

E-Voting System evaluation based on the Council of Europe recommendations: *n* Votes

David Yeregui Marcos del Blanco¹[0000-0001-7702-6602] David Dueñas-Cid^{2,3} [0000-0002-0451-4514] and Héctor Aláiz Moretón¹

¹ University of Leon, Campus de Vegazana, s/n, 24071 León
dmarch01@estudiantes.unileon.es

² Tallinn University of Technology, Akadeemia tee 3, 12618 Tallinn, Estonia

³ Kozminski University, Jagiellonska 57/59, 03-301 Warsaw, Poland
david.duenas@taltech.ee / dduenas@kozminski.edu.pl

Abstract. E-voting implantation has been facing important challenges in recent years. Several incidents, together with a lack of evaluation methodologies social and cultural customs hinder a broader application. In this work, the authors aim to contribute to a safer introduction of e-voting tools by applying a practical evaluation framework strongly based on the security requirements issued by the Council of Europe (CoE) in 2017 to nvotes, a system that has been utilized to cast over 2 million votes over the last 6 years.

The ultimate goal of the analysis is not to judge from a rigid, “infallible” but to contribute to a gradual and secure implementation of e-voting solutions in the democratic processes. The authors believe it can constitute a useful source of information for election officials, researchers and voters.

Keywords: E-democracy, E-voting, System evaluation, nvotes.

1 Introduction

Since the first implementation of remote electronic voting in the 90s [4], the process of dissemination of internet voting did not meet the initial and promised expectations. Several countries experimented with the possibility of adding internet voting systems to their elections¹, but it just turned into a reality in a reduced number of them: Estonia, Canada, Australia, Switzerland or Norway, amongst others. The Estonian case is the most prominent success story, using Internet Voting uninterruptedly since 2005 in all elections [12] an reaching high levels of acceptance [10] and cost efficiency [6, 7].

The dissemination of internet voting technologies is challenged by a complex set of factors that affect different layers of administration, law, society and technology [11] and that should be achieved in a constant dialogue between themselves: dealing with complexity in electoral management, reforming electoral laws, ensuring transparency,

¹ For a better understanding, see International IDEA’s database on use of ICT in Elections: <https://www.idea.int/data-tools/data/icts-elections> (last accessed 4 June 2020)

neutrality and participation and ensuring secure and risk-free technological apparatus. The latter factor, the security of the system, has been constantly labelled as an important element not only for the correct functioning of the internet voting and its integration in the electoral systems, but also as an element projecting trust in the society where the system is being implemented [5, 8, 9, 13].

Pursuing the same goal, the creation of trust as a key element for the adoption of internet voting systems, the Council of Europe proposes a set of recommendations to guide the process of implementation of electronic remote voting systems [2]. The CM/Rec(2017)5 updates the previous Recommendations from 2004 [1] and integrates lessons learned from previous experiences and developments in the electoral field to create a useful and up-to-date document. Specifically, proposes a set of Principles, Standards and Requirements that every electronic voting system should fulfil for the development of elections and for reinforcing the democratic principles that are the common heritage of its member states [3]: Elections should be Universal, Equal, Free and Secret, should meet a set of regulatory and organizational requirements, should be transparent and allow observation and should be accountable, and should use reliable and secure systems.

On the light of the aforementioned list, this paper presents an analysis on how the system *nVotes* fits on the Council of Europe requirements. The ultimate goal of the authors is not to judge from a rigid *inamovable* or *infallible* point of view for the sake of pin pointing shortcomings, but to establish a comprehensive, multi-faceted evaluation in order to improve the knowledge and security level in the deployment of e-voting systems

2 Related Works

The research work of Bräunlich, Grimm and Richter in 2013 [1] is considered one of the most relevant to date. The authors presented the first interdisciplinary collaboration which has transformed legal requirements into technical criteria. Specifically, they established thirty Technical Design Goals (TDG), using the KORA methodology (*Konkretisierung Rechtlicher Inforderungen, Concretization of Legal Requirements*) [2]. This methodology had been used previously for mobile devices amongst others.

Neumann combined the previous methodology of Bräunlich, Grimm and Richter with the *Common Criteria for IT-Security Evaluation* [3] and established sixteen technical requirements to relate the legal criteria to Bräunlich's TDGs.

While Neumann's work [4] has critically contributed to constructing a very valuable framework, it still had room for improvement, specifically from a practical standpoint:

On the one hand, the security evaluation framework is aimed at schemes rather than entire systems, with the author himself coming across an example of a structural flaw that would not be identified using his evaluation scheme: "*for instance, the Vote Forwarding Server and the Vote Storage Server of the Estonian Internet voting scheme are developed and maintained by the same vendor*" [4, p. 135].

Additionally, the security evaluation assumes that the voters will use the authentication tools sufficiently. Unfortunately, the tendency of the voters is not to verify: for instance, one of the largest electoral e-voting initiatives which took place in New South Wales in 2015, showed that only 1.7% of 283.669 votes were verified [5].

Furthermore, Neumann's framework is based on probabilistic attack strategies (an attacker may be able to make a certain impact or not), through Monte-Carlo simulations [4]. It is an interesting approach indeed, although less useful for a practical evaluation of the e-voting tool. As a result, the author concludes: "we therefore recommend to incorporate the security evaluation framework into a larger decision-support system for elections officials" [4, p. 138].

Following with the above recommendation, a decision-support system proposal was developed by Marcos, et al. to present a decision-support system as a practical evaluation framework [6]. It is in accordance with the guidelines from the 2017 Council of Europe's ("*Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*"), drawn up by the Directorate General of Democracy and Political Affairs [7] and deals with the five key principles of a democratic election (universal, free, equal, direct and secret) detailed in the same document.

