Paper submission to the 14th ICEGOV Conference in 2021

Remote e-voting overview

We can divide the process of voting in 4 distinct categories: In-person paper voting, In-person e-voting, Remote paper voting and Remote e-voting (REV[1]). Electoral processes must guarantee certain proprieties[2] as well as provide cybersecurity when done electronically[3]. The goal of this short paper is to do a small overview of the current tools of the ecosystem of remote e-voting and pin-point key components that will play an important role in its foreseeable evolution.

1 SUBJECT

Remote e-voting is the ability for a user to cast a vote during an election, or to answer a poll, from their own computer in any location with immediate effect. Elections that are run electronically are important because they are able to generate consensus faster than traditional voting and perhaps cheaper, considering that the same infrastructure can be re-used in different cycles.

2 USE CASES

One of the first pilot experiments with remote e-voting was in Estonia and took place in 2005 for the local elections where around 1% of the voters used the system. This later culminated in the 2019 Estonian parliamentary elections where 565 045 people voted of which 247 232 cast their votes on-line, at home, over the internet, which is about 43.8% of the total of the votes cast. Estonia is so far the only country to deploy remote e-voting for national elections across the entire population of the country.[4] To achieve this it made use of the smart card eID issued by their government.

In Switzerland, remote e-voting has been occurring a little bit earlier, since 2003, the first time in the small commune Anieres that is part of the canton of Geneva. Between 10-20% of the total of votes of permanent residents have since been cast over the internet while for the expat community it has been registered between 40-70% on-line voter turnout, depending on the specific cantons.[5] Switzerland uses a different mechanism other than smart cards for identification however, which relies solely on in-presence registration at the corresponding cantons and the insertion of a series of codes that are sent to the corresponding residential address by letter.

The Switzerland experience contrasts with Estonia's in that it has been occurring more at a local than at a national level.

Colombian government and FARC in 2016 went on a plebiscite for a peace treaty wherein around 5 400 000 otherwise excluded expats were able to express their opinion on-line through digital tools.[6]

South Korea successfully deployed a small-scale remote e-vote polling in the most populous province, Gyeonggi-do, with around 9000 participants that decided the destiny of 527 community projects. The trial used blockchain for improved security which has seen strong support for adoption by national authorities that plan to invest $380 million between 2021-2026. The Ministry of Science and Technology plans to implement DID[7] at a national level by the end of 2022.[8]

Other trials have been conducted with relative success at varied scales in other countries as the technology behind remote e-voting becomes better understood. There are numerous examples of private companies that claim to be able to accomplish this.

3 BASIC PROPRIETIES

The biggest challenge of remote e-voting is to achieve high level of security under an uncontrolled environment and insecure platform. E-voting properties and many different classifications that set the minimum requirements are already established. Some of these classifications are just the same properties under different names such as: confidentiality, integrity, privacy, democracy, universality, verifiability, etc.. Regardless, the goal is always to conciliate two apparently mutually exclusive proprieties:

Verifiability

Verifiability is the ability of any independent party to verify that all votes were counted correctly. Additionally, it should give voters the ability to verify that their own vote has been properly emitted, recorded and counted for the final tally results. The pursuit of this propriety culminated in the idea of end-to-end verifiability[9] (E2E-VIV). Intuitively, what this system must provide is

the ability for voters to detect fraud by distributing receipts for each vote while simultaneously preventing these from being used as proofs of their orientation to a third-party, in order to avoid coercion. Current practices stipulate that all receipts should be posted publicly in a secure append-only bulletin board once the final tally is published.

Privacy

The remote e-voting system must protect voters by concealing the relation between the voter and the votes cast, ensuring that the choice's made remain private. This can be expressed via several security properties[10]:

Basic ballot integrity guarantees that no one in possession of the (digital) ballots can disclose how voters voted individually while still being able to tally the results.

