Estonian Electronic Identity Card: Security Flaws in Key Management

Arnis Parsovs[1,2]

[1]Software Technology and Applications Competence Center (STACC)

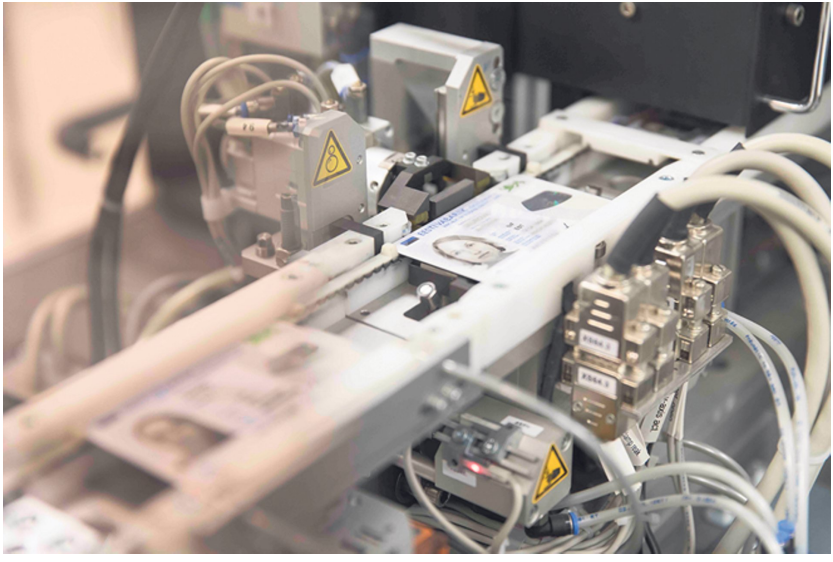
[2]University of Tartu

August 14, 2020

Estonian Electronic Identity Card (ID card)

- Nationwide PKI since 2002
- Contains two asymmetric keys with the corresponding X.509 certificates:
  - Authentication key:
    - TLS client authentication
    - Document decryption
  - Digital signature key:
    - Legally binding digital signatures (EU eIDAS regulation)

ID card manufacturing



ID card personalization line of Gemalto (formerly Trüb Baltic)

Recall of ID cards issued in 2011

September 2012:

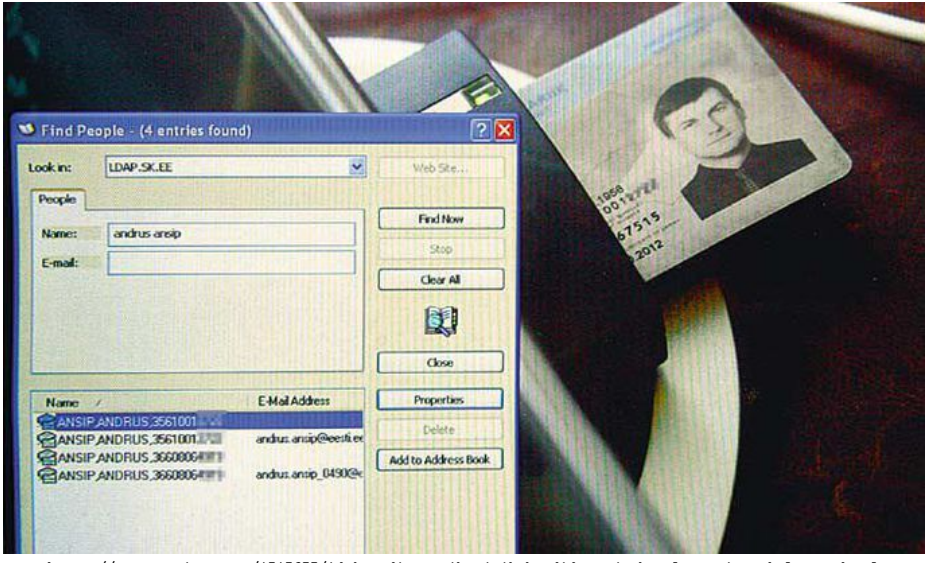
> "During a routine ID card analysis process we discovered that one of the electronic security measures of the ID card needs to be renewed. ID card users have no reason to be concerned. The **card is secure** and all transactions made with the card are fully reliable."

> "In July 2013 the **certificates of the non-renewed cards will be suspended** and the cards cannot be used electronically any more."

