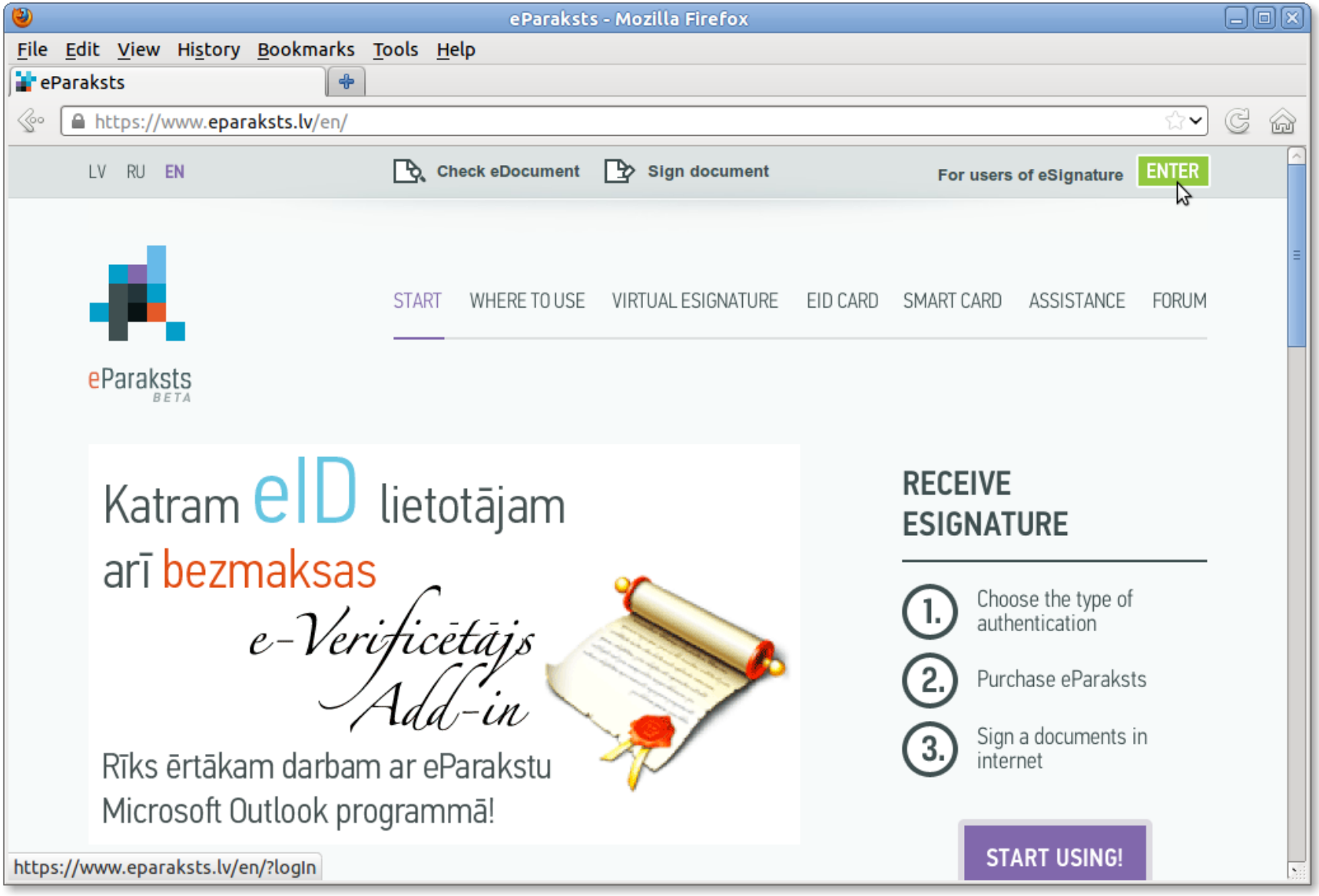
Security of Internet Bank (Bank Link) Authentication

