Relazione sulle modalità di voto telematico per la FNOMCeO

Roberto Reale

(firmato digitalmente)

Digitally signed
by REALE ROBERTO
C=IT

Premessa

L'art. 2, comma 5, del D.Lgs. C.P.S. n. 233/1946 e ss.mm.ii., e l'art. 1 comma 4, del D.M. Salute del 15 marzo 2018, attribuiscono a ciascun Ordine il potere di stabilire che le votazioni per il rinnovo degli organi istituzionali si svolgano con modalità telematiche.

Progetti esaminati

Vengono esaminati i seguenti progetti, pervenuti alla FNOMCeO con relativo protocollo in arrivo.

Ordine	**Protocollo arrivo**
Campobasso	9838/2020 del 20-08-2020
Grosseto	10072/2020 del 01-09-2020
Latina	N/D
Modena	N/D
Nuoro	N/D
Piacenza	N/D
Trieste	9971/2020 del 27-08-2020
Udine	9944/2020 del 27-08-2020

Nota: In taluni casi l'ordine capofila presenta un progetto condiviso con altri ordini.

Definizioni e requisiti del voto telematico

Collusion-free vote secrecy	Impossibilità di conoscere i voti individuali. La segretezza del voto deve essere garantita anche se tutti i mezzi elettorali (ad esempio, schede votate) e le chiavi di sicurezza sono rese note da un attacco o da un errore. In altri termini, la segretezza del voto non deve dipendere solo dal protocollo di comunicazione e da ipotesi crittografiche, o da una soglia di collusione per i portachiavi.
Fail-safe privacy in verification	Agli elettori non deve essere richiesta di rivelare la propria identità per verificare i propri voti o segnalare un errore percepito. La fail-safe voter privacy deve essere preservata anche quando gli elettori partecipano a un processo di verifica.
Fail-safe voter privacy	Impossibilità di collegare gli elettori ai voti. La privacy degli elettori deve essere assicurata anche se l'intero sistema di voto telematico non funziona correttamente o è costretto a funzionare in modo improprio ovvero le procedure elettorali sono viziate, senza limiti di tempo.
Immodificabilità	L'immodificabilità è la caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso.
Physical recounting and auditing	Le prove di auditing e di voto devono essere archiviate fisicamente offline e verificarne l'integrità in tempo reale durante le elezioni, senza compromettere altri requisiti e consentire un'efficace verifica umana.
Verifiable election integrity	Il sistema deve garantire la verificabilità che ogni voto conteggiato provenga da un elettore idoneo al voto e che tutti i voti siano conteggiati come espressi dagli elettori. Per ogni elettore il sistema deve anche prevedere la verificabilità che vi sia una sola scheda elettorale valida espressa dall'elettore nelle urne
Voto telematico	Esercizio per via telematica del diritto al voto.
Voto elettronico	Automazione del processo di voto attraverso strumenti elettronici.

Analisi delle procedure operative rilevanti

Operazioni preliminari

All'avvio del procedimento elettorale, contestualmente all'invio della convocazione delle assemblee elettive, vengono caricate sul sistema le anagrafi dell'elettorato attivo (distinto per organo da eleggere); il sistema genera automaticamente (in maniera casuale) credenziali univoche (user-name e password) monouso, che verranno inviate autonomamente via PEC a ogni avente diritto.

Coloro che non possiedono o non utilizzano il servizio PEC potranno recarsi direttamente al seggio dove, dopo aver sottoscritto una richiesta e previa identificazione, verranno abilitati al voto mediante la consegna delle credenziali che il Presidente di Seggio richiederà al sistema tramite mailbox di posta certificata che sarà specificatamente creato dall'OMCeO per la gestione della tornata elettorale.

