Prijava v OS Microsoft Windows s pametno kartico FRICard

Žiga Kern, 63140099

24. julij 2018

Kazalo

1 Uvod

Operacijski sistem Microsoft Windows podobno kot drugi zahteva prijavo v veljaven račun pred dostopom do podatkov in aplikacij. Glavni način prijave že dolgo predstavlja geslo, kar pa v določenih primerih ni idealen način avtentikacije. Veliko uporabnikov pogostokrat izbira preprosta gesla, uporabljajo enaka gesla za več storitev ali si ta celo zapisujejo na listke. Ena izmed alternativ avtentikacije v OS pa predstavljajo tudi pametne kartice. Dobra lastnost teh je da že v osnovi podpirajo dvo faktorsko avtentikacijo, kjer si mora uporabnik lastiti pametno kartico poleg tega pa poznati tudi geslo oziroma pin za dostop do podatkov shranjenih na njej in posledično za prijavo v OS.

V okviru te seminarske naloge bomo v poglavju 2 na grobo spoznali potek prijave v OS Microsoft Windows v naslednjem poglavju 3 pa kako lahko z minigonilnikom podpremo novo pametno kartico. V poglavju 4 so podani podatki o namestitvi razvitega minigonilnika in na koncu sledi še zaključek.

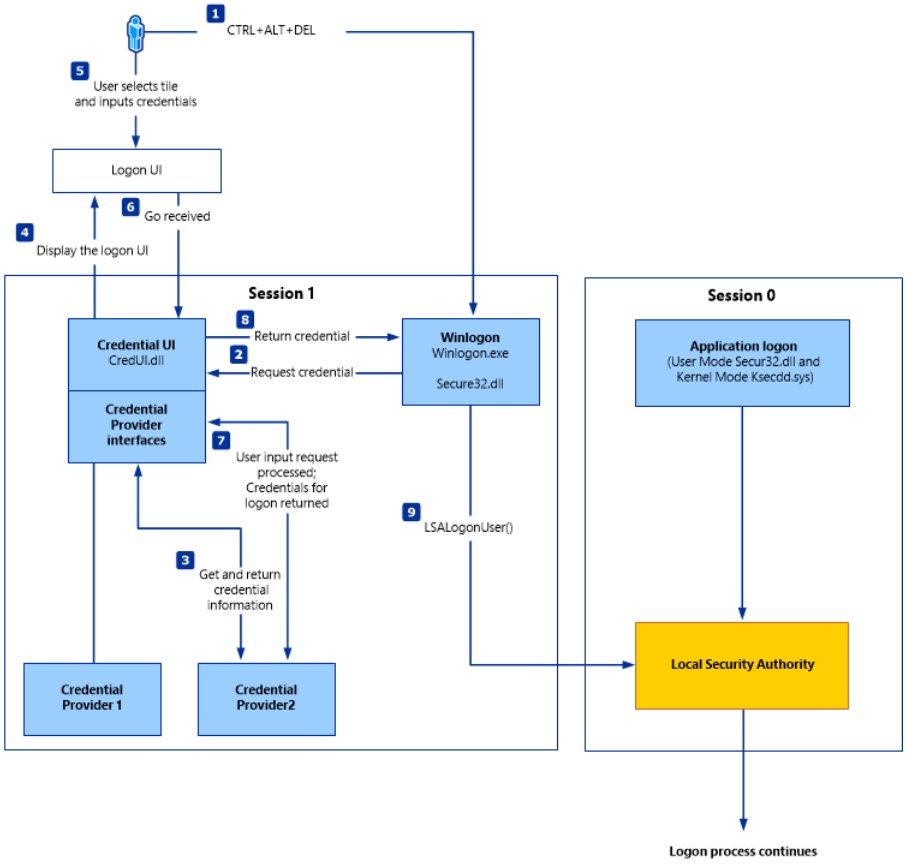
2 Potek prijave v OS Microsoft Windows

V starejših sistemih je za avtentikacijo skrbela GINA (Graphical Identification and Authentication) arhitektura, ki pa je bila zamenjana z modelom ponudnikov preverilnic (ang. credential provider, CP) od Windows Viste dalje. Ti ponudniki so predstavljeni kot različne možnosti za prijavo v sistem na prijavnem zaslonu, kot na primer prijava z geslom, pametno kartico ali biometričnim bralcem.