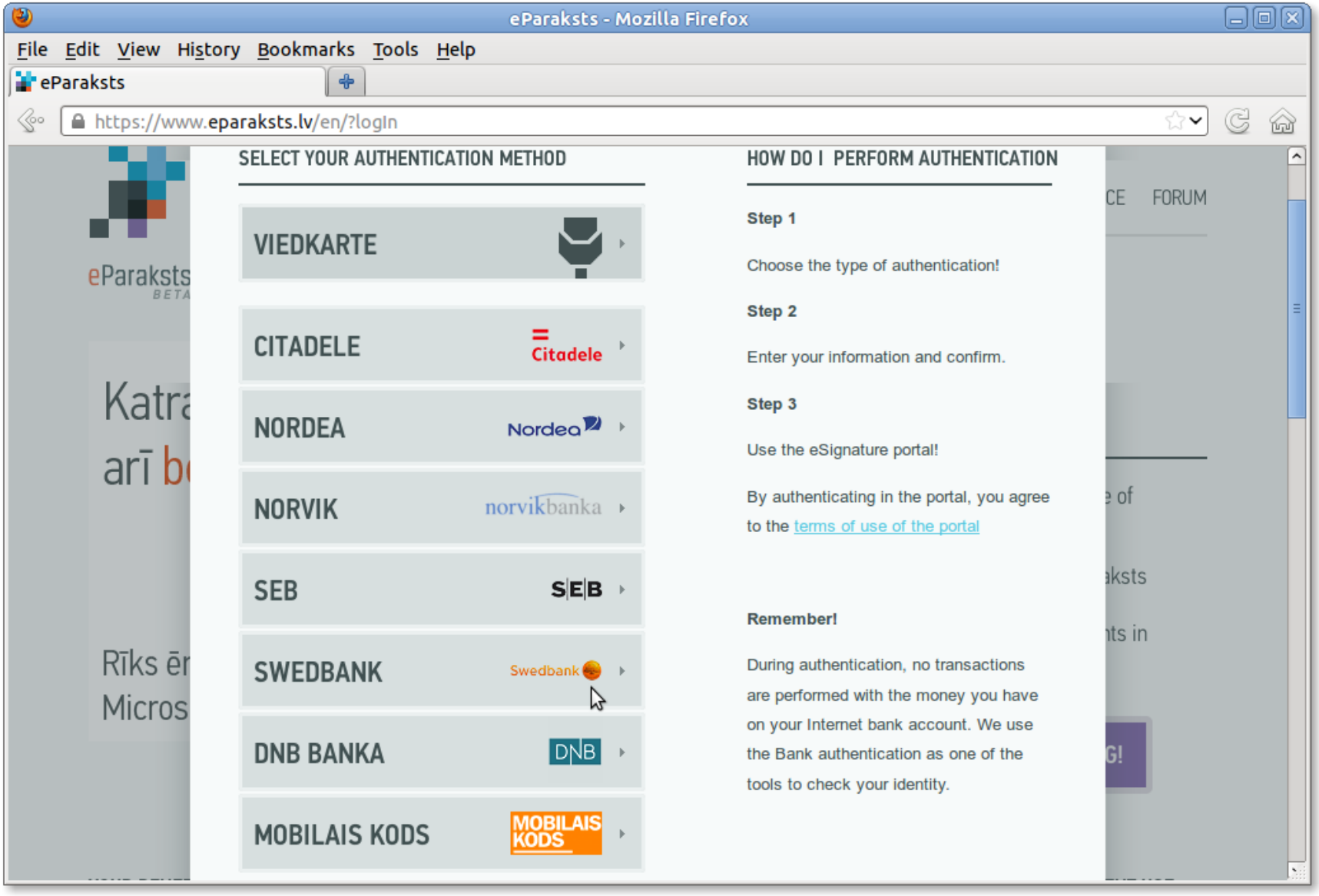
Arnis Paršovs

November 8, 2012

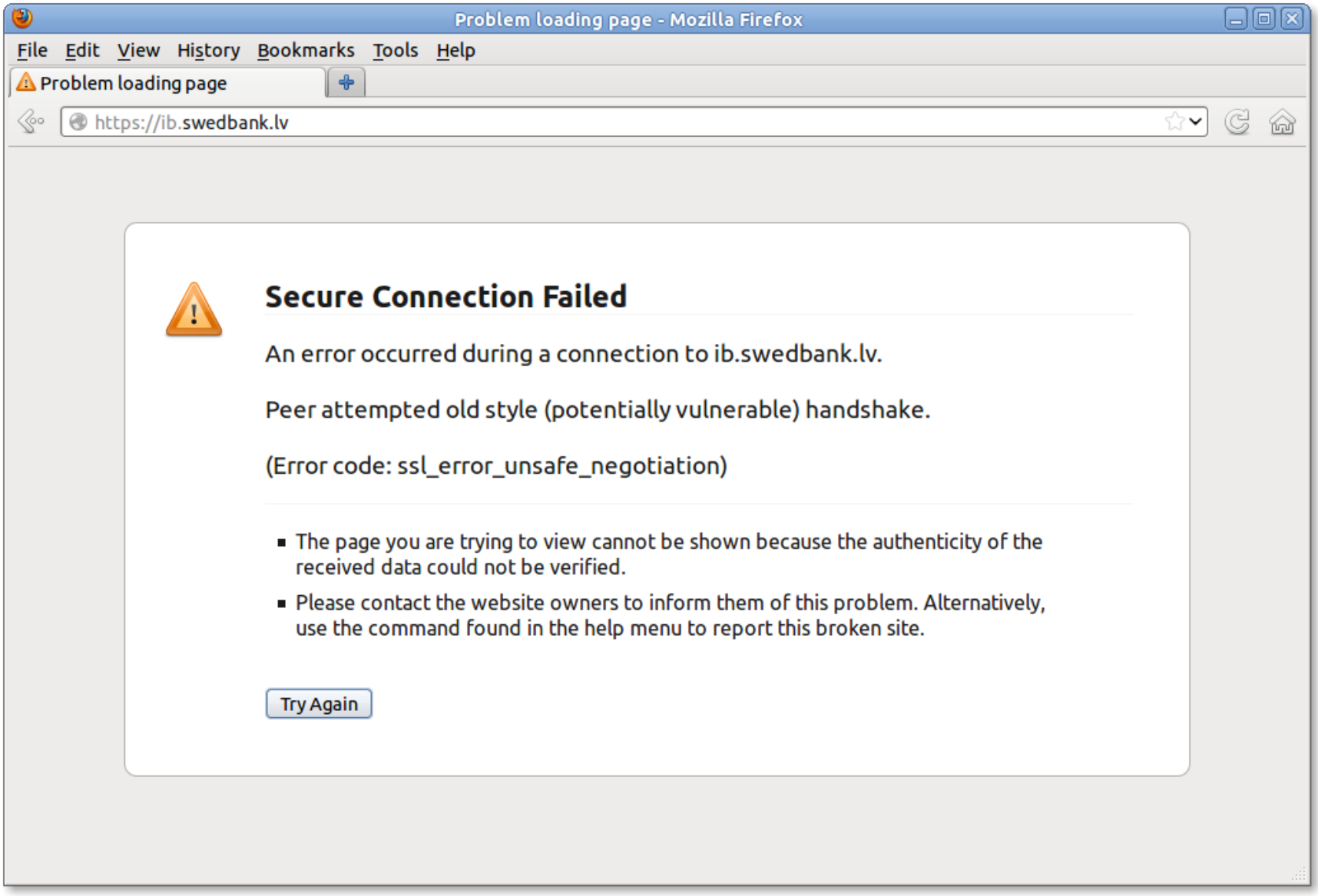
Internet Bank Authentication



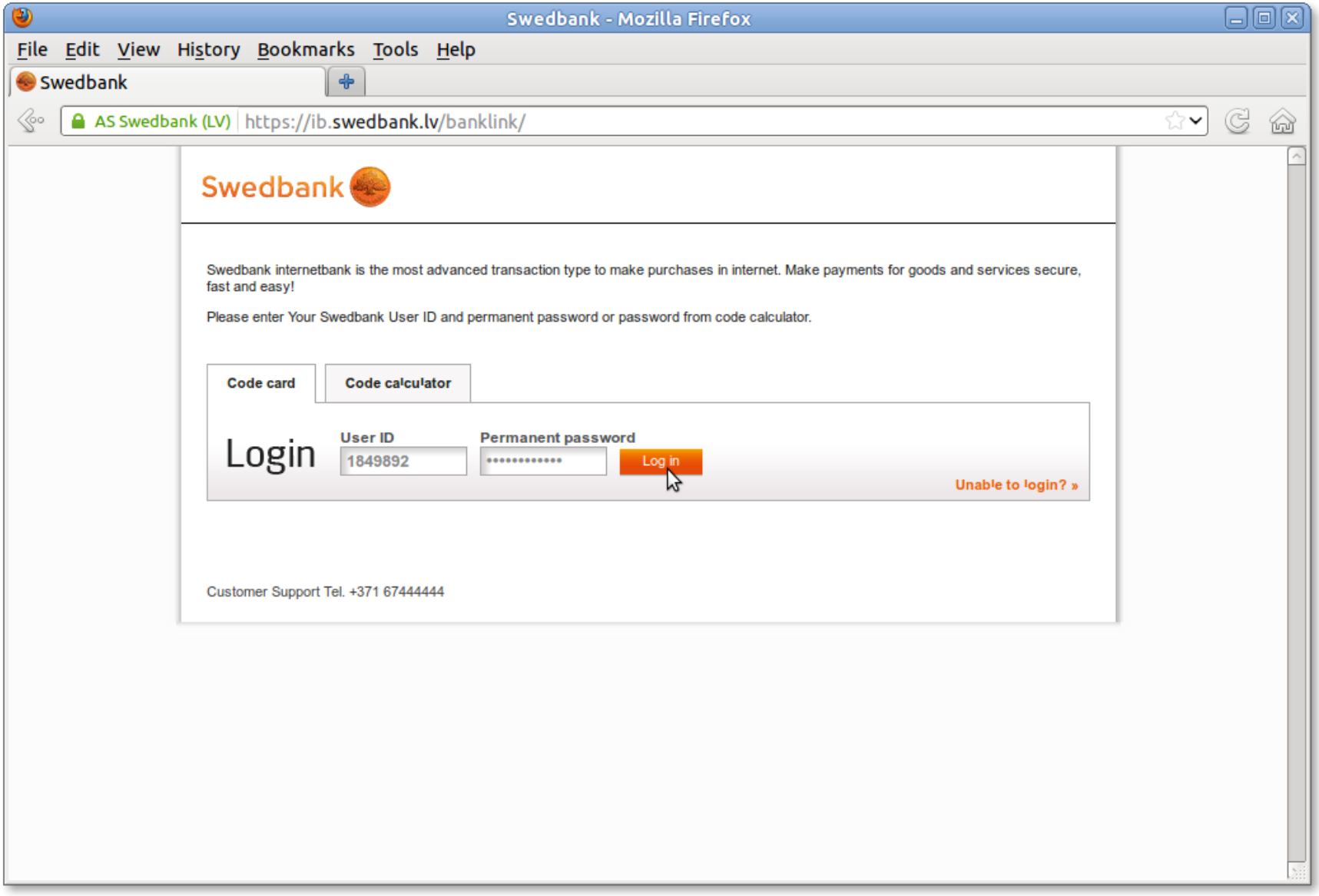
Internet Bank Authentication



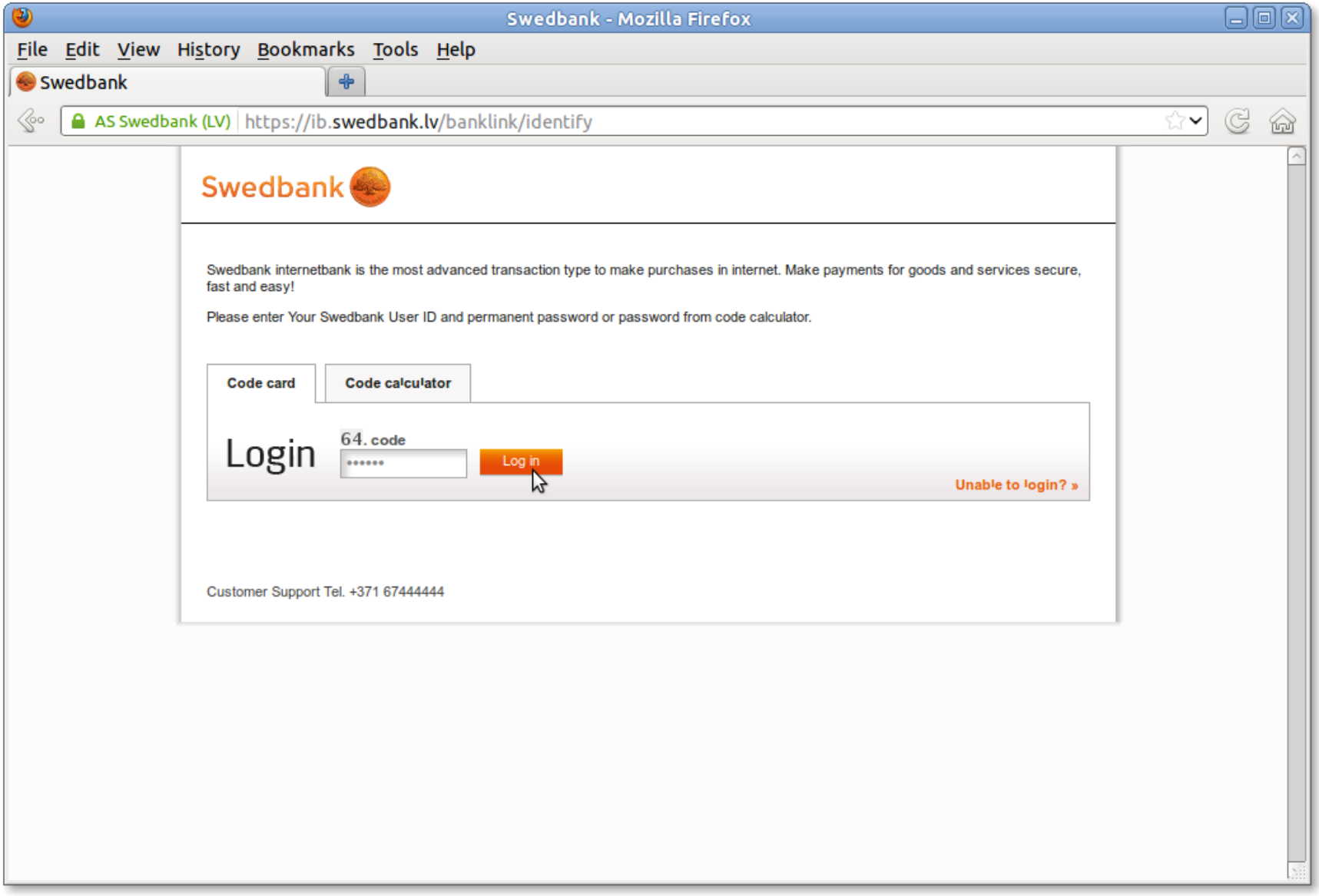
Internet Bank Authentication



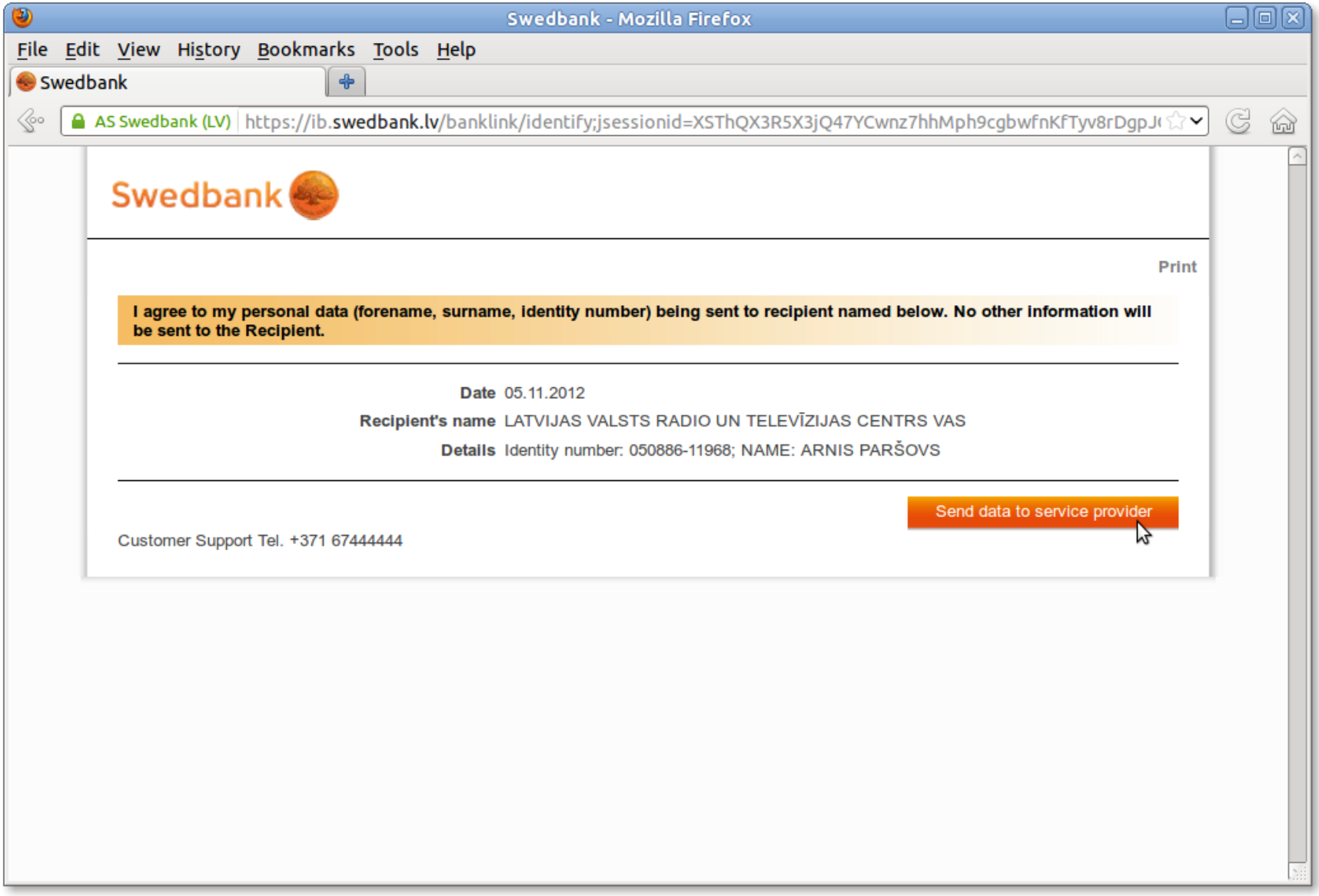
Internet Bank Authentication



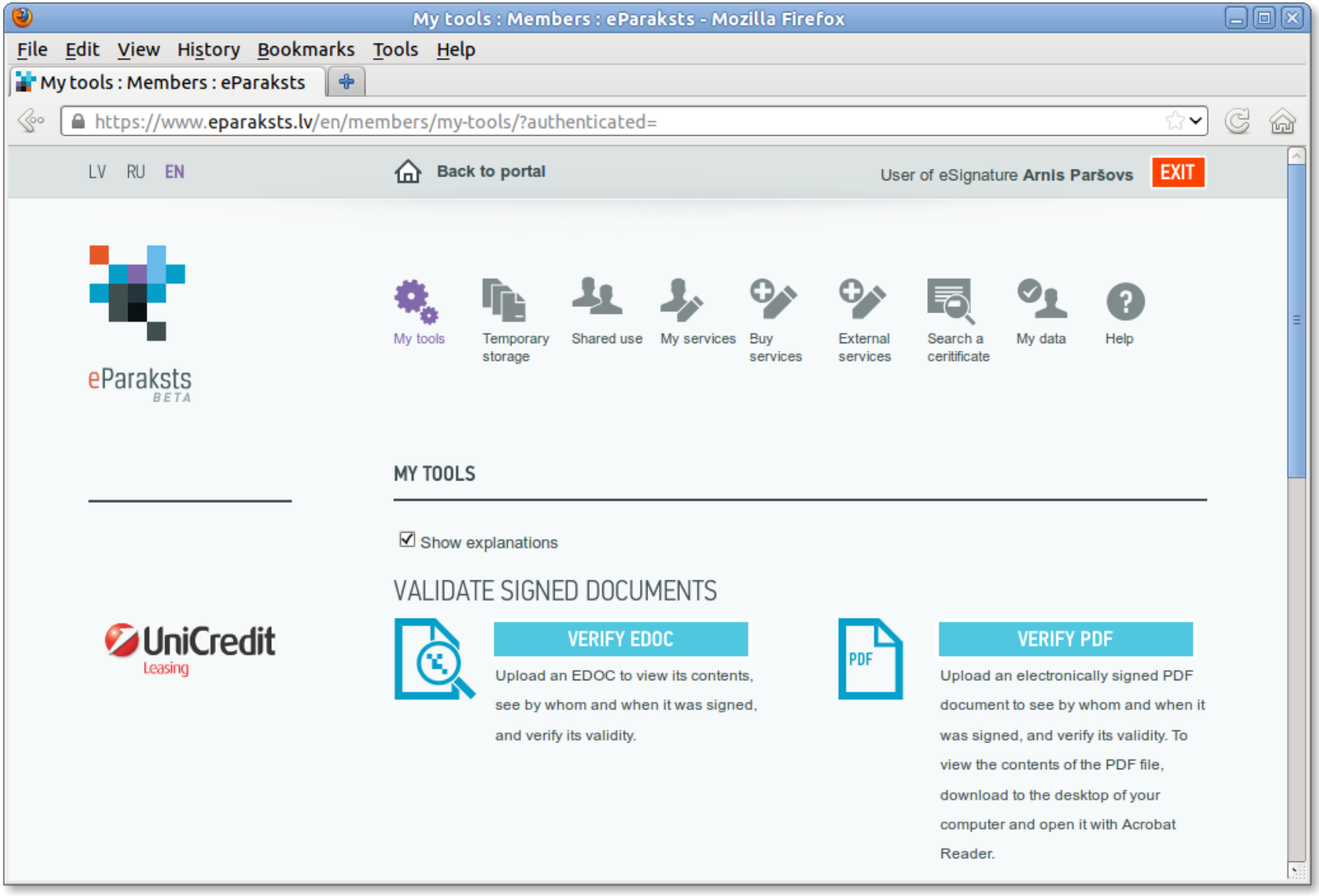
Internet Bank Authentication



Internet Bank Authentication



Internet Bank Authentication



Authentication Token

```
<form action="https://www.eparaksts.lv/services/swedbank/"
     method="POST">
     <input name="VK_SERVICE" type="hidden" value="3003">
     <input name="VK_VERSION" type="hidden" value="008">
     <input name="VK_SND_ID" type="hidden" value="HP">
     <input name="VK_REC_ID" type="hidden" value="EMELV">
     <input name="VK_NONCE" type="hidden"
          value="20121105095916667698826958287245355297845 9">
     <input name="VK_INFO" type="hidden"
          value="ISIK:050886-11998;NIMI:ARNIS PARSHOVS">
     <input name="VK_ENCODING" type="hidden" value="ISO-8859-13">
     <input name="VK_MAC" type="hidden"
