I-voting on mobile devices: the open issues

Arnis Parsovs
University of Tartu

May 27, 2022

1 Introduction

In April 2020, Cybernetica AS released the report “Mobile voting feasibility study and risk analysis” [1], which found that introducing a mobile i-voting application for Estonian i-voting has its risks but is possible. On March 2022, the Estonian Information System Authority (Riigi Infosüteemi Amet – RIA) announced that an agreement has been signed with Cybernetica AS for the development of an i-voting application for mobile devices [2]. The State Electoral Service (Riigi valimisteenistus – RVT) has yet to decide whether the i-voting mobile app will be provided for the upcoming RK2023 election, which is scheduled to take place in March 2023.

This report provides our input to the discussion on open issues concerning the introduction of i-voting on mobile devices. The discussion is based on the 2022-05-18 mobile voting risks table maintained by RVT that contains the issues highlighted by RVT and the corresponding comments added by Cybernetica AS.

1.1 The proposed mobile i-voting concept

The general concept of the proposed i-voting on mobile devices is as follows. The i-voting app will be created for both iOS and Android platforms. The app will only be distributed via Google Play Store and Apple App Store. The source code of the app will be made public. The i-voting protocol will be the same as implemented in the current desktop i-voting application. At the end of the voting process, a QR code will be displayed and another mobile device will be needed to verify the vote. The app will support only the Mobile-ID solution for casting the vote.

2 Issues

In this section, we discuss the issues raised by RVT and Cybernetica. We have skipped discussing, in our opinion, insignificant issues to which we had nothing to add. The issues listed below have been ordered based on our opinion of their significance.

2.1 Voting with ID card

RVT: Since it is not possible to vote with an ID card on a mobile device, there may be complaints about it.

Cybernetica: Actually, it is possible to implement ID card support – USB-C reader or NFC can be used. The second option would undoubtedly be more popular because it does not require additional esoteric hardware.

UT: As of May 2022, around 251,000 (19%) people in Estonia have Mobile-ID [3]. This means that if Mobile-ID is the only eID solution supported by the mobile i-voting app, less than 20% of the voters will be able to use this voting option[1].

For the pilot run of the i-voting mobile app, limiting the number of potential i-voters may even be a good measure to reduce the impact of issues that might occur in practice.

However, since the Estonian ID card is the base eID solution in Estonia, RVT should seek to implement ID card support in the i-voting mobile app. As of May 2022, around 910,000 (68%) people in Estonia have the NFC-enabled ID card. By March 2023, this number is estimated to be around 1,075,000, (80%). The ID card support in the i-voting mobile app will also serve as a good showcase, encouraging the development of other e-solutions where the Estonian ID card is used with mobile devices.

We note that the protocol that is used to communicate with the ID card over NFC interface has been well documented [4]. Additionally, a team of computer science BSc students from the University of Tartu have created a proof-of-concept Android app that implements NFC communication with the Estonian ID card [5].

2.2 Voting with Smart-ID (and Mobile-ID)

UT: As of May 2022, around 640,000 (48%) people in Estonia have Smart-ID [3]. Due to the large user base of Smart-ID, it may be very tempting to enable i-voting with Smart-ID, especially in the context of i-voting on mobile devices. However, we would strongly advise against enabling i-voting using Smart-ID[2].

The high rate of the successful banking scams that has taken place over the last couple of years in Estonia, has shown that the Smart-ID solution (and also the Mobile-ID solution) is highly susceptible to phishing attacks [7]. Estonian banks have played a key role in pushing the Smart-ID solution in almost every other mobile device in Estonia. However, a significant part of the Smart-ID users is not capable of understanding the working principles of Smart-ID, some of the users are even ready to confirm any Smart-ID transaction appearing on their device.

A related fundamental weakness of Smart-ID is that anonymous parties can initiate a Smart-ID authentication process, which will result in an unexpected Smart-ID authentication prompt appearing on the user's device. In the best

[1] In KOV2021, around 14% of votes were given using Mobile-ID.

[2] The reasons why RIA did not recommend enabling Smart-ID for KOV2021 are given in [6].

case, such requests will only disturb the Smart-ID user. However, if the user mistakenly confirms the request, the attacker will obtain access to the e-service in question. There is a public report of such an attack recently being carried out against the head of CERT-EE and his family members [8]. It is rather trivial to scale such attacks against the entire Estonian population (e.g., by using the i-voting service to initiate such transactions). Considering the war in Ukraine and the related cyber attacks against the Estonian cyber space, the risk of such attacks only increases.

We note that the Mobile-ID solution shares the fundamental weaknesses of Smart-ID. However, there are a couple of differences in these solutions that make the Mobile-ID solution somewhat less risky compared to Smart-ID:

1. In contrast to Smart-ID, which requires only the personal identification code to initiate the authentication process, Mobile-ID, in addition, requires knowledge of the person's phone number.

