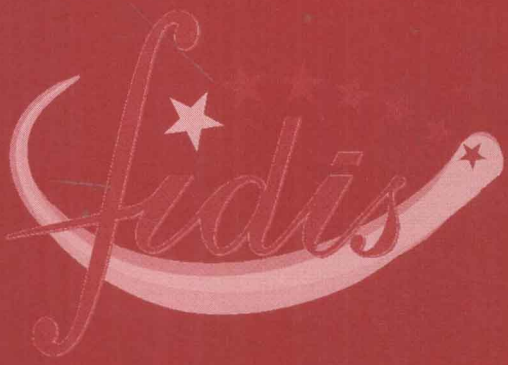
Ammar Alkassar
Melanie Volkamer (Eds.)

LNCS 4896

E-Voting and Identity

First International Conference, VOTE-ID 2007
Bochum, Germany, October 2007
Revised Selected Papers



Springer

Ammar Alkassar Melanie Volkamer (Eds.)

E-Voting and Identity

First International Conference, VOTE-ID 2007
Bochum, Germany, October 4-5, 2007
Revised Selected Papers

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 New York
ISBN-13 978-3-540-77492-1 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2007
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12210206 06/3180 5 4 3 2 1 0

Lecture Notes in Computer Science 4896

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

Editorial Board

David Hutchison
Lancaster University, UK

Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler
University of Surrey, Guildford, UK

Jon M. Kleinberg
Cornell University, Ithaca, NY, USA

Friedemann Mattern
ETH Zurich, Switzerland

John C. Mitchell
Stanford University, CA, USA

Moni Naor
Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz
University of Bern, Switzerland

C. Pandu Rangan
Indian Institute of Technology, Madras, India

Bernhard Steffen
University of Dortmund, Germany

Madhu Sudan
Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos
University of California, Los Angeles, CA, USA

Doug Tygar
University of California, Berkeley, CA, USA

Moshe Y. Vardi
Rice University, Houston, TX, USA

Gerhard Weikum
Max-Planck Institute of Computer Science, Saarbruecken, Germany

Foreword

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

此为试读,需要完整PDF请访问: www.ertongbook.com

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 panel 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

Organization

Program Chairs

Ammar Alkassar	Sirrix AG, Germany
Melanie Volkamer	Passau University, Germany

Program Committee

Josh Benaloh	Microsoft, USA
Rüdiger Grimm	Koblenz-Landau University, Germany
Marit Hansen	ICPP, Germany
Dirk Heckmann	Passau University, Germany
David-Olivier Jaquet-Chiffelle	University of Applied Sciences of Bern, Switzerland
Frank Koob	German Federal Office for Information Security, Germany
Robert Krimmer	evoting.cc, Austria
Ronald Leenes	Tilburg University, Netherlands
Helger Lipmaa	University College London, UK
Sjouke Mauw	Luxemburg University, Luxemburg
Margaret McGaley	NUI Maynooth, Ireland
Lilian Mitrou	University of the Aegean, Greece
Olivier Pereira	Université Catholique de Louvain, Belgium
Günther Pernul	Regensburg University, Germany
Andreas Pfitzmann	Dresden Technical University, Germany
Bart Preneel	Catholic University Leuven, Belgium
Kai Rannenberg	Frankfurt University, Germany
Peter Ryan	Newcastle University, UK
Ahmad-Reza Sadeghi	Ruhr University Bochum, Germany
Joseph Savirimuthu	Liverpool University, UK
Berry Schoenmakers	Eindhoven Technical University, Netherlands

Additional Reviewers

Roberto Araujo, Stefan Berthold, Sebastian Clauß, André Deuker, Stefan Duerbeck, Ludwig Fuchs, Sebastian Gajek, Yacine Gasmi, Jörg Gilberg, Jörg Helbach, Hugo Jonker, Andreas Juschka, Jan Kolter, Michael Kreutzer, Katja Liesebach, Olivier de Marneffe, Denis Royer, Hans Loehr, Tobias Scherner, Patrick Stewin, Martin Unger, Stefan Weber, Jan Zibuschka, Felix Zimmermann

Lecture Notes in Computer Science

Sublibrary 4: Security and Cryptology

Vol. 4896: A. Alkassar, M. Volkamer (Eds.), E-Voting and Identity. XII, 189 pages. 2007.