Proces prijave (slika 1) v sistem se začne s prikazom vmesnika za prijavo, ki od vsakega CP prejme možne načine prijave v sistem in te prikaže uporabniku. Uporabnik nato izbere način prijave v sistem, ponavadi kar privzeto možnost, in vnese podatke potrebne za avtentikacijo (geslo, pin, itd.). Ti podatki se posredujejo v CP, ki vrne preverilnico, katera se posreduje procesu LSA (Local Security Authority). LSA je zaščiten sistemski proces, ki preveri prejete podatke, avtenticira in prijavi uporabnike v lokalni sistem.

Postopek prijave s pametnimi karticami je skoraj enak zgoraj opisanemu. Ob izbiri primernega CP se preveri vse priključene pametne kartice in poišče primeren kriptografski ponudnik storitev (ang. Cryptographic Service Provider, CSP), preko katerega poteka komunikacija s kartico. Preko CSP se poišče vse certifikate, ki se nahajajo na pametni kartici, primerne za prijavo in preko vmesnika pridobi PIN kartice od uporabnika. CP te podatke zapakira v strukturo za prijavo ter jih posreduje preko vmesnika za prijavo in Winlogon procesa v LSA. LSA nato na podlagi teh podatkov s pomočjo AD (Active Directory) in komunikacije s pametno kartico preko CSP avtenticira uporabnika.

Prijava v OS Microsoft Windows s pametnimi karticami je privzeto mogoča le če je računalnik del domene. Posledično je v primeru ko se želimo prijaviti v samostojen računalnik potrebno implementirati CP ali uporabiti programsko opremo tretje osebe, ki vključuje tudi CP, ki podpira lokalno prijavo s pametno kartico.



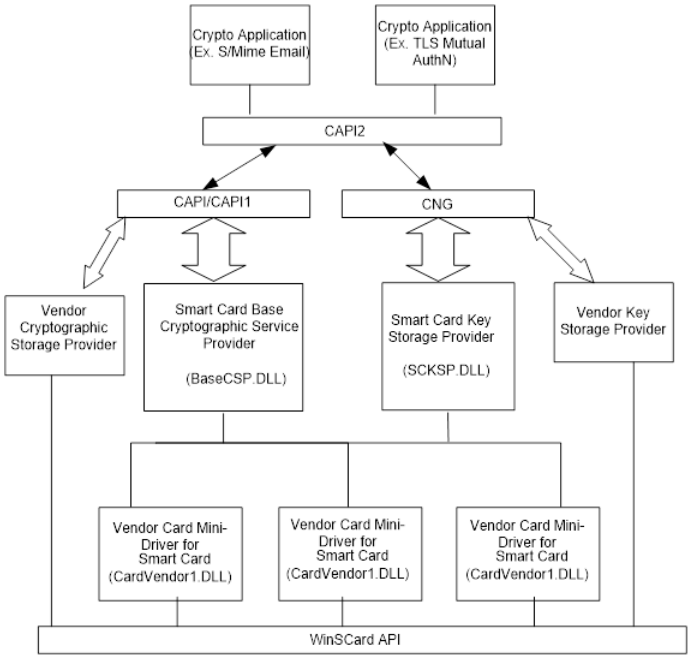
Slika 1: Proces prijave uporabnika v OS Microsoft Windows.

Podrobnejši opis postopka prijave najdemo v [1] in [2].

