SoK: Mechanisms Used in Practice for Verifiable Internet Voting

Florian Moser, Michael Kirsten, Felix Dörre

SoK: Mechanisms Used in Practice for Verifiable Internet Voting

Florian Moser [1], Michael Kirsten [2], and Felix Dörre [2]

Abstract: Increasing demands for internet voting instigated the deployment of a multitude of systems used in practice. Within this work, we are interested in which security mechanisms are currently used by vendors to implement verifiable and secret elections.

We perform a systematic market study and review academic literature, where out of 82 candidate systems, we find 29 internet voting systems that are both in active use and claim to employ some form of verifiability. Thereof, we characterize and systematize the 18 systems that provide sufficient information to extract their security mechanisms relevant for state-of-the-art verifiability and secrecy. Overall, we find that only eight systems are well-documented, of which only a few employ state-of-the-art mechanisms in all categories that we consider.

Keywords: Internet Voting, Systematic Study, Verifiable Elections, Security Mechanisms

1 Introduction

The internet plays an increasingly active role in many people's lives, and more and more scenarios, e.g., working from home, depend crucially on performing tasks over the internet. Hence, expectations and demand are growing that more aspects of our lives are accessible in a remote setting. Remote voting over the internet, also called *internet voting*, forms a natural part in this demand, which is also reflected in a growing interest in electronic voting (*e-voting*) by research [Ai24].

Internet voting comprises inherently uncontrolled environments with many stakeholders and potential adversaries, and comes with many requirements, e.g., robustness, integrity, verifiability, secrecy, usability, etc. [HGB23]. Depending on the specific trust assumptions, many of the requirements are inherently or partially in conflict [Kr23]. Moreover, simply adding new technologies may create new potential for attacks and can generally make voting systems more vulnerable [Pa21]. While various mechanisms for verifiable internet elections are state-of-the-art in academia [CT16; KHC22], bringing verifiable electronic voting into practice is still challenging [Te21]. Our primary interest in this work is hence to find out which mechanisms current systems actually use, to shed some light on gaps between academia and practice.

1 INRIA Nancy, France, florian.moser@inria.fr, https://orcid.org/0000-0003-2268-2367
2 KASTEL Security Research Labs, Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany, kirsten@kit.edu, https://orcid.org/0000-0001-9816-1504; felix.doerre@kit.edu, https://orcid.org/0009-0009-7244-7753

Contributions. Our contribution consists in a systematization of knowledge of the current implementation of verifiable internet voting systems used in practice, by classifying their mechanisms based on state-of-the-art criteria from academia, specifically the following:

1. a market study and an academic literature study identifying 82 different internet voting systems used in practice,
2. a systematization of security mechanisms suitable to characterize state-of-the-art internet voting systems,
3. a mapping of our systematization to the 18 voting systems sufficiently documented for our assessment,
4. a brief discussion about our findings and particular observations.

2 Related Work

Comparing practical voting systems based on requirements from academia is challenging. Most related works aim for satisfied security properties, but the challenges therein are multidimensional and not mutually aligned. First, there is no generally agreed-upon list of required properties with fixed definitions. Second, the trust assumptions within each voting system are different, each striving for different criteria and a different election context. In the following, we reflect on the most recent surveys targeting internet voting systems.

Li et al. [LKZ14] systematize 2014's state of the art for 14 electronic voting systems, 9 of them suitable for internet voting, both for cryptographic mechanisms and for satisfied properties. However, they do not report on how they choose the systems, and many of them are not actively used anymore. Moreover, as Li et al. do not specifically target internet voting systems, their classification does not consider the different phases therein. Kho et al. [KHC22] provide an extensive and fine-grained systematization of various cryptographic mechanisms from academia. They identify and compare different electronic voting approaches from literature, provide general structures for mixnet-based, homomorphic, blind signature-based, blockchain-based, and post-quantum electronic voting, and discuss the approaches based on various academic publications. However, they do not report on the selection of the discussed approaches and systems, as well as their relation to systems used in practice.

Most recently, Finogina et al. [FCC24] select twelve internet voting systems that they deem well-known, extract the stakeholders, and compare their trust assumptions for the properties cast-as-intended verifiability, recorded-as-cast verifiability, universal verifiability, privacy, and receipt-freeness. They also compare the systems on their communication channels, scalability, voting channel flexibility, support for preferential voting, as well as support for digital governmental identity. While proposing a unified convention and systematization, their selection of systems is limited, and it is unclear how their trust assumptions and property interpretations can be generalized for a wider comparison of systems. In the attempt to handle the actual situation on the market, our comparison is more general.

3 Method

In this section, we describe our method in detail. For this work, we aim to study verifiable internet voting systems in active use. In a first step, we discover candidate systems, trading recall for precision, and in a second step, we reduce the list to systems that meet our selection criteria, as described in Sect. 3.1. Moreover, we construct initial reviews of the systems, which we use as a basis to perform a systematization of mechanisms, as described in Sect. 3.2. Finally, using only publicly available material, we review each system in detail and assess the implemented mechanisms, as described in Sect. 3.3.

3.1 Discovery of Systems

To discover practical systems in active use, we emulate an organization who wishes to provide verifiable internet voting to their electorate. We assume that the organization has no specific election competencies, however, we assume some intrinsic motivation to do well by spending dedicated effort to learn about internet voting for choosing a system that meets appropriate security criteria. For this matter, we assume a high-level understanding of internet voting, i.e., knowledge about some relevant security requirements, e.g., "end-to-end verifiability" and related mechanisms, e.g., "mixnets". However, we do not assume any corresponding technical expertise or prior knowledge about existing systems. Assuming this coarse-grained understanding of secure internet voting, we perform a market study, with the (hypothetical) aim of choosing a secure state-of-the-art system.

To replicate this setting, we let a business consultancy perform the market study, with experience in market studies, but without prior knowledge in internet voting, thereby ensuring an unbiased perspective. The consultancy received a brief (less than one hour) introduction by an internet voting expert on the general process of holding elections, guarantees generally desired in such systems, and an overview of some of the mechanisms usually employed to reach these guarantees. We consider this sufficient to give a coarse-grained understanding, but not more than what we would expect from motivated but non-technical election organizers.

To check the output of the market study, and minimize chances of ignoring relevant systems, we complement the market study by gathering practical systems referenced in academic literature (e.g., previous comparisons or system proposals). Further, we cross-check the resulting list of systems with two other market analyzes and one list of systems maintained by a research team. Throughout this process, we prioritize recall over prevision, which however leads to discovering many products that are not relevant to our work. Hence, in a final step, we filter the *longlist* of discovered systems for a *shortlist* of systems that meet our criteria of being actively used for verifiable internet voting. See Tab. 1 for an overview on how many systems were added in which step.