Vol. 4893: S.W. Golomb, G. Gong, T. Helleseth, H.-Y. Song (Eds.), Sequences, Subsequences, and Consequences. X, 219 pages. 2007.

Vol. 4887: S.D. Galbraith (Ed.), Cryptography and Coding. XI, 423 pages. 2007.

Vol. 4886: S. Dietrich, R. Dhamija (Eds.), Financial Cryptography and Data Security. XII, 390 pages. 2007.

Vol. 4876: C. Adams, A. Miri, M. Wiener (Eds.), Selected Areas in Cryptography. X, 409 pages. 2007.

Vol. 4861: S. Qing, H. Imai, G. Wang (Eds.), Information and Communications Security. XIV, 508 pages. 2007.

Vol. 4859: K. Srinathan, C.P. Rangan, M. Yung (Eds.), Progress in Cryptology – INDOCRYPT 2007. XI, 426 pages. 2007.

Vol. 4856: F. Bao, S. Ling, T. Okamoto, H. Wang, C. Xing (Eds.), Cryptology and Network Security. XII, 283 pages. 2007.

Vol. 4833: K. Kurosawa (Ed.), Advances in Cryptology – ASIACRYPT 2007. XIV, 583 pages. 2007.

Vol. 4817: K.-H. Nam, G. Rhee (Eds.), Information Security and Cryptology - ICISC 2007. XIII, 367 pages. 2007.

Vol. 4812: P. McDaniel, S.K. Gupta (Eds.), Information Systems Security. XIII, 322 pages. 2007.

Vol. 4784: W. Susilo, J.K. Liu, Y. Mu (Eds.), Provable Security. X, 237 pages. 2007.

Vol. 4779: J.A. Garay, A.K. Lenstra, M. Mambo, R. Peralta (Eds.), Information Security. XIII, 437 pages. 2007.

Vol. 4776: N. Borisov, P. Golle (Eds.), Privacy Enhancing Technologies. X, 273 pages. 2007.

Vol. 4752: A. Miyaji, H. Kikuchi, K. Rannenberg (Eds.), Advances in Information and Computer Security. XIII, 460 pages. 2007.

Vol. 4734: J. Biskup, J. López (Eds.), Computer Security – ESORICS 2007. XIV, 628 pages. 2007.

Vol. 4727: P. Paillier, I. Verbauwhede (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2007. XIV, 468 pages. 2007.

Vol. 4691: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. VIII, 285 pages. 2007.

Vol. 4677: A. Aldini, R. Gorrieri (Eds.), Foundations of Security Analysis and Design IV. VII, 325 pages. 2007.

Vol. 4657: C. Lambrinoudakis, G. Pernul, A.M. Tjoa (Eds.), Trust, Privacy and Security in Digital Business. XIII, 291 pages. 2007.

Vol. 4637: C. Kruegel, R. Lippmann, A. Clark (Eds.), Recent Advances in Intrusion Detection. XII, 337 pages. 2007.

Vol. 4631: B. Christianson, B. Crispo, J.A. Malcolm, M. Roe (Eds.), Security Protocols. IX, 347 pages. 2007.

Vol. 4622: A. Menezes (Ed.), Advances in Cryptology - CRYPTO 2007. XIV, 631 pages. 2007.

Vol. 4593: A. Biryukov (Ed.), Fast Software Encryption. XI, 467 pages. 2007.

Vol. 4586: J. Pieprzyk, H. Ghodosi, E. Dawson (Eds.), Information Security and Privacy. XIV, 476 pages. 2007.

Vol. 4582: J. López, P. Samarati, J.L. Ferrer (Eds.), Public Key Infrastructure. XI, 375 pages. 2007.