3 Evaluation Methodology

As previously stated, Bräunlich, Grimm and Richter greatly contributed to the evaluation of e-voting systems against legal provisions by setting out the first draft of technical design proposals (TDGs) by refining the election principles.

Consequently, Neumann [4] identified the imperfections of Bräunlich's approach and set out a series of technical requirements to bracket the legal criteria with the TDGs.

While Neumann's work set out an irrefutable improvement, it constitutes a scheme evaluation tool with probabilistic proofs as its core with Monte-Carlo simulations rather than a practical evaluation framework tool for election officials and other stakeholders involved in the democratic processes.

In 2018, Panizo et al. proposed an extended evaluation approach in the context of the Spanish Constitution [8] and the Council of Europe's latest e-voting recommendations [7]. Their proposed methodology [9] involved the following steps:

1. Defining an homogeneous series of e-voting requirements with: the KORA methodology [2] as its basis, together with the CC and ISO 27001-IT Grundschutz guideline [3], their assimilation by Simic-Draws et al. [10], the Guidelines of the Council of Europe [7] and Neumann's methodology [4].
2. Formal conformity between point 1 and Bräunlich's TDG's [1], as in Figure 1 below.
3. Consultation with more than 30 international experts in e-voting (Research and Industry Experts or RIE, selected using the snowball [11] and judgement [12] sampling methodologies) to review the evaluation framework and add weighting factors.
4. Formal definition of the practical evaluation framework, including two sine-qua-non requirements (E2Ev and Coercion Resistance) and 41 evaluation items.

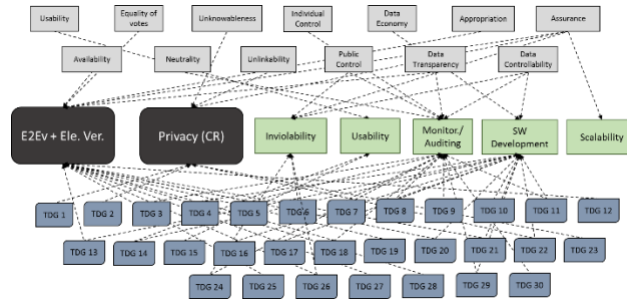


Fig. 1. Integration of Panizo [9] and Bräunlich [1]

The work in [6] established for the first time a correlation between the end to end verifiability (E2Ev) and coercion resistance (CR) to the legal requirements for a democratic process and the Council of Europe: “The five key principles of electoral law are: universal, equal, free, direct and secret suffrage and they are at the root of democracy” (article 68 of the Spanish Constitution [8]).

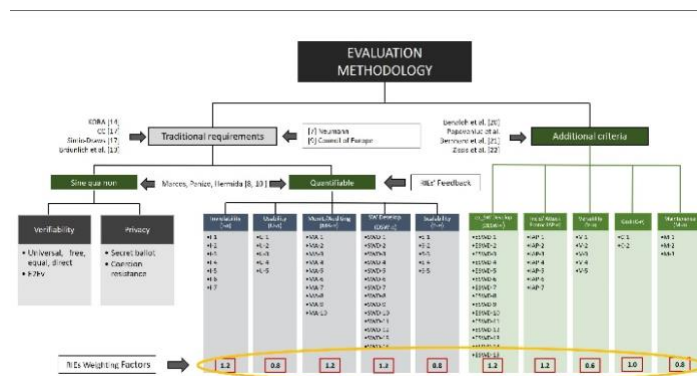
Specifically, Marcos et al. Set out the equivalence of the aforementioned five key principles, into a formal authentication of the E2Ev the universal, free, equal and direct properties and its coercion resistance for the secrecy prerequisite.

The methodology presented to this point is solid from a legal point of view but still lacks the technical and practical approach necessary for a complete evaluation.

In order to solve the shortcomings, five practical requisites were introduced, partially based on the research by Benaloh, Rivest, Ryan and Volkamer [13], [14]. Subsequently, the requisites were codified, refined and subdivided into 73 specific items by means of a partial application of Zissis and Lekkas [15] and New Zealand’s Department of Internal Affairs’s Communication on e-voting [16] ².

As a final step, e-voting RIEs from Canada, France, Norway, Switzerland, Germany and Spain among other countries were consulted again, with the purpose to assign a weighting score to each requisite.

The following Figure 2 visually represents the complete evaluation methodology:



² For a complete explanation of the previous process, please refer to the original work in [6], [8].

Fig. 2. Complete evaluation framework [6]

The sine-qua-non requirements (end-to-end verifiability and coercion resistance, representing the five compulsory principles of a democratic election), which evaluation is not a numerical value related to performance but instead in terms of “holds” (\circ) or “does not hold” (\times). There is a third possibility, when the property “stands under determined, credible assumptions” (Δ).

The second quantifiable and additional criteria, totaling 10 requirements, are evaluated from 0 to 10. In order to obtain the numerical evaluation for each criterion, the corresponding measurable sub-items are evaluated with three possible outcomes: non-compliant (\times), partially compliant (Δ) and compliant (\circ).

The explanation of the evaluation framework design, implementation and constituent requirements and items has been simplified because of page extension constraints. For a full version, the reader can refer to the original PhD thesis [17].

It is relevant to mention that this practical evaluation methodology has previously been applied to Helios Voting and published by the IEEE [9].

4 nVotes Analysis

4.1 Introduction

nVotes [18] is a remote e-voting system developed by the Spanish company Agora Voting SL in 2014. Its roots trace back to 2009 and the Internet Party, although the developing team has since then dropped any political affiliation and nVotes is currently an apolitical project. The key members are Lucas Cervera as CEO, Eduardo Robles as CTO and David Ruescas as Head of R&D.