Source	Longlist	Shortlist
Our Market Study	60	17
Our Literature Study	+12	+5
Analysis on French Market	+6	+5
Analysis on German Market	+2	+1
Researchers' List in France	+2	+1
Total	**82**	**29**

Tab. 1: We found a *longlist* of 82 systems broadly related to verifiable internet voting in practice. Filtering for our criteria, i.e., internet voting, end-to-end verifiability and privacy, and in recent use, leaves a *shortlist* of 29 systems for further analysis.

Market study. To discover products on the market, the business consultancy searched for products that are broadly related to online voting, thereby aiming for breadth over depth. They conducted the search primarily in January 2024 by using Google, Bing, and Yandex, as well as relevant Wikipedia articles and LinkedIn, with native language proficiency in English and German. In their search, the consultancy used keywords related to the general topic (e.g., "election", "voting"), mechanisms (e.g., "zero-knowledge proofs", "mixnet"), and security properties (e.g., "end-to-end verifiability", "privacy"). For cross-checking intermediate results, they consulted ChatGPT 4.0 with a dataset from around January 2022. In total, the consultancy identified between 250 and 350 products that fit one or more of the keywords. Within the discovery phase, the consultancy employed superficial judgement of the providers' marketing and immediately discarded products not directly related to *verifiable* internet voting. We included the remaining 60 products on our *longlist*.

Literature study. To discover products referenced in academic literature, we ran a manual search, primarily in October 2023, of online-accessible databases and webpages for all proceedings (including relevant satellite workshops) since 2016 of the most relevant academic venues.[3] Moreover, we included the preprint server *IACR Cryptology ePrint Archive* on which many academics publish technical reports or preprint versions of their submissions in cryptography- or security-related domains. In our search, we used the general keywords "voting" and "election", and then scanned the titles for any of the keywords "voting system", "voting protocol", "voting scheme", "internet voting", "remote voting", "electronic voting", "e-voting", "electronic election", "verifiable", "verifiability", "review", "study", or "survey". We then did a semantic scan by manually reading all titles and abstracts for whether the publication mentions any verifiable internet voting system, which comprises papers presenting specific systems of that nature, as well as surveys, evaluations, analyzes or employments. Moreover, we extended our search by scanning the papers' references from their introduction, related work section, and evaluation sections, for the same criteria.

3 These venues are the *International Joint Conference on Electronic Voting* (E-Vote-ID), the *ACM Conference on Computer and Communications Security* (CCS), the *IEEE Computer Security Foundations Symposium* (CSF), the *European Symposium on Research in Computer Security* (ESORICS), the *International Conference on Financial Cryptography and Data Security* (FC), and the *IEEE Symposium on Security and Privacy* (SP).

Our semantic scan aimed to identify systems with recent (i.e., within the last two years) usage in real-world internet elections, i.e., we excluded any kind of in-place systems. Our criterion of real-world comprises any election with decision power on the level of national governments, states or cantons, districts, municipalities, companies, associations or organizations, institutions (e.g., universities), or political parties. We disregarded systems used purely for demonstration purposes or scientific papers, as well as clearly abandoned systems. Collecting all systems proposed in academia would include many more systems, but is out of scope for our purpose. In total, we found 22 systems and, after deduplication and consultation of the systems' webpages and manuals, we added 12 systems to our longlist.

Cross-check with other system collections. To ensure that our list of systems does not contain significant gaps, we did a cross-check with the following two market studies and one list of systems:[4]

- market analysis focused on French market leaders in internet voting (9 systems, 2023)
- market analysis focused on the German market of internet voting (63 systems, 2022)
- list of systems maintained by a French research team focused on end-to-end verifiable systems (12 systems, continuously updated)

The added systems from the first analysis only provide information in French, and were hence hard to discover in our market study performed in English and German. From the second analysis, we directly discarded systems which provide only simple polls or conference voting, as this is in the scope of our work. In total, after deduplication, we added 6 systems from the analysis on the French market, 2 systems from the analysis on the German market, and 1 system from the list by French researchers (see Tab. 1).

Result. The discovery phase resulted in a longlist with 82 systems (see Tab. 1), for which we collected general facts, i.e., vendor, location and webpage. We further constructed a *shortlist*, for which we reduced the longlist's systems in order to fulfill the following criteria:

- Real internet voting systems. The system allows casting votes over the internet. This excludes, e.g., election management software, or systems which require a paper trail where the voter sends a receipt of their vote to the election authorities after voting.
- Aim for end-to-end verifiability and some form of privacy. We welcome different jargon, as long as the overall goal promises some form of end-to-end verifiability and privacy. Further, we admit claimed compliance to some electronic-voting-related certification (e.g., to the French CNIL [Co19a; Co19b] or the Common Criteria Protection Profiles published by the German BSI [IT23; VV08]), while we deem more generic certifications such as ISO 27001 as insufficient.

4 Made internally available as part of a study on E2E-verifiability for the Federal Office for Information Security.

- Active or recent use. We check the proxy criterion that some official communication (e.g., on LinkedIn), code or documentation was produced within the last two years.

Based on these criteria, we found that 9 systems do not provide internet voting, 15 systems already vanished (e.g., dead startups), and 29 systems have no claims related to verifiability. This resulted in a shortlist that leaves 29 systems which fulfill all our criteria, and which we aim to analyze in detail. We give an overview of which source contributed how many systems to the longlist and the shortlist in Tab. 1. The full longlist with all systems and their respective criteria evaluation is publicly available.[5]

Discussion. We observe that the market study alone already covers a large share of the systems on both lists (see Tab. 1), and we therefore expect our findings to represent the market well, by having found the most relevant systems used in practice. Further, more than 80 percent of the systems in the market study's longlist differ from the systems in the literature study, indicating that many systems in practice do not publish scientifically and are not considered when comparing systems in scientific publications.

For transparency, we report on indicators of gaps on our lists in the following. In our hypothetical scenario, we do not consider hard-to-find systems as explicit gaps, as the organization emulated in our market study would also fail to learn of the system. Yet, we expect gaps for systems that are neither advertised in English nor in German, as we observed in our cross-check for the French market. Further, our market study may exclude companies not explicitly advertising verifiability, but who only use it under the hood.

3.2 Systematization of Mechanisms

The chosen systematization aims to consider only mechanisms which are fundamentally different. Hence, we ignore implementation details, and collapse slight variations of a mechanism (small tweaks to achieve, e.g., improved verifiability or secrecy) into a single mechanism. Thereby, we aim to avoid noise in our evaluation, but still distinguish clearly separate approaches. To design this systematization, we first perform two independent coarse-grained reviews of some of the chosen systems. Each review results in a systematization proposal which captures the respective subset of systems from the shortlist. Second, we unify the two systematization proposals into our final systematization, in order to capture the full diversity of the systems.