Vol. 4579: B.M. Hämmerli, R. Sommer (Eds.), Detection of Intrusions and Malware, and Vulnerability Assessment. X, 251 pages. 2007.

Vol. 4575: T. Takagi, T. Okamoto, E. Okamoto, T. Okamoto (Eds.), Pairing-Based Cryptography – Pairing 2007. XI, 408 pages. 2007.

Vol. 4521: J. Katz, M. Yung (Eds.), Applied Cryptography and Network Security. XIII, 498 pages. 2007.

Vol. 4515: M. Naor (Ed.), Advances in Cryptology - EUROCRYPT 2007. XIII, 591 pages. 2007.

Vol. 4499: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security II. IX, 117 pages. 2007.

Vol. 4464: E. Dawson, D.S. Wong (Eds.), Information Security Practice and Experience. XIII, 361 pages. 2007.

Vol. 4462: D. Sauveron, K. Markantonakis, A. Bilas, J.-J. Quisquater (Eds.), Information Security Theory and Practices. XII, 255 pages. 2007.

Vol. 4450: T. Okamoto, X. Wang (Eds.), Public Key Cryptography – PKC 2007. XIII, 491 pages. 2007.

Vol. 4437: J.L. Camenisch, C.S. Collberg, N.F. Johnson, P. Sallee (Eds.), Information Hiding. VIII, 389 pages. 2007.

Vol. 4392: S.P. Vadhan (Ed.), Theory of Cryptography. XI, 595 pages. 2007.

Vol. 4377: M. Abe (Ed.), Topics in Cryptology – CT-RSA 2007. XI, 403 pages. 2006.

Vol. 4356: E. Biham, A.M. Youssef (Eds.), Selected Areas in Cryptography. XI, 395 pages. 2007.

Vol. 4341: P.Q. Nguyên (Ed.), Progress in Cryptology - VIETCRYPT 2006. XI, 385 pages. 2006.

Vol. 4332: A. Bagchi, V. Atluri (Eds.), Information Systems Security. XV, 382 pages. 2006.

Vol. 4329: R. Barua, T. Lange (Eds.), Progress in Cryptology - INDOCRYPT 2006. X, 454 pages. 2006.

Vol. 4318: H. Lipmaa, M. Yung, D. Lin (Eds.), Information Security and Cryptology. XI, 305 pages. 2006.

Vol. 4307: P. Ning, S. Qing, N. Li (Eds.), Information and Communications Security. XIV, 558 pages. 2006.

Vol. 4301: D. Pointcheval, Y. Mu, K. Chen (Eds.), Cryptology and Network Security. XIII, 381 pages. 2006.

Vol. 4300: Y.Q. Shi (Ed.), Transactions on Data Hiding and Multimedia Security I. IX, 139 pages. 2006.

Vol. 4298: J.K. Lee, O. Yi, M. Yung (Eds.), Information Security Applications. XIV, 406 pages. 2007.

Vol. 4296: M.S. Rhee, B. Lee (Eds.), Information Security and Cryptology – ICISC 2006. XIII, 358 pages. 2006.

Vol. 4284: X. Lai, K. Chen (Eds.), Advances in Cryptology – ASIACRYPT 2006. XIV, 468 pages. 2006.

Vol. 4283: Y.Q. Shi, B. Jeon (Eds.), Digital Watermarking. XII, 474 pages. 2006.

Vol. 4266: H. Yoshiura, K. Sakurai, K. Rannenberg, Y. Murayama, S.-i. Kawamura (Eds.), Advances in Information and Computer Security. XIII, 438 pages. 2006.

Vol. 4258: G. Danezis, P. Golle (Eds.), Privacy Enhancing Technologies. VIII, 431 pages. 2006.

Vol. 4249: L. Goubin, M. Matsui (Eds.), Cryptographic Hardware and Embedded Systems - CHES 2006. XII, 462 pages. 2006.

Vol. 4237: H. Leitold, E.P. Markatos (Eds.), Communications and Multimedia Security. XII, 253 pages. 2006.

