

Infrastruktura javnih ključev na MO

**Navodilo za namestitev strojne in programske opreme
ter uporabo osnovnih storitev MO-INTRANET**

Verzija 1.3

September 2017

Izdaja / Avtor	Spremembe glede na prejšnjo izdajo:
Infrastruktura javnih ključev na MO, Navodilo za namestitev strojne in programske opreme ter uporabo osnovnih storitev v omrežju MO-INTRANET / Ana Poklič, Ver. 1.3, 28.09.2017	Posodobljeno: Dodani napotki za delo z novo verzijo programske opreme za podporo pametnih kartic SafeNet Authentication Client 10.4. Dodana navodila za odklepanje pametne kartice IDPrime MD 840 in ponastavitev pozabljenega gesla.
Infrastruktura javnih ključev na MO, Navodilo za namestitev strojne in programske opreme ter uporabo osnovnih storitev v omrežju MO-INTRANET / Toni Senica, Aleksandra Habič, 14.10.2016	Posodobljeno: Dodani napotki za pravilno nastavitev parametra programske opreme za podporo pametnih kartic SafeNet Authentication Client 10.0 pred prevzemom in uporabo pametnih kartic ter pred inicializacijo pametnih kartic
Infrastruktura javnih ključev na MO, Navodilo za namestitev strojne in programske opreme ter uporabo osnovnih storitev v omrežju MO-INTRANET / Toni Senica, Aleksandra Habič, 06.05.2016	Posodobljeno: operacijski sistem MS Windows 7, sporočilni sistem MS Outlook 2010, programska oprema za podporo pametnih kartic SafeNet Authentication Client 10.0, programska oprema za upravljanje z digitalnimi potrdili Entrust Entelligence Security Provider 9.2..
Infrastruktura javnih ključev na MO, Postopek za namestitev strojne in programske opreme ter uporabo osnovnih storitev, Številka: 382-5/2006-99, Datum: 19.03.2010 / Darko Kučina	

KAZALO

1.	Namestitev strojne in programske opreme.....	2
1.1	Namestitev čitalca pametnih kartic	2
1.2	Namestitev programa za podporo pametne kartice SafeNet Authentication Client	8
1.3	Namestitev programa za upravljanje z digitalnimi potrdili Entrust Entelligence Security Provider.....	15
2.	Prezem digitalnega potrdila	20
2.1	Preverjanje delovanja čitalca pametne kartice in pametne kartice	20
2.2	Pravilna nastavitev programa za podporo pametne kartice SafeNet Authentication Client	21
2.3	Začetna določitev gesla za pametno kartico DATAKEY 330.....	22
2.4	Določitev gesla za pametno kartico GEMALTO IDPrime MD 840	23
2.5	Prezem digitalnega potrdila	25
2.6	Inicializacija pametne kartice DATAKEY 330.....	29
2.7	Odklepanje pametne kartice GEMALTO IDPrime MD 840 in ponastavitev pozabljenega gesla	35
3.	Obnova digitalnega potrdila	39
4.	Šifriranje in podpisovanje datotek ter elektronskih sporočil.....	43
4.1	Digitalno podpisovanje elektronskih sporočil v Outlooku 2010	43
4.2	Šifriranje elektronskih sporočil v Outlooku 2010.....	44
4.3	Šifriranje in podpisovanje elektronskih sporočil v Outlooku 2010	44
4.4	Šifriranje in podpisovanje datotek.....	45

1. Namestitev strojne in programske opreme

Za uporabo digitalnih potrdil v okviru infrastrukture javnih ključev na MO je potrebno na delovno postajo namestiti namensko strojno in programsko opremo v sledečem vrstnem redu:

- čitalec pametnih kartic s pripadajočim gonilnikom,
- program za podporo pametne kartice,
- program za upravljanje z digitalnimi potrdili in digitalno podpisovanje ter šifriranje datotek.

