



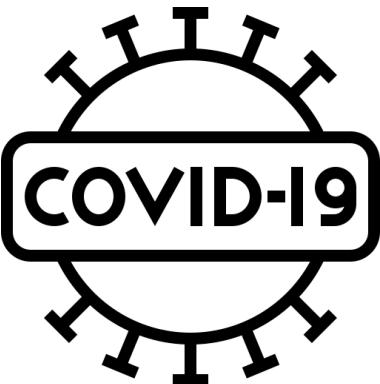
LATVIJAS UNIVERSITĀTE  
**DATORIKAS**  
**FAKULTĀTE**

Eduards Blumbergs (*sf30012*)

# VAKCINĀCIJAS SERTIFIKĀTU MOBILU LIETOTŅU DROŠĪBAS NOVĒRTĒŠANA

Magistra darbs · 2022 · Darba vadītājs: Dr. dat. Pēteris Paikens

# Aktualitāte



*Android* un *iOS* lietotņu veikalos pieejamas daudzas dažādas COVID-19 vakcinācijas sertifikātu mobilās lietotnes, tomēr nav izdarīts pētījums par šādu Latvijā izplatīto lietotņu kiberapdraudējumu un tehnisko drošības līmeni.

Lai pārliecinātos, vai drošība nav kompromitēta, un atklātu ievainojamības, nepieciešama vakcinācijas sertifikātu mobilo lietotņu draudu modelēšana un tehniskā drošības pārbaude.



LATVIJAS  
UNIVERSITĀTE

# Maģistra darba mērķis

Detalizēti izpētīt mobilo lietotņu tehniskās drošības prasības un aprobēt Latvijā populāru vakcinācijas sertifikātu lietotņu drošības līmeni, kā arī konstatēt iespējamās programmatūras ievainojamības.

## Darba uzdevumi

1. Izpētīt, analizēt un apkopot informāciju par mobilajām lietotnēm un to potenciālajām ievainojamībām.
2. Izaanalizēt tīmeklī pieejamo izlūkošanas informāciju par COVID-19 vakcinācijas sertifikātu kvadrātkodu mobilajām lietotnēm.
3. Izveidot vakcinācijas sertifikātu lietotnes potenciālo draudu modeli.
4. Apkopot Latvijā izplatītāko COVID-19 vakcinācijas sertifikātu mobilo lietotņu sarakstu.
5. Veikt tehnisko drošības pārbaudi un izanalizēt potenciālos draudus Latvijā izplatītākajās COVID-19 vakcinācijas sertifikātu mobilajās lietotnēs.



# Ierobežojumi

- Apskatītas Latvijā populāras mobilās lietotnes, kas apstrādā Eiropas digitālo COVID-19 sertifikātu.
- Uzrunātie izstrādātāji un uzturētāji neautorizēja pilnvērtīgu ielaušanās testēšanu un nesniedza piekļuvi iekšējai informācijai, tāpēc modelētos draudus var uzskatīt tikai par teorētiskiem.
- Aizmugursistēmu API un lietotņu saskarņu darbība ir apskatīta mērā, kas nerada nelabvēlīgu ietekmi uz sistēmām, jo piekļuve iekšējiem resursiem nebija autorizēta.
- Aplūkota ir datu aizsardzības perspektīva, nevis pašu vakcinācijas sertifikātu ģenerēšana.
- Lietotņu ievainojamības aplūkotas tikai no melnās kastes testēšanas principa, neveicot pirmkoda kvalitātes analīzi.



LATVIJAS  
UNIVERSITĀTE

# Nozīmīgākie mobilo lietotņu drošības draudi

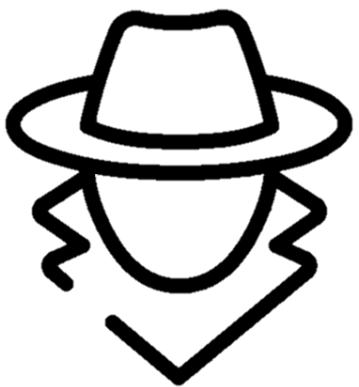


1. Neatbilstoša platformas lietošana (funkcijas izmantošana)
2. Nedroša datu glabāšana (datu iegūšana no ierīces)
3. Nedroša saziņa (nešifrēti dati, neuzticams datortīkls)
4. Nedroša autentifikācija (rekvizītu zādzība vai apiešana)
5. Neatbilstoša šifrēšana (pieklūšana šifrētiem datiem)
6. Nedroša autorizācija (autorizācijas apiešana)
7. Nekvalitatīvs kods (nepietiekama vērtību validācija)
8. Koda sagrozīšana (lietotnes modifcēšana)
9. Reversā inženierija (lietotnes analizēšana ar rīkiem)
10. Nezināma funkcionalitāte (apdraudējums no slēptas funkcionalitātes)



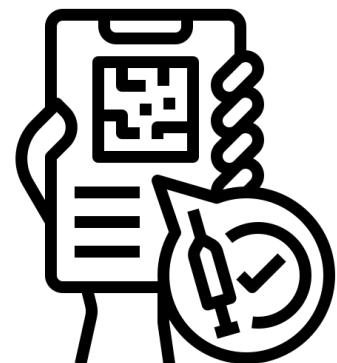
LATVIJAS  
UNIVERSITĀTE

# Testēšanas standarti un prasības



OWASP ir izstrādājis un regulāri papildina Mobilo ievainojamību risku apkopojumu standartu (MASVS), kas nosaka mobilo lietotņu drošības testēšanas scenāriju pamatprasības, un Mobilo lietotņu drošības testēšanas gidi (MSTG), kas detalizēti apraksta MASVS tehniskos procesus un rīkus.