          value="tULDMbLpqvWRyAVTRX5mB69urGSKjFD5g/auRfynIA2WWu...">
</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

Authenticity and Integrity

Attacks:

- Impersonation attacks

Measures:

- Digital signatures
  - Key management (HSM)
  - Key sizes and algorithms

Confidentiality

Attacks:

- Unauthorized access

Measures:

- HTTPS between: bank $\Longleftrightarrow$ client $\Longleftrightarrow$ service provider
- HTTP POST request method
- HTTP "Cache-Control" header

One-timeness

Principle of “one code - one authentication”

Attacks:

- Replay attacks

Measures:

- Service provider has to track already used tokens

Target-binding

Attacks:

- Cross-site replay attacks

Measures:

- Service provider specific signing key
- Service provider identifier in authentication token
    - Has to be checked by the service provider

Expiration

Attacks:

- Replay attacks

Measures:

- Timestamp field in authentication token
  - Has to be enforced by the service provider

Availability

Attacks:

- Denial-of-service attacks

Measures:

- Limit public key operations
- Verification order to fail fast

Control and Consent

European Data Protection Directive

Article 7

Member States shall provide that personal data may be processed only if:
(a) the data subject has **unambiguously given his consent**;

Attacks:

- Phishing attacks

Measures:

- User's consent has to be asked before forwarding token
  - Business relationship not a personal data?

Auditability

Prevention Eventually Fails

Attacks:

- Stealthy attacks

Measures:

- Detect, log and alert on attacking attempts
- Show authentication audit trail to authenticated users
- Regularly cross-check authentication audit trails

Protocols

- High diversity
- Single message protocol (bank $\Rightarrow$ provider)
- Request/response protocol (provider $\Rightarrow$ bank $\Rightarrow$ provider)

iPizza (Krediidipank, Sampo, SEB, Swedbank)

No	Field name	Value/Format	Description
1	VK_SERVICE	3002	Message ID
2	VK_VERSION	008	Signature method
3	VK_USER		Personal code of client
4	VK_DATE	DD.MM.YYYY	Date when message generated
5	VK_TIME	HH:MM:SS	Time when message generated
6	VK_SND_ID		ID of sender (bank)
7	VK_INFO		Personal data of client
–	VK_MAC		Digital signature of previous fields

Fields of the timestamped authentication response message 3002.

