# Voter Authentication in Remote Electronic Voting Governmental Experiences: Requirements and Practices

Adrià Rodríguez-Pérez[1,2](✉), Jordi Cucurull[1], and Jordi Puiggalí[1]

[1] Scytl Election Technologies, S.L.U., 08021 Barcelona, Spain
{adria.rodriguez,jordi.cucurull,jordi.puiggali}@scytl.com
[2] Universitat Rovira i Virgili, 43002 Tarragona, Spain

**Abstract.** How to ascertain that the person voting behind a computer or smartphone screen is actually who they claim to be remains one of the key challenges in remote electronic voting. Credentials to vote online can be shared, stolen, or traded. For this reason, it is generally argued that introducing remote electronic voting from uncontrolled environments for political public elections is only feasible as long as a robust infrastructure for the digital identification of voters (e.g., based on electronic identity documents, e-ID) is already in place. But is such a digital infrastructure for voter authentication a *sine qua non* condition for remote electronic voting? In this paper we assess how voters are authenticated in internet voting for political public elections in nine countries: Australia, Canada, Estonia, France, Mexico, Pakistan, Panama, Switzerland, and the United States of America (USA). To the best of our knowledge, this is the broadest comparative assessment of voter authentication methods in governmental remote electronic voting experiences. Our analysis reveals that the use of solely knowledge-based factors for voter authentication is the most common practice in these experiences. In most cases, a combination of several credentials is used (e.g., in Canada and Australia). Another alternative is to rely on a different combination of knowledge and ownership-based authentication methods that does not require neither e-IDs nor digital certificates (e.g., as in France and Mexico).

**Keywords:** Voter authentication · Remote electronic voting · Equal suffrage

## 1 Introduction

How to achieve both the "unique voter identification (only eligible voters can cast a vote and those only once) and anonymous vote casting (the voter must be anonymous when he [sic] casts a vote) at the same time"[1] (Volkamer 2009: 2) remains today one of the key

[1] It should be noted that it may not be necessary to guarantee the anonymity of encrypted votes as soon as they are cast. As a matter of fact, in certain cases it may be even necessary to maintain a link between the encrypted vote cast and the identity of the voter who has cast it until the decryption stage (e.g., when multiple voting is supported).

Published by Springer Nature Switzerland AG 2022
R. Krimmer et al. (Eds.): ePart 2022, LNCS 13392, pp. 3–18, 2022.
https://doi.org/10.1007/978-3-031-23213-8_1

challenges of remote electronic voting[2] from uncontrolled environments[3]. How could it be ascertained that the person voting behind the computer or smartphone screen is actually who they claim to be and not someone who has forced them to hand them their credentials? Or who has stolen them? Or who has bought them?

According to some commentators, introducing remote electronic voting from uncontrolled environments for political public elections is only feasible as long as a strong system for the digital identification for their citizens is already in place. For example, the former President of Estonia, Toomas Hendrik Ilves, recently noted that "[m]any countries realize that strong remote voter authentication is an immense practical problem that has to be dealt with before they can consider deploying any online voting system" (2016: xi) and then praised Estonia's electronic e-ID system.

In practice, however, a comparative assessment of the main countries using internet voting some years ago concluded that "Estonia is the only country with digital identification, while the two other countries [Norway and Switzerland] use(d) either existing physical IDs or wholly new unique identification methods valid only for each election" (Vinkel 2016: 48). Would Estonia remain the only country using eIDs for voter authentication in internet voting if we assessed governmental experiences today?

According to International IDEA's ICTs in Elections Database, at the time of writing there are 12 countries where Internet voting systems are used: Armenia, Australia (New South Wales[4]), Canada (Ontario[5]), Estonia, France, Mexico (Ciudad de México, CDMX[6]), New Zealand, Oman, Pakistan, Panama, Switzerland, and United Arab Emirates. We have assessed how voters are authenticated in these governmental experiences, with two exceptions: Oman and the United Arab Emirates, which can be considered illiberal or hybrid political contexts according to Romanov and Kabanov (2020) and thus

[2] Remote electronic voting is understood here as those systems "where votes are transferred via the Internet to a central counting server. Votes can be cast either from public computers or from voting kiosks in polling stations or—more commonly—from any Internet-connected computer accessible to a voter" (International IDEA 2011: 11). We will use the terms "remote electronic voting", "internet voting", and "online voting" indistinctively to refer to these systems.

[3] Whilst internet voting can be used from both controlled and uncontrolled environments, our focus here will be on the later (since it is in uncontrolled environments where it is more difficult to ascertain the identity and eligibility of a voter). In remote electronic voting from controlled environments (such as in polling stations, embassies and/or public libraries) a polling station officer could always verify, at least in principle, the identity of the voter.

[4] More recently, the Australian Capital Territory (ACT) has also introduced e-voting for voters overseas. This system was first used between 28 September and 17 October 2020.

[5] Online voting is also used, although to a lesser extent, in the Canadian province of Nova Scotia. However, and because of its size, we have decided to focus on Ontario: according to Cardillo, Akinyokun and Essex, "in the context of Ontario's 2018 municipal elections [...] as many as one million voters cast a ballot online" (2020: 7).

