UCL Université catholique de Louvain

École polytechnique de Louvain (EPL)

epl

Postal Voting

Dissertation presented by
Thierry Abeels

for obtaining the master's degree in
Cyber Security

Supervisor
Olivier Pereira

Readers
Edouard Cuvelier, Yves Deville, Henri Devillez

Academic year 2020-2021

1. Abstract

Voting is a fundamental element within our democratic countries. We here focus on remote voting, an alternative option for those who are unable to get to the voting booths on the specific voting date. The COVID-19 pandemic reminded how remote voting is vital for our democracies and therefore we find that securing this process is of the highest concern.

This study proposes state-of-the-art postal voting-related approaches and how security improvements can be addressed, specifically for the Belgian Federal elections for citizens living abroad. This study focuses on the Vote-by-Mail options for which four possible scenarios are studied, where three of them do include End-2-End verifiability for paper-based ballot voting, by relying on cryptographic features, and some of them relying for citizen authentication on the Belgian e-ID card.

The first scenario is a detailed illustration of a typical traditional Vote-by-Mail solution, to describe the fundamentals which will be used for the other 3 scenario explanations.

The second scenario is a personal proposal, inspired/derived and elaborated from the US ElectionGuard (Benaloh, 2021) and STAR-Vote (Bell, 2013) voting systems, applied to the Vote-by-Mail case.

The third scenario is a paper-based solution, named STROBE-Voting (Benaloh J., Sept. 2021), with some personal adaptations for the Belgian election's specificities, as the STROBE-Voting was initially developed for the US election case.

The fourth scenario was proposed by a Belgian inter-university consortium for the NETVOTING_BE (part 2) study (Pilet J.B., 2021) in which an innovative Vote-by-Mail solution has been described.

Revision history

Version	Date	Author	Comments / description of changes
1.0	22/08/2021	Thierry Abeels	Initial final version

Table of Contents

2. Introduction

Voting is a fundamental element within our democratic countries.

Remote voting is also coming back as a hot topic in different countries in the latest months, due to the COVID-19 disease. The goal of remote voting is to involve remote citizens within their originating democratic system.

Some key recent political communications have highlighted the specific attention on this topic:

- In November 2020, Mrs Wilmet (Belgian Minister of Foreign affairs, European affairs and Foreign trade) expressed, within her new policy brief (Wilmet S., 2020), a new development axis on e-consul portal in order to allow Belgian foreign residents to register for voting, and to develop new e-voting like possibilities.

- In March 2021, within a joined interuniversity study (Pilet J.B., 2021), Mr Pereira (UCLouvain) proposed an innovative Postal Voting option to the Belgian SPF Ministry of Interior.

The goal of this study is to provide a status on the Postal Voting approaches, and to propose some future evolutions while highlighting some key practical attention points.

This will include:

- An historical and international contextual overview
- A description of different possible Postal Voting options
- A Comparison table of the studied Postal Voting options
- Citizen's identification options, current limitations, and some proposed improvements
- Conclusion

Within the literature, Postal Voting and Vote-by-Mail (VbM) terms are used. We here considered both terms as related to the same concept.

3. Historical and international contextual overview

3.1. International conventions elections history

Free elections are linked to one of the fundamental rights of the United Nations Human Rights convention (UN-HR, 1966), signed by the Belgian authorities in 1968, cfr article 25 (b):
Every citizen shall have the right and the opportunity, without unreasonable restrictions:
(b) To vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors.

While respecting the particularities of their political system, many countries have incorporated this right to vote and its principles into their national laws, their charters of rights or their constitutions. Various intergovernmental and non-governmental organizations, mobilized around the cause of promoting the rule of law and democratic and pluralist governance, have enriched and concretized these concepts and principles through concerted commitments on elections and the exercise of the right to vote. This is particularly the case of the Venice Commission of the Council of Europe (Venice, 2012), the Organization for Security and Cooperation in Europe (OSCE, 2007), the Foundation International for Electoral Systems (IFES) and the International Institute for Democracy and Electoral Assistance (IDEA, 2010). (Elections Quebec, 2020).

Within the current literature, and worldwide governments references, one of the most used definition is taken from the OSCE organization, and more specifically its "Copenhague document" (OSCE, 1990):
It outlines commitments on democratic elections, rule of law and other fundamental rights and freedoms:
"In order to strengthen respect for, and enjoyment of, human rights and fundamental freedoms, to develop human contacts and to resolve issues of a related humanitarian character, the participating States agree on the following:
...
(5.1) — free elections that will be held at reasonable intervals by secret ballot or by equivalent free voting procedure, under conditions which ensure in practice the free expression of the opinion of the electors in the choice of their representatives;"

OSCE is perceived as a reference in this matter, and is often invited to observe elections correctness, including for the latest 2020 US presidential election (OSCE, 2020).

Within the western democracies, free elections are a key element and those principles are very well detailed in a recent Quebec publication (Elections Quebec, 2020):
In Western societies, elections are at the heart of representative democracy and are inseparable from the political, cultural and historical context in which they take place. In general, political systems and governance modes are meant to be inclusive, egalitarian and democratic. But it hasn't always been that way. Over time, many people mobilized and led a struggle relentlessly to extend the right to vote (based on universal suffrage, equality and the uniqueness of its exercise) to all citizens, regardless of their gender or their social situation. With a clear intention to strengthen freedom politics and democracy, this struggle has gradually led to the recognition of the vote as a fundamental right within different societies. Nowadays, the authority and legitimacy of public powers rest on the will of the people, who express themselves, freely and by secret ballot, in an electoral process that is accessible, egalitarian, transparent and with integrity. Elections must respect the principles underlying a democratic vote and use means that guarantee their implementation, regardless of the suffrage modalities expression. Postal voting and Internet voting should be bounded to the above described obligations.

Western area in this context is not linked anymore to a European geographical area, but "*More than a region or a relative indication in space, the West is a form of society, a set of beliefs and attitudes that have shaped its history and supported its economic and political expansion. It is no longer just the countries of Western Europe that represent the West, but also the United States, Canada, Australia. It is, in fact, a representation, that is, an idea that serves to interpret what is happening."* (Droit R.-P., 2008).

3.2. Remote voting and Postal voting history

In 2020 as COVID-19 came and disturbs some of the planned elections organization. Postal voting was then suddenly one of the options for some of key elections:

- In the USA (Presidential election) for example, we saw a massive increase of postal voting usage in 2020: more than 65 M postal votes, out of a total of more than 158 M votes (University of Florida, *The Elections project*, 2020).
- In Germany (Bavarian local elections), the last election was completely moved in March 2020 to postal election (Wagner R., 2020).

Those were just illustrations of some possible options of remote voting, which are in fact not a new concept.
Remote voting does include postal voting, also called vote-by-mail (VbM), and some other approaches like for example e-voting solutions. IDEA (Institute for Democracy and Electoral Assistance) covered an in-depth worldwide and historic study about those different available options (Braun N. & all, 2007). According to this study, which does include a full survey of the history of external voting, different historical examples are mentioned (p 41-44):

- *The first use of external voting appears to have been put in place by the Roman emperor Augustus, who is said to have invented a new kind of suffrage under which the members of the local senate in 28 newly established colonies cast votes for candidates for the city offices of Rome and sent them under seal to Rome for the day of the elections*.
- In 1862, the state of Wisconsin *enacted provisions to allow absentee voting by soldiers fighting in the Union army during the Civil War*.
- *Outside the military context, New Zealand introduced absentee voting for seafarers in 1890*.
- *Australia adopted it in 1902, although under operating arrangements which made its use outside Australia practically impossible*.
- And other examples are further illustrated and commented in this interesting paper.

In the USA, a very detailed study was published in 2018 by the National Academy of Sciences on "Securing the Vote" (National Academies of Sciences, Engineering, and Medicine, 2018). This study does cover the full history of US voting, describes the different possible issues, propose different actions to improve the current US voting organizations and processes. Within this study, human-readable paper ballot was recommended as currently the most advised option (p 80) for the 2020 presidential election: "*Elections should be conducted with human-readable paper ballots. These may be marked by hand or by machine (using a ballot-marking device); they may be counted by hand or by machine (using an optical scanner). Recounts and audits should be conducted by human inspection of the human-readable portion of the paper ballots. Voting machines that do not provide the capacity for independent auditing (e.g., machines that do not produce a voter-verifiable paper audit trail) should be removed from service as soon as possible. Every effort should be made to use human-readable paper ballots in the 2018 federal election. All local, state, and federal elections should be conducted using human-readable paper ballots by the 2020 presidential election*"
This paper provided also clear recommendation for the vote by mail (p 69): "*All voting jurisdictions should provide means for a voter to easily check whether a ballot sent by mail has been dispatched to him or her and, subsequently, whether his or her marked ballot has been received and accepted by the appropriate elections officials*". In March 2021, the US National Intelligence Council released a new document which describes the different recent attempts made during the latest 2020 US presidential election (NIC 2021). Influencing election results attempts game did not come to an end yet.

In the Netherlands, in November 2020, an NGO "Stichting Tegen Hackbare Verkiezingen", led by academics and experts wanted to shed the light on the current risks related to electronic voting systems, and to persuade their authorities to rely on paper ballots with manual counting for the coming elections. They published a very interesting and argued document (STHV, 2020).

In Belgium, in December 2020, an inter-university study (Pilet J.B., 2020) was conducted on behalf of the Federal Belgian authorities (Belgium, 2020). The goal was to study the feasibility of introducing the vote by internet for local citizens, and citizens living abroad. According to this study, full internet voting is not mature yet for the

2024 elections and could be possible for the 2034 elections. Starting on page 157, this study insists on postal voting option as an important initial step towards full internet voting. This path is recommended especially as it could combine some on-line capability and would help the citizens to be familiarized with a partial on-line voting process.

In May 2021, the French Senate published a very detailed study « *Législation Comparée – Recueil sur le droit Electoral (Vote par correspondance – Modalités d'inscription sur les listes électorales – Vote électronique)* » (French Senate, 2021)
This study is covering from another perspective the current remote voting options, projects and encountered issues in different countries (Australia, Austria, Belgium, Denmark, Estonia, Finland, Germany, Great Britain, Ireland, Italy, the Netherlands, Portugal, Spain, Sweden, Switzerland and United-States). This is one of the two the most recent international studies on this topic which is comparing the pro-and-con of the current respective countries voting evolutions plans. The other very interesting one being the "Vote par Internet – Etude en contexte Québécois" led by "élections Quebec" on behalf of the Quebec parliament (Elections Quebec, 2020).

According to those different studies, papers ballots is currently the safest way, while we should take all possible attentions to protect the different steps involved in the voting process.

3.3. Postal Voting concepts introduction

As our study will focus on the Vote-by-Mail options, we propose first to describe it with a typical example of the full postal voting process that can be illustrated from the Switzerland approach (Killer C., 2019) p90, where the different steps, actors and threats are clearly mentioned:

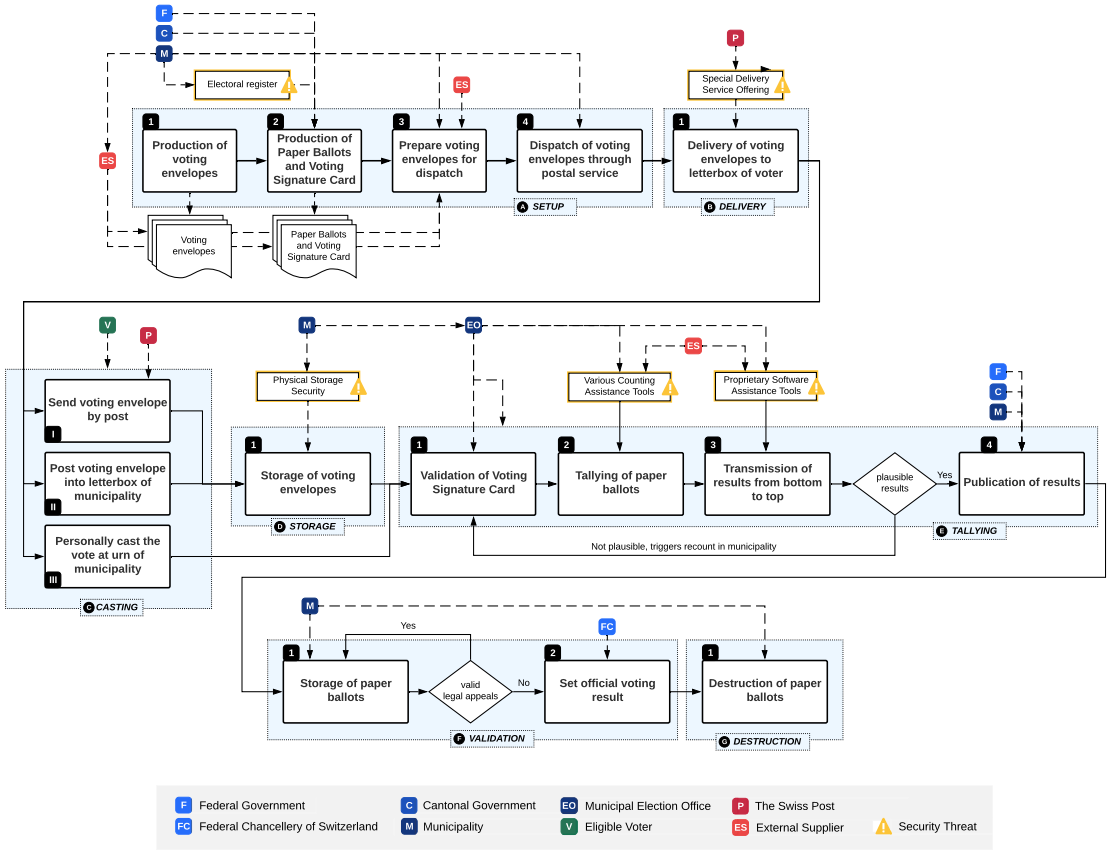


Figure 1: Switzerland Paper Voting Process Flow (PVPF)

Typical postal voting ballot approaches is illustrated here after, as extracted from (Killer C., 2019) page 95.

C. Killer, B. Stiller

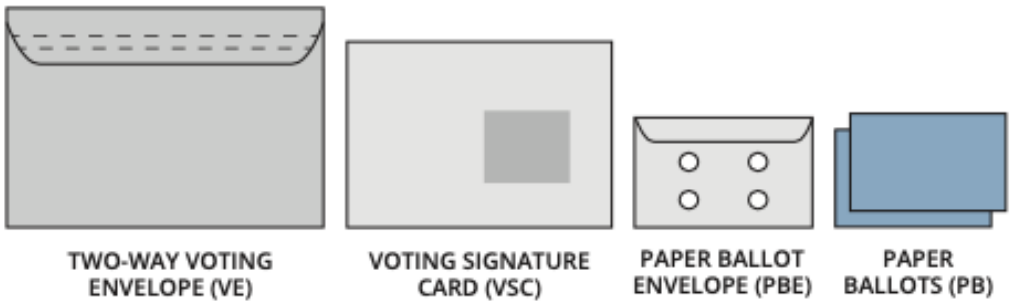


Figure 2: Abstract representation of the necessary voting paper artifacts

Voting Signature Card (VSC) is illustrated in Figure 2 from the Swiss approach. Within the UK approach, the VSC is replaced by a “Postal Voting Statement” which needs to be filled in (including date of birth AND signature).

The goal of the present study is to add cryptographic components within the process illustrated in Figure 1, which will allow each voter to ensure his/her ballot has been well received, accepted, and processed by the election officials. Additional techniques could also be added, like photo of the received envelope (like current Belgian bpost scan/picture solution), which would allow the citizen to verify the integrity of his/her vote by checking for example for example the post stamp (including date & location) mentioned on his voting envelope.
Another additional step could be foreseen to check whether the ballot sent by mail has been dispatched to her or him (like for any classical registered mail).

Adding some cryptography to postal voting solution is not a full new concept. In 2013, Josh Benaloh, Peter Y.A. Ryan, and Vanessa Teague have already published a detailed paper on this subject, and a very good powerpoint presentation to illustrate their proposal (Benaloh J., 2013).

