FIDIS

Future of Identity in the Information Society

Title:	"D16.2b: Conference on E-Voting and Identity"
Author:	WP16
Editors:	Ammar Alkassar, Rani Husseiki (Sirrix, Germany)
Reviewers:	Melanie Volkamer, Els Kindt
Identifier:	D16.2b
Type:	[Workshop]
Version:	0.3
Date:	Saturday, 09 May 2009
Status:	[Final]
Class:	[Public]
File:	fidis_wp16-del16.2b_conference_E-Voting and Identity.doc

Summary

The deliverable highlights the topics, presentations and results as well as the organizational aspects of the *First Conference on E-Voting and Identity (VOTE-ID 2007)* that was held on October 4 - 5, 2007 in Bochum, Germany.

The workshop was an international research meeting point for e-voting experts from different disciplines who gave presentations about the different aspects of e-voting and identity. The workshop ended with a panel discussion for reflection over previous sessions, and projections towards further research and development in the e-voting field. The revised selected papers of the workshop were published under the Lecture Notes in Computer Science (LNCS 4896) of Springer as "E-Voting and Identity". The second conference VOTE-ID is hosted by the University Luxembourg.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

PLEASE NOTE: This document may change without notice – Updated versions of this document can be found at the FIDIS NoE website at www.fidis.net.

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz (ICPP)	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University[1]	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne (MU)	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science (LSE)	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Centre Technique de la Gendarmerie Nationale (CTGN)	France
19. Netherlands Forensic Institute (NFI)[2]	Netherlands
20. Virtual Identity and Privacy Research Center (VIP)[3]	Switzerland
21. Europäisches Microsoft Innovations Center GmbH (EMIC)	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

[1] Legal name: Stichting Katholieke Universiteit Brabant
[2] Legal name: Ministerie Van Justitie
[3] Legal name: Berner Fachhochschule

Versions

Version	*Date*	*Description (Editor)*
0.1	30.09.2007	First Draft (Rani Husseiki)
0.2	15.10.2007	Revision (Ammar Alkassar)
0.3	06.05.2009	Final Revision after Review (Ammar Alkassar)

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1 (Executive Summary)	Rani Husseiki
2 (Call for Papers)	Rani Husseiki
3 (Preface and Forward)	Kai Rannenberg, Ammar Alkassar
4 (Agenda)	Rani Husseiki
5 (Springer Publication)	Rani Husseiki
6 (Participants)	Rani Husseiki, Céline Fischer

Table of Contents

1 Executive Summary

The *First Conference on E-Voting and Identity (VOTE-ID 2007)* was held on October 4 - 5, 2007 in Bochum, Germany. The workshop was an international research meeting point for more than 43 e-voting experts from different disciplines.

The main goals of the workshop were to shed the light on the interrelation between E-voting and identity, especially when anonymity, privacy, trust, identity fraud, technological means and legal issues are all involved while assessing the implications of identification on E-voting.

Forty-six participants joined the workshop, particularly computer scientists (security, usability, availability, and software engineering), lawyers, sociologist and politicians. Presentations and discussions spanned over several aspects like voting machines, remote electronic e-voting, evaluation of voting systems, verifiability techniques, e-voting in different countries, e-voting and trust, improving existing e-voting approaches and in particular code-voting schemes.

The workshop ended with a panel discussion for reflection over previous sessions, and projections towards further research and development in the e-voting fields.

The revised selected papers of the workshop were published under the Lecture Notes in Computer Science (LNCS 4896) of Springer as “E-Voting and Identity”.

2 Call for Papers

In this section, the Call for Papers (CfP) as published in the scientific community is presented.

2.1 Header

VOTE-ID 2007:
"First Conference on E-Voting and Identity"

Bochum (Germany), October 4 - 5, 2007

This workshop is the international research meeting point for e-voting experts from different disciplines: computer scientists (security, usability, availability, and software engineering), lawyers, sociologist and politicians.