Vol. 4236: L. Breveglieri, I. Koren, D. Naccache, J.-P. Seifert (Eds.), Fault Diagnosis and Tolerance in Cryptography. XIII, 253 pages. 2006.

Vol. 4219: D. Zamboni, C. Krügel (Eds.), Recent Advances in Intrusion Detection. XII, 331 pages. 2006.

Vol. 4189: D. Gollmann, J. Meier, A. Sabelfeld (Eds.), Computer Security – ESORICS 2006. XI, 548 pages. 2006.

Vol. 4176: S.K. Katsikas, J. López, M. Backes, S. Gritzalis, B. Preneel (Eds.), Information Security. XIV, 548 pages. 2006.

Vol. 4117: C. Dwork (Ed.), Advances in Cryptology - CRYPTO 2006. XIII, 621 pages. 2006.

Vol. 4116: R. De Prisco, M. Yung (Eds.), Security and Cryptography for Networks. XI, 366 pages. 2006.

Vol. 4107: G. Di Crescenzo, A. Rubin (Eds.), Financial Cryptography and Data Security. XI, 327 pages. 2006.

Vol. 4083: S. Fischer-Hübner, S. Furnell, C. Lambrinoudakis (Eds.), Trust and Privacy in Digital Business. XIII, 243 pages. 2006.

Vol. 4064: R. Büschkes, P. Laskov (Eds.), Detection of Intrusions and Malware & Vulnerability Assessment. X, 195 pages. 2006.

Vol. 4058: L.M. Batten, R. Safavi-Naini (Eds.), Information Security and Privacy. XII, 446 pages. 2006.

Vol. 4047: M.J.B. Robshaw (Ed.), Fast Software Encryption. XI, 434 pages. 2006.

Vol. 4043: A.S. Atzeni, A. Lioy (Eds.), Public Key Infrastructure. XI, 261 pages. 2006.

Vol. 4004: S. Vaudenay (Ed.), Advances in Cryptology - EUROCRYPT 2006. XIV, 613 pages. 2006.

Vol. 3995: G. Müller (Ed.), Emerging Trends in Information and Communication Security. XX, 524 pages. 2006.

Vol. 3989: J. Zhou, M. Yung, F. Bao (Eds.), Applied Cryptography and Network Security. XIV, 488 pages. 2006.

Vol. 3969: Ø. Ytrehus (Ed.), Coding and Cryptography. XI, 443 pages. 2006.

Vol. 3958: M. Yung, Y. Dodis, A. Kiayias, T.G. Malkin (Eds.), Public Key Cryptography - PKC 2006. XIV, 543 pages. 2006.

Vol. 3957: B. Christianson, B. Crispo, J.A. Malcolm, M. Roe (Eds.), Security Protocols. IX, 325 pages. 2006.

Vol. 3956: G. Barthe, B. Grégoire, M. Huisman, J.-L. Lanet (Eds.), Construction and Analysis of Safe, Secure, and Interoperable Smart Devices. IX, 175 pages. 2006.

Vol. 3935: D.H. Won, S. Kim (Eds.), Information Security and Cryptology - ICISC 2005. XIV, 458 pages. 2006.

Vol. 3934: J.A. Clark, R.F. Paige, F.A.C. Polack, P.J. Brooke (Eds.), Security in Pervasive Computing. X, 243 pages. 2006.

Vol. 3928: J. Domingo-Ferrer, J. Posegga, D. Schreckling (Eds.), Smart Card Research and Advanced Applications. XI, 359 pages. 2006.

Vol. 3919: R. Safavi-Naini, M. Yung (Eds.), Digital Rights Management. XI, 357 pages. 2006.

Vol. 3903: K. Chen, R. Deng, X. Lai, J. Zhou (Eds.), Information Security Practice and Experience. XIV, 392 pages. 2006.

Vol. 3897: B. Preneel, S. Tavares (Eds.), Selected Areas in Cryptography. XI, 371 pages. 2006.

Vol. 3876: S. Halevi, T. Rabin (Eds.), Theory of Cryptography. XI, 617 pages. 2006.

