Tallinn University of Technology

Masters Thesis in Cyber Security

Security Analysis of Internet Bank Authentication Protocols and their Implementations

Supervisors

Peeter Laud, PhD

Marko Kääramees, MSc

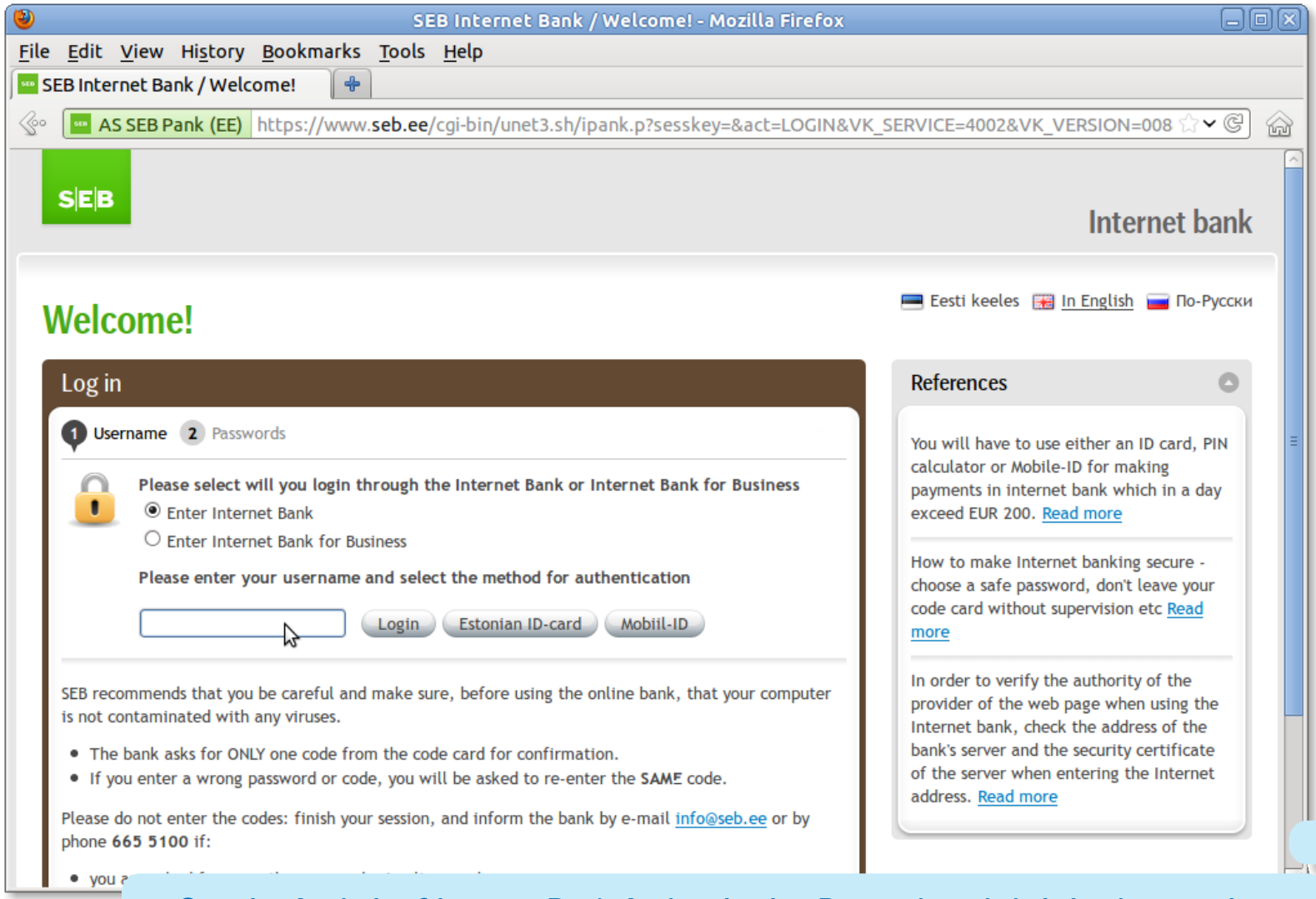
Author

Arnis Paršovs

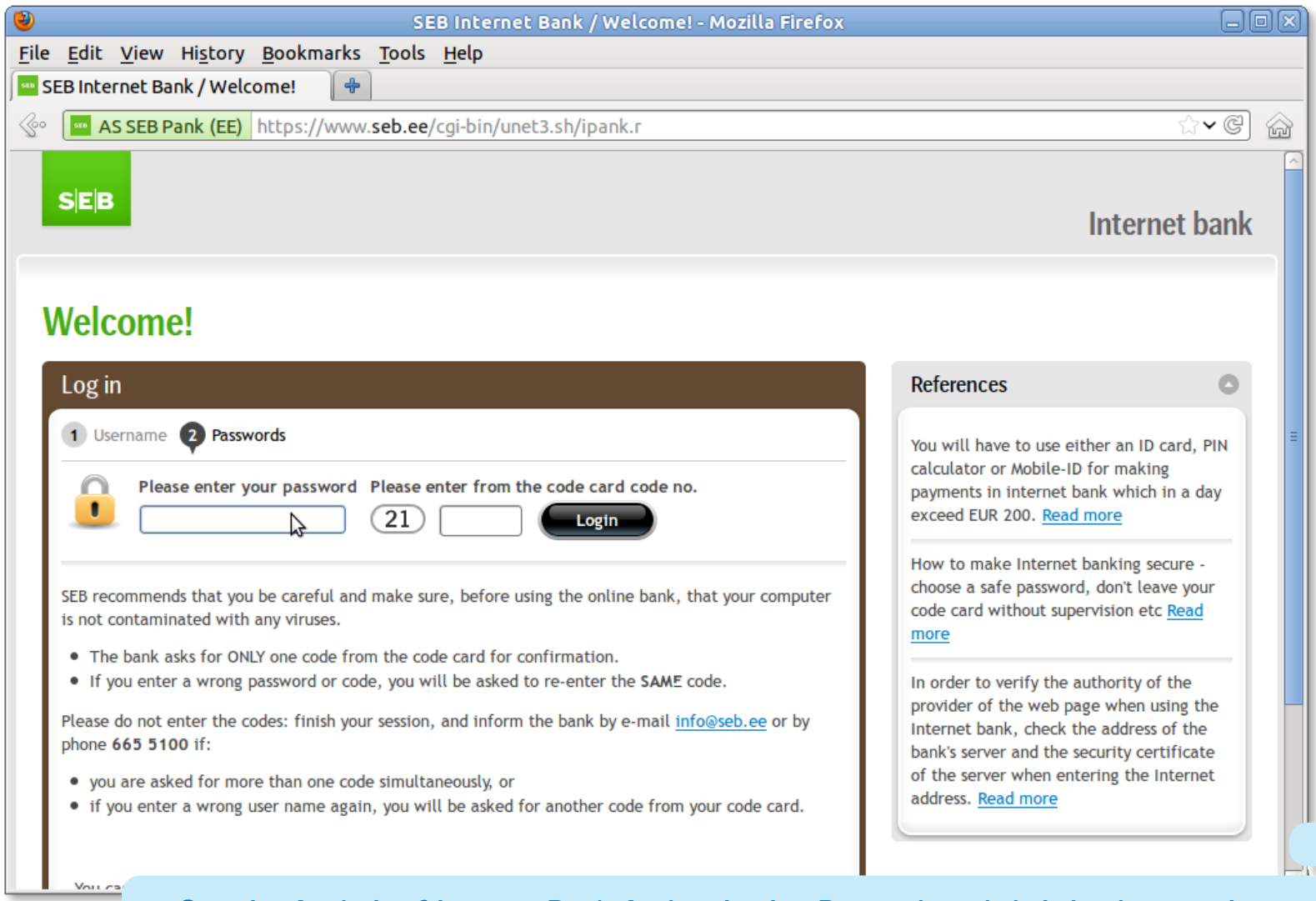
June 11, 2012

Internet Bank Authentication

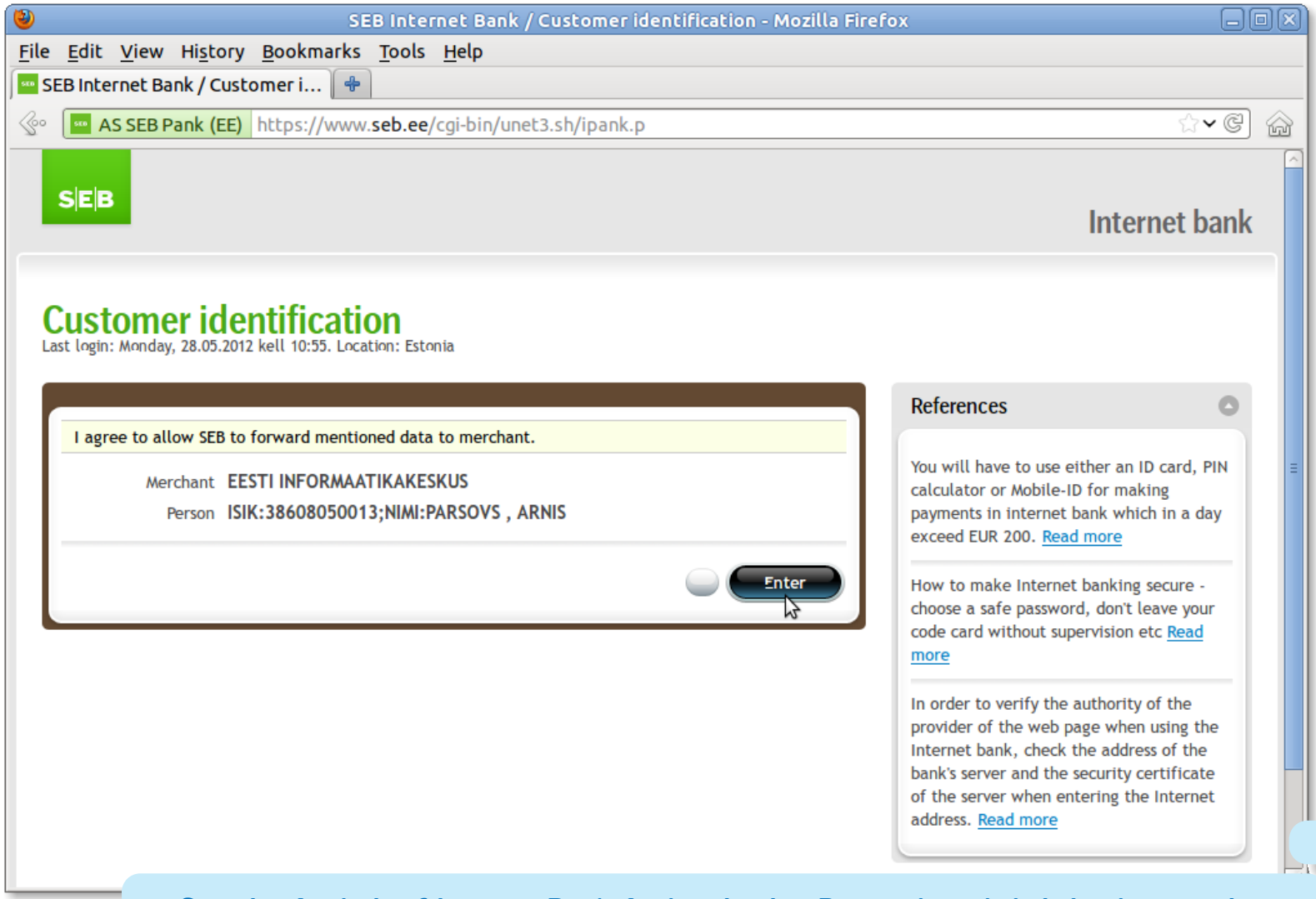
Internet Bank Authentication



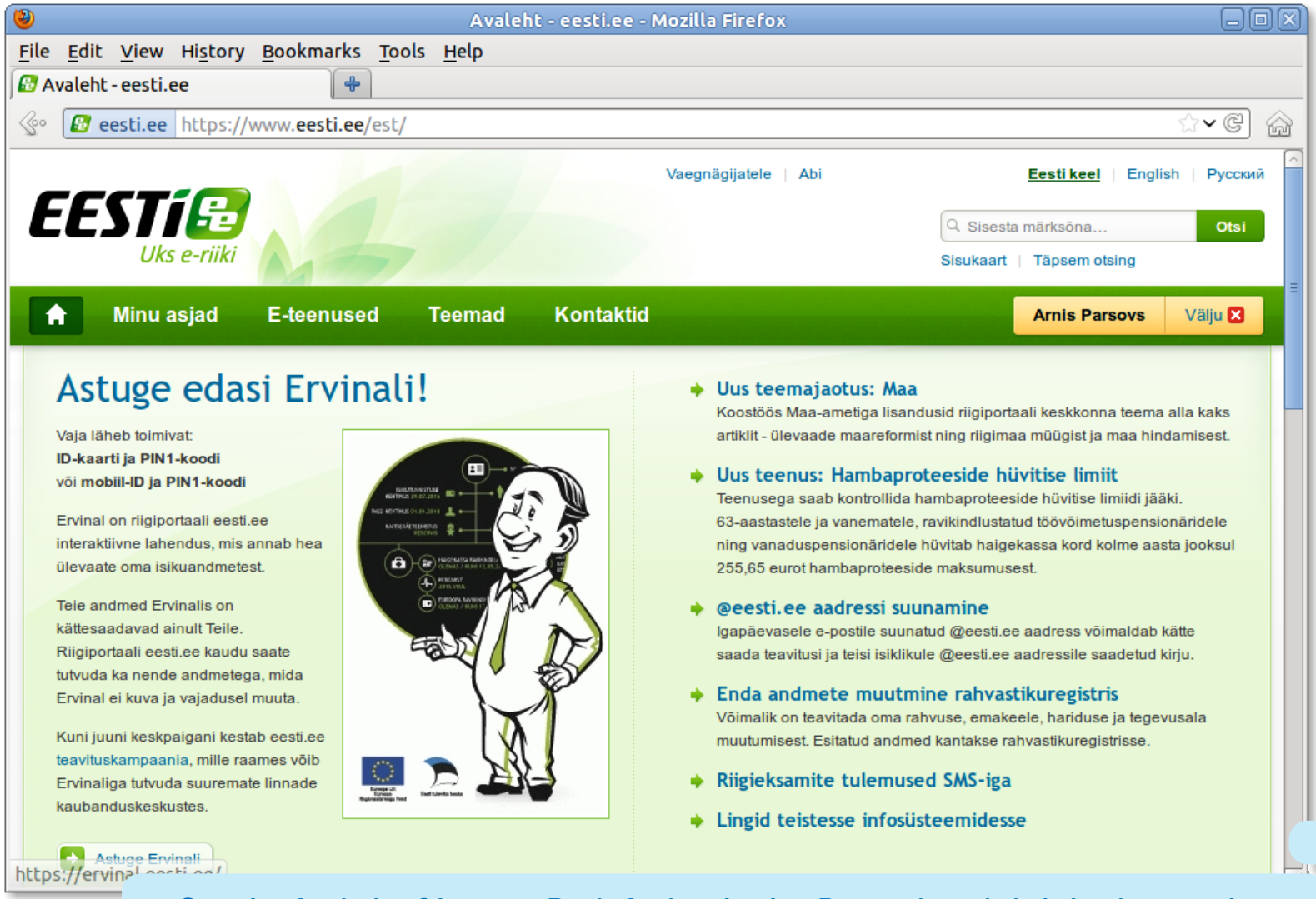
Internet Bank Authentication



Internet Bank Authentication



Internet Bank Authentication



Authentication Token

```
<form action="https://www.eesti.ee/portaal/!pangalink.autenditud"
     method="POST">
     <input type="hidden" name="VK_SERVICE" value="3003">
     <input type="hidden" name="VK_VERSION" value="008">
     <input type="hidden" name="VK_SND_ID" value="EYP">