2.2 Program Chairs

***** Ammar Alkassar (Sirrix AG security technologies – GE)

Melanie Volkamer (Institute of IT-Security and Security Law – GE)

2.3 Program-Committee

Josh Benaloh (Microsoft – US)

Klaus Brunnstein (University of Hamburg – GE)

Rüdiger Grimm (University of Koblenz-Landau – GE)

***** Marit Hansen (Independent Center of Privacy Protection – GE)

Dirk Heckmann (University of Passau – GE)

***** David-Olivier Jaquet-Chiffelle (University of Applied Sciences of Bern – CH)

Frank Koob (Federal Office for Information Security, BSI – GE)

Robert Krimmer (evoting.cc – AT)

***** Ronald Leenes (Tilburg University – NL)

Helger Lipmaa (University College London – UK)

Sjouke Mauw (University of Luxembourg – LU)

Margaret McGaley (NUI Maynooth – IR)

Lilian Mitrou (University of the Aegean – GR)

Olivier Pereira (Université Catholique de Louvain – BE)

Günther Pernul (University of Regensburg – GE)

***** Andreas Pfitzmann (Technical University of Dresden – GE)

***** Bart Preneel (Katholieke Universiteit Leuven – BE)

***** Kai Rannenberg (University Frankfurt – GE)

Peter Ryan (Newcastle University – UK)

Ahmad-Reza Sadeghi (University of Bochum – GE)

Joseph Savirimuthu (University of Liverpool – UK)

Berry Schoenmakers (TU Eindhoven – NL)

7 PC-members are affiliated with FIDIS partners and are marked with an asterisk.

2.4 Goals

The aim of this Workshop is to bring together e-voting specialists in order to discuss

- All forms of E-Voting (including but not limited to polling station, mobile voting, kiosk or remote voting by electronic means)
- The role of identity and identification for E-Voting systems
- Profiling aspects
- Role of commercial voting systems; are commercial identity management systems suitable for e-voting
- Threats: identity frauds/theft, privacy issues
- Usability and accessibility issues (both for voters and for administrators)
- Legal issues
- Design and analysis of E-Voting schemes and protocols, their deployment and lifecycle concerns
- Security requirements, formal analysis and evaluation of electronic voting schemes and systems
- Concrete issues, like necessity of verifiability/digital receipts problems/anonymous channel in practise
- Interdisciplinary issues involved (link between identity and digital identity and E-Voting)
- Interrelationship with and the effects of E-Voting on democratic institutions and processes as well as voter behaviour
- Social and political analysis of the effects of electronic voting
- New ways of solving the voting paradigm of unequivocal identification of the voter and full anonymity of the vote

2.5 Further Details

Submission Guidelines

There was a strict limit of 12 pages. Follow carefully the LNCS instructions at http://www.springer.de/comp/lncs/authors.html.

Send had to be submitted to VOTE-ID2007@sirrix.com till 31th July 2007 23:59 (CET). All submissions had be anonymized (an author's name should only occur in references to that author's related work, which should be referenced in the third person and not overtly distinguishable from the referenced work of others).

Each submission hat to have a contact author who should provide full contact information (email, phone, fax, mailing address). One author of each accepted paper was required to present the work at the workshop.

Submissions must not substantially duplicate work that any of the authors has published elsewhere or has submitted in parallel to any other conference or workshop with proceedings. Information about submissions may be shared with program chairs of other conferences for that purpose.

Accepted Contributions

Full paper submissions were subject to a double-blind review. Accepted papers were available as pre-proceedings at the conference. The post-proceedings are published within LNCS Springer, including the feedback of the workshop discussion and after a final approvement by Springer.

Deadlines

Conference of the paper..... 31th July 2007
Notification of acceptance ..... 3th September 2007
Receipt of the final paper..... 19th October 2007

Contact Address

Sirrix AG security technologies

Ammar Alkassar

Im Stadtwald, Geb. D3 2

66123 Saarbrücken

Germany

E-Mail: VOTE-ID2007@sirrix.com

http://www.sirrix.com/content/pages/voteidcfp.htm

3 Preface and Forward

3.1 Preface

Electronic voting has been one of the most controversial topics of discussion in the IT security community for the past 20 years. During the 1980s, the discussion was characterized by the development of new, powerful cryptographic schemes and protocols. These were driven by the necessity to meet the requirements for replacing the former analog systems with newer election systems and e-voting technologies.