3 Minigonilnik

Za podporo pametne kartice FRICard oz. bolj specifično pametne kartice z naloženim appletom FRIrsa za prijavo v OS Microsoft Windows je poleg primernega CP potreben tudi CSP za komunikacijo s kartico. Nekoliko preprostejša možnost kot implementacija celotnega CSP je implementacija ti. minigonilnika (ang. minidriver). Minigonilnik v primerjavi s CSP implementira samo operacije, ki se navezujejo na posamezno pametno kartico in ne tudi standarne kriptografske operacije. Večino kriptografskih operacij tako implemenitira BaseCSP, za operacije za katere je potrebna pametna kartica pa se BaseCSP sklicuje na standarden vmesnik, ki ga implementira minigonilnik (slika 2).

Naloga implementacije minigonilnikov je ponavadi na strani proizvajalca pa-



Slika 2: Vmesniki med minigonilniki in aplikacijami.

metnih kartic, toda ker gre tokrat za FRICard kartico z nestandardnim protokolom implementacija gonilnika spada pod to seminarsko nalogo. Minigonilnik smo tako v okviru te naloge implementirali v skladu s specifikacijo verzije 7.07 [3]. Ker Java Card privzeto ne podpira datotečnega sistema ISO 7816-4 niti ni ta implementiran v appletu FRIrsa smo napisali minigonilnik za ti. bralne (ang. read-only) kartice. V tem primeru mora minigonilnik implementirati le podmnožico definiranih funkcij, ki so podane v specifikaciji, hkrati pa je potrebno simulirati datotečni sistem v samem minigonilniku ter za določene datoteke vračati primerno vsebino.

Za asociacijo minigonilnika s pametno kartico ob vstavitvi te v bralnik specifikacija definira nekaj različnih pristopov. Za asociacijo našega gonilnika smo uporabili le ATR (answer to reset), vendar se močno priporoča tudi uporaba drugih metod, kot odgovori na določene ukaze, vendar teh kartica FRICard trenutno ne podpira. V vsakem primeru pa morajo v registru računalnika za vsako izmed podprtih kartic pod ključem
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards`
biti shranjenih nekaj vnosov, med njimi sta tudi ATR kartice ter mesto kjer je minigonilnik nameščen.

Za preverjanje funkcionalnosti in implementacije minigonilnika Microsoft ponuja tudi orodja za certifikacijo, toda žal certificiranje našega minigonilnika ni bilo mogoče, saj je za to potrebno večjo število računalnikov, čitalcev pametnih

kartic in seveda tudi kartic.

4 Namestitev

4.1 Pametna kartica

Namestitev FRIrsa appleta in inicializacijo pametne kartice lahko opravimo z že obstoječimi programi in orodji, ki so bila razvita za FRICard. Pri pripravi pametne kartice je pozornost potrebno nameniti edino izdelavi in nalaganju certifikata.

Za omogočanje prijave v OS Microsoft Windows moramo slediti določenim zahtevam za certifikatno agencijo (CA) in izdajo certifikatov [4]. V našem primeru se želimo prijaviti v samostojen računalnik, ki ni del domene, zato so najbolj pomemben podatek zahteve za certifikat. Da je certifikat mogoče uporabiti za prijavo mora ta podpirati vsaj digitalno podpisovanje, prijavo s pametno kartico in vsebovati alternativno ime uporabnika.

```
Key Usage = Digital Signature (1.3.6.1.5.5.7.3.2)
Enhanced Key Usage = Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
Subject Alternative Name: UPN = user1@name.com (1.3.6.1.4.1.311.20.2.3)
```

Ker računalnik ni del domene lahko za prijavo uporabimo kar samopodpisan certifikat (ang. self-singed certificate), ter se s tem izognemo kreaciji CA. Za kreacijo certifikata, ki ustreza zahtevam za prijavo v OS Microsoft Windows lahko uporabimo OpenSSL.

```
[ logon_cert ]
keyUsage = critical, nonRepudiation, digitalSignature,
        keyEncipherment
extendedKeyUsage = critical, clientAuth, emailProtection,
        msSmartcardLogin
basicConstraints = critical, CA:FALSE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
subjectAltName = otherName:msUPN;UTF8:user@lkrv.fri.uni-lj.si,
        email:user@lkrv.fri.uni-lj.si
```