Until 2017, nVotes was known as Agora Voting and under such moniker it was one of the 18 European start-ups to be accepted in the Impact Accelerator project, and awarded with 100,000 EUR [19].

According to their website, nVotes has been used to cast over 2 million votes for over 150 clients, including Public Administrations like the Barcelona Provincial Council, Madrid City Council; Political Parties like Podemos, Ahora Madrid and Barcelona en Comú, as well as Education Institutions like UNED University in Spain in processes up to 150,000 voters.

4.2 Main characteristics

As previously mentioned, the methodology presented in Section 3 has been already applied to other relevant e-voting tools, including Helios Voting [9] or iVote by Scytl [20]; in both cases with numerous bibliography and research resources available:

- Helios Voting is a very well-known open source e-voting system [21], which has been used as blueprint for several variations and improvements such as Helios KTV [22] or Belenios [23].

- Scytl is probably the most widely used e-voting system at a global level, including numerous legally-binding elections and pilots for a total of over 100,000 processes managed and more than 200 employees. The information available ranges from research papers to Government reports and corporate presentations.

In the case of nVotes, the available bibliography is much more limited due to the fact that they are neither a research standard tool, nor a global company. In order to complement the publicly available information, the authors of this document got in touch with nVotes and they key people have always been open and supporting in providing all the available information and answers to the questions raised.

Additionally, the authors were provided with two documents named “*Technical Overview*” and “*Client Action Protocol*”, which have been extremely useful for conducting the analysis. They are at the reader’s disposal upon request to the authors since they have not been published before.

nVotes scheme components and cryptographic primitives. According to the information included in the “*Technical Overview*” and complemented with a Q/A with nVotes technical team, the key elements are:

- **Registry:** Comprised basically of the registration database programmed in Python. It includes the SMS service platform Esendex [24], server certificate with TLS support, Cloudflare [25] and Fail2ban [26] for protection against DDoS attacks and hardware redundancy 1+1.
- **Virtual Polling Station:** TLS server validation, *cast-or-audit* voting javascript (similar to that of Helios Voting [21]), random number generator (not specified), HMAC client authentication, Election Manager with Scala REST API, Postgresql database and similar to the Registry case, Cloudflare and Fail2ban DDoS protection.
- **Electoral Authority:** HTTP distributed queue, TLS client/server authentication, mixnet library *Verificatum* [27] and tabulation library OpenSTV [28].
- **Election Verificator:** a Python/Java

With regards to the main cryptographic primitives, they are the following:

- El Gamal Homomorphic Encryption [29]
- Pedersen Threshold Distributed Key Generator [30]
- *Verificatum* verifiable mixnet [27]
- Fiat-Shamir heuristic to convert Zero Knowledge Proofs into Non-Interactive Zero Knowledge Proofs [31]
- Schnorr Signature [32] to make the ElGamal Encryption IND-CCA2.

nVotes voting sequence. As presented in the “*Technical Review*” and “*Client Action Protocol*” documents, the voting procedure is as follows:

1. Authorities distributedly generate the Election’s Public Key with Pedersen [30].

2. Eve (voter) access the Registry site and provides the required personal information, including a security code which has been sent independently by SMS
3. The Registry system compares the information provided with the census. If it is correct, Eve is forwarded to the Virtual Polling Station.
4. Eve fills her vote, encrypts it and sends it. Alternatively, she can audit it but in such case, the cast vote is no longer valid and will not be tallied. This *cast-or-audit* approach is also implemented in Helios Voting [21].
5. Once the vote casting period ends, the authorities jointly proceed with the mix and decryption of the ballots
6. The decrypted votes are tallied
7. The election results are published, together with the tally results, the vote's ciphertexts as well as the mixnet and decryption Zero Knowledge Proofs.
8. Voters and third parties can download and execute the election verifactor

Once nVotes has been introduced, together with its associated scheme components, cryptographic primitives and voting process, the practical evaluation methodology for e-voting systems [6] can be applied.

The analysis is intended to be a sort of a guideline, which introduces strengths and potential weaknesses in order to establish a safe range of utilization and to offer directions as to how to improve the voting system.

4.3 End to End Verifiability

Unfortunately, there is no formal, universal definition for end-to-end verifiability (E2Ev). Additionally, symbolic analysis of security protocols still find associative and commutative operators are out of reach. It is then not possible to analyze a homomorphic property [33] such as:

$$\text{enc}(\text{pk}; v_1) * \text{enc}(\text{pk}; v_2) = \text{enc}(\text{pk}; v_1 + v_2) \quad (1)$$

and therefore, a case by case analysis has to be conducted for each system.

Currently, probably the most widely accepted definition of E2Ev is the one by Benaloh et al. in [13] and is comprised of the properties: "Cast as intended", "Recorded as cast" and "Tallied as recorded"

For the first and second items, nVotes presents a similar approach to that of Helios Voting: the voter can audit her vote until she is convinced that it is trustable and once cast, she receives a hash of the encrypted, which she can check on public bulletin board. Finally, for the tallied as recorded condition, ElGamal (also present in Helios Voting) together with *Verificatum* mixnet [27] and Schnorr [32] are implemented.

So regarding the question of nVotes being E2Ev or not and similar to the analysis in [8] for Helios Voting giving the similarities, it can be considered end to end verifiable assuming certain preconditions:

- The cast and audit mechanism is used by a large enough number of voters so that ballot alteration will not go unnoticed.
- The Election Authorities and the Bulletin Board (BB) are honest
- An attack which gains control of the Registry/Ballot is detected.



For the first precondition, Acemyan in [34] and the New South Wales case [5] have shown that voters' ballot verification percentage is quite low and they should not be responsible of part of the security of an e-voting system.

