Verifiability Experiences in Government Online Voting Systems

Jordi Puiggalí[1(✉)], Jordi Cucurull[1], Sandra Guasch[1], and Robert Krimmer[2]

[1] Research and Security Department, Scytl Secure Electronic Voting, 08008 Barcelona, Spain
{jordi.puiggali,jordi.cucurull}@scytl.com
[2] Ragnar Nurkse Department for Innovation and Governance, Tallinn University of Technology, 12618 Tallinn, Estonia
robert.krimmer@ttu.ee

Abstract. Since the introduction of verifiability in the online government elections of Norway in 2011, different governments have followed similar steps and have implemented these properties in their voting systems. However, not all the systems have adopted the same levels of verifiability nor the same range of cryptographic mechanisms. For instance, Estonia (2013) and New South Wales (Australia, 2015) started by adopting individual verifiability to their systems. Switzerland updated its regulation in 2014 to include individual and universal verifiability in order to by-pass the previous limitation of voting online up to 30% of the electorate. Geneva and Swiss Post voting systems are adapting their systems to this regulation and currently provide individual verifiability (and universal in the case of Swiss Post). In this exploratory paper, we study the different approaches followed by the election organizers that offer online voting, their current status and derived future tendencies.

Keywords: Electronic voting protocols · Election verifiability

1 Introduction

Whenever an election process is carried out using traditional or electronic means, transparency and auditability are the basis to ensure the accuracy of the results. In traditional elections, audit processes can be easily implemented since they are based on physical tangible elements: paper ballots, physical ballot boxes, manual recount, etc. These items can be supervised by both, voters and external auditors or international election observers (see, amongst others, [7]).

However, in electronic environments, the same elements are not tangible and most of the processes are performed through computers and communication networks, making human audits almost impossible [35]. While security measures such as vote encryption or digital signatures can protect the secrecy and integrity of votes, it is also important to verify that these mechanisms are behaving properly: i.e., they are certainly encrypting, decrypting and digitally signing the selection made by the voter. Some governments publish the source code of

R. Krimmer et al. (Eds.): E-Vote-ID 2017, LNCS 10615, pp. 248–263, 2017.
DOI: 10.1007/978-3-319-68687-5_15

their voting systems to ensure that these security mechanisms have been correctly implemented (for a discussion of its relevance see [19]), like Norway in 2011 (fully disclosure), Estonia in 2013 (partial disclosure) or Geneva (Switzerland) in 2017 (partial disclosure). Nevertheless, while this measure provides certain transparency as it allows to auditing the implementation of the system, it does not provide any proof of accuracy in the election process. For instance, it does not avoid an undiscovered bug in the source code to be exploited during the election, neither it guarantees that the source code used in the voting system is the one published. For this reason, it is essential to provide means to audit the proper behavior of the systems during the election, regardless of the correctness of the software source code neither its proper execution. Apart from the evaluation and certification (for a discussion see [13]) the solution suggested would be the implementation of mechanisms that allow both voters and external auditors to verify the proper behavior of the voting system: verifiable voting.

1.1 Verifiability Concepts

Verifiable voting systems are those that implement mechanisms, based either on physical means (e.g., paper trails [36]) or cryptographic ones (e.g., cryptographic proofs [21]), that can be used to audit the proper execution of computer-based electronic processes. Generally, these mechanisms are classified in the electronic voting literature [5,10,23] in two types, based on who performs the verification: individual verifiability and universal verifiability.

- **Individual verifiability:** It is related to the verification mechanisms that can be used by the voter during the voting process. These can be subdivided in two complementary mechanisms [23]: cast-as-intended and recorded-as cast verifiability. Cast-as-intended verifiability enables the voter to verify if the electronic vote registered in the system really contains the selections made. In other words, it allows the voter to detect if any error or attack manipulated the vote contents when it was recorded (i.e., encrypted) by the voting system. Recorded-as-cast enables the voter to verify that her verified vote has been successfully stored in the electronic Ballot Box that will be used in the tallying phase. Like in any audit process, the number of verified votes is important to have a more accurate audit. So, the larger amount of voters able to verify their votes, the higher is the probability to detect even small inconsistencies. For instance, in an election with 10.000 votes, if there is a manipulation of 100 votes (1%) the verification of 1% of the voters (100 votes) has a probability of 64% of being detected (see General Recount Formula in [39]). Whether the manipulation is larger the chances are closer to 100% (e.g., a manipulation of 200 votes will be detected with a probability of 87% by the same amount of verifier voters). Therefore, it is important that these mechanisms facilitate the participation of the voters in the verification process.
- **Universal verifiability:** It refers to the verification mechanisms [23] that can be performed by anyone regardless of the level of privileges of the actor of the system (i.e., a voter or election manager of the voting system). In this sense,

universal verification does not include cast-as-intended and recorded-as-cast verifiability mechanisms because they are processes that can be only used by voters. However, it includes the so called counted-as-recorded verifiability mechanisms, whose purpose is allowing anyone the verification of accurate results in both vote opening (decryption) and counting.

In both cases, individual and universal verifiability should not compromise any of the other security requirements of an election, specially voter privacy. When individual and universal verifiability are given, it is said that systems provide end-to-end verifiability.