5 The list is available as supplementary material on `inria.hal.science`.

3.3 Extraction of Mechanisms from Systems

All the systems on our shortlist (see Sect. 3.1) claim some level of verifiability, and as verifiability aims to make a system observable to outsiders, this directly requires that the system's inner workings are communicated clearly and openly. We would therefore expect all systems to publish at least a detailed system specification, possibly also a reference implementation, security proofs, and expert reviews of their system.

Our goal consists in assessing which mechanisms are used in practice, not in assessing the systems themselves. We can hence relax the thoroughness of our reviews and require less documentation than would be necessary for full system reviews. Our classification targets the most positive and secure or secret interpretation of the described mechanisms, where we favorably fill gaps with educated guesses, and generally trust the claims by the vendors. Practically, often a high-level overview of the system (e.g., a whitepaper, or explicit claims on the vendor's webpage) is sufficient, if that allows to clearly identify which mechanisms are in use. However, even in this relaxed setting, many systems do not publicly provide sufficient information for extracting the mechanisms in use. The following list contains all systems on our shortlist for which we could not find sufficient information and which we therefore excluded from further analysis:

- *Electis* (France) [El24b]. The code is open source [El24a] and seems to integrate with ElectionGuard [Be24b] and the Tezos blockchain, but it is hard to extract the specific security mechanisms of the currently implemented solution. The product claims to follow the CNIL recommendations for electronic voting [Co19b].
- *Eligo* (Italy) [El24d]. The published documentation does not disclose security details apart from support for two-factor authentication.
- *Genolive* (Germany) [Co24]. While the product claims to be developed in compliance with the BSI Common Criteria Protection Profile for internet voting [VV08], the employed security mechanisms are not described.
- *Kercia Solutions* (France) [Ke24], *LegaVote* (France) [Le24], *Neovote* (France) [Ne24a], *WebVote* by Gedivote (France) [Ge24], and *WeeChooz* (France) [We24]. We could not find documentation about the security mechanisms by these systems. All products claim to follow the CNIL recommendations for electronic voting [Co19b].
- *Neuvote* (Canada) [Ne24b]. The webpage does not disclose any security details besides support for end-to-end encryption and two-factor authentication.
- *Nvotes* (Spain) [nV24]. The webpage does not contain any concrete details about their system. However, the technical leadership seems to have moved to Sequent, which we analyze as part of this work (see below).
- *Onlz* (Belgium) [On24]. The webpage does not contain details about the system and only mentions to employ client-side encryption, blockchain and ring signatures.

For the following systems, we are able to extract the mechanisms from public specifications:

- *Belenios* (France) [Gl24]. Besides the specification, there is a high-level academic publication which discusses some of the design decisions [CGG19]. Further, the code is open source [In24], and there are further supporting documents, including academically reviewed formal proofs [Be24a].
- *Electa* by AssemblyVoting (Denmark) [As23]. Besides the specification, some of the code is public [As24].
- *Helios* [Ad08]. Besides the initial academic publication and the specification, which was available until April 2024 [Ad12], the code is open source [He24]. Recent development in the repository seems to focus on dependency updates, minor usability features, and authentication mechanisms.
- *IVXV* by Cybernetica (Estonia) [Va22]. Besides the specification, the code is open source [Va24].
- *Polyas Core-3* (Germany) [Tr23]. Besides the system specification, there is an academic paper and a specification for their cast-and-audit approach [MT23; Tr24]. Further, there are some non-technical descriptions on the webpage [PO24].
- *Sequent* (USA) [Se24a]. There is a webpage with a system overview, documentation [Se24c] including usage demos, explanations, the high-level cryptographic protocol [Ru21], and system architecture [Ro22], as well as open-source code [Se24b].
- *Swiss Post Voting System* (Switzerland) [Sw24d; Sw24e]. Besides the specification, extensive documentation of the system, formal proofs, as well as the code is public [Sw24c]. The system is provided for political elections in the Swiss cantons [Sw24b], and is hence compliant to the corresponding Swiss law [BV13]. Further, numerous system reviews by independent experts are publicly accessible [Sw24a].
- *uniWAHL* by ElectricPaper (Germany) [El24c]. The webpage focuses on explanations and demos and is mostly aimed at election organizers. Under the hood, they use the security mechanisms provided by Sequent.[6]

For these systems, we use informal partial specifications, whitepapers, code, or webpages:

- *BigPulse Voting* (UK) [Bi24b]. The verification is sketched on the webpage [Bi24a]. We did not find details about authentication or encryption of the votes.
- *DecentraVote* (Germany) [De24a]. Besides the whitepaper [Fa20], the code is open source [De24b].
- *EVoters* by EVoting (Chile) [EV24a]. The used encryption, as well as the tally mechanism, are described on their webpage [EV24b]. We could not find details about

6 https://sequentech.io/case-study/bringing-sequents-end-to-end-verifiable-voting-solution-to-the-german-market/

how votes are verified by the voter or how the votes are stored, and found only very high-level information on the employed authentication.

- *Followmyvote* (USA) [Fo24a]. The webpage provides informal descriptions and some system code is public [Fo24b].[7]
- *Invote* by Scytl (Spain) [Sc24]. The specification is not public, but the mechanisms are sketched in an academic survey paper [FCC24].
- *Simply Voting* (Canada) [Si24b]. Some mechanisms are documented [Si24a].
- *V8te* (France) [V824]. The privacy policy describes some mechanisms [Cé23].
- *Voatz* (USA) [Vo24a]. The webpage features a video which describes some of the security mechanisms and links to a high-level whitepaper [Mo20]. It remains unclear how ballots are encrypted and authenticated.
- *Voxaly* (France) [Vo24b]. Other than compliance to the recommendations of CNIL, the webpage does not provide a closer description of the solution. However, a partial specification [Ch23], yet excluding authentication and record details, of the system used for the legislative elections in France is public and described as an adaptation of the Belenios system, which we also analyze as part of this work (see above).
- *zkVoting* (Korea) [Pa24]. An academic whitepaper describes cryptographic details.

4 Analysis

We organize the mechanisms into *Cast*, *Authentication*, *Cast Verification*, *User Record*, *System Record* and *Tally*. Cast considers all mechanisms which contribute towards forming the ballot. Authentication authenticates this ballot (or the corresponding voter). Cast verification helps the voter be assured that the ballot was formed correctly. Record tracks mechanisms which store data on the voter's device or system-side. Tally finally encompasses the mechanisms to cleanse the list of ballots (e.g., of revotes), and anonymize and decrypt.

