



**HAL**  
open science

## **French 2022 legislatives elections: a verifiability experiment**

Véronique Cortier, Pierrick Gaudry, Stéphane Glondu, Sylvain Ruhault

► **To cite this version:**

Véronique Cortier, Pierrick Gaudry, Stéphane Glondu, Sylvain Ruhault. French 2022 legislatives elections: a verifiability experiment. The E-Vote-ID Conference 2023, Oct 2023, Luxembourg City, Luxembourg. hal-04205615

**HAL Id: hal-04205615**

**<https://inria.hal.science/hal-04205615v1>**

Submitted on 13 Sep 2023

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - ShareAlike 4.0 International License

## French 2022 legislatives elections: a verifiability experiment

Véronique Cortier<sup>1</sup>, Pierrick Gaudry<sup>1</sup>, Stéphane Glondou<sup>1</sup>, Sylvain Ruhault<sup>2</sup>

**Abstract:** For the 2022 legislative elections, France made use of Internet voting for a fraction of its voters, namely French voters from abroad. For the first time, France introduced the notion of verifiability and third party. We report here the role of the third party, its interaction with the ANSSI, what it meant in terms of verifiability, as well as its limitations.

### 1 Context

Verifiability is a key property in electronic voting. It requires first a public and detailed specification of the system, as well as means for voters and observers to check that the result properly reflects the votes of the voters. Most academic protocols are verifiable by design, such as Helios [Ad08], Belenios [CGG19], Selene [RRI16], JCJ [JCJ05, CCM08], or Select [Kü16], just to cite a few ones. However, the deployment of verifiable electronic voting in politically binding elections is still an ongoing work in many countries. Switzerland is probably the country that has the most demanding regulation [Ord13], with public specification, open source code, cast-as-intended property, proxy-verifiability, and formally proved protocols. Estonia also relies on a system that offers proxy-verifiability and a cast-as-intended mechanism [HW14], with several associated publications that provide information about the system in use and its limitations [Mu22, SHR23]. Australia also tried to use a somewhat verifiable system, with some cast-as-intended property but at the price of a privacy loss since voters could hear confirmation of their vote by phone [HT15].

France makes use of Internet voting in its political elections only for the Legislative and Consulate elections, and only for the French voters from abroad. We focus here on legislative elections. Internet voting was offered in 2012 and was about to be used in 2017 but finally aborted a few months before the election. The last election for the French parliament happened in 2022, with a total of 577 deputies, out of which 11 deputies are elected by the French from abroad. These 11 deputies can be considered as a small proportion of the French parliament but this is still a high number, especially given the small margin between each party.

The Legislative election is run in two rounds: the first round selects the two (or three) candidates with the most votes and the second round determines the winner between the remaining candidates. Each deputy is elected by voters from a specific geographical area,

---

This work received funding from the France 2030 program managed by the French National Research Agency under grant agreement No. ANR-22-PECY-0006.

<sup>1</sup> Université de Lorraine, CNRS, Inria; Nancy, France

<sup>2</sup> Agence Nationale de la Sécurité des Systèmes d'Information; Paris, France

called *district* (*circonscription*, in French). Voters from abroad are offered three means for voting:

- in person voting: voters attend physical voting stations, typically in consulates. Of course, this may represent a long distance for voters, hence only 22.6% voters voted physically<sup>3</sup>.
- postal voting: voters receive their voting material by post, choose their preferred candidate and return their ballot by post. 0.4% voters used postal voting in 2022.
- Internet voting: voters can vote from any place, using their own voting device (smartphone, computer, tablet). This was the preferred mode of voting with 77% voters using Internet voting, with a total of more than 230 000 votes in the first round, and 270 000 in the second round [Res22].

The election is organized by the MEAE, the French ministry for Europe and foreign affairs. The ministry had a contract with the Docaposte Voxaly company for the Internet voting part, under the technical supervision of ANSSI, the French National Cybersecurity Agency. ANSSI was advising the MEAE for the definition of the desired level of security, as well as during the whole development process and during the deployment phase.