Namestitveni programi so dostopni na spletni strani v internem omrežju MO <http://www.simod-pki.mors.si/index.php?id=36>, *Infrastruktura javnih ključev SIMoD-PKI, Prezem in uporaba digitalnih potrdil*:

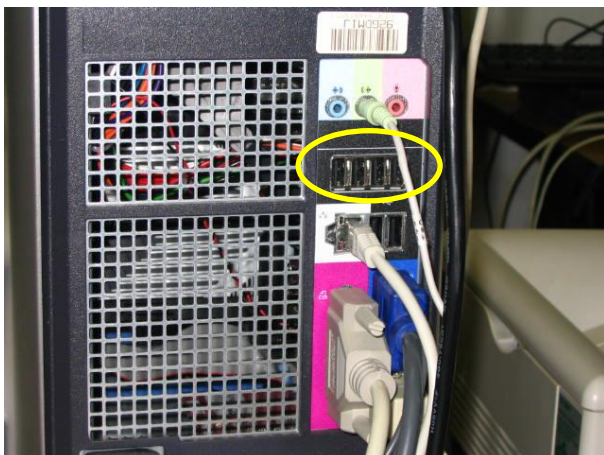
The screenshot shows a web browser window displaying the website 'Infrastruktura javnih ključev SIMoD-PKI'. The page is titled 'Prezem in uporaba digitalnih potrdil' and is part of the 'Izdajatelj SIMoD-CA-Restricted' section. The main content area is titled 'Prezem in uporaba digitalnih potrdil za fizične osebe'. It provides instructions for downloading and installing digital certificates and software. The instructions are organized into sections: 'Namestitveni programi za potrdila za fizične osebe', 'Gonilniki za čitalec pametnih kartic', 'Podpora za pametne kartice DATAKEY 330 in GEMALTO IDPrime MD 840:', 'Podpora za pametne kartice DATAKEY 330:', 'Podpora za pametne kartice GEMALTO .NET:', and 'Programska oprema za upravljanje z digitalnimi potrdili:'. Each section lists specific software and drivers with their respective versions and file formats. A footer note mentions that the installation process is detailed in a PDF document available on the website.

Za namestitev opreme so potrebne administratorske pravice na delovni postaji (administrator ali admin). Uporabniki zato za namestitev kontaktirajte Storitveni center oziroma lokalno informacijsko podporo. To navodilo predvideva uporabo programske in strojne opreme v okolju Windows 7 in sporočilni sistem Outlook 2010.

1.1 Namestitev čitalca pametnih kartic

Čitalec pametnih kartic je zunanja računalniška enota, ki se priključi na USB vhod. Na delovnih postajah z operacijskim sistemom WIN 7 predhodno nameščanje gonilnikov praviloma ni potrebno, ker so le ti že nameščeni.

Priključite čitalec pametnih kartic na prosto USB vtičnico računalnika:

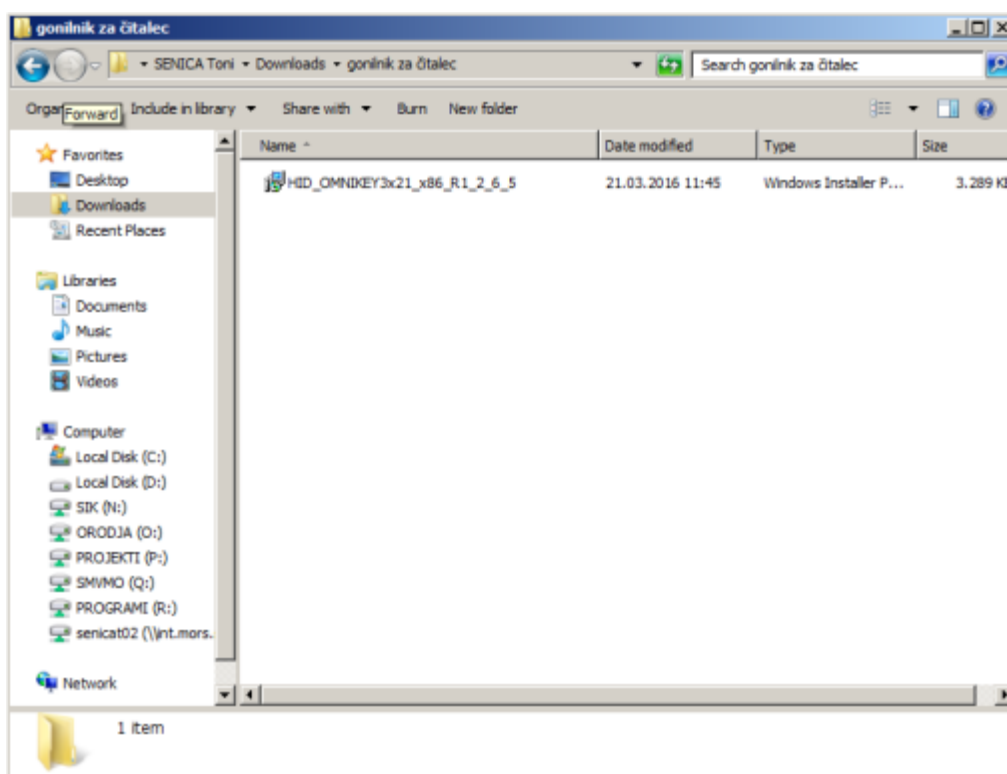


Če operacijski sistem ob priključitvi čitalca pametnih kartic le tega ne zazna oziroma ne namesti ustreznega gonilnika, ga namestite sami.

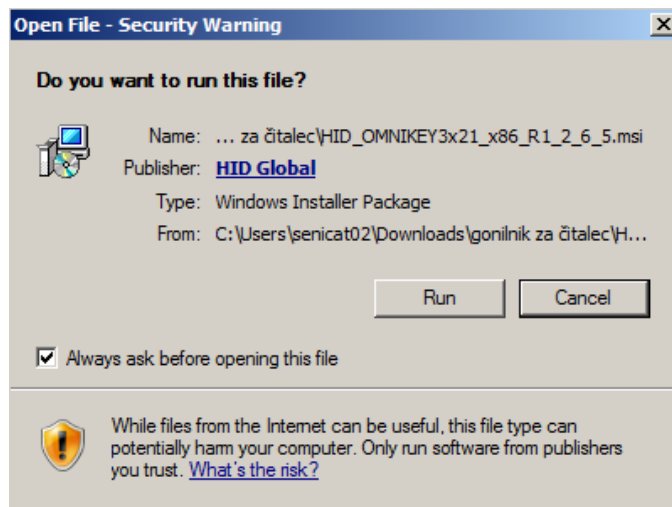
Namestitveni program prenesite s spletne strani <http://www.simod-pki.mors.si/index.php?id=36>, *Infrastruktura javnih ključev SIMoD-PKI, Prezem in uporaba digitalnih potrdil*. Tam se nahaja tudi mapa, ki vsebuje zbirko gonilnikov za različne čitalce pametnih kartic.

Izberite ustrezen gonilnik za vaš čitalec. Nekateri čitalci imajo oznako na sprednji strani (npr. DKR 730), nekateri pa na hrbtni strani. Za primer vzemimo čitalec proizvajalca Omnikey, ki ima na hrbtni strani oznako CardMan 3121. Ustrezen gonilnik zanj je "HID_OMNIKEY3x21_x86_R1_2_6_5". Prenesite ga na delovno postajo. Pred nameščanjem gonilnika zaprite vsa ostala okna.