Another significant aspect related to verifiability is to prove that the verifiable mechanism implements this property in a sound way. Therefore, it is possible to discern if the verification mechanism is weak or strong against attackers, or even if it just a fake claim. To this end, provable security [14] is used to make a formal statement of the security properties of the verification mechanism (security proof) and the assumptions under which these properties must be evaluated, so the academic community or experts can validate the correctness or robustness of the verifiability claims. Security proofs can be complemented with formal proofs (i.e., formal languages) to facilitate the security proof automatic validation.

1.2 Methodology

To date, verifiability is an understudied phenomenon in electronic voting, and elections in general. Hence there is a need for an empirical study within its real-life context, ideally by means of a case study [44]. The present topic at hand is ideal for an exploration of the matter in deep. For this study, election systems in countries, where verifiability has been introduced in a recent legally-binding election on regional or federal level, are analyzed.

1.3 Government Adoption

Since the first government experiences in early 2000 [33], the security of internet voting systems has improved notably. One of the main enhancements was the adoption of audit processes based on verifiability mechanisms, which provided more transparency to electronic voting elections. The relevancy of verifiability in elections was already present in the first version of the e-voting standards of the Council of Europe [6]. Being this concept further developed in the new revision of these standards [5] and related implementation guidelines [4]. Following the recommendations of the Council of Europe, verifiability mechanisms were initially introduced by the Norwegian government in 2011 [8], and later by Estonia (2013) [9], Switzerland (2015) [11] and Australia (2015). However, the approach followed in each of the four contexts differs on the verifiability **scope** (individual and/or universal) and the verifiability **mechanism** implemented. Despite there are other well-known government online voting experiences, such as Canada or other Swiss voting systems, they are not considered because they have not adopted yet any type of verifiability (e.g., Zurich that currently lost its authorization).

Scope: Norway adopted in 2011 individual and universal verifiability, with the particularity that universal verifiability was only publicly accessible on demand (i.e., auditors needed to apply for an audit). Estonia adopted in 2013 individual verifiability, and it is planing to include universal verifiability in the near future. Switzerland changed in 2014 its Federal regulation to request individual and universal verifiability in their voting systems. In addition to it, Swiss regulation has a particular interpretation of universal verifiability as the publication of information is not required for verification. Neuchâtel and Geneva adopted individual verifiability in 2015. Finally, Australia adopted individual verifiability in 2015 but without universal verifiability like the Estonian case.

Mechanism: Both Norway and Switzerland follow the approach based on Return Codes as the way voters can verify the content of their vote (see Sect. 2). The main difference within both countries is that while Norway allowed voters to vote multiple times and therefore, in case of discrepancy, voters could vote again, in Switzerland, voters are only allowed to cast one vote. In this scenario then, voters need to introduce a Confirmation Code to confirm or reject the vote after verification. On the other hand, Estonia and Australia use the approach of decrypting votes after casting them. In Estonia verification requires the installation of an application to the mobile phone and the verification period is only possible during a limited period after casting the vote (between 30 min and 1 h). In Australia (New South Wales State), the verification is done by contacting a specific call center that decrypts the vote and describes the content to the voter. In this case, the verification process was open until the end of the election.

This paper is focused on the verifiable internet voting systems implemented by different governments in the last years, their advances regarding verifiability and future plans. Section 2 includes an explanation of the individual verification mechanisms introduced by the governments who are or have been providing internet voting. Section 3 is focused on universal verification mechanisms, while in Sect. 4 there is a comparative analysis together with some conclusions.

2 Individual Verifiability in Government Implementations

There are multiple proposals in academia of cryptographic protocols implementing individual verifiability and more concretely cast-as-intended verifiability. However, current government implementations can be classified in two main groups:

– Return Codes mechanisms: In this case, voters cast their votes and receive from the voting system a set of numeric codes that are calculated over the encrypted vote (e.g., four numbers sent though SMS or shown in the same screen). By using a Voting Card sent during the election setup, voters can check whether the received codes are related to their selected voting options. The main references of this mechanism are the Norwegian [37] and Neuchâtel (Switzerland) [22] voting systems. Geneva implements Return Codes over unencrypted votes.

– Cast and decrypt: In this approach, voters cast their votes, latterly, they have the option of recovering and decrypting them to see the contents. Recovery can be done through a trusted device (e.g., mobile phone) or a trusted third party (e.g., a verification server). Reference implementations are Estonia [28] and Australia [16].

Despite that one of the most well known open source voting system is Helios, none of the government voting systems implement its "cast or verify" method [12]. That is why it is not considered for this analysis.

In addition to cast-as-intended, the recorded-as-cast verifiability is also implemented by some government electronic voting solutions. The most common approach consists in providing the voter with a Receipt that can be used to check whether the vote was recorded (stored) in the Ballot Box. The Receipt contains a fingerprint of the encrypted vote and whenever the vote is cast and recorded into the Ballot Box, a fingerprint of this encrypted vote is published in a Bulletin Board. A Bulletin Board is an append-only public repository (e.g., website) accessible to voters for them to search for the fingerprint contained within their Receipts. The presence of the fingerprint ensures voters that their votes are stored in the Ballot Box. The fingerprints in the Bulletin Board can also be used by auditors to crosscheck them with the actual votes, guaranteeing this way the integrity of the Ballot Box and adding the universal verifiability value to the process. The main reference of this mechanism is the Norwegian voting system [37].