French Internet elections are mainly shaped by an independent entity, CNIL (Commission nationale de l'informatique et des libertés), in charge of protecting data privacy. Since 2019, CNIL has introduced the notion of verifiability in its regulation [CNI19]. For the highest level of security, it requires that the Internet voting system “makes the ballot box transparent to all voters using third-party tools”. This notion of transparency and of third party are not precisely defined in the CNIL recommendations but the CNIL clarified that a “third party” should be outside both the Ministry (MEAE) and the company (Docaposte Voxaly) and should develop its own tool.

In 2021, and on behalf of the MEAE, ANSSI approached academic researchers to act as third party to offer some form of verifiability. The present article has been written by the 3 academic researchers forming the third-party (the first 3 authors) and a member of ANSSI (the 4th author). The 4th author is therefore not part of the third-party. As a member of ANSSI, his role was to offer technical and scientific support to the MEAE, and to assist them in the discussions with the company and with the third-party. In this paper, we describe the role of the third party, what it meant in terms of verifiability and its limitations. The election was run in May and April 2022. However, among the 11 elections, 3 of them were finally canceled early 2023. One cancellation is due to a fraud that is independent from the voting system [Dec23a], the two other ones are due to major technical malfunctioning: for example in the 2nd district, only 11% voters had received their password at the opening of the voting phase, only 38% at the end of the voting phase [Dec23b]. Hence the three elections were re-run in March and April 2023 and with again a third party, and some new findings.

---

<sup>3</sup> The figures are given for the first round of the election. They are similar for the second round.

## 2 Overview of the voting system

The voting system has a basis that is inspired by Helios [Ad08], with the notable difference that the bulletin board is not public.

During a setup phase, an encryption key is constructed, and the corresponding decryption key is split in 14 partial decryption keys. For each partial key, a member of the electoral board (we called them a trustee) is in charge. A threshold mechanism is in place, so that 4 trustees are enough to decrypt. The resulting encryption key is a classical ElGamal public key, based on the Ed25519 elliptic curve.

During the voting phase, the voters use a Javascript client to authenticate, form their encrypted ballot, and send it to the server. The authentication is based on personal data and a password sent over two distinct channels. It is interactive, in the sense that no data is added to the ballot that could prove that it comes from a legitimate voter (similar to Helios, but unlike Belenios [CGG19]).

A ballot is composed of several ElGamal encryptions of bits, together with zero-knowledge proofs of well-formedness, *à la* Chaum-Pedersen. The server collects the ballots and put them in a database, with metadata indicating for which of the 708 precincts this ballot is for. A precinct is a subdivision of a district, that corresponds to a physical polling station. Both electronic and paper ballots are counted in each precinct and then aggregated to provide the results at the level of the district.

At the end of the voter's journey, they are invited to (but not forced to) perform verifiability steps. They can download a PDF file as a receipt ("Récépissé") that contains the following data:

- A hash of the ballot, with a few characters indicating the precinct.
- A signature of this information, using a signing key from the server.
- Another hash of the ballot (that seemed to be unused in the process).
- Links to web services where the data can be verified.

An example of a Récépissé is shown in Appendix.

In total, 3 verification services are linked on the Récépissé. Two of them are hosted by the same entity (the MEAE) as the voting server, which defeats the purpose of verifiability, at least in some threat models. The other one was offered by the third-party auditors, whose role is described more thoroughly in the next section.

The voting phase ends a few days before the day where voters can physically go to a polling station. Voters who have voted by Internet have their names removed from the voter list, and therefore can no longer vote at polling station.

Finally, at the end of the voting day, the trustees meet at the MEAE. At least 4 of them come

to an isolated machine and type a password that unlocks their share of the decryption key and partially decrypt the result. Zero-knowledge proofs of correct decryption are produced as well. More precisely, the technique of homomorphic tally is used. Therefore, the trustees do not decrypt individual ballots but only the results for each of the 708 precincts.