[6] In addition to CDMX, 11 Mexican states used internet voting for the state elections of 6 June 2021, in partnership with Mexico's Election Management Body, the Instituto Nacional Electoral (INE): Baja California Sur, Chihuahua, Colima, Guerrero, Michoacán, Nayarit, Querétaro, San Luis Potosí y Zacatecas, Guerrero (*diputación migrante*) and Jalisco (*diputación representación proporcional*). More information can be found at: <https://www.dof.gob.mx/nota_detalle.php?codigo=5573949&fecha=01/10/2019> [retrieved: 18 March 2022].

do not necessarily comply with international standards for democratic elections[7]. In turn, no data has been found for Armenia nor for New Zealand. Additionally, we have also assessed voter authentication methods for the internet voting systems used in the United States of America (USA)[8], a country that is not included in International IDEA's database but where internet voting is used at different levels for political public elections and was piloted during the 2018 mid-term elections in the State of West Virginia.

To conduct this assessment, the following Sect. 2 first considers the requirements for voter authentication from an international perspective. Following, in Sect. 3 we provide a detailed assessment of voter authentication methods in each of these countries. To introduce these experiences, we rely on the classification from Volkamer (2009), who distinguished between voter authentication methods based on (a) something you know (i.e., knowledge), (b) something you have (i.e., ownership), and (c) something you are (i.e., biometrics), or (d) any combination of these. For each of these categories, we will provide detailed analysis for certain experiences that allow us to understand how and why these voter authentication methods are used and made more robust. The last section of the paper (4) provides an overview of the main methods used and offers a discussion of the advantages and limitations of each method. Lastly, the conclusion (5) highlights the contribution of this paper, acknowledges some constraints, and suggests some follow-up work.

This work is relevant for three main reasons. First, because it updates existing literature on voter authentication with the most recent practices in political public elections. Second, because it provides a comparative assessment of voter authentication methods, which offers guidance to researchers and to practitioners when it comes to understanding the bigger picture about voter authentication in remote electronic voting[9]. Third, our assessment is valuable because it offers an interdisciplinary approach to the topic of voter authentication.

## 2 Equal Suffrage and Voter Authentication: Legal Requirements

Volkamer rightly points out that "[e]very remote electronic voting system needs to implement voter identification and authentication techniques to ensure that only eligible voters

[7] For example, Oman has a score of 0.08 in the category of electoral process and pluralism in the Economist's Democracy Index (The Economist Intelligence Unit 2020), and the United Arab Emirates' score is 0.00. In contrast, Australia scores 10.00, Canada, Estonia, France, Panama and Switzerland score 9.58, Mexico scores 7.83, Armenia scores 7.50, and Pakistan scores 5.67. The same could be said of the Russian Federation, a country where internet voting has been used as well, but that is not included in International IDEA's database. Russia scores 2.17 in the category of electoral process and pluralism in the Economist's Democracy Index.

[8] The USA score 9.17 in the category of electoral process and pluralism in the Economist's Democracy Index (The Economist Intelligence Unit 2020).

[9] A recent study commissioned by the European Commission also offers a comparative assessment of voter authentication methods in governmental experiences with remote electronic voting (Lupiáñez-Villanueva and Devaux 2018). However, this study is not as comprehensive as our (several of our case studies are not considered, such as Mexico and New South Wales) and focuses more on providers than on actual experiences.

may cast a vote and those only once" (2009: 25). Certainly, the principle of equal suffrage requires that "[t]he principle of one person, one vote must apply, and within the framework of each State's electoral system, the vote of one elector should be equal to the vote of another" (Human Rights Committee 1996: 7). In Europe, for example, the European Commission for Democracy through Law – more commonly known as the Venice Commission – also identifies equal voting rights as one of the guidelines of democratic elections, ascertaining that "each voter has in principle one vote; where the electoral system provides voters with more than one vote, each voter has the same number of votes" (Venice Commission 2002: 6).

The Council of Europe's Recommendation Rec(2017)5 on standards for e-voting – which remains to date the only intergovernmental standard in the field[10] (see Driza Maurer 2017) – offers further guidance on how equal suffrage's requirements for voter authentication are to be understood when technology is introduced for the casting of the votes. For example, standard No. 7 of the Recommendation prescribes that "[u]nique identification of voters in a way that they can unmistakably be distinguished from other persons shall be ensured" (Council of Europe 2017a: 5). The Explanatory Memorandum to the Recommendation further details that "unique identification refers to validating the identity of a specific person by means of one or more features so that the person can unmistakably be distinguished from other persons" (Council of Europe 2017b: 7). The description for this standard also reads that "[a]uthentication can be identity-based and role-based [...] identity-based identification is advisable for voters registering or casting a vote" (Council of Europe 2017b: 7).

Additionally, standard No. 8 reads that "the e-voting system shall only grant a user access after authenticating her/him as a person with the right to vote" (Council of Europe 2017a: 5). Notwithstanding, the provisions in the Explanatory Memorandum for this standard clarify that "where anonymous voting tokens prove that a voter is eligible to vote, identification of the voter may not be required at this point as it has already taken place at an earlier stage, namely when the specific token is assigned to a specific voter" (Council of Europe 2017b: 8).

## 3 Voter Authentication in Practice: Governmental Experiences

In what follows, we classify the different experiences with remote electronic voting in political public elections based on the methods that they use for voter authentication. Throughout the paper, we will offer more specific description about some of these cases to illustrate the voter authentication methods they use.

Our analysis starts with Volkamer's three ways of identification and authentication as applied to remote electronic voting: something you know (knowledge), something you have (ownership), and something you are (biometrics) (Volkamer 2009: 25)[11]. A combination of any of these techniques is possible as well.