Finally, some of the individual verifiable propososals also included a vote correctness property [15]. Vote correctness allows the voting systems to check if the encrypted votes contain a valid vote without decryption. Hence, in case of a potential mistake or attack in the client side that could invalidate the vote casting, it will be detected in the server before storing the vote in the Ballot Box. This way, the voter can be notified and can try to cast the vote again. For instance, the system will detect whether the content of an encrypted vote has either an invalid option or an invalid combination of options without learning the vote contents (i.e., repeated candidates or an invalid combination of them). It is not a specific requirement for individual verifiability but a property used in Norway and Switzerland inherit from their verification mechanism.

2.1 Individual Verifiability in Norway

Norway introduced individual verifiability in the voting system requirements of the public process started in 2009 [29]. Among different proposals, the government finally chose a solution based on using Return Codes for individual verifiability. The voting system was used by 10 municipalities during the 2011 Municipal Elections, and 13 municipalities during the 2013 General Elections. After 2013 elections, there was a change of government and the new winning party (contrary to internet voting) stopped using the voting system [31]. However, online voting is currently still in use in Norway by municipalities, especially for referendums and consultations.

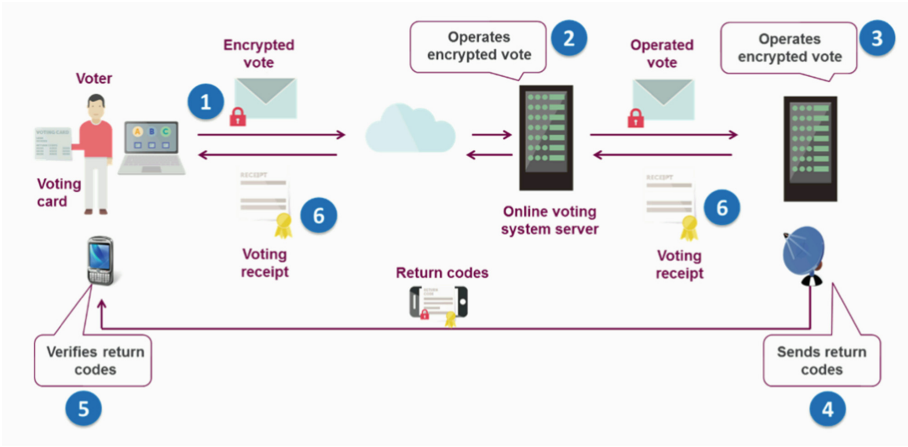

Fig. 1. Norwegian voting system

The Norwegian voting system (Fig. 1) is based on Return Codes, i.e. generation of specific Voting Cards for voters containing 4 digits code for each possible voting option. The 4 digits codes of each Voting Card are different for each voter, so it is not possible to deduce the Return Code without having the Voting Card. When the voter casts a vote, this is encrypted and digitally signed in the voter device, and it is also sent to the voting servers. One first server (Vote Collector Server) performs a cryptographic operation over the encrypted vote and sends the result of this operation to a second server (Return Code Generator). The Return Code Generator performs a second cryptographic operation, uses the result of this operation to obtain the 4 digits of the Return Code and sends it to the voter through SMS. Using their voting card, voters can verify if the received Return Code corresponds to their selection, ensuring that the encrypted vote received by the server contains the correct selections. If the contents of the encrypted vote are different, the operation will not return the correct Return Code. However, as the Norwegian voting system permits multiple voting, the voter can cast another vote if does not agree with the previous one. This cast-as-intended mechanism is responsible of the individual verifiability of the system, but does not include recorded-as-cast verification. For a detailed description of this voting system the following references are recommended [30,37].

In the 2013 National Elections, the Norwegian voting system included recorded-as-cast to individual verifiability by means of Voting Receipts. The Voting Receipt was provided to the voter once the vote was accepted and stored in the Ballot Box. This receipt contains a fingerprint of the encrypted and digitally signed vote cast by the voter.

In addition to the receipt, the fingerprints of all the votes stored in the Ballot Box were also published, so voters were able to check the presence of their votes by searching the fingerprint of the Voting Receipt in a public Bulletin Board.

The individual verifiability properties of the voting system were security proven using a security proof of the cryptographic protocol [24]. As an additional property, the system allowed to check the correctness of the votes in the server without decrypting them (vote correctness) applying some rules to the Return Codes generated. For instance, it detects if one Return Code appears multiple times (i.e., the same option is encrypted more than once in the vote) or if the Return Code is the expected one for the selection (e.g., if the Return Code of the selected Candidate is related to the Return Code of the selected Party).

One of the main concerns of the individual verifiability is the percentage of voters that verified their votes. The limitation of this system is that it cannot monitor the number of voters that performed the verification, since verification does not require interaction with the server after sending Return Codes. However, during some small-scale test elections (referendums) done before the 2011 municipal elections, the Ministry conducted a voter survey that shown that almost 90% of the voters admitted the Return Codes verification [40]. Furthermore, during these elections an error in the printing process made 1% of the voters of some municipalities to receive a wrong Voting Card. Based on the number of calls received from voters claiming that the Return Code was incorrect, the election manager was able to infer the percentage of voters that verified the votes. The verification was carried out by more than 70% of the affected voters. However, this number cannot be considered representative of the whole participants since in both cases was obtained from an small sample of voters (hundreds).