Vol. 3866: T. Dimitrakos, F. Martinelli, P.Y.A. Ryan, S. Schneider (Eds.), Formal Aspects in Security and Trust. X, 259 pages. 2006.

Vol. 3860: D. Pointcheval (Ed.), Topics in Cryptology – CT-RSA 2006. XI, 365 pages. 2006.

Vol. 3858: A. Valdes, D. Zamboni (Eds.), Recent Advances in Intrusion Detection. X, 351 pages. 2006.

Vol. 3856: G. Danezis, D. Martin (Eds.), Privacy Enhancing Technologies. VIII, 273 pages. 2006.

Vol. 3786: J.-S. Song, T. Kwon, M. Yung (Eds.), Information Security Applications. XI, 378 pages. 2006.

Vol. 3108: H. Wang, J. Pieprzyk, V. Varadharajan (Eds.), Information Security and Privacy. XII, 494 pages. 2004.

Vol. 2951: M. Naor (Ed.), Theory of Cryptography. XI, 523 pages. 2004.

Vol. 2742: R.N. Wright (Ed.), Financial Cryptography. VIII, 321 pages. 2003.

Table of Contents

The Development of Remote E-Voting Around the World: A Review of Roads and Directions

Robert Krimmer[1], Stefan Triessnig[1], and Melanie Volkamer[2]

[1] Competence Center for Electronic Voting and Participation (E-Voting.CC)
[2] Institute of IT-Security and Security Law (University of Passau)
{r.krimmer,s.triessnig}@e-voting.cc, melanie.volkamer@uni-passau.de

Abstract. Democracy and elections have more than 2.500 years of tradition. Technology has always influenced and shaped the ways elections are 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 a remote e-voting possibility based on research articles, working papers and also on press releases. We analyzed the cases with respect to the level where they take place, technology, using multiple channels, the 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, providers of e-voting systems are usually only operating in their own territory, as out-of-country operations are very rare. In 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.

1 Introduction

"While democracy must be more than [...] elections, it is also true [...] that it cannot be less," [2] former Secretary General Kofi Annan once said. Elections are the core element of democracy as a society's way to make decisions. Elections are the way to express how societies use technology and as new technologies have emerged and evolved, elections have changed accordingly. While there have been democratic structures in societies like India, the birthplace of democracy is attributed to old Athens in 507 BC [10]. From then on similar structures of direct democracy, bound by face-to-face societies, also developed in several places around the world like in ancient Rome [22], with the Vikings [32] or in the Cantons of Switzerland [34,19]. The next level of democracy developed with the creation of nation-states in the late 18th century with the need for representatives. This form of indirect democracy spread in three waves [24] from the United States and France around the globe to today's predominant role of democracy as a rule of government.

A. Alkassar and M. Volkamer (Eds.): VOTE-ID 2007, LNCS 4896, pp. 1–15, 2007.
© Springer-Verlag Berlin Heidelberg 2007

此为试读,需要完整PDF请访问: www.ertongbook.com

The political scientist Robert Dahl classifies these developments as the first and the second transformation of democracy [9]. With it, democracy moved away from the old ideal of identity of the ruler and the ruled. Thus, the worldwide decrease in voter turnout and the rapid development of information and communication technologies like the Internet have led him and others to think about a third transformation - the development of the electronic democracy.

Positive visionaries like Grossman [17], Fuller [15] and Fromm [13] conceived the electronic republic with a new, more direct and pervasive form of democracy. Fuller anticipated even "electrified voting, [...] a mechanical mean[s] for nation-wide voting, daily and secretly, by each adult citizen." The more pessimistic view is taken by Golding [16] and Haywood [18], who foresaw a negative effect of new technologies for democracy, due to inequalities in information access. The experience with the transformational effect of the Internet on private (e-commerce) and public (e-government) sectors has strengthened the position of neutral researchers that foresee a similar transformational change for democracy (Bimber [3] and Leggewie & Bieber [30]), which will in the end develop a direct representation where representatives can be held more accountable by the electorate.