[10] Even if the geographic scope of the Recommendation is in principle limited to the countries of the Council of Europe, there are several examples of non-European countries resorting to them. See for instance Stein and Wenda (2014) and Driza Maurer (2014). More recently, Essex and Goodman (2020) have also assessed the Council of Europe's approach towards the regulation of e-voting as a model for the development of internet voting standards in Canada.

[11] Similar classifications are offered by Krimmer et al. (2007) and Abu-Shanab et al. (2013).

Our assessment identifies knowledge-based authentication methods as the most common form of voter authentication in governmental experiences, in most cases combining different secrets or credentials that can be delivered to voters using different channels (e.g., by e-mail, SMS, post or by phone). It is used in Australia (New South Wales), Canada (Ontario), Pakistan, Panama, and Switzerland. To the best of our knowledge, biometric identification has only been used in the USA, during the 2018 mid-term elections when the State of West Virginia conducted a pilot using a blockchain-based internet voting system. Ownership-based voter authentication systems are not used in any of the cases we analyse, but a combination of ownership- and knowledge-based authentication methods.

### 3.1 Knowledge-Based Voter Authentication Methods

Our analysis reveals that the use of knowledge-based factors for voter authentication is the most common practice in governmental remote electronic voting experiences. It is used in the Australian States of New South Wales (with iVote Number and password), the Canadian province of Ontario (PIN and date of birth), Pakistan (where voters registering to vote online are asked several questions considered secret[12]), Panama (C1V verification key[13]), and Switzerland (password and birthdate, access code, and access code with validation code, depending on the cantonal implementation). This analysis also shows that more than one secret is needed to authenticate and vote in most of these experiences. In some cases, these secrets are delivered to voters through different channels (e.g., by e-mail, SMS, post or by phone) to mitigate the risk of voter impersonation.

In what follows, we explain how knowledge-based voter authentication methods work in Switzerland, Ontario (Canada), and New South Wales (Australia):

**Switzerland.** Since Switzerland started piloting remote electronic voting already in 2003, three different systems have been used in elections at all levels (communal, cantonal, federal) and in referendums: the ones in Geneva, Neuchâtel, and Zurich (later known as the *consortium*). According to the Swiss Federal Chancellery, Switzerland has held more than 300 electoral events in which Swiss voters in up to 15 cantons have been able to vote online (2020: 3). Even if the use of internet voting was recently discontinued, the federal government has already started working on a new legal framework and it is expected that internet voting will be offered again soon. Since it is the responsibility of the cantons to implement internet voting, we have found several alternatives when it comes to voter authentication:

For example, in Geneva the principle that has guided the development of remote electronic voting is "simplicity" (Swiss Federal Council 2006: 5222). The remote electronic voting process had to be as similar as possible to the one in place to vote by post (Swiss

[12] For more information about this specific voting experience, the reading by Haq et al. (2019) is suggested.

[13] There is not a lot of information about how this system works. However, we have found this reference to the C1V verification key in a document by the ACE Project: <https://aceproject.org/ero-en/regions/americas/PA/panama-carpeta-informativa-elecciones-generales> [retrieved: 18 March 2022].

Federal Council 2002: 649; Swiss Federal Chancellery 2004: 8): voters received their credentials (a password) by post, shielded by a tamper-evident overlay. To reveal their password, they had to scratch the area of their voting card where the password had been hidden. To authenticate themselves, they had to introduce this password as well as their birthdate into the system. The team responsible for this pilot project thus considered that the voting card was at the core of their system (Swiss Federal Chancellery 2004: 35).

The project in Neuchâtel was framed within a wider digitisation process, the so-called *guichet virtuel* (Swiss Federal Council 2002: 650) or *sécurisé* (Swiss Federal Chancellery 2004: 8) *unique*. Each voter eligible to vote online (namely, those registered at the *guichet*) would receive a unique confidential voter card together with their voting materials ahead of a contest (Swiss Federal Council 2002: 651). This voter card contained unique references (a barcode) and a security hologram (Swiss Federal Chancellery 2004: 41) and a unique access code to access the voting platform within the *guichet* (Swiss Federal Council 2002: 651). To cast their ballot, a voter had to type the validation code provided in their voting card. Thus, a two-step authentication was used here: first to ascertain the identity of the voter, and then to confirm the eligibility of the vote cast. This could be considered equivalent to have an OTP embedded in the voter card (i.e., sent by postal instead of SMS).

In Zurich's system, as in the two other pilot projects, each eligible voter received their credentials ahead of an election or referendum. However, in this experience voters could identify themselves against the internet voting system by typing just an access code printed on their voter card.

**Ontario, Canada.** Municipalities in the Canadian province of Ontario have been using internet voting for its municipal elections since 2003. Elections in Canada are considered "highly digital" (Essex and Goodman 2020: 163), with "more than 4.5 million online 'voting opportunities' in these municipalities since 2003" (Goodman and Smith 2017: 167). While online voting experiences have in general been positive for stakeholders (Goodman and Smith 2017: 169), some have warned that in Canada there is a lack of "safeguards in place such as standards, guidelines, or bodies that provide certification to regulate electronic voting" (Essex and Goodman 2020: 163). According to Essex and Goodman, "Canada's multilevel governance structure has meant municipalities mostly deliver election on their own terms, resulting in a patchwork of online voting models and security requirements" (2020: 162). This patchwork extends to voter authentication methods.