In the literature, receipt-freeness means protecting the voting process even when voters willingly interact with an attacker. Coercion-resistance, less strongly, is considered when an honest voter is, during some time, under the control of an attacker. Both these conditions assume that a voter should not be able to prove conclusively to anyone else how the vote was cast.

Protection from social profiling should also be considered by using a mix-net (an overlay network), correlations between the votes, the voters and their geolocations should be concealed.

Various concepts like receipt free voting, E2E, third-party verifiability, etc., led to development of different protocols. A common critical aspect concerns identity management, fundamenal to guarantee that each person can vote at most once during each election. The concept of a PKI (public key infrastructure) helps by providing an easy and highly secured way for authentication. PKI ensures that sensitive information is encrypted and can only be reverse verified with special keys that are in possession of only the voter and trusted entities, generally with the help of a CA (Certificate Authority).

The whole system is thus divided and analyzed in several phases or layers. With proper design each layer can be checked as well as the transactions in-between. Some interesting remote e-voting systems that offer end-to-end verifiability, under certain configuration assumptions, that were found during our research were Remotegrity[11], EVIV[12] and VoteAgain[13].

4 TECHNOLOGIES

Public-Key, Zero-Knowledge and Homomorphic Encryption

PKIs are well established cryptographic algorithms and the necessary underlying infrastructure that can be used to form secure channels between two parties while guaranteeing confidentiality, data integrity and identity.[14]

Although Public-Key Infrastructure does provide some of the necessary building blocks for secure communications, registering and authenticating eIDs generally relies on the issuance of digital certificates from a CA (the government or other public institutions) and the integrity of these is tied to the good behavior of the officials who issue and manage the certificates. Recently, decentralized PKI schemes which rely instead on a Network of Trust and blockchain were proposed to mitigate this design flaw.[15]

Zero-Knowledge Proofs (ZKP) are a way to prove to a party that you are in the possession of some information (a secret) without revealing it during communications. It's useful for anonymous authentication and consequentially, private voting.[16,17,18]

Homomorphic encryption allows votes to be saved and later tallied without disclosing clear-data. It achieves this by doing computations on top of ciphertexts and is useful to guarantee ballot integrity[19] when publishing a bulletin-board of the votes.

There are other cryptographies that may also prove to be useful such as Multi-Party computation[20], as an example whenever guaranteeing shared trust between members of a small set is a necessity.

PKI is embedded in government issued smart card eIDs.

Trusted Execution Environment

As mentioned unsecured platforms pose serious problems. We need to ensure that the applications necessary for remote e-voting are running in isolated environments in order to protect the voter's machine against malware. TEE[21] allows this by structuring access to hardware resources separately from the rich OS. With the proper setup of a nanokernel, with the use of microcode and private keys stored in firmware, namely in ROMs (Read-only Memory), and assuming a trust relationship between the hardware provider and the end-user, TEE allows the secure handling of private keys on the voter's machine and may be used to reassure that the correct software is running in isolation to other potentially malicious processes; however, this is frail in situations where backdoors are hidden that bypass security checks. This can only be alleviated by promoting open source software and hardware and is currently an issue given the monopoly of hardware manufacturers.

This technology is implemented in some of the AMD, Intel, ARM and RISC-V CPUs[22]. Smart cards are also one form of TEE because of their embedded microchips which are obviously detached from the devices with which they operate.[23]

Distributed ledgers

The blockchain[24] is a new technology for storing data in a secure and transparent way which is not subject to any form of central control. It provides strong resilience against attacks that can tamper the integrity of the data by making use of the immutability propriety that can be obtained from distributed ledgers.

The technology is based on a decentralized network consisting of multiple connected nodes that can interchange data transactions, are geographically disjoint, have different owners and which operate as a single database. The design makes it possible for the information stored in the blockchain to be preserved permanently and without the possibility of it being modified in one of the nodes without detection. It also ensures high availability by eliminating single points of failure (Byzantine fault tolerance) while always providing verifiability as all nodes maintain the consensus version of the ledger. Smart contracts are a novelty in the sense that blockchains become not only databases but can function as decentralized applications (dApps) as well.

