Evaluating RIES using the proposed Protection Profile

Hugo Jonker — Eindhoven University of Technology & University of Luxembourg

Melanie Volkamer — University of Passau

Introduction
rationale
Protection profile
RIES
Analysis
Conclusions

Why RIES?

Why the protection profile (PP)?

rationale

Introduction
rationale
Protection profile
RIES
Analysis
Conclusions

Why RIES?

- used for parlementarian elections
- security not thoroughly investigated

Why the protection profile (PP)?

rationale

Introduction
rationale
Protection profile
RIES
Analysis
Conclusions

Why RIES?

- used for parlementarian elections
- security not thoroughly investigated

Why the protection profile (PP)?

- Common Criteria (CC) = internationally accepted security standard
- PP (part of CC) has been recently developed
- test-case: how to apply the PP?

outline

Introduction

Protection profile
- outline
- requirements

RIES

Analysis

Conclusions

- describes specific security requirements for product category
- compliance to a PP does not imply total security(!)

This PP, *Core Requirements for Remote Electronic Voting*:

- aimed at “regular” elections
- geared towards interface

requirements

Introduction

Protection profile
- outline
- requirements

RIES

Analysis

Conclusions

- OverhasteProtection
- Correction
- Confirmation
- OneVoterOneVote
- VoteCount
- AnonElectionCommittee
- after-Integrity
- Cancel
- After-BallotBox
- EndElection
- IntegrityElectionCommittee
- SecretElectionCommittee
- Malfunction
- Log
- StartVoteCount
- SecretMessage
- AuthElectionCommittee
- UnauthorisedVoter
- NoProof
- after-ElectionSecrecy
- IntegrityMessage
- ElectionSecrecy

about

Introduction

Protection profile

RIES
- about
- verifiability
- pre-election
- election phase
- post election

Analysis

Conclusions

History:

- originally developed for water management board elections used in different regional elections, successful
- adapted for ex-pat voting (*RIES-KOA*, 2006)
- based on academic work, actively monitored by researchers, OSCE, WVSCN.NL

about

Introduction

Protection profile

RIES
- about
- verifiability
- pre-election
- election phase
- post election

Analysis

Conclusions

History:

- originally developed for water management board elections used in different regional elections, successful
- adapted for ex-pat voting (*RIES-KOA*, 2006)
- based on academic work, actively monitored by researchers, OSCE, WVSCN.NL

Noteworthy aspects:

- integrates mail-voting and e-voting
- 3 phases: pre-election, election, post election
- verifiability by hashes and commitments

verifiability

Introduction

Protection profile

RIES
- about
- verifiability
- pre-election
- election phase
- post election

Analysis

Conclusions

Per voter:

- identity i, secret key $sk(i)$
- “personalised” list of candidates $\mathcal{C}_i$

verifiability

Introduction

Protection profile

RIES
- about
- verifiability
- pre-election
- election phase
- post election

Analysis

Conclusions

Per voter:

- identity i, secret key $sk(i)$
- “personalised” list of candidates $\mathcal{C}_i$

i

1	can_1
$\vdots$	$\vdots$
n	can_n

$\mathcal{C}$

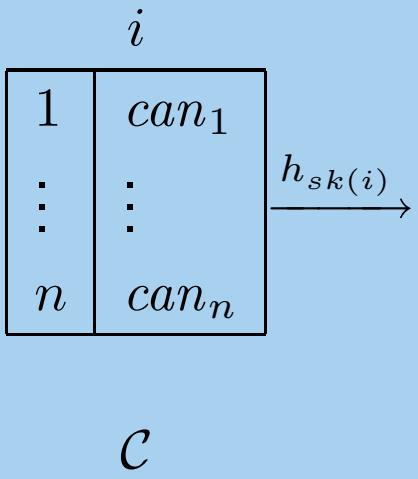
verifiability

Introduction
Protection profile
RIES
- about
- verifiability
- pre-election
- election phase
- post election

Analysis
Conclusions

Per voter:

- identity i, secret key $sk(i)$
- "personalised" list of candidates $\mathcal{C}_i$



verifiability

Introduction

Protection profile

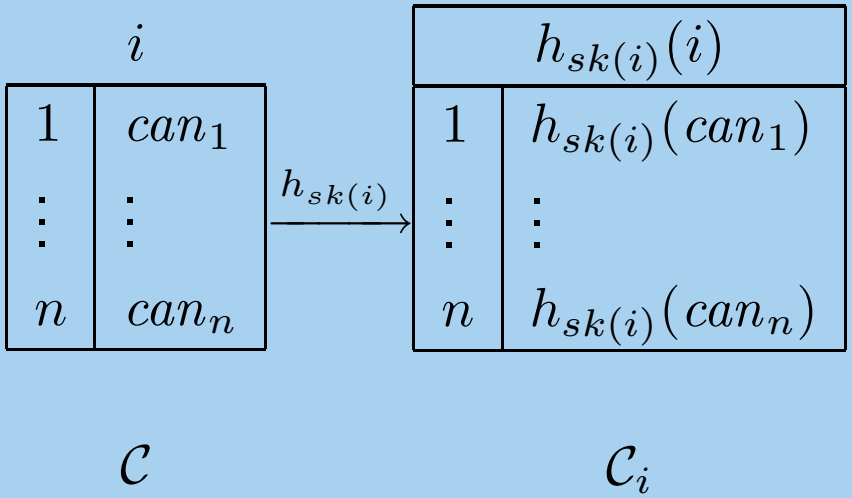
RIES
- about
- verifiability
- pre-election
- election phase
- post election

Analysis

Conclusions

Per voter:

- identity i, secret key $sk(i)$
- “personalised” list of candidates $\mathcal{C}_i$

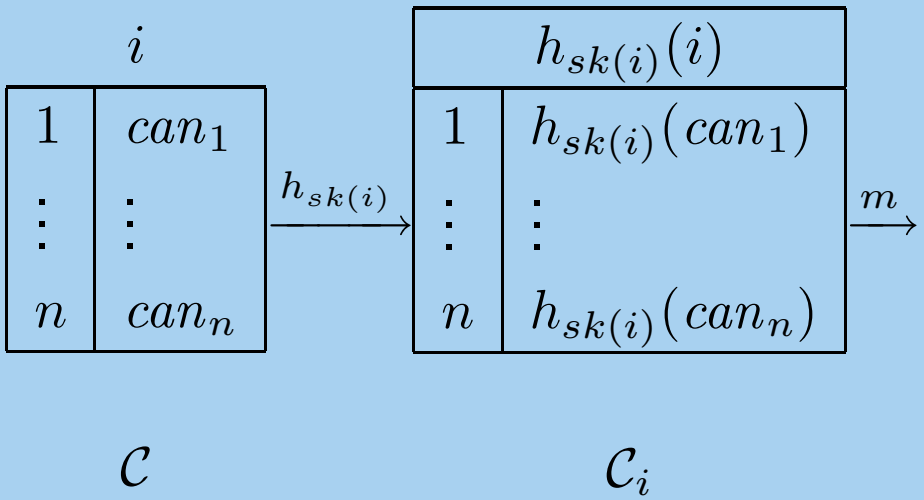


Introduction
Protection profile
RIES
- about
- verifiability
- pre-election
- election phase
- post election

Analysis
Conclusions

Per voter:

- identity i, secret key $sk(i)$
- "personalised" list of candidates $\mathcal{C}_i$