We can remark here that the management of the decryption keys is not fully decentralized, and that a single machine is used for all the trustees during decryption (the same is true during the setup).

### 3 The role of the third-party auditors

The first role of the third-party auditors was to *define* with the MEAE what is the role of a third party. With the help of the ANSSI, they obtained an agreement on three transparency principles:

1. All the documents used for understanding the system and writing the third-party code will ultimately be made public, before the election. This is not as transparent as a fully public system specification but a partial specification of the voting system is now available [Spe22]. This was the first time in France.
2. As third party, no NDA was signed but instead a responsible disclosure clause, that let 90 days to the MEAE and Docaposte Voxaly to fix an issue before publication. The notion of responsible disclosure was new to the ministry and the company in this context.
3. The third party was given access to the ballot box, that is the set of the encrypted ballots. These ballots were treated as confidential material and destroyed a few weeks after the election, as requested by regulation. As a compromise towards a public bulletin board, the third party obtained however the right to publish the hash of each ballot of the ballot box, so that each voter could directly check that their ballot was counted.

Then their role was divided in two main steps:

- some sort of individual verifiability, during and after the election;
- some sort of universal verifiability, after the election.

A webpage<sup>4</sup> (in French, of course) describes the role of the third party to voters, and also gave access to the verification tool and services.

---

<sup>4</sup> <https://verifiabilite-legislatives2022.fr/>

### 3.1 Verifying the tally

The system has no public bulletin board. However the list of ballots, the decryption results, and the associated zero-knowledge proofs form a data set that allows to verify that the results that are claimed on the web site of the MEAE correspond to the list of ballots.

After the tally, the third-party auditors received the aforementioned data, together with the setup information (list of the precincts, list of candidates for each legislative district, the 14 partial public keys). Based on the public documentation that describes the format of the ballots, a command-line tool was written to perform the following operations:

- Check the consistency of the partial public keys;
- Check the validity of the zero-knowledge proofs in each ballot;
- Compute the homomorphic composition of the ballots, for each precinct;
- Check the validity of the zero-knowledge proofs for the decryption;
- Check (manually) that the result corresponds to what is announced on the official web site of the Ministry, at the district level;
- Compute the list of hashes of the ballot, exactly as they should appear on voter's Récépissé;
- Publish this list, and a report on all the checks.

This verification tool, called VVFE, is made publicly available as a git repository<sup>5</sup>, under a free software license. Even though the voters or external auditors can not run this code themselves, since the board is not public, this improves transparency and complements the specification.

The system is similar to Helios / Belenios, and the specification is actually close to that of Belenios, when it comes to the structure of the zero-knowledge proofs. Therefore, it was natural to start from the Belenios source code, and VVFE is a derivative of (part of) Belenios. At that time, Belenios did not have support for elliptic curves. It was using multiplicative groups of finite fields. Everything was in place to be able to switch from one group to another, and therefore adding elliptic curve support to VVFE was not too costly.

For efficiency reasons, on the server side, the `Libsodium` library was used for the critical function that does scalar multiplication on the Ed25519 curve. Bindings for this library in OCaml were added. The dedicated off-line machine that was used for the verification is a 10-core Intel i9-10900K. A single core of this machine can perform 12,000 elliptic scalar multiplications per second. The benchmark tool of VVFE allows to run a test with a fake election setup that includes 15 to 20 candidates per district, which is typical for the first round. With this setup, the whole election verification with 100,000 ballots takes 7 minutes and 56 seconds (using all available cores on the machine). It could be deduced that all the

<sup>5</sup> <https://gitlab.inria.fr/vvfe/vvfe>

checks for the first round of the election could be done in about half an hour, which was indeed the case.

We remark that the elliptic curve code written for VVFE was integrated back into Belenios a few months after.

It was necessary to check manually that the results of each of the 11 districts correspond to what is announced on the official web site of the Ministry. For verifiability purposes, it would have been better to perform this check for each of the 708 precincts but of course, this is no longer possible manually. Unfortunately, automating these checks was not possible for these elections since even the format of the results varied from one precinct to another.

