

Pranešėjas: Kęstas Gudinavičius

KAIP PAVOGTI ELEKTRONINĘ TAPATYBĘ

Asmens tapatybės kortelė (ATK)

- 2048 bitų ilgio kriptografiniai raktai (viešo ir privataus raktų pora)
- Privatus raktas apsaugotas lusto programinėmis ir aparatinėmis priemonėmis ir negali būti eksportuotas į kitas laikmenas
- 8 simbolių PIN kodas

ATK naudojimas

- Elektroninės valdžios vartai (EVV)
 - Viešosios paslaugos gyventojams
- SODRA
 - Gyventojų ir draudėjų sritys
- AB Ūkio bankas
 - Elektroninės bankininkystės portalas
- SIGNA – taikomoji programa
 - Elektroninių dokumentų pasirašymas

Pagrindinės ATK integravimo klaidos

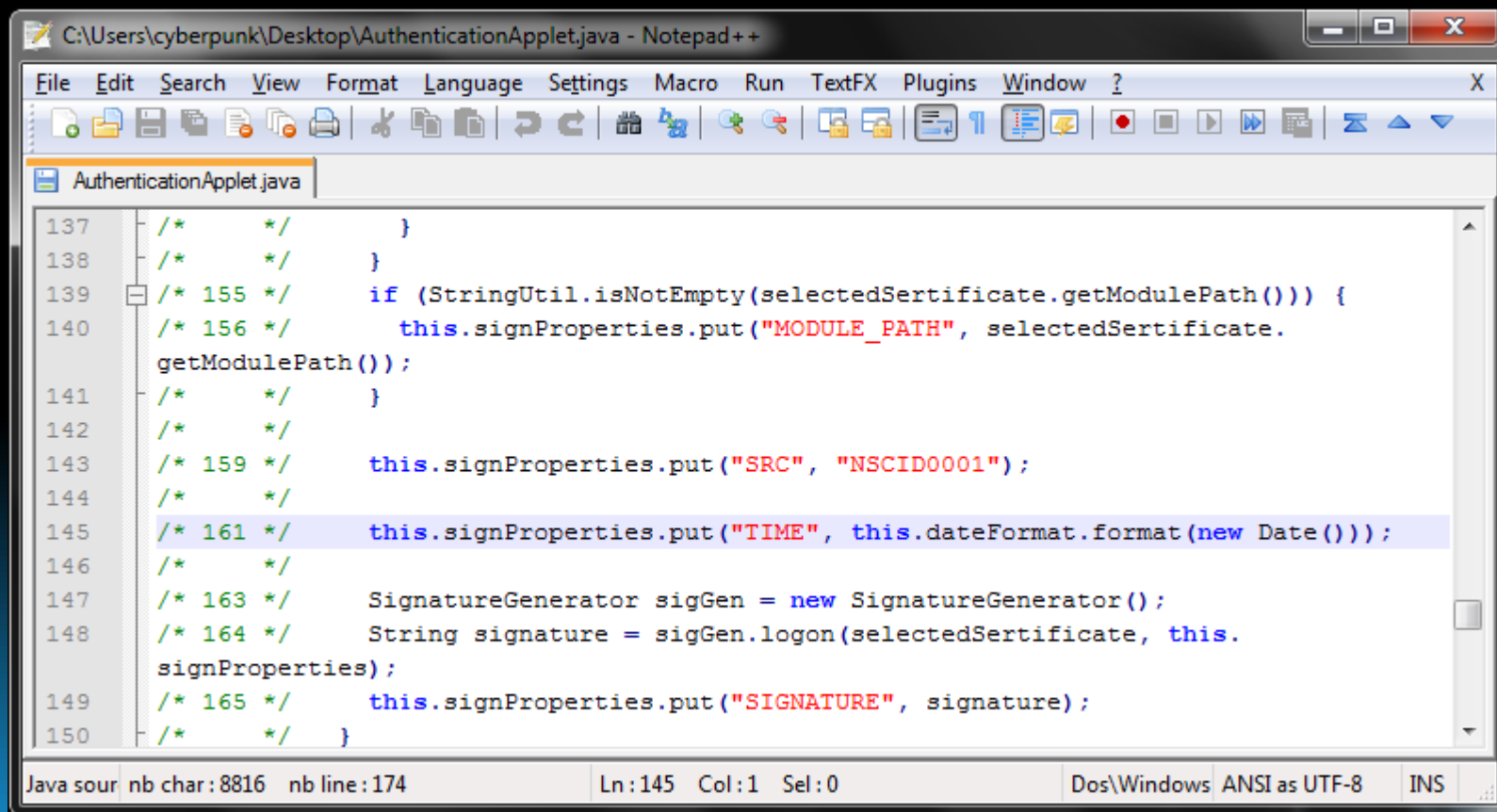
- Netinkamas autentifikacijos paketo galiojimo laiko tikrinimas
- Netinkamas privataus kriptografinio rakto naudojimas
- Netinkamas skaitmeninio sertifikato asmens duomenų panaudojimas