`http://www.id.ee/?id=35927`

- Renewal – reinstalling the JavaCard applet in PPA customer service points
- To this day the authorities have not disclosed the details of the flaw

ID card certificate repository



https://www.postimees.ee/1515655/id-kaardi-omanike-isikukoodid-on-jatkuvalt-netis-vabalt-saadaval

Certificate pairs with duplicate RSA public keys

No	Time of cert issuance	Type	Cardholder	Issuance	Expiry date	Revoked	Warranty
1	2012-11-06 15:35:09	sign	Ülle	PPA renewal	2016-07-07	2016-06-27	2014-10-09
	2012-11-06 15:35:46	auth	Toivo	PPA renewal	2016-07-04	2014-11-21	2014-10-09
2	2013-02-06 15:35:54	auth	Phillip	PPA renewal	2016-11-14	2015-05-04	2015-01-06
	2013-02-06 15:35:56	sign					
3	2013-02-07 12:18:34	auth	Sandra	PPA renewal	2016-01-02	expired	not issued
	2013-02-07 12:18:37	sign					
4	2013-02-19 09:09:58	auth	Nadiia	PPA renewal	2016-11-24	2016-11-08	2014-12-22
	2013-02-19 09:10:08	sign					
5	2013-02-25 09:33:17	auth	Moonika	PPA renewal	2016-08-22	2014-12-30	2014-12-22
	2013-02-25 09:33:29	sign					
6	2013-03-04 11:36:08	sign	Richard	PPA renewal	2016-11-30	2014-10-13	2014-10-09
	2013-03-04 11:36:38	auth	Anu	PPA renewal	2016-08-12	2014-10-23	2014-10-09
7	2013-03-30 13:40:38	auth	Leili	initial	2018-03-26	2015-05-14	2014-12-22
	2013-03-30 13:40:40	sign					
8	2013-03-30 13:42:03	auth	Jaan	initial	2018-03-26	2014-12-30	2014-12-22
	2013-03-30 13:42:05	sign					
9	2013-04-15 09:16:11	auth	Liis	PPA renewal	2016-05-06	expired	2014-12-22
	2013-04-15 09:16:28	sign					
10	2014-10-08 12:01:16	auth	Siim	initial	2019-10-07	2017-10-03	not issued
	2014-10-08 12:04:31	sign					

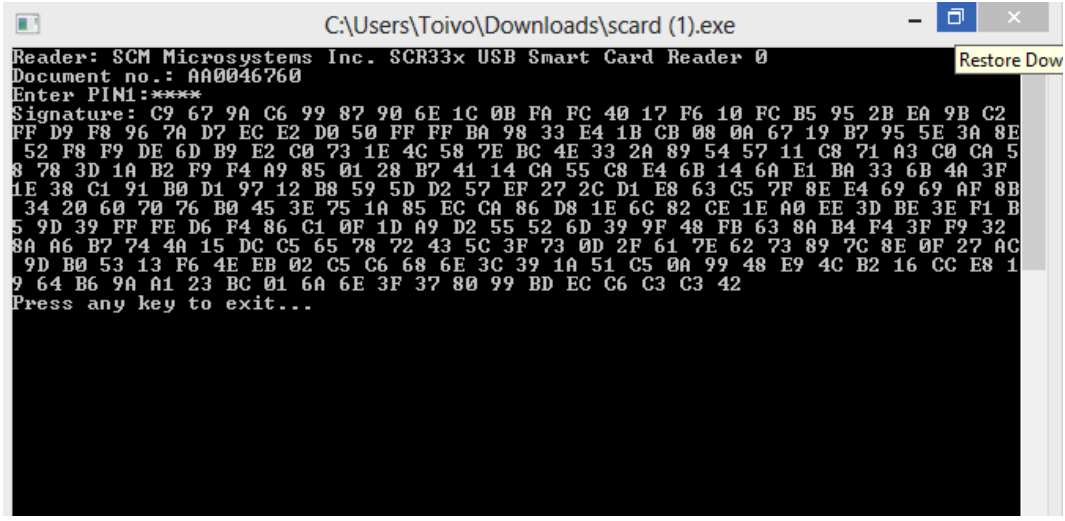
Duplicate keys – Toivo

```
Serial Number: 31:a4:3f:20:73:03:4b:cc:50:99:12:32:13:e4:b0:e4
Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=EE, O=AS Sertifitseerimiskeskus, CN=ESTEID-SK 2011/emailAddress=pki@sk.ee
    Validity
        Not Before: Nov  6 13:35:46 2012 GMT
        Not After : Jul  3 21:00:00 2016 GMT
    Subject: C=EE, O=ESTEID, OU=authentication,    CN=...,TOIVO,...
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                    00:d4:05:92:2f:ef:38:1a:26:96:9e:cd:5a:53:88:e5:a2:77:72:3e:
                    60:a7:d0:ff:be:7c:90:60:82:c3:47:a3:7c:06:f1:6c:fe:b4:18:8c:
                    53:4a:50:b1:0b:21:d2:fd:39:9b:39:28:b1:2d:a2:7b:15:eb:b2:aa:
                    27:00:46:ff:ad:53:2f:f5:74:af:1d:d6:87:e7:5d:15:16:53:65:03:
                    3d:b5:9f:1f:bf:cb:2e:6e:85:2b:23:8e:00:30:55:60:2e:c3:62:fc:
                    50:cc:c0:9c:95:0e:f2:8a:1d:04:2a:8d:31:3e:cb:b3:e4:59:3f:4f:
                    32:70:d8:ef:37:a0:52:d8:b5:5c:49:3d:9d:03:35:70:e7:d7:78:55:
                    9b:90:49:55:98:2c:ee:e9:a7:09:51:74:e0:5c:82:2d:ad:ac:84:c1:
                    b1:b9:37:9e:08:92:2a:dc:52:50:84:16:20:fb:04:3b:b3:c6:64:56:
                    50:da:04:81:83:fd:b8:d1:f4:6b:53:bc:c2:84:72:06:37:2d:b0:e2:
                    f5:60:d7:75:c9:f4:87:d6:56:6d:6b:98:f9:c5:a0:2c:25:55:ec:6f:
                    1f:97:8c:3a:89:9e:54:9c:49:da:50:e0:d7:13:15:5c:9f:b2:ae:cd:
                    74:27:d7:a5:48:5f:cb:57:8d:ad:b5:6a:fb:65:77:3a:7d
            Exponent: 65537 (0x10001)
```