In relation to the other two prerequisites, in a perfect scenario nVotes would comply with both of them but in real elections, both the Election Authorities and/or the BB can illegally introduce votes in what is known as "ballot stuffing". For public, legally binding elections, that is something no to be taken lightly.

To sum up, if nVotes use is limited to elections with a low risk of corruption such as student government bodies, local clubs, online groups, and other education-related organizations, the pre-assumptions could be acceptable. For other, more demanding types of elections, E2Ev cannot be asserted.

Evaluation: Δ . E2Ev holds if the preconditions set in nVotes' *Technical Overview* document are accepted and its use is limited to low corruption risk elections.

4.4 Coercion Resistance

Assuming probably the most accepted definition of privacy levels by Juels et al. [35] and the proof by Hirt and Sako [36] that receipt-freeness is not enough for preserving it in electronic elections, the level to reach is Coercion Resistance. It implies that a voter cannot provide to an attacker any proof of her vote or even whether she voted or not, even if she is willing to cooperate.

As for nVotes, the voter receives a verification code after casting the ballot, therefore she can prove it to a potential attacker.

Additionally, the Election Administrator of an Election can verify whether a specific person in the census has voted or not, which clearly compromises the privacy.

Evaluation: X . Does not hold.

4.5 Inviolability (I-n)

nVotes' *Technical Overview* document includes an integrity, privacy and availability analysis. The authors acknowledge the possibility of "ballot stuffing" if the Election Administrators are corrupt and of DDoS attacks despite implementing specific tools [25], [26].

There have also been questions raised about the census integrity used in consultative referenda [37], [38] and the separation between the tally administrator and the census administrator, which can be the same person and thus lead to potential collusions (I-4).

Safe authentication protocols, tracking tools, Risk Assessment and modularity principles are partially compliant, with room for improvement.

Table 1. Inviolability in nVotes

I-n	Definition	Val
-----	------------	-----



I-1	Software and auxiliary system's protection w/ safe authentication protocols. Access via third-parties/vulnerable-servers not permitted.	Δ
I-2	Action protocols in the event of compromised inviolability.	X
I-3	Tracking tools and offline backup copies available.	Δ
I-4	Distributed control in the critical nodes with division of responsibilities to minimize collusion risks.	X
I-5	Existence of <i>Risk Assessment</i> and <i>Threat Modelling</i> protocols.	Δ
I-6	Modularity principles to confine potential attacks and coding bugs.	Δ
I-7	Proper updating of items I-1...I-6	Δ

Evaluation: 4/10 points. The inviolability policy presents certain vulnerabilities which, in the case of a private election, while being very serious, are ultimately up to the organizer's criteria whether to take the risk or not. For legally binding public elections, they are not acceptable and nVotes inviolability should be improved before being used in such environment.

4.6 Usability (U-n)

nVotes presents a satisfactory performance in terms of simplicity and clarity in the voting process (U-1, U-3) as well as in intuitiveness and lexicon choice both for the voter and the administrators.

Concerning the aspects to be improved, there is no version adapted to collectives with special needs, the SMS authentication might prove challenging for the elders and the verification codes are too long and "imposing" voters with no technical background. An intermediate usability layer might be advisable.

Overall, usability is satisfactory while it could be enhance with some simple, easy to implement changes.

Table 2. Usability in nVotes

U-n	Definition	Val
U-1	Simplicity in the authentication, voting and verification	O
U-2	Special attention to vulnerable groups pursuant to the Council of Europe and the United Nations' resolutions on the matter.	X
U-3	Transparency & clarity communicating the voter that the voting process has successfully ended/vote has been received.	O
U-4	Privacy and integrity preference over usability in a compromise.	X
U-5	Intuitive/user-friendly admin interface for setup and management.	O

Evaluation: 6/10 points

4.7 Monitoring/Auditing (MA-n)

This aspect is especially relevant for nVotes due to the possibility of *Ballot Stuffing* attacks through Registry and Eligibility if the Administrators are corrupt or collide or DDoS hostile actions.

Probably due to the nature and scope of the elections managed, the Monitoring and Auditing Protocol is based on Administrators training. According to the key team

members of nVotes, they are currently developing a unified protocol including all the auditing-related activities.

Until it is available, nVotes generates retrievable logs, and provides reasonable amounts of information and data in an easily understandable format. Even so, at this point the Monitoring/Auditing Protocol is still largely to be developed and implemented; therefore not satisfactory.

Table 3. Monitoring/Auditing in nVotes

MA-n	Definition	Val
MA-1	External, independent and distributed.	X
MA-2	MA protocol from the design phase, to assure a correct development throughout the whole lifecycle of the project.	X
MA-3	<i>Specific control on Risk Assess and Thread Modelling strategies.</i>	X
MA-4	Generation of periodical, tamper-proof, indelible logs; stored offline in premises guarded by different personnel from other critical nodes.	Δ
MA-5	Implementation from census collecting to post-electoral maintenance.	Δ
MA-6	Well-documented, detailed information in the appropriate format.	Δ
MA-7	Existence of a test bench to verify that the system is working correctly.	X
MA-8	The members of the monitoring/auditing team must be independent from the rest of authorities/administrators involved.	X
MA-9	Auditing protocol for previous attacks and the MA protocol itself.	X
MA-10	In the event of a successful attack, the system will give total priority to the vote/voter's privacy, even calling off the elections.	X

Evaluation: 3/10 points

4.8 Software Development (SWD-n)

nVotes displays an overall solid Software Development (partly because of its open source approach), with a satisfactory performance in usual software engineering practices (SWD-1), FAQ (SWD-4), impartiality (SWD-5), ballot cast termination (SWD-8), compatibility (SWD-9), third party access (SWD-10), and protocolized application (SWD-13).

