



TTÜ1918

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

The screenshot shows the main page of the EESTI.ee website in a Mozilla Firefox browser. The browser's address bar displays "https://www.eesti.ee/eng". The website header includes the EESTI.ee logo with the tagline "Uks e-riiki" and navigation links for "My Data", "Services", "Topics", and "Contacts". A search bar is located in the top right corner. A "Login" overlay window is positioned in the foreground, featuring several authentication options: "Login with ID-card" (KAART), "Login with mobile-ID" (MOBIL), and "Login via bank". The "Login via bank" section includes buttons for SEB, Swedbank, Sampo Bank, Nordea, and i-pank. The background content includes a "Study in Estonia" section with text and a photo of students in a classroom.

Internet Bank Authentication

SEB Internet Bank / Welcome! - Mozilla Firefox

File Edit View History Bookmarks Tools Help

SEB Internet Bank / Welcome!

AS SEB Pank (EE) https://www.seb.ee/cgi-bin/unet3.sh/ipank.p?sesskey=&act=LOGIN&VK_SERVICE=4002&VK_VERSION=008

SEB Internet bank

Esti keeles [In English](#) [По-Русски](#)

Welcome!

Log in

1 Username 2 Passwords

Please select will you login through the Internet Bank or Internet Bank for Business

- Enter Internet Bank
- Enter Internet Bank for Business

Please enter your username and select the method for authentication

SEB recommends that you be careful and make sure, before using the online bank, that your computer is not contaminated with any viruses.

- The bank asks for ONLY one code from the code card for confirmation.
- If you enter a wrong password or code, you will be asked to re-enter the SAME code.

Please do not enter the codes: finish your session, and inform the bank by e-mail info@seb.ee or by phone 665 5100 if:

- you e...

References

You will have to use either an ID card, PIN calculator or Mobile-ID for making payments in Internet bank which in a day exceed EUR 200. [Read more](#)

How to make Internet banking secure - choose a safe password, don't leave your code card without supervision etc [Read more](#)

In order to verify the authority of the provider of the web page when using the Internet bank, check the address of the bank's server and the security certificate of the server when entering the Internet address. [Read more](#)

Internet Bank Authentication

The screenshot shows the SEB Internet Bank login page. The browser title is "SEB Internet Bank / Welcome! - Mozilla Firefox". The address bar shows "AS SEB Pank (EE) https://www.seb.ee/cgi-bin/unet3.sh/ipank.r". The page features the SEB logo and the text "Internet bank".

Welcome!

Log in

1 Username 2 Passwords

Please enter your password Please enter from the code card code no.

21

SEB recommends that you be careful and make sure, before using the online bank, that your computer is not contaminated with any viruses.

- The bank asks for ONLY one code from the code card for confirmation.
- If you enter a wrong password or code, you will be asked to re-enter the SAME code.

Please do not enter the codes: finish your session, and inform the bank by e-mail info@seb.ee or by phone 665 5100 if:

- you are asked for more than one code simultaneously, or
- if you enter a wrong user name again, you will be asked for another code from your code card.

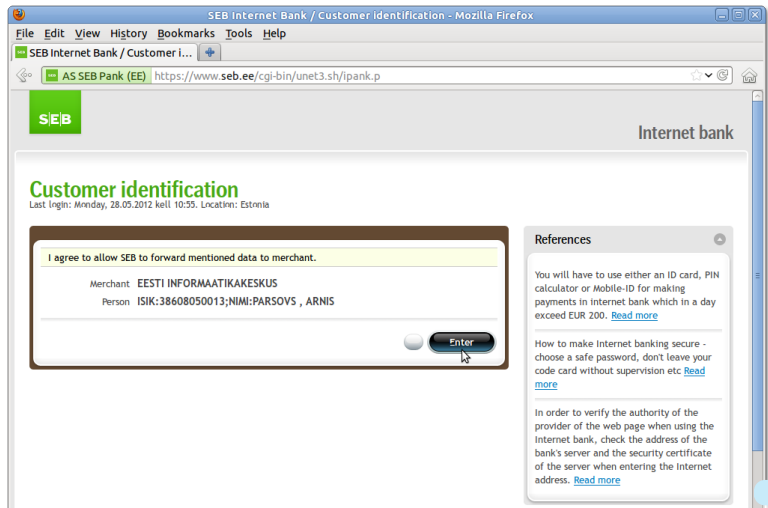
References

You will have to use either an ID card, PIN calculator or Mobile-ID for making payments in internet bank which in a day exceed EUR 200. [Read more](#)