Either way, the development of an electronic democracy with transnational character [21] needs the further development of e-enabled instruments of democracy [20], i.e., e-initiatives, e-referenda and of course also e-voting instruments. Amongst them remote e-voting has received the largest attention, and it reached the national level in Estonia first. On March 3^{rd}, 2007 the Estonian national election offered the world's first legally binding remote electronic voting (e-voting) possibility [7]. With that event remote e-voting has finally reached the stage of international attention even though experts warned three years earlier in the SERVE report that the Internet is not ready for elections yet [25]. Most other nations are still in the phase of experimentation. To date most trials do not follow classical experimental setups [1] and are embedded in their national context [41] which makes it hard for comparison and learning from others.

This paper is the first attempt to conduct a state-of-the-art analysis [12] of 104 remote e-voting uses in the past twelve years to build knowledge on the future of voting. We analyzed the documentation in research articles, working papers and press releases of 104 e-elections conducted around the world. While we aimed for a representative sample, it is clear that the current cases cannot serve this purpose. Rather it gives an indication how remote e-voting has developed so far. In the following we will first give a theoretical background on remote e-voting, and then present the results of our review. Finally, we will discuss the findings and give our conclusions.

2 Theoretical Background

In this chapter we will explain what we mean by remote electronic voting and which methodology we used.

2.1 The Terminus Technicus Remote Electronic Voting and Its Variants

Definition. When talking about e-voting it is necessary to define the subject. The Council of Europe recommendations define electronic voting as "the use of electronic means in at least the casting of the vote" [35]. We first have to look at elections in a broad sense (for our purposes this includes e-referendums) and then concentrate on the implications of ICT usage therein.

The Electoral Process. The United Nations facilitated the agreement on the International Covenant on Civil and Political Rights [42]. Article 25 defines eight principles for elections that depict the whole electoral process: (i) periodic elections, (ii) genuine elections, (iii) stand for election, (iv) universal suffrage, (v) voting in elections on the basis of the right to vote, (vi) equal suffrage, (vii) secret vote, and (viii) free expression of the will of the voters. Suksi [40] groups these principles into a cycle consisting of three periods:

1. Pre-Electoral Period: This is the time from calling an election until the actual start of the polling.
2. Electoral Period: This is the actual Election Day where the vote casting takes place.
3. Post-Electoral Period: This is the time during which the results are announced and a new election is called.

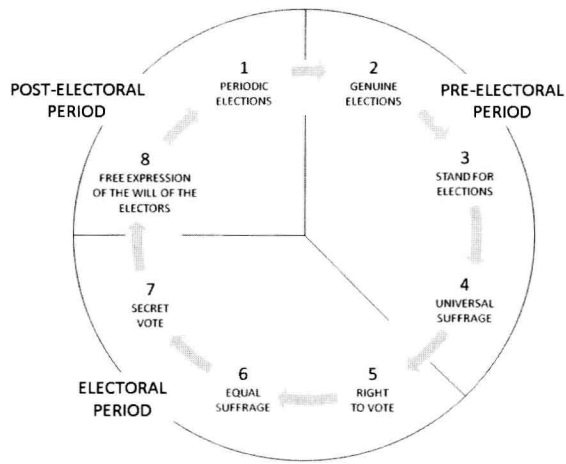


Fig. 1. The electoral cycle [40]

Local/Remote. The electoral process usually takes place at the polling station and is supervised. This can be referred to as voting at presence. But there is also the possibility of remote voting. The criterion to differentiate those two is if an election commission supervises the act of voting or not [27]. At current elections

the voter comes to the polling station where the election commission checks the identity and eligibility and ensures the voter's anonymity when casting the ballot. When the election has finished the election commission counts the votes. With remote elections the identity and the right to vote is checked beforehand or remotely and the voter has to make sure that his anonymity is not compromised. This raises questions of voter coercion and vote buying [29].