**Lesson learned 1:** *In order to obtain verifiability up to the detailed results provided to the public, it is necessary to develop an API or at least machine-readable results, while ensuring that voters and machines are reading the same data.*

### 3.2 Individual verifiability

During the election, the third party only had the server verification key. A service was offered to voters in order to check that the signature they received after voting (in their Récépissé) was indeed a valid signature from the Server. This forms a commitment from the system to the voters: if their signed ballot does not belong to the final ballot box, they hold a cryptographic proof that the Server misbehaved.

After the election, the third party were given the ballot box for each district. As mentioned earlier, the hash of each ballot was published so that voters can control that the ballot box contains their ballots. For usability reasons, a service was offered to allow voters to check that the hash appearing on their Récépissé was part of this set of hashes. The validity of the Server signature was also checked, although this was no longer necessary after the tally. Note that voters could also download the list of hashes from the third-party server and check directly that hashed ballot appeared inside.

This service was hosted on the webpage<sup>6</sup>. The underlying cryptographic code simply consists in a signature check and was also published as part of the VVFE tool. Figure 1 displays a screenshot of the online tool for verifying a ballot after the election.

## 4 Which verifiability properties are targeted?

In the MEAE terminology, the third-party auditors guaranteed individual and universal verifiability. With respect to the usual academic terminology, their role was more restricted. Note that the third-party auditors did not play any role w.r.t. vote secrecy.

<sup>6</sup> The service was available from <https://verifiabilite-legislatives2022.fr/>, but is no longer active.



Fig. 1: Screenshot of the verification service for voters.

*Individual verifiability.* The system in use does not offer any cast-as-intended verification mechanism, hence the voting client has to be fully trusted. On the other hand, the system offers the usual recorded-as-cast property: a voter can check that their ballot belongs to the ballot box, thanks to the fact that the list of hashed ballots of the ballot box was published.

*Universal verifiability.* Since neither the ballot box nor the zero-knowledge proofs are public, the system cannot claim universal verifiability. Only the third-party auditors selected by the MEAE, could verify the zero-knowledge proofs. The process was not opened to other entities. Moreover, the system does not provide any form of eligibility verifiability: the Server has to be trusted regarding the fact that the ballots all came from legitimate voters. Third-party auditors can not check whether some ballots had been added.

In conclusion, we would say that the system offers recorded-as-cast verifiability and proxy tallied-as-recorded verifiability. This is true up to the attack found by Debant and Hirschi [DH23], as explained in Section 6.1.

## 5 Retrospective

### 5.1 During the development phase

The third-party auditors were hired at a late stage of the process (during Fall 2021, for an election running in June 2022). Furthermore, they first had to discuss with the MEAE and the ANSSI about their precise role.



A first difficulty came from the fact that the (partial) specification that was required to write an independent software was not stabilized. Details that would have been easy to figure out in an open-source setting were difficult to fill-in. An example of this situation is given by the byte-encoding of the various data that must be hashed in the zero-knowledge proofs (in the Fiat-Shamir setting). The encoding of large integers is not the same everywhere, and the field separator is not always the same character. The third party had access to a few test data, but when the check fails, the combinatorics of all possible plausible encoding choices was too large.

This sounds like a simple problem to solve: just ask the developers. This leads to a second difficulty: the third party did not have a direct communication channel with the developer team at Voxaly, and had to communicate via the project manager, who was very busy with other important issues, at this late stage of the project.

The general impression was that even at the last minute, the process was not yet fully settled and that there was room for mistakes on D-day. We give two examples of remaining imperfections that were mentioned to the MEAE but were not fixed, due to time constraints:

- The character encoding of the files that are sent to the third party varies. From one test to the other, or even, in the real election, from one round to the other, the same file is sometimes encoded in UTF-8, and sometimes in ISO-8859-1. This is visible in particular in the file that contains the general information about the election, with the names of the candidates that contain accents.  
The VVFE software was made robust to this kind of change.
- For a given round of an election, the third party first receives the general information before the election starts, and then receives the ballots, after the election ends. These two transmissions both contain a file that describes the public key of the server that signs the ballots. During the 2023 elections, during the tests and at each round, the public key was wrong during the second transmission.  
The third party decided to work around this, but failed to do so during the first round. This led us to observe the behaviour of the voters when verifiability failed. See Section 6.2.