However, recurring problems with the election systems that were deployed, as well as inherent weaknesses, have burdened the argument for pushing forward. Now, after what could be characterized as a turbulent wave of pros and cons, the discussion focus has moved to address how the democratic spirit of elections can be respected in full, while also gaining the confidence of the public in the latest voting systems.

With respect to this new discussion, it was quite natural for the FIDIS Network of Excellence (NoE) to address the topic of E-Voting and Identity as well as its relevance in democratic society.

"Future of IDentity in the Information Society" (FIDIS) is a project funded by the European Commission. The network consists of 24 partners from 11 European countries collaborating on topics such as privacy, data protection, profiling and identity in both the public and private sectors.

An important aspect of the FIDIS NoE, as well as the recent conference, is to provide a highly-interdisciplinary forum for researchers stemming from various fields and organizations. Hence, the Program Committee was selected to represent leading experts in the related areas of cryptography, voting systems and ID management as well as legal and social sciences.

The conference was successful in bringing together researchers from universities and research institutes as well as practitioners from industry and electoral boards to discuss the central aspects of e-voting as well as the more pragmatic issues.

We would like to thank Berry Schoenmakers from the Technical University in Eindhoven (The Netherlands) for his excellent keynote on "E-Voting Crises" and also the members of the panel discussion: Klaus Brunnstein (University of Hamburg, Germany), Hans van Wijk (NEDAP, The Netherlands), Robert Stein (Head of Election Division, Federal Ministry of Interior, Austria) and Craig Burton (Everyone Counts).

We would like to extend a special thanks to Cline Fischer, who was kind enough to arrange the conference venue and take care of the administrative tasks which allowed the conference to run so smoothly. The conference was hosted by Sirrix AG and held at the European Center for IT-Security in Bochum.

November 2007

Ammar Alkassar

Melanie Volkamer

3.2 Forward

Voting and identity have a very delicate relationship. Only a few processes depend so much on an identity management respecting the fine line between reliable identification and reliable non-identifiability each at its part during the process. And only a few processes may change their outer appearance so much with the advent of new IT as voting and identity management do.

So it was no surprise in FIDIS, the interdisciplinary Network of Excellence working on the Future of Identity in the Information Society, when Ammar Alkassar proposed analyze the technical, socio-ethical and legal relations between Identity and E-Voting as part of Sirrix's activity in FIDIS.

There are many reasons for doing this, e.g., the open question of the implications of identity and identification to the emerging field of E-Government and E-Democracy, especially E-Voting. Issues to be discussed are from several domains, e.g., is identity fraud a crucial matter in E-Voting? What is the trade-off between anonymity and free speech vs. content-related offences? Is it appropriate to use ID cards or health-insurance cards with digital identities for citizen tasks or voting? What about using SIM cards? Can we employ biometrics for identification purposes with respect to E-Democracy?

Last but not least nearly all areas of E-Government rely on a reliable link between the citizens and their governments and administrations. However, in contrast to business processes, the effects are much more crucial: Identity fraud may cause more problems than in the business domain; the consequences of misuse cannot be measured just by financial means.

With these and many other issues at stake it was great to see VOTE-ID 2007 become such a great success with high-quality papers and discussions. It is a great pleasure to thank all the submitters, the Program Committee, and especially the Program Chairs Ammar Alkassar (Sirrix AG security technologies) and Melanie Volkamer (Institute of IT-Security and Security Law, University Passau) for the tremendous work in getting this conference off the ground.

November 2007

Kai Rannenberg
Goethe University Frankfurt
FIDIS Co-ordination

4 Agenda and Presentations

4.1 First Session: Improvements/Extensions of existing Approaches

(Session Chair: Hugo Jonker)

Simulation-based analysis of E2E voting systems

By: Olivier de Marneffe, Olivier Pereira and Jean-Jacques Quisquater

Abstract: End-to-end auditable voting systems are expected to guarantee very interesting, and often sophisticated security properties, including correctness, privacy, fairness, receipt-freeness… However, for many well-known protocols, these properties have never been analyzed in a systematic way. In this paper, we investigate the use of techniques from the simulation-based security tradition for the analysis of these protocols, through a case-study on the ThreeBallot protocol. Our analysis shows that the ThreeBallot protocol fails to emulate some natural voting functionality, reflecting the lack of election fairness guarantee from this protocol. Guided by the reasons that make our security proof fail, we propose a simple variant of the ThreeBallot protocol and show that this variant emulates our functionality.