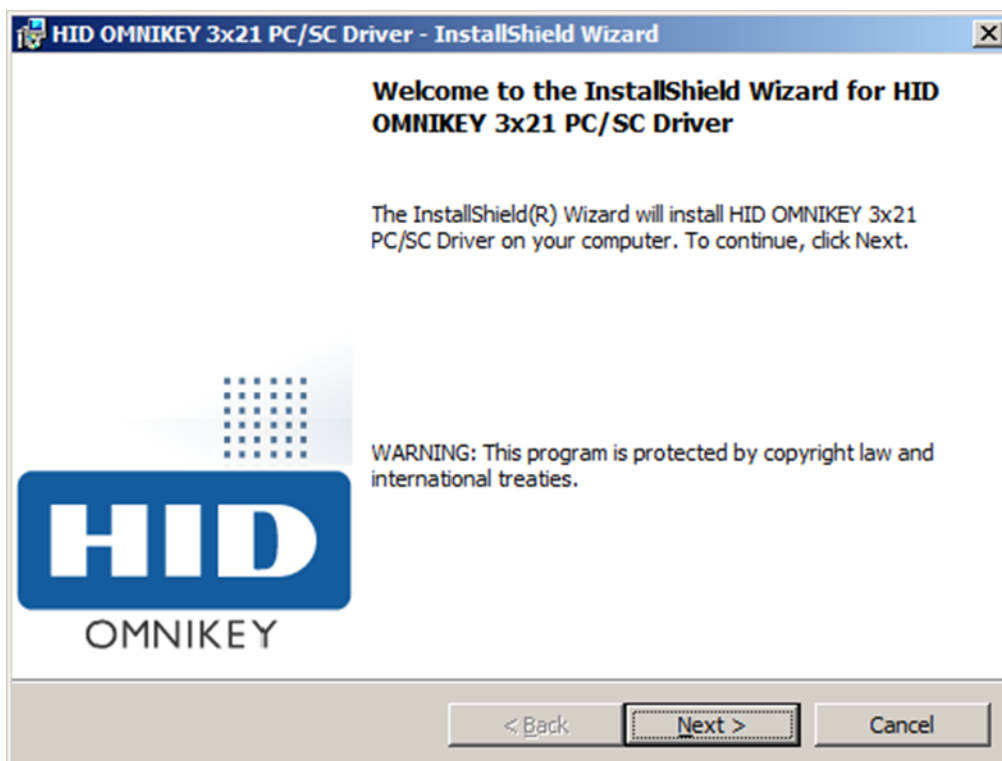
Z dvojnim klikom po imenu datoteke se bo sprožila namestitev gonilnika:



Program vpraša, če res želite zagnati namestitev gonilnika. Potrdite s klikom na "RUN":



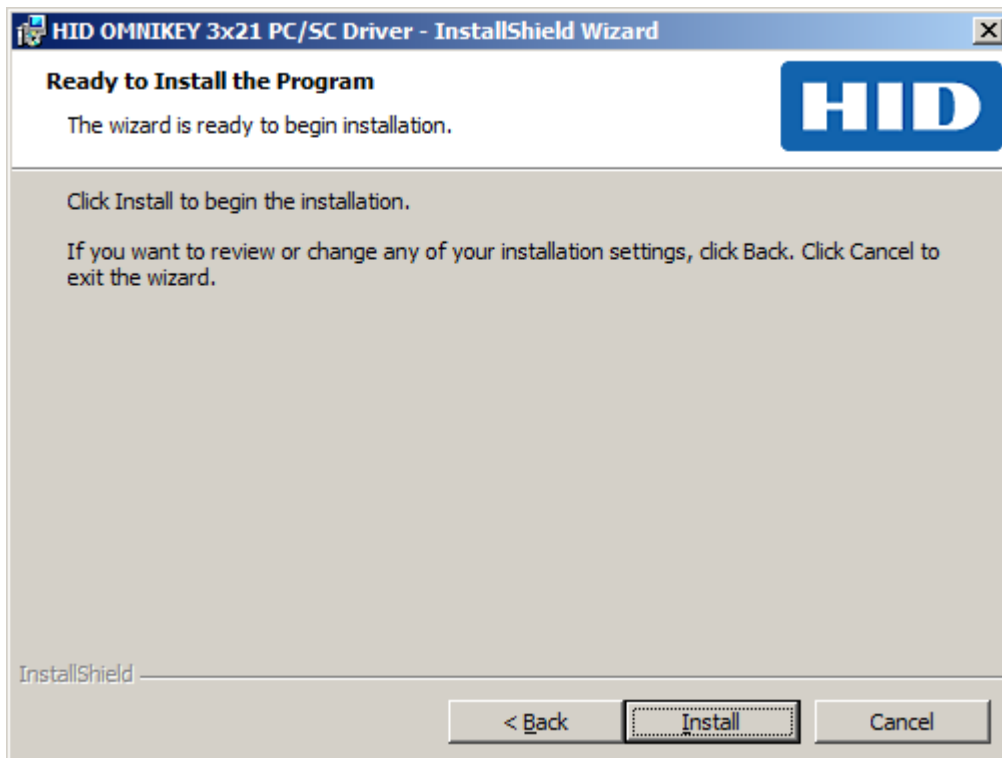
Sledite postopku namestitve gonilnika za čitalec pametnih kartic. Kliknite "Next >":



