

# Reproducing Vote Verification Application Builds for Estonian I-Voting System

Report in Research Seminar in Cryptography  
(MTAT.07.022)

Annika Tammik

December 5, 2017

# Introduction

## Internet voting and Vote Verification Apps

- Internet voting in Estonia (from 2005)
- In 2011 several potential attacks were published
- From 2013 possibility to verify cast vote with a mobile device
  - Android and iOS supported
  - Distributed in Google Play Store and iOS App Store
  - Source code available in Estonian National Electoral Committees GitHub repository

## Objective of the work

Verify if binary distributed during I-voting held in October 2017 matches the source code published in GitHub

# Tasks

- Monitoring the Apps in the App Stores
- Building the Android Vote Verification App from Source Code
- Reproducing the Android Vote Verification App
- Recommendations for VVA Developers

# Monitoring the Apps in the App Stores

- Downloading Android apps
  - Unofficial web-sites
  - Downloading tools
  - Google Play Unofficial Python API
    - No monitoring functionality
    - Google Play Store App Monitor
- Downloading iOS apps
  - Web-sites with a promise
  - No downloading tools
  - Removed functionality from iTunes
  - No relevant documentation

# Downloaded Android Binaries

I-voting period from 5th until the 11th of October 2017

1. ee.ivxv.ivotingverification 21.apk<sup>1</sup> (downloaded on October 2, 2017)
2. ee.ivxv.ivotingverification 22.apk<sup>2</sup> (downloaded on October 10, 2017)
  - recentChangesHtml: "Parandused seoses uuendamata ID-kaartidega"

---

<sup>1</sup>SHA256:

35dac3859ffbe4d85acd20e51c117f17425b26e2db4520ce9aea7533e7583c94

<sup>2</sup>SHA256:

cbb1f86cebfcfd2c02715e6ca2999b5d609ab6aecb092115d25b205ddc00f221b

# Building the Android App

- Lack of documentation / required versions information
- Assumptions based on the technology stack
  - Android SDK
  - Java JDK
  - Gradle
- Assumptions based on the runtime errors
  - Dependencies in the lib folder

# Reproducing the Android Vote Verification App

- Expected differences
  - Signed vs un-signed
  - Only one commit in GitHub (from the 3rd of September)
  - Version differences in `ivotingverification/app/build.gradle` (vc. 16 and vs. 3.1.3 versus vc. 21 and vs. 3.1.7)
  - Versions of dependencies
- Comparing the binaries
  - Different tools available (diffoscope and apkdiff)
  - Challenges in related to the reproduction