The added cryptography and other security aspects to the postal voting will improve the global reliability of the remote voting process, even if this will not solve all possible issues illustrated in the UK parliament report (Pickles E., 2016).
Example: Coercion, vote buying, or family voting is typically a risk which remains. Those kinds of risks are present for all remote voting options.
That's why some countries do allow remote voting for specific cases only (people living abroad, exceptional circumstances (like COVID-19 in 2020 Bavarian elections)).

For ballot delivery to the voter, some countries (like the Netherlands) do propose a self-print option (Baruch B. p 8), and this also an option proposed in the Belgian study (Pilet J.B., 2020). This option speed-up the process but may add additional risk (risk of ballot copy). This report (Baruch B., 2018) does also illustrate that *UK uses scanning machines to validate signatures in postal voting* (Baruch B., 2018, p8). This document provides a very detailed state about remote voting as it was in 2018. The described situation should probably be updated after the latest COVID-19 crisis, as for example the postal voting usage scale in such kind of crisis.

Postal voting is not limited to the voting act, but it is a whole process. Like ITIL processes definition have been initially mainly developed from the UK, in 2003-2004 the House of Commons (UK) has produced a whole report about Postal Voting and the related processes (The House of Commons, 2004). This includes the different procedures, the electoral security aspects which does cover the declaration of identity, the voter registration, the different kind of verification, a national database of electoral offences.
This report is very useful as it is not only describing the processes but provides also detailed data on past experiences and issues encountered, including suggestions how to increase voter turnout (p 15).

Australia, due to its specific broad geography, has a very detailed procedure accessible to each citizen, and clear registration form. The light design does help the clear citizen comprehension (AEC, 2020), and could be an inspiration for our future elections for our non-resident citizens.

The most recent and highlighted postal voting election case was the last November American president election.
MIT-Stanford published a paper recently (October 2020) within their "Healthy Elections Project" called "Behind the Scenes of Mail Voting: The Rules and Procedures for Signature Verification in the 2020 General Election".
The US case is specific as its mail voting is decentralized (county based), meaning each county may have different approaches for signature verification, based on their respective sizes. Different control examples, statistics across different states are provided. Even small size county may have pragmatic processes, like in Wakulla County (Florida), (Bloomgarden A. (2020), p 13).

And finally, I advise to discover *Josh Benaloh* point of view about the possible voting evolution (including mail) published during an interview published in July 2020 in "The New Yorker" newspaper (Halpen S., 2020):
"*I'm not going to claim that we have any way of securing elections, and that's a problem*,"
"*We've got an asymmetric battle with nation-state actors who are attacking little counties, and they can destroy data and they can corrupt data and they can do all sorts of things. But I am claiming that adding end-to-end*

verifiability makes any tampering with the data detectable—and not just by election officials, but detectable by you and me and candidates and news media and anybody else. And that's a real value."
Benaloh is making here a reference to his ElectionGuard initiative (Thornton A., 2020).

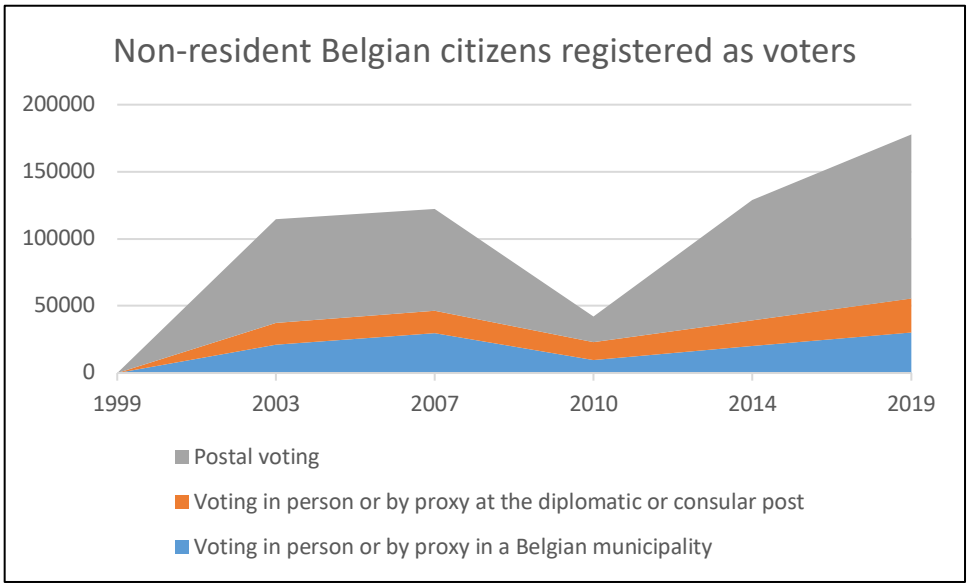
Allowing remote citizens to participate in our democratic elections while avoiding fraud through possible tampering detection, that's the goal of this project initiative.

4. The current Postal Voting project

The context of this Postal Voting project is driven by the Belgian Federal elections which do occur every 5 years (the next ones will be held in 2024), and more specifically for their citizens living abroad.

This is typically an opportunity to strengthen the links with their home country.

Current Belgian elections for citizens living abroad is held mostly by mail, followed around equally by votes within embassies/consulates and votes in Belgium (personally or through proxy).



Source: Own elaboration based on data of the Belgian Electoral Service[1].

Figure 3: Overall number of non-resident nationals registered to vote for federal elections in Belgium (1999-2019)

For the previous elections (2003-2014), a full comparative analysis between abroad citizens and those living in Belgium was conducted by the CRISP research centre. (Blaise P., 2016, p29). In 2010, the participation to the election was relatively low due to the short period between the notification of the election and the voting date (Lafleur J.-M., 2018). Postal voting is the most growing channel over the years. Another important attention point: the above figure 3 is related to the registration to the election. The participation level at those elections, from the non-resident population, is at around 70% for the postal voting channel, while the participation for the Belgian resident population is at around 90%. Part of this discrepancy can be explained by the postal delays, for more details cfr reference (Blaise P., 2016, p31).

Belgian Federal elections are in some countries also an occasion for meetings and celebrations within the Belgian community hosted at the embassy (Ex. Prague), but within some big countries, some of those citizens are nearly excluded as they will not be able to travel hundreds or thousands of kilometers (e.g. In Italy, different Belgian citizens are living in Milano or northern area while the embassy is located in Roma; other example being the US where the interstates distances are even bigger).

Even if voting is not compulsory for those citizens, they are often more than interested to participate in Belgian elections. Average education level of Belgian citizens living abroad is quite higher than average education level (OECD, 2006). A more detailed and recent OECD study focused on French citizens emigration even demonstrate an increase of those previous numbers (Barbara, 2021); we should expect similar trends for Belgian citizens. This phenomenon could allow better acceptance of new voting options from this part of our population.

[1] Data available here: http://www.elections.fgov.be/index.php?id=3286, and summarized till 2014 in (Blaise P., 2016) p29.

In 2020, in the USA, the CISA/NIST/FBI/EAC published jointly a risk summary overview paper about the different options for electronic ballot delivery, marking and return. This study does confirm current technology is not yet ready for “electronic only” ballot return option (CISA, 2020).

We will propose here after a 4 steps approach for postal voting:

1. A traditional paper based voting procedure (for illustration of our base scenario)
2. A personal proposal paper-based option combined with some cryptography through “electronic ballot marking”, inspired from STAR-Vote (Bell, 2013) and ElectionGuard (Benaloh, 2021) solutions
3. A paper-based option based on the new STROBE-Voting solution (Benaloh, Sept. 2021) with some personal adaptations for the Belgian election’s specificities, as the STROBE-Voting was initially developed for the US election case.
4. A paper-based option proposed by a Belgian inter-university consortium within the Belgian NETVOTING_BE (part 2) study (Pilet, 2021), in which an innovative Vote-by-Mail solution has been described

Within each of those approaches, we will limit the different kind of risks while with the three last options we will propose an End-2-End verifiability option for the voter, while keeping confidentiality and using Risk Limiting Audit approach.

4.1. Paper based voting procedure

In order to provide a full comprehension of the further options to our reader, we propose to begin by describing a typical traditional paper based Postal Voting solution based on a dual envelope process.

1. Registration
    a. At the embassy, or consulate
    b. Via Web portal
        i. Without strong authentication -> Proof of Identify to be sent (Passport copy)
        ii. With strong authentication, through their Belgian eID card

2. First feed-back – Confirmation:

    Twelve weeks prior to the election, citizens will receive through post mailing: Voting procedure, the Postal Voting Attest document (Cfr Figure 4)

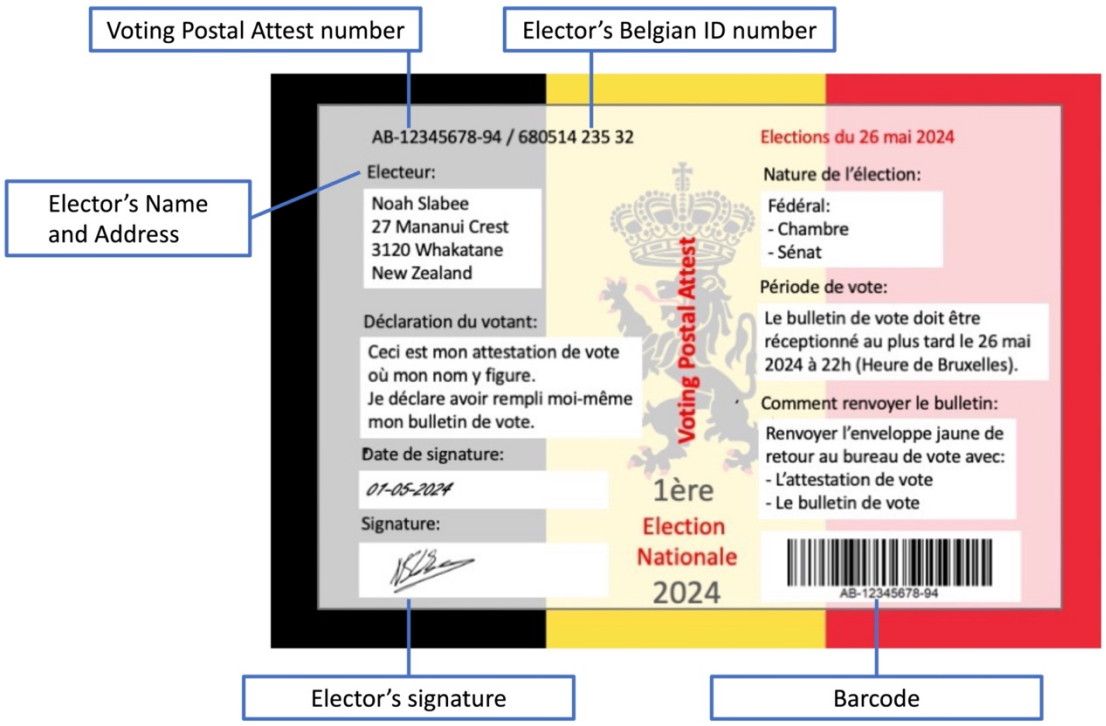


Figure 4: Voting Postal Attest example illustration

3. Second feed-back – Ballot received by mail:

    Eight weeks prior to the election, citizens will receive through post mailing, an "How to vote procedure" document + an empty ballot + two envelopes (one for sealing the ballot, and one which will contain the first envelope and the Postal Voting Attest).

4. Voting:

    Citizen is voting:

        i. Filling the ballot
        ii. Put the filled-in ballot into the first envelope and sealed/close it.

iii. Date and sign the Postal Voting Attest.
iv. Put the first envelope and the filled-in Postal Voting Attest into the second envelope.
v. Post the second envelope well on time as it must arrive on the date of the election in Belgium at 10PM the latest.

5. Controls:
    a. The citizen will be able to check via the Belgium.be portal:
        i. It he/she is well registered as voter for the next postal voting election
        ii. If his/her first envelope (Step 2) has been mailed and when
        iii. If his/her second envelope (Step 3) has been mailed and when
        iv. If his/her returned ballot envelope has been received, and his/her signed Postal Voting Attest has been validated
    b. He/She will not be able to check if his/her vote has been tabulated or not.

6. Additional options:
    a. In case he/she didn't receive the first envelope within a 3-week time frame, he/she should be able to request a new "sending"
    b. In case he/she didn't receive the second envelope within a 3-week time frame, he/she should be able to download and print an empty ballot and the voting procedure

4.2. Paper based voting procedure + cryptographic options

On top of the above paper based voting procedure, some cryptographic add-ons are proposed to be used to ensure End-2-End verifiability and Risk Limiting Audit control.

The proposed cryptographic approach is taken mainly from the "STAR-Vote" (Bell, 2013) system which is proposed to be adapted to the present Postal voting approach. As mentioned within this paper page 35, "*printing a paper ballot returned through the postal mail, might well be feasible as a replacement for current vote-by-mail practices. A full consideration of this is left for future work*". Within this paragraph we will develop a possible option for this postal mail option. Additional ideas for this paragraph have been also inspired from the recent ElectionGuard solution (Benaloh J., 2021).

Steps which are different from "step 1 Paper based voting" are **highlighted in blue** in the following paragraph.

1. Registration
    a. At the embassy, or consulate
    b. Via Web portal
        i. Without strong authentication -> Proof of Identify to be send (Passport copy)
        ii. With strong authentication, through their Belgian eID card

2. First feed-back – Confirmation:

    Twelve weeks prior to the election, citizens will receive through post mailing: Voting procedure, the Postal Voting Attest document (Figure 4).

    A possible alternative would be to send this confirmation by e-mail and allow the citizen to download/print his/her Postal Voting Attest document after being authenticated by his/her Belgian eID card. This alternative option will reduce the number of postal mail to be sent.

3. Second feed-back – Ballot received by mail:

    Eight weeks prior to the election, citizens will receive through post mailing, an "How to secure vote procedure" document + a backup paper empty ballot + two envelopes (one for sealing the ballot, and one which will contain the first envelope and the Postal Voting Attest).

    The "How to secure vote procedure" will describe the two possible options for voting:

    1. an E2E voting option which will be an electronic ballot marking based option approach (The citizen will fill in his/her ballot on a screen, print it locally and return it by postal mail). The printed filled in paper ballot will contain a unique ballot number AND a bar code related to this number. After printing his/her filled in paper ballot, the citizen will also print an anonymized voting proof document which will contain a hash of his/her filled in e-ballot.
    2. Classical pen paper-based voting, as in paper based only version described in step 1. above. This paper based only option can be used as a fallback option if the citizen can't or doesn't want to use the electronic marking ballot option. If the citizen is using this paper ballot "basic" option, no End-2-End verifiability feature will be available.

4. Voting:

    Citizen is voting:

    Filling the e-ballot through a specific signed application, which could be obtained from the voting.belgium.be web portal. No Authentication will be required for downloading or using the app to guarantee the true anonymity of the vote procedure. The usage of a local application will also allow the

citizen to verify his/her ballot is correctly filled in and will ensure the full secure transmission of the encrypted possible vote to the central authority system. He/She will be able to validate and, print/challenge as many ballots as he/she would like, but only one ballot will be allowed to be returned within the paper envelope. After the validation of his/her vote, the citizen will get 2 possible options:

1. He/She will challenge his/her vote so that he/she will be able to validate his/her encryption proof does correspond to his vote. This an important step to guarantee integrity. In this case his/her vote will be spoiled and directly published on the bulletin board. The challenge could/should be performed via another device than device used for encoding the vote, in order to improve the security level.
2. He/She will print his/her ballot (cfr Figure 5), which will contain a unique ballot number required also for E2E verifiability, and an anonymous voting proof document (cfr Figure 6). This voting proof document will contain a hashed version of the citizen voting choices, which will be kept by the voter and used for End-2-End verifiability control.

The system should not allow to print a ballot which has been challenged. This voting scheme does guarantee integrity by using so called "Benaloh challenges" (Benaloh, 2006).