Netinkamas autentifikacijos paketo galiojimo laiko tikrinimas

- Kiekvienas autentifikacijos paketas turi laiko parametrą
 - Laikas sekundės tikslumu
 - TIME="2010.06.19 01:03:05"
- Ribotas autentifikacijos paketo galiojimo laikas
 - Apsauga nuo pakartojimo atakų

Netinkamas autentifikacijos paketo galiojimo laiko tikrinimas

- EVV cert-chooser-0.0.1-SNAPSHOT.jar

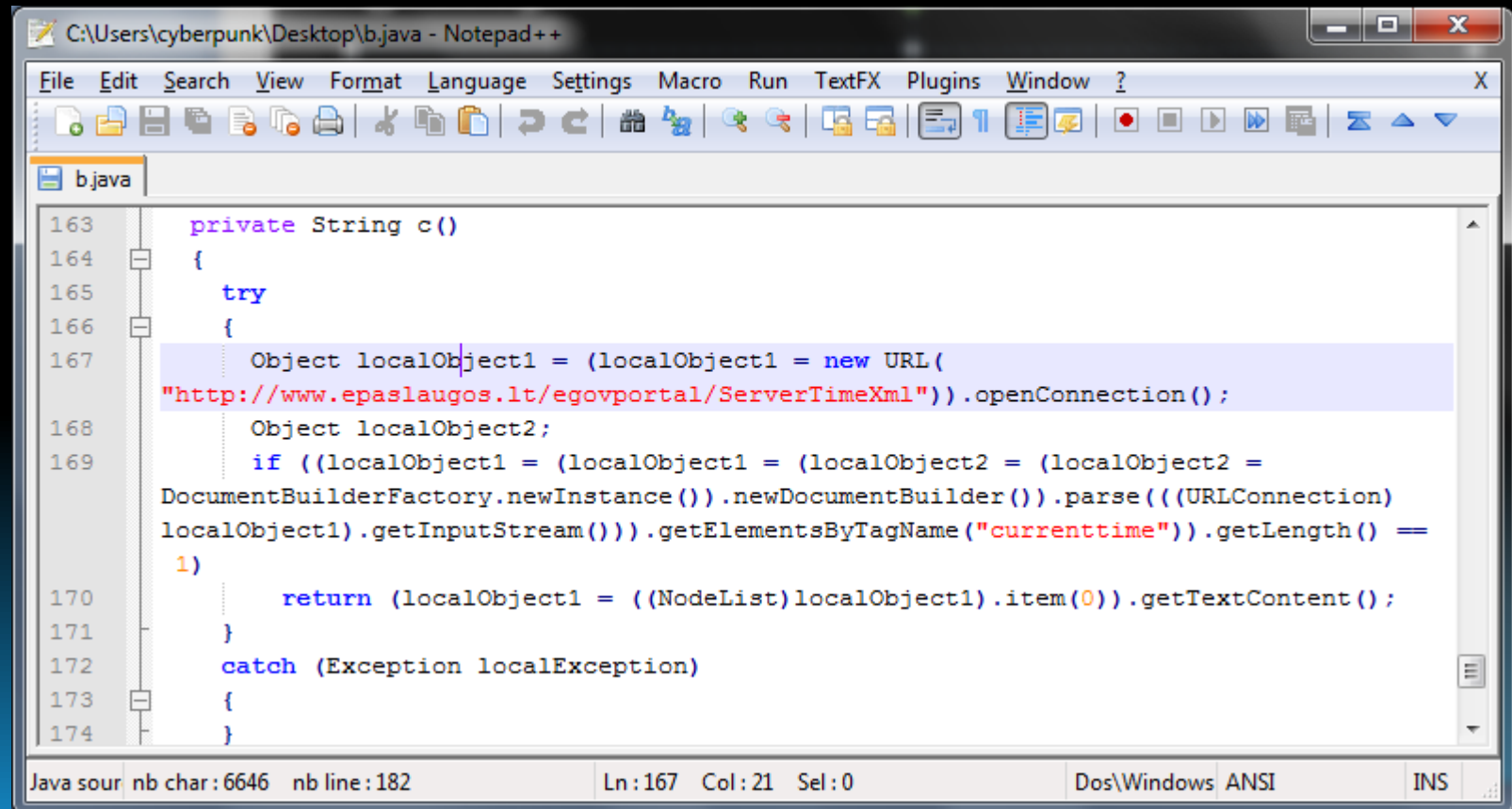


```

C:\Users\cyberpunk\Desktop\AuthenticationApplet.java - Notepad++
File Edit Search View Format Language Settings Macro Run TextFX Plugins Window ?
AuthenticationApplet.java
137  /* */      }
138  /* */      }
139  /* 155 */    if (StringUtil.isNotEmpty(selectedCertificate.getModulePath())) {
140  /* 156 */      this.signProperties.put("MODULE_PATH", selectedCertificate.
getModulePath());
141  /* */      }
142  /* */
143  /* 159 */    this.signProperties.put("SRC", "NSCID0001");
144  /* */
145  /* 161 */    this.signProperties.put("TIME", this.dateFormat.format(new Date()));
146  /* */
147  /* 163 */    SignatureGenerator sigGen = new SignatureGenerator();
148  /* 164 */    String signature = sigGen.logon(selectedCertificate, this.
signProperties);
149  /* 165 */    this.signProperties.put("SIGNATURE", signature);
150  /* */      }
Java sour nb char: 8816 nb line: 174 Ln: 145 Col: 1 Sel: 0 Dos\Windows ANSI as UTF-8 INS
  
```

Netinkamas autentifikacijos paketo galiojimo laiko tikrinimas

- EVV cert-chooser-o.o.2.jar



```

C:\Users\cyberpunk\Desktop\b.java - Notepad++
File Edit Search View Format Language Settings Macro Run TextFX Plugins Window ?
b.java
163     private String c()
164     {
165         try
166         {
167             Object localObject1 = (localObject1 = new URL(
168             "http://www.epaslaugos.lt/egovportal/ServerTimeXml")).openConnection();
169             Object localObject2;
170             if ((localObject1 = (localObject1 = (localObject2 = (localObject2 =
171             DocumentBuilderFactory.newInstance()).newDocumentBuilder()).parse(((URLConnection)
172             localObject1).getInputStream()).getElementsByTagName("currenttime").getLength() ==
173             1)
174                 return (localObject1 = ((NodeList)localObject1).item(0)).getTextContent();
175         }
176         catch (Exception localException)
177         {
178         }
179     }
Java sour nb char: 6646 nb line: 182 Ln: 167 Col: 21 Sel: 0 Dos\Windows ANSI INS