7 The provided code includes smart contracts and some UI code, but notably no code employed by the registrar.

4.1 Cast

When the voter casts their vote, they form their ballot. We track the employed encryption (if any) and how the corresponding (decryption) keys are handled.

Encryption. We distinguish whether the ballot is encrypted using *symmetric encryption* or *asymmetric encryption*. In the internet voting setting, asymmetric encryption is desirable, as it is a precondition to employ any of the privacy-preserving tally methods (see Sect. 4.6). Voting systems which assume anonymous channels may omit encrypting the ballots.

Keys. We place special attention to how encryption keys are handled. Storing the decryption key in a *distributed storage* requires multiple trustees to reconstruct the decryption key. Further, to prevent that a single trustee learns the decryption key when it is generated, we track support for *distributed generation*.

	Belenios	Electa	uniWAHL	Helios	IVXV	Polyas	Sequent	Swiss Post	BigPulse	DecentraVote	followmyvote	Invote	SimplyVoting	V8te	Voatz	EVoters	Voxaly	zkVoting
Encryption																		
symmetric										•								•
asymmetric	•	•	•	•	•	•	•	•				•		•		•	•	
Keys																		
distr. storage	•	•	•	•	•	•	•	•				•		•		•	•	
distr. generation	•	•	•	•		•	•	•										

Tab. 2: Comparison of voting systems concerning their mechanism used for encryption and keys, well-documented systems to the left of the dashed line. DecentraVote uses a hash to hide the plain vote, taken from the plain vote concatenated with secrets, with the secrets published in the tally phase to count the votes. zkVoting uses a hybrid encryption scheme, with the ballot itself encrypted under a symmetric key, and that symmetric key under the public election key. For BigPulse, followvoting, Simply Voting and Voatz, we did not find claims about the used encryption.

4.2 Authentication

Most systems document that the voter needs to pass one or multiple logins, similar to how the voter would interact with other online systems. We are however interested in whether and how the system employs credentials, which we understand as cryptographic keys with a private and a public part, necessary for state-of-the-art cryptographic ballot authentication.

Credential generation. Credentials may be generated *centralized*, where a single authority learns all credentials, or *distributed* by multiple authorities. Some systems may generate the credentials *on the voter's device*, and others rely on *election-independent* credentials established outside the specific election context, e.g, for other uses such as electronic IDs.

Credential interface. For credentials that were not already generated on the voter's device, we distinguish the interface for the credentials' usage. Credentials may be explicitly delivered to the voter on a dedicated channel, where the credential is then *directly entered* by the voter into the voter's device, possibly looking similar to entering a long password. Another possibility is that the credential is stored on *trusted hardware*, such as an electronic ID card, to ensure that the credential can only be used by the holder of the trusted hardware.

Credential properties. Most systems use credentials that are *cryptographically bound* to the ballot, to harden against a dishonest voter attempting to (re)use the authentication for a different ballot. Systems may further use *distributed authentication*, where they rely on multiple authorities who authenticate the public part of the credential.

	Belenios	Electa	uniWAHL	Helios	IVXV	Polyas	Sequent	Swiss Post	BigPulse	DecentraVote	followmyvote	Invote	SimplyVoting	V8te	Voatz	EVoters	Voxaly	zkVoting
Credential Generation																		
centralized	•					•		•				•						
distributed		•																
on the voter's device		•								•	•							•
election-independent					•													
Credential Interface																		
directly entered	•	•				•		•				•						
trusted hardware					•													
Credential Properties																		
cryptographically bound	•	•			•	•		•		•		•						•
distributed authentication		•																

Tab. 3: Comparison of voting systems on how credentials are generated and used, well-documented systems to the left of the dashed line. Electa supports credential-based authentication, where credentials are distributed by credential authorities and entered by the voter, and identity-based authentication, where the voter's device generates the credential, which the voter authenticates using identity providers.

4.3 Cast Verification

When casting the vote, systems often allow verifying whether the ballot has been formed correctly. These verification mechanisms may deliver either probabilistic or definite guarantees. In the former, the voter gets probabilistic (game-based) guarantees over whether their ballot is correct, which get stronger when the voter repeats the verification multiple times. In the latter, if the verification succeeds, the ballot represents only with negligible probability something different (assuming that the system's trust assumptions are fulfilled).

Verification. We observe the probabilistic *audit-or-cast* approach in use, where after the ballot is formed, the voter is given the choice to either audit or cast the ballot. If the voter chooses the former, they may verify whether the ballot was formed correctly, but must restart the cast procedure until they finally choose to cast the ballot. If the voter chooses to cast the ballot, they need to check that the ballot reached the voting system exactly as formed.

Some systems allow auditing the cast vote, which we name *cast-then-audit* approach. Such systems may take precautions attempting to avoid that the voter gets a trivial receipt, e.g., limiting the time during which the voter can audit, keeping the bulletin board private, and employing zero-knowledge proofs. We name the mechanism *clear-text receipt* if the voter gets some confirmation which includes the plaintext vote. If the voter receives opaque codes that correspond to their vote in the voting phase, we name it *return codes*. We name it *audit codes* when the voter may look up the content of their anonymized vote using a code.

	Belenios	Electa	uniWAHL	Helios	IVXV	Polyas	Sequent	Swiss Post	BigPulse	DecentraVote	followmyvote	Invote	SimplyVoting	V8te	Voatz	EVoters	Voxaly	zkVoting
audit-or-cast		•	•	•			•											
cast-then-audit					•	•						•						•
return codes								•										
clear-text receipts													•		•			
audit codes						•			•				•		•			

Tab. 4: Comparison of voting systems on their cast verification mechanism, well-documented systems to the left of the dashed line. Some systems do not employ cast verification, notably Belenios, and the Voxaly system which adapted Belenios. Audit codes are sometimes combined with other mechanisms.

4.4 User Record

Once the authenticated vote is cast, the system may provide an artifact to the user that the ballot has really been stored. Further, this artifact may be authenticated to avoid disputes over the artifacts' validity, and chained, to harden against later changes to the system state.

User artifact. The voter may receive a *storage reference*, which upon querying the system reveals the stored ballot (e.g., a transaction ID in a blockchain). Otherwise, the voter may receive the *ballot hash*, or even the *plain vote* itself as artifact. Some systems also provide a *return code*, which asserts that some, possibly previously verified, ballot has been stored.