Le relative credenziali di accesso saranno consegnate dall'amministrazione dell'Ordine al Presidente di Seggio all'insediamento del seggio, che provvederà a personalizzarle tramite il cambio della password. Contestualmente agli elettori viene comunicata una Url (link alla cabina elettorale) per partecipare alla votazione. Coloro che smarriscano le proprie credenziali potranno richiederne la rigenerazione tramite la PEC su indicata al Presidente del seggio, che provvederà tramite il sistema a un nuovo invio alla PEC dell'iscritto. Il sistema automaticamente bloccherà la votazione qualora già avvenuta.

Nei 10 giorni antecedenti la data di svolgimento delle votazioni vengono caricate sul sistema le anagrafi dell'elettorato passivo (liste e singoli candidati).

Identificazione degli elettori

L'accertamento dell'identità degli elettori nel sistema avviene, oltre che mediante l'utilizzo delle credenziali personali ricevute via PEC, attraverso l'inserimento di un secondo codice di controllo (OTP one time password) che verrà inviato via SMS sul numero di telefono cellulare comunicato dall'elettore. La password, da sostituire già al primo accesso, deve rispettare requisiti di sicurezza come di seguito indicati (o simili):

- lunghezza di almeno 8 caratteri alfanumerici
- utilizzo di almeno una cifra numerica
- utilizzo di caratteri speciali

Relativamente all'invio di SMS diretti al numero di telefono indicato dall'elettore, si rileva che il sistema di autenticazione prevede un legame univoco tra utenza telefonica e singolo elettore, cioè l'impossibilità di indicare più di una utenza telefonica per elettore.

A tal fine, chi scrive fa notare che l'identificazione degli utenti è un segmento estremamente critico di ogni sistema informativo (cfr. ISO/IEC 24760-1:2019). Per i servizi pubblici, entro il cui perimetro si possono senz'altro ricomprendere i sistemi di voto esaminati, il regolamento eIDAS fornisce le indicazioni normative generali.

È auspicabile che i sistemi di voto non adottino proprie procedure di identificazione dell'identità degli elettori ma che quest'ultima venga gestita attraverso schemi di identificazione conformi alle indicazioni degli organi tecnologici di vertice e allo stesso regolamento eIDAS: per l'Italia, il Sistema Pubblico di Identità Digitale (SPID) e la Carta di Identità Elettronica (CIE). È noto che tali schemi di identificazione hanno elevatissime caratteristiche di sicurezza e affidabilità, con una base di utenti dell'ordine della decina di milioni, che un sistema di identificazione "custom" non può in alcun caso possedere. Quest'ultimo, inoltre, non avrebbe alcun valore probatorio che è invece attributo ex lege ai due schemi nazionali anzidetti.

Si tenga ad esempio conto del fatto che il meccanismo di autenticazione tramite OTP inviata attraverso SMS costituisce già una vulnerabilità, soggetta ad attacchi di tipo SMS swapping/SIM hijacking. Le linee guida ENISA *"eIDAS COMPLIANT eID SOLUTIONS"* del marzo 2020 riportano a tal proposito quanto segue:

Email OTP is problematic regarding the risks linked to a mail account takeover by an attacker. Indeed, a mailbox is attractive to an attacker, and a successful phishing attack can't be overlooked. Therefore, this technology is not massively used anymore in eID schemes and should not be promoted.

Regarding OTP transmitting via SMS, this technology can be considered too reliant on the network's operator processes. Recent examples of SIM swapping (incl. Twitter's CEO on 31st August 2019) show the danger of having a mobile number both as identifier and authenticator.

Moreover, the SS7 protocol used by telecommunications companies to coordinate how texts and calls are rooted has a long-known security flaw allowing malefactors to send commands and route text messages as they wish.

Svolgimento delle operazioni di scrutinio

Successivamente alla chiusura delle votazioni e alla verifica del raggiungimento del quorum, viene attivata la fase di scrutinio. Concluse le operazioni di scrutinio il sistema genera automaticamente un report standard in formato PDF per singola votazione, contenente le seguenti informazioni:

- dati della votazione (titolo, descrizione, data e ora di apertura e chiusura)
- elenco e numero degli aventi diritto in anagrafe
- elenco nominale e numero dei votanti
- numero di schede bianche
- elenco dei candidati in ordine decrescente di preferenze ricevute.

