E-Voting: A Scalable Approach using XML and Hardware Security Modules

EEE Conference 2005
Hong Kong, 31st March 2005

Thomas Rössler
About A-SIT

**Secure Information Technology Center – Austria**

- **Founded:** 1999
- **Business Fields:**
  - Attestation of Secure Signature Creation Devices according to the EU Directive on Secure Electronic Signatures (1999/93/EC)
  - Austrian E-Government Initiative
  - Attestation of Online Payment Systems

Secure Information Technology Center – Austria
Contents

- Introduction
- The Concept
  - Phase 1 and Phase 2
- The Counting Process
- Outlook & Summary
Introduction

◆ This project aims to create an electronic voting system especially for Austrian elections
  - remote voting via the Internet
◆ It is heavily leant on the procedure of real elections which is taken from the Austrian electoral law
  - we “implement” the concept for postal voting in Austria
◆ We follow the Recommendations of:
  - the European Commission
    “Recommendation of the Committee of Ministers to member states on legal, operational and technical standards for e-voting”
Requirements

◆ Major principles of democratic elections:
  ✤ universal
  ✤ equal
  ✤ free
  ✤ secret
  ✤ direct suffrage

◆ Additionally to these requirements, the voting system should…
  ✤ … provide recounts at any time
  ✤ … the result has to be accurate and detailed
  ✤ … enable write-in votes
  ✤ … provide a permanent audit trail
  ✤ … authenticate/identify voters uniquely
Requirements

- we make use of the technical framework given by the Austrian E-Government

- Austrian E-Government Framework:
  - XML technologies
  - Citizen Card
    - Signature Creation Device according 1999/93/EC
    - XML-Signatures and XML-Encryption
    - unique identification/authentication of citizens
  - various base services
    - e.g. electronic delivery, etc.
Contents

- Introduction
- The Concept
  - Phase 1 and Phase 2
- The Counting Process
- Outlook & Summary
The Concept

- Our e-voting model is a two phase model
  - **Phase 1**: voter registers for e-voting
  - **Phase 2**: voter casts the vote

- Key-Element is the *Electronic Urn*
  - its core is a hardware security module (HSM) for which all votes are encrypted
  - only inside the urn (inside the HSM) a vote can be decrypted and counted
Phase 1: Registration

Voter

Registration Authority (RA)

Identify and authenticate voter
Phase 1: Registration

Voter

Registration Authority (RA)

RA generates voter’s unique voting identifier and blank ballot

Voting Identifier itself and the whole document is signed by the RA

XML

Constituency Region Nord
Voting Identifier 12345678ABCDEFG

Ballot

- 

- 

- 

-
Phase 1: Registration

Voter sends a request to the Registration Authority (RA).

RA generates voter’s unique voting identifier and blank ballot.

Voter receives the public key of the Election Authority for encrypting his/her ballot.
Phase 1: Registration

◆ At the end of Phase 1, the voter...
  ▶ ...has got a **voting token** containing his unique **voting identifier**
  ▶ ...has received the **blank ballot**
  ▶ ...has received the **public key** of the electronic urn in order to be able to encrypt the vote before casting
  ▶ ...has verified the **electronic signatures** on the voting token/identifier and on the blank ballot

◆ the **Registration Authority**...
  ▶ has marked the voter in the voting register in order to prevent multiple cast votes
Phase 1: Registration
Phase 2: Voting

Voter votes and encrypts the vote using the urn's public key.

signs the vote and the voting token by the use of his citizen card.
Phase 2: Voting

Voter votes and encrypts the vote using the urn's public key.

signs the vote and the voting token by the use of his citizen card.

Election Authority (EA)
Phase 2: Voting

Voter

votes and encrypts the vote using the urn's public key

signs the vote and the voting token by the use of his citizen card

Election Authority (EA)

verify signature
mark voter
stamp vote
store vote

send confirmation
Contents

- Introduction
- The Concept
  - Phase 1 and Phase 2
- The Counting Process
- Outlook & Summary
Counting-Process

- set of cast votes
- sorted by constituency
- sorted by voting identifier
- detect erroneous multiple cast votes

Electronic Urn

- separates voting identifier from ballot
- decrypts ballot
- increases counter

Result available only when all votes of a given set are counted
Counting-Process

Hardware Security Module

check for:
duplicates & constituency

Incremental Hash-Value of voting-IDs

stop counting

Result

Constituency Region Nord Voting Identifier

Wer Geistern dient, die nicht seine eigenen sind, ist ein Schmähling. Wer eine Gelegenheit zu rechtschaffenem Tun sieht, sie aber nicht ergreift, der ist ein Feigling.
Counting-Process

Audit

check for: duplicates & constituency

Incremental Hash-Value of voting-IDs

split

Hardware Security Module

0|1|4|3

0|2|2|3

Result

stop counting

Constituency
Region Nord
Voting Identifier
Contents

◆ Introduction
◆ The Concept
  ▪ Phase 1 and Phase 2
◆ The Counting Process
◆ Outlook & Summary
Summary

we follow a very pragmatical approach using the Austrian E-Government infrastructure

- i.e. XML, Citizen Card, etc.

following…

- … the Austrian Electoral Law
- … Recommendations given by the EC

key element: *Electronic Urn*

- for which all ballots are encrypted
- only inside this urn (HSM) and only for counting ballots become decrypted
Ongoing Work and Outlook

◆ we are developing a prototypical implementation of this concept
◆ Currently, we mainly…
  ◦ … specify all XML-interfaces/documents based on the Election Markup Language (EML)
  ◦ … specify the electronic urn in detail and create a simulator for it
◆ we make use of our existing E-Government framework, such as
  ◦ … Citizen Card for XML-Signatures and Encryption
  ◦ … Electronic Delivery Service

we aim to be prepared for a simulation of an election by the end of this year
Thank you for your attention…

Thomas Rössler
thomas.roessler@a-sit.at

Secure Information Technology Center – Austria