx requires the collaboration of a pre-determined number of electoral authority members.
- It is impossible, even for a technician or a collusion of technicians with privileged access to the voting system, to know partial results of the election before the end of the voting period and the official opening of the urn.

"81. The e-voting system shall protect authentication data so that unauthorised entities cannot misuse, intercept, modify, or otherwise gain knowledge of all or some of this data. In uncontrolled environments, authentication based on cryptographic mechanisms is advisable."

- Cryptography is the base of Pnyx. All the configuration data, logs and election information is digitally signed. This allows the verification of the authenticity and integrity of any relevant data.

- Pnyx uses standard cryptographic algorithms and, therefore, the authenticity of the data can be checked by external auditors at any time without the need of using proprietary tools.

"82. Identification of voters and candidates in a way that they can unmistakably be distinguished from other persons (unique identification) shall be ensured."

- Pnyx uses strong authentication methods, based on digital certificates, to identify the voters.
- Pnyx additionally supports multiple authentication methods, including biometrics, smartcards, PINs, etc.

"83. E-voting systems shall generate reliable and sufficiently detailed observation data so that election observation can be carried out. The time at which an event generated observation data shall be reliably determinable. The authenticity, availability and integrity of the data shall be maintained."

- Pnyx records all the actions executed in the platform in a tamperproof log.
- The log registers are digitally chained using cryptographic techniques that protect their integrity. These techniques allow the detection of any manipulation of the log registers and also the removal of one or more of the log registers.
- The log also contains information that can be used to crosscheck the register with the election data (such as the digital urn contents).
- Additionally, Pnyx provides voters with tamperproof voting receipts that allow them to verify the correct treatment of their votes.
- The log information and the voting receipts cannot be used the break voters' privacy or to facilitate vote buying and coercion.

"84. The e-voting system shall maintain reliable synchronised time sources. The accuracy of the time source shall be sufficient to maintain time marks for audit trails and

observations data, as well as for maintaining the time limits for registration, nomination, voting, or counting."

- Pnyx components use reliable time sources (e.g., the time of the voter's device is never used to timestamp any information).
- Additionally, Pnyx uses digital signatures to timestamp the generation-time of the contents of the logs and critical data.

"85. Electoral authorities have overall responsibility for compliance with these security requirements, which shall be assessed by independent bodies."

- Pnyx gives complete control over the election to the electoral authorities.
- The electoral authorities are able to verify the fulfillment of the security requirements in a secure environment protected even against potential attacks from the technical personnel.
- With Pnyx, a technician or a collusion of technicians with privileged access to the voting system can never be able to breach the critical security requirements.

II. Requirements in pre-voting stages

"86. The authenticity, availability and integrity of the voters' registers and lists of candidates shall be maintained. The source of the data shall be authenticated. Provisions on data protection shall be respected."

- During the configuration of the election, the electoral authorities review and digitally sign the electoral roll information.
- The digital signature on the electoral roll is verified by Pnyx before importing the electoral roll. Any tampering with the electoral roll would be detected before starting the voting or counting processes.

“87. The fact that candidate nomination and, if required, the decision of the candidate and/or the competent electoral authority to accept a nomination has happened within the prescribed time limits shall be ascertainable.”

- This process is out of the scope of Pnyx.

“88. The fact that voter registration has happened within the prescribed time limits shall be ascertainable.”

- The voter registration process is also out of the scope of Pnyx. As described in standard 86, Pnyx protects the integrity of the electoral roll (registered voters) after this has been digitally signed by the electoral authorities.

III. Requirements in the voting stage

“89. The integrity of data communicated from the pre-voting stage (e.g. voters’ registers and lists of candidates) shall be maintained. Data-origin authentication shall be carried out.”

- Pnyx verifies that the configuration data generated on the pre-voting stage has been digitally signed by the electoral authorities.
- Any changes in the configuration data must be approved and digitally signed by the electoral authorities before being accepted. Any changes without that approval would be detected by Pnyx.