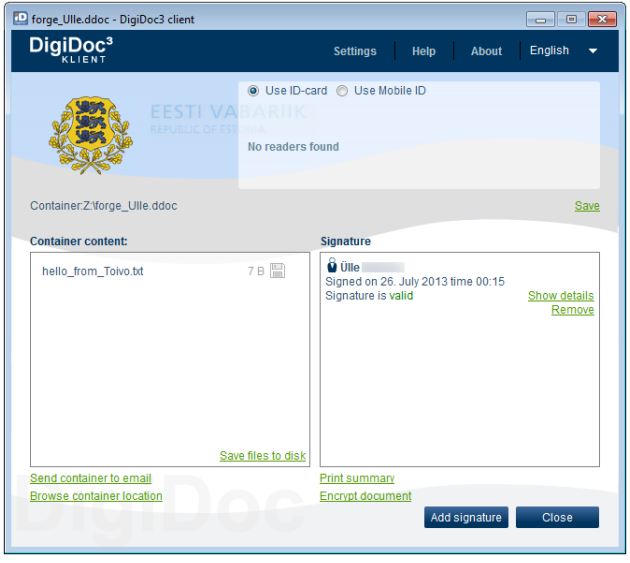
Duplicate keys – Ulle

```
Serial Number: 31:19:01:da:3e:91:9c:c9:50:99:12:0d:0d:6f:d0:f6
Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=EE, O=AS Sertifitseerimiskeskus, CN=ESTEID-SK 2011/emailAddress=pki@sk.ee
    Validity
        Not Before: Nov  6 13:35:09 2012 GMT
        Not After : Jul  7 20:59:59 2016 GMT
    Subject: C=EE, O=ESTEID, OU=digital signature, CN=...,ULLE,...
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                    00:d4:05:92:2f:ef:38:1a:26:96:9e:cd:5a:53:88:e5:a2:77:72:3e:
                    60:a7:d0:ff:be:7c:90:60:82:c3:47:a3:7c:06:f1:6c:fe:b4:18:8c:
                    53:4a:50:b1:0b:21:d2:fd:39:9b:39:28:b1:2d:a2:7b:15:eb:b2:aa:
                    27:00:46:ff:ad:53:2f:f5:74:af:1d:d6:87:e7:5d:15:16:53:65:03:
                    3d:b5:9f:1f:bf:cb:2e:6e:85:2b:23:8e:00:30:55:60:2e:c3:62:fc:
                    50:cc:c0:9c:95:0e:f2:8a:1d:04:2a:8d:31:3e:cb:b3:e4:59:3f:4f:
                    32:70:d8:ef:37:a0:52:d8:b5:5c:49:3d:9d:03:35:70:e7:d7:78:55:
                    9b:90:49:55:98:2c:ee:e9:a7:09:51:74:e0:5c:82:2d:ad:ac:84:c1:
                    b1:b9:37:9e:08:92:2a:dc:52:50:84:16:20:fb:04:3b:b3:c6:64:56:
                    50:da:04:81:83:fd:b8:d1:f4:6b:53:bc:c2:84:72:06:37:2d:b0:e2:
                    f5:60:d7:75:c9:f4:87:d6:56:6d:6b:98:f9:c5:a0:2c:25:55:ec:6f:
                    1f:97:8c:3a:89:9e:54:9c:49:da:50:e0:d7:13:15:5c:9f:b2:ae:cd:
                    74:27:d7:a5:48:5f:cb:57:8d:ad:b5:6a:fb:65:77:3a:7d
            Exponent: 65537 (0x10001)
```