The main purpose of using blockchain in remote e-voting is to guarantee that the servers where data is stored and processed are not in control of a single entity (although different parties may be assigned different roles).

Overlay networks

Encryption (with the use of PKI) is enough to guarantee some degree of privacy. However, it does not deal with the risks of correlating the voters machine IP address, which is present in the exchanged data packets and which can be traced to specific geolocations. To protect against this type of attacks a technique known as onion routing can be deployed by using overlay networks; a network that is layered on top of another network and used to scramble and hide the IPs.

The basic idea is that the signal between each node of the network is randomly mixed between a set of proxies, also known as relays (nodes). This is coupled with the procedure that at each intersection of the packet's route, information is carried only about the predecessor and successor nodes but not of the entire mapping.

This architecture if properly setup can be used to obfuscate the user's source and destination IPs. No-Log VPNs may provide this service but require some level of trust between the users and the VPN provider.

Tor[25] on the other hand, is a decentralized trustless solution first developed by the U.S. Navy in the mid-1990s which provides reasonable anonymity against non-state actors.

Endpoint monitoring

Correct remote e-voting deployments must make use at each node of the decentralized infrastructure as well as on the end user's terminals, of proper endpoint threat detection and response techniques. These can range from the use of reverse firewalls and updated software to the correct choice and setup of the OS, which in particular, should be amnesic by default.[26]

Additionally, practices such as never sharing personal smart cards with other users or sharing keys and passwords with the public are important.

5 IDENTITY MANAGEMENT

There are currently 53 countries that have smart cards as national ID documents of which we found 11 to provide publicly available SDKs: in Belgium, Cabo Verde, Czech Republic, Estonia, Germany, Italy, Latvia, Lithuania, Perú, Portugal and Uruguay.

In 41 other countries in order to fully use eIDs it's required to use specific software: such as in Afghanistan, Albania, Algeria, Bangladesh, Brunei, Croatia, Finland, Ghana, Guatemala, India, Indonesia, Ireland, Israel, Kuwaiti, Lebanon, Liechtenstein, Luxembourg, Malawi, Malta, Malaysia, Mauritius, Mongolia, Monaco, Morocco, Nepal, the Netherlands, Nigeria, Norway, Oman, Pakistan, Poland, Romania, Serbia, Slovakia, Somalia, Spain, Sweden, Thailand, Turkey, United Arab Emirates and Uruguay.

We know that Philippines[27] has successfully deployed government issued smart card eIDs but failed at finding information about the availability of the middleware. France[28] is soon to deploy smart card eIDs.

In other countries no eID service is provided and identification is mostly done in person and paper based, or dependent on centralized IT structures that issue a voter eID specifically during elections such as in the case of Switzerland.

Another hypothetical way to implement remote e-voting is to make use of W3C DID standard. The only country that has pledged publicly to the allocation of public resources to this end is the already mentioned case of South Korea. In this spirit, CanDID[29] seems to be an interesting innovative approach to implement remote e-voting in countries that still rely on legacy systems.

Biometrics may also prove to be an alternative to eID provided by state issued smart cards.[30]

The present authors consider that the conditions to deploy E2E-VIV are to a large extent sufficiently understood and that further investment should be made. We also consider that with the exception of Estonia where national elections were already successfully conducted few other countries are actively pursuing this end. Most need to improve or disclose their technology in order to facilitate implementation. Disclosing official eID smart card SDKs in order to facilitate IDM is important for the ecosystem to evolve.

6 FINAL REMARKS

The present authors consider that the conditions to deploy E2E-VIV are to a large extent sufficiently understood and that further investment should be done. We also consider that with the exception of Estonia where national elections were already successfully conducted few other countries are actively pursuing this end. Most need to improve or disclose their technology in order to facilitate implementation. Disclosing official eID smart card SDKs is important for the ecosystem to evolve.