Finally, the source code of the voting system was also made publicly available before the election [30].

2.2 Individual Verifiability in Estonia

The Estonia voting system individual verifiability was introduced in 2013 Municipal Elections [28]. The individual verifiability cast-as-intended mechanism is based on using a mobile phone application for the voter verification process. In the Estonian example (Fig. 2), the votes are encrypted and digitally signed in the voting terminal (computer) and sent to the server. If the vote is accepted, the voting terminal displays a 2D barcode containing the ballot identity and the secret padding used for encrypting the vote. By using this application, voters can scan the 2D barcode, obtain the ballot identifier and used it to download the encrypted vote from the voting server. Once the encrypted vote is downloaded, the mobile application uses the secret padding to recover the contents of the encrypted vote and present it to the voter. Since the Estonian voting system allows multiple voting, voters can cast another vote if they do not agree with the contents shown in the mobile phone application. To avoid coercion or vote buying, the voter has a predefined limited verification period (between 30 min and 1 h). More details about the voting systems can be found in the following reference [28].

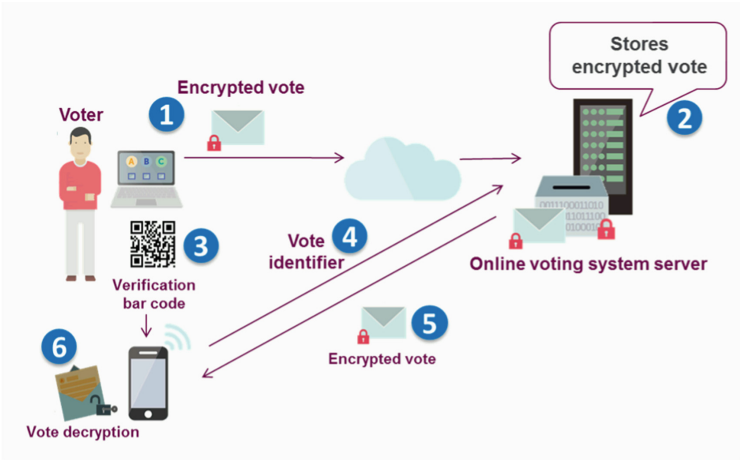

Fig. 2. Estonian voting system

Since the voter downloads the encrypted vote from the voting system, it can be assumed that the verification process also involves recorded-as-cast verifiability. However, the limitation of verification time does not ensure that the vote remains in the Ballot Box or reaches the counting process.

This system allows monitoring the number of voters that performs the verification process, since voters need to be connected to the server to download the ballot. Current verification percentage is about 4% of the voters [27].

Regarding provable security, there is no proof yet published that demonstrates the security of the individual verifiable protocol properties of the system. Additionally, it does not support server vote correctness verification of the encrypted vote. In 2013, the Estonia government published the source code of the system, but just the server and mobile application part [3]. The source code of the voting client was not published to avoid the creation of fake voting clients.

2.3 Individual Verifiability in Switzerland

Switzerland updated its Internet Voting regulation in 2014 including both individual and universal verifiability [18]. The main aim was to authorize Swiss Cantons to increase up to 50% and 100% the percentage of the electorate that could use online voting (Originally, authorization was restricted to 30% of the Canton electorate). In order to authorize to increase the electorate up to 50%, systems needed to include individual verifiability and must be certified by an entity accredited by the Federal Chancellery. The certification process includes the provision of security and formal proofs of the individual verifiability protocol, as well as passing a Common Criteria certification with assurance level 2. Geneva [2] and Neuchâtel [22] cantons updated their voting systems to achieve individual verifiability in 2015, but they did not start the 50% electorate authorization

process. In 2016 Swiss Post implemented a voting system [41] with individual verifiability (based on the same technology used in Neuchâtel) and started the authorization process to achieve the 50% electorate regulation requirements. In the meantime, Geneva announced plans to redesign its voting system to achieve 100% electorate authorization in the future [25].

Geneva and Swiss Post voting systems (Neuchâtel is currently using Swiss Post one), provide individual verifiability based on Return Codes (Fig. 3). However, the approach differs on how the Return Codes are generated. In the Swiss Post voting system, the protocol is an evolution of the one used in Norway but without the need of using two servers for the Return Codes. In this implementation, the encrypted and digitally signed vote is concatenated with verification information obtained by performing a second cryptographic operation over each voting option (known as partial Return Codes). The encrypted and digitally signed vote together with the verification information is sent to the voting server. This server validates the received information and performs a second operation over the verification information, obtaining the information that allows to recover the 4-digit Return Code of the selected voting options. These Return Codes are sent back to the voter and displayed in the same voting device. If the voter agrees, then a Confirmation Code is sent, which is required for the acceptance of the vote in the counting process and the update of the voting status in the electoral roll. If the voter disagrees, the vote remains unconfirmed and the Internet voting channel cannot be used again, but the voter can still use another voting channel for contingency (postal or pollsite) because her vote casting status in