Regarding the distributed approach (SWD-2), it has been correctly implemented for key generation and encryption/decryption but there is no separation between the census and the bulletin board. If the same person is responsible for both of them, there is an important risk of collusion.

Finally, the primitives are well implemented but some of them have been already been proven flawed and should be reviewed (SWD-11). Additionally, more frequent updates would be preferable (SWD-14).

Table 4. Software Development in nVotes

SWD-n	Definition	Val
SWD-1	Usual software engineering requirements in terms of design, implementation and documentation.	O

SWD-2	Distributed approach on critical operations. No authority should have attributions to single-handedly modify critical parameters.	Δ
SWD-3	User-friendly approach. User's guide and administrator's guide well documented and available well in advance.	Δ
SWD-4	Secure and accessible website, with a well-documented FAQ.	O
SWD-5	The voting options must be presented in a totally objective and unbiased way, showing no preference whatsoever.	O
SWD-6	System must not provide the voter with evidence to proof her vote.	X
SWD-7	The system must guarantee the voter's privacy throughout the whole voting process, not being possible to rebuild the vote/voter link.	Δ
SWD-8	The voting process must offer the possibility to be terminated at any time, not saving any information compromising the voter's privacy.	O
SWD-9	SW to be tested in every platform, operational system and browser with a market share $\geq 1\%$.	O
SWD-10	Software must neither allow for third-party access (incl. social media) nor include links to programs/sites outside the e-voting infrastructure.	O
SWD-11	The cryptographic primitives shall be tested in advance under conditions more demanding than the ones expected during the elections in order to avoid breakdowns and foresee shortages.	Δ
SWD-12	Access to the source code by independent experts to reinforce security. The code developer can demand an NDA to protect its IP.	Δ
SWD-13	Use of protocolized systems/open standards to improve interoperability.	O
SWD-14	Update policy, against new e-voting attacks as they are discovered.	X

Evaluation: 7/10 points

4.9 Scalability (S-n)

nVotes has managed elections up to 150,000 votes in consultative referenda of political parties, although they didn't managed many of the ex_software activities, which were handled by the Party itself.

So far, the system has proved to be scalable to the amount of votes already managed in private elections. The shortcomings related to monitoring, ex-software development and potential collusion request a further in-depth improvement before being considered for introduction in public binding elections.

Table 5. Scalability in nVotes

S-n	Definition	Val
S-1	Maximum capacity tests both from a SW and a HW standpoint in environments more demanding than the elections to be managed.	Δ
S-2	Ad-hoc performance tests for the most critical operations (authentication, encryption/decryption, cryptographic primitives, tallying ...).	X
S-3	Existence of test benches more demanding than the actual elections.	X
S-4	Clear indicators and metrics on the max manageable size and complexity from a SW (cryptographic capabilities, number of voters) and ex_SW (infrastructure, costs, logistics, second channels etc.) standpoints.	Δ
S-5	Clear definition of election which can be adequately handled by the <i>e-voting</i> system (from consultative referenda to politically binding elections).	Δ

Evaluation: 5.5/10 points



4.10 Ex-Software Development (ESWD-n)

Ex_Software development is intimately related to the increased complexity of public binding elections. The lower the score in this category, the less recommended it is for the analyzed e-voting system to be implemented for such type of elections.

In the case of nVotes, it has been deployed only for private elections and referenda, and therefore has not implemented ESWD1-4, ESWD6-7, and ESWD-10.

The aspects in which the development is satisfactory are: authentication by alternative channels (ESWD-11) and the master initialization protocol (ESWD-12).

As for the communication/problem solving/back up policy (ESWD5, 6, 8, 9, 14, 15), nVotes stated that they offer different levels of services according to the needs and budget of each election. They can even let the client handle most of the activities related to back-up protocols, responsibilities attributions etc.

While that could make sense from a business perspective, the security implications in case of a misuse or a scandal, and the potential impact in the reputation of nVotes, advice against allowing the election organizer to handle such sensitive actions.

Table 6. Ex_Software Development in nVotes

ESWD-n	Definition	Val
ESWD-1	Design, development & update of SWD/ESWD protocols in parallel.	N/A
ESWD-2	Safe protocol for credential, permission & responsib. distribution.	N/A
ESWD-3	Automated access control and infrastructure surveillance.	N/A
ESWD-4	Auditing and independent observers' protocol.	X
ESWD-5	Distributed <i>back-up</i> protocol.	Δ
ESWD-6	Distribution of attributions and responsibilities throughout the whole ex_sw development to minimize collusion risks.	X
ESWD-7	Availability of complementary, non e-voting systems.	X
ESWD-8	Voters must be informed about the e-voting process in advance, through websites, telephone, information stands...	Δ
ESWD-9	If re-voting is permitted, provide a reinforced information campaign to explain the prevalence of paper ballot.	Δ
ESWD-10	Organize opinion polls on selected cohorts to gather reliable feedback on usability, tendencies and improvements.	X
ESWD-11	Authentication of credential submission by alternative channels.	O
ESWD-12	Master initialization protocol to be executed right before the start of the e-voting period to verify the correct operation/readiness.	O
ESWD-13	Implementation, to the extent possible, of protocolized and standardized systems to improve interoperability.	Δ
ESWD-14	Free assistance phone service available before/during the election.	
ESWD-15	Complete PR strategy to promote e-voting and train voters, including: webinars, stands, demos, open days etc.	Δ

Evaluation: 4/10 points

4.11 Incidents and Attacks Protocol (IAP-n)

Elections imply a power transfer from the voters to the elected representatives.