A simple technique for safely using Punchscan and Prêt à Voter in mail-in elections

By: Stefan Popoveniuc and David Lundin

Abstract: We apply a technique inspired by Scantegrity to Punchscan and Prêt à Voter and show how this results in a mail-in ballot system that is auditable, simple to use and easy to understand.

Threat analysis of a practical voting scheme with receipts

By: Sebastien Foulle, Steve Schneider, Jacques Traore and Zhe Xia

Abstract: Kutylowski et al. have introduced a voter-verifiable electronic voting scheme “a practical voting scheme with receipts”, which provides each voter with a receipt. The voter can use her receipt to check whether her vote has been properly counted in the final tally, but she cannot use the receipt to prove others how she has voted. Another interesting property of this scheme is that, thanks to the repetitive robustness mix network, the ballot tallying phase only needs to be audited if the final results fail to achieve some conditions. However, this paper will show that this scheme is vulnerable to some threats, adversaries can not only violate voter privacy, but also forge the election result.

4.2 Second Session: Overview on Remote Electronic Voting

(Session Chair: Roland Vogt)

The Development of Remote E-Voting around the World: A Review of Roads and Directions *By: Robert Krimmer, Stefan Triessnig and Melanie Volkamer*

Abstract: Democracy and elections have more than 2,500 years of tradition. Technology has always influenced and shaped the ways elections were held. Since the emergence of the Internet there has been the idea of conducting remote electronic elections. In this paper we reviewed 104 elections with remote e-voting possibility based on research articles, working papers and also press releases. We analyzed the cases in respect to the level where they take place, technology, using multiple channels, size of the election and the provider of the system. Our findings show that while remote e-voting has arrived on the regional level and in organizations for binding elections, on the national level it is a very rare phenomenon. Further paper based elections are here to stay, most binding elections used remote e-voting in addition to the paper channel. Interestingly provider of e-voting systems are usually only operating in their own territory, out-of-country operations are very rare. On the long run, for remote e-voting to become a reality of the masses a lot has to be done. The high number of excluded cases shows that not only documentation is scarce but also the knowledge of the effects of e-voting is rare as most cases are not following simple experimental designs used elsewhere.

Remote voting schemes: A comparative analysis

By: Jordi Puiggali and Victor Morales

Abstract: Some governments initially introduced postal voting as a way to facilitate overseas and absentee voter's access to the electoral process. However, reliability issues that are part of postal voting have helped to introduce new remote voting channels based on electronic means. In some cases, electronic voting channels based on Fax, email or Internet, are currently used in binding elections. In other cases their adoption has been delayed or cancelled due to security concerns. In this paper we identify which are the current remote voting channels used in binding elections. We also identify which are the main criteria requirements used to evaluate the implementation of these remote voting channels, and provide a general comparison of the fulfillment of these requirements by these remote voting channels.

Internet-Voting: Opportunity or Threat for Democracy?

By: Emmanuel Benoist, Bernhard Anrig and David-Olivier Jaquet-Chiffelle

Abstract. During the last decade, Internet-voting (i-voting) moved from the field of fundamental reasearch to practical application. First, we will see that theoretical research provides satisfying algorithms for some of the challenges raised by i-voting and that some real world experiments have already been developed. Unfortunately, in current i-voting systems, the citizen looses its control over the overall electoral process. Indeed, usually, only insiders have access to the programming code and to the servers used in i-voting. The confidence in the

democracy itself could be harmed by this opacity. The European Convention on Human Right emphasizes that votes should remain secret. This can not be assured for i-voting, since it is not possible to have a booth around each computer for example. Family voting cannot be prevented and vote buying could be a major threat for democracy. Moreover, we can not assume that the voter's computer does not contain any viruses or Trojan horses. Therefore, it is optimistic to assume that the ballot transferred to the server is the one chosen by the voter. Finally, we will see that the effect of i-voting on the turnout at polls might remain marginal.