How to make Internet banking secure - choose a safe password, don't leave your code card without supervision etc [Read more](#)

In order to verify the authority of the provider of the web page when using the Internet bank, check the address of the bank's server and the security certificate of the server when entering the Internet address. [Read more](#)

Internet Bank Authentication



The screenshot shows a Mozilla Firefox browser window displaying the SEB Internet Bank Customer Identification page. The browser's address bar shows the URL `https://www.seb.ee/cgi-bin/unet3.sh/ipank.p`. The page features the SEB logo and the text "Internet bank".

The main content area is titled "Customer identification" and includes the text "Last login: Monday, 28.05.2012 kell 10:55. Location: Estonia". Below this is a form with a yellow header that reads "I agree to allow SEB to forward mentioned data to merchant." The form contains the following information:

- Merchant: EESTI INFORMAATIKAKESKUS
- Person: ISIK:38608050013;NIMI:PARSOVS, ARNIS

At the bottom of the form is a radio button and an "Enter" button. To the right of the form is a "References" section with the following text:

References

You will have to use either an ID card, PIN calculator or Mobile-ID for making payments in internet bank which in a day exceed EUR 200. [Read more](#)

How to make internet banking secure - choose a safe password, don't leave your code card without supervision etc [Read more](#)

In order to verify the authority of the provider of the web page when using the Internet bank, check the address of the bank's server and the security certificate of the server when entering the Internet address. [Read more](#)

Internet Bank Authentication

Avaleht - eesti.ee - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Avaleht - eesti.ee

eesti.ee https://www.eesti.ee/est/

Vaegnäijajatele | Abi

Eesti keel | English | Русский

Sisesta märksõna... Otsi

Sisukaart | Täpsem otsing

Minu asjad E-teenused Teemad Kontaktid

Arnis Parsovs Välju

Astuge edasi Ervinali!

Vaja läheb toimivat:
ID-kaarti ja PIN1-koodi
või **mobili-ID ja PIN1-koodi**

Ervinal on riigiportaali eesti.ee interaktiivne lahendus, mis annab hea ülevaate oma isikuandmetest.

Teie andmed Ervinalis on kättesaadavad ainult Teile.

Riigiportaali eesti.ee kaudu saate tutvuda ka nende andmetega, mida Ervinal ei kuva ja vajadusel muuta.

Kuni juuni kesksaigani kestab eesti.ee **teavituskampania**, mille raames võib Ervinaliga tutvuda suuremate linnade kaubanduskeskustes.

- Uus teemajaotus: Maa
Kooostöös Maa-ametiga lisandusid riigiportaali keskkonna teema alla kaks artiklit - ülevaade maareformist ning riigimaa müügist ja maa hindamisest.
- Uus teenus: Hambaproteeside hüvitise limiti
Teenusega saab kontrollida hambaproteeside hüvitise limidi jääki. 63-aastastele ja vanematele, ravikindlustatud töövõimetuspensionäridele ning vanaduspensionäridele hüvitab haigekassa kord kolme aasta jooksul 255,65 eurot hambaproteeside maksumusest.
- @eesti.ee aadressi suunamine
Igapäevasele e-postile suunatud @eesti.ee aadress võimaldab kätte saada teavitusi ja teisi isiklikule @eesti.ee aadressile saadetud kirju.
- Enda andmete muutmise rahvastikuregistris
Võimalik on teavitada oma rahvuse, emakeele, hariduse ja tegevusala muutmises. Esitatud andmed kantakse rahvastikuregistrisse.
- Riigiesamite tulemused SMS-iga
- Lingid teistesse infosüsteemidesse

Astuge Ervinali
https://ervinal.eesti.ee/

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