For example, a recent report about the Ontario municipal elections of 2018 found "weak voter authentication" practices (Cardillo et al. 2020: 5). According to these authors, "[t]he primary credential needed to cast a ballot online consisted of a knowledge factor (a PIN and/or ID) transmitted to the voter in a voter information package via postal mail"[14] (Cardillo et al. 2020: 5). Due to this already-mentioned multilevel governance, these passwords ranged in length in each municipality from 9 digits (with Simply Voting, used in 28 municipalities) to 16 digits (with Intelivote and Scytl, used in 100 municipalities). These authors have also observed that the channel used to deliver the

[14] These authors identify one exception in the city of Cambridge, where PINs were sent by email (Cardillo et al. 2020: 5).

credentials could be compromised. According to their findings, "some voters observed that the PINs were legible through the envelope when held up to bright light" (Cardillo et al. 2020: 5).

Possibly in an effort to mitigate this risk, "[i]n almost all cases a second knowledge factor (date of birth) was required" to authenticate a voter (Cardillo et al. 2020: 5). While adding a second knowledge factor could seem as increasing the robustness of voter authentication[15], Cardillo et al. (2020: 5) argue that "[d]ates of birth, however, make a poor login credential [...] knowledge of a PIN or date of birth does not establish a voter's identity. It merely establishes to the voting server that some entity on the other end of the connection knows a secret. Secrets, of course, can be transferred or intercepted". Therefore, they conclude, "authentication is still considered single-factor (as opposed to multi-factor) authentication since both credentials are knowledge factors" (Cardillo et al. 2020: 5).

**New South Wales, Australia.** In Australia, certain groups of voters in the state of "New South Wales, the most populous of Australia's six states, are able to cast their votes via the internet or telephone using the iVote system" (Goodman and Smith 2017: 171). According to these authors, "since 2011, [New South Wales'] voters have cast nearly 339,000 votes across nine elections" (Goodman and Smith 2017: 171). To this number, one should add the online votes cast during the last 2019 State elections.

To vote with iVote, New South Wales' internet voting system, a voter has to follow an online registration process first in which they prove their identity introducing several personal data (e.g., birth name, surname or family name, postal code, location, street name and, optionally, a passport, driver licence or Medicare details as a secondary confirmation of identity)[16]. Then, the voters have to introduce their contact information, which includes a mobile phone number, an e-mail and/or telephone number. After selecting to vote online, voters have to introduce a password that will be used to authenticate them to vote at a later stage. Passwords are scored, and at least a score of 4 out of 5 has to be obtained for the password to be accepted (according to its length, combination of letters, numbers, etc.).

Each password is then associated to an iVote Number that represents the voter. The iVote Number is a numeric value of 8 digits and is sent to each voter through the channel of their choice (SMS, email, post, or telephone call). Both values, the iVote Number and the password, are used to authenticate a voter in the iVote system before they can cast their vote.

### 3.2 Biometric-Based Voter Authentication Methods

To the best of our knowledge, biometric authentication has only been used as a voter authentication method in governmental elections in the USA and, more specifically, in

[15] The authors highlight that "[t]he use of single credential for voter authentication is inadvisable since access to the voter information package is sufficient to cast a ballot on another's behalf" (Cardillo et al. 2020: 5). However, we have already seen that a single credential for voter authentication is the method that has been used in some cantons in Switzerland for both internet voting as well as postal voting.

[16] More information about this method can be found online: <https://www.elections.nsw.gov.au/Voters/Other-voting-options/iVote-online-and-telephone-voting> [retrieved: 18 March 2022].

West Virginia[17]. Although the use of this system has been limited (during the 2018 mid-term elections 114 voters from 31 countries used the system[18]), this approach to voter authentication is quite novel and deserves some specific attention. In what follows, we explain this experience with more detail:

**West Virginia, the USA.** As already mentioned, the States of West Virginia piloted the use of an internet voting application during the 2018 mid-term elections. It was the first time that voters in the USA could cast their ballot on a mobile phone (Specter et al. 2020: 1535). The possibility to vote online was offered to deployed members of the military and overseas citizens[19]. The mobile application used, provided by the company Voatz Inc., relied on blockchain technology and biometric voter authentication. More specifically, voter authentication worked in three steps[20]: (1) the voter scans their driver's license, ID or passport; (2) they take a live snapshot of their face (what Voatz calls a "video selfie"); and (3) touches the fingerprint reader or uses the facial recognition feature on their smartphone, which links the device to the voter (alternatively, this last step could be substituted by just introducing a 8 digit PIN).

According to Voatz, "[t]he app first does a liveness check on the 'selfie', then compares the voter's "selfie" to the photo on their passport or driver's license, and finally, compares the ID data to the state's voter registration database to confirm that the voter is eligible to vote". One of the advantages of such a biometric authentication method is that there is no need to store a central biometric template database of eligible voters beforehand, since the comparison is done between the picture in the voter's physical ID and the live snapshot. Additionally, it is possible to delete all the data once the voter has been authenticated.

### 3.3 Combinations: Ownership- and Knowledge-Based Voter Authentication Methods

As we have mentioned, a combination of the three ways of identification and authentication is also possible. In the case of internet voting, we have found three experiences in which voter authentication is done based on a combination of ownership - and knowledge-based voter authentication methods: Estonia, France, and Mexico. In these three cases, voter authentication is achieved by means of knowledge and ownership. In what follows, we explain these three voter authentication methods:

[17] Additionally, there are several proposals from academia and from industry for biometric voter authentication in remote e-voting. See for example Hof (2004) and Morales-Rocha et al. (2008). However, we are not aware that any of these proposals has been implemented in actual governmental experiences.

[18] Due to security concerns and vulnerabilities found by a group of researchers (see Specter et al. 2020), the system was not used during the 2020 presidential and legislative elections.