Ustrezen certifikat ustvarimo tako, da na konec konfiguracijske datoteke orodja OpenSSL pripnemo zgornji razdelek `logon_cert` in ustvarimo certifikat ter privaten ključ z naslednjim ukazom. Generiran certifikat in ključ lahko uvozimo na pametno kartico v applet FRIrsa.

```
openssl req -x509 -newkey rsa:2048 -keyout key.pem
        -out cert.pem -days 365 -extensions logon_cert
```

4.2 Minigonilnik

Pri nameščanju programske opreme OS Microsoft Windows preveri izvor te tako, da preveri verigo certifikatov s katerimi je programska oprema podpisana. Če

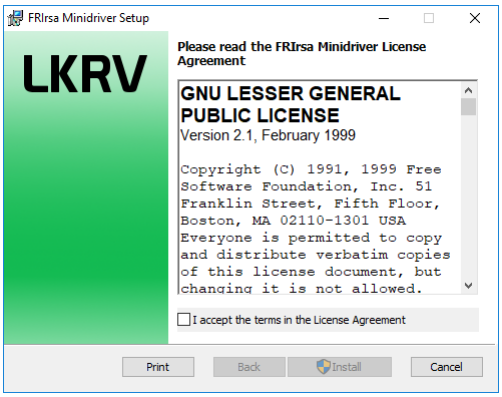
ne želimo prejemati opozoril in za uspešno namestitev minigonilnika omogočiti testnega načina operacijskega sistema mora biti paket podpisan s strani Microsofta ali drugega pooblaščenega certifikata. Za testiranje gonilnikov v razvojnem okolju pa obstaja možnost testnega podpisovanja [5], toda je za uspešno namestitev potrebno opraviti še nekaj dodatnih korakov.

Minigonilnik se namesti s pomočjo MSI paketa, toda ker je ta podpisan le s testnim certifikatom predvsem iz cenovnih razlogov samo zagon instalacijskega programa ni dovolj. Pred namestitvijo moramo s spodnjim ukazom omogočiti nalaganje testno podpisanih gonilnikov in ponovno zagnati računalnik.

```
bcdedit /set testsigning on
```

Po ponovnem zagonu dodamo certifikat s katerim je bil paket podpisan v shrambo zaupanja vrednih certifikatov z naslednjima ukazoma.

```
CertMgr.exe /add lkrv.fri.uni-lj.si.cer /s /r localMachine root
CertMgr.exe /add lkrv.fri.uni-lj.si.cer /s /r localMachine trustedpublisher
```

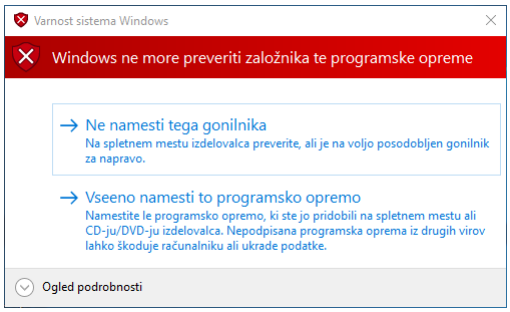


Slika 3: Namestitev FRIrsa minigonilnika.