4.3 Third Session: Evaluation of Electronic Voting Systems

(Session Chair: Robert Krimmer)

Assessing Procedural Risks and Threats in e-Voting: Challenges and an Approach

By: Adolfo Villafiorita, Komminist Weldemariam and Andrea Mattioli

Abstract: Performing a good security analysis on the design of a system is an essential step in order to guarantee a reasonable level of protection. However, different attacks and threats may be carried out depending on the operational environment in which the system is used, i.e. the procedures that define how to operate the systems. Using strong-passwords to limit access to a system is useless - to make a simple example - if users are allowed to write the passwords on paper and leave them near the computers they operate. We are interested in reasoning about the security of e-Voting procedures, namely on the risks and attacks that can be carried out during an election. Our focus is more on people and organizations than on systems and technologies.

In this paper we describe some ongoing work that we are carrying out within the ProVotE project (a project sponsored by the Autonomous Province of Trento to switch to e-Voting for local elections) to analyze and (possibly) improve procedural security of electronic elections. To do so, we are we are providing models of the Italian electoral laws using the UML and we are developing a custom methodology for analyzing threats from the models. Our reasoning approach is based on asset mobility, asset values and existence of multiple instances.

Compliance of RIES to the proposed e-Voting Protection Profile

By: Hugo Lennaert Jonker and Melanie Volkamer

Abstract: The RIES-KOA e-voting system was used in the Netherlands as an additional system for the elections by expatriates for the Tweede Kamer (roughly: the Dutch House of Commons) elections in 2006. Although the system has been used in other elections in the Netherlands as well, there have been few independent evaluations of the system. In this paper, we apply the recently proposed Protection Profile for e-voting systems to the RIES-KOA system. This serves a two-fold purpose: it is an independent analysis of RIES-KOA and it is the first application of the Protection Profile. We indicate several issues with RIES-KOA and the Protection Profile, respectively, as learned during the analysis.

Compliance of Polyas to the Protection Profile for Remote Electronic Voting

By: Kai Reinhard and Wolfgang Jung

Abstract: In the past one and a half year a group of experts in electronic voting developed a Common Criteria Protection Profile lead-managed by the German Federal Office for Information Security (BSI) and the German Research Center for Artificial Intelligence (DFKI). To complete this work initiated by the German Gesellschaft für Informatik (GI, society for informatics), it is planed to evaluated the Polyas system from Micromata which is used for the GI elections against this Protection Profile. As a first step a high-level evaluation based on the security objectives has been done. The result is presented in this paper.

4.4 Fourth Session: Code Voting

(Session Chair: David Lundin)

Secure Internet Voting With Code Sheets

By: Jörg Helbach and Jörg Schwenk

Abstract: Malware on Personal Computers is a major security issue today. This fact implies that all solutions intended to secure Internet-based voting have to be re-evaluated under the assumption that a local malware application is capable of controlling the interface between user and PC. We propose to use paper-based code sheets, originally introduced by Chaum, to overcome this problem, and for the first time give a security analysis of this solution. We show that a modified, 3-step-scheme, can be considered secure against local malware attacks. Our scheme could then particularly be used to held shareholder elections or votes in an association over the Internet.

Code Voting - Protection Against Automatic Vote Manipulation in an Uncontrolled Environment *By: Rui Joaquim and Carlos Ribeiro*

Abstract: One of the major problems that prevent the widespread of Internet voting is the vulnerability of the voter's computer. A computer connected to the Internet is exposed to virus, worms, spyware, malware and other threats that can endanger the election's integrity. For instance, it is possible to write a virus that changes the voter's vote to one predefined vote on election's day. It is possible to write such a virus so that the voter wouldn't notice anything wrong with the voting application. This attack is very frightening because it may pass undetected. To prevent such attack it is necessary to prevent automatic vote manipulation at voter's computer. Here we present Code Voting, a solution to this problem that is simple enough to be successfully used by the voter and, at the same time, allows the use of cryptographic voting protocols that protect election's integrity at the server side of the voting application.