Form. According to the dimensions of medium and place of voting the systems can be assigned to six basic groups. The medium hand is characterized by its inherent need of presence and is limited to a certain number of people and does not allow for voting in an uncontrolled environment. In modern institutionalized elections this medium is very seldom used. Most modern day elections use paper as a medium of choice. Polling station voting using paper ballots is characterized by the controlled environment and the usage of paper as a medium. Postal voting also uses the medium paper, but provides no controlled environment. If the ballot is cast electronically one can differentiate between voting machines that are placed in the controlled environment of a voting station and remote electronic voting that also uses an electronic channel as a medium, but provides no controlled environment. Table 1 gives an overview for detailed information see [43].

Table 1. Forms of electronic voting

Environment / **Medium**	Controlled	Uncontrolled
Hand	In-Person	-
Paper	Polling Place	Postal Voting
Electronic	Voting Machine	Remote Electronic Voting

Multi-channel. It is possible that one election uses more than one form of voting. Critical from the operational viewpoint is if more than one channel is allowed and if paper and electronic channels have to be combined. When counting the votes the system must ensure that multiple voting in different channels is not possible. One has to make sure that the individual results of the channels are combined in such a way that the end result is correct. For the time being, democracy theory and constitutional law (requirement of universality) require additional paper channels as long as not everyone has the skill and access to the Internet, thus remote e-voting can only be an optional channel in legally binding elections for the time being.

Remote e-voting can take place at elections of diverse levels of attention. We differentiate five different levels determined by political importance, legal commitment, and parallel testing. The political importance is defined by Lijphart [37] as such that the first and the second level elections are politically binding which means they are regulated by law and the results of the elections have consequences. The most rigid legal framework is found with first level elections like presidential or parliamentarian. On the second level less important political elections can be found. Typical elections for that level would be local elections.

Elections of lesser importance, because of their lesser political impact like (student) union elections or elections in corporations, can be considered as the third level. These tend to have fewer rules on how the election has to be conducted. Still some kind of outcome is dependent on the result of the election. Critical for all of them is that they have to fulfill certain rules so the outcome of the election can be binding and some kind of action can be derived.

This leads to another classification of elections. A test is an election that's sole purpose is to test the system. Such tests are often conducted in an early stage of the development of a system and their sole purpose is to test the system. A logical next step is to simulate an election and test the system parallel to a binding one. The aim of such a test is to trial the system under realistic conditions and the results of which are not legally binding. These five categories build the five levels of elections:

Table 2. Levels of elections

Levels	Leg. Binding	Org. Binding	Non-Binding
1st Level: national	X		
2nd Level: regional, local	X		
3rd Level: org., assoc., companies	(X)	X	
4th Level: shadow, parallel			X
5th Level: technical test			X

Identification and Anonymity. The basic problem of electronic voting is how to solve of the unequivocal identification of a voter and at same time being able to guarantee anonymity with a secret ballot casting [31].

Identification. For identifying a voter three basic criteria can be used to differentiate the technologies: (i) knowledge, (ii) possession, and (iii) properties. A fourth possibility is a combination thereof. These identification technologies are used in remote e-voting:

1. *Username and Password:* The identification relies on the voter knowing a secret.
2. *Transaction Number (TAN):* The voter possesses something that identifies him/herself.
3. *Biometrics:* The voter him/herself with his/her individual biometric properties identifies him/herself. A reader for the biometric feature is needed.
4. *Smart Cards:* The voter knows a secret that in combination with the possession of the card identifies him. Or a property pattern of the voter is stored on the smart card that is checked against the voter's property when casting a ballot -either way, a reader for the smart card is needed.

Anonymity. Critical for a voting system is the question of guaranteeing anonymity. There have been many articles written to categorize and cluster protocols guaranteeing anonymity [26,37,33,23]. While the criteria used in these papers are

very sophisticated, in practice a simpler and more distinctive criterion is time [39]: At which point in the electoral cycle is secrecy (anonymity) established?