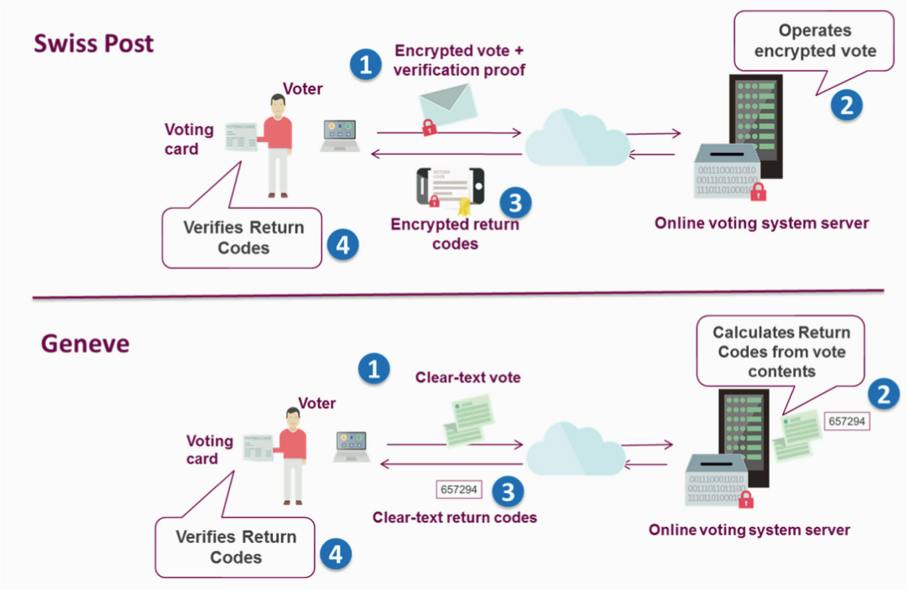

Fig. 3. Swiss voting systems

the electoral roll has not been updated. More detailed information of the voting system can be found in [41,42].

In the Geneva voting system, the cast vote is not encrypted in the voter device but sent though an encrypted communication channel (SSL) to the voting server. The voting server can see the selected voting options, calculates the 4-digit Return Codes and sends the codes back to the voter. The vote is then encrypted by the server and stored waiting for voter confirmation. Voter confirmation is also based on a Confirmation Code that must be sent by the voter after verification. Without confirmation, the vote will not be used in the counting phase. Detailed information about the voting system can be found in [2].

Both voting systems provide cast-as-intended verifiability, nevertheless Geneva checking the presence of the vote in the counting phase (recorded-as-cast) is not possible in the Genevan model. Only in the case of Swiss Post voting system a Voting Receipt is provided together with a fingerprint of the encrypted and digitally signed vote (as in Norway). Apart from that, the list of the fingerprints of the votes present in the Ballot Box is published after the voting period ends. Both voting systems provide vote correctness properties as in Norway, but only the Swiss Post model has security and formal proofs of the individual verifiability protocol. Geneva published in 2017 the source code of its voting system, but only the administration offline components [1]. In none of the cases, there are numbers of the percentage of voters that verified their votes, since the verification is offline.

2.4 Individual Verifiability in Australia

Australia introduced individual verifiability in 2015 through the New South Wales (NSW) State election [16]. The year before, the State of Victoria implemented a pollsite voting system that provided also individual verifiability (vVote [17]). However, this voting system was designed to be deployed in local and remote polling stations (e.g., consulates), so it has not been considered as an online voting system for this study.

The individual verifiability mechanism implemented by the NSW voting system (Fig. 4), known as iVote, was based on phone calls that voters had to make to verify the content of their cast votes (i.e., cast-and-decrypt approach). During the voting process, votes were encrypted and digitally signed in the voter device and after casting, the voter received a Receipt with a unique Receipt Number. Votes were encrypted with a double encryption mechanism, to allow both the decryption by the Electoral Board and the decryption by a Verification Server with the help of the voter (using the Receipt Number). The voter was able then to call before the voting period expired to validate her vote. When calling, the voter needed to introduce her voting credentials and the voter Receipt Number. The Verification Server used the voter credentials to retrieve the encrypted vote, and used its private key and Receipt Number to decrypt it. Through the phone, the voter was able to listen the vote contents. To make the phone voting process more user friendly, the voter credentials and Receipt Number were numerical. In case voters did not agree with the voting options, they had to contact the

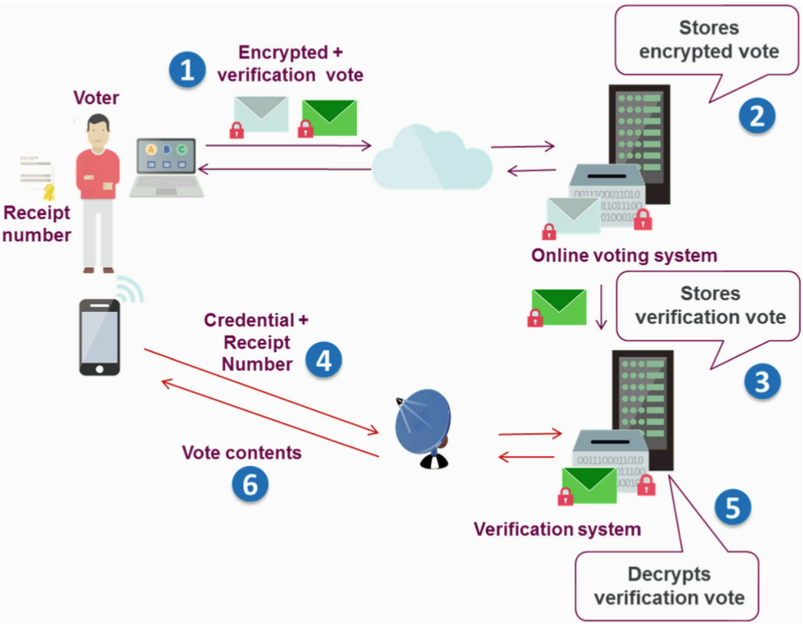

Fig. 4. New South Wales voting system

election authorities. Multiple voting was not allowed, but election officers were able to cancel the vote and provide new credentials to the voter when necessary.