$$Base64_{enc}(RSA_{sign}(SHA1(\text{“004”}||\text{“3004”}||\text{“003”}||\text{“008”}||\text{“002”}||\text{“}HP\text{”}||...$$

- No field specifying intended recepient of the token
- Timestamp in timezone dependent machine unfriendly form
- Lacks unique ID of the token

iPizza (Krediidipank, Sampo, SEB, Swedbank)

No	Field name	Value/Format	Description
1	VK_SERVICE	4002	Message ID
2	VK_VERSION	008	Signature method
3	VK_SND_ID		ID of sender (service provider)
4	VK_REC_ID		ID of receiver (bank)
5	VK_NONCE		Random nonce
6	VK_RETURN	https://...	URL where to send response
–	VK_MAC		Digital signature of previous fields

No	Field name	Value/Format	Description
1	VK_SERVICE	3003	Message ID
2	VK_VERSION	008	Signature method
3	VK_SND_ID		ID of sender (bank)
4	VK_REC_ID		ID of receiver (service provider)
5	VK_NONCE		VK_NONCE from initial request 4002
6	VK_INFO		Personal data of client
–	VK_MAC		Digital signature of previous fields

- Contains recepient field, but no timestamp
- Used only as request/response protocol (not used much)
- Nonce checking is not sufficient to prevent cross-site replay

Swedbank (Latvia) PHP sample code