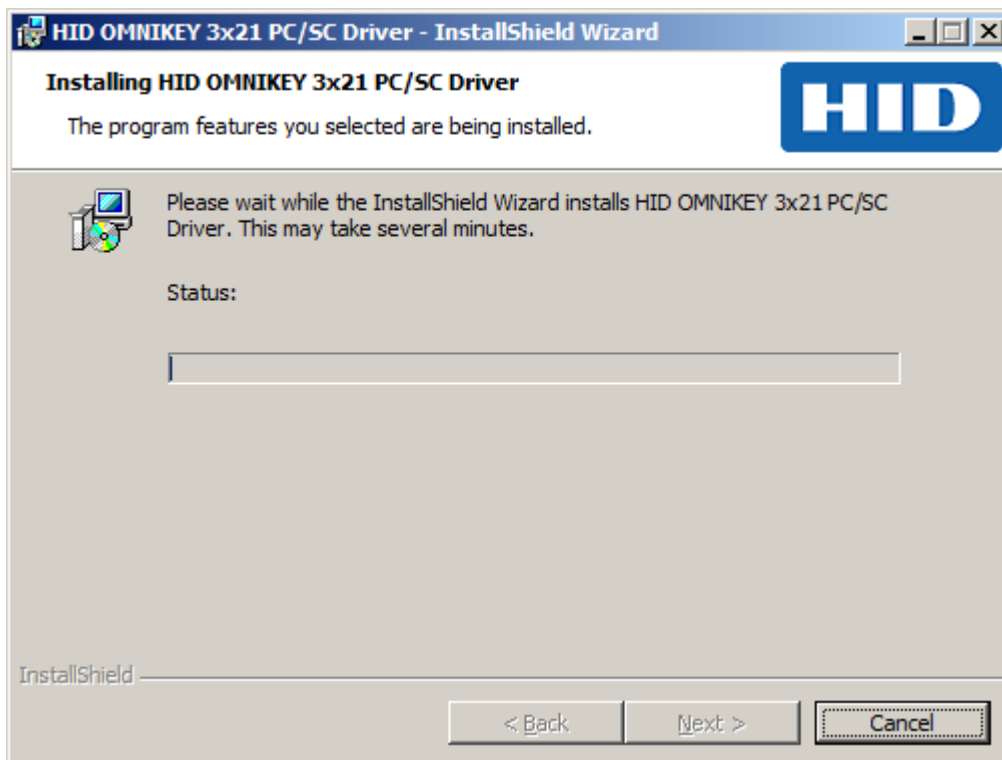
Potrdite licenčno izjavo in kliknite "Next >":



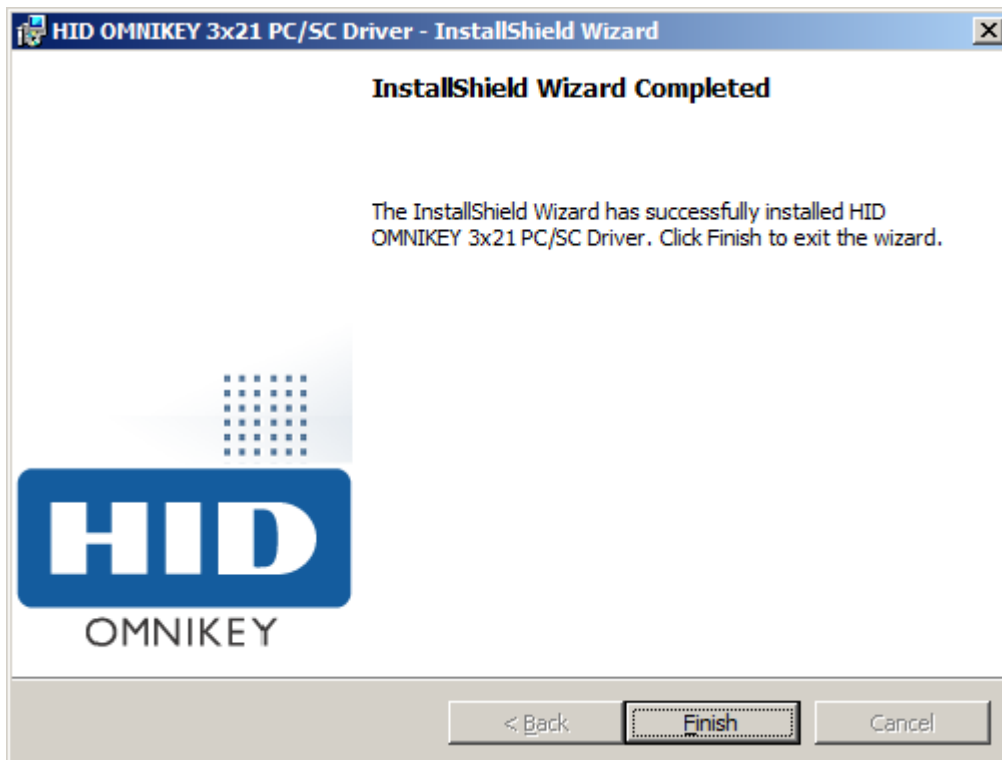
Za namestitev gonilnika za čitalec pametnih kartic kliknite "Install":