     <input type="hidden" name="VK_REC_ID" value="XTEE">
     <input type="hidden" name="VK_NONCE"
          value="1339269003a81eebe445c50256b8395ec5057b967f">
     <input type="hidden" name="VK_INFO"
          value="ISIK:38608050014;NIMI:PARSHOVS , ARNIS">
     <input type="hidden" name="VK_MAC"
          value="QV+S/2PcGGycy+0xLjeIHXCS56KxuqCsVTKKI3LG5T3Wo...">
     <input type="hidden" name="VK_CHARSET" value="UTF-8">
     <input type="hidden" name="SubmitButton" value="Enter">
</form>
```

Security Assumption

Authentication to the service provider through an Internet bank is as secure as authentication to the Internet bank

?

Required Security Properties

1. Authenticity and Integrity
2. Confidentiality
3. One-timeness
4. Target-binding
5. Expiration
6. Availability
7. Control and Consent
8. Auditability

Scope - Banks

Estonia:

1. Krediidipank
2. Nordea
3. Sampo
4. SEB
5. Swedbank

Latvia:

1. Citadele
2. DNB
3. Nordea
4. Norvik
5. SEB
6. Swedbank

Scope - Service Providers (Estonia)

1. arved.ee
2. arvekeskus.ee
3. compensalife.ee
4. eesti.ee
5. elion.ee
6. elisa.ee
7. emta.ee
8. emt.ee
9. energia.ee
10. eparkimine.ee
11. e-register.ee
12. ergo.ee
13. e-seif.ee
14. ettevotjaportaal.rik.ee
15. g4s.ee
16. gaas.ee
17. iizi.net
18. kindlustus.ee
19. kinnistusraamat.rik.ee
20. korteriyhistu.net
21. lkf.ee
22. mandatumlife.ee
23. paberivaba.ark.ee
24. parkimine.ee
25. partnercard.net
26. pensionikeskus.ee
27. pilet.ee
28. stat.ee
29. stv.ee
30. tallinnavesi.ee
31. tallinn.ee
32. tele2.ee

Scope - Service Providers (Latvia)

1. dabasgaze.lv
2. eglinfo.lv
3. e-latvenergo.lv
4. epakalpojumi.lv
5. eparaksts.lv
6. eriga.lv
7. if.lv