Duplicate keys – signature forgery



Duplicate keys – signature forgery



Incident response

10. oktoober 2014, 13:09 Helen Koltšanov <Helen.Koltsanov@politsei.ee> Kirjutas:

> Lugupeetud Toivo [redacted]
>
> Teavitame, et Teie ID-kaardile 06.11.2012 tehtud uuendamine on kahjuks ebaõnnestunud ja seda kaarti ei saa elektrooniliselt kasutada. Tootsime Teile garantii korras uue ID-kaardi (vana kaardi kehtivusaja lõpuni), mille saate kätte Pärnu teeninduses. Küsimuste korral saate pöörduda e-posti aadressil ppa@politsei.ee või tel 612 3000.
>
> Teeninduse kontaktid ja lahtiolekuajad leiate meie kodulehe aadressilt http://www.politsei.ee/et/kontakt/teeninduspunktid/kmb/.
>
> Austusega
>
> Helen Koltšanov
> peaekspert
> identiteedi ja staatuse büroo

Incident response

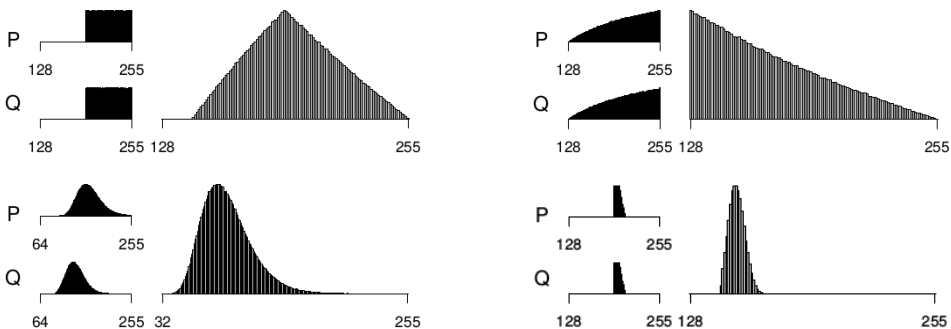
The Million-Key Question – Investigating the Origins of RSA Public Keys

https://crocs.fi.muni.cz/public/papers/usenix2016

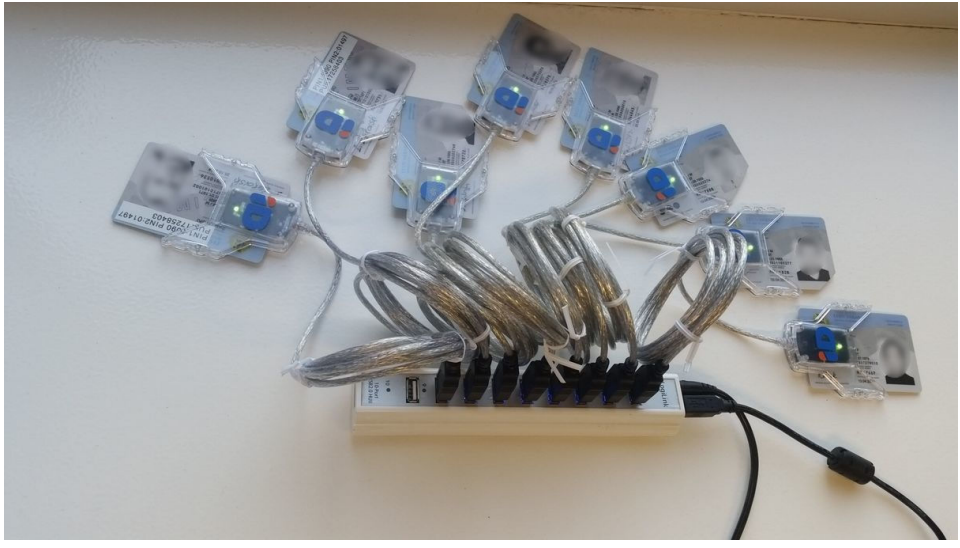
RSA public key modulus N carries a fingerprint that can be used to distinguish between key generation algorithms.