Il file generato dal sistema contenente i risultati elettorali sarà conservato nei tempi previsti dalla normativa per tutte le eventuali contestazioni e verifiche e successivamente inviato all'OMCeO.

Il file PDF generato dal sistema viene descritto come non modificabile. Tale requisito, come normato dalle *Linee guida sulla formazione, gestione e conservazione dei documenti informatici* emanate da AgID, par. 2.1.1, è ottenibile esclusivamente attraverso una o più delle seguenti operazioni (a seconda delle modalità di formazione del documento informatico *de quo*):

- apposizione di una firma elettronica qualificata o di un sigillo elettronico qualificato o firma elettronica avanzata
- memorizzazione su sistemi di gestione documentale che adottino idonee politiche di sicurezza
- registrazione dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema
- versamento ad un sistema di conservazione.

È inoltre opportuno osservare che il report contenente i risultati elettorali deve essere associabile in maniera certa all'autore (l'OMCeO stesso o il soggetto da questi delegato per le procedure di voto), che ad esso devono essere associati in maniera permanente opportuni metadati e che la disponibilità e la riservatezza del contenuto del report medesimo devono essere garantite attraverso l'adozione di specifiche politiche e procedure contenute nel manuale di gestione documentale dell'OMCeO stesso, in conformità con quanto previsto dal par. 3.5 delle predette Linee guida.

Requisiti funzionali

Viene ritenuto opportuno il possesso dei seguenti requisiti funzionali in ordine alla fornitura del software in oggetto.

Requisito	**Osservazioni**
autenticazione a due fattori e modifica della password al primo accesso	Sui requisiti di autenticazione è opportuno fare riferimento ai requisiti ENISA.
anonimizzazione del voto, ossia applicazione delle misure tecniche finalizzate a impedire l'identificazione diretta e indiretta dei votanti e dei voti espressi	La letteratura scientifica sul voto elettronico concorda sulla necessità di disaccoppiare a monte i votanti ed i voti espressi. Forme di cifratura o di hashing del voto non sono generalmente sufficienti a garantire una anonimizzazione in senso stretto, ma semplicemente una pseudonimizzazione.
unicità del voto	
oscuramento delle preferenze espresse per i candidati e le liste fino a chiusura del seggio	Va rilevata l'assenza di requisiti in merito al protocollo crittografico di oscuramento
utilizzo dello standard di comunicazione HTTPS	L'uso di HTTPS è da considerarsi requisito minimo; è auspicabile che in ciascuna comunicazione machine-to-machine entrambe le parti siano identificati attraverso certificati. Vanno prese in considerazione le *Linea di indirizzo sull'interoperabilità tecnica* emanate da AgID con Circolare n. 1 del 9 settembre 2020
interfaccia di monitoraggio, in tempo reale, finalizzata a verificare il corretto funzionamento del sistema online e a ottenere la percentuale di voto, nonché il raggiungimento del quorum per ciascun Organo da eleggere	Come sopra; è necessario definire le modalità
piattaforma per l'esercizio del diritto di voto per via telematica attraverso tecnologia Cloud mediante servizi di tipo SaaS e laaS certificati ai sensi delle circolari AgID N. 2 e N. 3 del 2018	Le circolari AgID forniscono i requisiti a cui devono soddisfare i servizi SaaS e IaaS nel caso in cui essi vengano forniti ad una Pubblica Amministrazione. Esse tuttavia non impongono l'uso di servizi in cloud. L'uso di un'infrastruttura on premise può essere comunque oggetto di valutazione.
conservazione dei dati e delle schede elettorali per 120 giorni presso i loro sistemi, per tutte le eventuali contestazioni e verifiche, inviandone successivamente all'OMCeO copia su supporto digitale, garantendo l'anonimato di detti dati	La conservazione dei dati e delle schede elettorali deve essere conforme al manuale di conservazione dell'ente.
dovrà, al fine di permettere lo svolgimento di indagini conseguenti all'apertura di procedimenti di tipo civile o penale, assicurare la conservazione di una copia del codice	Gli artt. 68-69 del Codice dell'Amministrazione Digitale e le relative Linee guida sul Riuso dettano le condizioni e le modalità per l'acquisizione del codice sorgente dell'applicativo di voto, da