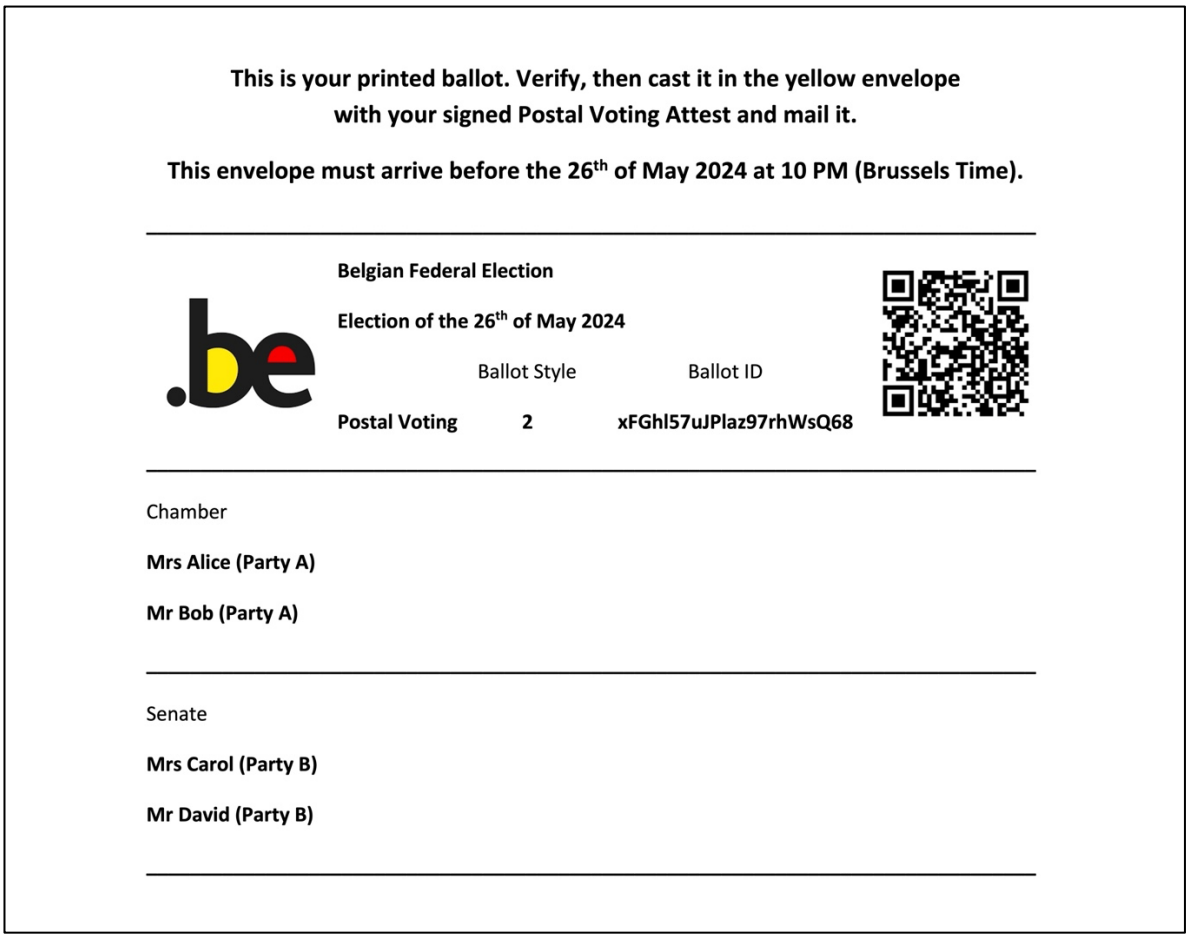


Figure 5: Illustration of a printed e-ballot

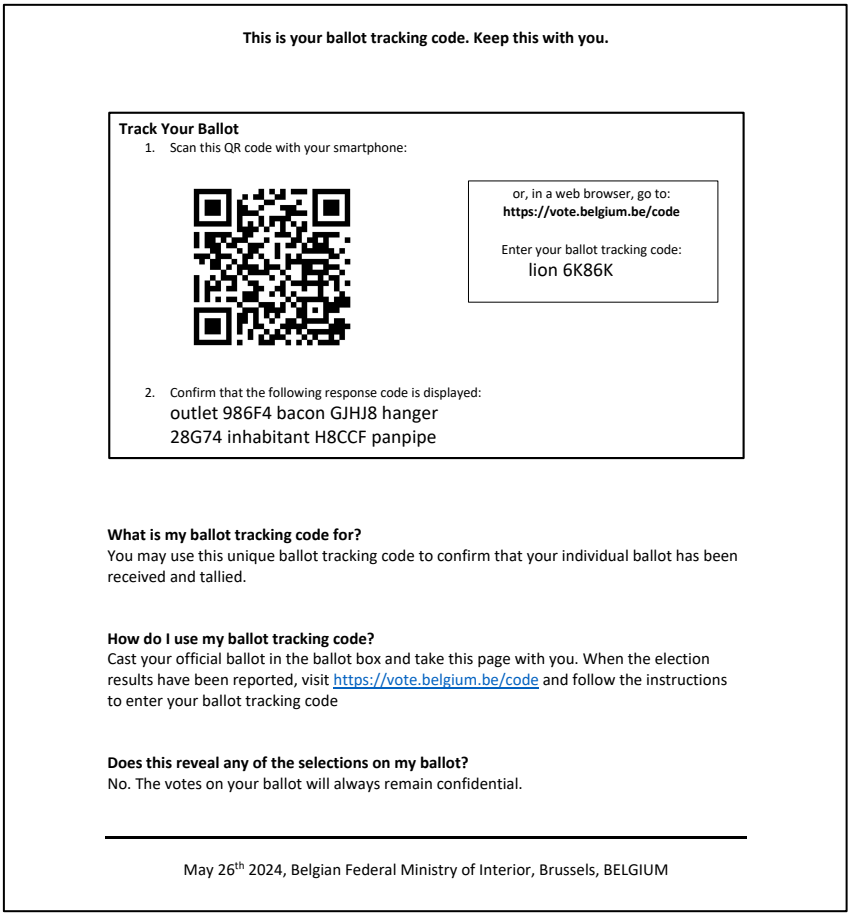


Figure 6: Illustration of a proposed tracking code (inspired from ElectionGuard solution (Benaloh, 2021))

i. Put the printed e-ballot within the first envelope and seale/close it.

Keep securely the voting proof document, and don't put it in the envelope with your ballot.

ii. Date and sign the Postal Voting Attest.

iii. Put the first envelope and the filled-in Postal Voting Attest into the second envelope.

iv. Post the second envelope well on time as it must arrive on the date of the election in Belgium at 10PM the latest.

5. Controls:

a. The citizen will be able to check via the Belgium.be portal:

i. It he/she is well registered as voter for the next postal voting election

ii. If his/her first envelope (Step 2) has been mailed and when

iii. If his/her second envelope (Step 3) has been mailed and when

iv. If his/her returned ballot envelope has been received, and his/her signed Postal Voting Attest has been validated

b. Via another web link or iOS/Android app, the citizen will be able to check if the hash code mentioned on his/her voting proof document has been tabulated or not.

He/she will also be able to check if his/her other voting proof codes related to his/her other ballot(s) which he/she generated, but which were not sent back, were tabulated or not.

c. All challenged ballots will be visible on the public bulletin board. This is step named as "cast-as-intended verification", and as explained in (Culnane, 2015), "*it also provides dispute resolution and some accountability: there is no need to take the voter's word for how they voted. A ballot confirmation check that completes with an invalid proof can be used as evidence; an attempted ballot confirmation check that does not complete at all can have multiple (human) witnesses. Ballot confirming is separate from voting, so additional ballot confirming by independent observers would be a convenient and practical addition to voter initiated ballot confirmations. … (vVote, Wombat, StarVote and some other systems also separate the process of generating an encrypted vote from casting it.) These processes are additive in the sense that they do not interfere with each other: the audits and inferences associated with particular trust assumptions are not affected by other audits based on different trust assumptions.*"

d. Risk limiting audit will be done against all printed returned e-ballot.

6. Additional options / remarks:
    a. In case he/she didn't receive the first envelope within a 3-week time frame, he/she should be able to request a new "sending"
    b. In case he/she didn't receive the second envelope within a 3-week time frame, he/she should be able to download the voting procedure, his/her ballot, and of course generate his/her e-ballot.
    c. The voting proof document may not leak any information about the voter choices, therefor it will not contain the ballot ID in clear text, but only a hash of the encrypted ballot, and some additional info like a date&timestamp (cfr StarVote – (Bell, 2013)).
    d. "The whole notion of end-to-end verifiability is not to say that a system can't be attacked," says Benaloh. "Rather than 'prevention,' it's all about *detection*." (Wofford, 2020)

For the current postal project, we propose the usage of the following concept:

- End-to-end verifiability (voter being able to check his/her vote intention does match his voting draft voting proof, and if his/her ballot has been added to the tally).
- Postal Mailing of the vote, cfr The Netherlands, UK or Switzerland process
- Web portal to allow "anyone who wishes to monitor the election can check all votes have been tallied".

We propose now to go into the details about how the security and crypto aspects are handled within the different phases of the above proposed process:

Paper ballots: for both options, relying on paper ballots is currently the most secure options, while offering real only full post-election audit, by hand if required. E-paper-ballot option allows users/citizens to verify their vote are correctly tabulated.

Design:

For the citizen, the paper approach is very similar to the procedure for citizens of the Netherlands living abroad, or UK citizens relying on postal voting in their own country.

On top of this "classical" approach, the printing e-ballot and its e-ballot proof document do both include some cryptographic features which are described here after, and which are taken/inspired from the STAR-Vote design (Bell, 2013). The *italic* text in the next part of this paragraph is referencing the original STAR-Vote paper text (Bell, 2013), while the non-italic text is the present paper author's text.

Crypto Overview:

As for the STAR-Vote, we need to generate cryptographic keys, with a set of n trustees designated as key holders and a threshold number k. So, any k of the n trustees can complete the election.

As for STAR-Vote, we will rely on their approach: "*From the perspective of election officials, the first new element in the election regimen is to generate the cryptographic keys. A set of election trustees is designated as key holders and a threshold number is fixed. The functional effect is that if there are n election trustees and the threshold value is k, then any k of the n trustees can complete the election, even if the remaining n − k are unavailable. This threshold mechanism provides robustness while preventing any fewer than k of the trustees from performing election functions that might compromise voter privacy. Threshold cryptosystems are straight forward extensions of traditional public-key cryptosystems [Desmedt and Frankel 1989]. The trustees each generate a key pair consisting of a private key and a public key; they publish their public keys. A standard public procedure is then used to compute a single public key from the n trustee public keys such that decryptions can be performed by any k of the trustees. This single election public key K is published and provided to all voting terminals* (local applications instances in our specific postal voting case) *together with all necessary ballot style information to be used in the election.*" Instead of the unique z_0 of STAR-Vote, we propose to take 1000 z_0 to z_{999} initial values, which will be unique and unpredictable. We will take 1000 different initial values instead of 1 as we will have a central web e-voting ballot portal and want to avoid possible frauds based on multiple vote simulations.

After a citizen will have made his/her choice, he/she will generate two paper printouts:

The first paper will be the ballot printout, which will contain the candidates selected by the citizen, and a random (non-sequential) serial number (and its related barcoded version). The second paper will be the e-ballot proof document which will contain, the originating country of the IP address of the citizen PC/terminal (instead of the identification number for the voting terminal as mentioned in original STAR-Vote description), and as illustrated in STAR-Vote paper, *date and time of the vote, and a short hash of the encryption of the voter's selections together with the previous* i-1000 *hash value. Specifically, if the voter's selections are denoted by v, the* i^{th} *hash value produced* from a particular country *m in an election is computed as*

$$z_i = H(E_K(v), m, z_{i-1000})$$

Where H denotes the hash function and E denotes encryption. This separation of the ballots into two parts makes sure that the ballot summary does not contain any voter-related information, while the second paper kept by the citizen *does not leak any information about the voter choices. Furthermore, since we only store votes in an encrypted form, and since the decryption keys are kept out of the system, there is no problem with storing the votes with timestamps: they could only allow linking a voter to a ciphertext that will never be decrypted, which is harmless.*

As additional "protection" measure, we may limit the number of voting tentative a citizen may submit within a certain time period, based on his/her IP address or IP range for example (even if this is not a full protection, and taking into account that some countries, like Morocco, don't provide often public IP address to their citizen, but IPs in the 10.X.Y.Z range. Those different Moroccan citizens are then visible/presented on the Internet as coming from a limited set of public IP address).

The central IT system will only keep the encrypted votes, the ballot IDs, and the hash values.

On reception of the citizens envelope, there will be the following steps:

1. Verification of the validity of the Voting Postal Attest information
    a. If OK,
        i. record the positive ballot envelope reception
        ii. the second envelop which does contain the vote is put into the ballot box.
    b. If not OK,
        i. Record the negative, and notify the citizen about the reason
2. On the date of the election, the ballot box is opened, and the ballots IDs are scanned:
    a. Based on ballot's id's, we can identify which encrypted voted are to be kept as valid ballots

b. The encrypted ballots for which no ballot's ids are being scanned will be marked as "invalid" and will not take part of the tally.

3. The valid encrypted ballots are aggregated.
4. The aggregated encrypted ballot's summary results are being computed and decrypted.
5. The invalid and not received ballots have their encrypted version decrypted, and their respective decrypted value are published on the public bulletin board.
6. RLA is performed to provide a second validity check, and if required/wished a full manual paper ballot count can take place.

As with the STAR-Vote system, the citizen can check the following aspects on a web bulletin board, through different web pages entries, or via a specific iOS/Android app:

1. His/her Voting Postal Attest has been well received AND has been validated
2. Based on the code mentioned on his/her second paper, he/she can verify this related ballot is part of the total tabulated or not.
3. If his/her code is not part of the total tabulated, he/she should be able to display the details of this related non-tabulated ballot

As described within the STAR-Vote system, the following cryptographic aspects are handled:

"*Upon completion of the election, the election office homomorphically combines the cast ballots into an aggregate encryption of the election tally (this can be as simple as a multiplication of the public encrypted ballots). At least k of the election trustees then each perform their share of the decryption of the aggregate as well as individual decryptions of each of the spoiled ballots. The trustees also post data necessary to allow observers to verify the accuracy of the decryptions. A privacy-preserving risk-limiting audit is then performed by randomly selecting paper ballot summaries and matching each selected ballot with a corresponding encrypted ballot to demonstrate the correct matching and provide software-independent evidence of the outcome [Rivest and Wack2006; Lindeman and Stark 2012; Stark and Wagner 2012]"*

This ensures the STAR-Vote triple assurance:

1. *The homomorphic tallying process proves that the announced tally corresponds to the posted encrypted ballot records*
2. *The ballot challenge and receipt checking processes allow voters to check that these encrypted ballot records correctly reflect their selections*
3. *The risk-limiting audit process serves to verify the correspondence between the paper records and the electronic record*

Limitations of the current proposed Postal Voting approach with this Electronic Ballot Marking option vs the original STAR-Vote approach:

1. The citizen can generate as many votes as he/she would like, but he/she may only send one ballot vote through his/her voting envelope.
2. The citizen will not be able to conduct e2e challenge audit before the election closing date.
3. Only one single ballot can be returned by mail, as the citizen will by default receive only one Voting Postal Attest. In case a double Voting Postal Attest for the same citizen is received, only the first received Voting Postal Attest will be accepted, and its related ballot envelope. This phenomenon may happen if the citizen is declaring he/she would like a new Voting Postal Attest as he/she didn't receive within the initial planning. If at the end he/she may receive two physical paper Voting Postal Attest, he/she could theoretically submit two voting ballots. To differentiate those Attests, each Postal Voting Attest will have a unique ID.
4. In case an Electronic Postal Voting Attest is sent to the citizen, and printed by him/herself, the codes/IDs related to the previous Postal Voting Attest(s) delivered to this citizen will be "canceled" and those cancellation will be notified to the citizen.

5. Limitations due to paper ballots do remains:
    a. A lot of postal mails envelope will be received, and related physical storage needs to be foreseen.
    b. Time required for receiving postal mails sent from distant countries
6. Potential data leakage from the computer/device on which the Electronic Ballot Marking application is run. This may occur for example if the computer/device is infected by a third-party malware.
7. In case of malware on the citizen computer/device and malicious code being injected within the Electronic Ballot Marking Application, potential data corruption on the data sent to the central server, while correct data are being printed, is a theoretically possible situation. This specific kind of cases should be discovered through the RLA, and manual paper audit control. In that specific case, a full manual tally of all paper ballots will be required and will provide the only real election results. If the client application is suspected to be compromised, a hash control of the app can be used. If one app instance is compromised, it should only impact the citizens where this app is used, but not directly all citizens votes.