<p><b>Lesson learned 2:</b> <i>Integration of verifiability should be done at the beginning of the process, in order to avoid a last-minute rush, that can lead to anomalies.</i></p>
---

## 5.2 Statistics

As explained in Section 3, a service was offered during the election in order for voters to check that their ballot has been counted. Before the tally, since the ballots were not yet known, it was only possible to check that their ballot was correctly signed by the server. After the tally, the service could check that their ballot was in the ballot box of their district. The MEAE offered a similar service, except that, since they were also hosting the voting

server, they also checked that the ballot was in the ballot box during the voting phase. Of course, in some threat models, having the same entity running the server and verifying the presence of ballots does not bring additional guarantee.

We report in Table 1 the number of verifications made by voters during the election (signature verif) and after the election (ballot verif), using the verification service. For comparison, we also give the figures provided by the MEAE service. No misbehavior from the server was detected during the verification, that is, no discovery of any correctly signed ballot that does not appear in the ballot box. We can note that there are much more visits of the verification page than the number of successful verifications. We see several explanations: voters (or even robots) may access the webpage and stop there. Moreover, the verification may fail due to bad copy-paste or simply voters playing with the interface.

	1st round	2nd round
# of votes	237379	273927
# of MEAE verifs	40148	37174
# of 3rd-party verif visits	3150	2064
# of 3rd-party successful signature verifs	603	324
# of 3rd-party successful ballot verifs	357	68

Tab. 1: Number of verifications made by voters during the 2022 French legislative elections. The last three lines report the usage on the third-party verification service. Signature verifications occur *during* the election, full ballot verifications occur once the election is tallied.

The main lesson learned is that very few voters successfully verified their ballot using the third-party service (less than 1%). Unsurprisingly, this is even lower if we count only the voters who returned after the election. In comparison, the MEAE service has a 17% verification rate<sup>7</sup>. Note that figures given by the MEAE may count the total number of accesses to their verification service (be it successful or not). The fact that the MEAE service was much more used than the third-party service could be explained by the fact that this service was the first proposed service on the Récépissé given to voters. It was probably hard for voters to understand why it would be meaningful to verify their ballot twice. This gives some hope that a third party could be much more used if better advertised. Note that anyway, the MEAE service provides less guarantee in the sense that if the service is trusted for verifiability then it should also be trusted to keep the received ballots.

**Lesson learned 3:** *Very few voters used the third-party service. But a better publicity could make a big change. Why not having the third-party service(s) be the only one(s) pointed to voters, or at least be the one(s) publicized in priority?*

One can also notice that voters verified less during the second round, while the participation

<sup>7</sup> All the figures from the MEAE service have been provided by the MEAE to the third party.

was similar (even slightly higher). This may come from the fact that voters were reassured by their verification during the first round and did not see the point of verifying again during the second round.

## 6 Verifiability issues

### 6.1 The attack of Debant and Hirschi

The verification service assumes that the voting client is honest. This was made clear to voters on the third-party website. However, the third-party auditors implicitly assumed that the behaviour of the voting client was close to the behaviour of the Helios or Belenios voting clients. Debant and Hirschi [DH23] performed some reverse-engineering of the voting client and discovered that the hash of the ballot was sent back and forth between the voting client and the Server, leading to the following flaw: the voting client did not check that the hash of the ballot displayed to the voter was the one corresponding to the actual ballot of the voter. Moreover, the Récépissé (a pdf) offered to the voter was entirely generated by the Server, with no check from the voting client. Hence a dishonest Server could easily drop the voter's ballot and send a (valid) Récépissé for another ballot, encrypting a vote of its choice. Note that the paper from Debant and Hirschi [DH23] also reports flaws w.r.t. ballot secrecy, that we do not discuss here.