sorgente dell'applicativo che sarà utilizzato per la piattaforma di voto. Dovrà, altresì, rendere noti i seguenti elementi identificativi, che saranno citati all'interno dei verbali della Commissione Elettorale, di tale codice: versione software, data di rilascio, impronta digitale del pacchetto sorgente.	rilasciare sotto licenza aperta e da mettere a disposizione delle altre Amministrazioni per il riuso.

Valutazione conclusiva

I progetti presentati risultano estremamente simili tra di loro se non addirittura perfettamente sovrapponibili. In ordine a una valutazione conclusiva, è anzitutto da rilevarsi come l'adozione di strumenti di voto elettronico consente certamente una riduzione dei tempi e dei costi delle operazioni di voto, incentivando nel contempo una più ampia partecipazione alle stesse.

Resta tuttavia fermo che il voto elettronico deve garantire i requisiti che qui di seguito si riassumono:

- disaccoppiamento dei voti dai votanti
- segretezza e anonimità del voto
- identificazione certa delle credenziali degli elettori
- ogni elettore può votare una e una sola volta

Pertanto si rileva che gli elementi implementativi forniti non sono adeguati a rispondere ai requisiti sopra menzionati.

Le maggiori criticità sono da rilevarsi:

- nell'identificazione degli elettori, da implementare attraverso schemi riconosciuti a livello nazionale ed EU
- nel disaccoppiamento tra votante così come identificato dallo schema indicato al punto precedente e voto espresso
- nel disaccoppiamento tra elenco dei votanti ed elenco dei voti, descritta genericamente come realizzata attraverso protocolli crittografici senza alcuna specificazione sulla scelta degli stessi; è essenziale che il disaccoppiamento non si limiti semplicemente a una cifratura delle anagrafiche, potenzialmente vulnerabile in futuro, ma avvenga attraverso l'uso di protocolli a conoscenza zero (zero-knowledge security) in grado di consentire la verifica dell'integrità degli esiti della votazione senza alcuna possibilità di de-anonimizzare il voto stesso, indipendentemente dalla capacità computazionale dell'attaccante.

Va infine rilevato che i progetti proposti non presentano una chiara distinzione tra requisiti funzionali e modalità implementative.

È auspicabile invece che future proposte tengano conto della possibilità di adottare tecnologie basate su registri distribuiti e smart contract così come definiti all'art. 8-ter del Decreto-Legge 14 dicembre 2018, n. 135 convertito con modificazioni dalla L. 11 febbraio 2019, n. 12.