Advantages of the Electronic Ballot Marking paper option, on top of the cryptographic aspects described here above, vs full only paper ballot option:

1. Lower invalid filled-in ballot ratio, as before printing the filled-in ballot vote, the Electronic Ballot Marking program will check the vote validity and inform the user about any potential conflict. We could allow the user to confirm an invalid vote combination, but we would recommend to not print any invalid choice selection. The citizen would still have the right/choice to submit an empty ballot, while he/she will be informed he/she is submitting an empty ballot.
2. E2E verifiability as the citizen can check if his/her vote is part of the final total tally
3. RLA is easily computable, while a full manual tally remains still possible from all the received paper ballots.
4. As for the STAR-Vote, this system makes the choice of paper to ensure security and auditability. In case of any security doubt, paper ballot tally will always remain the fallback option.
5. In case of coercion risk, which are always possible in postal voting, the citizen is always able to request a new postal e-voting attest and will be able to submit and send a new ballot, while his/her previous ones will be automatically canceled.

User Interface Design specification

As highlighted in the “Recueil sur Le droit electoral” (French Senate – May 2021), a specific attention should be taken in the application design interface to avoid any favoritism for some candidates. This kind of attention should be handled with care, especially when there are a lot of candidates/parties involved in the election, and the citizens are using relatively small/low resolution screens.

Audit

- As for the STAR-Vote, *the E2E feature enables individual voters to confirm their votes were* received and *included in the tabulation, and that the encrypted votes were added correctly*. *The challenge feature* (multiple vote simulation made by the citizen) *assures that the encryption was honest and that substantially all the votes are included in the tabulation*.
- The couple paper ballot / e-ballot version of each ballot is handled completely independently and do both provide voter intents. In case of any doubt about discrepancy, the full validated paper ballots can be counted/tallied separately.
- As mentioned within the STAR-Vote paper (Bell, 2013), *a risk-limiting audit guarantees a large minimum chance of a full hand count of the audit trail if the reported outcome (i.e., the set of winners) disagrees with the outcome that the full hand count would reveal. The full hand count then sets the record straight,*

correcting the outcome before it becomes official. Risk-limiting audits are widely considered best practice for election audits [Lindeman et al. 2008; Bretschneider et al. 2012].

The cryptographic workflow

The proposed cryptographic scheme is nearly fully based on the STAR-Vote system. (Bell, 2013).

The core elements, *the Hardening encryption*, *Hardening decryption*, *Hardening the timeline*, *Hardening the link between the paper and electronic election outcome*, and *the full cryptographic protocol* described in "*6. The cryptographic workflow*" in (Bell, 2013) are fully maintained, with just a few differences.

Those proposed differences are:

1. The STAR-Vote terminals are replaced here by citizens computers, which will transmit directly the encrypted ballots and their current hash value to the central system. The STAR vote identification of the terminals will be replaced by the id of one of the contacted central servers. The punctual central server which will be contacted by the citizen device will provide to the app its server terminal ID, and the z_{i-1} value which will have to be used for generating the new i^{th} hash value to be produced on the citizen device.
2. Instead of a unique z_0 initial value, we will have a range of initial values like for example z_0 to z_{999}. This change is required has we are now relying on citizens computers/network and would like to avoid a set of pseudo citizens generating a set of z_i to be able to capture and try to get leakage from the content of the next vote linked to z_{i+1} for example.
3. Coercion and Chain voting risks are still possible. Those can be mitigated/limited by the option in which the citizen is able to resubmit a new vote which will cancel his/her previous submitted vote.
4. Challenge verification will only be possible after voting closing date. Reason: As paper ballots will be transmitted by postal mailing, the Postal Voting Attest validation and ballots receipt handling will only be possible after those postal mails have been received. So, the present situation is similar to the provisional approach described within the STAR-Vote paper. As the citizens may resubmit a new vote till election closing time (cfr coercion here above), we can't publish validated ballot hashes till election closing time.
5. All generated e-marked paper ballots, for which no paper ballot counterpart will be received by election closing time, will be marked as "spoiled". The vote details of those spoiled ballots will be published on the bulletin board.
6. The Benaloh challenge/spoil option which would allow on-line citizen direct vote verification has not been retained, as this could add confusion: there is a risk that after the challenge, the citizen would keep this printed ballot and send it within the voting envelope. A possible alternative (not described in the current version of this document) is to allow the citizen to challenge the vote prior to the "printing" option. In case the citizen would challenge the vote, the printing option would then be disabled in order to avoid this ballot to be postal mailed back.

As for the STAR-Vote system (Bell, 2013, p31), the full cryptographic protocol workflow is copied here after, with the modification highlighted in blue:

(1) The trustees jointly generate a threshold public key/private key encryption pair. The encryption key K is published.

(2) Each voting terminal is initialized with the ballot and election parameters, the public key K and seeds z^p_0 and z^i_0 that are computed by hashing all election parameters and a public random salt $z_{0\text{-}999}$.

(3) When a voter completes the ballot marking process selection to produce a ballot v, the voting terminal performs the following operations:

(a) It selects a unique and unpredictable ballot identifier bid, as well as a unique (but possibly predictable) ballot casting identifier bcid.

(b) It computes an encryption $c_v=E_K(v)$ of the vote, as well as a NIZK proof p_v that c_v is an encryption of a valid ballot. This proof is written in such a way that it can be verified from Ext(cv) only.

(c) For each race $r_1,...,r_n$ to which the voter takes part, it computes an encryption cbid = $E_K(bid||r_1)||\cdots||EK(bid||r_n)$.

(d) It computes a public hash code $z^p_i = H(bcid||Ext(c_v)||p_v||m||z^p_{i-1})$, where m is the voting terminal unique identifier, as well as an internal hash $z^i_i=H(bcid||c_v||p_v||cbid||||m||z^i_{i-1})$

*(e) It prints a paper ballot in two parts. The first contains v in a human readable format as well as cbid and bcid in a robust machine readable format (e.g., as barcodes). The second is a voter ~~take~~*keep*-home receipt that includes, the ~~voting terminal~~* front-end server *identifier m, the date and time, and the hash code z^p_i (or a truncation thereof), all in a human-readable format.*

*(f) It transmits $(bcid,c_v,p_v,cbid,m,z^p_i,z^i_i)$ to the ~~judge's station~~*central server*.*

(4) When a ballot is cast, after the postal voting attest has been validated*, the ballot casting id bcid is scanned and sent to the ~~judge's station~~*central server*. The judge~~'s station~~* managing the central server *then marks the associated ballot as cast and ready to be included in the tally. This information is also broadcast and added in the two hash chains.*

(5) When the polls are closed, the tally is computed: the product of all cast encrypted votes is computed and verifiably decrypted, providing an election result.

*(6) The data needed for the risk limiting audit is computed, as described ~~above~~*after*. All the data included in the public hash chain are eventually digitally signed and published by the ~~local~~ authority. Those audit data are considered to be valid if the hash chain checks, if all cryptographic proofs check, that is, if the ballot validity proofs check, if the homomorphic aggregation of the committed votes is computed and opened correctly, and if all spoiled ballots are decrypted correctly.*

Similarly, the Risk Limiting Audit process, described in the STAR-Vote (Bell, 2013) paper (p 31), is also used within the present postal voting solution:

The requirement for running the RLA is to commit on a full electronic record including a 1-to-1mapping and evidence that this electronic record leads to the announced outcome. This is achieved as follows.

*(1) For each ballot, the ballot marking ~~device~~*application *selects a random ballot id sequence number bid. This bid is printed on the ballots as a barcode. Furthermore, for each race r to which the voter participates, an encryption of H(bid||r) is also computed and appended to the encryption of the choices.*

(2) At the end of the election *day, and before decryption of the tallies, the trustees (or their delegates) shuffle and rerandomize all encrypted votes, race by race. This shuffle does not need to be verifiable, even though a verifiable shuffle would improve accountability by making it possible to verify that the shufflers did not cheat if it happens that a discrepancy is detected during the RLA. However, in the case of a non verifiable shuffle, the shufflers must save their permutation and randomness until the end of the election audit. The non-verifiable solution is preferred for its simplicity (verifiable shuffles are particularly challenging to implement properly) and for its efficiency (permutations and reencryption factors can be precomputed, leaving only one multiplication to perform per ciphertext in the online phase, which is convenient when millions of ciphertexts have to be shuffled).*

(3) When the trustees decrypt the homomorphically added votes, they also decrypt the output of this shuffle. For each race, this provides a list of elements of the form H(bid||r) and the corresponding cleartext choices.

(4) Now, auditors can sample the paper ballots, read the bid printed on them, recompute the value of H(bid||r) for all races present on the paper ballot, and compare to the electronic record (as well as check many other things, as prescribed for the risk-limiting audit). The use of hashed bid's has the important benefit of making sure that someone who does not know a bid value cannot, by looking at the electronic record, link the selections made for the different races on a single ballot, which protects from pattern voting attacks. There is no need for such a protection from someone who can access the paper ballots, since that person can already link all races just by looking at the paper.

Threats:

The typical STAR-Vote threats, and countermeasure are described in (Bell, 2013) paper.

For this specific postal voting implementation, the following typical specific threats and impacts are evaluated:

1. Denial of service:

   The core exposed component in this case is the server's infrastructure hosted centrally and used for the eBallot marking, for the public bulletin board and the ones used for the Postal Voting e-Attest. In case of massive Distributed Denial of Service attacks, those services may be impacted. This kind of attacks may impact the whole ePostal Voting process. Mitigation: As the ePostal Voting period will be spread over a few weeks, the probability is relatively limited to get a massive attack during such a long period. We need to limit the potential attack, especially in the last days and hours of the elections. Typical measures will need to be taken upfront against those kind of DDoS attacks, especially based on the experience encountered in Belgium by the Federal Authorities on the 4th of May 2021.

2. Coercion and Chain voting:

   Coercion and chain voting are typical risks which may occur in distant voting scheme. The proposed counter measure for those issues is to allow the citizen to generate new eMarked ballots, to generate/print new Postal Voting eAttest which will cancel at the same time his/her previous submitted ballots. The only possible limitations are related to the E2E verifiability: it will be visible on the public board for the instructor(s) voter(s) that those specific ballots have been canceled.

3. Fraudulent voting receipt. Different cases are possible:
   a. The voter provides a fake attest, with no references available on the public bulletin board (nor confirmation of valid vote, nor trace of spoiled ballot). Proposed solution: as soon an eBallot is being marked, a reference should be available on the public bulletin board with the mention "waiting paper ballot reception and validation". This information should be available for the voter as soon as he/she submitted his/her eBallot choice. This will ensure that the citizen can check his/her ballot reference is well known on the central system. As we want to avoid hard links between Postal Voting Attests and paper ballots for confidentiality reason, we will not have any solutions to ensure we have well received the expected ballot linked to a specific Postal Voting Attest.
   b. The voter claimed his/her paper ballot was correctly sent, but was never delivered, or not delivered on time, to the election office, nor validated. This case may happen. For citizens who wants to be covered, we may propose different options:
      i. Registered mail. This will ensure postal tracking. This may be a paid option for the citizen.
      ii. A barcode sticker on the external returned envelope combined with a picture of the returned envelope could be published as soon the envelope is centrally received (before being opened). This could ensure the citizen his/her envelope has been received, even if not yet opened and Postal Voting Attest has not yet been validated. The barcode sticker could be the Postal Voting Attest ID.
   c. A voter has submitted multiple envelopes and Postal Voting Attests:
      i. If multiple paper Postal Voting Attest for the same citizen are received, we propose keep the most recent related ballot received (based on reception date). Constraint: the received envelope containing the Postal Voting Attest must be opened starting with the most recent ones.
      ii. Once a Postal Voting eAttest is generated (due to claim for absence of Postal Voting Attest delivery to the voter, or coercion claim), all paper Postal Voting Attest for this voter will be marked as "spoiled". So, only the most recent Postal Voting eAttest will be kept as "valid".

iii. If multiple paper Postal Voting Attests are received on the same day for the same citizen, we will keep the first one handled for the same citizen. The second one will be refused with, and the related reason will be published on the public bulletin board. The related voting paper ballot will be considered as spoiled.

d. A voter is inserting multiple paper ballots within his/her single returned envelope. This case is possible as he/she may generate multiple ballots from the eBallot marking application. If that case is happening, we suggest spoiling all ballots linked to this envelope. This kind of case should be logged and documented. Envelope opening should be made in public with auditors' presence to avoid fraud claims during those phases.

4. Additional proposed option for additional security against possible fraud:
    a. Use pre-watermarked paper for printing the ballot and receipt: eMarked ballot and receipt will have to be printed on specific pre-printed watermarked paper. Those 2 pages could be delivered via the second postal mailing to the voter. In case of issues, paper jam, printing ink issue, coercion complain, the voter will need to order new watermarked paper from the central election office. Those new watermarked papers could be eventually also delivered from the diplomatic sites (embassies or consulates). This additional option adds indeed more complexity to the process.
    b. Digitally sign the ballot with a printed watermarked signature. This would be a safer option but at the cost of the vote anonymity lost
    c. In case a Postal Voting eAttest is generated, it can be digitally signed by the citizen and include a watermark. As this document does not require confidentiality, this can be a valid option against fake Postal Voting eAttest. The risk for fake eAttest is relatively limited if prior to the generation of new eAttest, the voter has to be authenticated on the eVoting site with his/her eID card authentication.

4.3. STROBE-Voting based solution

This 3rd approach is a new solution which will be soon published (Benaloh J., Sept.-2021).
It does allow end-2-end verifiability, like for the previous proposal, while it avoids any computer and printer usage requirement for the voting act from the voter.
It has the advantage it can be used for vote-by-mail (VbM) and in traditional Belgian paper-based voting booths, as it only requires the paper ballot and a pen.
Providing E2E verifiability only for Belgian citizens living abroad could have a legal impact. The STROBE-Voting approach would allow all Belgian citizens who vote on paper, including in traditional booths, to rely on E2E verifiability capability by just replacing the current traditional paper ballot by a new type of paper ballot described here after.

As mentioned in STROBE-Voting paper which we do recommend as reading for all readers of the present paper,
it is based on the same traditional paper-based ballot we all know, with the addition of some short code beside each possible option, 2 alphanumeric digits in our example (A-Z, 0-9) and a large 32 bytes hash code at the bottom of the ballot (Figure 7).