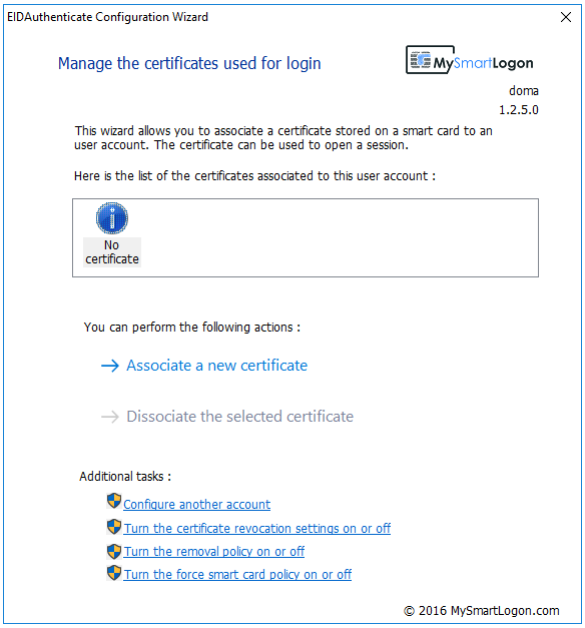
Sedaj lahko zaženemo bodisi `minidriver-1.0.0.12.x64.msi` bodisi `minidriver-1.0.0.12.x86.msi` odvisno od verzije operacijskega sistema in namestimo minigonilnik (slika 3). Med nalaganjem tega se bo pojavilo tudi opozorilo "`Microsoft Windows ne more preveriti založnika te programske opreme`"(slika 4), kjer izberemo možnost "`Vseeno namesti to programsko opremo`".

4.3 EIDAuthenticate

OS Microsoft Windows prijavo s pametno kartico podpira le če je računalnik del domene, ki ima nastavljeno varnostno politiko prijave s pametnimi karticami. Posledično za prijavo v OS Microsoft Windows na samostojnem računalniku, ki ni del domene, potrebujemo dodatno programsko opremo. Za podpiranje prijave s pametnimi karticami lahko implementiramo svoj CP ali namestimo programsko opremo kot EIDAuthenticate [6], ki vključuje implementiran CP s podporo prijave s pametno kartico.



Slika 4: Opozorilo pri namestitvi minigonilnika.

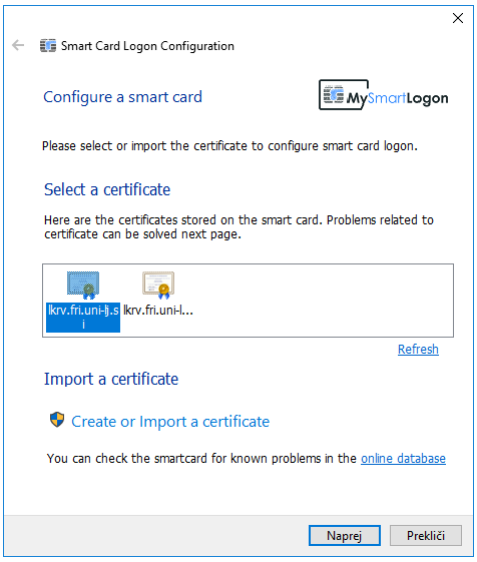


Slika 5: EIDAuthenticate konfiguracijski čarovnik.

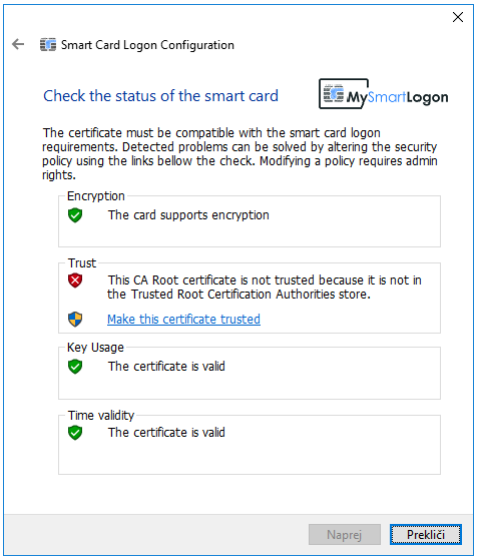
Za konfiguracijo po namestitvi EIDAuthenticate zaženemo konfiguracijski čarovnik. V čarovniku, kot je prikazan na sliki 5, izberemo opcijo asociacije novega certifikata z uporabniškim računom.

V naslednjem oknu (slika 6) po vstavitvi pametne kartice izberemo certifikat, ki smo ga prej naložili na to in nadaljujemo s konfiguracijo s klikom na gumb "`Naprej`".