References

[1] "Remote Voting in the Age of Cryptography", Nathaniel Williams, MIT Computational Law Report, 2022. https://www.attejuvonen.fi/thesis-voting-security-2019-10-01.pdf

[2] "A framework for comparing the security of voting schemes", Atte Juvonen, University of Helsinky, Finland, 2019. https://www.attejuvonen.fi/thesis-voting-security-2019-10-01.pdf

[3] "Formalising security properties in electronic voting protocols", Steve K. et al, FR, 2013. http://www.lsv.fr/Projects/anr-avote/RAPPORTS/deliv1-2.pdf

[4] Valimised Eestis, Government organisation, 2019 parliamentary election results. https://rk2019.valimised.ee/en/voting-result/voting-result-main.html

[5] "Fifteen years of internet voting in Switzerland [History, Governance and Use]", Uwe Serdult et al., 2nd ICEDEG, 2015. https://www.researchgate.net/publication/283878260_Fifteen_Years_of_Internet_Voting_in_Switzerland_History_Governance_and_Use

[6] "How Blockchain can change voting: the Colombian Peace plebiscite", entry on Organisation for Economic Co-operation and Development Forum, Charlotte van Ooijen, 2017, https://www.oecd-forum.org/posts/28703-how-blockchain-can-change-voting-the-colombian-peace-plebiscite

[7] DID Working Group, https://www.w3.org/2019/did-wg/

[8] "South Korea unveils Blockchain Strategy to Launch Online Voting and Election System by 2022". https://v.kakao.com/v/20200624165519865

[9] "The Future of Voting, End-to-End Verifiable Internet Voting, Specification and Feasibility Assessment Study", U.S Vote Foundation, Galois, 2015. https://usvotefoundation-drupal.s3.amazonaws.com/prod/E2EVIV_full_report.pdf

[10] "BeleniosRF: A Non-interactive Receipt-Free Electronic Voting Scheme" by Pyrros Chaidos et al., 2016. https://eprint.iacr.org/2015/629.pdf

[11] "Remotegrity: Design and Use of an End-to-End Verifiable Remote Voting System" by R. T. Carback et al., 2013. https://eprint.iacr.org/2013/214.pdf

[12] "EVIV: An end-to-end verifiable Internet voting system" by Paulo F. et al., 2013, https://www.researchgate.net/publication/257006739_EVIV_An_end-to-end_verifiable_Internet_voting_system, https://github.com/EVIVoting/EVIV

[13] "VoteAgain: A scalable coercion-resistant voting system" by Wouter Lueks et al., 29th USENIX Security Symposium, 2020. https://arxiv.org/abs/2005.11189, https://github.com/spring-epfl/voteagain

[14] "Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms", National Institute of Standards and Technology, U.S. Department of Commerce, 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175b.pdf

[15] "A Decentralized Dynamic PKI based on Blockchain" by M. T. and Christian G., Lund University, Sweden, 2020. https://arxiv.org/abs/2012.15351v1

[16] "Towards Anonymous, Unlinkable, and Confidential Transactions in Blockchain" by Kalpana Singh et al., IEEE Blockchain, Halifax, Canada, 2018. https://hal.archives-ouvertes.fr/hal-01812004/document

[17] "ethVote: Towards secure voting with distributed ledgers", Johannes M. and Emmanouil V., International Conference on Cyber Security and Protection of Digital Services, 2020. https://www.researchgate.net/publication/341000573_ethVote_Towards_secure_voting_with_distributed_ledgers

[18] Semaphore, https://semaphore.appliedzkp.org/

[19] "Secure Electronic Voting using BlockChain and Homomorphic Encryption" by C. Sravani et al.,International Journal of Recent Technology and Engineering, 2019. https://www.ijrte.org/wp-content/uploads/papers/v8i2S11/B11680982S1119.pdf