Počakajte, da se namestitev konča:

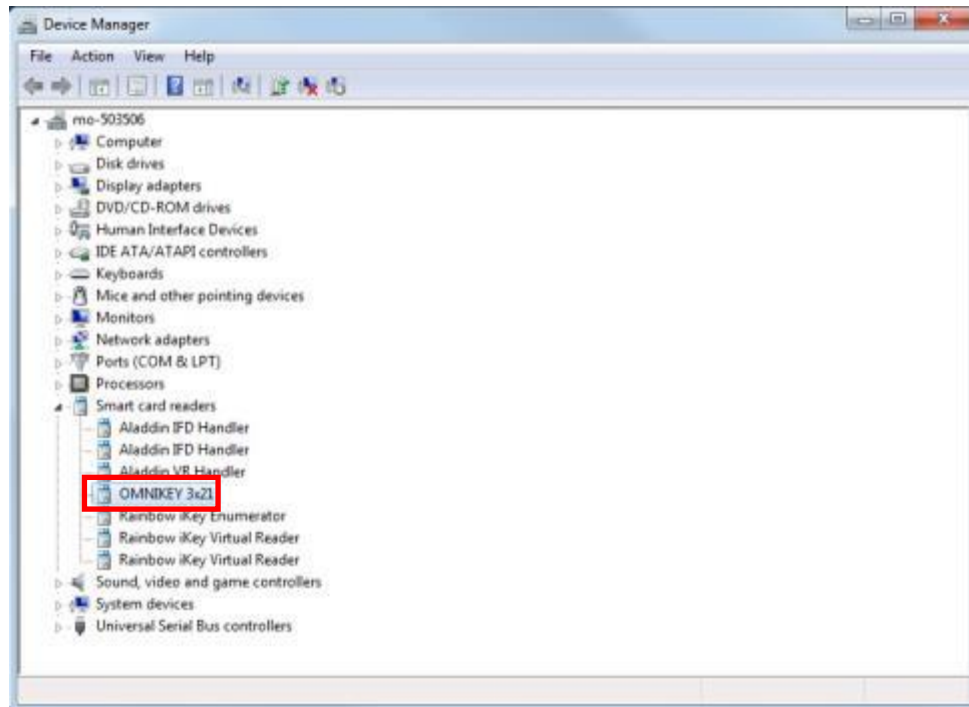


S klikom na "Finish" zaključite nameščanje gonilnika za čitalec pametnih kartic:



Če je bila namestitev gonilnika in čitalca pametnih kartic pravilna, bo na čitalcu zasvetila zelena luč.

Priporočljivo je, da namestitev gonilnika preverite tudi v sistemskih nastavitvah. Pojdite v meni Start, desno kliknite "Control Panel", nato "Hardware and Sound", v skupini "Devices and Printers" dalje kliknite " Device Manager ". Ustrezno nameščen gonilnik je uvrščen na seznam vseh gonilnikov brez opozorilnih oznak.