Riferimenti bibliografici

- Agenzia per l'Italia digitale, Linee guida sulla formazione, gestione e conservazione dei documenti informatici
- Agenzia per l'Italia digitale, Linee guida sull'interoperabilità tecnica
- Battisti Daniela (2005), "The Italian Way to e-Democracy", in Oxford Internet Institute (Ed.), A New Agenda for e-Democracy:Position Papers for an OII Symposium, Oxford, pp. 3–7
- Beckert, B. (2011), E-Voting in Europe: Why we should look at it, which arguments we should consider and what to expect in thefuture.: A background paper for the workshop on "E-voting in Europe"
- Beckert, B. (2011), E-public, e-Participation and e-Voting in Europe - Prospects and Challenges: Final Report, Brussels
- Bryl, V., Dalpiaz, F., Ferrario, R., Mattioli, A. and Villafiorita, A. (2007), "Evaluating Procedural Alternatives. A Case Study in E-Voting", in Corradini, F. and Polzonetti, A. (Eds.), Proceedings of MeTTeG 2007, 1st International Conference on Methodologies,Technologies and Tools enabling e-Government, Camerino, Italy, Halley Editrice, pp. 125–138
- Bryl, V., Dalpiaz, F., Ferrario, R., Mattioli, A. and Villafiorita, A. (2009), "Evaluating procedural alternatives. A case study in e-voting", Electronic Government, an International Journal, Vol. 6 No. 2, pp. 213–231
- Buchsbaum, T.M. (2004), "E-Voting: International Developments and Lessons Learnt", in Prosser, A. and Krimmer, R. (Eds.), Electronic Voting in Europe - Technology, Law, Politics and Society, Gesellschaft für Informatik, pp. 31–41
- Caarls, S. (2010), E-voting Handbook: Key steps in the implementation of e-enabled elections, Council of Europe
- Caporusso, L. (2008), "There is more to e- than meets the eye towards automated voting in Italy", in Reniu, J.M. (Ed.), E-voting: the last electoral revolution,Workshop Barcelona, Institut de Ciencies Pollitiques i Socials
- Caporusso, L., Buzzi, C., Fele, G., Peri, P. and Sartori, F. (2008), "Transition to electronic voting and citizen participation", in Krimmer, R. (Ed.), Electronic voting 2008 (EVOTE08): 3rd international conference, Castle Hofen, Bregenz, Austria, August, 2nd -4th, 2006, Ges. für Informatik, Bonn, pp. 191–200
- Chadwick, A. and May, C. (2003), "Interaction between States and Citizens in the Age of the Internet: "e-Government" in theUnited States, Britain and the European Union", Governance, Vol. 16 No. 2, pp. 271–300
- Council of Europe (2004), Legal, operational and technical standards for e-voting
- Council of Europe (Ed.) (2005), Reflections on the future of democracy in Europe, Making democratic institutions work, Strasbourg
- Council of Europe (2006), E-Voting: Lessons Learnt and Future Challenges
- Council of Europe (2011), Guidelines on transparency of e-enabled elections
- Council of Europe (2011), Guidelines on transparency of e-enabled elections
- Delis, A., Gavatha, K., Kiayias, A., Koutalakis, C., Nikolakopoulos, E., Roussopoulou, M., Sotirellis, G., Stathopoulos, P., Paschos, L., Vasilopoulos, P., Zacharias, T. and Zhang, B. (2014), "Pressing the Button for European Elections: Verifiable E-voting andPublic Attitudes Toward Internet Voting in Greece", in Krimmer, R. and Volkamer, M. (Eds.), 6th International Conference on Electronic Voting, EVOTE 2014, Lochau/Bregenz, Austria, October 28-31, 2014, TUT Press, Tallinn, pp. 129–135