http://www.swedbank.lv/lib/PHP_piemeri.rar

```
$ cat -n PHP\ piemeri/example_swedbank_return.php
     ..
    27  function _verify($mac, $signature) {
    28      $cert = file_get_contents(KEY_LOCATION.'/swedbank.pem');
    29      $key = openssl_get_publickey($cert);
    30      $ok = openssl_verify($mac, $signature, $key);
    31
    32      openssl_free_key($key);
    33      return $ok;
    34  }
     ..
    74      $signature_ok = _verify($mac, base64_decode($_POST['VK_MAC']));
     ..
    80  if($signature_ok == false || $signature_ok == 0) {
    81      echo '<!--signature is bad-->';
    82      exit;
    83  }
     ..
```

openssl_verify — Verify signature

Return Values

Returns 1 if the signature is correct, 0 if it is incorrect, and -1 on error.

Nordea

- Based on the TUPAS standard of the Federation of Finnish Financial Services
- Uses MAC instead of digital signatures (so what?)
- Key is 32 alphanumeric characters long
- Uses concatenated hash $H(\mathit{message} \parallel \mathit{key})$ instead of HMAC
- Hash algorithm is MD5 (supports SHA1)
- TUPAS updated to force SHA256 from 2012.01.01

Citadele (Latvia)