Range for p and q selection: $N = p \cdot q$ (2048 bits)

Observable from the probability distribution of most-significant byte of N



Key generation and export



PPA renewal (Jul-2012 – Jul-2017)

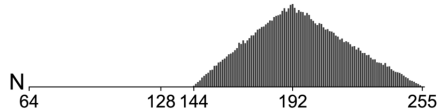


Figure: Keys from the certificates renewed in PPA

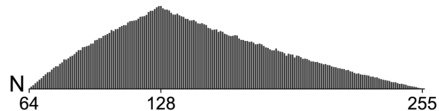


Figure: Keys generated by the platform

- Keys generated by setting the two most significant bits of p and q to 11_2
- Key import feature had to be programmed into the JavaCard applet
- We hope that the intent was to speed up the ID card renewal process
- From more than 74 000 ID cards renewed in PPA, only 12 500 were still valid

Incident response

- In May 2018, PPA announced the replacement of the affected ID cards

"In the case of the cards in question, keys were generated externally, which means that they could have been copied and could be applied without actually using the corresponding ID cards. The PPA has filed a claim against the manufacturer of the ID card for violation of security requirements."

https://news.err.ee/832236/police-12-500-id-card-certificates-to-be-deleted-due-to-security-issue

"Gemalto has fulfilled the ID-card agreement and the obligations agreed upon in the proper manner. The statements made are a surprise to Gemalto."

https://tehnika.postimees.ee/4490671/gemalto-eesti-riigi-tehtud-avaldused-on-ullatus

- In September 2018, the state brought Gemalto to court demanding a contractual penalty of 152 million EUR
- Have any lessons been learned?

Corrupted RSA public keys

No	Date of cert issuance	Cardholder (cert type)	N	Work	N-res	Factors (min / max)	Date of revocation	Corruption of N
1	2014-12-30 08:41:14	Toomas (auth)	2048	t45.76	2048	0	2017-11-03 23:59:59	?
2	2014-12-30 09:57:22	Raja (auth)	*2040*	t54.58	1713	3 (132-bit / 196-bit)	2015-08-26 16:37:53	117th byte missing
3	2014-12-30 16:03:43	Valentina (auth)	2048	t45.76	2048	0	2017-11-03 23:59:59	?
4	2014-12-30 16:05:23	Valentina (sign)	2048	t47.06	2048	0	2017-11-03 23:59:59	?
5	2015-01-05 11:25:19	Raisa (auth)	*2040*	t54.52	1958	4 (3-bit / 38-bit)	2017-06-09 14:07:57	27th byte missing
6	2015-01-27 13:48:40	Lennart (auth)	2048	t54.70	1937	4 (2-bit / 56-bit)	2016-07-01 09:36:57	64th byte changed
7	2015-02-19 09:19:21	Svetlana B. (sign)	2048	t47.47	–	7 (9-bit / 1762-bit)	2017-02-22 10:35:49	160th byte changed
8	2015-03-13 12:27:40	Imre (auth)	2048	t54.55	1895	6 (2-bit / 81-bit)	2015-04-06 13:54:33	?
9	2015-03-13 12:27:45	Imre (sign)	2048	t54.86	1757	7 (2-bit / 133-bit)	2015-04-06 13:54:33	?
10	2015-03-27 09:21:51	Vyacheslav (sign)	2048	t54.75	1808	9 (7-bit / 110-bit)	2017-06-09 14:17:20	71st byte changed
11	2015-06-01 12:07:45	Svetlana S. (auth)	*2040*	t54.54	1924	2 (25-bit / 92-bit)	2017-06-09 14:18:39	254th byte missing
12	2015-07-21 12:52:10	Rasmus (auth)	2048	t56.46	1844	4 (3-bit / 161-bit)	2017-06-09 14:21:50	254th byte changed
13	2015-08-06 14:18:44	Armand (sign)	2048	t54.42	1884	7 (11-bit / 50-bit)	2016-01-07 13:54:10	254th byte changed
14	2015-09-11 12:30:06	Paul (sign)	2048	t54.29	1973	4 (2-bit / 69-bit)	2017-06-09 14:23:09	230th byte changed
15	2015-11-04 11:27:25	Vambola (auth)	2048	t55.00	1604	6 (2-bit / 172-bit)	2017-06-09 14:50:32	87th byte changed
16	2015-12-02 10:10:37	Erki (sign)	2048	t54.34	2011	2 (2-bit / 35-bit)	2017-06-09 14:51:51	254th byte changed
17	2016-01-18 09:07:15	Pentti (auth)	2048	t46.44	2048	0	2017-11-03 23:59:59	?
18	2016-05-10 10:13:54	Laura (auth)	2048	t56.49	2002	5 (3-bit / 17-bit)	2017-06-09 14:53:29	92nd byte changed
19	2016-06-20 10:29:55	Ilja (auth)	2048	t54.58	1819	9 (2-bit / 124-bit)	2017-06-09 14:54:41	128th byte changed
20	2017-06-16 14:13:04	Vladislav (auth)	2048	t45.76	2048	0	2017-11-03 23:59:59	MSB as a minimum
21	2017-06-16 14:13:26	Vladislav (sign)	2048	t45.99	2048	0	2017-11-03 23:59:59	?
22	2017-06-16 16:28:30	Pirgit (auth)	2048	t45.86	2048	0	2017-11-03 23:59:59	MSB as a minimum
23	2017-06-16 16:28:55	Pirgit (sign)	2048	t45.73	2048	0	2017-11-03 23:59:59	MSB as a minimum