Artifact properties. The artifact that the voter receives may be authenticated, i.e., *signed* using a digital signature, which allows proving that the artifact really originated from the system. This makes the system accountable for the artifacts that it issues. Further, the artifact may cryptographically reference the ballots already cast by other voters, which we then name *chained*. This forces the system to commit to the ballots it already stores at the time of issuing the artifact, which hardens against later tampering with that state.

	Belenios	Electa	uniWAHL	Helios	IVXV	Polyas	Sequent	Swiss Post	BigPulse	DecentraVote	followmyvote	Invote	SimplyVoting	V8te	Voatz	EVoters	Voxaly	zkVoting
User Artifact																		
storage ref		•							•	•	•	•		•	•			•
ballot hash	•		•	•	•	•	•										•	
plain vote													•					
return code								•										
Artifact Properties																		
signed		•			•	•			•								•	
chained										•	•				•			•

Tab. 5: Comparison of voting systems concerning their user record mechanism, well-documented systems to the left of the dashed line.

4.5 System Record

Once the authenticated vote is cast, the system needs to record the vote until the tally. The system may provide access to the vote's current state. This state may be distributed over multiple authorities, with some consistency procedure in place.

System access. Some systems may provide voters with access to the *individual entry* of the individual voter, or even to *all entries* of all voters. More permissive systems may improve (public) verifiability, possibly at the cost of (everlasting) privacy.

System consistency. When a new ballot is submitted, *centralized* systems trivially achieve consistency, i.e., they register the ballot as submitted (or not). When the state is instead distributed over multiple authorities, some systems still achieve *immediate* consistency; i.e., the ballot is added immediately to the list of to-be-tallied ballots' state of the system. Other distributed systems may feature *delayed* consistency, with an explicit consistency agreement procedure at the latest before the ballots are tallied.

	Belenios	Electa	uniWAHL	Helios	IVXV	Polyas	Sequent	Swiss Post	BigPulse	DecentraVote	followmyvote	Invote	SimplyVoting	V8te	Voatz	EVoters	Voxaly	zkVoting
Access																		
indiv. entries	●	●	●		●		●		●	●	●	◐	●					●
all entries	●	●	●				●		●	●	●	◐	●	●				●
Consistency																		
centralized	●	●	●	●		●	●											
immediate										●	●				●			●
delayed					●			●										

Tab. 6: Comparison of voting systems on their system record mechanism, well-documented systems to the left of the dashed line. Invote makes the receipts publicly accessible, but not the ballots themselves.

4.6 Tally

After the voting phase closes, the system will calculate the result. First, the system may perform a cleansing to, e.g., filter out revotes. Then, ballots are anonymized, i.e., the link to the submitting user is removed, and decrypted.

Cleansing. Some systems support *revotes*, where voters may vote multiple times and the latest ballot overrides the previous ones. Further, *revoked ballots* (e.g., in case a voter later-on decides to cast in person) and *fake ballots* (i.e., ballots cast with invalid credentials) need to be prevented from entering the tally. These mechanisms can be used to increase voter privacy in case the system hides which ballots are removed in the cleansing process.

Anonymization. To anonymize, *homomorphic aggregation* allows aggregating all ciphertexts into a single ciphertext which sums up the chosen candidates from its contributing ciphertexts. Then, only this resulting ciphertext is decrypted. However, the implementation of homomorphic aggregation is difficult and computation-intensive for arbitrary counting functions, which is one of the reasons a system may use a *verifiable shuffle*. The shuffle preserves each ballot in their own ciphertext, while removing the link to the submitted ciphertext using verifiable re-encryption and secret shuffling.

Decryption. Decryption may be *verifiable*, hence the decrypting trustee needs to prove that the provided plaintext corresponds to the ciphertext. Additionally, decryption may be *distributed*, where the trustees never share their (partial) decryption keys among the other trustees, thereby allowing the trustee to remain in control over which ciphertext is decrypted.

	Belenios	Electa	uniWAHL	Helios	IVXV	Polyas	Sequent	Swiss Post	BigPulse	DecentraVote	followmyvote	Invote	SimplyVoting	V8te	Voatz	EVoters	Voxaly	zkVoting
Cleansing																		
revotes	●	●	●	●	●		●		●						●			
revoked ballots					●	●												
fake ballots																		●
Anonymization																		
homomorphic aggr.	●			●								●		●		●	●	◐
verifiable shuffle	●	●	●		●	●	●	●				●						
Decryption																		
verifiable	●	●	●	●	●	●	●	●		●		●					●	●
distributed	●	●	●	●		●	●	●										

Tab. 7: Comparison of voting systems on their tally mechanism, well-documented systems to the left of the dashed line. In zkVoting, a single authority decrypts the (hybridly-encrypted) ballots, sums up the plaintexts, and then publishes the sum with a proof that it corresponds to the authenticated ballots.

5 Conclusion

We found as many as 82 internet voting systems that are broadly related to *verifiable* internet voting. The initial barrier of providing an internet voting system seems to be low, and small and local products are prevalent. Almost all systems use security as a sales argument, largely independently of the actually taken (and publicly documented) security measures. Most systems do not even claim to implement verifiability in their products, and out of those that do, most systems document their solution poorly. As an example, from the systems claiming to implement the CNIL e-voting recommendations [Co19b], six out of nine systems did not publish concrete documentation, and two published a very partial description. Already for other secure systems, such a lack of documentation would be surprising, considering the security principle of *open design* [SJT08]. In the context of internet voting, however, transparency is especially crucial, and voters do consider it important [Ag23].

When evaluating the mechanisms, most of the eight sufficiently documented systems do not implement state-of-the-art security mechanisms in all relevant categories. While asymmetric encryption is typically used to encrypt the vote, only seven systems combine it with distributed generation and distributed storage of the corresponding private key. Similarly, while homomorphic aggregation or verifiable shuffling are used in practice, only the same seven systems then perform the decryption in a verifiable and distributed fashion. All other systems omit at least the distributed generation and the distributed decryption, making the component which learns the full decryption key a potential single point of failure. While the state-of-the-art for casting and tallying seems mostly established, and most systems use the same mechanisms, many different approaches are in use for authentication, cast verification and recording, generally with no clearly emerging favorite. Notably for authentication, some systems support multiple mechanisms and let the election organizer pick the approach that suits their election context best.