## Vakcinācijas sertifikātu mobilās lietotnes



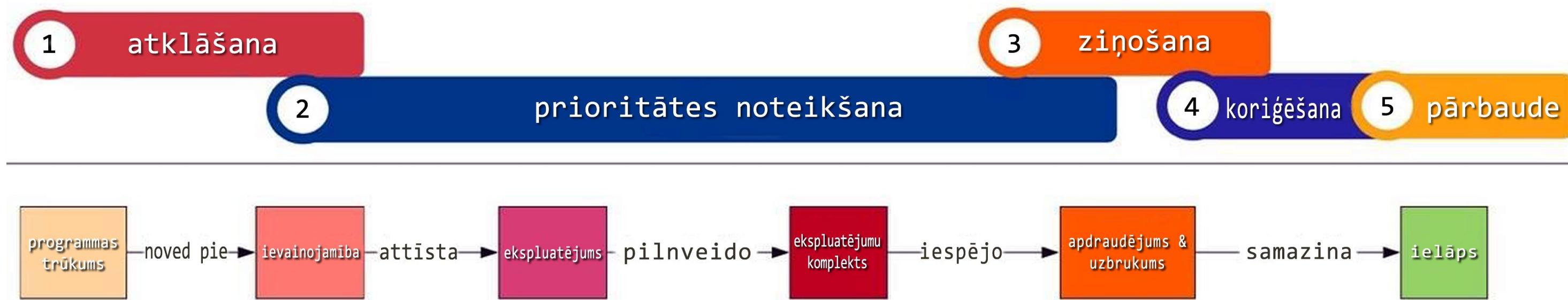
Vakcinācijas sertifikātu mobilās lietotnes izmanto, lai uzglabātu un pārbaudītu vakcinācijas sertifikātu kvadrātkodus. Tās no centralizēta servera regulāri iegūst informāciju par sertifikāta derīguma statusu.



LATVIJAS  
UNIVERSITĀTE

# Programmatūras trūkumi un ievainojamības

- Izplatītāko programmatūras trūkumu saraksts CWE (*Common Weakness Enumeration*).
- Brīvs un atvērts industrijas standarts — CVSS punktu sistēma (*Common Vulnerability Scoring System*) izplatītāko ievainojamību nopietnības izvērtēšanai ļauj prioritizēt resursus problēmu novēršanai.



Avots: European Network and Information Security Agency



LATVIJAS  
UNIVERSITĀTE

# Pētījuma rezultāti



- Latvijā populārāko vakcinācijas sertifikātu mobilo lietotņu apkopojums
- Draudu modelis
- Tehniskās drošības pārbaudes rezultāti

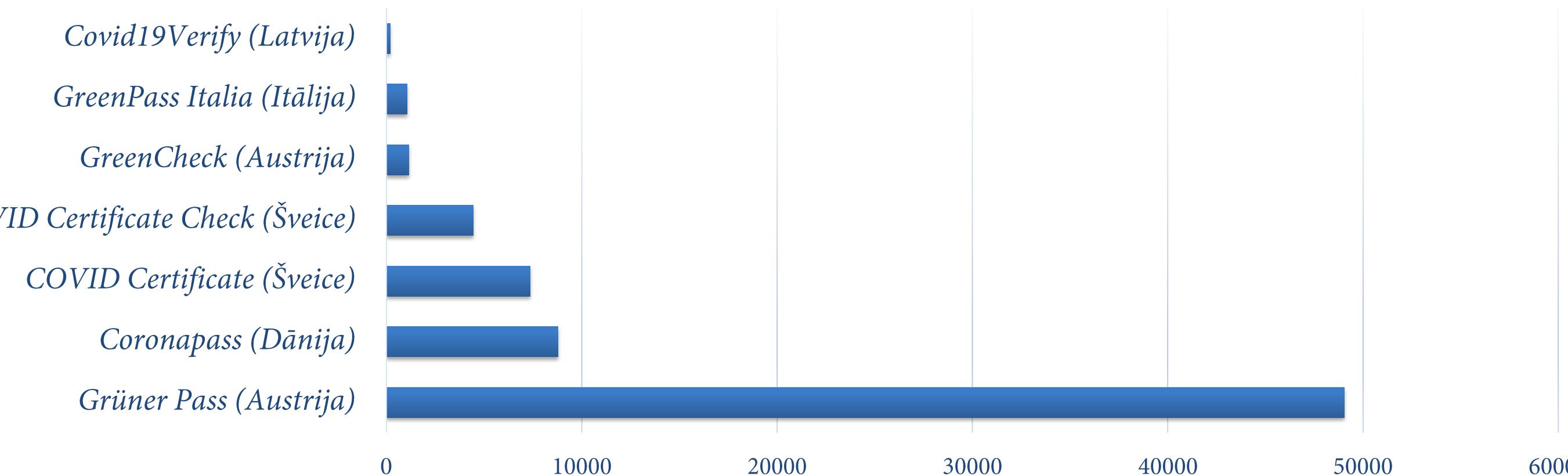


LATVIJAS  
UNIVERSITĀTE

# Latvijā populārāko vakcinācijas sertifikātu mobilu lietotņu apkopojums

- Autors uzstādīja 20 dažādu valstu lietotnes un pārliecinājās par to atbilstību Eiropas vakcinācijas sertifikāta atbalstam.
- Izmantojot *Appmagic* vietni, autors atlasīja populārākās lietotnes, kas pieejamas gan *Android*, gan *iOS* platformā.
- Sarakstā iekļauta arī oficiālā Latvijā izveidotā lietotne *Covid19Verify*.