Corrupted key – Svetlana B.

```
x@nuc:~/factorize$ ./factor_ecm.py
[?] Input integer: 93467124171EB7B68408B85BEA88412E927160B9236F74C5747ED35843E91BD04F0EADFEDB3393B775B124CD0C7C26D771627FC6F7DBA3152A
CA846C4A43250ED07D28C403F18299891495782950918671EDF94C91350F1657D7908650EA5AC00AC43FEF298397950E130ADF3ABE432DE691DF2173EC9F2616636922
004DB21CD6987979DA8ED2BF5A08D3CA2BAB6821A45E4E7D0671019EFFED3804BB13A7CA6280900B0B4D95930AE6E73A0E914FE9FE3C31B48D95F2EA88E81ADDD6551
BA478E323EECC6339A35EDC37DCD532BED6C572BEDECDC9E47DEC1FA39F0657E1628970C02F829BE36500ED2FAAE86E2E77712707E26EB01EBB02AC0A01440429633
[+] Using GMP-ECM 7.0.1, Powered by GMP 6.1.0
[+] detected Intel(R) Core(TM) i5-6260U CPU @ 1.80GHz
[+] detected L1 = 32768 bytes, L2 = 4194304 bytes, CL = 64 bytes
[+]  div: found prime factor = 337
[+]  rho: found prp5 factor = 19373
[+]  rho: found prp7 factor = 1355533
[+]  pm1: found prp12 factor = 283995516641
[+] [work:0.00] [progress:0.0/30.0]
[+] [work:1.00] [progress:2.0/30.0]
[+] [work:2.00] [progress:4.0/30.0]
[+] [work:3.00] [progress:6.0/30.0]
[+] [work:4.00] [progress:8.0/30.0]
[+] [work:5.00] [progress:10.0/30.0]
[+] [work:6.00] [progress:12.0/30.0]
[+] [work:7.00] [progress:14.0/30.0]
[+] [work:8.00] [progress:16.0/30.0]
[+] [work:9.00] [progress:18.0/30.0]
[+] [work:10.00] [progress:20.0/30.0]
[+] [work:11.00] [progress:22.0/30.0]
[+] [work:12.00] [progress:24.0/30.0]
[+] [work:13.00] [progress:26.0/30.0]
[+] [work:14.00] [progress:28.0/30.0]
[+] [work:15.00] [progress:30.0/30.0]
[+] [work:15.18] [progress:0.0/74.0]
[+] [work:15.31] [progress:2.0/74.0]
[+] [work:15.44] [progress:4.0/74.0]
[+] [work:15.57] [progress:6.0/74.0]
[+] [work:15.70] [progress:8.0/74.0]
[+] [work:15.83] [progress:10.0/74.0]
[+]  ecm: found prp16 factor = 6586291483612177
[+] [work:15.99] [progress:0.0/62.0]
[+] [work:16.12] [progress:2.0/62.0]
[+] [work:16.25] [progress:4.0/62.0]
[+] [work:16.38] [progress:6.0/62.0]
```