2. The relatively small percentage of Mobile-ID users makes attacks against randomly selected people less likely to succeed.

3. At least initially, more tech-savvy people applied for Mobile-ID. However, looking at the number of successful scams involving Mobile-ID users, we are not sure whether this distinction is significant anymore.

Anyhow, it is clear that the Mobile-ID solution is not able to satisfy cyber security demands of a modern e-state and hence the state should seek to replace it with an improved solution. However, regardless of whether a new eID solution is introduced in the near future, RVT should be prepared to remove the Mobile-ID support from i-voting, in case such a need becomes evident.

2.3 Integrity of the app distributed via app stores

RVT: Mobile app final version is not the same that the developer provides. The shop owner makes the final changes in app, and we cannot prove that the app would act as it should be. (Maybe it changes some candidates). Even when one app that is downloadable in Estonia can be verified there is no possibility to verify all the shop apps worldwide (maybe US apps are modified).

UT: Yes, in the case of a mobile app, the maintainer of the app store becomes a middle man in the distribution of the i-voting app.

However, since only the official Android and Apple app stores will be used to distribute the i-voting app, the trust assumptions here are similar to trusting these entities to not distribute malicious operating system updates. While, in practice, the infrastructure for distributing operating system updates is likely better protected than the infrastructure for distributing apps, we are not aware of cases where the offical app stores of these vendors would have been compromised to distribute malicious app versions.

In the case of the Android platform, it is relatively easy to verify whether the package distributed in the app store has been compiled from the claimed source code. Such a verification was done for the Android vote verification app distributed for KOV2017 [9]. A similar verification should also be possible for iOS apps, but it requires much more effort, as Apple applies their own modifications to apps.

2.4 Another mobile device needed to verify the vote

RVT: QR code needs to be verified by another smart device. To scan the code and verify that your choice is correct you need another smart device or borrow it from a friend, but in that case your vote will be downloaded to device that is not yours.

Cybernetica: Vote checking is primary for assuring that your vote has arrived to the server. Vote secrecy is a secondary issue here. That is why you need to be aware whose phone you borrow for verification.

UT: The official vote verification app does not store the vote and only displays the result for a limited period of time. An attack, where a person (from whom the device is borrowed) has modified the app or has installed surveillance software on their phone, is indeed possible in practice. However, such an attack setting is far from optimal if the attacker's goal is to restrict the voter's right to free election (which is the main purpose of a secret vote and not the protection of the voter's private life).

A more significant issue here is the fact that another mobile device is required to verify the vote. There are not too many people who have several mobile devices in their possession. While another mobile device could be borrowed from a friend, family member or colleague, it is not clear whether the potential vote verifiers will have enough motivation to bother another person with their wish to verify the vote. Not to forget that the sharing of the device also implies privacy risks to the person who shares their device.

It is likely that the voters who wish to verify their vote will simply stick to the desktop-based i-voting application. Therefore, it is rather safe to assume that the number of votes verified among the votes cast using the mobile i-voting app will be very low. This in turn means that special attention should be paid to ensure that a benign i-voting app is distributed to the voters.

2.5 Fixing the app during election

RVT: If a critical app update is needed, it will take a long time, and the update may not be available in the app stores.

UT: Yes, pushing updates through app stores will take significantly more time, compared to the desktop i-voting application that can be updated simply by replacing the executable hosted on the `valimised.ee` website.

The need to update the app during election is real, and indeed it can take a significant amount of time. For example, there has been a need to issue a critical update to the vote verification app during election. In EP2014, on the first day of i-voting, a bug in the iOS-based vote verification app was discovered. The bug was fixed and an updated iOS application was placed in the iOS App Store on the second day of i-voting (see Section 4.4 in [10]).

However, considering that there are alternative means for i-voting, we do not consider this availability risk to be a major issue.

In order to reduce the impact of such incidents, RVT should consider implementing a remote run-time configuration mechanism that would provide the possibility to display information in the mobile i-voting app in case there are known issues with the app. The voters could be instructed to wait for an update or to pursue alternative means of i-voting. It would be wise to also implement a similar mechanism for the vote verification app and the desktop i-voting application.[3]

2.6 Security-critical remote configuration

RVT: Creating an m-voter application in every election is more complicated and takes more time.

RVT: Mobile app can be forwarded to download incorrect configuration file – to avoid that the configuration file signer data needs to be hardcoded to mobile app.

UT: Since pushing an app update through app stores takes more effort and time, it is tempting to use the same i-voting app over several elections. This requires the election specific configuration to be distributed in a remote configuration file.