*Lietotņu popularitātes indekss COVID-19 ierobežojumu laikā Latvijā 2021.g.*



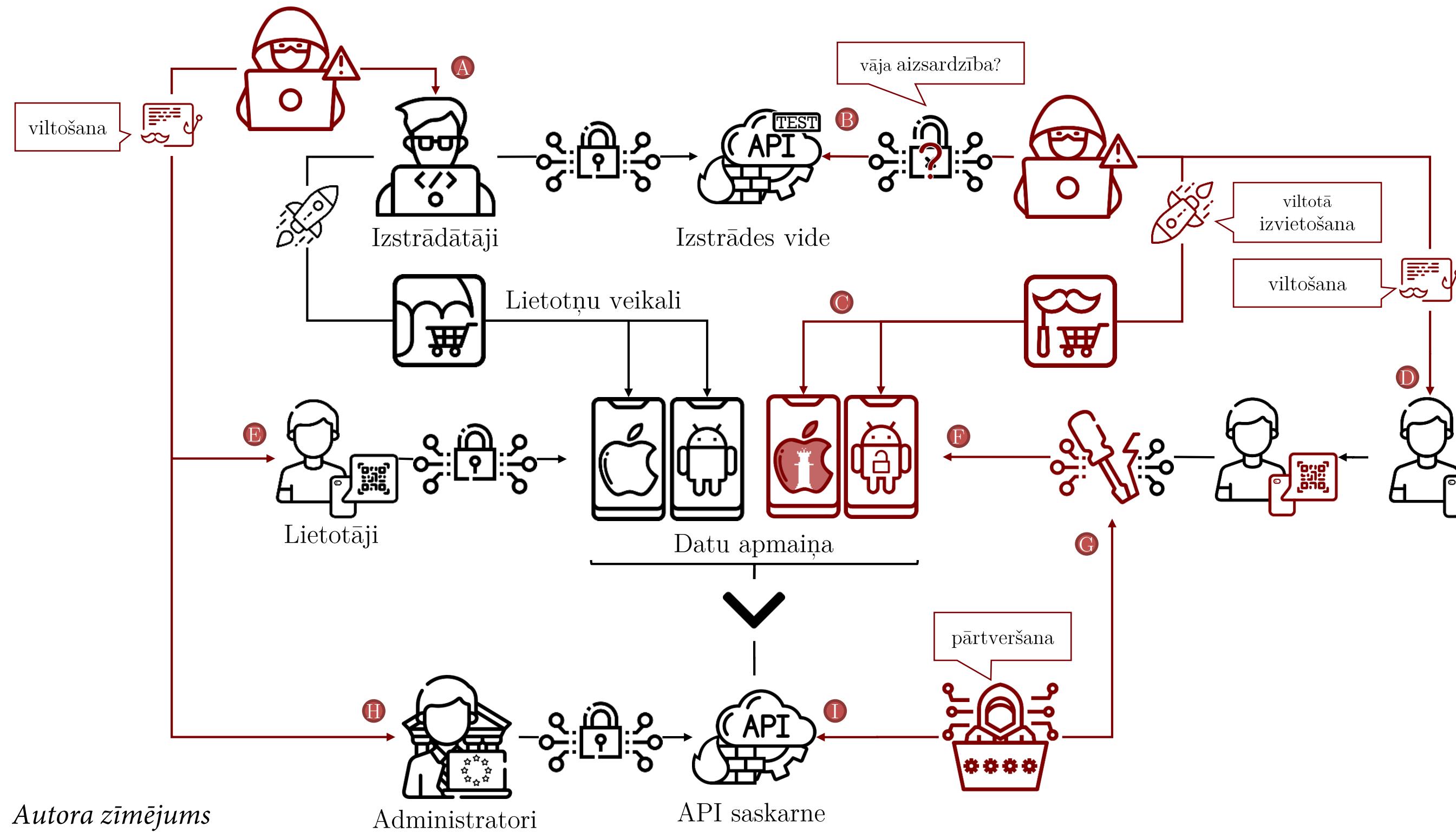
Avots: <https://appmagic.rocks>



LATVIJAS  
UNIVERSITĀTE

# Draudu modelis

*Vakcinācijas sertifikātu mobilo lietotņu potenciālās ievainojamības, draudi un uzbrukuma vektori*



**Galvenie punkti:**

- A: piegādes kēdes uzbrukumi, pikšķerēšana.
- B: datu noplūde no testa vides vai infrastruktūras.
- C: uzbrukumi uzlauztu ierīču lietotājiem.
- D: izstrādātāja radīts apdraudējums, nomelnošanas kampaņas.
- E: sensitīvu datu noplūde, izmainīšana.
- F: lietotnes logikas izmainīšana, datu vākšana no ierīces.
- G: datu pārveršana, izmainīšana, 3.puses bibliotēkas kompromitēšana.
- H: infrastruktūras pārņemšana, kompromitējot priviliģētu lietotāju, pikšķerēšana.
- I: datu pārveršana un noplūde no API saskarnes, datu integratītes ietekmēšana no API ievainojamības.



**LATVIJAS  
UNIVERSITĀTE**

# Tehniskās drošības pārbaudes rezultāti



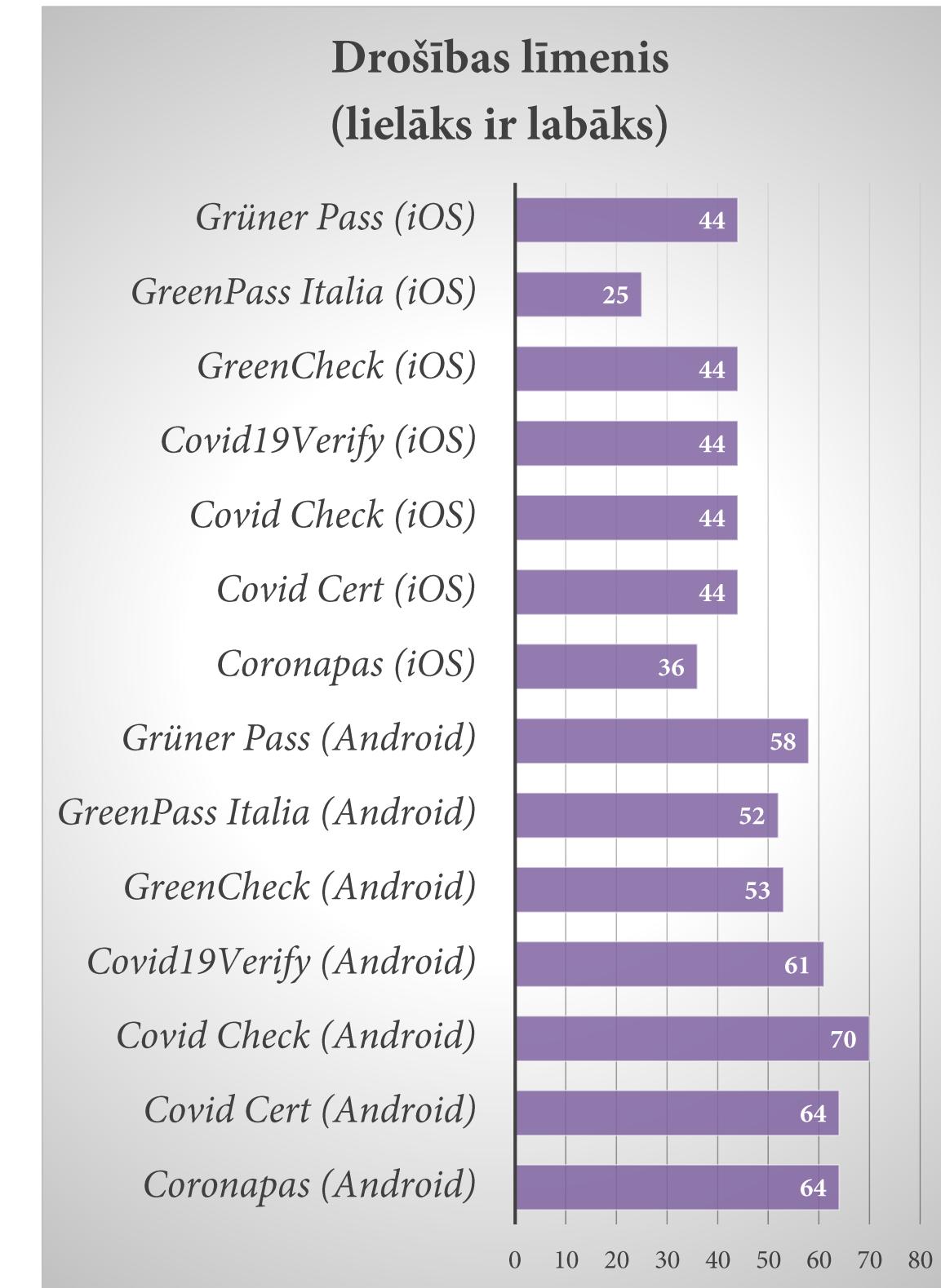
- Lietotņu statistiskā analīze
- Attālo galapunktu datplūsmu pārbaude
- Nozīmīgākie konstatējumi