```

Netinkamas autentifikacijos paketo galiojimo laiko tikrinimas

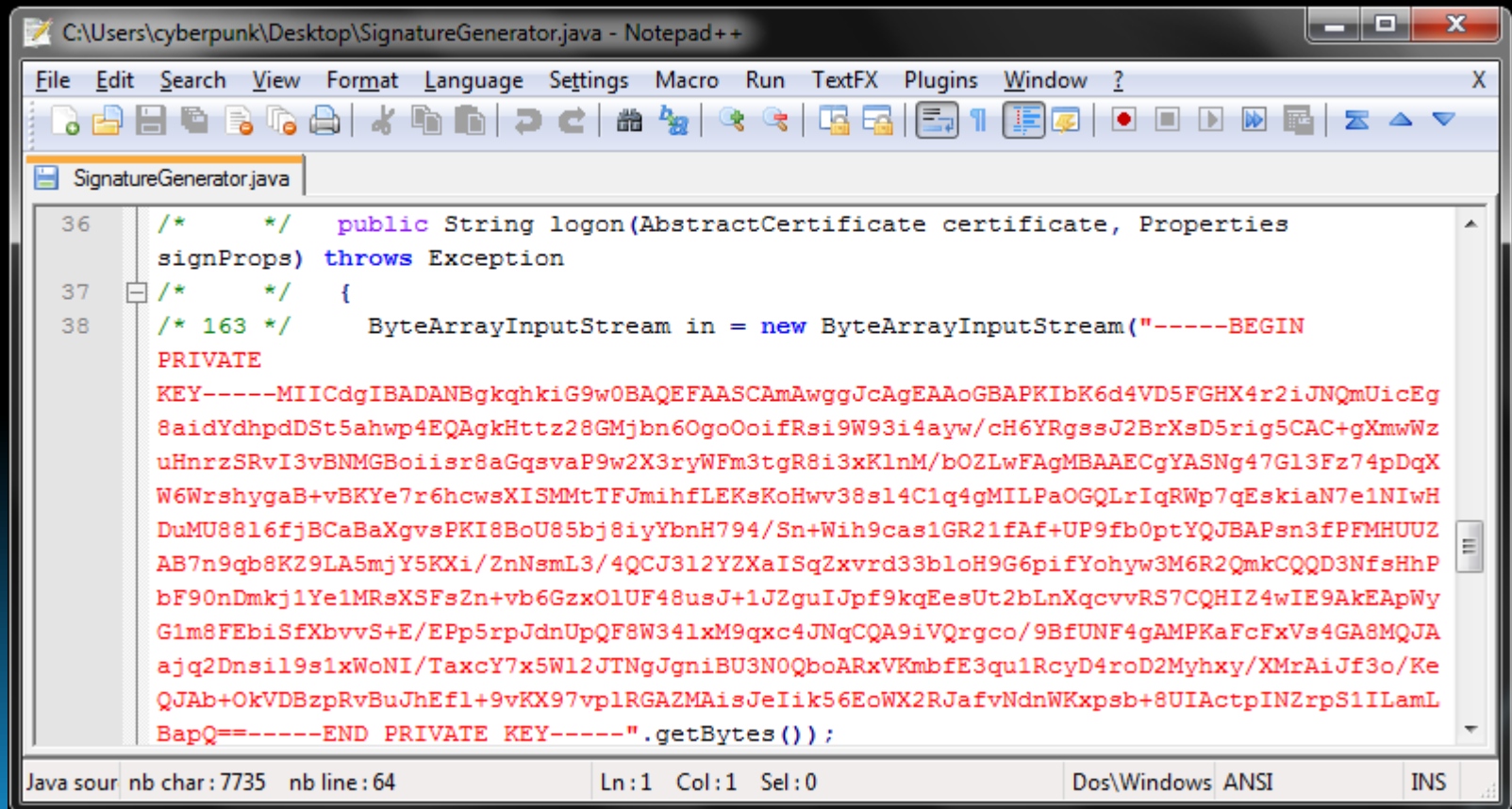
- Laikas nustatomas klientinėmis priemonėmis
 - Serverinė aplikacija nežino, kada realiai buvo sugeneruotas autentifikacijos paketas
- Autentifikacijos paketo generavimas ateičiai
 - Ilgalaikė tapatybės vagystė