[19] More information about the results of the pilot can be found online: <https://sos.wv.gov/news/Pages/11-16-2018-A.aspx> [retrieved: 18 March 2022].

[20] More information about this method can be found online: <https://voatz.com/wp-content/uploads/2020/07/voatz-security-whitepaper.pdf> [last accessed: 18 March 2022].

**France.** Internet voting in France dates back to 2003, with the passing of the first law allowing the use of internet voting for the elections to the High Council of French Citizens Abroad (Anziani and Lefèvre 2014: 38). Nowadays, remote electronic voting is foreseen as an additional voting channel for French voters abroad: they can cast a remote electronic vote for the elections to the National Assembly and for the election of the Consular Advisers and Delegates. In 2012, voters had the possibility to vote online for 11 seats at the National Assembly (Anziani and Lefèvre 2014: 37). However, in 2017 this possibility was halted due to concerns of foreign cyber threats as well as over certain technical issues (Deromedi and Détraigne 2018: 35–36). On their side, Consular Advisers and Delegates are based at each embassy with a consular district and at each consular post. They are elected for a six-year mandate during the month of May, their first elections taking place in 2014 (Anziani and Lefèvre 2014: 37).

In France, the Electoral Code describes quite in detail the voter authentication method for internet voting. In this sense, Article R176-3-7 of the Code reads that the voter's identity when voting online has to be satisfied by means of an *identifiant* (username) and a *mot de pass* (password). These two credentials, which according to the aforementioned article cannot be linked to the civil status of the voter, are created randomly and delivered to them using two different channels[21]. The length of the credentials is 12 characters each with an alphabet of 58 symbols. Following the provisions of the Electoral Code, these credentials are randomly generated by a module of the voting system devoted to this purpose. Two ceremonies are held to create these credentials, one to start the key generation and another one to finish it[22], within a secure room. For the secure delivery of these credentials, the *identifiant* is protected with a One Time Secret (OTS) and delivered to voters in a personalised e-mail. The *mot de pass* is delivered by SMS, in clear text.

Up until here, this authentication method would seem no different from the ones we have just explained. However, for the voter to be able to confirm their choices, a third secret is needed. In order to access the voting platform, the voters identify themselves introducing just the *identifiant* and the *mot de pass*. This authentication method is enough for them to select the voting options and cast their vote. However, the vote is confirmed only if they can provide a third credential. Upon casting their vote, voters receive a One Time Password (OTP) of six digits by e-mail. The voter has to open the OTP and introduce it into the voting website in order to confirm the casting of the vote. If the password is not introduced, the vote is not confirmed. Therefore, since and e-mail account is also needed to confirm the vote, an ownership-based method is introduced.

**CDMX, Mexico.** Internet voting has been used in CDMX since 2010. This option has been offered to voters abroad for the election of the Head of Government of the City of México (in 2012, when both online voting and postal voting were available) and for several participatory processes (Chorny 2020: 60–61). Internet voting has been used recently in two participatory processes, from 8 to 15 March 2020: for the election of

[21] The article also reads that the credentials are to be delivered to voters at the opening of the voting phase at the latest and at least one of the two credentials is needed to recover the other one in case of loss.

[22] There are two ceremonies because the process takes many hours (for the consular elections of 2021, about 1.3 million credentials are needed), and it is not suitable to have the observers during all the time.

different citizen bodies (*Comisiones de Participación Comunitaria*), and for its participatory budgets for 2020 and 2021. Internet voting was used as an advanced voting channel (8 to 12 March) and in four polling stations on election day (15 March). In 2012, CDMX used the internet voting system of a private vendor (Scytl). After this project, the city's election administration decided to develop its own system.

With this new system, as in New South Wales, voters willing to vote online in CDMX have to register beforehand. Voters can register in person or online. They can register online by introducing their voting credentials (voter key and a code called *Código de Reconocimiento Óptico de Caracteres*, OCR). The introduction of these credentials can be done by taking a picture to the voter card or by typing them manually. After introducing these credentials, they have to register a mobile phone number and choose a channel for the delivery of an 8-digit password (to choose between e-mail or post). If they choose to have their password delivered by e-mail, face recognition techniques are used to ascertain the identity of the voter[23].

To vote, each voter has to introduce their voter key and the OCR by taking a picture of their voter card, as well as the password that was handed to them (when registering in person) or delivered by e-mail or post. If the three credentials are correct, the voter then receives an SMS to the phone number they registered with a 6-digit key. Only when they introduce this last key, they can access the voter portal and vote.

**Estonia.** Estonia remains, to date, the only country where all voters are offered the possibility to vote online, and at all levels: for municipal and parliamentary elections, as well as for elections to the European parliament and in referendums. With online voting being offered since 2005, the share of i-voters has increased steadily and in the last 2019 parliamentary elections about 44% of all votes were cast electronically (Heiberg et al. 2020: 82). The success of Estonia's internet voting experience cannot be divorced from the country's digital agenda, at whose core lies the e-ID. After passing the Identity Document Act in 1999 and the Digital Signature Act in 2000, the first ID cards were issued in January 2002. Between 2002 and 2014, "about 1.2 million of these credit-card size personal identification documents have been issued, allowing citizens to digitally identify themselves and sign documents or perform actions" (Vassil 2016: 16). Nowadays, Estonia's citizens and residents can use the mobile version of the electronic identity document (ID) to prove who they are (Mobile-ID), as well as the Digi-ID.