LATVIJAS  
UNIVERSITĀTE

# Lietotņu statiskā analīze

Nr. p.k.	Nosaukums	Drošības līmenis	Riska novērtējums	Ierīču izsekošana	Augsta prioritāte	Brīdinājumi	OS
1.	Coronapas	64/100	A (zems risks)	0	0	4	Android
2.	Covid Cert	64/100	A (zems risks)	0	0	8	Android
3.	Covid Check	70/100	A (zems risks)	0	0	5	Android
4.	Covid19Verify	61/100	A (zems risks)	0	1	5	Android
5.	GreenCheck	53/100	B (vidējs risks)	0	2	9	Android
6.	GreenPass Italia	52/100	B (vidējs risks)	1	2	13	Android
7.	Grüner Pass	58/100	B (vidējs risks)	0	1	8	Android
8.	Coronapas	36/100	C (augsts risks)	0	3	2	iOS
9.	Covid Cert	44/100	B (vidējs risks)	0	2	2	iOS
10.	Covid Check	44/100	B (vidējs risks)	0	2	2	iOS
11.	Covid19Verify	44/100	B (vidējs risks)	0	2	2	iOS
12.	GreenCheck	44/100	B (vidējs risks)	0	2	2	iOS
13.	GreenPass Italia	25/100	F (kritisks risks)	2	3	3	iOS
14.	Grüner Pass	44/100	B (vidējs risks)	0	2	2	iOS



Autora apkopojums



**LATVIJAS  
UNIVERSITĀTE**

# Attālo galapunktu datplūsmu pārbaude

Nr.p.k.	Nosaukums	Galapunkti	Vidēja prioritāte	Zema prioritāte
1.	<i>Coronapas</i>	<a href="https://api.coronapas.sunhedsdata.dk">https://api.coronapas.sunhedsdata.dk</a>	n/a	n/a
2.	<i>Covid Cert</i>	<a href="https://www.cc.bit.admin.ch">https://www.cc.bit.admin.ch</a>	n/a	n/a
3.	<i>Covid Check</i>	<a href="https://www.cc.bit.admin.ch">https://www.cc.bit.admin.ch</a>	n/a	n/a
4.	<i>Covid19Verify</i>	<a href="https://api.covid19sertifikats.lv">https://api.covid19sertifikats.lv</a>	0	41
5.	<i>GreenCheck</i>	<a href="http://greencheck.gv.at">http://greencheck.gv.at</a>	0	33
6.	<i>GreenPass Italia</i>	<a href="https://firebaseinstallations.googleapis.com">https://firebaseinstallations.googleapis.com</a>	1	1
7.	<i>Grüner Pass</i>	<a href="https://dgc-trust.qr.gv.at">https://dgc-trust.qr.gv.at</a>	0	6



1. Drošības galveņu trūkums vai nepareiza konfigurācija.
2. Satura drošības politikā nav prasīta apakšresursu integritāte.
3. Satura noklausīšanās nav atspējota.
4. Pārlūkprogrammas starpvietņu skriptēšanas filtru nepareiza konfigurācija.
5. *JavaScript* elementiem trūkst apakšresursu integritātes atribūtu.



LATVIJAS  
UNIVERSITĀTE

# Lietotnes «Coronapas» nozīmīgākie konstatējumi

iOS:

1. Lietotne izmanto nedrošus API.
2. Lietotne izmanto nedrošas gadījuma skaitļu funkcijas.
3. Lietotne fona režīmā neslēpj informāciju.

Lietotnes TLS savienojums var tikt pakļauts pakalpojumatteices uzbrukumam.