The NSW individual verification approach, provided cast-as-intended and recorded-as-cast verifiability, since the validation process allowed to check that the vote was present in the Ballot Box until the voting period ended. Since the verification required to be connect to a server, it was possible to monitor the number of voters that verified their votes. In this case the verification ratio was 1,7% in 2015 election [16]. Regarding the availability of the source code and security proofs, the source code is not available and no security proofs of the voting protocol were generated. The verification mechanism did not provide vote correctness either.

3 Universal Verifiability in Government Implementations

Currently, universal verifiability is only implemented the Norwegian and the Swiss Post voting systems. In both cases, this is mainly achieved by means of a universal verifiable mixnet and decryption components.

In the case of Norway, in 2011 a universal verifiable mixnet designed by Scytl [38] was used, while in 2013 the Verificatum Mixnet [43] was also used. In both cases, instead of publishing the verification data, the Norwegian government made a public call for participating in the universal verification of the results. However, the source code of the system was made publicly available.

In Switzerland, the Swiss Post voting system has been using a verifiable Mixnet since 2015 (Geneva only implements a standard Mixnet without verifiability). However, the Federal Chancellery regulation requires a specific universal verifiability approach to certify a voting system and achieve the 100% electorate authorization process [18]. This model requires that the universal and individual verification processes use specific and independent trusted components for the audit proofs generation, known as Control Components. According to the regulation [18], these Control Components can be implemented in two different ways: (i) as two Hardware Security Modules (HSM) from two different vendors, or (ii) as 4 standard computers using different operating systems. These Control Components should be deployed completely isolated one from the other and operated by different teams. With these conditions, the Federal Chancellery considers that universal verifiability can be implemented without publishing the verification information.

Swiss Post and Geneva are working on adapting their voting system architecture to achieve these requirements (Geneva announced in 2016 a new redesign of the voting protocol to accomplish these requirements).

Estonia does not implement universal verifiability (it does not implement any Mixing process), but announced plans to incorporate it in a short-mid term [26]. In Australia, the NSW voting system does not implement any Mixing process and it has not announced any plans for universal verifiability yet. However, it implements a mechanism to match the decrypted votes with the ones present in the Verification Server (performing a reencryption of the decrypted votes).

4 Comparison

Table 1 summarizes the different verifiability properties compiled from the information of the online voting systems studied in this paper.

Despite the Norwegian voting system was the first in introducing verifiability to online voting systems, it can be still considered one of the most complete ones in the sector.

Switzerland (and more concretely the Swiss Post voting system) has a similar level of verifiability, which is explained by the fact the Chancellery used the Norwegian government experience as a reference for its regulation.

The other voting systems (except for Australia) have already started incorporating individual verifiability and have even announced plans to incorporate universal verifiability in a near future. Therefore, it is clear that verifiability is becoming essential for any online voting system.

Regarding the percentage of voters that participate in the verification process, it is easier to monitor it on the systems that perform vote decryption for verification (i.e. Cast and decrypt). Numbers in these cases seem to be low, but they are a good reference to calculate the probability in issues detection. In the case of Return Codes, the only reference comes from Norway and it seems extraordinarily high. However, further analysis should be done in this mechanism because numbers are based on small samples.

Table 1. Properties of evaluated systems

	Norway	Estonia	Switzerland (Swiss Post)	Switzerland (Geneva)	Australia (NSW)
Cast-as-intended	Return codes	Decryption in device	Return codes	Return codes	Decryption in server
Recorded-as-cast	At any time with receipts	Up to 1 h	After counting with receipts	None	N
Counted-as-recorded	Verifiable mixnet	None	Verifiable mixnet	None	Yes, through vote re-encryption
Voter verification	90–70% (small sample)	4% (large sample)	No data	No data	1% (large sample)
Public source code	All the system	Only server side	None	Only counting side	None
Vote correctness	Yes	None	Yes	Yes	None
Provable security	Yes (Individual and Universal)	None	Yes (Individual and Universal)	None	None

Regarding the publication of the source code, only Norway had a full disclosure. The other voting systems that published the source code did it partially. This can be in part justified based on the fact that these other voting systems do not provide end-to-end verifiability and therefore, the risk of an undetected attack is higher. In any case, Estonia and Geneva announced plans of full disclosure in the future, which indicates a general tendency among online voting systems. In the meantime, the Swiss Federal Chancellery is not demanding source code disclosure yet for systems that are under the 100% electorate authorization.