4.5 Fifth Session: Electronic Voting in Different Countries

(Session Chair: (tbc)

Electronic Voting in Belgium: Past and Future

By: Danny De Cock and Bart Preneel

Abstract: This paper provides an overview of the electronic (and paperbased) voting systems that are used in Belgium. It compares the advantages and disadvantages of these systems, and presents a selection of voting systems that will be recommended to the federal and local governments for future elections in Belgium.

The Digital Voting Pen at the Hamburg Elections 2008: Electronic Voting Closest to Conventional Voting *By: Jörg Arzt-Mergemeier, Willi Beiss and Thomas Steffens*

Abstract: Due to recent changes of the election law of the Free and Hanseatic City of Hamburg, Germany, the counting of the votes at the next elections for the state parliament will be complicated and time consuming. To nevertheless enable the Election Supervisor to announce the preliminary results of the election on the evening of the Election Day the Parliament has chosen to make use of an electronic voting system, i.e. the Digital Voting Pen System ("Digitales Wahlstift-System" – DWS). The main reasons for favoring this electronic voting system have been its closeness to the conventional voting procedure and therefore its acceptance among the voters, its security, and its verifiability.

The Security Analysis of e-voting in Japan

By: Hiroki Hisamitsu and Keiji Takeda

Abstract: To assess trustworthiness of e-voting practices in Japan, security of e-voting systems and their operational procedures are examined. All e-voting systems available on the market are covered in the analysis. Through these analyses we concluded that current e-voting security is heavily depending on protection by operational process rather than security feature of the system and it is confirmed that the systems provide only limited security feature though there is large room for technical improvement. Typical security issues are lack of protection mechanism of programs and data on counting machines and on tabulate machines. This vulnerability enables malicious poll worker or manufacturer to insert malicious code to generate arbitrary election result.

4.6 Sixth Session: E-Voting and Trust

(Session Chair: Klaus Brunstein)

Bingo Voting: Secure and coercion-free voting using a trusted random number generator

By: Jens-Matthias Bohli, Jörn Müller-Quade and Stefan Röhrich

Abstract: It is debatable if current direct-recording electronic voting machines can sufficiently be trusted for a use in elections. Reports about malfunctions and possible ways of manipulation abound. Voting schemes have to fulfill seemingly contradictory requirements: On one hand the election process should be verifiable to prevent electoral fraud and on the other hand each vote should be deniable to avoid coercion and vote buying. This work presents a new verifiable and coercion-free voting scheme Bingo Voting, which is based on a trusted random number generator. As a motivation for the new scheme two coercion/vote buying attacks on voting schemes are presented which show that it can be dangerous to let the voter contribute randomness to the voting scheme. A proof-of-concept implementation of the scheme shows the practicality of the scheme: all costly computations can be moved to a non time critical pre-voting phase.