The bigger the election or its reach, the more attention they conceal, also from potential attackers. Hence the critical importance of a protocol to prevent and avoid attacks and in case they occur, to isolate and mitigate the pernicious effects.

Due to the track record of elections managed by nVotes, they do not have a proper such protocol in place, presenting only partial compliance in distributed/modular approach and actions taken towards limiting the risk of an attack with the introduction of Cloudflare [25] and Fail2Ban services[26].

In conclusion, nVotes needs to develop a proper Incidents and Attacks Protocol before being used for legally binding, public elections.

Table 7. Incidents and Attacks protocol in nVotes

IAP-n	Definition	Val
IAP-1	Risk Assessment (RA), Privacy Impact Assessment (PIAS), Penetration Testing (PT), Control Validation Plan (CVP) and Control Validation Audit (CVA) protocols.	Δ
IAP-2	Specific prevention protocols for each cryptographic scheme.	X
IAP-3	All the information shall be kept to the extent possible in the country's National soil.	O
IAP-4	Implementation of protocols and reinforcement operations to minimize the risk of permanent losses of information.	Δ
IAP-5	Reinforced distributed approach to contribute to the absence of critical nodes which undermine the e-voting system's viability.	Δ
IAP-6	Training and awareness campaigns to minimize the risk of voter-driven attacks (<i>phishing</i> , social engineering, etc.).	X
IAP-7	Hackers/indep. experts to test and compromise the system beforehand.	X

Evaluation: 4/10 points

4.12 Versatility (V-n)

nVotes can be used by the voter with a standard internet connection, hardware and Operative System. While it works in most of the available browsers and devices, there is no compatibility study available.

Regarding the existence of different versions depending on the type of election (yes/no, 1/N, N/M, order etc.) there are no adapted versions but according to the data in *Verificatum* [27], its performance is satisfactory enough to not require adapted versions. The authors believe that such statement is only partially true and largely depends on the range of the election.

Finally, the score against the WCAG 2.0 standard was good but not brilliant (A).

Table 8. Versatility in nVotes

V-n	Definition	Val
V-1	Versions adapted to different election typologies (yes/no, 1/N...).	Δ
V-2	Specific solutions for vulnerable groups (disabilities, illiterates etc.).	X
V-3	The voter shall be able to vote using her personal device, through a standard internet connection without installing any additional SW.	O
V-4	E-voting system tested in browsers/devices w/ a market share $\geq 1\%$.	Δ
V-5	The interface is WCAG 2.0 AA compliant.	Δ



Evaluation: 5/10 points**4.13 Cost (C-n)**

Cost is a sensitive issue for e-voting systems. Most of them are not transparent in their pricing policy. That is understandable to a certain point, but even the cheapest option should offer a sufficient security level.

nVotes used to have a very clear, direct policy with 3 plans with a fixed cost of 0.2 EUR per voter plus other associated costs. In its simplest version, it was possible to organize a 1,000 voter election with all the required elements for a little over 1,000 EUR. Currently, the policy has changed and there is no clear indication of the cost for the organization of an election.

While probably still an affordable option, the authors believe that the previous, more transparent approach was better from a user's point of view.

Table 9. Cost in nVotes

C-n	Definition	Val
C-1	Transparency and clarity in the cost breakdown.	
C-2	System cost related to quality and performance. Comparison with other e-voting solutions.	

Evaluation: Review (6/10 points)**4.14 Maintenance (M-n)**

Both from a software and ex-software perspective. On the software side, nVotes is an open source project and therefore very open and verifiable. It is regularly updated. Regarding the ex_software aspect, there is not much improvement and it would be very advisable in order to extend the safe utilization range of the system.

As for everlasting privacy and post-quantum security, nVotes team is working on it but there is no expected imminent announcement.

Finally, the maintenance cost is quite limited and performed internally.

Table 20. Maintenance in nVotes

M-n	Definition	Val
M-1	Covering both SW and ex_SW aspects. Frequency, thoroughness and existence of security logs to check the maintenance process are also evaluated.	Δ
M-2	Maintenance as <i>everlasting privacy</i> .	N/A
M-3	Maintenance cost itself.	Δ

Evaluation: 6.5/10 points

5 Final Results and Conclusion

nVotes [18] is a remote e-voting system developed by the Spanish company Agora Voting SL and active since 2014. It has managed a total of 2 million votes with up to 150.000 votes in the same election.

In order to complement the relatively limited publicly available information for the analysis in this article, they have been diligent and helpful and the authors with like to extend their gratitude for their availability.

The ultimate goal of the analysis is not to judge from a rigid, “infallible” perspective for the sake but to try contribute to a gradual and secure implementation of e-voting solutions in the democratic processes.

The formula and table below summarize the findings and scores of nVotes:

$$\sum_{i=1}^n \frac{f_i \cdot w_1 + \dots + f_n \cdot w_n}{n} \cdot \frac{n}{t} = \sum_{i=1}^n \frac{f_i \cdot w_1 + \dots + f_n \cdot w_n}{t} \quad (2)$$

Table 31. Practical Evaluation Methodology [6] applied to nVotes

Requirement	Code	Weight	nVotes
<i>E2Ev</i>	E2Ev	N.A.	Δ
<i>Coerc. Resistance</i>	CR	N.A.	X
<i>Inviolability</i>	(I-n)	1.2	4 * 1.2 = 4.8
<i>Usability</i>	(U-n)	0.8	6 * 0.8 = 4.8
<i>Monitoring/Audit</i>	(MA-n)	1.2	3 * 1.2 = 3.6
<i>Software Devel.</i>	(SWD-n)	1.2	7 * 1.2 = 8.4
<i>Scalability</i>	(S-n)	0.8	5.5 * 0.8 = 4.4
<i>Ex_Soft. Develop.</i>	(ESWD-n)	1.2	4 * 1.2 = 4.8
<i>Incid./AttackProt.</i>	(IAP-n)	1.2	4 * 1.2 = 4.8
<i>Versatility</i>	(V-n)	0.6	5 * 0.6 = 3
<i>Cost</i>	(C-n)	1.0	7 * 1.0 = 7
<i>Maintenance</i>	(M-n)	0.8	6.5 * 0.8 = 5.2
TOTAL		10	50.8