Besides the large gaps between practice and research reported above, we want to briefly discuss the systems which employ some of the relevant state-of-the-art security mechanisms. The systems Belenios and Helios, both largely developed directly within academia, provide very transparent and extensive documentation: While Helios shows no recent development anymore and is a considerably smaller system with not as much documentation, both systems provide source code and a range of academic publications about the systems and proposed variants, and Belenios even provides formal proofs [Ad08; Be24a]. Yet, also some systems developed in industry publish extensive documentations and source code. Most notably, the Swiss Post System provides detailed specification, source code, formal proofs, as well as extensive third-party expert reviews [Sw24a; Sw24c]. These extensive transparency measures are required by law for the Swiss national political elections [BV13], for which the Swiss Post System is built. Both, the Sequent (and hence also uniWAHL) and the IVXV system also publicly provide many details on their mechanisms and their source code [Se24a; Va22; Va24]. Moreover, the Electa system also provides an easily-accessible and high-quality specification describing their used cryptographic mechanisms [As23]. Also, for the Polyas system, system specifications and an academic publication are available [Tr23].

Finally, we have seen many systems report using the open-source libraries and development kits Verificatum [Wi24] and ElectionGuard [Be24b] under the hood, profiting from their well-vetted implementation of core security mechanisms, including extensive specifications.

Limitations. Despite the large number of inspected systems and our general systematization thereof, our study has some limitations to be considered. First, as the quality of the systems' documentations varied widely, our systematization only considers the general mechanisms claimed to be used by the system, and not necessarily the specific implementations or variations of the mechanisms. Second, while employing critical judgement of the advertised systems and mechanisms, our study is bound to believe the officially available statements for a fair comparison between those systems which provide implementation details and other systems which only provide high-level and informal descriptions. Our characterization may hence slightly favor an ambitious high-level description over disadvantageous implementation details.

Future work. Our study and systematization provide a basis for further, more specialized endeavors for a systematization and assessment of practical systems. It would be interesting to, e.g., use the recommendations for source code examinations by Haines and Rønne [HR21] within each of the categories for mechanisms from systems in practice, where the systems provide public access to their code. Moreover, our systematization opens up the potential for using more detailed analysis frameworks for specific trust models within each of the categories, instead of challenging comparisons of complete systems. Such category-specific assessments could allow more fine-grained comparisons of adversarial capabilities [NNV17], trust levels [Ne21] and trust assumptions [Kr23] in a meaningful way. Finally, practical systems do not only aim for security and privacy, and it might be sensible to also include further dimensions on which internet voting systems are assessed, instead of focusing solely on the security mechanisms [Wi18].

Acknowledgements

Parts of this work were based on a study on end-to-end-verifiability by the Federal Office for Information Security (BSI). We thank Jeremy L. Meyer from Performance Partners GmbH for support when executing the market analysis. This work was supported by funding from the topic Engineering Secure Systems of the Helmholtz Association (HGF) and by KASTEL Security Research Labs. Further, this work benefited from funding managed by the French National Research Agency under the France 2030 program with the reference ANR-22-PECY-0006. It was also partly supported by the ANR Chair IA ASAP (ANR-20-CHIA-0024) with support from the region Grand Est, France.

References

[Ad08] Adida, B.: Helios: Web-based Open-Audit Voting. In: 17th USENIX Security Symposium, San Jose, CA, USA July 28–Aug. 1, 2008. USENIX Association, pp. 335–348, 2008, URL: https://www.usenix.org/legacy/events/sec08/tech/full_papers/adida/adida.pdf.

[Ad12] Adida, B.: Helios v4, tech. rep., Helios, 2012, URL: https://web.archive.org/web/20240417102302/https://documentation.heliosvoting.org/verification-specs/helios-v4.

[Ag23] Agbesi, S.; Budurushi, J.; Dalela, A.; Kulyk, O.: Investigating Transparency Dimensions for Internet Voting. In: 8th International Joint Conference on Electronic Voting (E-Vote-ID 2023), Luxembourg City, Luxembourg Oct. 3–6, 2023. Springer, pp. 1–17, 2023, DOI: 10.1007/978-3-031-43756-4_1.

[Ai24] Aidynov, T.; Goranin, N.; Satybaldina, D.; Nurusheva, A.: A Systematic Literature Review of Current Trends in Electronic Voting System Protection Using Modern Cryptography. Applied Sciences 14 (7), 2742, 2024, DOI: 10.3390/app14072742.

[As23] Assembly Voting: Electa: Documentation of the cryptographic protocol (Version 2.0), tech. rep., Assembly Voting, 2023, URL: https://web.archive.org/web/20240714102041/https://downloads.assembly-voting.com/download/marketing/electa_-_documentation_of_the_cryptographic_protocol.pdf.

[As24] Assembly Voting: Assembly Voting SDKs, 2024, URL: https://github.com/aion-dk.

[Be24a] Belenios: Belenios documentation, 2024, URL: https://web.archive.org/web/20240708065438/https://www.belenios.org/documentation.html.

[Be24b] Benaloh, J.; Naehrig, M.; Pereira, O.; Wallach, D.: ElectionGuard: a Cryptographic Toolkit to Enable Verifiable Elections. In: 33rd USENIX Security Symposium (USENIX Security 2024), Philadelphia, PA, USA Aug. 14–16, 2024. USENIX Association, 2024, URL: https://www.usenix.org/conference/usenixsecurity24/presentation/benaloh.

[Bi24a] BigPulse: Election vote count verification protocol, 2024, URL: https://www.bigpulsevoting.com/about/vote-count-verification-protocol/.

[Bi24b] BigPulse: Secure Online Voting System, 2024, URL: https://www.bigpulsevoting.com/.

[BV13] Bozzini, D.; Varone, A.: Federal Chancellery Ordinance on Electronic Voting, ordinance, Swiss Federal Chancellery, 2013, URL: https://cva.unifr.ch/content/federal-chancellery-ordinance-electronic-voting.

[Cé23] Cécile: Privacy Policy - V8TE, tech. rep., V8TE, 2023, URL: https://web.archive.org/web/20240822085749/https://drive.usercontent.google.com/download?id=1SOxRXNdHsTazUjcJt1EOcYw3hA6fy5JG&export=download&authuser=0.

[CGG19] Cortier, V.; Gaudry, P.; Glondu, S.: Belenios: A Simple Private and Verifiable Electronic Voting System. In: Foundations of Security, Protocols, and Equational Reasoning - Essays Dedicated to Catherine A. Meadows. Vol. 11565. LNCS, Springer, pp. 214–238, 2019, DOI: 10.1007/978-3-030-19052-1_14.

[Ch23] Chenon, B.: MEAE - Transparence et vérifiabilité V2 (Version 2.04), tech. rep., Voxaly, 2023, URL: https://web.archive.org/web/20240308073039/https://www.voxaly.com/wp-content/uploads/VOXALY-LEG2023-Transparence-et-Verifiabilite-Specifications-publiques-v2-04.pdf.

[Co19a] Commission nationale de l'informatique et des libertés: Délibération n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet, tech. rep., Journal Officiel de la République Française, 2019, URL: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038661239.