1.2 Namestitev programa za podporo pametne kartice SafeNet Authentication Client

V tem poglavju je opisana namestitev programske opreme SafeNet Authentication Client 10.4 za podporo pametni kartici:



- DATAKEY CIP 330 (starejše): ,
- GEMALTO IDPrime MD 840 (nove)

OPOMBA: Nekaj uporabnikov ima pametne kartice GEMALTO IDPrime .NET 510. Pametna kartica GEMALTO IDPrime .NET 510 za svoje delovanje potrebuje mini gonilnik *IDGo800*.

Na računalnikih, kjer se bo uporabljala samo kartica GEMALTO IDPrime .NET 510, namestite samo *IDGo800*, ne nameščati *SafeNet Authentication Client*. Na računalnikih, ki jih uporablja več ljudi, ki imajo bodisi kartice DATAKEY ali GEMALTO IDPrime MD 840 bodisi GEMALTO IDPrime .NET 510, je potrebno namestiti *SafeNet Authentication Client* in *IDGo800* on sicer v vrstnem redu najprej *SafeNet Authentication Client* nato *IDGo800*.

Za upravljanje s pametno kartico GEMALTO IDPrime .NET 510, kot sta npr. operaciji menjave gesla ali pregled vsebine pametne kartice, je potreben izvršljiv program *Gemalto.NETTool.exe*. Uporabniku program *Gemalto.NETTool.exe* enostavno prenesite na namizje ali v želeni imenik.

Program SafeNet Authentication Client 10.4 deluje kot programski vmesnik (ang. middleware) med pametno kartico in aplikacijami, ki uporabljajo digitalna potrdila. Poskrbi, da so digitalna potrdila na pametni kartici objavljena v skladišču digitalnih potrdil operacijskega sistema (MS Certificate Store), od koder jih črpajo aplikacije. Program omogoča tudi nastavitev in spremembo uporabniškega gesla za aktivacijo pametne kartice ter inicializacijo pametne kartice.

Program SafeNet Authentication Client 10.4 se nahaja na spletni strani <http://www.simod-pki.mors.si/index.php?id=36>, *Infrastruktura javnih ključev SIMoD-PKI, Prezem in uporaba digitalnih potrdil*.

Namestitev zaženite s klikom na verzijo, ki ustreza vašemu operacijskemu sistemu (običajno 32 bit) in potrdite s klikom na "Run":

The screenshot shows a web browser window displaying the website for the Ministry of Defense of the Republic of Slovenia, specifically the SIMoD-PKI infrastructure. The page is titled "Prezvem in uporaba digitalnih potrdil" (Download and use digital certificates). It provides instructions for physical users, including a list of software programs to be installed. A file named "SAC_29AVG17-x32-10.4.msi" (10.8 MB) is being downloaded from "simod-pki.mors.si". A dialog box asks if the user wants to run or save the file, with the "Run" button highlighted.

Prezvem in uporaba digitalnih potrdil - Windows Internet Explorer by SIK
http://www.simod-pki.mors.si/index.php?id=36

Republika Slovenija Ministrstvo za obrambo
Infrastruktura javnih ključev SIMoD-PKI

SIMoD-PKI > Izdajatelj SIMoD-CA-Restricted > Prezvem in uporaba digitalnih potrdil

Izdajatelj SIMoD-CA-Root
Izdajatelj SIMoD-CA-Restricted

Prezvem in uporaba digitalnih potrdil za fizične osebe

Za prevzem digitalnega potrdila za fizično osebo potrebujete referenčno številko in avtorizacijsko kodo. Referenčno številko ste prejeli po elektronski pošti, avtorizacijsko kodo pa skupaj s pametno kartico v kuverti po pošti. Pred pričetkom uporabe je potrebno na delovno postajo namestiti čitalec pametnih kartic in programsko opremo in sicer v naslednjem vrstnem redu:

- čitalec pametnih kartic z gonilnikom,
- program za upravljanje z uporabniškimi parametri pametne kartice (*SafeNet Authentication Client* ali *GemaltoNet.Tool*) in
- program za upravljanje z digitalnimi potrdili, podpisovanje in šifriranje datotek (*Entrust Enhanced Security Provider*).

Za namestitev programske opreme so potrebne administratorske pravice na delovni postaji. Namestitvene programe v komprimirani obliki prenesite na delovno postajo, jih dekomprimirajte in namestite.