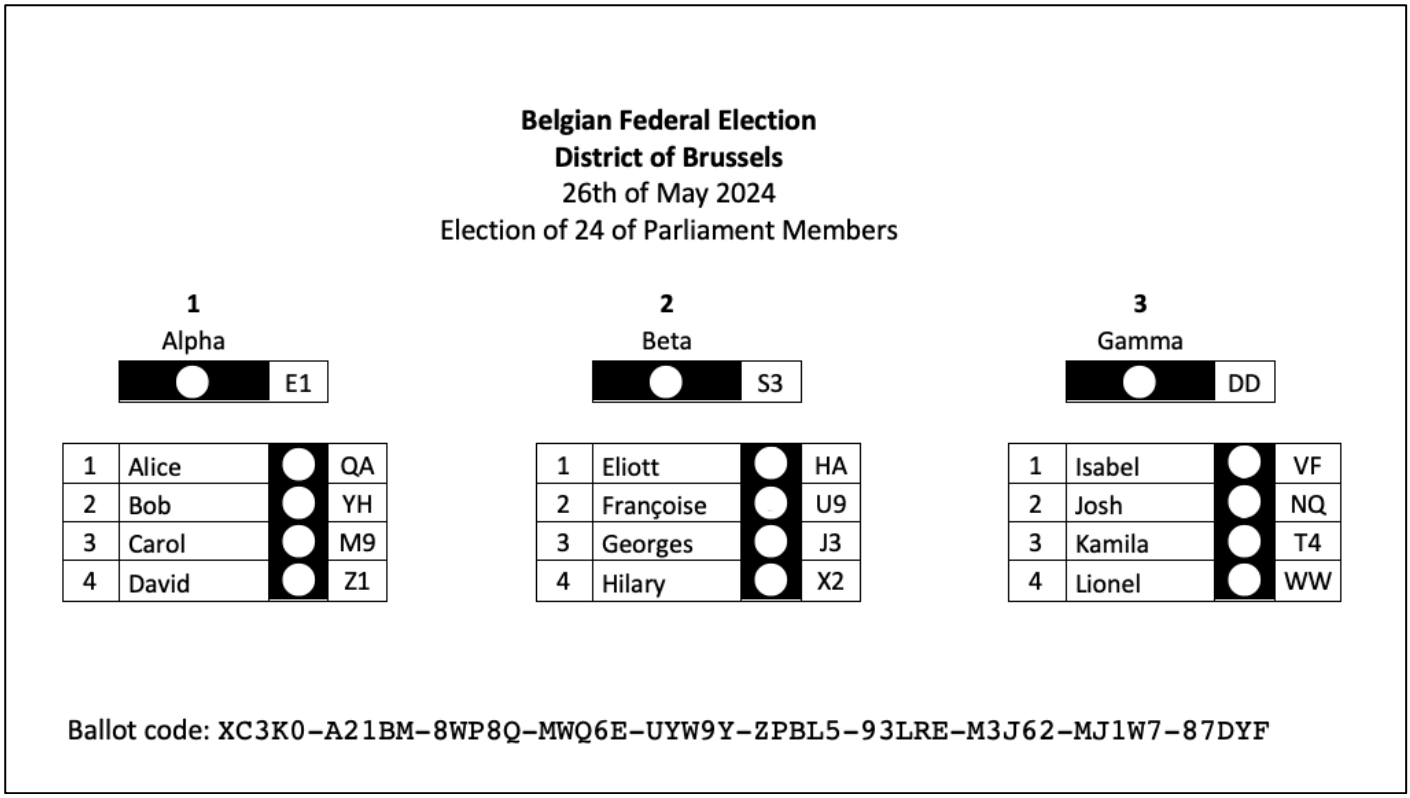


Figure 7: Example of STROBE-Voting ballot

Voters do fill-in their ballot as for classical paper vote.
The full cryptography methodology is described in the STROBE-Voting paper and has not been fully copied in detail here.

A few sentences extracted from this paper illustrates the concept: "*a randomized encryption is produced for each selectable option on each ballot (the encryption changes for each new ballot). These encryptions are retained but* ***not*** *printed on ballots. Instead, the encryptions are locked by being hashed together, and this has of all encryptions are locked by being hashed together, and this hash of all encryptions on a ballot is printed at the bottom of the ballot*".

"***It is important to recognize that even though the selection codes are very short, there is no way to search for or deduce the selections to which they correspond without breaking the corresponding encryptions. The ease with which one can find other encryptions which produce identical short selection codes is not a security threat since the encryptions are fully locked by the long ballot code****.*
As with Helios, STAR-Vote, ElectionGuard, and related systems, every selectable option is encoded with exponential ElGamal."

In STROBE-Voting paper, the code beside each option was proposed to be a 2-characters base derived from a 256 options set. For the Belgian elections, we propose to keep the 2-digit approach, but from a 1024 options set. Reason: In some districts, like in Brussels, we may have more than 256 possible candidates list for a single election!
Non-iterative zero-knowledge proof (NIZK) is handled by delivering two voting ballots to each voter. The voter should return only one of those 2 ballots. This allows ballot verification correctness, on top of results verification.

Additional proposed options on top of STROBE-Voting paper (Benaloh J., Sept.-2021) described solution:

1. “Last-vote-count”:
We propose here an option to cover the “last-vote-count” case, inspired from the Helios solution (Adida, 2009).
In Helios, each voter may submit has many ballots as he/she would like. Only the latest submitted received ballot will be counted in the final tally. If we do combine the printing at home Voting Pass Attest, (cfr paragraph “*4.2. Paper based voting procedure + cryptographic options - 2. First feed-back – Confirmation*”), with the print @home STROBE-Voting ballot approach, we can handle this: we just need to open all the received envelopes by starting with the most recent ones received. All previous posted Voting Past Attests received will have their related ballots spoiled. Those spoiled ballots will be published on the public bulletin board similarly as explained in previous model. It is a relatively simple optional solution to cover this kind of attacks.
Impact: the envelopes will only be opened after the election closure, and the voters will not be able to check if his/her Voting Postal Attest has/have been received prior to the election closure. A key major constraint for the election administrator is the fact they must be very cautious about the envelopes received order, and another constraint is the fact that received order may not be the same as sent order.

A simpler alternative option is to allow an additional field on the ballot itself which can be filled in by the voter.
It may be filled in with a number. If no value is filled in, it would be assumed to have the “0” value. We will keep in the final tally only the ballot with the highest number returned for a specific ballot. So, every time the voter is resubmitting his/her ballot, he/she may increase this counter number.
The question is then: do we publish this counter on the public board for this ballot?
Advantage of publication: the voter is sure about the ballot’s number which is part of the tally.
Disadvantage of publication: in case of coercion, the coercer could see the voter has submitted another ballot…
For this latest case, we could implement a solution like the one proposed (Juels, 2002), but this may be quite complex for standard public elections.

2. Challenge:
In the STROBE-Voting, for ballot verification two options have been proposed:
- dual ballot approach delivered to each voter (cfr example described here above)
- An additional challenge on the ballot itself (like A-B choice), or based on how the ballot was folded, but this latest solution was not advised as it could be confusing for the voter.

The preferred dual ballot option was preferred by its authors, at the cost of dual ballot prints for each voter.
We do propose here an alternative option where the citizen may just select (or not) the challenge option, cfr Figure 8 here after, which may not be so confusing, as if it is not filled-in, it would not void the validity of the ballot. This proposed option would limit the number of printed ballots by a factor 2.
It is inspired from the did-not-vote option concept explained in the STROBE-Voting paper (Benaloh J., Sept.-2021).
This option would still permit ballot verification, but not as tangible as the dual ballot option as the voter would not keep the physical other ballot as proof as in the dual ballot proposed option. The selected “Choice” option could be added to the information published on the bulletin board.

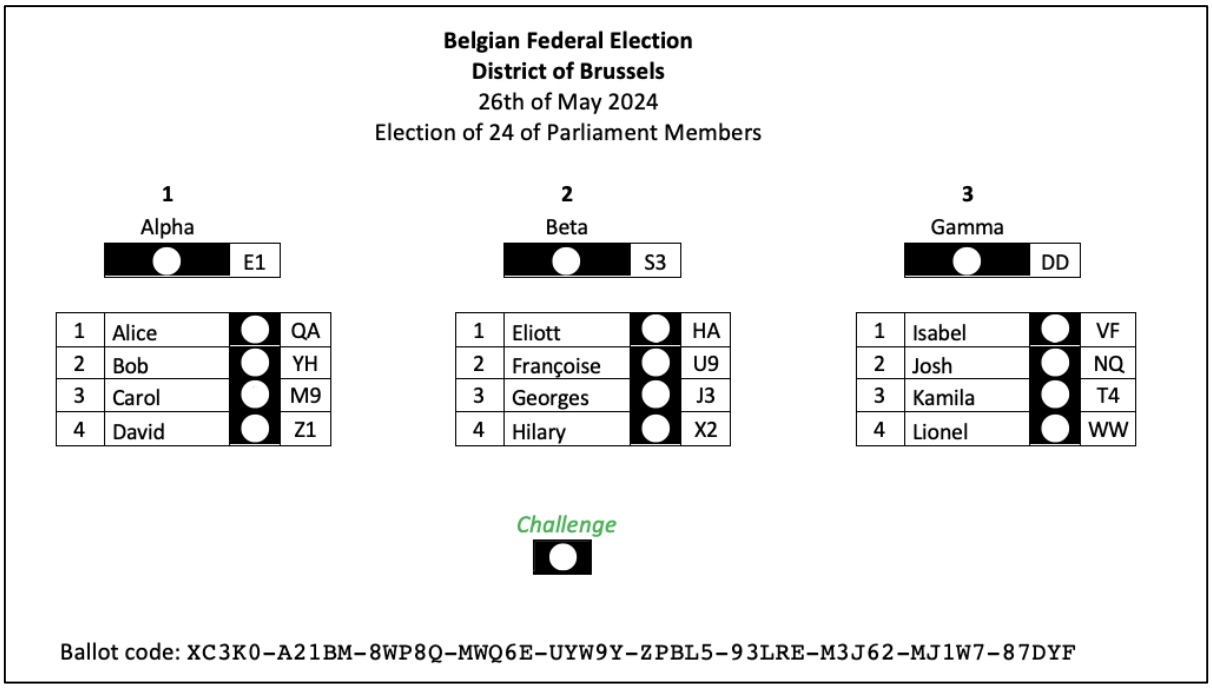


Figure 8: Proposed alternative option for the single ballot challenge approach for STROBE-Voting

3. The current STROBE approach was mainly oriented initially towards a US style election. Within Belgian elections, there are additional constraints. In particular, it is not allowed to vote for different persons within different voting lists.

In order to cope with this additional constraint, without bringing additional complexity, we would recommend splitting the voting ballot in different pages, one per voting list. The voter would only be allowed to submit one single page back (Cfr Figure 9, Idea inspired from the approach described in the next section from the NETVOTING_BE solution). If multiple different pages are returned, linked to the same ballot code, the ballot will be considered as invalid.

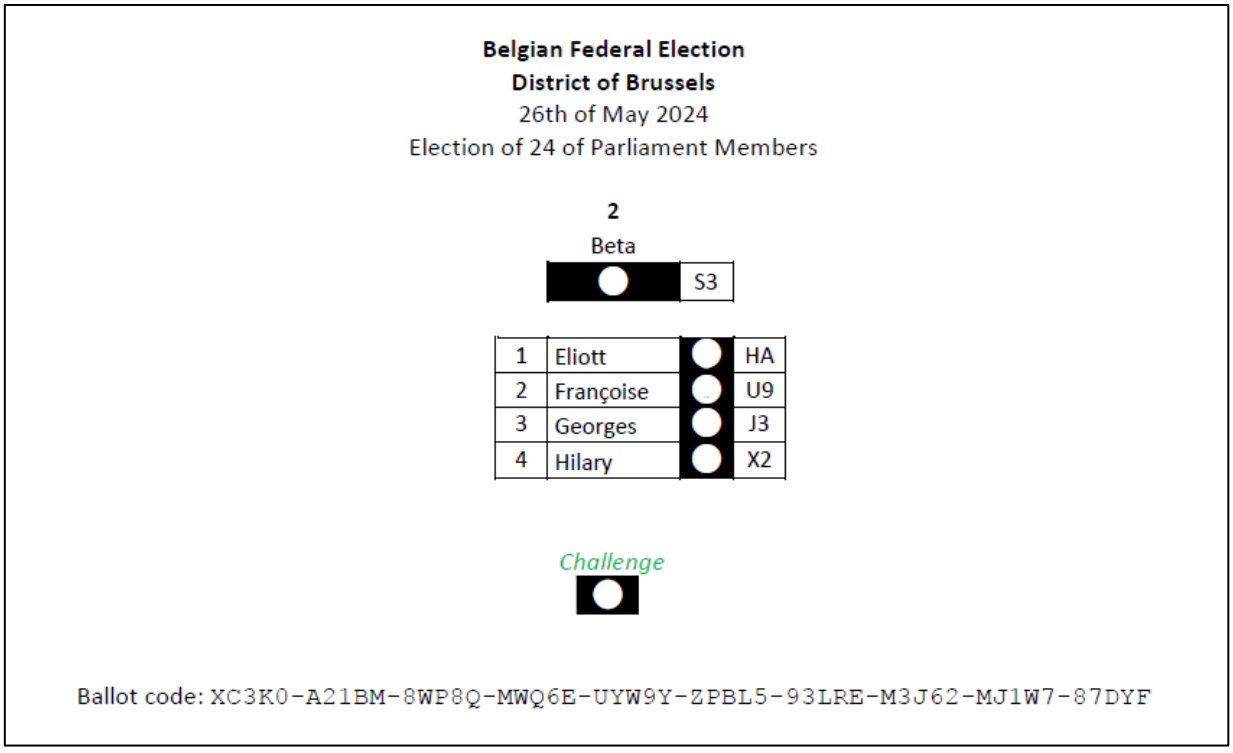


Figure 9: Second ballot STROBE-Voting option example, avoiding potential invalid selection

4.4. NETVOTING_BE based solution

Within the current inter-universities NETVOTING_BE (part 2) study related to the possibility of Internet voting introduction in Belgium (Pilet J.B., 2021), another innovative approach for Postal Voting has been proposed.
This new approach is combining postal voting with some on-line components:

1. Voter's identification is improved versus current Belgian postal voting approach
2. The proposed solution is compatible with other voting options, like the paper based voting solution used within embassies and consulates.

First principle: Ballots exchange simplification
Current Belgian postal voting solution imply sending blank ballots to voters, who needs then to send them back to Belgium. This process is quite complex, time consuming and costly (In a recent election, DHL had been used for ballots exchanges towards Belgian US residents).
Current proposed change: rely on Belgian e-id identity card to download blank ballots. One postal exchange is then avoided through this new approach.

Second principle: Vote verifiability
Current solution does not allow voter to check if his/her ballot has been received and tabulated, or if the ballot would have been manipulated.
The NETVOTING_BE solution will allow ballot tracing (on-time received), AND if it was correctly tabulated. This is in line with the Council of Europe recommendation for e-voting norms (CoE, 2017)

Third principle: Transition phase for future Internet voting
This proposed postal voting solution would allow Belgium to build experience (including the fact of e-id usage for authentication). This experience should be a first step towards possible full internet future voting.

For the full description of this proposed innovative postal voting solution, we do recommend the read of the very didactic paper (Pilet J.B., 2021) p9 and onwards). We advise the reader of the present paper to read this referenced paper for a full detailed comprehension of the topic. We have copied here after the concept of this new solution, as described in the above referenced document (p9-14), in order to allow the reader a first feeling of the proposed approach:

In the proposed system, the conduct of an election involves the participation of a certain number of actors:
• A blank ballot server BS. We assume that this server has the voters list who have been previously registered for the vote of Belgians living abroad. This server allows a voter to identify herself and obtain her ballot blank vote. In certain circumstances, it could possibly offer an interface allowing you to vote on a computer before printing your bulletin.
• Voters $V_1, \ldots, V_n$. These voters identify themselves with BS by means of their card electronic identity or other authorized means, obtain their ballot paper, print it, complete it, and return it by post.
• One or more ballot reception offices RO. The RO receives the ballots vote transmitted by voters. The ballots received are encoded or scanned in order to obtain an electronic version. The RO also interacts with scrutineers in order to perform and guarantee the verifiability of the statement.
• A group of tellers $T_1, \ldots, T_t$. These tellers independently carry out the count of ballots encoded by the RO. They produce the data that enables voters to verify that their ballot has been received and taken into account, and can also ensure that the encoding of paper ballots has been done correctly.
• A verification server VS. Voters can identify themselves to this server in order to check that their ballot has been correctly received and taken into account during the tally.

Ballots preparation:
Blank ballots are prepared by BS. When a voter identifies herself to the BS, by means of his electronic identity card or other means of identification (here we are thinking of the mechanisms validated by CSAM (cfr https://csam.be), or possibly of a subset of these), the BS checks the voter registration and, if successful, he transmits, in the form of a document in pdf

format, a blank ballot paper as well as additional documents that the voter can use to check that they have been taken into account of her vote.