```
<Header>
    <Timestamp>20120502155029000</Timestamp>
    <From>10000</From>
    <Request>AUTHRESP</Request>
    <RequestUID>68a434e6-1763-7b3c-7b64-d0f327738334</RequestUID>
    <Version>1.0</Version>
    <Language>LV</Language>
    <PersonCode>05047711038</PersonCode>
    <Person>John Smith</Person>
    <SignatureData>
        <SignatureValue>GFzAo2U5fY...</SignatureValue>
        <KeyInfo>
            <X509Certificate>MIIFSTCCAzGgAwIBA...</X509Certificate>
        </KeyInfo>
    </SignatureData>
</Header>
```

- Uses XML-Signature
- Uses the same 4096-bit RSA signing key
- No recepient field
- What is the certificate for?

Citadele (Latvia)

6.1.4. Having received a request in Citadele Online Banking or in the External system, the following verifications should be performed:

- XML signature verification;
- If the difference between the value indicated in the “Timestamp” element and current time exceeds 15 minutes, the request is not processed;
- If during last 15 minutes a request with the value indicated in the “RequestUID” element had been already registered, the request is not processed.

Service Provider	Protocol	Target-binding	One-timeness	Expiration
e-latvenergo.lv	AUTHRESP	–	+	15min
e-latvenergo.lv	ESERVICEREQ	–	+	15min
epakalpojumi.lv	AUTHRESP	–	+	5min
epakalpojumi.lv	ESERVICEREQ	–	–	10min
eparaksts.lv*	AUTHRESP	–	–	–
eriga.lv	AUTHRESP	–	+	5min
eriga.lv	ESERVICEREQ	–	–	10min
if.lv	AUTHRESP	–	–	–
lattelecom.lv	AUTHRESP	–	–	–
latvija.lv	AUTHRESP	–	+	25sec
latvija.lv	ESERVICEREQ	–	–	25sec
luis.lanet.lv*	AUTHRESP	–	–	–
lursoft.lv	AUTHRESP	–	–	–
manabalss.lv*	AUTHRESP	–	–	–
parbaudi.lv	AUTHRESP	–	–	–

Citadele (Latvia) authentication as implemented by the service providers.

Norvik (Latvia) and lursoft.lv

```
https://www.lursoft.lv/lapsaext?act=NORVIK&act=NORVIK
&name=PAR%C5%A0OVS+ARNIS&pcode=050886-11998&sign=
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

PAR%C5%A0OVS+ARNIS050886-11968
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.5 (GNU/Linux)

iQEVAwUBT6GBOzOqGTzcbxslAQKeDQf%2BPqnk1kkPTwe0P5QjpkyxcLAhdDVUOrgz%0D%0A4ql
f7iQIRtTFN%0D%0AUu1uQUditIZbg0kT2v61rKfNUe1iVQ0k0Hqw1OH8Mef48hNkOrQErVpCvVk
0Umj9UEQiBa%2BRgNGYWa5sO1mrEv6M6%2BTGOGmUhdNydDg7uG2y%0D%0Ar5zEwkD5EquE675j
..
-----END PGP SIGNATURE-----
```

- PGP cleartext signed message
- “name” and “pcode” not compared with PGP message
- Detached PGP signature would have helped

Key Management