Therefore, to vote online in Estonia "Identity document (ID card), Mobile-ID, and digital identity document (Digi-ID)[24] can be used as tools for giving digital signature" (State Electoral Office of Estonia 2017: 6). According to the country's State Electoral Office, "most of the persons who have the right to vote possess an ID card that enables

[23] While the resort to these techniques could imply that biometrics are used for voter authentication, we have not considered face recognition as a method used for voter authentication *as such* (since the use of these techniques is limited to the registration phase and they are not used at the time of voting). In a similar vein, Barrat Esteve and Morales-Rocha have noted that the authentication process could be strengthened if biometrics were used at the time of voting instead (2020: 8).

[24] However, according to Heiberg, Krips, and Willemson, "[r]ight now, only ID-card and mID are used for i-voting" (2020: 83).

secure electronic identification and giving digital signature; many people also have an additional legally backed electronic ID document, like Digi-ID or Mobile-ID" (2017: 4). In this sense, and while Estonia's internet voting system "supports a variety of authentication methods that the Voter can choose from depending on the authentication credentials at his [sic] disposal" (State Electoral Office of Estonia 2017: 11) such as knowledge-based methods (e.g., username, password, PIN), "stronger identification security is ensured by a physical authentication token (e.g., chip card, SIM-card, etc.) combined with a knowledge-based PIN" (State Electoral Office of Estonia 2017: 11).

## 4 Discussion

All in all, it is clear that the main authentication method used is knowledge-factors (see Table 1). These methods may be used as the unique factor, or in combination with others (mainly ownership-based methods). Biometrics has only been used in one of the experiences that have been analysed.

**Table 1.** Voter authentication methods in each governmental experience

| | Australia, New South Wales | Canada, Ontario | Estonia | France | Mexico, CDMX | Pakistan | Panama | Switzerland | The USA, West Virginia |
|---|---|---|---|---|---|---|---|---|---|
| Knowledge-based | • (2) | • (2) | • (2) | • (2) | • (3) | • | • | • | |
| Ownership-based | | | • A | • B | • C | | | | |
| Biometric-based | | | | | | | | | • |

( ) number of secrets that compose the voter credential.
A Identity document (ID card), Mobile−ID, and digital identity document (Digi−ID).
B OTP delivered by e−mail.
C OTP delivered by SMS.

As we have seen, there are important variations on how voter authentication is based on knowledge factors in these experiences. In some cases, just one knowledge factor has been used for voter authentication (as in Zurich, Switzerland). However, in the majority of cases two different credentials are required. Our analysis shows that adding a second credential does not necessarily prevent impersonation, since it is always possible to share this second secret as well (and sometimes the two credentials are delivered together, which makes it very easy for them to be shared or traded).

Notwithstanding, our assessment reveals that there are different ways in which secrets can be delivered to a voter. For instance, in New South Wales voters can choose their own password (as long as it meets some security requirements) and then have their username (i.e., iVote Number) delivered to them through the channel of their choice (e.g., SMS, email, post, or telephone call). In Ontario some information about the voter is used as this second secret (i.e., their birthdate).

In all circumstances, it seems that while highly usable and with low costs (although these can increase depending on how the credentials are delivered to voters), knowledge-based authentication is not the most secure choice. As Volkamer already noted, with knowledge-based voter authentication "vote buying cannot be excluded, because voters could easily send electronically their login data to a potential buyer" (2009: 25). At the end of the day, this risk will have to be evaluated on a case-by-case basis (e.g., in Switzerland, where this risk may be higher if compared to the other experiences, the authorities seem to have accepted it since it is similar to the risk of voter impersonation in postal voting, which relies on the same authentication method).

Overall, biometric-based voter authentication has the key advantage of assuring that the voters are who they claim to be (since biometrics cannot be shared or traded). However, it is also important to notice that there may be errors in the biometric technologies used which could prevent an authentic voter from authenticating themselves or allowing a non-eligible voter to access the voting platform. On the other hand, concerns about cost as expressed by Volkamer when she noted that "[l]argescale biometric infrastructures do in general not yet exist" (2009: 26) are to some extent mitigated if biometric voter authentication is implemented as it was done in West Virginia (since there is no need for the Electoral Management Body to keep biometric templates for all the electorate). Notwithstanding, this method restricts the devices that can be used to vote and increases dependence on third parties. For instance, Specter, Koppel and Weitzner noted that in Voatz's internet voting system, "[t]he user verifies their identity, using Voatz's integration with a third-party service called Jumio" (2020: 1538). Thus, not all costs can be overcome.

Lastly, combination of methods deserves a specific mention. In Mexico and France, an OTP is delivered to the voter at the time of voting, provided that they have introduced the proper credentials. In the French case, ownership is based on email addresses. While this method may have some advantages in terms of robustness, it is also important to highlight that the choice of e-mail for the delivery of the OTP may not compensate for the additional complexity added to the casting of the vote. In this sense, it does not seem unfeasibly to share the email account where the OTP is going to be received with someone else, since e-mail accounts can be opened from any device with a browser and internet connection, and the same e-mail account can have several concurrent sessions opened in different devices. The Mexican alternative, where an OTP is received by SMS, seems more robust[25].