“90. It shall be ensured that the e-voting system presents an authentic ballot to the voter. In the case of remote e-voting, the voter shall be informed about the means to verify that a connection to the official server has been established and that the authentic ballot has been presented.”

- Pnyx uses a client component from which voters can cast their votes securely and privately. This client component is an applet that is executed in the voter's voting device (e.g., personal computer).
- Pnyx applet is digitally signed and voters can check the authenticity of this signature before using it to cast their votes.
- Additionally, Pnyx digitally signed applet generates a voting receipt that allows the voter to verify that his/her vote has been delivered, unaltered, by the voting system to the electoral authorities.

"91. The fact that a vote has been cast within the prescribed time limits shall be ascertainable."

- During the election configuration, the electoral authorities generate two digitally signed opening and closing tokens that ensure that ballots are cast only during the allowed voting period.
- Pnyx digitally signs each encrypted vote with its generation-time information. This provides a tamper-proof timestamp to the vote.

"92. Sufficient means shall be provided to ensure that the systems that are used by the voters to cast the vote can be protected against influence that could modify the vote."

- Pnyx applet is a simple piece of code that can be easily audited and digitally signed by the electoral authorities.
- Voters can check the authenticity of the digital signature on the applet before casting their votes.
- Additionally, Pnyx generates a voting receipt that allows each individual voter to verify the correct treatment of his/her vote.

93. Residual information holding the voter's decision or the display of the voter's choice shall be destroyed after the vote has been cast. In the case of remote e-voting, the voter *shall be provided with information on how to delete, where that is possible, traces of the vote from the device used to cast the vote.*

- The voter casts his/her vote in a digitally signed applet that is executed in his/her voting device (e.g., personal computer). Votes are sealed (i.e., encrypted) in the applet before they are cast and therefore they are never sent unprotected to the voting servers.
- Additionally, the digitally signed applet does not store information on temporary files and destroys all the information after casting a ballot (e.g., it rewrites the memory registers before freeing them).
- Finally, the voting receipt (that the voter can use to verify that his/her vote has been delivered unaltered by the voting system to the electoral authorities) does not disclose the voter's intent (i.e., the content of the vote).

94. The e-voting system shall at first ensure that a user who tries to vote is eligible to vote. The e-voting system shall authenticate the voter and shall ensure that only the appropriate number of votes per voter is cast and stored in the electronic ballot box.

- Pnyx authenticates the voter when he/she first connects to the voting system and again when he/she casts his/her vote.
- Each vote is encrypted (with the public key of the electoral authorities) and the resulting encryption is digitally signed by the corresponding voter. This prevents the addition of bogus ballots in the ballot box without threatening voters' privacy.
- When the digital urn is opened, Pnyx checks that the digital signature on each encrypted vote corresponds to a valid voter in the electoral roll and allows electoral authorities to eliminate bogus and duplicate votes.
- Finally, when the votes are decrypted, a mixing process takes place to break the correlation between votes and voters in order to protect voters' privacy.

"95. The e-voting system shall ensure that the voter's choice is accurately represented in the vote and that the sealed vote enters the electronic ballot box."

- Voters can review their selected voting options and confirm them before casting their votes from the digitally signed applet.
- Voters are provided with a voting receipt (which is based on a unique identifier randomly generated by the digitally signed applet) that allows them to verify that their votes have been delivered by the voting system to the electoral authorities. Note that Pnyx voting receipts go beyond the requirement in this standard since they allow voters to verify not only that their votes have "entered the electronic ballot box" but also that they have reached the electoral authorities, completely unaltered.

"96. After the end of the e-voting period, no voter shall be allowed to gain access to the e-voting system. However, the acceptance of electronic votes into the electronic ballot box shall remain open for a sufficient period of time to allow for any delays in the passing of messages over the e-voting channel."

- Pnyx allows the electoral authorities to define the period of time during which the system will accept votes. This period of time is controlled by two tamperproof tokens (i.e, opening token and closing token) which are digitally signed by the electoral authorities.
- Pnyx only accepts votes cast by voters authenticated before the pre-determined closing time for the election.