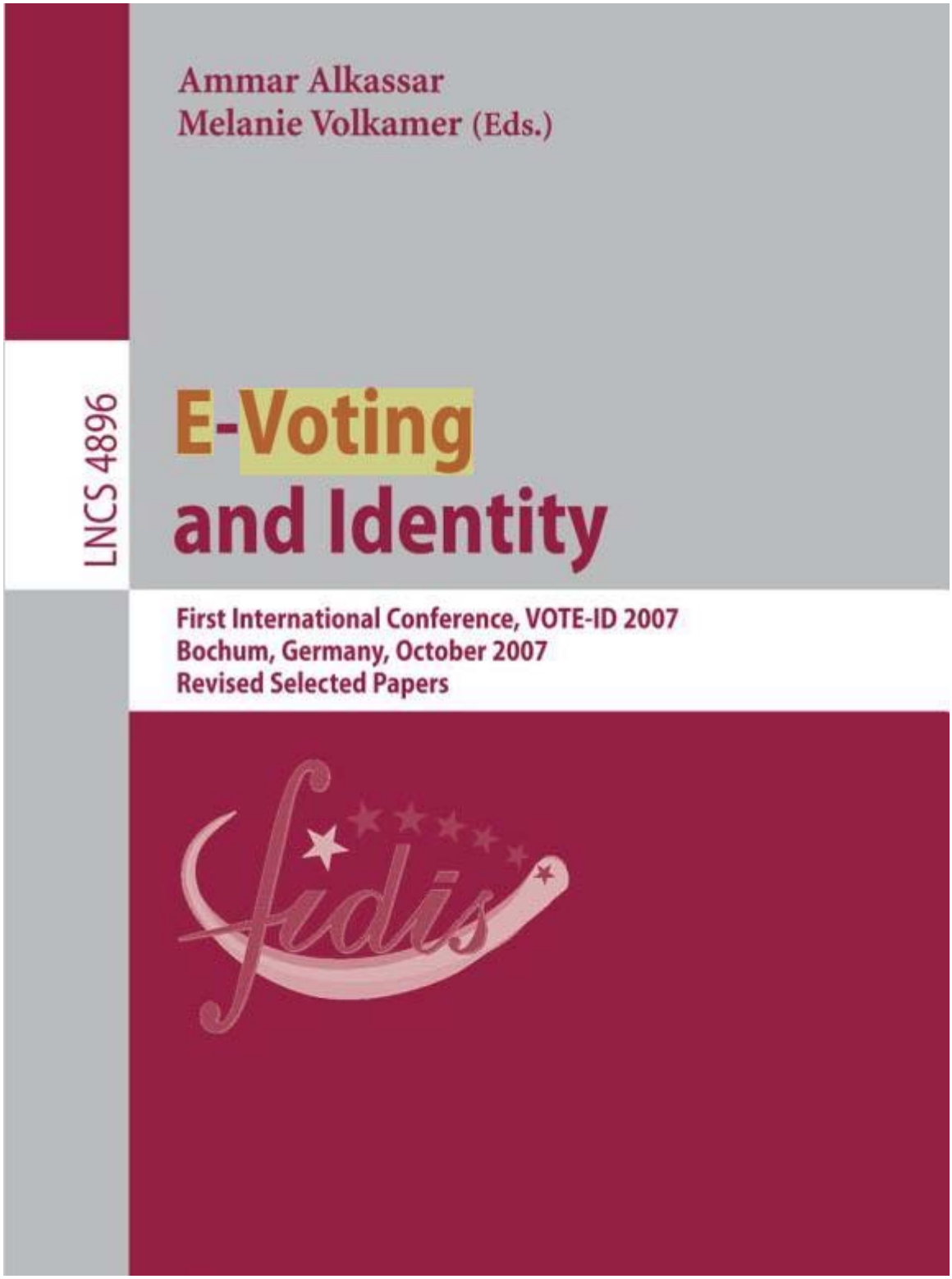
Enhancing the trust and perceived security in e-cognocracy

By: Joan Josep Piles Contreras, José Luis Salazar Riaño, José Ruíz Más and José María Moreno-Jiménez

Abstract: e-Cognocracy is a new, creative, innovative and cognitive democratic system based on the evolution of living systems which focuses on the extraction and social diffusion of the knowledge derived from the scientific resolution of highly complex problems associated with public decision making related to the governance of society. Among the many tools needed to fully develop e-cognocracy, we will focus in e-voting, as it is the first needed to gather the information supplied by the citizens. One of the things that may drive people away from this kind of systems is their complexity. In this paper we present an e-voting protocol designed to work with e-cognocracy, much simpler than the previously existing one [1], through the use of short linkable ring signatures. Short linkable ring signatures are a cryptographic primitive that allows one person to sign as a member of a group, but without giving any information about the identity of the signer and with no previous set up and, furthermore, all the signatures from the same signer can be linked together but keeping the anonymity. The key element they present is that, unlike other schemas, they have a constant size (making them independent of the number of people in the group). Keywords: Short linkable ring signatures, e-voting, e-cognocracy, e-government