[Co19b] Commission nationale de l'informatique et des libertés: Sécurité des systèmes de vote par internet: la CNIL actualise sa recommandation de 2010, 2019, URL: https://www.cnil.fr/fr/securite-des-systemes-de-vote-par-internet-la-cnil-actualise-sa-recommandation-de-2010.

[Co24] Conventex: Digitale Wahlen, 2024, URL: https://conventex.com/digitale-wahlen/.

[CT16] Culnane, C.; Teague, V.: Strategies for Voter-Initiated Election Audits. In: 7th International Conference on Decision and Game Theory for Security (GameSec 2016), New York, NY, USA Nov. 2–4, 2016. Vol. 9996. LNCS, Springer, pp. 235–247, 2016, DOI: 10.1007/978-3-319-47413-7_14.

[De24a] DecentraVote: Decentralized e-voting protocol powered by blockchain, 2024, URL: https://decentra.vote/.

[De24b] DecentraVote: DecentraVote-Core, 2024, URL: https://github.com/DecentraVote-eVoting/DecentraVote-Core.

[El24a] Electis: Electis Core, 2024, URL: https://gitlab.com/electisNGO/electis-core/.

[El24b] Electis: Vote électronique CSE, 2024, URL: https://www.tessi.eu/.

[El24c] Electric paper Wahlsysteme: Wahlen sicher und effizient durchführen, 2024, URL: https://wahlen-organisieren.de/.

[El24d] Eligo: Electronic and online voting platform, 2024, URL: https://www.eligo.social/.

[EV24a] EVoting: Electronic Voting Service, 2024, URL: https://www.evoting.com/.

[EV24b] EVoting: Encryption and voting secrecy, 2024, URL: https://www.evoting.com/en/seguridad-integral/secreto-voto/.

[Fa20] Fazekas, Z.: DecentraVote: Electronic Voting secured by Blockchain (Version 1.0), tech. rep., DecentraVote, 2020, URL: https://github.com/DecentraVote-eVoting/DecentraVote-Core/blob/72c0a20ed1764fb5e80d4475934965a2f57a743e/Whitepaper_DecentraVote.pdf.

[FCC24] Finogina, T.; Cucurull Juan, J.; Costa, N.: Selective comparison of verifiable online voting systems. Security and Privacy, 2024, DOI: 10.1002/spy2.394.

[Fo24a] Followmyvote: Blockchain Voting: Cryptographically Secure Voting, 2024, URL: https://web.archive.org/web/20240820075328/https://followmyvote.com/cryptographically-secure-voting-2/.

[Fo24b] Followmyvote: Followmyvote SmartContract code, 2024, URL: https://github.com/FollowMyVote/Pollaris-Contract.

[Ge24] Gediote: Expert en solutions de vote, 2024, URL: https://www.gedivote.fr/.

[Gl24] Glondu, S.: Belenios specification (Version 2.5.1), tech. rep., Belenios, 2024, URL: https://web.archive.org/web/20240708064854/https://www.belenios.org/specification.pdf.

[He24] Helios: Helios-Server, 2024, URL: https://github.com/benadida/helios-server/tree/c7ed0608e2cdfc75bf323a834f0ca579e6273e34.

[HGB23] Heinl, M.; Gölz, S.; Bösch, C.: Remote Electronic Voting in Uncontrolled Environments: A Classifying Survey. ACM Computing Surveys 55 (8), 167, pp. 1–44, 2023, DOI: 10.1145/3551386.

[HR21] Haines, T.; Rønne, P.: New Standards for E-Voting Systems: Reflections on Source Code Examinations. In: International Workshops on Financial Cryptography and Data Security (FC 2021), Revised Selected Papers, Virtual Event Mar. 5, 2021. Vol. 12676. LNCS, Springer, pp. 279–289, 2021, DOI: 10.1007/978-3-662-63958-0_24.

[In24] Inria@CNRS: belenios, 2024, URL: https://gitlab.inria.fr/belenios/belenios/.

[IT23] IT Security Evaluation Facility of Deutsche Telekom Security GmbH: Protection Profile for E-Voting Systems for non-political Elections: BSI-CC-PP-0121 (Version 0.9), tech. rep., Federal Office for Information Security Germany - BSI, 2023, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Schutzprofile/BSI-CC-PP-0121-Protection-Profile-for-E-Voting-Systems.pdf.

[Ke24] Kercia: Solutions de vote électronique sécurisées, 2024, URL: https://www.kercia.com/.

[KHC22] Kho, Y.; Heng, S.; Chin, J.: A Review of Cryptographic Electronic Voting. Symmetry 14 (5), 858, 2022, DOI: 10.3390/sym14050858.

[Kr23] Krips, K.; Snetkov, N.; Vakarjuk, J.; Willemson, J.: Trust Assumptions in Voting Systems. In: ESORICS 2023 International Workshops on Computer Security, Revised Selected Papers, The Hague, The Netherlands Sept. 25–29, 2023. Vol. 14399. LNCS, Springer, pp. 309–329, 2023, DOI: 10.1007/978-3-031-54129-2_18.

[Le24] LegaVote: Vous avez un projet de scrutin, nous avons une solution de vote électronique, 2024, URL: https://www.legavote.fr/.

[LKZ14] Li, H.; Kankanala, A.; Zou, X.: A taxonomy and comparison of remote voting schemes. In: 23rd International Conference on Computer Communication and Networks (ICCCN 2014), Shanghai, China Aug. 4–7, 2014. IEEE Computer Society, pp. 1–8, 2014, DOI: 10.1109/icccn.2014.6911807.

[Mo20] Moore, L.: Voatz Mobile Voting Platform – An Overview: Security, Identity, Auditability (Version 1.1), tech. rep., Voatz, Inc., 2020, URL: https://web.archive.org/web/20240822073616/https://voatz.com/wp-content/uploads/2020/07/voatz-security-whitepaper.pdf.

[MT23] Müller, J.; Truderung, T.: CAISED: A Protocol for Cast-as-Intended Verifiability with a Second Device. In: 8th International Joint Conference on Electronic Voting (E-Vote-ID 2023), Luxembourg City, Luxembourg Oct. 3–6, 2023. Vol. 14230. LNCS, Springer, pp. 123–139, 2023, DOI: 10.1007/978-3-031-43756-4_8.

[Ne21] Nemes, M.; Schwerdt, R.; Achenbach, D.; Löwe, B.; Müller-Quade, J.: And Paper-Based is Better? Towards Comparability of Classic and Cryptographic Voting Schemes. IACR Cryptology ePrint Archive, 2021, Report 2021/1122.