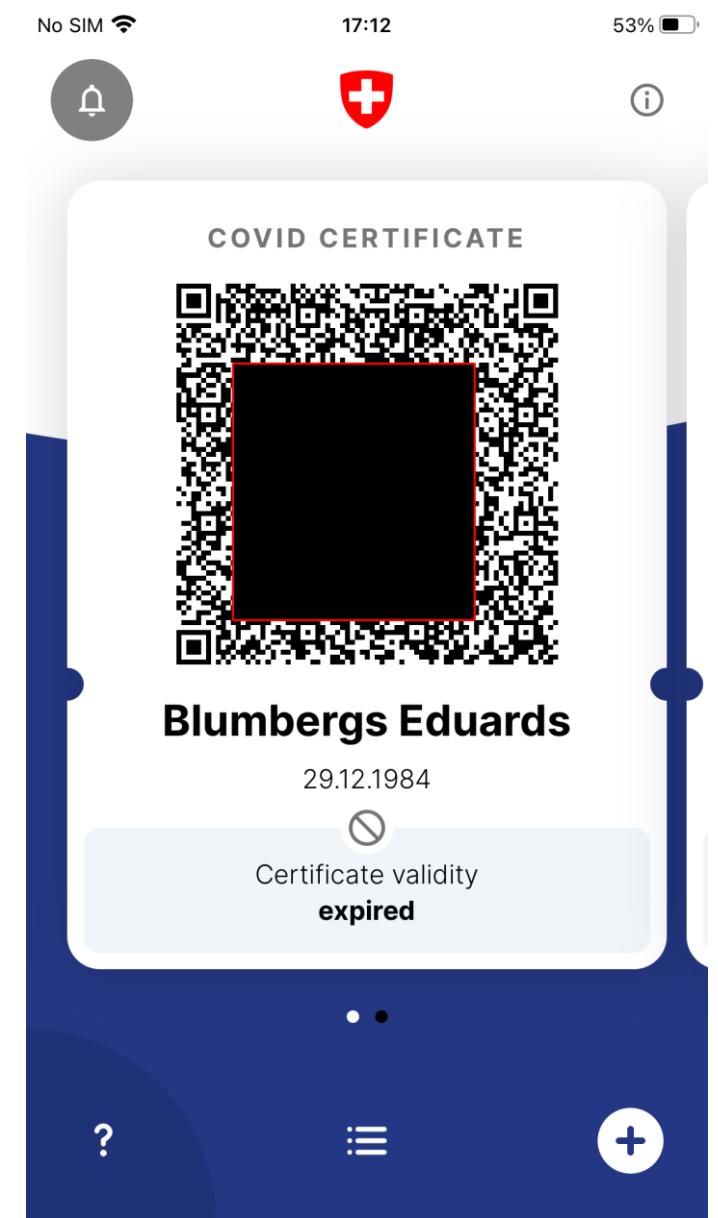


**LATVIJAS  
UNIVERSITĀTE**

# Lietotnes «COVID Certificate» nozīmīgākie konstatējumi

iOS:

1. Lietotne izmanto nedrošus API.
2. Lietotne izmanto funkciju “malloc”.
3. iOS saskarnē *NSUserDefaults*, parametrā “lastConfigURL” glabājas lietotnes konfigurācijas saite.
4. Kešatmiņas datu bāzē ir apskatāmi galapunkti.



```
+-----+
| request_key
+-----+
| https://www.cc.bit.admin.ch/trust/v2/keys/list
| https://www.cc.bit.admin.ch/trust/v1/metadata
| https://www.cc.bit.admin.ch/trust/v2/verificationRules
| https://www.cc.bit.admin.ch/app/wallet/v1/config?appversion=ios-4.1.0&buildnr=ios-220429.1021.99279&osversion=ios14.4
| https://www.cc.bit.admin.ch/trust/v2/keys/updates?certFormat=IOS&since=12310&upTo=12310
| https://www.cc.bit.admin.ch/trust/v2/revocationList?since=11822982
| https://www.cc.bit.admin.ch/trust/v2/revocationList?since=11823021
+-----+
```



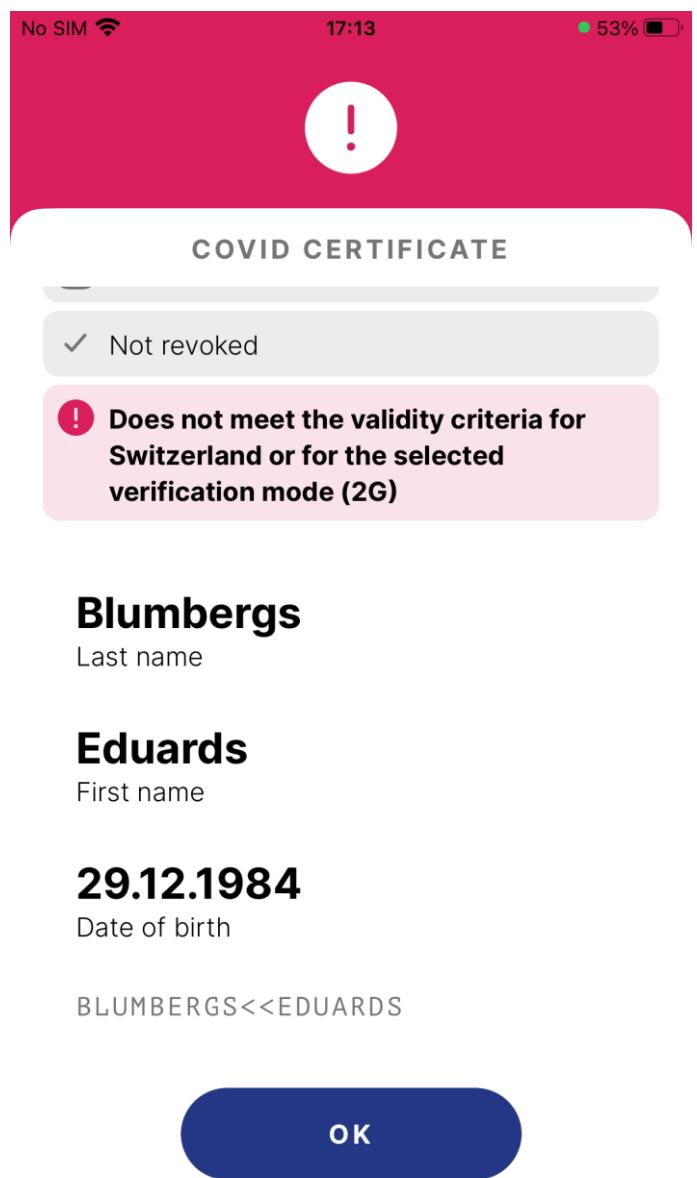
LATVIJAS  
UNIVERSITĀTE

# Lietotnes «COVID Certificate Check» nozīmīgākie konstatējumi

iOS:

1. Lietotne izmanto nedrošus API.
2. Lietotne izmanto funkciju “malloc”.
3. iOS saskarnē *NSUserDefaults*, parametrā “lastConfigURL” glabājas lietotnes konfigurācijas saite.
4. Kešatmiņas datu bāzē ir apskatāmi galapunkti.

```
+-----  
| request_key  
+-----  
  
| https://www.cc.bit.admin.ch/trust/v1/metadata  
| https://www.cc.bit.admin.ch/trust/v2/keys/list  
| https://www.cc.bit.admin.ch/trust/v2/verificationRules  
| https://www.cc.bit.admin.ch/app/verifier/v1/config?appversion=ios-4.0.0&buildnr=ios-220411.1820.99268&osversion=ios14.8  
| https://www.cc.bit.admin.ch/trust/v2/keys/updates?certFormat=IOS&since=&upTo=12307  
| https://www.cc.bit.admin.ch/trust/v2/keys/updates?certFormat=IOS&since=12307&upTo=12307  
| https://www.cc.bit.admin.ch/trust/v2/revocationList?since=11822103  
+-----
```



LATVIJAS  
UNIVERSITĀTE

# Lietotnes «Covid19Verify» nozīmīgākie konstatējumi

iOS:

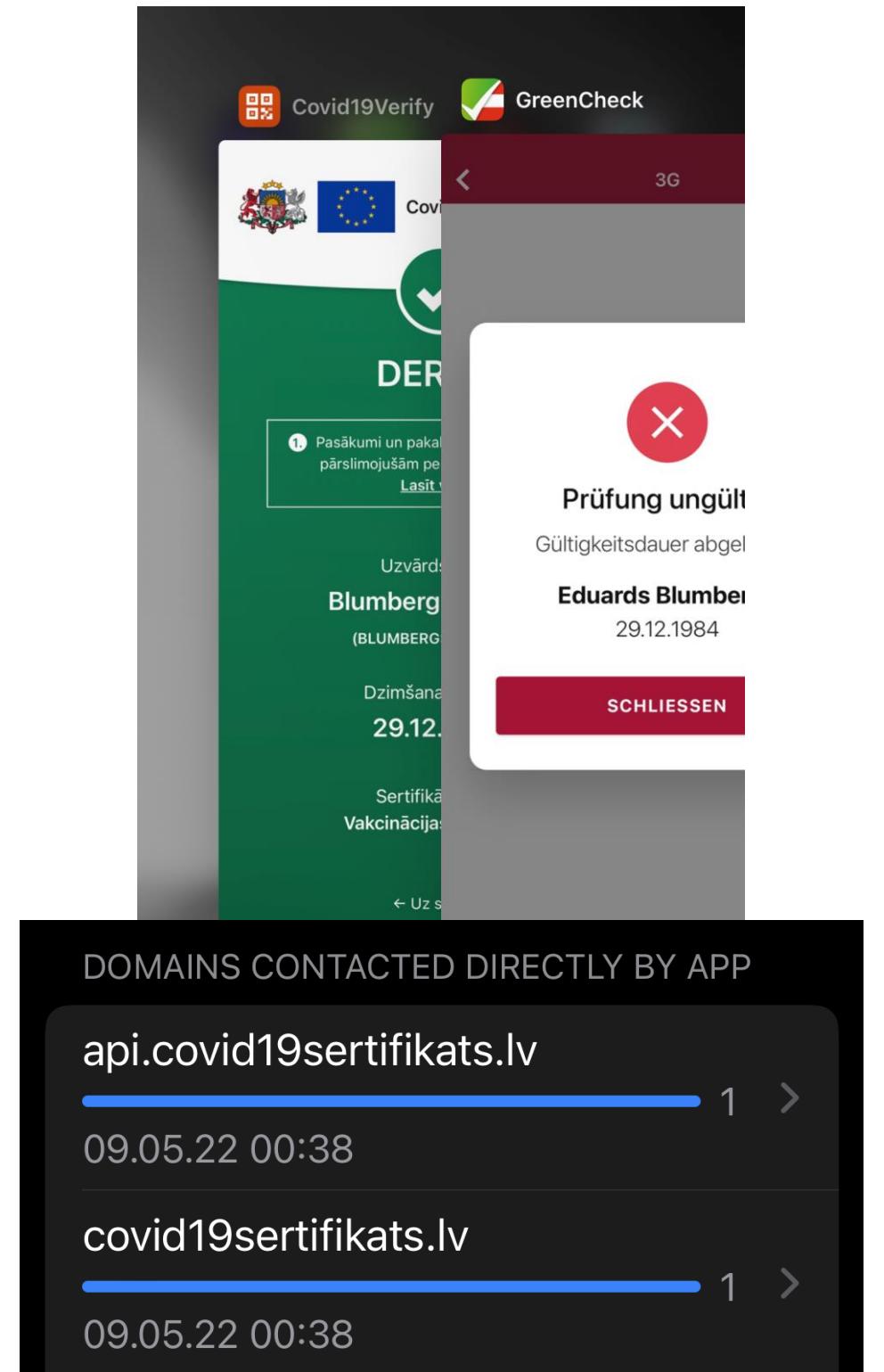
1. ATS (*App Transport Security*) nedroša savienojuma izmantošana domēniem, kas nav iekļauti saskarnē *NSEExceptionDomains*.
2. Neizmanto funkciju “-fstack-protector-all”, kas pasargātu no steka adreses pārrakstīšanas.
3. Fona režīmā neslēpj informāciju.
4. Pagaidu failu mapē “tmp” saglabā visus augšupielādētos failus, un tie automātiski netiek dzēsti. Lielas iespējas nozagt sensitīvu informāciju, ja tiek iegūtas pilnas tiesības ierīcē.

*Android:*

1. Serviss “com.google.android.play.core.AssetPack ExtractionService” nav aizsargāts no citu lietotņu piekļuves.

Lietotne lejupielādē konfigurāciju no galapunkta

<https://covid19sertifikats.lv/verify/rules.json>, kas izmanto nedrošu TLS konfigurāciju un šifrus, kas ir pakļauti zināmām ievainojamībām.