5 Springer Publication: LNCS 4896

5.1 Cover



5.2 Table of Contents

5.3 Publication Details

Lecture Notes in Computer Science 4896

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Volume Editors

Ammar Alkassar
Sirrix AG security technologies
Im Stadtwald D3.2, 66123 Saarbrücken, Germany
E-mail: a.alkassar@sirrix.com

Melanie Volkamer
University of Passau, Institute of IT-Security and Security Law
Innstr. 43, 94032 Passau, Germany
E-mail: volkamer@uni-passau.de

Library of Congress Control Number: 2007941815

CR Subject Classification (1998): E.3, D.4.6, C.2, J.1, H.2.0, K.5.2, K.6.5, K.4.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743

ISBN-10 3-540-77492-0 Springer Berlin Heidelberg NewYork

ISBN-13 978-3-540-77492-1 Springer Berlin Heidelberg NewYork

6 Conference Participants

1	Ammar	Alkassar	Germany	Sirrix AG
2	Dr. Joerg	Arzt-Mergemeier	Germany	BFI Hamburg
3	Emmanuel	Benoist	Switzerland	Berner Fachhochschule-TI
4	Klaus	Brunstein	Germany	University of Hamburg
5	Craig	Burton	USA	Everyonecounts
6	Danny	de Cock	Belgium	K.U.Leuven, ESAT/COSIC
7	Olivier	de Marneffe	Belgium	UCL Crypto Group
8	Ross	Ensor	UK	Election Systems and Software
9	Rop	Gonggrijp	Netherlands	Gonggri
10	Norbert	Greif	Germany	Physikalisch-Technische BA
11	Hiroki	Hisamitsu	Japan	Carnegie Mellon CyLab Japan
12	Hugo	Jonker	Luxembourg	Université du Luxembourg
13	Wolfgang	Jung	Germany	Micromata Objects GmbH
14	Robert	Krimmer	Austria	E-Voting.CC
15	Lucie	Langer	Germany	Darmstadt University of Techn.
16	Leontine	Loeber	Netherlands	Dutch Electoral Council
17	Rui Filipe	Lopes Joaquim	Portugal	INESC-ID / GSD
18	David	Lundin	UK	University of Surrey
19	Katarzyna	Mlynczak	Poland	
20	Jörn	Müller Quade	Germany	Universität Karlsruhe (EISS)
21	Olivier	Pereira	Belgium	UCL Crypto Group
22	Joan J.	Piles	Spain	Unizar
23	Jordi	Puiggalí	Spain	Scytl Secure Electronic Voting
24	Jean	Ramaekers	Belgique	University of Namur
25	Kai	Reinhard	Germany	Micromata Objects GmbH
26	Stefan	Röhrich	Germany	Universität Karlsruhe (EISS)
27	Roberto	Samarone dos Santos	Germany	Darmstadt University of Techn.
28	Thomas	Schaaf	Germany	DATAGROUP GmbH
29	Axel	Schmidt	Germany	Darmstadt University of Techn.
30	Berry	Schoenmakers	Netherlands	Technical University Eindhoven
31	Irene	Schwehla	UK	Election Systems and Software
32	Jörg	Schwenk	Germany	Horst-Görtz-Institut
33	Robert	Stein	Austria	Bundesministerium für Inneres
34	Keiji	Takeda	Japan	Carnegie Mellon CyLab Japan
35	Jacques	Traore	France	Orange Labs
36	Brendan	Van Alsenoy	Belgium	Researcher ICRI
37	Gert-Jan	van den Nieuwenhuijzen	Netherlands	ICTU
38	Rita	Van Nuffelen	Belgium	Privacy Commission

39	Adolfo (Sisai Weldemariam)		Villafiorita	Italy	IRST
40	Roland	Vogt	Germany	DFKI	
41	Melanie	Volkamer	Germany	ISL - Universität Passau	
42	Sonja	Weddeling	Germany	T-Systems Enterprise Services	
43	Zhe	Xia	UK	University of Surrey	

7 Bibliography

Ammar Alkassar, Melanie Volkamer (Eds): *"Proceedings of the 1st International Conference on E-Voting and Identity"*, selected revised papers in Lecture Notes in Computer Science (LNCS), Volume 4896, Springer, Heidelberg.