- Delwit, P., Pilet, J.-B. and Kulahei, E. (2007), “Stumbling Blocks of Electronic Voting Revealed by U.S. and European Experiences”, in Anttiroiko, A.-V. and Mälkiä, M. (Eds.), Encyclopedia of digital government, Idea Group Reference, Hershey [etc.], pp. 1479–1484
- Driza Maurer, A. (2013), Report on the possible update of the Council of Europe Recommendation Rec(2004)11 on legal, operationaland technical standards for e-voting
- Driza Maurer, A. (2014), “Ten Years Council of Europe Rec(2004)11: Lessons Learned and Outlook”, in Krimmer, R. and Volkamer,M. (Eds.), 6th International Conference on Electronic Voting, EVOTE 2014, Lochau/Bregenz, Austria, October 28-31, 2014, TUT Press, Tallinn, pp. 111–117
- ENISA, eIDAS COMPLIANT eID SOLUTIONS, https://www.enisa.europa.eu/publications/eidas-compliant-eid-solutions/at_download/fullReport
- Gibson, R. (2005), “Internet voting and the European Parliament elections: Problems and prospects”, in Trechsel, A.H. and Mendez, F. (Eds.), The European Union and E-Voting: Addressing the European Parliament’s Internet Voting Challenge, Routledge, London, pp. 29–59
- Grabenwarter, C. (2004), “Report on the compatibility of remote voting and electronic voting with the standards of the Council ofEurope”, available at: http://www.venice.coe.int/webforms/documents/CDL-AD(2004)012.aspx (accessed 16 December 2013)
- Grönlund, K. (2004), “Cyber Citizens: Mapping Internet Access and Digital Divides in Western Europe”, in Kersting, N. andBaldersheim, H. (Eds.), Electronic voting and democracy: A comparative analysis, Palgrave Macmillan, pp. 20–38
- International Standardization Organization, ISO/IEC 24760-1:2019, IT Security and Privacy — A framework for identity management
- Kies, R. and Kriesi Hanspeter (2005), “Internet voting and opinion formation: the potential impact of a pre-voting sphere”, inTrechsel, A.H. and Mendez, F. (Eds.), The European Union and E-Voting: Addressing the European Parliament’s Internet Voting Challenge, Routledge, London, pp. 147–165
- Kies, R., Mendez, F., Schmitter, P.C. and Trechsel, A.H., Evaluation of the Use of New Technologies in Order to Facilitate Democracyin Europe, Scientific and Technological Options Assessment Series
- Krimmer, R. (2008), “The development of remote electronic voting in Europe”, in Reniu, J.M. (Ed.), E-voting: the last electoral revolution, Workshop Barcelona, Institut de Ciencies Pollitiques i Socials
- Kubicek, H. and Westholm, H. (2005), “Scenarios for Future Use of E-Democracy Tools in Europe”, International Journal of Electronic Government Research, Vol. 1 No. 3, pp. 33–50
- Kushchu, I. and Kuscu, M.H. (Eds.) (2005), Proceedings of EURO mGOV 2005: The first European Mobile Government Conference, Mobile Government Consortium International LLC
- Ladeur, K.-H. (2005), “e-Voting: a new political institution for the network society? New Life for an old democratic procedure”, inTrechsel, A.H. and Mendez, F. (Eds.),
- The European Union and E-Voting: Addressing the European Parliament’s Internet VotingChallenge, Routledge, London, pp. 202–222
- Magkos, E., Kotzanikolaou, P. and Douligeris, C. (2007), “Towards secure online elections. models, primitives and open issues”, Electronic Government: An International Journal, Vol. 4 No. 3, pp. 249–268
- McGaley, M. and McCarthy, J. (2004), “Transparency and E-Voting: Democratic vs. commercial interests”, in Prosser, A. andKrimmer, R. (Eds.), Electronic Voting in Europe - Technology, Law, Politics and Society, Gesellschaft für Informatik, pp. 153–164