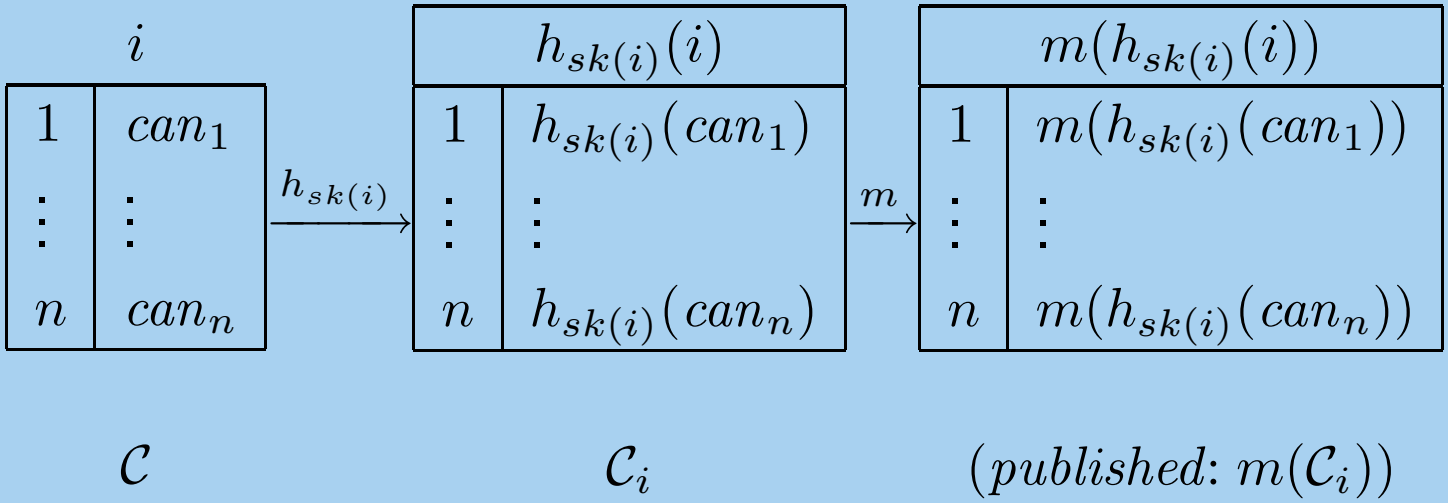
verifiability

Introduction
Protection profile
RIES
- about
- verifiability
- pre-election
- election phase
- post election

Analysis
Conclusions

Per voter:

- identity i, secret key $sk(i)$
- "personalised" list of candidates $\mathcal{C}_i$