LATVIJAS  
UNIVERSITĀTE

# Lietotnes «Green Check» nozīmīgākie konstatējumi

iOS:

1. Lietotne izmanto nedrošus API.
2. Lietotne izmanto funkciju “malloc”.
3. Fona režīmā neslēpj informāciju.

Android:

1. Darbība “at.itsv.mobile.cochap.MainActivity” nav aizsargāta no citu lietotņu piekļuves.
2. Lietotne izmanto nedrošus CBC kriptogrāfiskos šifrus.

Lietotne sazinās ar galapunktu, kas izmanto nedrošus CBC šifrus, kuri ir pakļauti zināmām ievainojamībām.



LATVIJAS  
UNIVERSITĀTE

# Lietotnes «GreenPass Italia» nozīmīgākie konstatējumi

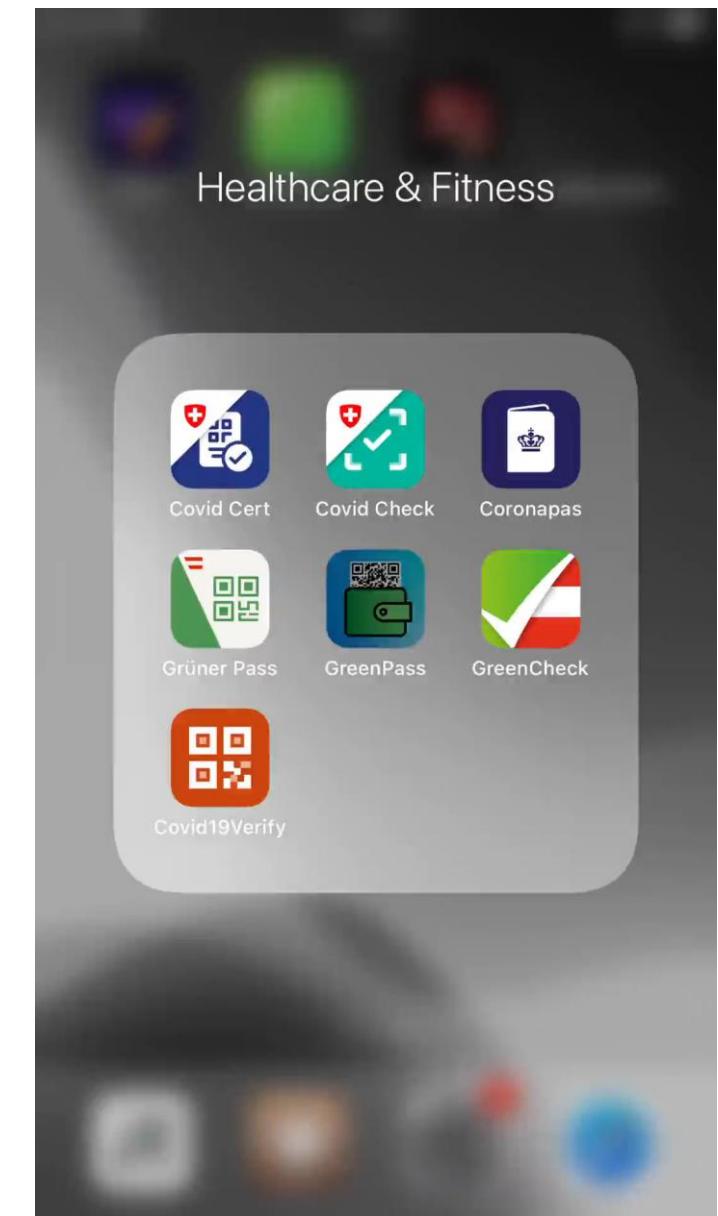
iOS:

1. Lietotne izmanto nedrošus API.
2. Lietotne izmanto nedrošas gadījuma skaitļu funkcijas.
3. Lietotne izmanto funkciju “malloc”.
4. Lietotne fona režīmā neslēpj informāciju .
5. Lietotne izmanto (6.12. att.) novecojušu un nedrošu *OpenCV* bibliotēkas versiju 3.4.0, kā arī neatbalstītu *Python* valodas versiju 2.7.6.
6. Lietotne visu sertifikātu informāciju nešifrēti glabā saskarnē *NSUserDefaults*, parametrā “flutter.green\_pass\_list”, kur iespējams izmanīt lietotāja personas datus, jo sertifikāta informācija tiek nolasīta tikai pirmajā pievienošanas reizē.
7. Pagaidu failu mapē “tmp” saglabā visus augšupielādētos failus, un tie automātiski netiek dzēsti. Lielas iespējas nozagt sensitīvu informāciju, ja tiek iegūtas pilnas tiesības ierīcē.

*Android* statiskās analīzes augstas prioritātes konstatējumi:

1. Lietotne var sazināties, izmantojot atvērtu tekstu.
2. Serviss “com.google.android.play.core.AssetPackExtractionService” nav aizsargāts no citu lietotņu piekļuves.

Lietotne sazinās ar galasistēmu <https://firebaseinstallations.googleapis.com>, kura izmanto nedrošu konfigurāciju: novecojušus TLS protokolus 1.0 un 1.1, kā arī šifrus, kas ir pakļauti vairākām zināmām ievainojamībām: SWEET32, BEAST, LUCKY13.