[20] "Incoercible Multi-Party Computation and Universally Composable Receipt-Free Voting", Joël Alwen, Rafail Ostrovsky, Hong-Sheng Zhou, and Vassilis Zikas, Advances in Cryptology -- CRYPTO 2015, Santa Barbara, USA, 2015. https://web.cs.ucla.edu/\~rafail/PUBLIC/182.pdf

[21] "The Trusted Execution Environment: Delivering Enhanced Security at a Lower Cost to the Mobile Market", GlobalPlatform, 2015. https://globalplatform.org/wp-content/uploads/2018/04/GlobalPlatform_TEE_Whitepaper_2015.pdf

[22] "A Clean Slate Approach to Linux Security RISC-V Enclave", Sandro Pinto et al., Embedded World Conference, Germany, 2020. https://www.researchgate.net/publication/339784918_A_Clean_Slate_Approach_to_Linux_Security_RISC-V_Enclave

[23] "Design Principles for Tamper-Resistant Smartcard Processors", Oliver Kömmerling et al., USENIX Workshop on Smartcard Technology, USA, 1999. https://www.usenix.org/legacy/events/smartcard99/full_papers/kommerling/kommerling.pdf

[24] "Bitcoin: A Peer-to-Peer Electronic Cash System" by S. Nakamoto, 2008. https://bitcoin.org/bitcoin.pdf

[25] "Tor: The Second-Generation Onion Router" by Roger D. et al., 2004. https://svn-archive.torproject.org/svn/projects/design-paper/tor-design.pdf

[26] "Tails Linux Operating System: Remaining Anonymous with the Assistance of an Incognito System in Times of High Surveillance" by Maurice Dawson and Jose Antonio Cardenas-Haro, International Journal of Hyperconnectivity and the Internet of Things, United States of America, 2017. https://www.academia.edu/31947046/Tails_Linux_Operating_System_Remaining_Anonymous_with_the_Assistance_of_an_Incognito_System_in_Times_of_High_Surveillance

[27] Unified Multi-Purpose ID application form, https://www.sss.gov.ph/sss/DownloadContent?fileName=SSSForms_UMID_Application.pdf

[28] "La nouvelle carte nationale d'identité", Ministère de l'Intérieur, France, 2021. https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/La-nouvelle-carte-nationale-d-identite

[29] "CanDID: Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability", by Deepak Maram et al, The Initiative for CryptoCurrencies & Contracts, USA, 2021. https://eprint.iacr.org/2020/934.pdf

[30] "Securing Fingerprint Template Using Blockchain and Distributed Storage System", Moses Arhinful Acquah et al, Shandong University of Science and Technology, Shandong, China, 2020, https://res.mdpi.com/d_attachment/symmetry/symmetry-12-00951/article_deploy/symmetry-12-00951-v2.pdf

Available SDKs

Belgium, https://github.com/Fedict/eid-mw, Cabo Verde, https://sniac.cv/mw/, Czech Republic, https://github.com/premek/obcanka-reader, Estonia, https://www.id.ee/en/for-developers/, Germany, https://github.com/Governikus/AusweisApp2, Italy, https://www.cartaidentita.interno.gov.it/identificazione-digitale/software-cie/, Latvia, https://github.com/eID-LV/Middleware, Lithuania, https://www.nsc.vrm.lt/downloads_en.htm, Malaysia, https://github.com/OpenSC/OpenSC/wiki/Malaysian-MyKAD (OpenSC), Perú, https://dnielectronico.pe/ (OpenSC), Portugal, https://github.com/amagovpt/autenticacao.gov, Uruguay, https://github.com/eIDuy/apdu-services

Authors

Abdelmoumene Lahmidi, Computer Engineer, University M'Hamed Bougara de Boumerdes, Algerie

Nuno Chainho Amiar, Lisbon, Portugal