pre-election

Introduction

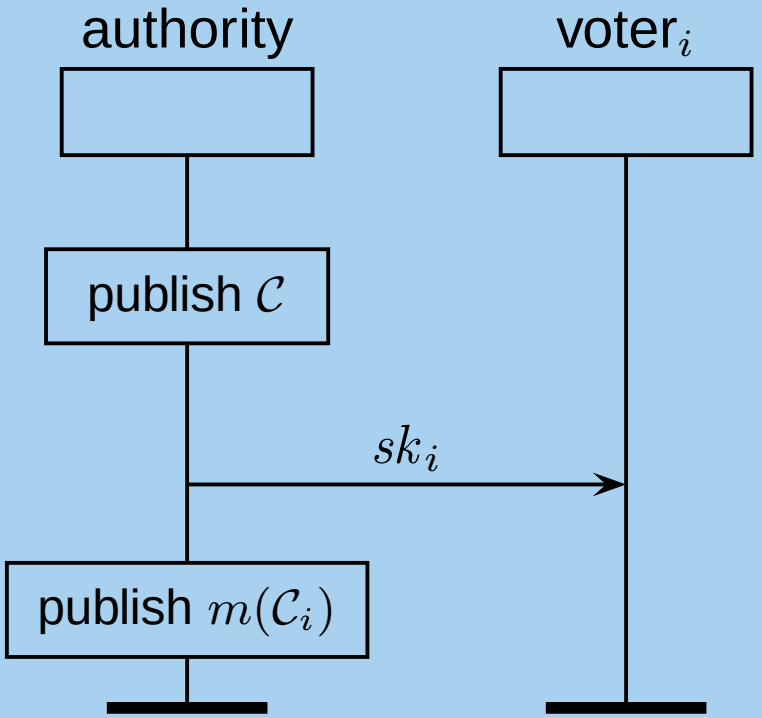
Protection profile

RIES
- about
- verifiability
- pre-election
- election phase
- post election

Analysis

Conclusions

via post office



election phase

Introduction

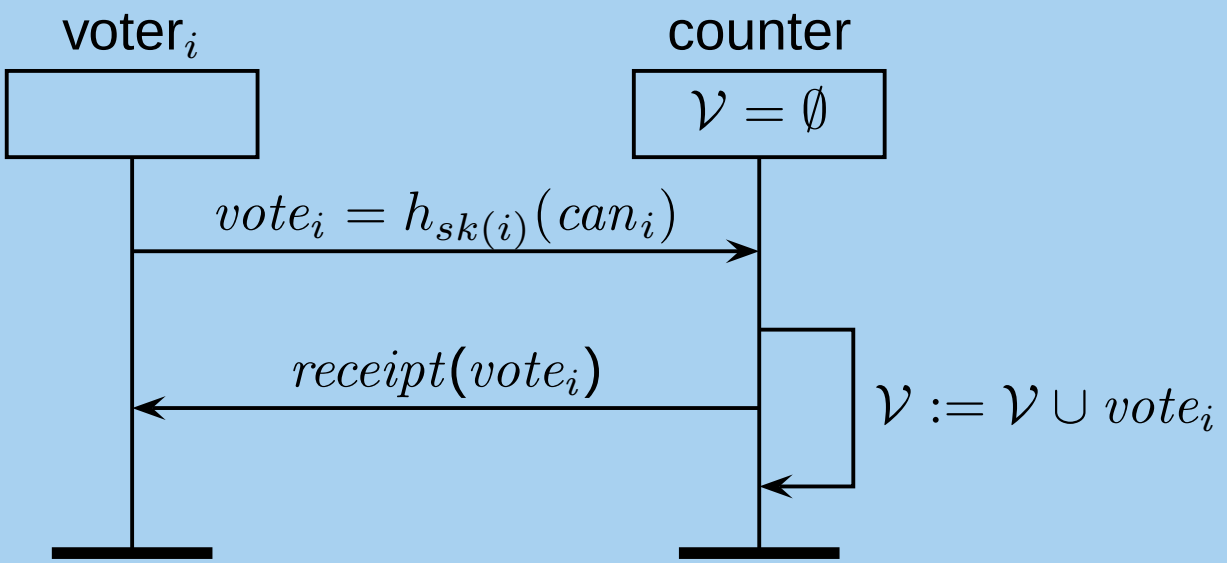
Protection profile

RIES
- about
- verifiability
- pre-election
- election phase
- post election

Analysis

Conclusions

over ssl channel



post election

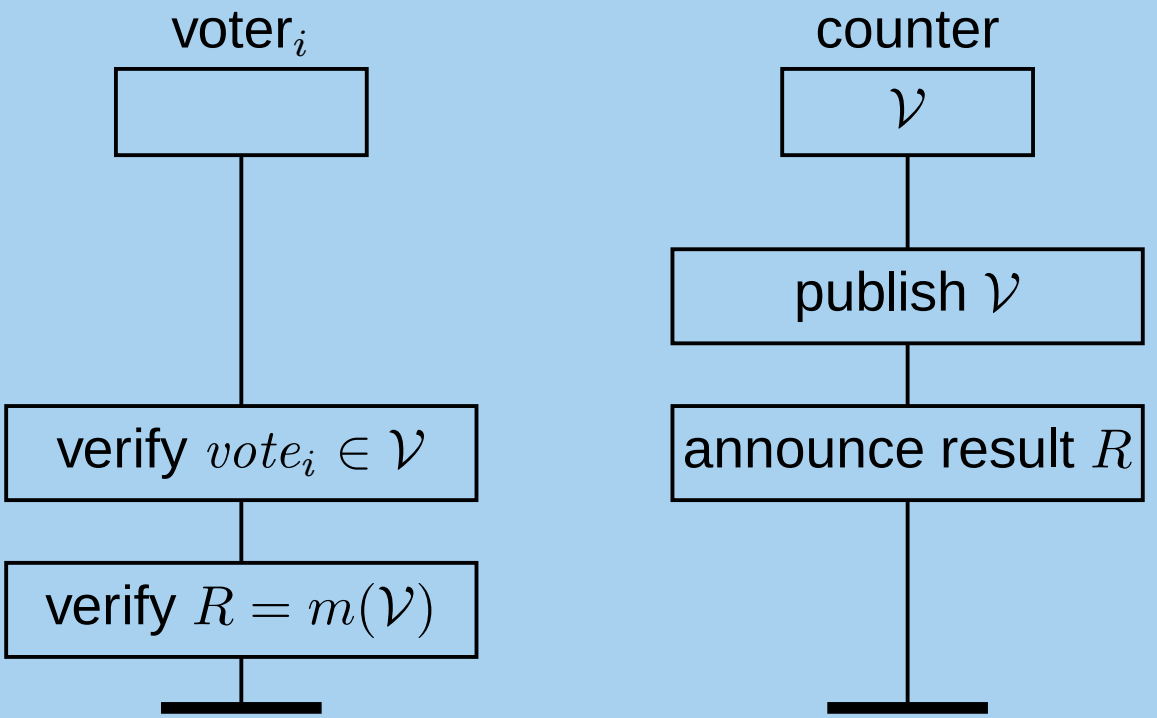
Introduction

Protection profile

RIES
- about
- verifiability
- pre-election
- election phase
- post election

Analysis

Conclusions



approach

Introduction

Protection profile

RIES

Analysis
- approach
- results
- results (cont.)