[Ne24a] Neovote: Neovote, 2024, URL: https://www.neovote.com/.

[Ne24b] Neuvote: Online Voting, 2024, URL: https://www.neuvote.com/.

[NNV17] Neumann, S.; Noll, M.; Volkamer, M.: Election-Dependent Security Evaluation of Internet Voting Schemes. In: 32nd IFIP TC 11 International Conference on ICT Systems Security and Privacy Protection (SEC 2017), Rome, Italy May 29–31, 2017. Vol. 502. IFIP Advances in Information and Communication Technology, Springer, pp. 371–382, 2017, DOI: 10.1007/978-3-319-58469-0_25.

[nV24] nVotes: Secure Online Voting Software, 2024, URL: https://nvotes.com/.

[On24] Onlz: Electronic voting you can trust. 2024, URL: https://www.onlz.com/.

[Pa21] Park, S.; Specter, M.; Narula, N.; Rivest, R.: Going from bad to worse: from Internet voting to blockchain voting. Journal of Cybersecurity 7 (1), 2021, DOI: 10.1093/cybsec/tyaa025.

[Pa24] Park, S.; Choi, J.; Kim, J.; Oh, H.: zkVoting: Zero-knowledge proof based coercion-resistant and E2E verifiable e-voting system. IACR Cryptology ePrint Archive, 2024, Report 2024/1003.

[PO24] POLYAS: POLYAS, 2024, URL: https://www.polyas.de/.

[Ro22] Robles, E.: Sequent Voting SystemArchitecture Overview (Work in progress), tech. rep., Sequentech, 2022, URL: https://web.archive.org/web/20240830084927/https://sequentech.github.io/documentation/assets/files/2022-04-10-arch-1-5bc31f49172dc628367719c7785abe36.pdf.

[Ru21] Ruescas, D.: Sequent Tech Cryptographic Protocol, tech. rep., Sequentech, 2021, URL: https://web.archive.org/web/20240830085125/https://sequentech.github.io/documentation/assets/files/2021-03-19-proto-1-18fd36c9669813aadcf59e672f0f7a84.pdf.

[Sc24] Scytl: Secure Online Voting, 2024, URL: https://scytl.com/.

[Se24a] Sequent: Open source end-to-end verifiable online voting, 2024, URL: https://sequentech.io/.

[Se24b] Sequent: Sequent, 2024, URL: https://github.com/sequentech/.

[Se24c] Sequent: Sequentech docs, 2024, URL: https://sequentech.github.io/documentation.

[Si24a] Simply Voting: Checking, Interpreting, and Publishing Results, 2024, URL: https://web.archive.org/web/20240711091037/https://help.simplyvoting.com/docs/checking-interpreting-and-publishing-results.

[Si24b] Simply Voting: Simply Voting, 2024, URL: https://www.simplyvoting.com/.

[SJT08] Scarfone, K.; Jansen, W.; Tracy, M.: Guide to General Server Security, tech. rep. Special Publication 800-123, National Institute of Standards and Technology (NIST), 2008, DOI: 10.6028/nist.sp.800-123.

[Sw24a] Swiss Federal Chancellery: Examination of systems, 2024, URL: https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting/ueberpruefung_systeme.html.

[Sw24b] Swiss Post: E-Voting: Online voting and elections, 2024, URL: https://digital-solutions.post.ch/en/e-government/digitization-solutions/e-voting.

[Sw24c] Swiss Post: swisspost-evoting, 2024, URL: https://gitlab.com/swisspost-evoting.

[Sw24d] Swiss Post Ltd.: Swiss Post Voting System – System Specification (Version 1.4.1), tech. rep., Swiss Post Ltd., 2024, URL: https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/a3e1063615e2efcdf2692e8a47697daf7ccdb2d1/System/System_Specification.pdf.

[Sw24e] Swiss Post Ltd.: Swiss Post Voting System Verifier Specification (Version 1.5.2), tech. rep., Swiss Post Ltd., 2024, URL: https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/blob/a3e1063615e2efcdf2692e8a47697daf7ccdb2d1/System/Verifier_Specification.pdf.

[Te21] Teague, V.: Which E-Voting Problems Do We Need to Solve? In: 41st Annual International Cryptology Conference on Advances in Cryptology (CRYPTO 2021), Virtual Event Aug. 16–20, 2021. Vol. 12825. LNCS, Springer, pp. 3–7, 2021, DOI: 10.1007/978-3-030-84242-0_1.

[Tr23] Truderung, T.: POLYAS 3.0 Verifiable E-Voting System (Version 1.3.2), tech. rep., Berlin, Germany: POLYAS GmbH, 2023, URL: https://github.com/polyas-voting/core3-verifiable-doc/blob/d23fdb8d2627e17b181e06f97fb44e38865bf157/pdf/polyas3.0-verifiable.pdf.

[Tr24] Truderung, T.: POLYAS-Core3 Second Device Protocol (Version 1.1), tech. rep., Berlin, Germany: POLYAS GmbH, 2024, URL: https://github.com/polyas-voting/core3-verifiable-doc/blob/432434bb85ee24e5aa9caaacf3e5e24bc6d50708/pdf/second-device-spec.pdf.

[V824] V8TE: Online voting platform 100% self-service, 2024, URL: https://www.v8te.com/.

[Va22] Valimised.ee: IVXV protocols: Specification (Version 1.8.0), tech. rep., Valimised.ee, 2022, URL: https://web.archive.org/web/20240623062715/https://www.valimised.ee/sites/default/files/2023-02/IVXV-protocols.pdf.

[Va24] Valimised Eestis: IVXV, 2024, URL: https://github.com/valimised/ivxv/.

[Vo24a] Voatz: Voatz secure and convenient voting anywhere, 2024, URL: https://voatz.com/.

[Vo24b] Voxaly: Vote électronique - Voxaly vous accompagne, 2024, URL: https://www.voxaly.com/vote/electronique/.

[VV08] Volkamer, M.; Vogt, R.: Common Criteria Protection Profile for Basic set of security requirements for Online Voting Products: BSI-PP-0037 (Version 1.0), tech. rep., Federal Office for Information Security Germany - BSI, 2008, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0037b_engl_pdf.pdf.

[We24] WeChooz: Vote électronique - Solutions de vote par internet sécurisées - WeChooz, 2024, URL: https://www.wechooz.fr/solution-de-vote-electronique/.

[Wi18] Willemson, J.: Bits or paper: Which should get to carry your vote? Journal of Information Security and Applications 38, pp. 124–131, 2018, DOI: 10.1016/j.jisa.2017.11.007.

[Wi24] Wikström, D.: Open Verificatum, 2024, URL: https://www.verificatum.org/.