

Requirements and Evaluation Procedures for eVoting

Margaret McGaley

NUI Maynooth

13th December 2006

Thanks to Melanie Volkamer

mmcgaley@cs.nuim.ie

Previous work

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- EVT 06
- A Critical Analysis of the Council of Europe Recommendations on e-voting
- With Paul Gibson

Other requirements 'catalogues'

- Council of Europe recommendations
- German regulations
- PTB 'Online-Voting Systems for Non-parliamentary Elections'
- Other nation-specific catalogues
 - Australia
 - The Netherlands
 - Hamburg
 - US

Other requirements 'catalogues' - issues

- Too abstract/too concrete
- Internally inconsistent/incomplete
- Tied to context
- Impossible to evaluate

Proposal

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- New catalogue
- Aim to avoid previous flaws
- Start with a subset of systems
 - Polling place
 - Not networked
 - Exclude mark-sense, digital pen
 - Exclude registration, authentication
- Develop requirements
 - Leave out those that apply to paper system
- Discuss evaluation

Terminology

- SHALL and SHOULD as in RFC 2119
- Normal form, non-core
- Election terminology ambiguous
- Glossary (eg)
 - election: the proceedings accompanying the formal choosing of the winner(s) of one or more polls
 - poll: a decision between options such as candidates for a position, or choices in a referendum which is determined by votes cast by eligible voters
- links between reqs

Election principles

- Secret: [se] The voting system SHALL prevent anyone without the appropriate authority* from deducing or proving the link between a particular elector and his vote.
- Free: [fr] The voting system SHALL protect the voters right to express his vote in a free manner, without any coercion or undue influence.
- Equal: [eq] The voting system SHALL ensure that each voter may only cast one vote per poll.
- Universal: [un] The voting system SHALL protect the right of an eligible voter to cast his vote.
- Direct: [di] The voting system SHALL determine the results of a poll based on all votes cast and only such votes.
- Trust: [tr] The voting system SHALL be implemented with the aim of maximising public trust.
- All: [all]

Election phases

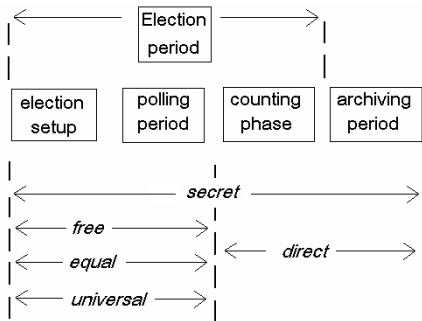


Figure: election phases

Categories of requirements

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- security (reqs for hw and sw which mitigate against threats)

Categories of requirements

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- security (reqs for hw and sw which mitigate against threats)
- functional (reqs specify the behaviour)

Categories of requirements

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- security (reqs for hw and sw which mitigate against threats)
- functional (reqs specify the behaviour)
- usability (functional reqs related to user-interfaces)

Categories of requirements

- security (reqs for hw and sw which mitigate against threats)
- functional (reqs specify the behaviour)
- usability (functional reqs related to user-interfaces)
- operational (responsible election authority and poll-workers)

Categories of requirements

- security (reqs for hw and sw which mitigate against threats)
- functional (reqs specify the behaviour)
- usability (functional reqs related to user-interfaces)
- operational (responsible election authority and poll-workers)
- assurance (measures taken during dev and eval of the product to assure compliance with requirements)

Requirements

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Security: 27
- Functionality: 10
- Usability: 7
- Organisational: 11
- Assurance: 13

Requirements - examples

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Sec 12 [se] The voting device SHOULD not store any information which could link the voter with his vote. Where such information is stored it SHALL only be accessible to those with appropriate authority

Requirements - examples

- Sec 19 [all] The voting devices behaviour SHALL map onto the finite state machine in figure 2