Conclusions

- not full blown CC-analysis
- based on available documentation
- extended with information gained from discussions / meetings

results

Introduction
Protection profile
RIES
Analysis
- approach
- results
- results (cont.)

Conclusions

objective	outcome
OverhasteProtection	PASS
Correction	PASS
Confirmation	PASS
OneVoterOneVote	PASS
VoteCount	PASS
AnonElectionCommittee	PASS
after-Integrity	PASS
Cancel	PASS
after-BallotBox	PASS

results (cont.)

Introduction

Protection profile

RIES

Analysis
- approach
- results
- results (cont.)

Conclusions

objective	outcome
EndElection	INCONCL
IntegrityElectionCommittee	INCONCL
SecretElectionCommittee	INCONCL
Malfunction	INCONCL
Log	INCONCL
StartVoteCount	INCONCL
SecretMessage	FAIL
AuthElectionCommittee	FAIL
UnauthorisedVoter	FAIL
NoProof	FAIL
after-ElectionSecrecy	FAIL
IntegrityMessage	FAIL
ElectionSecrecy	FAIL

on RIES

Introduction
Protection profile
RIES
Analysis
Conclusions
on RIES
on PP

- documentation lacking (SSL configuration)

on RIES

Introduction
Protection profile
RIES
Analysis
Conclusions
on RIES
on PP

- documentation lacking (SSL configuration)
- voter proofs available

on RIES

Introduction
Protection profile
RIES
Analysis
Conclusions
on RIES
on PP

- documentation lacking (SSL configuration)
- voter proofs available
- self-tests? availability of ballot box? logging? starting/stopping guards?

on RIES

Introduction
Protection profile
RIES
Analysis
Conclusions
- on RIES
- on PP

- documentation lacking (SSL configuration)
- voter proofs available
- self-tests? availability of ballot box? logging? starting/stopping guards?
- authorised voters only!

on RIES

Introduction
Protection profile
RIES
Analysis
Conclusions
- on RIES
- on PP

- documentation lacking (SSL configuration)
- voter proofs available
- self-tests? availability of ballot box? logging? starting/stopping guards?
- authorised voters only!

Impact:
Suggestions for improvements will be in paper and communicated to voting officials and RIES developers.

on PP

- emphasis on interfaces and correctness

Introduction
Protection profile
RIES
Analysis
Conclusions
on RIES
on PP

on PP

Introduction
Protection profile
RIES
Analysis
Conclusions
- on RIES
- on PP

- emphasis on interfaces and correctness
- not enough requirements on environment

on PP

Introduction
Protection profile
RIES
Analysis
Conclusions
on RIES
on PP

- emphasis on interfaces and correctness
- not enough requirements on environment
- strong assumptions

on PP

Introduction
Protection profile
RIES
Analysis
Conclusions
on RIES
on PP

- emphasis on interfaces and correctness
- not enough requirements on environment
- strong assumptions
- compliance does not imply a secure voting system

on PP

Introduction
Protection profile
RIES
Analysis
Conclusions
on RIES
on PP

- emphasis on interfaces and correctness
- not enough requirements on environment
- strong assumptions
- compliance does not imply a secure voting system
- compliance does (strongly) indicate a correct and somewhat secure voting system

on PP

Introduction
Protection profile
RIES
Analysis
Conclusions
on RIES
on PP

- emphasis on interfaces and correctness
- not enough requirements on environment
- strong assumptions
- compliance does not imply a secure voting system
- compliance does (strongly) indicate a correct and somewhat secure voting system

Future work:

on PP

Introduction
Protection profile
RIES
Analysis
Conclusions
on RIES
on PP

- emphasis on interfaces and correctness
- not enough requirements on environment
- strong assumptions
- compliance does not imply a secure voting system
- compliance does (strongly) indicate a correct and somewhat secure voting system

Future work:

- widen scope of PP to accomodate RIES (and similar)
- extend coverage of PP to catch more security

Introduction
Protection profile
RIES
Analysis
Conclusions
- on RIES
- on PP

Thank you for your attention!

hugo.jonker@uni.lu
http://satoss.uni.lu/hugo/