Lastly, voter authentication based on tokens is not ideal either (in spite of Estonia's combination seems most robust and secure if compared to the other ones). It offers more security when it comes to ascertaining the identity of the voter, but physical tokens and passwords can be traded as well, and vote-buying cannot be completely excluded. More

[25] At the same time, delivering the OTP using another channel (such as SMS), which would require sharing the mobile phone or at least the SIM-card, does not seem suitable either, since internet voting is offered to French voters abroad and the delivery of the OTP would be subject to certain constraints that could render voting online almost impossible (i.e., if the SMS is not received before the voting session expires, the vote cannot be confirmed and thus remains not cast). This is not unimportant in view that up to 50% of voters involved in a User Acceptance Test (UAT) ahead of the 2017 French legislative elections had connection problems, mostly due to issues with their e-mail and the delivery of the SMS (Deromedi and Détraigne, 2018: 40). Issues with SMS were especially concerning in countries like China (Deromedi and Détraigne, 2018: 31).

recently, it has been highlighted that an attacker could submit a vote using a compromised e-ID environment without the voter noticing "where ID-card is left attached to the working terminal for extended periods of time, e.g. as a login token" (Heiberg et al. 2020: 84)[26]. Furthermore, this method is not as usable (at least when physical cards and associated card readers are required) and the costs are considerable. Estonia seems to have overcome this usability and infrastructure costs in the long term, as the e-ID is extensively used in the country and the internet voting system also supports Mobile-ID (and, according to the State Electoral Office of Estonia, Digi-ID). Notwithstanding, this method does not seem optimal for voter authentication unless the physical or digital tokens are extensively used[27]. The Mexican alternative, which relies on a mobile phone to deliver a third secret during the authentication phase (and which thus requires having at least the SIM-card at the time of voting) seems more feasible. However, as we have seen, it has its own shortcomings as well.

## 5 Conclusion

In this paper, we have aimed at assessing different methods for voter authentication in governmental remote electronic voting experiences. To do so, we have analysed international standards for voter authentication and their practical implementation in different countries. Our analysis sits somewhere in between a legal and a technological study. However, and because of the constrains of the format in which it is presented, it does not offer a deep assessment neither of the technological nor the legal aspects of these experiences. This has not been our goal either. Instead, we aimed at (1) clarifying which methods exist and are used to ensure that only eligible voters vote in governmental experiences when remote electronic voting is introduced, and (2) to understand which mechanisms can be put in place to make these methods more robust. We are aware that national differences in electoral policy impose different requirements for voter authentication, and thus we have not been willing to evaluate all these methods against abstract standards and requirements.

Notwithstanding, our contribution is valuable for several reasons. First, because it updates existing literature on voter authentication with the most recent practices. Second, because it provides a comparative assessment which can offer guidance to researchers and to practitioners when it comes to understanding the bigger picture about voter authentication in remote electronic voting. This comparative assessment has also allowed us to challenge some conventional wisdom about the necessary pre-conditions for the introduction of internet voting: that an infrastructure for the digital identification of voters is a *sine qua non* condition and the best way to achieve voter authentication. As we have seen, only one country in our analysis uses digital identification cards (Estonia). By contrast, most of countries we have analysed have opted: (1) for analogous methods to those already existing for paper-based voting channels, such as postal voting (i.e.,

[26] This vulnerability, described as the Ghost Click Attack by Springall et al. (2014), was first identified in 2013.

[27] While not very common for governmental experiences, it is not unlikely that such digital identification infrastructures could exist for private settings, such as in universities, political parties or professional associations, to name just a few examples.

Switzerland), (2) for more than one knowledge factor (e.g., Ontario in Canada), sometimes delivered to voters using different channels (e.g., New South Wales in Australia), or (3) for a combination of knowledge- and ownership-based authentication methods, without requiring e-IDs or digital certificates (e.g., France and Mexico).

Lastly, our assessment is valuable because it offers an interdisciplinary approach to the topic of voter authentication. This is important because, and while requirements for voter authentication tend to be formulated in similar ways in international standards and national regulations (with exceptions, such as France), our research shows that the scope of alternatives for Election Management Bodies to choose among is quite broad. This is relevant for two main reasons. On the one hand, countries where remote electronic voting is regulated can introduce changes to the mechanisms used for voter authentication without having to start lengthy and complex processes to amendments their legislation. On the other hand, countries willing to introduce internet voting can regulate the requirements for voter authentication in a way that is broad enough to accommodate those mechanisms that are more suitable at a later stage (i.e., by means of executive orders or administrative acts).

**Acknowledgements.** This work received support from the mGov4EU project, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 959072.

## References

Abu-Shanab, E., Khasawneh, R., Alsmadi, I.: Authentication mechanisms for E-Voting. In: Saeed, S., Reddick, C.G. (eds.) Human-Centered System Design for Electronic Governance, pp. 71–86 (2013)

Anziani, A., Lefèvre, A.: Vote électronique: preserver la confiance des électeurs. Rapport d'information fait au nom de la commission des lois (2014)

Barrat Esteve, J., Morales Rocha, V.M.: Informe de Voto Electrónico (2020)

Cardillo, A., Akinyokun, N., Essex, A.: Online voting in Ontario municipal elections: a conflict of legal principles and technology? Whisper Lab Research Report, Western University (2020)

Chorny, V.: El voto por internet en México: La libertad y la secrecía del voto condicionadas. R3D. Red en Defensa de los Derechos Digitales, Ciudad de México (2020)

Council of Europe: Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting (2017a)

Council of Europe: Explanatory Memorandum to Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting (2017b)

Deromedi, J., Détraigne, Y.: Réconcilier le vote et les nouvelles technologies. Rapport d'information fait au nom de la commission des lois (2018)

Driza Maurer, A.: Ten years Council of Europe Rec(2004)11. Lessons learned and outlook. In: Krimmer, R., Volkamer, M. (eds.) Proceedings of Electronic Voting 2014 (EVOTE 2014), pp. 111–117. TUT Press, Tallinn (2014)