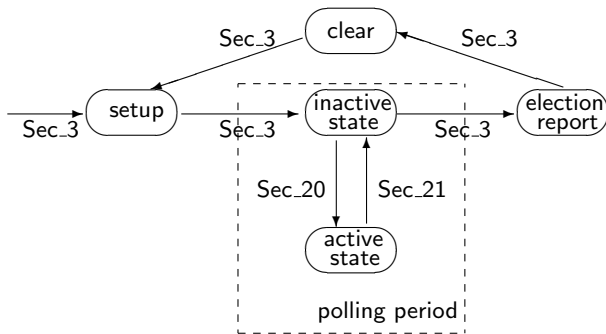


Figure: election phases

Requirements

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Funct 10 [fr] [non-core] The vote-casting interface SHOULD warn the voter when he tries to spoil his vote in one or more polls (ref Funct 9)

Requirements

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Usab 6 [fr] The vote-casting interface SHALL protect the voter from accidentally casting his vote

Requirements

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Org 11 [all] The poll-workers SHALL respond to system messages in accordance with the user-guide (ref Assur 5 and Org 9)

Requirements

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Assur 6 [tr] The manufacturer SHALL disclose the documentation from Assur 5, executable program, source code, bug tracking, version control (at least to the testing authority) (Org 5)

Evaluation

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Common criteria

Evaluation

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Common criteria
 - Framework for security requirements

Evaluation

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Common criteria
 - Framework for security requirements
 - Protection profile

Evaluation

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Common criteria
 - Framework for security requirements
 - Protection profile
 - Set of pre-defined requirements with evaluation procedures

Evaluation

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Common criteria
 - Framework for security requirements
 - Protection profile
 - Set of pre-defined requirements with evaluation procedures
 - Equate our reqs with CC reqs, eval for free!

Evaluation

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Common criteria
 - Framework for security requirements
 - Protection profile
 - Set of pre-defined requirements with evaluation procedures
 - Equate our reqs with CC reqs, eval for free!
 - All our security and assurance requirements

Evaluation

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Other categories don't fit common criteria

Evaluation

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Other categories don't fit common criteria
 - Functional

Evaluation

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Other categories don't fit common criteria
 - Functional
 - Usability

Evaluation

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Other categories don't fit common criteria
 - Functional
 - Usability
 - Organisational

Evaluation

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Normal form

Evaluation

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Normal form
 - **A SHALL ensure that B.**

Evaluation

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Normal form
 - **A SHALL** ensure that **B**.
 - **A SHOULD** ensure that **B**. **A SHALL** ensure that **C**.

Evaluation

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Normal form
 - **A** SHALL ensure that **B**.
 - **A** SHOULD ensure that **B**. **A** SHALL ensure that **C**.
- More reviewers

Evaluation

Requirements
and
Evaluation
Procedures for
eVoting

Margaret
McGaley

Introduction

Proposal

Requirements

Evaluation

Future work

- Normal form
 - **A** SHALL ensure that **B**.
 - **A** SHOULD ensure that **B**. **A** SHALL ensure that **C**.
- More reviewers
- Rearrange to uncover gaps

Evaluation

- Normal form
 - **A** SHALL ensure that **B**.
 - **A** SHOULD ensure that **B**. **A** SHALL ensure that **C**.
- More reviewers
- Rearrange to uncover gaps
- Check internal, external consistency

Evaluation

- Normal form
 - **A** SHALL ensure that **B**.
 - **A** SHOULD ensure that **B**. **A** SHALL ensure that **C**.
- More reviewers
- Rearrange to uncover gaps
- Check internal, external consistency
- Non-core, audit reqs

Evaluation

- Normal form
 - **A** SHALL ensure that **B**.
 - **A** SHOULD ensure that **B**. **A** SHALL ensure that **C**.
- More reviewers
- Rearrange to uncover gaps
- Check internal, external consistency
- Non-core, audit reqs
- Contradictions/dependencies

Evaluation

- Normal form
 - **A** SHALL ensure that **B**.
 - **A** SHOULD ensure that **B**. **A** SHALL ensure that **C**.
- More reviewers
- Rearrange to uncover gaps
- Check internal, external consistency
- Non-core, audit reqs
- Contradictions/dependencies
- More systems