Vote correctness was present in the Norwegian voting system and latterly adopted by the Swiss voting system as well. It is still uncertain whether other voting systems will also adopt this trend, which was initially provided by homomorphic tally voting systems [20] and currently by those using Return Codes.

Finally, from the point of view of provable security, only Norway and Switzerland used security proofs to demonstrate the security properties of their verification mechanisms. In fact, Switzerland is even more exigent as also formal proofs for authorization of the voting systems are required. Proving the security of the voting systems using cryptographic and formal proofs is a recommended practice that it is expected to be extended, since it allows security experts to verify whether the claimed verifiability properties are certainly present in the voting system and whether they are robust (i.e., under which assumptions these properties are present). This way the governments can certify the verifiability of

the voting systems and discard those that are not providding these guarantees or are poorly implemented.

As a general conclusion, the assumption is that verifiability in elections will be implemented in the future, in particular due to transparency needs and to the inherent general distrust in not visible or tangible processes. Still, none approach can be identified as "best-practice". However, Norway and Switzerland can be identified as the ones that have made so far more efforts towards verifiability implementation. It can be certainly stated that election operators start implementing individual verifiability before the universal one due to the mentioned additional advantage for the individual voter. Nevertheless, while universal verifiability brings a significant security gain, its implementation is less frequent mainly due to trusted arguments defended by governments (audit environments considered secure because they are under the control of election authorities) and due to its mathematical complexity hard to understand for most.

Acknowledgments. The contributions of R. Krimmer to this article are partially supported by Estonian Research Council Project PUT1361 and Tallinn University of Technology Project B42.

Disclaimer. The authors of the paper affiliated to Scytl Secure Online Voting have been involved in some of the electronic voting systems described.

References

1. E-voting system chvote 1.0. source code offline administration application. https://github.com/republique-et-canton-de-geneve/chvote-1-0
2. E-voting system chvote 1.0. system overview. https://github.com/republique-et-canton-de-geneve/chvote-1-0/blob/master/docs/system-overview.md
3. Estonia voting system source code repository. https://github.com/vvk-ehk
4. Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726c0b
5. Recommendation CM/Rec(2017)5[1] of the Committee of Ministers to member States on standards for e-voting. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680726f6f
6. Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum. http://publiweb104.coe.int/t/dgap/goodgovernance/Activities/GGIS/E-voting/Key_Documents/Default_en.asp
7. Election Observation Handbook: Sixth Edition. OSCE/ODIHR, Warsaw (2010)
8. Final Report of the Election Assessment to Norway. OSCE/ODIHR, Warsaw (2011)
9. Final Report of the Election Assessment Mission to Estonia. OSCE/ODIHR, Warsaw (2013)
10. Handbook for the Observation of New Voting Technologies. OSCE/ODIHR, Warsaw (2013)
11. Final Report of the Election Assessment Mission to Switzerland. OSCE/ODIHR, Warsaw (2015)

12. Adida, B.: Helios: web-based open-audit voting. In: van Oorschot, P.C. (ed.) USENIX Security Symposium, pp. 335–348. USENIX Association (2008)
13. Barrat, J., Bolo, E., Bravo, A., Krimmer, R., Neumann, S., Parreño, A.A., Schürmann, C., Volkamer, M., Wolf, P.: Certification of ICTs in Elections. International IDEA, Stockholm (2015)
14. Bellare, M.: Practice-oriented provable-security. In: Damgård, I.B. (ed.) EEF School 1998. LNCS, vol. 1561, pp. 1–15. Springer, Heidelberg (1999). doi:10.1007/3-540-48969-X_1
15. Bibiloni, P., Escala, A., Morillo, P.: Vote validatability in mix-net-based eVoting. In: Haenni, R., Koenig, R.E., Wikström, D. (eds.) VOTELID 2015. LNCS, vol. 9269, pp. 92–109. Springer, Cham (2015). doi:10.1007/978-3-319-22270-7_6
16. Brightwell, I., Cucurull, J., Galindo, D., Guasch, S.: An overview of the iVote 2015 voting system (2015). https://www.elections.nsw.gov.au/about_us/plans_and_reports/ivote_reports
17. Burton, C., Culnane, C., Schneider, S.: Secure and Verifiable Electronic Voting in Practice: the use of vVote in the Victorian State Election. CoRR abs/1504.07098 (2015). http://arxiv.org/abs/1504.07098
18. The Swiss Federal Chancellery: Federal chancellery ordinance on electronic voting (2013). http://www.bk.admin.ch/themen/pore/evoting/07979
19. Clouser, M., Krimmer, R., Nore, H., Schürmann, C., Wolf, P.: The Use of Open Source Technology in Election Administration. International IDEA, Stockholm (2014)
20. Cramer, R., Gennaro, R., Schoenmakers, B.: A secure and optimally efficient multi-authority election scheme. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 103–118. Springer, Heidelberg (1997). doi:10.1007/3-540-69053-0_9
21. Damgård, I.: On sigma-protocols. http://www.cs.au.dk/ivan/Sigma.pdf
22. Galindo, D., Guasch, S., Puiggalí, J.: 2015 Neuchâtel's cast-as-intended verification mechanism. In: Haenni, R., Koenig, R.E., Wikström, D. (eds.) VOTELID 2015. LNCS, vol. 9269, pp. 3–18. Springer, Cham (2015). doi:10.1007/978-3-319-22270-7_1
23. Gharadaghy, R., Volkamer, M.: Verifiability in electronic voting - explanations for non security experts. In: Krimmer and Grimm [32], pp. 151–162
24. Gjøsteen, K.: Analysis of an internet voting protocol. Cryptology ePrint Archive, Report 2010/380 (2010)
25. Haenni, R., Koenig, R.E., Dubuis, E.: Cast-as-intended verification in electronic elections based on oblivious transfer. In: Krimmer, R., Volkamer, M., Barrat, J., Benaloh, J., Goodman, N., Ryan, P.Y.A., Teague, V. (eds.) E-Vote-ID 2016. LNCS, vol. 10141, pp. 73–91. Springer, Cham (2017). doi:10.1007/978-3-319-52240-1_5
26. Heiberg, S., Martens, T., Vinkel, P., Willemson, J.: Improving the verifiability of the estonian internet voting scheme. In: Krimmer, R., Volkamer, M., Barrat, J., Benaloh, J., Goodman, N., Ryan, P.Y.A., Teague, V. (eds.) E-Vote-ID 2016. LNCS, vol. 10141, pp. 92–107. Springer, Cham (2017). doi:10.1007/978-3-319-52240-1_6
27. Heiberg, S., Parsovs, A., Willemson, J.: Log analysis of Estonian internet voting 2013–2014. In: Haenni, R., Koenig, R.E., Wikström, D. (eds.) VOTELID 2015. LNCS, vol. 9269, pp. 19–34. Springer, Cham (2015). doi:10.1007/978-3-319-22270-7_2
28. Heiberg, S., Willemson, J.: Verifiable internet voting in Estonia. In: 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE 2014), Lochau/Bregenz, 29–31 October 2014. pp. 1–8 (2014). http://dx.doi.org/10.1109/EVOTE.2014.7001135