- Mendez, F. and Trechsel, A.H. (2004), The European Union and E-Voting (Electronic Voting), Routledge Advances in EuropeanPolitics, Taylor & Francis
- Mendez, F. and Trechsel, A.H. (2005), “The European Union and e-voting Upgrading Euro-elections”, in Trechsel, A.H. andMendez, F. (Eds.), The European Union and E-Voting: Addressing the European Parliament’s Internet Voting Challenge, Routledge, London
- Monnoyer-Smith, L. and Maigret, E. (2002), “Electronic Vote and Internet Campaining. State of the Art in Europe and RemainingQuestions”, in Traunmüller, R. and Lenk, K. (Eds.), Electronic government: First international conference, EGOV 2002, Berlin /Heidelberg, Springer, Berlin, New York, pp. 280–283
- O'Donnell, D. (Ed.) (2010), The proceedings of the 10th European Conference on eGovernment: National Centre for Taxation Studies and University of Limerick, Ireland, 17 - 18 June 2010, Academic Publ. Limited, Reading
- Pammett, J.H. and Goodman, N. (2013), Consultation and Evaluation Practices in the Implementation of Internet Voting in Canadaand Europe
- Peltu, M. and Coleman, S. (2005), A New Agenda for e-Democracy: Position Papers for an OII Symposium, Oxford
- Prandini, M. and Ramilli, M. (2011), “Taking the Best of Both Worlds: A Comparison and Integration of the U.S. and EU Approaches to E-Voting Systems Evaluation”, in Sprague, R.H. (Ed.), Proceedings of the 44th Annual Hawaii International Conference on System Sciences, IEEE Computer Society Press, Los Alamitos, Calif
- Pratchett, L., Wingfield, M., Fairweather, B.N. and Rogerson, S. (2005), “Balancing security and simplicity in e-voting: towards aneffective compromise?”, in Trechsel, A.H. and Mendez, F. (Eds.), The European Union and E-Voting: Addressing the EuropeanParliament’s Internet Voting Challenge, Routledge, London, pp. 166–184
- Prosser, A. and Krimmer, R. (Eds.) (2004), Electronic Voting in Europe - Technology, Law, Politics and Society, Gesellschaft fürInformatik
- Prosser, A. and Krimmer, R. (2004), “The Dimensions of Electronic Voting”, in Prosser, A. and Krimmer, R. (Eds.), Electronic Votingin Europe - Technology, Law, Politics and Society, Gesellschaft für Informatik, pp. 21–28
- Remenyi, D. (Ed.) (2009), 9th European conference on e-government: Westminster Business School University of Westminster,London UK, 20-30 June 2009, ECEG, Dublin
- Remmert, M. (2004), “Towards European Standards on Electronic Voting”, in Prosser, A. and Krimmer, R. (Eds.), Electronic Votingin Europe - Technology, Law, Politics and Society, P-47, Gesellschaft für Informatik, pp. 13–16
- Schmitt, H. (2005), “Second-order elections to the European Parliament: is e-voting the solution?”, in Trechsel, A.H. and Mendez,F. (Eds.), The European Union and E-Voting: Addressing the European Parliament’s Internet Voting Challenge, Routledge, London, pp. 91–107
- Schmitter, P.C. (2005), “e-Voting, e-democracy and EU-democracy: a thought experiment”, in Trechsel, A.H. and Mendez, F. (Eds.), The European Union and E-Voting: Addressing the European Parliament’s Internet Voting Challenge, Routledge, London, pp.187–201
- Stein, R. and Wenda, G. (2014), “Ten Years of Rec(2004)11 - The Council of Europe and E-voting”, in Krimmer, R. and Volkamer,M. (Eds.), 6th International Conference on Electronic Voting, EVOTE 2014, Lochau/Bregenz, Austria, October 28-31, 2014 ,TUT Press, Tallinn, pp. 105–110
- Svensson, J. and Leenes, R. (2003), “E-voting in Europe: Divergent democratic practice”, Information Polity, Vol. 8 No. 1, pp. 3–15

- Tambouris, E. (2002), “An Integrated Platform for Tele-voting and Tele-consulting within and across European Cities. The EURO-CITI Project”, in Traunmüller, R. and Lenk, K. (Eds.), Electronic government: First international conference, EGOV 2002, Berlin /Heidelberg, Springer, Berlin, New York, pp. 350–357
- Tambouris, E. and Gorilas, S. (2003), “Evaluation of an e-democracy Platform for European Cities”, in Traunmüller, R. (Ed.), Electronic government: Second international conference, EGOV 2003, Lecture Notes in Computer Science, Vol. 2739, Springer,Berlin / Heidelberg, pp. 43–48
- Trechsel, A.H. and Mendez, F. (2005), The European Union and E-Voting: Addressing the European Parliament’s Internet Voting Challenge, Routledge, London.Udris, J. (2014), “iVote.lt - Practical Attempt to Overcome Internet Voting-Related Fears”, in Krimmer, R. and Volkamer, M. (Eds.), 6th International Conference on Electronic Voting, EVOTE 2014, Lochau/Bregenz, Austria, October 28-31, 2014, TUT Press,Tallinn, pp. 19–22
- Unione Europea, REGOLAMENTO (UE) N. 910/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (eIDAS)
- Whitmore, K. (2008), Information Report on the Electronic Voting in the Finnish Municipal Elections, Congress of Local and Regional Authorities