Due to the nature of the elections in which nVotes has been deployed, it is in an intermediate position between Helios Voting and Scytl’s iVote systems. nVotes can manage elections with a number of voters that Helios Voting has not been able to proof so far but it presents undeniable shortcomings when it comes to legally binding elections, where a strong infrastructure, ex-software policies and monitoring/auditing protocols are a must.

Therefore, currently nVotes’ safe range of use is that of private elections.

Concerning the areas in which nVotes present a better performance, those are:

- Open source approach, with good software engineering and possibility of review by researchers/academia
- Intuitive, simple and user-friendly interface for both the voter and the administrators.
- Compatibility
- Open standards, modularity

- Support service during the elections

As for the aspects which should be improved:

- No proper Audit/Monitoring or Incidents/Attacks protocols in place
- Policy for credential, access and permit distribution. Currently allows for collusion to happen between the census administrator and the election administrator
- Ex_software development
- Certain cryptographic primitives implemented are vulnerable [31]
- No version for voters with special needs

Additionally, the election administrator can know whether a voter has voted or not and a voter with a fake ID might be able to authenticate to vote. Even for private elections, it should be an issue to be solved.

In short and considering all the points reviewed in the analysis, the authors estimate that nVotes is currently not ready to be introduced for public, politically binding elections due to the limitations in auditing, monitoring, backup and potential collusion. Its current secure range is that of private elections, always taking into account the highly recommended distribution of administrative roles.

The authors hope that this article can contribute, even if modestly, to improve the knowledge and security level in the deployment of e-voting systems, through the comprehensive, multi-faceted evaluation presented.

Acknowledgement. The contribution of Dr. David Dueñas-Cid is based upon work supported by the Estonian Research Council grant (PUT 1361 “Internet Voting as Additional Channel for Legally Binding Elections: Challenges to Voting Processes Reengineering”, 2017–2020); and by the Polish National Research Center grant (Miniatura 3 - 2019/03/X/HS6/01688 “Zaufanie do technologii w e-administracji: Powtórna analiza nieudanego wdrożenia elektronicznych maszyn do głosowania w Holandii (2006-07)”)

References

1. Vinkel, P., Krimmer, R.: The how and why to internet voting an attempt to explain e-estonia. In: Krimmer, R., et al. (eds.) E-Vote-ID 2016. LNCS, vol. 10141, pp. 178–191. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-52240-1_11
2. Solvak, M., Vassil, K.: Could internet voting halt declining electoral turnout? new evidence that e-voting is habit forming. *Policy Internet* 10(1), 4–21 (2018)
3. Krimmer, R., Duenas-Cid, D., Krivososova, I., Vinkel, P., Koitmae, A.: How much does an e-vote cost? Cost comparison per vote in multichannel elections in estonia. In: Krimmer, R., et al. (eds.) E-Vote-ID 2018. LNCS, vol. 11143, pp. 117–131. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-00419-4_8
4. Krimmer, R. et al.: New methodology for calculating cost-efficiency of different ways of voting: is internet voting cheaper? *Public Money Manage.* 1–10 (2020)

5. Trechsel, A.H., et al.: Potential and Challenges of E-Voting in the EU Study. Bruss (2016)
6. Gjøsteen, K.: Analysis of an internet voting protocol. *IACRCryptol. ePrintArch.* 1–16 (2010). https://doi.org/10.1007/978-3-642-32747-6_1
7. Kulyk, O., et al.: Electronic voting with fully distributed trust and maximized flexibility regarding ballot design. In: *EVOTE 2014*. pp. 139–149. TUT Press, Bregenz (2014)
8. Oostveen, A.-M., Van den Besselaar, P.: Security as belief user's perceptions on the security of electronic voting systems. *Electron. Voting Eur. Technol.* 47, 73–82 (2004)
9. Council of Europe: Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting (2017)
10. Driza Maurer, A.: Updated European standards for e-voting. In: Krimmer, R., Volkamer, M., Braun Binder, N., Kersting, N., Pereira, O., Schürmann, C. (eds.) *E-Vote-ID 2017*. LNCS, vol. 10615, pp. 146–162. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-68687-5_9
11. Bräunlich, K., Grimm, R., Richter, P.: Sichere Internetwahlen Ein rechtswissenschaftlichinformatisches Modell. *Nomos* (2013)
12. Hammer, V., Pordesch, U.: KORA (Konkretisierung Rechtlicher Inforderungen). *Betriebliche Telefon und ISDN-Anlagen rechtsgemäss gestaltet* (1993)
13. Common Criteria for Information Technology Security Evaluation Part 1 : Introduction and general model July 2009 Revision 3 Final Foreword. Nist, vol. 49, 93, July 2009
14. Neumann, S.R.: Evaluation and Improvement of Internet Voting Schemes Based on Legally-Founded Security Requirements. Technische Universität Darmstadt (2016)
15. Electoral Commission New South Wales. <http://www.elections.nsw.gov.au/voting/ivote>. Accessed 12 May 2020
16. Marcos del Blanco, D.Y., Panizo Alonso, L., Hermida Alonso, J.A.: The need for Harmonization in the online voting field: towards an European Standard for democracy. In: *E-Vote-ID 2016*, Bregenz, Austria, 18-21 October 2016, Proceedings, pp. 339–340 (2016)
17. Standards: Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting. 1289 th Meet., 14 June 2017 2. 3 Ad hoc Comm. Expert. Leg., Oper. Tech. Stand. e- voting (CAHVE), June, pp. 1–19 (2017)
18. Constitución Española, pp. 101931–101941. <https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf>. Accessed 12 May 2020
19. Panizo Alonso, L., Gasco, M., Marcos del Blanco, D.Y., Hermida Alonso, J.A., Alaiz Moreton, H.: E-voting system evaluation based on the Council of Europe recommendations: Helios Voting. *IEEE Trans. Emerg. Top. Comput.* (2018)
20. Simić-Draws, D., et al.: Holistic and law compatible IT security evaluation: integration of common criteria, ISO 27001/IT- and KORA. *Int. J. Inf. Secur. Priv.* 7, 16–35 (2013)
21. Goodman, L.: Snowball sampling. *Ann. Math. Stat.* 32, 148–170 (1961)
22. Kish, L.: *Sample Design in Business Research*. American Statistical Association, Ltd E-Voting System Evaluation Based on the Council of Europe Recommendations 165
23. Benaloh, J.D.C., Rivest, R., Ryan, et al.: End-to-end verifiability. *arXiv e-prints* (2014)
24. Bernhard, D., Neumann, S., Volkamer, M.: Towards a practical cryptographic voting scheme based on malleable proofs. In: Heather, J., Schneider, S., Teague, V.