1. In the Pre-electoral Period: Anonymity is established in the pre-election period by the organizing institution. The most common implementation of such a system uses transaction numbers (TAN). These numbers are generated centrally and a scratch-field is applied. Then in a second step the voter's address is applied and sent to the voter who can use the number anonymously for exactly one vote.
2. During the electoral period: With this method the anonymity is established during the vote casting procedure. It can either be done by separating the servers in an identification and ballot box server or by blind signatures; the most common implementation of Chaum's blind signature [36] is in the Fujioka et al. algorithm [5]. The process can be explained as follows: the voter fills out his/her ballot sheet, then puts it in an carbon-copy envelope. The voter then signs another envelope with his/her personal signature and inserts the carbon-copy envelope and sends the package to his/her register. They check the voting eligibility based on the voter's signature, then sign the carbon copy envelope and return it to the voter. The voter opens the cc-envelope and has a signed ballot sheet (due to the carbon copy) without the voter's register ever having seen the ballot sheet. Finally she returns the ballot sheet to the ballot box and has thereby cast a valid vote anonymously.
3. In the post-electoral period: In this case the anonymity is established after the end of the election day, when the votes can still be identified but the count can only be conducted together meaning the content of a single vote is never released. The most common implementations use homomorphic encryption like the Schoenmakers algorithm [14] or hardware security modules like the Estonian system [38]. Provider. To conduct an electronic election is a complex undertaking and is usually operated by a consortium. We identified the provider that was critical or characteristic for the whole system. Of special interest was in which country the provider operated and how much experience the company had.

Size. One important criterion for assessing e-voting use is how many votes are cast. Looking at the sample we found it useful to group the elections into three size groups. The first group (A) contains all elections with more than 30,000 votes. The middle group (B) contains elections with a number of e-votes between 3,000 and 30,000. The last group (C) consists of small elections with a number of e-votes smaller than 3,000.

2.2 Research Methodology

Conducting a review can be organised in many ways; the approach we selected follows the handbook of review synthesis [6] which proposes five phases: (i) problem description, (ii) literature research, (iii) literature analysis, (iv) analysis, and (v) presentation.

Table 3. Criteria to categorize remote e-voting

Criterion	Category
Level	National - Regional - Association - Shadow - Test
Channels	Electronic - Paper and Electronic
Identification	Username/PWD - TAN - Signature - Biometric
Anonymity	Pre-electoral period - Electoral period - Post-electoral period
# Votes	# > 30,000 - 30,000 > # > 3,000 - # < 3,000

(i) The goal of this review was to conduct a review on the progress of remote electronic voting. (ii) To use as sources we consulted research articles, system documentation, whitepapers, technical reports, and even press releases if necessary. As remote electronic voting is a very new topic for the general public, often more than one source had to be consulted to gain a complete picture. Not surprisingly research articles usually gave a better insight on the project setup and system description while lacking actual election related data. This was where we consulted press releases. To find the appropriated sources we used a network of experts around the world that were invited to provide data or point to relevant documents. We provided them an online questionnaire on a public website to identify relevant elections. Because of the multitude of sources the data had to be consolidated. That makes it difficult to find common ground, so we needed to add an extensive array of integration work. (iii) The criteria that were developed in the previous chapter were used to characterize the elections. (iv) The collected data was then entered it into a database for analysis, and (v) then presented and discussed in the following chapters.

3 Results

In total we identified 139 elections in 16 countries within the time period of 1996 to the 30^{th} of April 2007 where remote e-voting occurred. For the analysis we needed a minimum amount of information about every election. We had to eliminate 35 (!) elections in total. Three elections were excluded from analysis because of missing data about voters and turnout. The largest exclusion reason was for not having system documentation available, which applied to thirty elections. Without the documents we could not assess which forms of identification or anonymity were used. Finally, two could not be included at all because we lacked information on the voter data and on the used system. In total we had 104 fully documented elections which we could include in the following analysis. These elections were held in 13 different countries on three continents; two elections were held transnationally. The first election was held in 1996 in Finland and the last in 2007 in Estonia. The following table shows the distribution of all elections over time and by country. From the analysis, excluded elections are put in brackets.

The countries with the most elections were Germany (30), Switzerland (24) and the United Kingdom (19). Surprisingly the United States has just 2 publicly documented elections.

此为试读,需要完整PDF请访问: www.ertongbook.com