We would advise against distributing a security-critical configuration using a remote configuration file. I.e., at least the election public key should be hardcoded in the app. This, however, will require an app update to be issued before each election.

However, if a fully election-agnostic i-voting app is needed, the integrity of the configuration file should be ensured by digital signatures of at least two persons authorized by the election organizers, and each change in the configuration file should be protocoled.

2.7 Spread of unofficial i-voting apps

RVT: Self-made mobile application brings in more incorrect ballots. Person who has more IT knowledge can make his own app and produce incorrect or unreadable ballots.

RVT: There could be more complaints. If the self-made application is easier to produce, then there could be complaints like why my cryptogram is invalid just because the candidate's name is uppercase, or the number of the candidate is after the candidate's name etc.

RVT: Easier to show that voter application can be manipulated – trust for elections is decreasing.

RVT: Voter downloads wrong app from store that looks like voting app that changes the voter choice. These situations can happen and the voter can not verify the vote because second smart device is needed.

[3] This would also enable the time of the opening of the corresponding application to be established, which may be beneficial from the log analysis perspective.

UT: The availability of an open source reference implementation of the i-voting app will make it easier to develop unofficial i-voting apps or desktop applications. However, strongly motivated activists could have done this already since 2013, when the server-side code of the i-voting system was made public on GitHub. We do not see a large market for unofficial i-voting applications, as the official i-voting application is well maintained and available for the most popular desktop operating systems and now will also be available for mobile platforms. If, however, some unofficial i-voting application enters the market, the election organizers should clearly communicate to the public that only the official i-voting application has been audited and is guaranteed by the state to work correctly.

UT: There is indeed a risk that malicious modifications could be added to the official i-voting app and such a repackaged app could be redistributed in other app stores or in the official app stores but under different names. Voters who will locate the i-voting app through the links published on the `valimised.ee` website should not be affected. However, voters who will search for the app in their favorite app store may be tricked into installing such a malicious app. Preferably, the election organizers or CERT-EE should actively monitor various app stores for malicious versions of the i-voting app and, if found, submit takedown requests to the corresponding app store owners.

UT: The casting of invalid i-votes and the demonstration of proof-of-concept i-voting malware will become somewhat easier. However, since we, as a society, have already been there, we should not assign too much significance to the possibility of the occurrence of such incidents.

Acknowledgements. This work has been carried out with financial support from the European Social Fund through the IT Academy programme and financial support from the Estonian Ministry of Economic Affairs and Communications.

References

[1] Cybernetica AS. Mobile voting feasibility study and risk analysis, April 16, 2020. `https://www.valimised.ee/sites/default/files/uploads/eng/2020_m-voting-report.pdf`.

[2] Estonian Information System Authority. A pilot application is created for e-voting on smart devices, March 21, 2022. `https://www.ria.ee/en/news/pilot-application-created-e-voting-smart-devices.html`.

[3] Estonian Information System Authority. The number of Mobile-ID and Smart-ID users in Estonia, May 25, 2022. `https://www.id.ee/en/`.

[4] Sander-Karl Kivivare. *Secure Channel Establishment for the NFC Interface of the New Generation Estonian ID Cards*. BSc thesis, University of Tartu, 2020. `https://comserv.cs.ut.ee/ati_thesis/datasheet.php?id=70557&year=2020`.

[5] Geenius. Students created software that allows them to use an ID card with a smartphone (in Estonian), January 19, 2022. https://digi.geenius.ee/rubriik/uudis/tudengid-loid-tarkvara-mis-laseb-id-kaarti-kasutada-nutitelefoniga/.

[6] Estonian Information System Authority. Smart-ID and elections (in Estonian), May 28, 2020. https://blog.ria.ee/smart-id-ja-valimised/.

[7] Postimees. The application, created for security reasons, has become a trap for Estonians (in Estonian), December 4, 2021. https://majandus.postimees.ee/7400602/turvalisuse-huvides-loodud-rakendusest-on-saanud-uus-eestlaste-petuloks.

[8] Ohtuleht.ee. A hacker, who made a fake Tinder account of the guardian of the digital state, will be left without a reward (in Estonian), September 26, 2021. https://www.ohtuleht.ee/1044266/enneolematu-tuli-digiriigi-valvurile-tinderisse-libakonto-teinud-hakker-jaab-preemiata#.

[9] Annika Tammik. Reproducing Android Vote Verification Application Builds for Estonian I-Voting System, February 20, 2018. https://cybersec.ee/2018/02/20/reproducing-vote-verification-application-builds-for-estonian-i-voting-system/.

[10] Sven Heiberg, Arnis Parsovs, and Jan Willemson. Log Analysis of Estonian Internet Voting 2013–2015. Cryptology ePrint Archive, Report 2015/1211, 2015. http://eprint.iacr.org/2015/1211.