29. KRD: Specification, tenders, evaluation and contract (2009). https://www.regjeringen.no/en/dep/kmd/prosjekter/e-vote-trial/source-code/specification-tenders-evaluation-and-con/id612121/
30. KRD: evalg2011 system architecture (2011). https://web.archive.org/web/20120309072858/http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project/source-code/the-system-architecture-.html?id=645240
31. KRD: Internet voting pilot to be discontinued - KRD press release (2014). https://www.regjeringen.no/en/aktuelt/Internet-voting-pilot-to-be-discontinued/id764300/
32. Krimmer, R., Grimm, R. (eds.): Electronic Voting 2010 (EVOTE 2010), 4th International Conference, Co-organized by Council of Europe, Gesellschaft für Informatik and E-voting.CC, 21st–24th July 2010, in Castle Hofen, Bregenz, Austria. LNI, vol. 167. GI (2010)
33. Krimmer, R., Triessnig, S., Volkamer, M.: The development of remote E-voting around the world: a review of roads and directions. In: Alkassar, A., Volkamer, M. (eds.) Vote-ID 2007. LNCS, vol. 4896, pp. 1–15. Springer, Heidelberg (2007). doi:10.1007/978-3-540-77493-8_1
34. Kripp, M.J., Volkamer, M., Grimm, R. (eds.): 5th International Conference on Electronic Voting 2012, (EVOTE 2012), Co-organized by the Council of Europe, Gesellschaft für Informatik and E-voting.CC, 11–14 July 2012, Castle Hofen, Bregenz, Austria, LNI, vol. 205. GI (2012)
35. Lenarcic, J.: Opening Address on 16 September 2010 at the OSCE Chairmanship Expert Seminar on the Present State and Prospects of Application of Electronic Voting in the OSCE Participating States, Vienna (2010)
36. Mercury, R.: A better ballot box? IEEE Spectr. **39**, 46–50 (2002)
37. Puigalli, J., Guasch, S.: Cast-as-intended verification in Norway. In: Kripp et al. [34], pp. 49–63
38. Puiggalí, J., Guasch, S.: Universally verifiable efficient re-encryption mixnet. In: Krimmer and Grimm [32], pp. 241–254. http://subs.emis.de/LNI/Proceedings/Proceedings167/article5682.html
39. Saltman, R.G.: Effective Use of Computing Technology in Vote-Tallying. Technical report, NIST (1975)
40. Stenerud, I.S.G., Bull, C.: When reality comes knocking norwegian experiences with verifiable electronic voting. In: Kripp et al. [34], pp. 21–33, http://subs.emis.de/LNI/Proceedings/Proceedings205/article6754.html
41. Swiss Post: Individual Verifiability, Swiss Post Online Voting Protocol Explained. https://www.post.ch/-/media/post/evoting/dokumente/swiss-post-online-voting-protocol-explained.pdf?la=en&vs=3
42. Swiss Post: Swiss Post Online Voting Protocol. https://www.post.ch/-/media/post/evoting/dokumente/swiss-post-online-voting-protocol.pdf?la=en&vs=2
43. Wikström, D.: A sender verifiable mix-net and a new proof of a shuffle. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 273–292. Springer, Heidelberg (2005). doi:10.1007/11593447_15
44. Yin, R.: Case Study Research: Design and Methods. Applied Social Research Methods. Sage Publications, London (2003). https://books.google.es/books?id=BWea_9ZGQMwC