**Lesson learned 4:** *A partial specification is unsafe. At the very least, the specification of all trusted components should be provided.*

**Lesson learned 5:** *Publishing a specification a few weeks before the election is risky. In case flaws are discovered, there is no time to fix them.*

Of course, all the flaws reported in [DH23] need to be corrected.

### 6.2 Rerun in 2023

The results of legislative elections were canceled in three districts, hence the election was re-run in March and April 2023 for these three districts, with again a third-party auditor. The setting was very similar, with two main differences, from the verifiability point of view.

First, the attack from Debant and Hirschi [DH23] was fixed in the sense that the voting device now displays the hash of the ballot, *as computed by the voting device* as well as the hash received from the server. The voter is invited to check that the two hashes are equal (they are displayed on the same screen). However, the Récépissé is still generated by the Server. An informed voter can check that the same hash appears on the Récépissé but is not

instructed to do so. The voter is not instructed either to keep a copy of the hash displayed by its voting device.

Second, since very few voters return to the verification service after the election, it was decided to capture all valid signatures of ballots verified by voters during the election. It was then possible, after the election, to check that all verified ballots were present in the received ballot box. This way, voters do not need to come back after the election and their verification during the election is as powerful as the one after the tally.

We report in Table 2 the number of verifications made by voters. The number of verifications was again very low. No misbehavior from the server was detected.

	1st round	2nd round
# of votes	26667	28574
# verif visits	534	442
# of successful signature verifs	20	27
# of successful ballot verifs	3	2

Tab. 2: Number of third-party verifications made by voter during the 2023 French legislative elections. Signature verifications occur *during* the election, full ballot verifications occur once the election is tallied.

However, the verification service did not properly function w.r.t. the first round during 11 days after the election. Indeed, once the election is tallied, the third-party auditors received the ballots and checked that the results of the election correspond to the ballots, thanks to the zero-knowledge proofs. The set of hashes of ballots was then published on the third-party webpage. While uploading the set of hashes, the third-party auditors also wrongly updated the Server verification key with an invalid one, given by mistake by Docaposte Voxaly, as explained in Section 5.1. Hence, voters that verified their ballot of the first round after the election got an error message, saying that the signature was invalid, while this was not the case.

Interestingly, the analysis of the log showed that 18 voters (only) did encounter this error message. In principle, they should all have vigorously complain since their ballot was valid. Only 1 out 18 voters filled a form to complain. One week later, the complaint was correctly identified as a signature issue and the third-party auditors were notified. They fixed the incorrect verification key one hour later.

**Lesson learned 6:** *Voters do not complain! This unfortunate real-life experiment shows that verifiability is not enough. Even when voters are in position to detect a potentially severe issue, they do not complain.*

## 7 Conclusion

The French 2022 legislatives introduced the notion of verifiability for the first time in France, for politically binding elections. Verifiability was still limited: no cast-as-intended nor eligibility verifiability. However, third party auditors could check the tallied-as-recorded property and offered individual verifiability to the voters, up to the attack found by Debant and Hirschi [DH23], partially fixed in 2023. Moreover, and for the first time, the specification of the system was made partially public. We believe that this 2022 election forms an important step towards full verifiability in France. We hope that this effort will be pursued and amplified in the next years.


We note that France made the choice of proxy-verifiability rather than universal verifiability. This is also the case in Switzerland and Estonia for example. It seems that election authorities of national elections are reluctant to publish the encrypted ballots because of a possible loss of vote privacy, in case decryption keys are lost, or in case a weak random generator is used on the voter side [Gj16]. On the other hand, in order to achieve full verifiability, publishing some data related to the ballots seems unavoidable. This data does not necessarily leak information about the voters and may even hide the votes in an information-theoretical way [CPP13]. What can be disclosed on a public board, for national political elections, will certainly continue to be discussed in the next years.