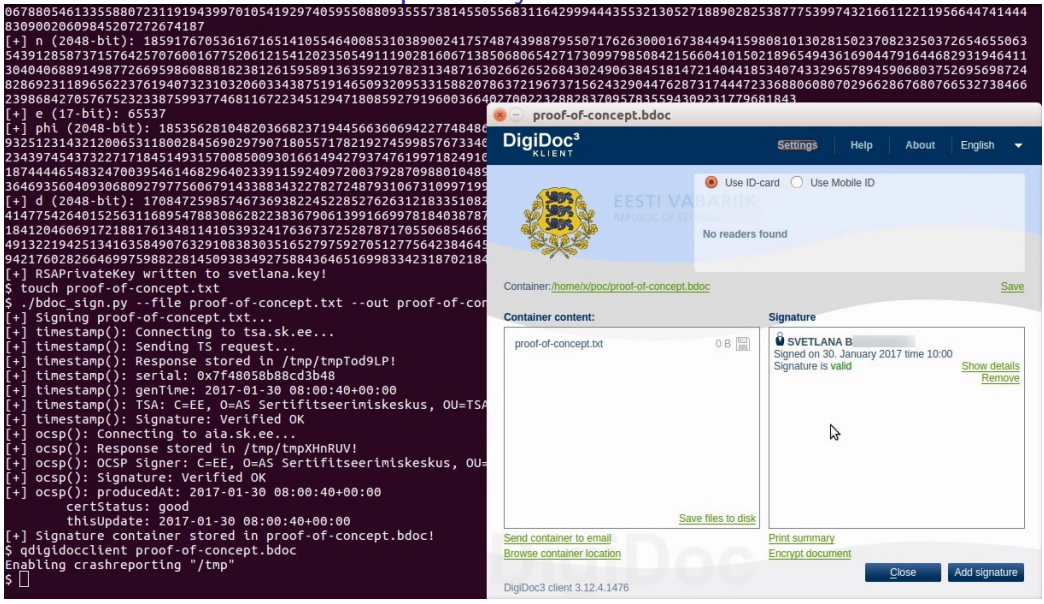
Corrupted key – Svetlana B.

```
[+] [work:40.75] [progress:120.0/4480.0] ETA:  204.17 hrs
[+] [work:40.75] [progress:122.0/4480.0] ETA:  204.08 hrs
[+] [work:40.75] [progress:124.0/4480.0] ETA:  203.97 hrs
[+] [work:40.75] [progress:126.0/4480.0] ETA:  203.87 hrs
[+] [work:40.75] [progress:128.0/4480.0] ETA:  203.76 hrs
[+] [work:40.76] [progress:130.0/4480.0] ETA:  203.64 hrs
[+] [work:40.76] [progress:132.0/4480.0] ETA:  203.55 hrs
[+] [work:40.76] [progress:134.0/4480.0] ETA:  203.45 hrs
[+] [work:40.76] [progress:136.0/4480.0] ETA:  203.36 hrs
[+] [work:40.76] [progress:138.0/4480.0] ETA:  203.25 hrs
[+] [work:40.77] [progress:140.0/4480.0] ETA:  203.15 hrs
[+] [work:40.77] [progress:142.0/4480.0] ETA:  203.05 hrs
[+] [work:40.77] [progress:144.0/4480.0] ETA:  202.94 hrs
[+] [work:40.77] [progress:146.0/4480.0] ETA:  202.85 hrs
[+] [work:40.77] [progress:148.0/4480.0] ETA:  202.74 hrs
[+] [work:40.78] [progress:150.0/4480.0] ETA:  202.82 hrs
[+] [work:40.78] [progress:152.0/4480.0] ETA:  203.51 hrs
[+] [work:40.78] [progress:154.0/4480.0] ETA:  203.39 hrs
[+] [work:40.78] [progress:156.0/4480.0] ETA:  203.27 hrs
[+] [work:40.78] [progress:158.0/4480.0] ETA:  203.18 hrs
[+] [work:40.79] [progress:160.0/4480.0] ETA:  203.06 hrs
[+] [work:40.79] [progress:162.0/4480.0] ETA:  202.96 hrs
[+] [work:40.79] [progress:164.0/4480.0] ETA:  202.85 hrs
[+] [work:40.79] [progress:166.0/4480.0] ETA:  202.78 hrs
[+] [work:40.79] [progress:168.0/4480.0] ETA:  202.66 hrs
[+] [work:40.80] [progress:170.0/4480.0] ETA:  202.54 hrs
[+] [work:40.80] [progress:172.0/4480.0] ETA:  202.43 hrs
[+] [work:40.80] [progress:174.0/4480.0] ETA:  202.32 hrs
[+] [work:40.80] [progress:176.0/4480.0] ETA:  202.22 hrs
[+] [work:40.80] [progress:178.0/4480.0] ETA:  202.11 hrs
[+] [work:40.81] [progress:180.0/4480.0] ETA:  201.99 hrs
[+]  ecm: found prp46 factor = 835205607860886666672620265739644124552467236 9
[+] Total factoring time = 212957.8331 seconds
[+] Factors: 337*19373*1355533*283995516641*6586291483612177*835205607860886666672620265739644124552467236 9*134473888232739224604277767976773587582543147467175305712412317901198989487842765816698627656015632200781042793204797561697947226785755223653582605083915429595087203285014891341184294840840430770787154781477530860979825226127477370821405761331760388655031943023131386206920177447253879160646165171391356563481764992405710211394500835412759203272467434408997878141698490992067880546133558807231191943997010541929740595508809355573814550556831164299944435532130527188902825387775399743216611221195664474144483090020609845207272674187
[-] Child died! Exiting...
x@nuc:~/factorize$ exi
```