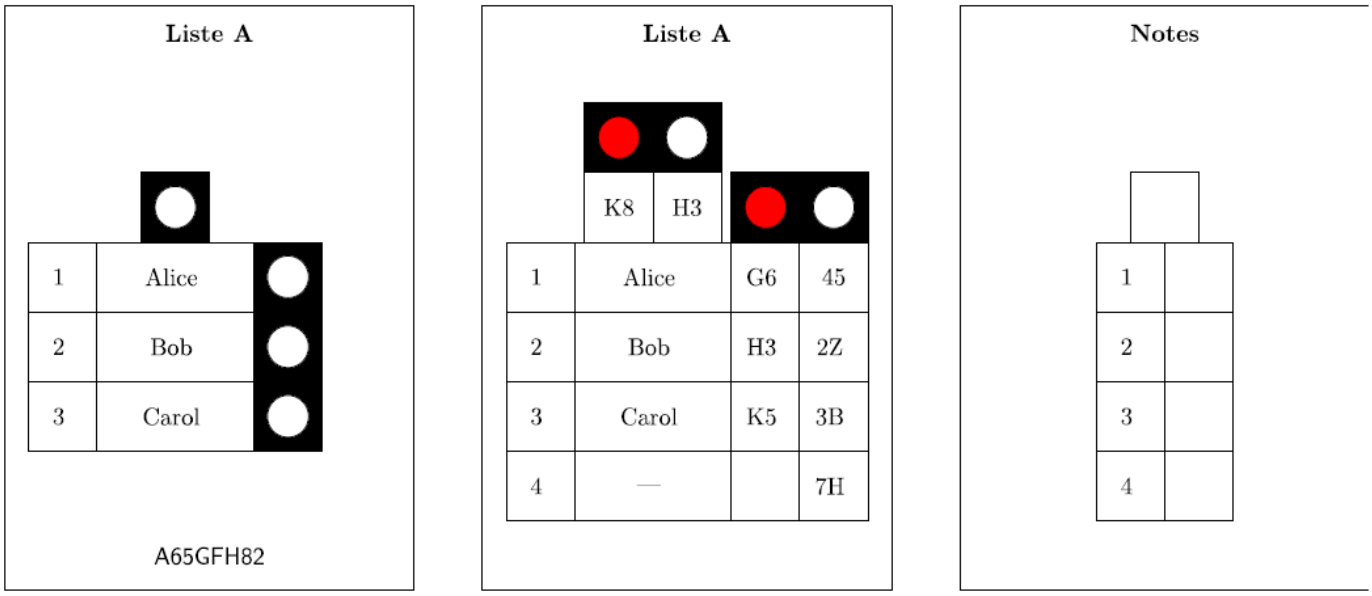
The blank ballot looks like a regular ballot, with two exceptions.
First, since this is to print this bulletin on A4 size paper using a conventional printer, it is not possible to indicate all the candidates on a single-sided as is the case on paper ballots used in polling stations today, ballots that are considerably larger than an A4 page. We therefore propose a presentation close to what is proposed for electronic voting: the ballot is structured over several pages, the first of which contains a list of parties among which candidates can be selected, and the following contain the candidates. It is suggested to use one A4 page per party.

Second, on each page of the ballot listing candidates, BS add a voting 128-bit random k token (or a little less if precautions are taken elsewhere). This token is the same on all pages of a ballot and unique per ballot - random choice is sufficient to guarantee this in practice. This token is printed in an easy-to-scan form, which could be an alphanumeric string of about twenty characters in OCR-B font for example (font which is used on machine-readable passports), or which could also be a QR-code. The first solution would be preferable in order to keep a ballot entirely readable by humans.

BS also provides each voter with code sheets. These look like the blank ballot paper, with two exceptions.
First of all, the k token is not there.
Second, each box that the voter can tick is replaced by two randomly chosen confirmation codes. The first of these codes will be used if the box is checked, the second will be used if the box is not checked. Each of these codes will be written with one easily readable by human beings, and is for example formed of 2 symbols at the Base32 format, which can be chosen from the 26 capital letters of the alphabet and the digits 2 through 7, providing a total of 1024 options. This length seems to be a good compromise between ease of use and safety.

The random distribution within which the confirmation codes are chosen should ensure that we never find two identical codes in the same row of an electoral list within the same ballot. For example, the confirmation codes associated with the third candidate listed on two separate lists must always be distinct. But it wouldn't be problematic to find the same confirmation code associated with the second candidate from a list and the fourth candidate from the same list, or from another list.

In practice, it is common for parties to nominate a different number of candidates. It is however necessary to ensure that the same number of codes is offered for all parties. This can be solved as follows: (1) we identify the greatest number of candidates proposed by a party, including list heading case. We will call this number c^{max}; (2) For all parties proposing less than c^{max} candidates, we will add a sufficient number of confirmation codes so that c^{max} pairs of confirmation codes are available. Finally, BS provides a note sheet for each voter, with c^{max} blank boxes. Each box has enough space for the voter to write down a confirmation code.
An example of a ballot, code sheet and score sheet is provided in the next figure (Figure 10).



Ballot sheet | Related code sheet | Notes sheet

Figure 10: The 3 different paper sheets type involved in the NETVOTING_BE solution

As BS produces these documents, it performs at the same time a series of cryptographic operations aimed at enabling the reception office and the scrutineers to produce the verification data for the voters.
We will assume that:
• BS has a public encryption key pk_T, the decryption key of which is distributed among the tellers (the participation of all the tellers is therefore necessary to decrypt information encrypted using pk_T - a system encryption like ElGamal can do this efficiently);
• Each ballot paper contains C candidates $c_1, ..., c_c$ where C is c^{max} multiplied by the number of lists;
• BS associated the candidate with the confirmation codes c_i^{yes} and c_i^{no} for the two possible options;
• F is a pseudo-random function (HMAC for example), which takes as input a key and a message.

When all the ballot papers have been produced, BS transmits to the scrutineers, for each ballot, 2C tuples calculated as $(c_i, j, Enc_{pkT}(c_i^j), F_k(i \,||\, j))$
where $i \in 1, ..., C$ and $j \in \{yes, no\}$. Before being passed to the tellers, these tuples are randomly permuted (which can be done simply by sorting them in order of $F_k(i \,||\, j)$ for example). These operations are intended to provide voters with guarantees that their ballot will be taken into account, and their role will be detailed in the stages of ballot processing at the reception desk and vote verification.

Finally, BS transmits to VS a list of tuples of the form (id, H (k)) where id is the identity (for example, the national registry number) of the person with whom the token k is associated, and where H is a hash function. BS is able to generate this information since he knows to whom he is giving the ballot containing the token k.

How to vote:
The voter who has registered for the postal vote can vote as follows. He / she starts by logging into the BS and identifies himself by means of his / her electronic identity card or other validated means and combining several factors (among the CSAM offer options, for example). Following this identification, the registered voter obtains their blank ballot, their code sheet and their score sheet as described above, all in pdf format.

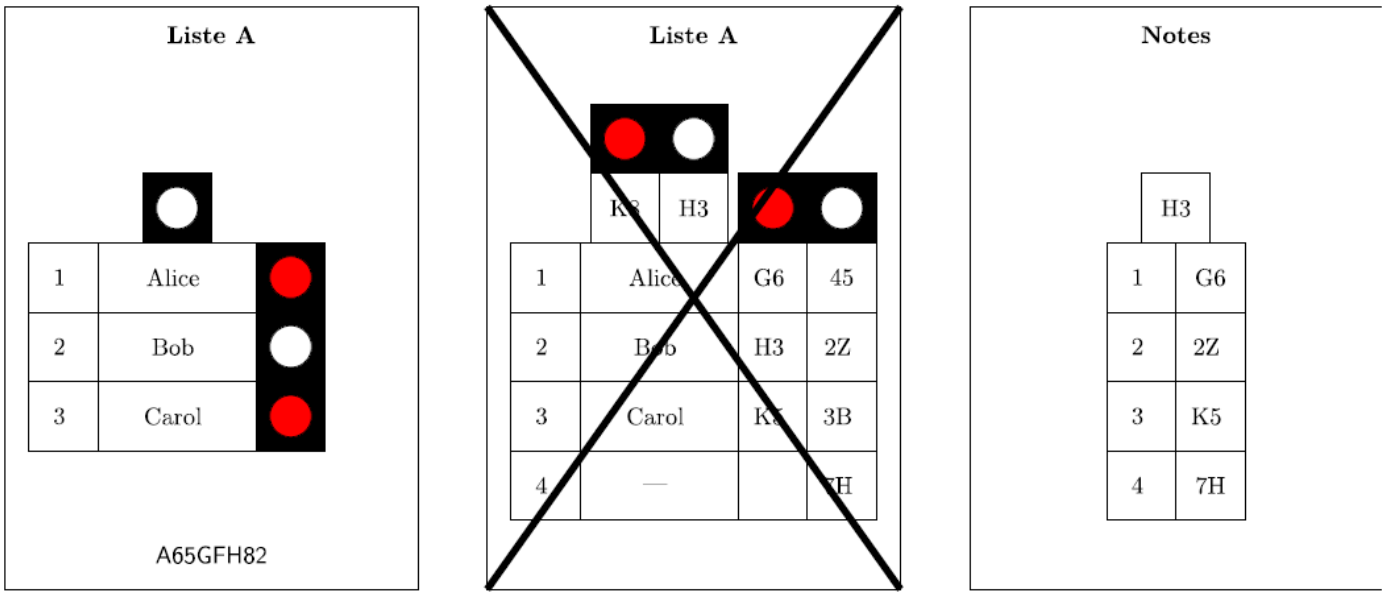
The voter prints these documents and completes his / her ballot which he / she can, if he / she wishes, return immediately. It should be noted that, in view of the size of the ballot papers used in Belgium, the return of all the pages of the ballot paper could come out of the standardized mailings and raise practical difficulties. The voter may, however, be content to return the single page of the ballot paper that corresponds to the list he / she supports. In case of blank vote, the sending of any page of the ballot, left blank, can also be done.
The vote will be considered valid when a valid key k is printed at the bottom of the ballot.

These steps are sufficient to vote. The voter who so wishes is, however, invited to take additional steps before returning his ballot, in order to allow monitoring and verification that it has been taken into account.

A first possibility offered to the voter is to connect to the verification server VS in order to ensure the validity of the token ó k present on his ballot paper. Preferably using a different machine from the one that was used to download the ballot, the voter will be invited to enter his token k in a web form, which will then calculate H(k) and send it to VS who will thus be able to verify that H(k) is well known to him and that the token is therefore valid.

Besides this guarantee of validity of the blank ballot paper, the voter has the possibility to ensure that his voting intention is correctly taken into account. To do this, the voter copies on his / her score sheet the confirmation codes associated with the choice made for each of the candidates within the party for which he / she has decided to vote, as well as the codes additional provided for parties proposing less than c^{max} candidates. Thus, if c^{max} = 20, the voter is invited to copy on his / her notes sheet 20 codes, i.e. 40 letters and numbers according to the example above. Attention should be given to facilitate this note taking as much as possible. For example, dotted marks could be added, indicating where to fold the code sheet and the score sheet so that the selected candidates, codes, and score boxes are facing each other, facilitating transcription.

At the end, the voter is invited to destroy his/her code sheet. It is important to destroy this sheet in all cases, both in paper version and in electronic version, whether the codes associated with the choices made or not have been noted: this is an important element to guarantee the confidentiality of the vote and may limit the risk of coercion. An example of a completed ballot paper, as well as the corresponding score sheets are given below (Figure 11).



Filled in ballot to be sent back | Code sheet to be destroyed | Optional notes sheet with associated copied codes

Figure 11: The 3 different paper sheets type involved in the NETVOTING_BE solution, filled in

The verification code encoding mechanism described above obviously raises important questions in terms of usability, and we will come back to this later when the description of the system is complete. We would just like to stress at this point that this step is absolutely not necessary to vote.

There are also significant differences and, in some respects, also a simplification, compared to the postal voting system currently offered to Belgians living abroad. As a reminder, the mail voting system currently used uses a double envelope system. In this system, the voter places their ballot in a first envelope (or their ballots in several separate envelopes if there are several elections). All these envelopes, along with an identification form, are put together in another envelope, which is sent to the main office chairperson on whom the voter depends.
At the main office, the outer envelope is opened, the identification form is examined and the elector's participation is marked on the attendance list. Then, each envelope containing a ballot paper is sent to the appropriate counting station. This double envelope system is necessary since the voter has no other way of proving her/his right to vote than by

attaching an identification form to his ballot paper. What is more, this mechanism is greatly facilitated in practice by the fact that the voter receives all envelopes, of the appropriate size, via their consular post.

In the process described above, the verification of identity and voting rights are done upstream, via the Internet, to obtain a ballot. It is the token k printed on the ballot paper that will guarantee, at the time of the count, that a ballot has indeed been transmitted by an authorized voter. It is thus possible to transmit a single envelope, which is less restrictive for a voter who therefore does not have to obtain envelopes of multiple sizes. The system is of course also compatible with a double envelope mechanism, which could for example be maintained in the event that it is deemed desirable to continue to allow the sending of an identification form in addition to the use of the token k.

The further steps upon ballot reception, tally phase, and so on are further described in the NETVOTING_BE paper (Pilet J.B., 2021).

This solution provides key major changes from previous STROBE Voting and other proposed postal voting solution options:

- It does not require a dual envelope concept, the empty ballot being downloaded and printed by the citizens from their computer
- It provides an end-2-end verifiability (Ballot being delivered AND part of the tally)
- It rely on the Belgian e-id or any Belgian CSAM authentication methods
- During the tally process, there is no direct mean for the involved people to get access of the voters identity
- It allows the usage of Risk Limit Audit (RLA)
- It is a transition step towards future possible Internet e-voting solution

Specific attention points raised by this solution:

- Limited Belgian e-id deployment (and activation) within Belgian abroad population. According to the Belgian Ministry of Foreign Affairs, there are currently 398.228 registered Belgian adult citizens living abroad (July 2021). From this population, only 3.797 have a Belgian e-id card, activated with a PIN and which have been used at least once on the Belgian e-consul portal.
  There are multiple reasons behind those numbers:
  - Belgian citizens living outside Europe do not need at all a Belgian ID card. Their Belgian passport and a local resident card are enough for them. Getting a Belgian e-ID is not so simple: they need to go in person to the Belgian embassy or general consulate. This embassy may be quite far away, especially in big countries like within the USA or, even long countries like Italy. Activating the e-ID does require a second journey to the Belgian embassy/consulate. Therefor some embassies are sending back the e-id card through postal mailing and advise the citizen to activate it in a later phase. This activation phase does often never happen, especially as the citizen has also to remember where she left her PUK paper. Typical cost for a Belgian e-ID abroad is 10 EUR. Belgian citizens living abroad may also request their Belgian e-ID at any Belgian municipality, while there are on visit in Belgium, but at the cost of 100-120 EUR/card (This latest option is not available for Belgian citizens who never were Belgian residents during their entire life. For those people, their e-ID must be issued by a Belgian embassy or general consulate).
    Furthermore, the expiration length of a Belgian ID is not the same as for the Belgian passport. So, they are not requested at the same time.
  - Belgian citizens living within Europe could rely only on their Belgian ID card, without the need of a passport. But for those citizens, their Belgian e-ID was often not activated as it was often sent back through the postal service, except within some smaller countries' embassies (Czech Republic for example). In those smaller countries, the e-ID are always activated (Source: Belgian embassy in Prague).
  - Especially within the long-term Belgian expat population, they do not use the Belgian e-id services: they don't need to fill in any Belgian tax form (taxonweb), they don't have any strong link with the Belgian social security (pension or any Belgian health insurance fund), nor use any other Belgian Federal e-services
  - The only e-ID service where the e-ID Belgian card is bringing a true added value today: remote e-signature for Belgian notarial acts. This service is used very infrequently, does require a compatible e-ID reader, and of course the pre-activation of the e-ID card.

- Belgian CSAM (outside the e-ID) main alternative option is the Itsme ® solution, especially since it allows to be used on non-Belgian mobile numbers since 2020. Unfortunately, the initial set-up for Itsme® registration for Belgian citizens living outside Belgium does first absolutely require an authentication through their Belgian e-ID card (so back to previous point), no Itsme® registration through any Belgian bank portal possible for this specific population (Source: Itsme® Onboarding service, Sylvie Vandevelde).

- If there is a collusion between someone who has access to the *BS* server (which does contain the link between the citizens and tokens), and another person who has access to the ballot's repository, there is a theoretical possibility to get the vote details of each citizen and the linked voters identity. In a country like Belgium today, this risk is probably limited. In order to avoid any issue, I would suggest:

    - to destroy the BS ballots-voters links repository, and any related paper versions, after a pre-defined period (ex. Max 3 months).
    - to monitor very precisely any activity on those two repositories, at least with the same audits/control level as the ones performed today on the Belgian National Register.