## Bibliography

- [Ad08] Adida, B.: Helios: Web-based Open-Audit Voting. In: USENIX'08. pp. 335–348, 2008.
- [CCM08] Clarkson, M. R.; Chong, S.; Myers, A. C.: Civitas: Toward a Secure Voting System. In: IEEE Symposium on Security and Privacy (S&P'08). IEEE Computer Society, pp. 354–368, 2008.
- [CGG19] Cortier, Véronique; Gaudry, Pierrick; Gloudu, Stéphane: Belenios: A Simple Private and Verifiable Electronic Voting System. In: Foundations of Security, Protocols, and Equational Reasoning: Essays Dedicated to Catherine A. Meadows. Springer International Publishing, pp. 214–238, 2019.
- [CNI19] CNIL recommandations. 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, <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038661239>.
- [CPP13] Cuvelier, Edouard; Pereira, Olivier; Peters, Thomas: Election Verifiability or Ballot Privacy: Do We Need to Choose? In: 18th European Symposium on Research in Computer Security (Esorics 2013). LNCS. Springer, 2013.
- [Dec23a] Décision n° 2022-5773 AN du 3 février 2023, <https://www.conseil-constitutionnel.fr/decision/2023/20225773AN.htm>.
- [Dec23b] Décision n° 2022-5813/5814 AN du 20 janvier 2023, [https://www.conseil-constitutionnel.fr/decision/2023/20225813\\_5814AN.htm](https://www.conseil-constitutionnel.fr/decision/2023/20225813_5814AN.htm).

- [DH23] Debant, Alexandre; Hirschi, Lucca: Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol. In: Usenix Security. 2023.
- [Gj16] Gjøsteen, Kristian: E-voting in Norway. CRC Press, 2016. Chap. 5 in Real-World Electronic Voting: Design, Analysis and Deployment.
- [HT15] Halderman, J. Alex; Teague, Vanessa: The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election. In: 5th International Conference on E-Voting and Identity, VoteID 2015. LNCS. Springer, 2015.
- [HW14] Heiberg, Sven; Willemson, Jan: Verifiable internet voting in Estonia. In: EVOTE' 14. IEEE, 2014.
- [JCJ05] Juels, A.; Catalano, D.; Jakobsson, M.: Coercion-Resistant Electronic Elections. In: Workshop on Privacy in the Electronic Society (WPES'05). ACM, pp. 61–70, 2005.
- [Kü16] Küsters, Ralf; Müller, Johannes; Scapin, Enrico; Truderung, Tomasz: sElect: A Lightweight Verifiable Remote Voting System. In: 29th IEEE Computer Security Foundations Symposium (CSF' 16). pp. 341–354, 2016.
- [Mu22] Mueller, Johannes: Breaking and Fixing Vote Privacy of the Estonian E-Voting Protocol IVXV. In: Workshop on Advances in Secure Electronic Voting 2022. 2022.
- [Ord13] Ordonnance de la ChF sur le vote électronique (OVotE) du 13 décembre 2013 (Etat le 15 janvier 2014). Chancellerie fédérale ChF.
- [Res22] Élections législatives - Résultats du 1er tour pour les Français de l'étranger. <https://www.diplomatie.gouv.fr/fr/services-aux-francais/voter-a-l-etranger/resultats-des-elections/article/elections-legislatives-resultats-du-1er-tour-pour-les-francais-de-l-etranger>, Last visited on July 3rd 2023.
- [RRI16] Ryan, Peter; Rønne, Peter; Iovino, Vincenzo: Selene: Voting with Transparent Verifiability and Coercion-Mitigation. In: Voting'16. pp. 176–192, 2016.
- [SHR23] Sutopo, Anggrio; Haines, Thomas; Roenne, Peter: On the Auditability of the Estonian IVXV System and an Attack on Individual Verifiability. In: Workshop on Advances in Secure Electronic Voting 2023. 2023.
- [Spe22] MEAE – Vérifiabilité – Spécifications v1.0. [https://www.voxaly.com/wp-content/uploads/VOXALY\\_LEG2022\\_Verifiabilite\\_Specifications.pdf](https://www.voxaly.com/wp-content/uploads/VOXALY_LEG2022_Verifiabilite_Specifications.pdf).