Corrupted key – Svetlana B.

```
5557381455055683116429994443553213052718890282538777539974321661122119566447414448309002060984520727 26741 87
[-] Child died! Exiting...
x@nuc:~/factorize$ exit
logout
Connection to nuc closed.
$ ./factors_to_privkey.py --out svetlana.key
[?] Input factors: 337*19373*1355533*283995516641*6586291483612177*835205607860886666672602065739644124552467 2369*134473888232739224 6
042777679776773587582543147467175305721412317901198989487842765816698627656015632200781042793204797561697947226785755223653582605083 91
542959508720328501489134118429484084043077078715478147753086097982522612747737082140576133176038865503194302313138620692017744725387 9
160646165171391356563481764992405710211394500835412759203272467434408997878141698490992067880546133558807231191943997010541929740595 5
088093555738145505568311642999444355321305271889028253877753997432166112211956644741444830900206098452072726741 87
    [+] factor (9-bit): 337
    [+] factor (15-bit): 19373
    [+] factor (21-bit): 1355533
    [+] factor (39-bit): 283995516641
    [+] factor (53-bit): 6586291483612177
    [+] factor (153-bit): 835205607860886666672602065739644124552467 2369
    [+] factor (1762-bit): 134473888232739224604277767976773587582543147467175305712412317901198989487842765816698627656015632200781042793204797561697947226785755223653582605083 91542959508720328501489134118429484084043077078715478147753086097982522612747737082140576133176038865503194302313138620692017744725387916064616517139135656348176499240571021139450083541275920327246743440899787814169840992067880546133558807231191943997010541929740595088093555738145505568311642999444355321305271889028253877753997432166112211956644741444830900206098452072726741871762(9-bit): 337
[+] factor (15-bit): 19373
[+] factor (21-bit): 1355533
[+] factor (39-bit): 283995516641
[+] factor (53-bit): 6586291483612177
[+] factor (153-bit): 835205607860886666672602065739644124552467 2369
[+] factor (1762-bit): 134473888232739224604277767976773587582543147467175305712412317901198989487842765816698627656015632200781042793204797561697947226785755223653582605083915429592047956169794722678575522365358260508391 4279320479756169794722678575522365358260508391542959508720328501489134118429484084043077078715478147753086097982522612747737082140576133176038865503194302313138620692017744725387916064616517139135656348176499240571021139450083541275920327246743440899787814169840992067880546133558807231191943997010541929740595088093555738145505568311642999444355321305271889028253877753997432166112211956644741444830900206098452072726741871762
[+] n (2048-bit): 185917670536167165141055464008531038900241757487439887955071762630001673844941598081011302815023708232503726546555063 5439128587371576425707600167752061215412023505491119028160671385068065427173099798508421566041015021896549436169044791644682931946411 3040406688914987726695986088818238126159589136359219782133487163026626526843024906384581147214044185348743329657894590680375269569872 8286923118965622376194073231032060334387519146509320953315882078637219673715624329044762873174447233688060807029662867680766532738466 2398684270576752323387599377468116722345129471808592791960036640270022328828370957835594309231779681843 87
[+] e (17-bit): 65537
[+] phi (2048-bit): 185356281048203668237194456636069422774848608733805864046823157291256663487735614770387652218058985671038407490293 9325123143212006531180028456902979071805571782192745998576733408401981029559077319824335822878916171842936399435970490802257771486293 2343974543732271784514931570085009301661494279374761997182491006120296649675527011866936550899378556528326033168881791625712615552 5 1874446454832470039546146829640233911592409720037928709880104892700140340651943830143049557351424645484875180954686315949017859503564 3646935604093068029777560679143388343227827248793106731099719983751594692185036466350016097293663469568 0
[+] d (2048-bit): 170847259857467369382245228527626312183351082713322410691310961174495952993021427307243342043979571042776097185811 2 4147754264015256311689547883086282223836790613991669978184038787454181310187403094225956948387428309367475763015222995222423748450073 4 1841204606917218817613481141053932417636737252878717055068546654059349637143836337617839728730146400385523750623810097910103025250908 4913221942513416358490763291083830351652797592705127756423846458240959393566948361156590339697435890878213918747785659295240610695961 9421760282664699759882281450938349275884364651699833423187021843917570314604192719045031415722161405953 4[+] RSAPrivateKey written to svetlana.key!
$
```

Corrupted key – Svetlana B.



Thank you!

Questions, comments?

arnis.parsovs@ut.ee