Netinkamas privataus kriptografinio rakto naudojimas

- Sudarytas autentifikacijos paketas nėra pasirašomas ATK esančiu privačiu raktu
- Naudojamas klientinėje aplikacijoje hardcodintas privatus raktas
 - Dekompilijuojame/reversiname klientinę aplikaciją ir išgauname privatų kriptografinį raktą

Netinkamas privataus kriptografinio rakto naudojimas

- EVV cert-chooser-o.o.1-SNAPSHOT.jar



```

C:\Users\cyberpunk\Desktop\SignatureGenerator.java - Notepad++
File Edit Search View Format Language Settings Macro Run TextFX Plugins Window ?
SignatureGenerator.java
36  /* */ public String logon(AbstractCertificate certificate, Properties
    signProps) throws Exception
37  /* */ {
38  /* 163 */   ByteArrayInputStream in = new ByteArrayInputStream("-----BEGIN
PRIVATE
KEY-----MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBAPKIbK6d4VD5FGHX4r2iJNQMUicEg
8aidYdhpdDSt5ahwp4EQAgkHttz28GMjbn6OgoOoiFRsi9W93i4ayw/CH6YRgssJ2BrXsD5rig5CAC+gXmwWz
uHnrzSRvI3vBNMGBoiisr8aGqsvaP9w2X3ryWfm3tgr8i3xKlnM/bOZLwFAGMBAAECgYASNg47G13Fz74pDqX
W6WrshygaB+vBKYe7r6hcwsXISMMtTFJmihfLEKsKoHwv38s14C1q4gMILPaOGQLrIqRWp7qEskian7e1NIwH
DuMU8816fjBCaBaXgvsPKI8BoU85bj8iyYbnH794/Sn+Wih9cas1GR21fAf+UP9fb0ptYQJBAPsn3fPFMHUuz
AB7n9qb8KZ9LA5mjY5KXi/ZnNsmL3/4QCJ312Y2XaISqZxvrd33bloH9G6piFYohyw3M6R2QmCQQD3NfsHhP
bF90nDmkj1Ye1MRsXSFsZn+vb6GzxO1UF48usJ+1JZguIjpf9kqEesUt2bLnXqcvvRS7CQHIZ4wIE9AkEApWy
G1m8FEbiSfXbvvs+E/EPp5rpJdnUpQF8W341xM9qxc4JNqCQA9iVQrgco/9BfUNF4gAMPKaFcFVs4GA8MQJA
ajq2Dnsil9s1xWoNI/TaxcY7x5Wl2JTNgJgniBU3N0QboARxVKmbfE3qu1RcyD4rod2Myhxy/XMrAiJf3o/Ke
QJAb+OkVDBzpRvBuJhEfl+9vKX97vplRGA2MAisJeIik56EoWX2RJafvNdnWKxpsb+8UIActpINZrps1ILamL
BapQ=====END PRIVATE KEY-----".getBytes());
    
```

Java sour nb char: 7735 nb line: 64 Ln: 1 Col: 1 Sel: 0 Dos\Windows ANSI INS

Netinkamas privataus kriptografinio rakto naudojimas

- ATK esantys skaitmeniniai sertifikatai yra lengvai nuskaitomi
 - Nėra reikalaujama PIN kodo
- “Pasiskoliname” ATK esančius skaitmeninius sertifikatus
 - Pasirašome anksčiau išgautu privačiu raktu

Netinkamas skaitmeninio sertifikato duomenų panaudojimas

- ATK skaitmeniniame sertifikate esantys asmens duomenys:
 - Vardas
 - Pavardė
 - Asmens kodas
 - Pilietybė
- Autentifikacijos paketas sudaromas pridedant papildomus laukus su asmens duomenimis