## A Example of a voter's Récépissé



MINISTÈRE  
DE L'EUROPE  
ET DES AFFAIRES  
ÉTRANGÈRES

*Liberté  
Égalité  
Fraternité*

### Elections législatives 2022 1er tour

 **Preuve de dépôt du bulletin de vote dans l'urne**

Voici la preuve de dépôt de votre bulletin dans l'urne.

Votre bulletin de vote a bien été introduit dans l'urne électronique.

La référence ci-dessous vous permet de contrôler que votre bulletin est bien dans l'urne.


**80011&1&3318f83ea80861c9e6274f049c8df87c2da4fe03e43b7aa46b71  
92c0cfc3129c53**

[Pour contrôler la référence de votre bulletin : cliquez ici](https://votefae.diplomatie.gouv.fr/pages/verifierEmpreinte)  
<https://votefae.diplomatie.gouv.fr/pages/verifierEmpreinte>

Une fois le dépouillement effectué, vous pouvez vérifier que votre bulletin a bien été pris en compte dans le calcul des résultats, à l'aide d'un outil tiers développé par le CNRS, conformément aux exigences de la CNIL en matière de transparence de l'urne. Pour ce faire, vous devrez renseigner le cachet électronique ci-dessous.

[Vous pouvez accéder à l'outil en cliquant ici.](#)

Ce cachet électronique vous permet également de vérifier que votre preuve de vote a bien été produite par le système de vote homologué.



```
eyJpbmZvU1U1OiI4MDAxMkxwZDF1cmVfQ21yY29uc2NyaXB0aW9uX2Rlc19GcmFuY2Fpc19kZV9aJ2V0cmFuZ2VyFDE  
wOXwzMcE4ZjgzZWE4MDg2MmM5ZTYyZmRmMDQ5YzhkZjg3YzkyYTRmZTAzZTQzYjdhYTQ2YjcxOTJjMGNmYzZmMjIjFj  
UzI1w1c2Noem9yci161jFzAwAaTVZOHQzMGs3NXZhbnZhtWhic2924tc1bGE3WQ2cX8aemNoXZlajU5c2tub3E1W  
TRsdVWkMG9zc2E5YmGtqWRtOWUxa2M3MDFaMXRPMWc0bTQza2w4am5qM2hmNmFyNWg4dCIaInBlYm9pY0tleVNI1joi  
LS0tLS1CRUdJTi19WRVJRk1lDQVRJT05fS0VZLS0tLS1cc1xunZmYTM0ZTQ0YVwqZG14ZDkxMDg1MmQ4Y2U0ODNkZc  
OYTYmYTRmOTNhMmRlYzRhNjRmNzhmMGFjZmI2NDJjOCUzNjYxNmVlNTUxMzY2OWJmZDE2Y2d1Y2NiZmMzY2Q1NmM3MD  
UyMzh1YzksOFRhNDMOM2QwZTgzOWVjNjM3OTVhX2R1c292LS0tRU5EX1ZFUk1GSUNBE1PT19LRVktLS0tLS1SImNsZ  
UNhY2h1dEJydkQ1O11yOSJ9
```

[Pour contrôler le cachet électronique, cliquez ici](https://votefae.diplomatie.gouv.fr/pages/verificationCachetServeur)  
<https://votefae.diplomatie.gouv.fr/pages/verificationCachetServeur>

La valeur chiffrée de votre bulletin de vote ci-dessous vous permet de vérifier que le contenu de votre bulletin de vote est identique tout au long du scrutin. Cette valeur est à comparer avec celle obtenue en vérifiant la présence de votre bulletin dans l'urne.

b4e49757a5ae4cf256e5466a5d7e04476b31186a89ba02773549e68524f8181e