IV. Requirements in post-voting stages

"97. The integrity of data communicated during the voting stage (e.g., votes, voters' registers, lists of candidates) shall be maintained. Data-origin authentication shall be carried out."

- Pnyx uses cryptographic techniques to protect the integrity of the data generated during the voting stage. Votes are digitally signed before cast, the digital urns are digitally signed when the vote casting period ends, and the logs are digitally chained and signed during the election process.

"98. The counting process shall accurately count the votes. The counting of votes shall be reproducible."

- The counting process takes place in a controlled and audited environment and it can be started only by a pre-determined number of electoral authority members.
- All data used in the counting process is digitally signed to ensure its authenticity and integrity.
- The counting of votes can be reproduced in a second controlled environment, by the same electoral authority members and using the same digital urn, to check for the consistency of electoral results.
- Additionally Pnyx provides voters with voting receipts that allow them to verify that their votes have been delivered, unaltered, by the voting system to the electoral authorities.
- Voting receipts are based on unique identifiers randomly generated by the digitally signed applets which are sealed with the votes before they are cast.
- At the end of the counting process, the electoral authorities publish the results along with a list of the unique identifiers corresponding to the votes that have been included in the final tally. This allows voters to verify the correct treatment of their votes.

- The voting receipts also represent a mechanism that voters can use to prove the incorrect treatment of their votes. A fraudulent impugnation is impossible because the valid voting receipts are digitally signed.

“99. The e-voting system shall maintain the availability and integrity of the electronic ballot box and the output of the counting process as long as required.”

- Individual votes, the ballot boxes as a whole, and the vote contents list are digitally signed.
- This information can be backed up without compromising voters’ privacy and election integrity.

Audit Standards

I. General

"100. The audit system shall be designed and implemented as part of the e-voting system. Audit facilities shall be present on different levels of the system: logical, technical and application."

- Pnyx generates an audit trail of each of the actions executed in the voting system. The log registers are cryptographically chained and digitally signed to detect and prevent any fraudulent practice.

"101. End-to-end auditing of an e-voting system shall include recording, providing monitoring facilities and providing verification facilities. Audit systems with the features set out in sections II – V below shall therefore be used to meet these requirements."

- Pnyx audit logs allow the verification and reproduction of the status of the election at any time during the process.
- Pnyx incorporates tools that can be used during the election to view the logs and to check the integrity of the log contents (registers).

II. Recording

"102. The audit system shall be open and comprehensive, and actively report on potential issues and threats."

- Pnyx records the information in a human readable form. Log registers are stored in a data base system to facilitate the generation of audit reports.

- Pnyx provides cryptographic information that allows to check the integrity of the log registers.
- The log integrity can be checked without the need of proprietary tools because Pnyx uses standard cryptographic algorithms (RSA, AES, SHA-1…).
- The contents of the audit logs allow the verification and reproduction of the status and integrity of the election at any given time.

"103. The audit system shall record times, events and actions, including:"

> *"a. all voting-related information, including the number of eligible voters, the number of votes cast, the number of invalid votes, the counts and recounts, etc.;"*

- All this information is recorded by Pnyx.

> *"b. any attacks on the operation of the e-voting system and its communications infrastructure;"*

- Pnyx verifies the integrity and authenticity of all the processed data. In case of any inconsistency, this situation is reported immediately.

> *"c. system failures, malfunctions and other threats to the system."*

- Any malfunction or threat that causes a problem with the election integrity is detected, rejected (or isolated) and reported.

III. Monitoring

"104. The audit system shall provide the ability to oversee the election or referendum and to verify that the results and procedures are in accordance with the applicable legal provisions."

- Logs, configuration information and election data have a standardized format (XML). The authenticity and integrity of these data can be verified by standard means (digital signature).

“105. Disclosure of the audit information to unauthorised persons shall be prevented.”