Driza Maurer, A.: Updated European standards for E-voting. In: Krimmer, R., Volkamer, M., Braun Binder, N., Kersting, N., Pereira, O., Schürmann, C. (eds.) E-Vote-ID 2017. LNCS, vol. 10615, pp. 146–162. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-68687-5_9

Essex, A., Goodman, N.: Protecting electoral integrity in the digital age: developing E-voting regulations in Canada. Election Law J. **19**(2), 162–179 (2020)

French Electoral Code

Goodman, N., Smith, R.: Internet voting in sub-national elections: policy learning in Canada and Australia. In: Krimmer, R., et al. (eds.) E-Vote-ID 2016. LNCS, vol. 10141, pp. 164–177. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-52240-1_10

Haq, H.B., McDermott, R., Ali, S.T.: Pakistan's internet voting experiment. In: Krimmer, R., et al. (eds.) Fourth International Joint Conference on Electronic Voting E-Vote-ID 2019, Lochau/Bregenz, Austria, 1–4 October 2019. Proceedings. TalTech Press, Tallin (2019)

Heiberg, S., Krips, K., Willemson, J.: Planning the next steps for Estonian Internet voting. In: Krimmer, R., et al. (eds.) Fifth International Joint Conference on Electronic Voting E-Vote-ID 2020, 6–9 October 2020. Proceedings. TalTech Press, Tallin (2020)

Hof, S.: E-voting and biometric systems. In: Electronic Voting in Europe - Technology, Law, Politics and Society, Workshop of the ESF TED Programme Together with GI and OCG, Schloß Hofen/Bregenz, Lake of Constance, Austria, 7–9 July 2004. Proceedings, pp. 63–72 (2004)

Human Rights Committee: United Nations: General Comment No. 25 (1996)

Ilves, T.H.: Foreword. In: Solvak, M., Vassil, K. (eds.) E-Voting in Estonia: Technological Diffusion and Other Developments Over Ten Years. Johan Skytte Institute of Political Studies, in cooperation with Estonian National Electoral Committee, Tartu and Tallin (2016)

International IDEA: Introducing Electronic Voting: Essential Considerations (2011)

Krimmer, R., Triessnig, S., Volkamer, M.: The development of remote E-voting around the world: a review of roads and directions. In: Alkassar, A., Volkamer, M. (eds.) Vote-ID 2007. LNCS, vol. 4896, pp. 1–15. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-77493-8_1

Lupiáñez-Villanueva, F., Devaux, A. (eds.): Study on the Benefits and Drawbacks of Remote Voting. European Commission, Brussels (2018)

Morales-Rocha, V., Puiggalí, J., Soriano, M.: Secure remote voter registration. In: Proceedings of 3rd International Symposium on Electronic Voting (EVOTE 2008), Bregenz, Austria, 7–9 August 2008, pp. 95–108 (2008)

Romanov, B., Kabanov, Y.: The oxymoron of the internet voting in illiberal and hybrid political contexts. In: Krimmer, R., et al. (eds.) E-Vote-ID 2020. LNCS, vol. 12455, pp. 183–195. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-60347-2_12

Specter, M.A., Koppel, J., Weitzner, D.: The ballot is busted before the blockchain: a security analysis of Voatz, the first internet voting application used in U.S. federal elections. In: 29th USENIX Security Symposium (USENIX Security 2020), pp. 1535–1553 (2020)

Springall, D., et al.: Security analysis of the Estonian internet voting system. In: Proceedings of the 21st ACM Conference on Computer and Communications Security (CCS 2014), November 2014

State Electoral Office of Estonia: General Framework of Electronic Voting and Implementation thereof at National Elections in Estonia (2017)

Stein, R., Wenda, G.: The Council of Europe and e-voting: history and impact of Rec(2004)11. In: Krimmer, R., Volkamer, M. (eds.) Proceedings of Electronic Voting 2014 (EVOTE 2014), pp. 105–110. TUT Press, Tallinn (2014)

Swiss Federal Chancellery: Le vote électronique dans sa phase pilote - Rapport intermédiaire (2004)

Swiss Federal Chancellery: Restructuration et reprise des essais. Rapport final du Comité de pilotage Vote électronique (CoPil VE) (2020)

Swiss Federal Council: Rapport sur le vote électronique du 9 janvier 2002: Chances, risques et faisabilité (2002)

Swiss Federal Council: Rapport sur les projets pilotes en matière de vote électronique (2006)

The Economist Intelligence Unit: Democracy Index 2020: In sickness and in health? (2020)

Vassil, K.: The Estonian e-government ecosystem. In: Solvak, M., Vassil, K. (eds.) E-Voting in Estonia: Technological Diffusion and Other Developments Over Ten Years. Johan Skytte Institute of Political Studies, in cooperation with Estonian National Electoral Committee, Tartu and Tallin (2016)

Venice Commission: Code of Good Practice in Electoral Matters: Guidelines and Explanatory Report (2002)

Vinkel, P.: Historical development and legal aspects. In: Solvak, M., Vassil, K. (eds.) E-voting in Estonia: Technological Diffusion and Other Developments Over Ten Years. Johan Skytte Institute of Political Studies, in cooperation with Estonian National Electoral Committee, Tartu and Tallin (2016)

Volkamer, M.: Evaluation of Electronic Voting: Requirements and Evaluation Procedures to Support Responsible Election Authorities. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-01662-2