# diffoscope

zipinfo ()	13.3 KB
1 Zip file size: 300258 bytes, number of entries: 458	1 Zip file size: 320683 bytes, number of entries: 453
2 ----- 2.0 fat 3200 b-defn 80-000-00-00 AndroidManifest.xml	2 ----- 2.0 fat 3200 b-defn 80-000-00-00 AndroidManifest.xml
3 ----- 2.4 fat 3820 b-defn 80-000-00-00 META-INF/CIEST.FIF	3 ----- 2.4 fat 3827 b-defn 80-000-00-00 META-INF/CIEST.FIF
4 ----- 2.4 fat 407690 b-defn 80-000-00-00 META-INF/CIEST.FIF	4 ----- 2.4 fat 407696 b-defn 80-000-00-00 CIEST.FIF
5 ----- 2.4 fat 46660 b-defn 80-000-00-00 META-INF/CIEST.FIF	
6 ----- 2.4 fat 473800 b-defn 80-000-00-00 classes.dex	
7 ----- 2.0 fat 65526 b-defn 80-000-00-00 resources/characters.dat	5 ----- 2.0 fat 65516 b-defn 80-000-00-00 resources/characters.dat
8 ----- 2.0 fat 23247 b-defn 80-000-00-00 resources/compositions.dat	6 ----- 2.0 fat 23247 b-defn 80-000-00-00 resources/compositions.dat
9 ----- 2.0 fat 6 b-defn 80-000-00-00 resources/version.txt	7 ----- 2.0 fat 6 b-defn 80-000-00-00 resources/version.txt
10 ----- 2.0 fat 42868 b-defn 80-000-00-00 resources/org/pongcastle/s509/CertPathReviewerMessages.properties	8 ----- 2.0 fat 42868 b-defn 80-000-00-00 resources/org/pongcastle/s509/CertPathReviewerMessages.properties
11 ----- 2.0 fat 48660 b-defn 80-000-00-00 resources/org/pongcastle/s509/CertPathReviewerMessages.de.properties	9 ----- 2.0 fat 48660 b-defn 80-000-00-00 resources/org/pongcastle/s509/CertPathReviewerMessages.de.properties
12 ----- 2.0 fat 184 b-defn 80-000-00-00 resources/anim/abc_fade_in.xml	10 ----- 2.0 fat 184 b-defn 80-000-00-00 resources/anim/abc_fade_in.xml
13 ----- 2.0 fat 104 b-defn 80-000-00-00 resources/anim/abc_fade_out.xml	11 ----- 2.0 fat 104 b-defn 80-000-00-00 resources/anim/abc_fade_out.xml
Offset 96, 21 lines modified	Offset 94, 21 lines modified
96 ----- 1.0 fat 390 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_text_select_handle_middle_right_light.png	94 ----- 1.0 fat 390 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_text_select_handle_middle_right_light.png
97 ----- 1.0 fat 262 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_text_select_handle_right_dark.png	95 ----- 1.0 fat 262 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_text_select_handle_right_dark.png
98 ----- 1.0 fat 262 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_text_select_handle_right_light.png	96 ----- 1.0 fat 262 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_text_select_handle_right_light.png
99 ----- 1.0 fat 192 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_activated_mtrl_alpha.9.png	97 ----- 1.0 fat 192 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_activated_mtrl_alpha.9.png
100 ----- 1.0 fat 190 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_default_mtrl_alpha.9.png	98 ----- 1.0 fat 190 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_default_mtrl_alpha.9.png
101 ----- 1.0 fat 182 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_search_activated_mtrl_alpha.9.png	99 ----- 1.0 fat 182 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_search_activated_mtrl_alpha.9.png
102 ----- 1.0 fat 182 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_search_default_mtrl_alpha.9.png	100 ----- 1.0 fat 182 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_search_default_mtrl_alpha.9.png
103 ----- 1.0 fat 208 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_close.png	101 ----- 1.0 fat 208 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_close.png
104 ----- 1.0 fat 212 b-stor 80-000-00-00 res/drawable-hdpi-v4/notification_bg_low_normal.9.png	102 ----- 1.0 fat 212 b-stor 80-000-00-00 res/drawable-hdpi-v4/notification_bg_low_normal.9.png
105 ----- 1.0 fat 225 b-stor 80-000-00-00 res/drawable-hdpi-v4/notification_bg_low_pressed.9.png	103 ----- 1.0 fat 225 b-stor 80-000-00-00 res/drawable-hdpi-v4/notification_bg_low_pressed.9.png
106 ----- 1.0 fat 212 b-stor 80-000-00-00 res/drawable-hdpi-v4/notification_bg_normal.9.png	104 ----- 1.0 fat 212 b-stor 80-000-00-00 res/drawable-hdpi-v4/notification_bg_normal.9.png
107 ----- 1.0 fat 225 b-stor 80-000-00-00 res/drawable-hdpi-v4/notification_bg_normal_pressed.9.png	105 ----- 1.0 fat 225 b-stor 80-000-00-00 res/drawable-hdpi-v4/notification_bg_normal_pressed.9.png
108 ----- 1.0 fat 93 b-stor 80-000-00-00 res/drawable-hdpi-v4/notify_panel_notification_icon_bg.png	106 ----- 1.0 fat 93 b-stor 80-000-00-00 res/drawable-hdpi-v4/notify_panel_notification_icon_bg.png
109 ----- 1.0 fat 212 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_close.png	107 ----- 1.0 fat 208 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_close.png
110 ----- 1.0 fat 390 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_text_select_handle_middle_right_light.png	108 ----- 1.0 fat 390 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_text_select_handle_middle_right_light.png
111 ----- 1.0 fat 400 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_text_select_handle_right_dark.png	109 ----- 1.0 fat 400 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_text_select_handle_right_dark.png
112 ----- 1.0 fat 387 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_activated_mtrl_alpha.9.png	110 ----- 1.0 fat 387 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_activated_mtrl_alpha.9.png
113 ----- 1.0 fat 127 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_default_mtrl_alpha.9.png	111 ----- 1.0 fat 127 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_default_mtrl_alpha.9.png
114 ----- 1.0 fat 253 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_search_activated_mtrl_alpha.9.png	112 ----- 1.0 fat 253 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_search_activated_mtrl_alpha.9.png
115 ----- 1.0 fat 342 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_search_default_mtrl_alpha.9.png	113 ----- 1.0 fat 342 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_search_default_mtrl_alpha.9.png
116 ----- 1.0 fat 176 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_close.png	114 ----- 1.0 fat 176 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_close.png
Offset 185, 15 lines modified	Offset 183, 15 lines modified
165 ----- 1.0 fat 310 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_text_select_handle_middle_right_light.png	163 ----- 1.0 fat 310 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_text_select_handle_middle_right_light.png
166 ----- 1.0 fat 187 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_text_select_handle_right_dark.png	164 ----- 1.0 fat 187 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_text_select_handle_right_dark.png
167 ----- 1.0 fat 180 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_text_select_handle_right_light.png	165 ----- 1.0 fat 180 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_text_select_handle_right_light.png
168 ----- 1.0 fat 180 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_activated_mtrl_alpha.9.png	166 ----- 1.0 fat 180 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_activated_mtrl_alpha.9.png
169 ----- 1.0 fat 182 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_default_mtrl_alpha.9.png	167 ----- 1.0 fat 182 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_default_mtrl_alpha.9.png
170 ----- 1.0 fat 181 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_search_activated_mtrl_alpha.9.png	168 ----- 1.0 fat 181 b-stor 80-000-00-00 res/drawable-hdpi-v4/abc_textfield_search_activated_mtrl_alpha.9.png

Figure: Output from diffoscope

## Recommendations for VVA Developers

- Detailed build instructions
- Commit tags for build versions
- Updated source code

Thank you!

Questions?