V naslednjem koraku (slika 7) se preveri veljavnost certifikata za prijavo v OS Microsoft Windows in primernost pametne kartice ter minigolnilnika, bolj specifično, če ta dva podpirata potrebne operacije. V primeru samopodpisanega certifikata ali če CA, ki je izdal certifikat, ni v shrambi zaupanja vrednih



Slika 6: Asociacija certifikata z uporabniškim računom.



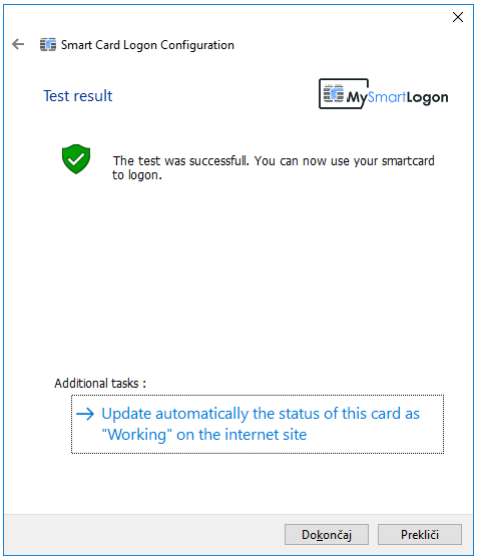
Slika 7: Preverjanje primernosti certifikata in pametne kartice.

certifikatov, lahko tega dodamo s klikom na gumb "`Make this certificate trusted`".

V naslednjem koraku (slika 8) vnesemo geslo uporabniškega računa in nadaljujemo na testiranje konfiguracije (slika 9), kjer je potrebno vnesti tudi PIN

Slika 8: Vnos gesla uporabniškega računa.

pametne kartice. Po uspešnem testiranju je konfiguracija zaključena.



Slika 9: Testiranje konfiguracije.

5 Zaključek

V okviru seminarske naloge smo razvili minigonilnik, ki omogoča prijavo v OS Micfosoft Windows s pomočjo pametne kartice FRICard. Minigonilnik je bil testiran na OS Microsoft Windows 10, vendar naj bi deloval na vseh računalnikih z nameščenim OS novejšim od OS Microsoft Windows Vista ne glede na to ali je računalnik del domene ali ne. Le v slednjem primeru je potrebna dodatna programska oprema kot na primer EIDAuthenticate.

Poleg tega poročila lahko najdemo posnetek `demo.mp4`, na katerem je prikazana demonstracija delovanja prijave s pametno kartico FRICard, izvorno kodo minigonilnika in vse potrebne datoteke za namestitev tega. Nadaljni koraki pri razvoju gonilnika pa bi prav gotovo bili dodajanje možnosti spreminjanja pina, odblokiranja pametne kartice s PUK kodo, certificiranje gonilnika in podpis tega z uradnim certifikatom.

Literatura

[1] Microsoft. Windows smart card technical reference. [Online]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff404297(v%3dws.10)

[2] ——. Windows authentication overview. [Online]. Available: https://docs.microsoft.com/en-us/windows-server/security/windows-authentication/windows-authentication-overview

[3] ——. Windows smart card minidriver specification v7.07. [Online]. Available: http://download.microsoft.com/download/3/3/2/332fd70b-f04d-470a-a135-040350b9563f/sc-minidriver_specs_v7.07.docx

[4] ——. Guidelines for enabling smart card logon with third-party certification authorities. [Online]. Available: https://support.microsoft.com/en-us/help/281245/guidelines-for-enabling-smart-card-logon-with-third-party-certificatio

[5] T. Hudek. Test signing. [Online]. Available: https://docs.microsoft.com/en-us/windows-hardware/drivers/install/test-signing

[6] MySmartLogon. Eidauthenticate. [Online]. Available: https://www.mysmartlogon.com/products/eidauthenticate.html