- Pnyx protects the election privacy and integrity even in the case of an unauthorized access.

“106. The audit system shall maintain voter anonymity at all times.”

- Voter anonymity is protected during the audit process. It is possible to prove that the electoral results derive from the digital urn with the encrypted votes. However, there are no means to correlate the decrypted final votes to the original encrypted votes.

IV. Verifiability

“107. The audit system shall provide the ability to cross-check and verify the correct operation of the e-voting system and the accuracy of the result, to detect voter fraud and to prove that all counted votes are authentic and that all votes have been counted.”

- Pnyx logs and election data allow auditors to verify the integrity of the overall election.
- Additionally, the voting receipts allow voters to verify by themselves the correct treatment of their corresponding votes.

"108. The audit system shall provide the ability to verify that an e-election or e-referendum has complied with the applicable legal provisions, the aim being to verify that the results are an accurate representation of the authentic votes."

- Pnyx generates tamperproof election and audit data that can be checked by auditors using standard (non-proprietary) tools.
- Additionally, as stated above, the voting receipts allow voters to verify the correct treatment of their corresponding votes.

V. Other

"109. The audit system shall be protected against attacks which may corrupt, alter or lose records in the audit system."

- The integrity and authenticity of the log registers and all the election data are cryptographically protected.

"110. Member states shall take adequate steps to ensure that the confidentiality of any information obtained by any person while carrying out auditing functions is guaranteed."

- With Pnyx, it is unfeasible for auditors, system administrators or electoral authorities to threaten voters' privacy.

About Scytl

Scytl is a software company specialized in application-level cryptography and a worldwide leader in developing security solutions for the electronic voting industry.

Scytl was formed in 2001 as a spin-off from a leading research group at the *Universitat Autònoma de Barcelona* that has pioneered the research of security solutions for the electronic voting industry since 1994. This group accounts for over 20 scientific papers published in international journals, holds the only two European PhD thesis on the subject and participated in the first Internet binding election in Europe in 1997. One of these PhD thesis, "Design of Implementable Solutions for Large Scale Electronic Voting Schemes", is from Andreu Riera, Scytl's co-founder and Chairman.

Scytl commercializes a unique software product, Pnyx, that derives from its more than 10 years of research and development and is protected by international patent applications. Pnyx is a set of software modules that are integrated into electronic voting platforms to guarantee the same level of trust, privacy and security that you get in conventional electoral systems.

Pnyx has been successfully installed in several e-voting platforms in Europe, including the platform of the Swiss Cantons of Neuchâtel, one of the only two permanent Internet voting platforms for binding elections and consultations in the world. Pnyx has also been used in numerous e-voting projects for the public and private sectors. Recently, Pnyx was used as the secure voting engine in Madrid Participa, one of the largest e-participation events in Europe. Approximately 135.000 residents of the Centre district of Madrid were consulted on three key issues affecting their district and were allowed to participate through the Internet (remotely and from kiosks) and mobile phones. The project was led by Scytl and Accenture with the cooperation of companies such as Intel, Hewlett Packard, Oracle and Telefonica.

Scytl has received recognition and numerous awards from European, Spanish and Catalan institutions for its technology and achievements. Scytl finished second in the 2002 edition of the 50K contest organized by the San Telmo foundation (Seville), finished third in the first European Technology Company competition held in London in September 2002 (organized by Hewlett Packard), received the Best Technology Company award in Barcelona in March 2003 and was one of the 60 Nominees in the IST Prize 2004. The Spanish Science and Technology Ministry has supported Scytl through CDTI's Neotec initiative.

More recently, the European Commission selected Scytl as one of the twenty European IST Prize Winners, the most prestigious award for a technology company in Europe. The decision was made by 16 independent experts nominated by Euro-CASE among the 430 innovative companies from 29 European countries that competed for the 2005 European IST Prize.

Secured by scytl

Entença 95, 4-1
08015 Barcelona
SPAIN

tel:. +34 934 230 324
fax: +34 933 251 028

http://www.scytl.com