8. lattelecom.lv
9. latvija.lv
10. luis.lanet.lv
11. lursoft.lv
12. manabalss.lv
13. manslmt.lv
14. parbaudi.lv
15. rekini.lv
16. tele2.lv
17. zemesgramata.lv

Security Issues Found

1. The service providers `eparaksts.lv`, `lattelecom.lv`, `luis.lanet.lv`, `lursoft.lv`, `manabalss.lv` and `parkimine.ee` have flaws in their signature verification implementations: this allows a malicious user to completely bypass the authentication process.

2. Citadele (Latvia), Krediidipank (Estonia), Sampo (Estonia), SEB (Estonia), Swedbank (Estonia) and Swedbank (Latvia) use protocols that have a flaw in their design and therefore allow malicious service providers to use the received authentication tokens to authenticate to other service providers on behalf of the users.

Security Issues Found

3. Almost none of the banks outline sufficient requirements for authentication token verification in their technical specifications. As a result, the majority of the service providers fail to verify whether the token has been issued for the particular service provider, has not been received previously and is not outdated, therefore allowing an attacker to execute successful replay attacks and cross-site replay attacks.

Security Issues Found

- Tokens sent unencrypted over HTTP
- Not using HSM for private key storage
- Weak key sizes (1024-bit RSA)
- No access to audit trails
- Does not ask for consent
- Imprecise system time

Conclusions

1. Internet bank authentication is insecure in practice
2. Banks have to update processes and instructions
3. All service providers have to fix their implementations
4. Legal framework and standardization needed

Thank you!

Questions?