- Within the proposed NETVOTING_BE, there is a good suggested option to rely on scanners within the Belgian embassies/consulates for sending the ballots back to Belgium, with an adequate signature solution. We would recommend taking very specific measures to ensure confidentiality and integrity for those ballots content transmission, especially as the Belgian Ministry of Foreign Affairs network has been already confronted to intrusions in the past (Anciaux B., 2014) and (Vanhecke N., 2019).

- NETVOTING_BE security aspects should be handled very carefully at all layers: during the design phase, at applications layer, databases, middleware, servers, network, monitoring and access management layers. Different security best practices should be part of this solution implementation: Clear networks segregation of the BS server from the other components, encryption at DB layers and applications layers, token-users links DB contents with a short expiration time period, …
  If the SPF Interior IT environment would be hacked, all votes could theoretically be linked to their respective voters. This is not a theoretical hypothesis as hacking already did happen recently within this SPF Ministry (Vanhecke N., 2021).

  It is not only the election itself which could be damaged due to a security flaw, but also the citizen trust within the Belgian authorities. Such kind of trust damages could take a very long time to be recovered.

4.5. Proposed Postal Voting options comparison summary

Within the above paragraphs, we have covered different possible postal voting options, starting from current pure traditional paper based dual envelope concept, then elaborating an evolution step by including some crypto options inspired from the STAR-Vote, up to the new STROBE and NETVOTING_BE solutions.

Before going into the summary comparison, we would like to identify some attention criteria for the different Postal Voting options evaluated. We will rely on some of the feedbacks proposed within the "Summary of the expert dialog" document which has taken place last year for the evaluation of the Internet Voting Trials in Switzerland by the CH Federal Authorities (Bundeskanzlei BK - CH, 2020).
Conducting an expert dialog for drafting recommendations with international experts from different horizons for various possible issues on proposed new voting solutions is an open approach to build a future oriented and trustworthy solution.
We will not go throughout all questions/feedbacks which have been submitted to those experts, but we selected some of them which seems key attention points or differentiators for at least one of the 3 new proposed Postal Voting solutions.

1. Examination of Cryptographic Protocol and proofs
   The "4.2 Paper based voting procedure + cryptographic options" is a pure *personal* evolution from STAR-Vote solution. This personal proposal has not been validated/reviewed/challenged by known experts yet. There is a higher risk for cryptographic issues due this its lower maturity vs the STROBE-Voting and NETVOTING_BE proposed solution.
   The "4.3 STROBE-Voting" has been not yet officially peer reviewed and the proposed implementation for the specific Belgian context is proposed by a humble student. Even if this paper has been written by a renowned expert, the proposed specific implementation may still contain holes.
   The "NETVOTING_BE" has been specifically developed for the Belgian Federal election's context, and validated by renowned experts, based on well-known cryptographic standards. The cryptographic holes risk is then perceived lower than for the other proposed options.

2. Reviews of Operations
   The "NETVOTING_BE" has been relatively detailed in its proposed implementation within the (Pilet J.B., 2021) document, specifically for the Belgian context, while the other scenario are kept at higher level. The devil is often in the details, and risks are then perceived higher within those other options at the current stage. The "NETVOTING_BE" solution requires only papers to be sent from the citizen, while empty ballots are being downloaded by the citizens and no postal mailing are required from the Ministry of Interior.

3. Diversity to support security and trust-building
   As well detailed and recommended by the experts to the CH authorities (Bundeskanzlei BK - CH, 2020, p17 "*Diversity in IT Security*" and p19 "In short"), diversity justifies the added complexity for improved security, and this at all stages and levels (development and infrastructure). This is applicable for the different proposed solutions. On top of the experts recommended diversification in 5.2.3 "Independence" (Bundeskanzlei BK - CH, 2020, p11), we propose to add also diversity at the IAM (Identity and Access Management) layer used for the different components for the future voting system: If there is a single IAM solution at Ministry of Interior or Ministry of Foreign Affairs, and this IAM solution is hacked, all the proposed secure voting solution could be compromised. With the recent attacks both of those Ministries were facing ((Vanhecke N., 2021) and (Vanhecke N., 2019)), this possible threat may not be only theoretical anymore in the future.
   With this possible theoretical IAM risk context, the NETVOTING_BE option is perceived with a little higher risk than the STROBE-Voting, as the votes could theoretically be identified in those specific circumstances.

4. Central Printing-Office
   It is key component which imply that the printed cryptographic values are not divulged. Specific care needs to be taken for all operations related to printing and paper handling. Fully printed @Home approach proposed by the NETVOTING_BE scenario is not exposed to the experts' described risks as the printed documents will be done directly by the citizens on his/her own printer.

5. Verifiability
   In the CH proposition the voters can use a Public bulletin Board (PB) for individual and universal verifiability. With this alternative they do not have to trust the voting system. The trust-assumptions are shifted. The "4.2 Paper based

voting procedure + cryptographic options" and "4.3 STROBE-Voting" rely on a PB concept, while the "4.4 NETVOTING_BE" do propose a different Verifiability mechanism which is at least as robust as the PB concept. The NETVOTING_BE could even be perceived by some experts to be higher in quality as the citizens have to authenticate against the *VS*, to get their verification codes, and can then confront it with their note sheet. Those experts are sometimes not in favor of PB as they may leak information how a voter voted (Bundeskanzlei BK - CH, 2020, 7.4.5 p30).

6. Usability and Performance
   "*Usability and performance have been mentioned as examples of external attributes of the software that should be taken up in the examination framework*" (Bundeskanzlei BK - CH, 2020, 7.4.5 p35). We may perceive the usability relatively equivalent between the different proposal, except for the "4.2" which does require the usage of your own computer to vote and print the filled in ballot. This vote through computer requirement may increase the usability complexity and be a lowering factor to the vote participation.

7. Integrity
   With the current vote by mail solution, we may see threat to integrity, as ballot modification would be undetected. The risk is limited as it would require major manual activities to represent real elections result modification. The main risks are at places where a lot of ballots would be handled.
   Within option "4.2 Paper based voting procedure + cryptographic options", this risk is negligeable as the vote is transmitted through a dual channel (electronically AND ballot paper). Any discrepancy will be directly detected.
   Within STROBE-Voting and NETVOTING_BE options, threat to integrity do exist as for current traditional Vote-by-Mail but should be detected if citizens do perform their verification.

8. Confidentiality
   Possible threats are already described here above, Cfr specific required care (cf here above "4. Central Printing-Office") for all options requiring ballots/Postal Voting Attest being centrally printed and sent; and for NETVOTING_BE there is also a risk in case of collusion between the administrator of the *BS* and *VS*, or in case of the IAM system(s) managing those *BS* and *VS* is/are compromised (cfr here above "3. Diversity to support security and trust-building").

9. DDoS & Social Engineering
   Some of the proposed solutions do require an online connection to some central servers (printing a ballot, a Postal Voting Attest, transmitting an encrypted vote, authentication for vote verification, …) and could be affected by a massive DDoS. A massive DDoS attack could affect the central Ministry of Interior accessibility, and therefore the participation to the elections, cfr the 4th of May 2021 DDoS attack (Safeonweb, 2021). The STROBE-Voting option, with Postal Voting Attest, do not require any on-line connectivity for the vote process, just for the verification, and is therefore a bit less exposed to this risk than the other proposed options. Even though the DDoS risk is more limited than for a pure Internet voting solution as the Vote-by-Mail do require a paper ballot to be sent back and so those actions are typically spread over a few days period prior to the election date.

10. Malware infection at the voter side
    For the options where a computer is required at some steps from the voter (downloading a ballot or Postal Voting attest, ballot pre-filling via a computer, printing a ballot or a Postal Voting Attest), there is always a risk of local infection. This could allow leakage of sensitive/vote information, or even vote manipulation in case of ballot pre-filling on a computer (Distinct information could be shown/printed versus information sent encrypted to the central server).
    For this topic, the most secure option is the STROBE-Voting option with the PVA, as this will not involve any computer activity from the voter.
    The most exposed option will probably be the "4.2" as it includes ballot filling/validation on a computer, which could lead to partial vote manipulation. In case of such kind of attack, this should be identified through (RLA) audits which could highlight ballots discrepancy. This kind of attack could also allow vote content leakage for this option. That's why we have allowed the voter to print different possible voting scheme, while he/she will only be able to send back one of his/her printed ballot. This could limit the possible leakage impact in case of voter's doubt about his/her computer security.

The other options are exposed to suck risk when a download is required from the voter's computer, this could allow the attacker to submit a similar ballot. This would lead to two same ballots (with different votes) being submitted, but no voter's content has not leaked. Duplicated ballots with the same ballot IDs should be rejected.

We propose here after (Figure 12) a key summary of pro/con and attention points of those different proposed solutions, based on the experts' criteria explained here above:

	4.1 Current VbM	4.2 STAR-vote/ElectionGuard like	4.3 Strobe w/ PVA	4.3 Strobe wo PVA	4.4 NetVoting_BE
Cryptographic Protocol & proofs	N/A	*	**	**	***
Usability	**	*	**	**	**
Integrity					
Ballot Integrity	-	***	**	**	***
Confidentiality					
Central Printing-Office	***	***	**	N/A	N/A
at user side	**	*	**	**	**
At Ministry of Interior, after ballot ta	***	***	***	**	**
E2E verifiability					
Postal Voting Attest received	-	**	**	N/A	N/A
Verify My Vote is part of the tally	-	***	***	***	***
Ballot not tallied on BB	N	Y	Y	Y	N
Attacks					
DDoS exposure	N/A	*	**	**	**
Option					
Multiple Voting option	N/A	N/A	N/A	Optional	Optional

Figure 12: Table summary differences for the different Postal Voting solution analyzed

Legend:

N/A	: Not Applicable
-	: Major risk
*	: Low quality for this criterion
**	: Medium quality for this criterion
***	: High quality for this criterion

The STROBE solution has been evaluated with two flavors: one with the Postal Voting Attest (PVA), and the other one without any paper based Postal Voting Attest. In this latest flavor, we would rely on the NETVOTING_BE proposed option (e-ID authentication) where the citizen would download his/her empty ballot.

If we would like to add a possible Multiple Voting option (the voter has change her/his mind), we could add a value field on each ballot. If two ballots are counted with the same token, we would keep the ballot with the highest number on it (suggestion proposed by mail by J. Benaloh).

As expected, the least secure approach is the current one used for the Vote by Mail.

We have then two categories: one with Postal Voting Attest (PVA), ElectionGuard like and STROBE, and another one without PVA (STROBE and NETVOTING_BE). The main risks exposure is different between those two options.
For the first one (with PVA), the main risk exposure does happen during mail transport and the first envelope opening. In order to limit the risk during the first envelope opening phase, we would recommend allowing this phase to be handled only with the presence of assessors, but can't manage the risk during the mail transport. The risk could be perceived as high for a low scale, while being with a lower probability at a very high scale (but can't be excluded).
For the second one (without PVA), the risk is completely different: the risk is low, but if it happens, the entire voters and ballots link could be exposed (cfr description at the end of 4.4 paragraph).

NETVOTING_BE is probably the most mature proposed solution, where specific security measures and isolation should be taken during design, implementation, and production phase (Cfr 4.4 paragraph).

We would also recommend performing:

- Recurrent security pen-tests and audits on both SPF Ministries (Interior and Foreign affairs) IT environments. If no major concerns or hacking issues have been raised during, for example the latest 3 years period, we could recommend a postal voting solution based on e-ID authentication (without paper based Postal Voting Attest).
- As recommended by the experts for the Switzerland e-voting project, specific pen-tests and bounty program for the new proposed postal voting solution.
- Global experts dialog review of the proposed solution as the Helvetic Federal authorities did for their e-voting solution review.
- Make the required IT investments within both SPF Ministries (Interior and Foreign affairs) to update their IT environment to the required security level for such kind of project.
- TNG (Tests Grandeur Nature as the French government is calling it). For the latest French elections which did happened in May 2021 for the French citizens living abroad (205.895 voters, from which 176.734 did vote through Internet) (France, 2021), the French government performed two major tests at a relative big scale with 12.943 test users (France, 2019). This helped a lot to fine tune the different processes and technical components. This kind of tests should also be used for the rollout of a future new Belgian Postal Voting project.
- A review of the current e-ID and its related PIN code activation processes for the Belgian citizens living abroad (Cfr details developed in paragraph 4.4 above). We suggest using some of the following ideas to increase the e-ID usage and PIN activation:
    - Lower the cost for the Belgians living abroad for requesting their e-ID card while they travel in Belgium
    - Propose to deliver/renew the e-ID card for this population free of charge while they renew their Belgian passport
    - Change the current process to request only one single visit to the embassy/consulate instead of the current two ones (Current required visits: One for the e-ID card request, and another one a few weeks later for the e-ID card activation). Possible options are for example: initial random PIN code can be preloaded on the eID card and sent via SMS to the citizen, while the eID could be “activated” after validation through an out-of-band validation (SMS and/or eMail validation). PIN codes can also be changed by the citizen through the eID viewer app.
    - Monitor the level of e-ID PIN activation for Belgian citizens living abroad. This should be done in collaboration with SPF Interior. This monitoring is not performed yet, nor planned for the near future, according to Mrs Van de Voorde (SPF Foreign Affairs, in charge of Population and Electoral affairs).
    - In some big countries like in the USA, there is a Belgian truck crossing some states to handle specific Belgian administrative matters. This truck, where available, is coming only once a year and is only accessible during a single weekday during office hours. This is quite limiting, especially in a country like the US where holidays periods are very limited. Extending the opening hours of this mobile office could also help its accessibility (feed-back received from some Belgian US residents)
    - Add some new additional value/services to the current limited services provided through the e-consul portal, like on-line delivery of some official attests (ex. Attest of residence, Belgian birth certificate, …)
    - Develop some marketing towards this specific population for some other services which can be used with their e-ID: Belgium notarial services which can be “e-signed”, registering a new company within Belgium, …
    - In collaboration with the Itsme® company, motivate this population to create their Itsme® account. If this population could be authenticated on the e-consul portal thanks to Itsme® app, they could also on-line declare when they have lost some of their Belgian papers (passport, e-ID or driving license) and request on-line a new one. Thanks to Itsme®, other services might be developed specifically for this population, like opening of a banking account in Belgium remotely. Itsme® usage would also lowering the often issues encountered with USB e-reader conflicts, and this could be very useful in peak usage periods, like during elections periods.

5. Conclusion:

Even if vote by Internet is not fully ready yet for public elections as highlighted from most worldwide specialists, there are now solutions for vote-by-mail which allow End-2-End verifiability AND public results verification.
In this study, three major different possible options have been highlighted and described in the context of Belgian Federal elections.
Some may still see those approaches as relatively "heavy" as they still rely on paper-based ballots. According to the current literature and specialists, paper-based ballots is for the moment still the most reliable and safer option.
We could avoid the paper Postal Voting Attest and the related dual envelope concepts by relying on the Belgian e-ID. This would also eliminate to send the paper ballots to the citizens as they could print them directly locally.

Some important steps prior to the implementation of this new voting schema:

- E-ID deployment and activation should be increased (Cfr details in paragraphs 4.4 and 4.5)
- IT Security aspects should be handled with required methods, processes, and investments, especially for both involved Ministries (Interior and Foreign Affairs) (Cfr details in paragraph 4.5)
- Plan a real TNG test ("Tests Grandeur Nature" like the French authorities called it) prior to the real elections (France, 2019)
- Plan an open dialog with international experts like for the Helvetic Federal e-voting project (Bundeskanzlei BK - CH, 2020).

Remote voting could help to increase the current voting ratio of this population, currently around 30% (from the 400.000 Belgian adults known living abroad, from which 44% did register for the latest elections) (Numbers provided by the Ministry of Foreign Affairs). This could also help to strengthen the links with their Belgian country.

After the recent COVID-19 experience, we are convinced vote-by-mail will be gradually more and more an option evaluated and piloted in different countries. To keep/improve citizens confidence in our election systems, bringing end-2-end verifiability and public results verification could be a good step forward, not only for vote-by-mail but also for all voters.