- (eds.) Vote-ID 2013. LNCS, vol. 7985, pp. 176–192. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39185-9_11
25. Zissis, D., Lekkas, D.: Design, Development, and Use of Secure Electronic Voting Systems (2014). <http://services.iglobal.com/resolvedoi/resolve.aspx?>
26. Taiwhenua, T.T.: The Department of Internal Affairs - Online voting. <https://www.dia.govt.nz/online-voting>. Accessed 12 May 2020
27. Marcos del Blanco, D.Y.: Cybersecurity applied to e-democracy: cryptographic analysis and development of a practical evaluation methodology for remote electronic voting systems and its application to the most relevant solutions. University of Leon (2018). http://riasc.unileon.es/archivos/documentos/tesis/Tesis_David_Y_Marcos.pdf
28. nVotes. <https://nvotes.com/>. Accessed 14 May 2020
29. Impact Accelerator. <https://www.impact-accelerator.com/>. Accessed 14 May 2020
30. Marcos del Blanco, D.Y., Gascó, M.: A protocolized, comparative study of helios voting and Scytl/iVote. In: International Conference on eDemocracy & eGovernment (ICEDEG), pp. 31–38 IEEE (2019)
31. Adida, B.: Helios: web-based open-audit voting. In: Proceedings of the 17th Conference on Security Symposium, pp. 335–348. USENIX Association, Berkeley (2008)
32. Kulyk, O., Teague, V., Volkamer, M.: Extending helios towards private eligibility verifiability. In: Haenni, R., Koenig, R., Wikström, D. (eds.) VOTELID 2015. LNCS, vol. 9269, pp. 57–73. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-22270-7_4
33. Cortier, V., Gaudry, P., Glondu, S.: Belenios: a simple private and verifiable electronic voting system. In: Foundations of Security, Protocols, and Equational Reasoning, pp. 214–238 (2019)
34. Esendex. <https://www.esendex.es/>. Accessed 14 May 2020
35. Cloudflare. <https://www.cloudflare.com>. Accessed 15 May 2020
36. Fail2ban. <https://www.fail2ban.org>. Accessed 14 May 2020
37. Verificatum. <https://www.verificatum.org/>. Accessed 14 May 2020
38. Open STV. <https://www.opavote.com/?openstv=1>. Accessed 14 May 2020
39. ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 10–18. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7_2
40. Pedersen, T.P.: A threshold cryptosystem without a trusted party. In: Davies, D., W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 522–526. Springer, Heidelberg (1991). https://doi.org/10.1007/3-540-46416-6_47
41. Fiat, A., Shamir, A.: How to prove yourself: practical solutions to identification and signature problems. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (1987). https://doi.org/10.1007/3-540-47721-7_12
42. Schnorr, C.P.: Efficient identification and signatures for smart cards. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 239–252. Springer, New York (1990). https://doi.org/10.1007/0-387-34805-0_22
43. Cortier, V.: Formal verification of e-voting: solutions and challenges. ACM SIGLOG News 2(1), 25–34 (2015)
44. Acemyan, C.Z., Kortum, P., et al.: From error to error: why voters could not cast a ballot and verify their vote with Helios, Pret a Voter and Scantegrity II. Usenix J. Elect. Technol. Syst. (2015)
45. Juels, A., Catalano, D., Jakobsson, M.: Coercion-resistant electronic elections. In: Chaum, D., Jakobsson, M., Rivest, R.L., Ryan, P.Y.A., Benaloh, J.,



- Kutyłowski, M., Adida, B. (eds.) Towards Trustworthy Elections. LNCS, vol. 6000, pp. 37–63. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-12980-3_2
46. Hirt, M., Sako, K.: Efficient receipt-free voting based on homomorphic encryption. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 539–556. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-45539-6_38
47. El Español. https://www.elespanol.com/espana/20160511/123987880_0.html. Accessed 15 May 2020
48. 20 Minutos. <https://www.20minutos.es/noticia/2419700/0/podemos-defiende-fiabilidad/sistema-votacion-acusaciones/primarias/>. Accessed 15 May 2020