**LATVIJAS  
UNIVERSITĀTE**

# Lietotnes «Grüner Pass» nozīmīgākie konstatējumi

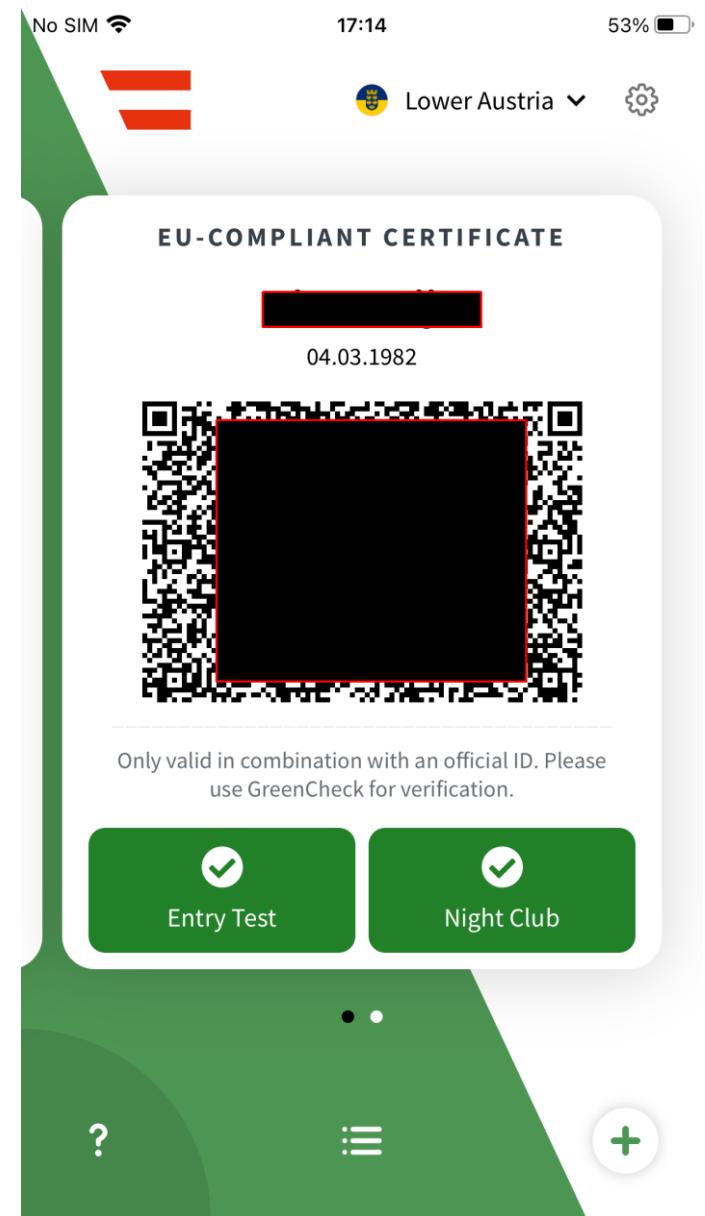
iOS:

1. Lietotne izmanto nedrošus API.
2. Lietotne izmanto funkciju “malloc”.
3. Lietotnē failā Info.plist ir pieejams API markieris. Failā esošā informācija nav šifrēta un tas ir iekļauts arī lietotnes uzstādīšanas pakotnē.

Android:

1. Serviss “com.google.android.play.core.AssetPackExtractionService” nav aizsargāts no citu lietotņu piekļuves.

Lietotnes tīmekļa datplūsmu var noklausīties un izmainīt.



LATVIJAS  
UNIVERSITĀTE

# Secinājumi (1)

1. Vakcinācijas sertifikātu kvadrātkodu apstrādei izmantotās lietotnes ir plaši izplatītas, tomēr publiski pieejams maz informācijas par to drošības novērtējumu.
2. Tīmeklī ir pieejama plaša informācija par mobilo lietotņu potenciālajām ievainojamībām, kā arī dažādas specifikācijas, kas palīdz potenciālo draudu modelēšanā.
3. Potenciālo draudu modelēšana ļauj vieglāk apkopot prasības vakcinācijas sertifikātu lietotņu drošības līmeņa aprobācijai un programmatūras ievainojamību konstatēšanai.
4. Pilnvērtīgas biznesa informācijas apkopošana par trešās puses COVID-19 lietotņu popularitāti ir sarežģīts un dārgs process, jo pieejamie rīki nav pieejami bez reģistrācijas un tie piedāvā ļoti nelielu bezmaksas funkcionalitāti.



LATVIJAS  
UNIVERSITĀTE

# Secinājumi (2)

5. Veicot tehnisko drošības pārbaudi izdevās atklāt vairākas ievainojamības, kas saistītas ar nepienācīgu datu saglabāšanu un pārsūtīšanu, kā arī nesavlaicīgu datu dzēšanu.
6. Vairāku lietotņu datu datplūsmu bija iespējams noklausīties un izmainīt.
7. Nēmot vērā, ka lietotnes varēja darbināt ar augstākā līmeņa pilnvarām un pieklūt pilnīgi visiem sensitīvajiem datiem, kas nebija saglabāti vai pārsūtīti šifrētā veidā, var secināt, ka vakcinācijas lietotnēm nepieciešamas augstākas prasības gan tiesību līmeņa kontrolei, gan datu šifrēšanai.
8. Lai mazinātu datu pārtveršanas uzbrukumus, izstrādātājiem vienmēr ieteicams izmantot sertifikātu piespraušanu, gan lai verificētu atzītus sertifikātus, gan ļautu droši izmantot pašparakstītus sertifikātus.
9. Dažas lietotnes joprojām izmanto neaizsargātus TLS savienojumus, ļaujot uzbrucējiem pārtvert datplūsmu, jo tās vai nu akceptē visus pašparakstītos sertifikātus, vai arī nepārbauda domēna vārdu.

# Turpmākais darbs

Paveiktajā darbā ir apskatīta tikai neliela daļa lietotņu, koncentrējoties uz lietotnēm, kas tiek visvairāk izmantotas Latvijā, tomēr nepieciešami tālāki pētījumi, iesaistot un aktivizējot izstrādātājus, kurus šoreiz ieinteresēt neizdevās, lai varētu pilnvērtīgi pārbaudīt aizmugursistēmas, kā arī iegūt pirmkodus kvalitātes analīzei un caurskatīšanai.

Nepieciešams celt arī sabiedrības zināšanu līmeni par niansēm, kas ir atklājušās tehnisko drošības testu laikā, kā arī par veidiem, kas jaunajiem lietotājiem palīdzētu izvēlēties visdrošākās un kvalitatīvākās lietotnes no pieejamā klāsta. Pieaugot lietotņu skaitam, kas apstrādā sensitīvu informāciju, obligāti jāanalizē, kā lietotnes piekļūst un pārsūta informāciju.



LATVIJAS  
UNIVERSITĀTE

# PALDIES PAR UZMANĪBU!



LATVIJAS  
UNIVERSITĀTE