Netinkamas skaitmeninio sertifikato duomenų panaudojimas

- EVV autentifikacijos paketas

```

https://www.epaslaugos.lt/egovportal/idplugin/index.jsp - Original Source
File Edit Format
571         try {
572             var pageTracker = _gat._getTracker("UA-7789071-1");
573             pageTracker._trackPageview();
574         } catch(err) {}
575     </script>
576 </div>
577 </div>
578 </div>
579 <form name="loginForm" method="post"
    action="https://www.epaslaugos.lt/egovportal/bank/auth_response.jsp">
580     <input name="SRC" type="hidden" value="" />
581     <input name="TIME" type="hidden" value="" />
582     <input name="PERSON_CODE" type="hidden" value="" />
583     <input name="PERSON_FNAME" type="hidden" value="" />
584     <input name="PERSON_LNAME" type="hidden" value="" />
585     <input name="PERSON_DUTY" type="hidden" value="" />
586     <input name="PERSON_ORGANIZATION" type="hidden" value="" />
587     <input name="ISSUER_COUNTRY" type="hidden" value="" />
588     <input name="CERTIFICATE_SUMMARY" type="hidden" value="" />
589     <input name="PERSON_CERT" type="hidden" value="" />
590     <input name="SIGNATURE" type="hidden" value="" />
591     <input name="TYPE" type="hidden" value="" />
592     <input name="MODULE_PATH" type="hidden" value="" />
593 </form>
594

```

Netinkamas skaitmeninio sertifikato duomenų panaudojimas

- Informacinė sistema patikrina autentifikacijos paketo vientisumą bei skaitmeninio sertifikato galiojimą
- Autorizacija atliekama naudojant ne skaitmeninį sertifikatą, o papildomuose laukuose esančius asmens duomenis
 - ▣ Modifikuojame asmens duomenis prieš pasirašant autentifikacijos paketą

Įrankiai

- Klientinės aplikacijos dekompiliavimas
 - JD | Java Decompiler
- Duomenų pasirašymas
 - `openssl dgst -sha1 -sign key.pem -out packet.txt.sha1 packet.txt`
- Asmens duomenų/laiko modifikavimas
 - JavaSnoop

Atakos prieš ATK naudotojus

- Man-in-the-Browser
- ATK PIN kodo pasisavinimas
- Phishing
- Tapatybės atskleidimas

Man-in-the-Browser

- Kenkėjiška programa veikia tarp naršyklės ir apsaugos mechanizmo
- Perduodamų duomenų perėmimas ir modifikavimas
 - Balsavimas už reikiamą kandidatą
- Sudėtinga aptikti

ATK PIN kodo pasisavinimas

- Kenkėjiška programa perima vartotojo įvedamą ATK PIN kodą
 - Standartiniuose skaitytuvuose nėra pinpado
- Skaitytuve paliekama vartotojo ATK
 - Fone atliekami kenkėjiški veiksmai
- Nepalikinti ATK skaitytuve

Phishing

- Įsilaužėliai suklastoja autentifikacijai ATK naudojamą portalą
 - Analogiška tradicinei phishing atakai
- Auka autentifikuojasi su savo ATK
 - Sugeneruotas autentifikacijos paketas iškart panaudojamas prisijungimui prie tikrojo portalo
 - Sugeneruojamas autentifikacijos paketas ateičiai
- Nesilankyti įtartinuose tinklalapiuose

Tapatybės atskleidimas

- Pažeidžiamas ActiveX komponentas/ Java programa
 - Nesaugių funkcijų darbui su skaitmeniniais sertifikatais naudojimas
- Vartotojas apsilanko specialiai suformuotame tinklalapyje, kuris perimą sertifikatą
 - Įsilaužėlis išgauna vartotojo vardą, pavardę, asmens kodą
- Nepalikinėti ATK skaitytuve



Klausimai?