```
Version: 3 (0x2)
Serial Number: 10 (0xa)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=EE, ST=Estonia, L=Tallinn, O=Hansabank, OU=0025200, CN=Hansabank Server Certif
Validity
    Not Before: Mar 17 14:08:07 1999 GMT
    Not After : Jun  3 14:08:07 2007 GMT
Subject: C=EE, ST=Estonia, O=Hansabank, CN=Virtual POS
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
        Modulus (1024 bit):
        Exponent: 65537 (0x10001)
X509v3 extensions:
    Netscape Cert Type:
        Object Signing
```

- Weak key sizes (1024-bit RSA) for 7 banks
- Not using HSM for private key storage
  - HSM confirmed for Sampo (Estonia), SEB (Estonia, Latvia)

Regulation and supervision

FINANŠU UN KAPITĀLA TIRGUS KOMISIJA

Rīgā **DATUMU SKATĪT DOKUMENTA PARAKSTA LAIKA ZĪMOGĀ**
Nr. **REĢISTRĀCIJAS NUMURU SKATĪT DOKUMENTĀ IEKĻAUTO FAILU NOSAUKUMĀ**

Arnim Paršovam
E-pasts: arnis@parsovs.lv

Par banku trešajām pusēm sniegtiem autentifikācijas pakalpojumiem

God. A. Paršova kungs

Finanšu un kapitāla tirgus komisija (tālāk tekstā – Komisija) ir saņēmusi Jūsu 07.05.2012. vēstuli ar lūgumu sniegt skaidrojumu par to, vai banku trešajām pusēm sniegtie autentifikācijas pakalpojumi tiek regulēti Latvijas normatīvajos aktos.

Informējam, ka spēkā esošie tiesību akti šobrīd tieši nenosaka autentificēšanās prasības valsts informācijas sistēmās un iestāžu klientu portālos, bet nepieciešamo tiesisko regulējumu ir paredzēts izstrādāt. Ar Ministru kabineta 30.03.2011. rīkojumu Nr. 140 apstiprinātā koncepcija par vienota autentifikācijas mehānisma ieviešanas iespējām valsts informācijas sistēmās paredz, ka Vides aizsardzības un reģionālās attīstības ministrija sadarbībā ar Satiksmes ministriju un Iekšlietu ministriju izstrādās tiesību aktus, kas turpmāk noteiks vienotu tiesisko regulējumu personas autentifikācijai.

Savukārt banku informācijas sistēmu drošības prasības saistībā ar banku sniegtajiem pakalpojumiem nosaka Komisijas 08.10.2010. normatīvie noteikumi Nr. 278 "Finanšu un kapitāla tirgus dalībnieku informācijas sistēmu drošības normatīvie noteikumi" (sk. www.fktk.lv/texts_files/IS%20drosibas%20noteikumi.pdf). Minētie noteikumi konkrētas tehniskās prasības nenosaka, tomēr izmantotie tehnoloģiskie risinājumi tiek vērtēti uzraudzības procesā.

Ar cieņu

ŠIS DOKUMENTS IR ELEKTRONISKI PARAKSTĪTS AR DROŠU ELEKTRONISKO PARAKSTU UN SATUR LAIKA ZĪMOGU

Jānis Brazovskis
Finanšu un kapitāla tirgus komisijas
priekšsēdētāja vietnieks

A. Šinka
6777 4891
arnis.sinka@fktk.lv

KUNGU IELĀ 1 • LV-1050 RĪGĀ • TĀLRUNIS +371 6777 4800 • FAKSS +371 6722 5755

Status quo

- Estonia:
  - 60% bank authentication
  - 37% ID-card authentication
  - 3% Mobile-ID
- Latvia:
  - 99.9..% bank authentication?
    - ID-cards have no use cases
    - Banks are the real Certification Services Providers
- Estonian Banking Association working on new common protocol update

Principle of least privilege

The principle that a security architecture should be designed so that each system entity is granted the **minimum** system resources and **authorizations that the entity needs** to do its work.

`http://www.ietf.org/rfc/rfc2828.txt`

- Bank credentials for online banking only
- No choice to opt out
- No security awareness

Weakest link

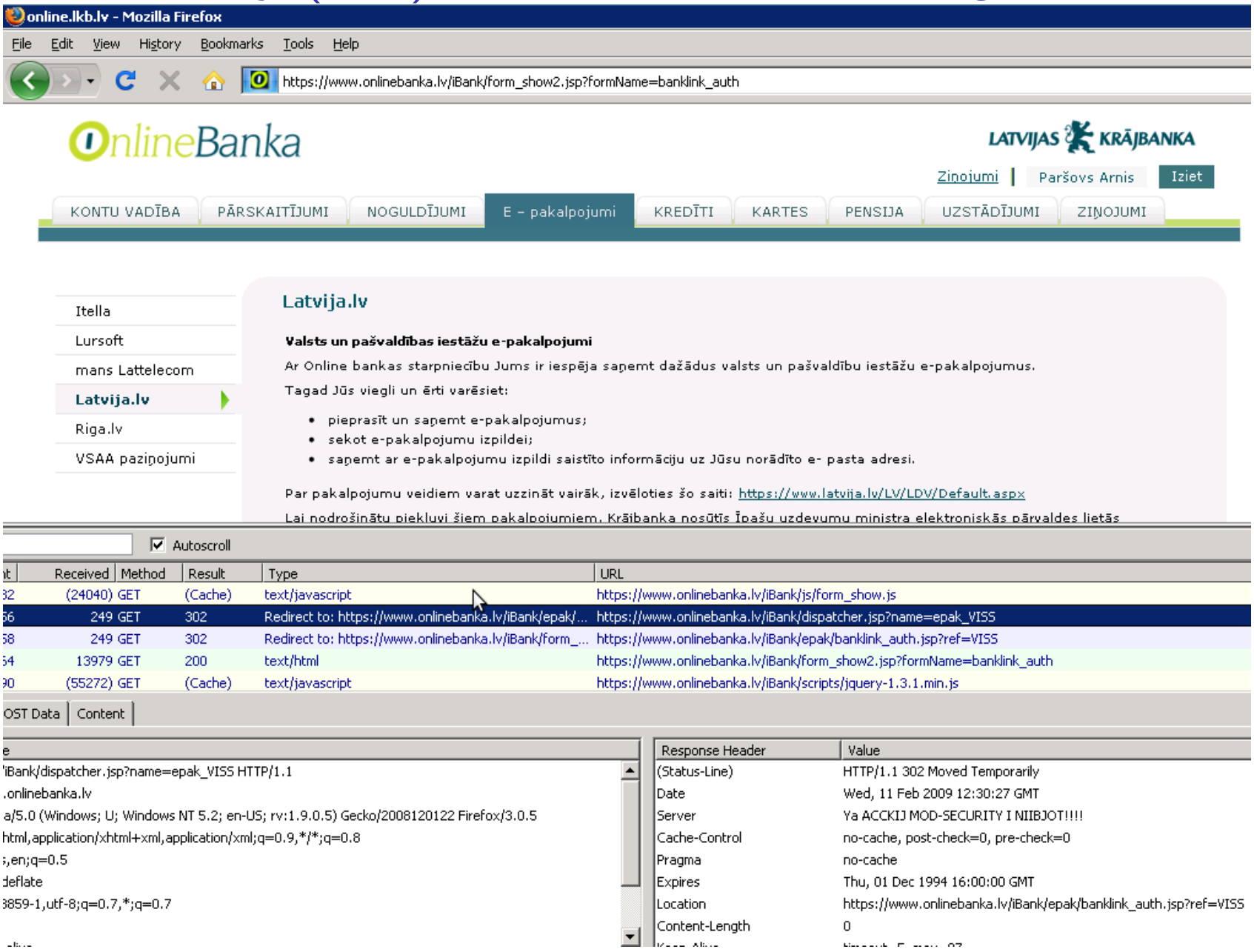
- The chain of trusted authorities
- Trust = being vulnerable to
- The chain of authorities you are vulnerable to
- Enlargement of the attack surface

Security (and) Culture in the Banking Sector

Response Header	Value
(Status-Line)	HTTP/1.1 302 Moved Temporarily
Date	Wed, 11 Feb 2009 12:30:27 GMT
Server	Ya ACCKIJ MOD-SECURITY I NIIBJOT!!!!
Cache-Control	no-cache, post-check=0, pre-check=0
Pragma	no-cache
Expires	Thu, 01 Dec 1994 16:00:00 GMT
Location	https://[redacted]ak/banklink_auth.jsp?ref=VISS
Content-Length	0

Can you guess the bank?

Security (and) Culture in the Banking Sector



Food for thought

- Who is liable?
- Are audits and pentests useless?
- Am I the only one who noticed the flaws?
- What about payment protocols?
- Internet bank authentication in other countries?

Thank you!

Questions, comments, opinions?

`http://math.ut.ee/~arnis/bankauth/`