As similarly mentioned by other authors (Bundeskanzlei BK - CH, 2020, p. 76), *the inherent risks of deploying new voting solution*, like the ones presented in this report, *must be carefully balanced against the bigger picture risks of not having it*. Especially as those new solutions can be an initial first step before implementing a full mature internet voting solution.

We hope this work have helped the comprehension of this broad hot subject through another angle than each of the separated paper already published on this subject.

6. Acknowledgments:

This study would not have been possible with the collaboration of different people.
I would like to thank them all for the support, feedbacks and help:

At UCLouvain, Olivier Pereira and his team for the fast responses, trust, suggestions, and availability.

At ULB, Olivier Markowitch for his precious advises and review feedbacks.

Different Belgian expats shared a lot of information about their current experiences, made suggestions and performed some tests for this study: Benjamin de Foy (USA), Claire Jonard (Switzerland), Pierre-Nicolas Pirotte (Spain), Vinciane Abeels (Italy).

At the SPF Foreign affairs, I did receive a lot of attention for this project. They were always trying to get the requested information throughout their different departments. They also took the time to share with me how different aspects were currently handled: Grégoire Cuvelier (Ambassador in Czech Republic) and his wife Bernadette, Laura Van de Voorde (Population service & Electoral affairs), Alain Gérard (Archives responsible), and all their colleagues who provided me continuously all possible useful information.

At Itsme®, I did receive also fast response for my inquiries, even during their holiday periods: Sylvie Vandevelde (Onboarding service).

Josh Benaloh (Microsoft Research) who took quite some time to exchange ideas and suggestions about Postal Voting with an unknown student from the other side of the world.

Louise Nikolic (previous Belgian country expert representative to the GLOBALCIT's – Global Citizenship Observatory) for her precious and precise information provided.

At IBM: Bert De l'Arbre, Jeroen Caubergs, Marie-Catherine Schrans, and other IBM colleagues who helped and supported me to combine this program with my current professional activities.

At home, from my whole family who lived with an additional student. They also took the time to understand the proposed Postal voting topic and asked right questions.

To all of you, and those who I forgot to list, I would like to thank you all as this work would not have been possible without you.

7. References

Here after the different references used within the present document.

Adida B., de Marneffe O., Pereira O., Quisquater J.-J. (2009), *Electing a university president using open-audit voting: analysis of real-world use of Helios*, EVT/WOTE'09: Proceedings of the 2009 conference on Electronic voting technology/workshop on trustworthy elections

http://www.usenix.org/events/evtwote09/tech/full_papers/adida-helios.pdf

AEC – Australian Electoral Commission, General Postal Voters (2020),

https://www.aec.gov.au/Enrolling_to_vote/Special_Category/general-postal-voters.htm

General Postal Voter application form:

https://formupload.aec.gov.au/Form?FormId=GPV

Anciaux B. (2014), *de mogelijke hacking van de computers bij Buitenlandse Zaken*, Belgische SENAAT, SENAAT Schriftelijke vraag nr. 5-10462
https://www.senate.be/www/?MIval=/Vragen/SVPrint&LEG=5&NR=10462&LANG=nl

Barabara M.-A., Dumont J.-C. (OECD), Spielvogel G. (OECD) (2021), *De la France vers le monde : que révèle l'augmentation de l'émigration française ?*, in Trésor-Éco Nr 275, Direction Générale du Trésor (FR)
https://www.tresor.economie.gouv.fr/Articles/0aedd999-fc50-4533-98af-063144a42a54/files/b5428cf3-e5dd-41d2-90de-ca97b181c834

Baruch B., Devaux A., Faulí C., Folkvord F., Lupiáñez-Villanueva F., Nederveen F., Porcu F., Stewart K, Taylor J. & Theben A. (2018), *Study on the Benefits and Drawbacks of Remote Voting*, European Commission DG Justice & Consumers, Brussels

Summary: https://ec.europa.eu/info/sites/info/files/remote_voting_main_findings.pdf

Full: https://ec.europa.eu/info/sites/info/files/20181121_remote_voting_final_report_final_clean.pdf

Belgium - Direction générale Institutions et Population (2020), *Procédure ouverte pour la réalisation d'une étude empirique sur la faisabilité de l'introduction du vote par internet en Belgique*

Numéro de référence: IBZ-ADIB-ELECT-1-2020-F03_0

https://ted.europa.eu/udl?uri=TED:NOTICE:270135-2020:TEXT:ES:HTML&tabId=1&tabLang=fr

Bell S., Benaloh J., Byrne M., DeBeauvoir Dana, Eakin Bryce, et. al. (2013), *STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System.*, USENIX Journal of Election Technology and Systems (JETS), Vol. 1, no.1, p. 18--37

http://hdl.handle.net/2078.1/142427

Benaloh J. (2006), *Simple verifiable elections*, InProc. 1st USENIX AccurateElectronic Voting Technology Workshop
https://www.usenix.net/legacy/events/evt06/tech/full_papers/benaloh/benaloh.pdf

Benaloh J., Ryan P., Teague V. (2013), *Verifiable Postal Voting - Security Protocols XXI: 21st International Workshop*, Cambridge UK
Detailed paper: https://www.microsoft.com/en-us/research/publication/verifiable-postal-voting/
Summary presentation: https://wwwen.uni.lu/content/download/61906/723034/file/Teague.pdf

Benaloh J. (2021), *Microsoft ElectionGuard - Enabling voters to verify that their votes are correctly counted*. Microsoft project and presentation
https://github.com/microsoft/electionguard
https://www.microsoft.com/en-us/research/video/microsoft-electionguard-enabling-voters-to-verify-that-their-votes-are-correctly-counted/

Benaloh J. (Sept., 2021), *STROBE-Voting: Send Two, Receive one Ballot encoding* – E-Vote-ID: 6th International Joint Conference on Electronic Voting 2021.
Proceedings should be published soon by Springer.

Blaise P. (2016), Le vote des Belges de l'étranger, Courrier hebdomadaire du CRISP, 2016/25 n°2310
https://www.crisp.be/2017/02/le-vote-des-belges-de-letranger/
https://www.cairn.info/revue-courrier-hebdomadaire-du-crisp-2016-25-page-5.htm (free pdf version)

Bloomgarden A., Gupta A., Jensen G., Levine Z., Middleton C., Sikora K. (2020), *Stanford-MIT Healthy Elections Project: Behind the Scenes of Mail Voting: The Rules and Procedures for Signature Verification*
https://healthyelections.org/sites/default/files/2021-06/Signature_Verification.pdf

Braun N., Ellis A., Gratschew M., Morales I., Navarro C. (2007), *Voting from Abroad – The International IDEA Handbook*, Stockholm: IDEA (International Institute for Democracy and Electoral Assistance). Page 41.
https://www.idea.int/sites/default/files/publications/voting-from-abroad-the-international-idea-handbook.pdf

Bundeskanzlei BK – CH (2020), *Summary of the expert dialog, Redesign of Internet Voting Trials in Switzerland 2020*, Confédération Suisse
https://www.bk.admin.ch/bk/en/home/politische-rechte/e-voting.html
https://www.bk.admin.ch/dam/bk/en/dokumente/pore/Summary%20of%20the%20Expert%20Dialog%202020.pdf.download.pdf/Summary%20of%20the%20Expert%20Dialog%202020.pdf

Burt T. (2020), *Innovative new uses of ElectionGuard*, Microsoft – On the Issues.
https://blogs.microsoft.com/on-the-issues/2020/12/04/electionguard-2020-elections-security-pilot/

Culnane C., Ryan P. Y. A., Schneider S. and Teague V. (2015), *vVote: a Verifiable Voting System*, Technical Report Version 4.0. Page 10
https://arxiv.org/pdf/1404.6822.pdf

CISA/NIST/FBI/EAC (June 2020), *Risk Management for Electronic Ballot Delivery, Marking and Return*.
This document was available on https://www.cisa.gov/protect2020. It has been recently "archived" from the authors' web site. A copy is still available from the AAAS (American Association for the Advancement of Science):
https://www.aaas.org/sites/default/files/2020-06/CISA%20Risk%20Management%20Electronic%20Ballot.pdf

CoE (2017), Council of Europe, *Recommendation CM/Rec(2017)5[1] of the Committee of Ministers to member States on standards for e-voting*
https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680726f6f

Droit R.-P. (2008), *L'Occident expliqué à tout le monde*, Le Seuil, Paris.

Elections Québec (2020), *Vote par Internet*
https://docs.electionsquebec.qc.ca/ORG/5ee22b6ce7bac/DGE-10627_VPI-VF.pdf

FRANCE (2109), *Elections des conseillers des français de l'étranger et des délégués consulaires vote électronique – compte-rendu du second test grandeur nature*.
https://www.diplomatie.gouv.fr/IMG/pdf/compte-rendu_du_second_test_grandeur_nature_cle8199cc.pdf

France (2021), *Elections consulaires des 29 et 30 mai 2021 - résultats*
https://www.diplomatie.gouv.fr/fr/services-aux-francais/voter-a-l-etranger/resultats-des-elections/article/elections-consulaires-des-29-et-30-mai-2021-resultats

French Senate – FR (2021), *Législation Comparée – Recueil sur le droit Electoral (Vote par correspondance – Modalités d'inscription sur les listes électorales – Vote électronique),* « Allemagne - Australie - Autriche - Belgique - Danemark - Espagne - Estonie - États-Unis - Finlande - Grande-Bretagne - Irlande - Italie - Portugal - Pays-Bas - Portugal - Suède – Suisse », Direction de l'initiative parlementaire et des délégations, Document LC 293.
http://www.senat.fr/lc/lc293/lc293.pdf

Halpen S. (2020), *The Future of Democracy - Can Our Ballots Be Both Secret and Secure?* – based on an interview of Josh Benaloh
https://www.newyorker.com/news/the-future-of-democracy/can-our-ballots-be-both-secret-and-secure

IDEA (2010), *Electoral Justice: The International IDEA Handbook*, Institute for Democracy and Electoral Assistance
https://www.idea.int/sites/default/files/publications/electoral-justice-handbook.pdf

IFES, *The International Foundation for Electoral Systems*
https://www.ifes.org/issues/electoral-management

Juels A., Catalano D. and Jakobsson M. (2002), *Coercion-Resistant Electronic Elections*
https://eprint.iacr.org/2002/165

Killer C., Stiller B. (2019), *The Swiss Postal Voting Process and Its System and Security Analysis*, Zurich.
DOI: 10.1007/978-3-030-30625-0_9, "Fourth International Joint Conference on Electronic Voting, E-Vote-ID 2019". Proceedings. Page 90-105
https://www.zora.uzh.ch/id/eprint/175950/1/Krimmer_et_al_E-Vote-ID_2019.pdf#page=102

Lafleur J.-M., Nikolic L., Vintila C. D. (2018), *Report on political participation of mobile EU citizens : Belgium*, GLOBALCIT, Political Participation Reports, 2018/13, [Global Citizenship]
https://cadmus.eui.eu//handle/1814/59565

National Academies of Sciences, Engineering, and Medicine (2018), *Securing the Vote: Protecting American Democracy*. Washington: The National Academies Press.
https://www.nap.edu/resource/25120/Securing%20the%20Vote%20ReportHighlights.pdf
https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy

NIC, National Intelligence Council (2021), *Foreign Threats to the 2020 US Federal Elections*. ICA 2020-00078D
https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf

OECD (2006), Emigrations rates of high-educated to OECD countries, 2000 and 2005/2006
https://www.oecd.org/els/mig/Emigration%20rates.pdf

OSCE, Organization for Security and Co-operation in Europe (1990), *Copenhague document*
https://www.osce.org/files/f/documents/9/c/14304.pdf

OSCE, Organization for Security and Co-operation in Europe (2007), *Election Observation Handbook*
https://www.osce.org/files/f/documents/e/b/14348.pdf

OSCE, Organization for Security and Co-operation in Europe (2020), *General Elections, 3 November 2020*
https://www.osce.org/odihr/elections/usa/456787

Pickles E. (2016), *Securing the ballot - Report of Sir Eric Pickles' review into electoral fraud*, London.
Sir Eric Pickles MP - Government Anti-Corruption Champion (UK). Page 22, points 70 – 72 + 73-84
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/545416/eric_pickles_report_electoral_fraud.pdf

Pilet J.-B., Preneel B., Erzeel S., Pereira O. et al. (2020), ULB Cevipol – KULeuven Cosic – VUB PolicyLab – UCLouvain Crypto Group, *PROJET NETVOTING_BE Étude sur la possibilité d'introduire le vote Internet en Belgique*.
https://elections.fgov.be/sites/default/files/inline-files/Rapport_volet_1_4Dec2020_Def_F.pdf

Pilet J.-B., Preneel B., Erzeel S., Pereira O. et al. (2021), ULB Cevipol – KULeuven Cosic – VUB PolicyLab – UCLouvain Crypto Group*PROJET NETVOTING_BE Étude sur la possibilité d'introduire le vote Internet en Belgique, Volet 2*.
https://elections.fgov.be/sites/default/files/inline-files/Report_volet2_25March2021_Def_F.pdf

Safeonweb (2021), *Belnet victim of DDoS attack. What is this and how could it happen?*, Center for Cybersecurity Belgium (CCB)
https://www.safeonweb.be/index.php/en/news/belnet-victim-ddos-attack-what-and-how-could-it-happen

STHV - Stichting Tegen Hackbare Verkiezingen – NL (2020), *Verkiezingen en optelcomputers: een oproep tot onafhankelijke controle in het belang van betrouwbare verkiezingen*
https://hackbareverkiezingen.nl/wp-content/uploads/2020/11/Verkiezingen-en-optelcomputers-een-oproep-tot-onafhankelijke-controle-in-het-belang-van-betrouwbare-verkiezingen-v1.0.pdf

The House of Commons – UK (2004), *Postal Voting*, Seventh Report of Session 2003-04, London.
https://publications.parliament.uk/pa/cm200304/cmselect/cmodpm/400/400.pdf

Thornton A. (2020), *What is ElectionGuard?*, Microsoft – On the Issues.
https://news.microsoft.com/on-the-issues/2020/03/27/what-is-electionguard/

University of Florida (2020), *The Elections project*.
Postal votes : https://electproject.github.io/Early-Vote-2020G/index.html
Total number of votes : http://www.electproject.org/2020g

UN-HR, United Nations Human Rights (1996), *International Covenant on Civil and Political Rights*, article 25 (b).
https://www.ohchr.org/Documents/ProfessionalInterest/ccpr.pdf

Vanhecke N. (2019), *Hackers Buitenlandse Zaken blijven nuiten schot*, De Standaard (20/09/2019)
https://www.standaard.be/cnt/dmf20190920_04618665

Vanhecke N. (2021), *Binnenlandse Zaken al twee jaar gehackt*, De Standaard (25/05/2021)
https://www.standaard.be/cnt/dmf20210525_96103510

Venice (2012), *The European Commission for Democracy through Law* - better known as the Venice Commission as it meets in Venice - is the Council of Europe's advisory body on constitutional matters. Cfr in particular their "*Declaration of global principles for non-partisan election observation and monitoring by citizen organizations and code of conduct for non-partisan citizen election observers and monitors"*.
https://www.venice.coe.int/webforms/documents/default.aspx?pdf=CDL(2012)032-e&lang=EN

Wagner R. (2020), *Responding to COVID-19 with 100 per cent postal voting: Local elections in Bavaria, Germany*. Stockholm: IDEA (International Institute for Democracy and Electoral Assistance). Page 8
https://www.idea.int/sites/default/files/responding-to-covid-19-with-postal-voting-local-elections-in-bavaria.pdf

Wilmet S. (2020), *Note de Politique Générale - Affaires étrangères, Affaires européennes et Commerce extérieur*, Brussels, *Chambre des Représentants de Belgique*, Doc 55 1580/020, Page 17
https://www.lachambre.be/flwb/pdf/55/1580/55K1580020.pdf

Wofford B. (2020), *A Texas County Clerk's Bold Crusade to Transform How We Vote*, WIRED magazine
https://www.wired.com/story/dana-debeauvoir-texas-county-clerk-voting-tech-revolution/

8. Table of Figures

Rue Archimède, 1 bte L6.11.01, 1348 Louvain-la-Neuve, Belgium **www.uclouvain.be/epl**