Namestitveni programi za potrdila za fizične osebe

Gonilniki za čitalec pametnih kartic:

- DKR 730 za Win XP
- Omnikey 3121 za Win XP
- DKR 730 - ZIP za Win7 32 bit (preberi [navodilo za namestitev](#))
- Omnikey 3121 za Win7 32 bit
- Omnikey 3121 za Win7 64 bit
- Gemalto

Podpora za pametne kartice DATAKEY 330 in GEMALTO IDPrime MD 840:

- Safenet Authentication Client 10.4 32 bit 29AVG17 **NOVO**
- Safenet Authentication Client 10.4 64 bit 29AVG17 **NOVO**

Podpora za pametne kartice DATAKEY 330:

- Safenet Authentication Client 10.0 32 bit 10AVG16
- Safenet Authentication Client 10.0 64 bit 10AVG16
- Safenet Borderless Security 7.3

Podpora za pametne kartice GEMALTO .NET:

- IDGo800 - minidriver 32 bit

Do you want to run or save SAC_29AVG17-x32-10.4.msi (10,8 MB) from simod-pki.mors.si?

This type of file could harm your computer.

Run Save Cancel

Ignorirajte varnostno opozorilo, kliknite »Run«:

The screenshot shows a Windows security warning dialog box. The text reads: "The publisher of SAC_29AVG17-x32-10.4.msi couldn't be verified. Are you sure you want to run the program?". There are two buttons: "Run" and "View downloads".

The publisher of SAC_29AVG17-x32-10.4.msi couldn't be verified. Are you sure you want to run the program?

Run View downloads

Sledite postopku namestitvenega programa. Kliknite "Next >":



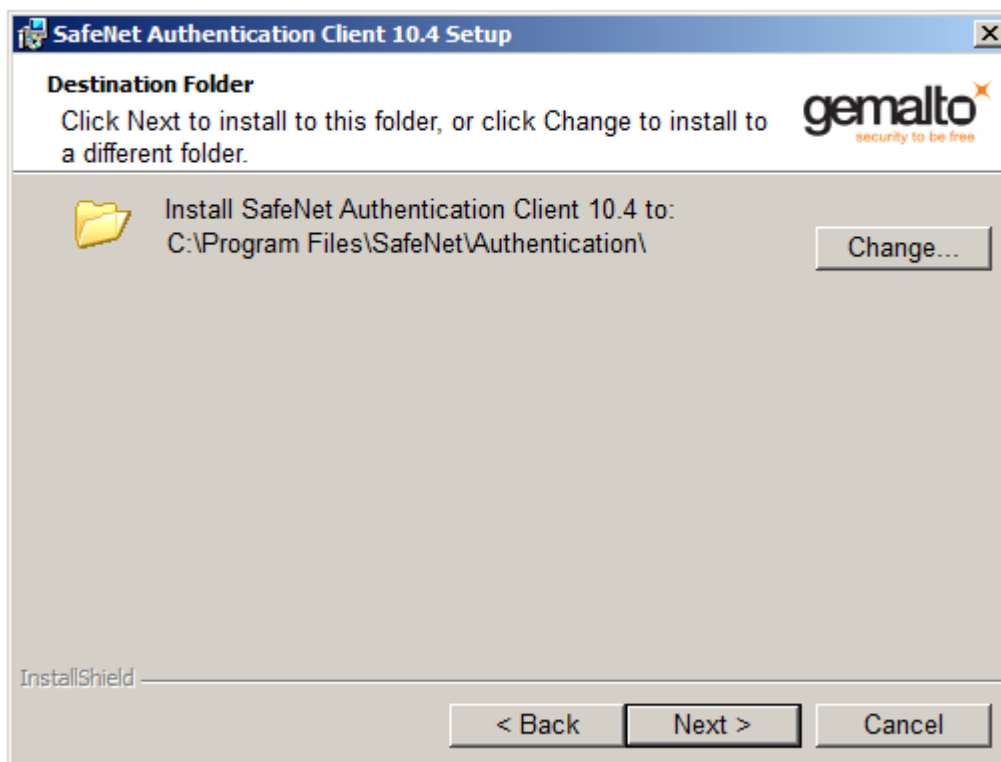
Izberete žaljani jezik. Kliknite "Next >":



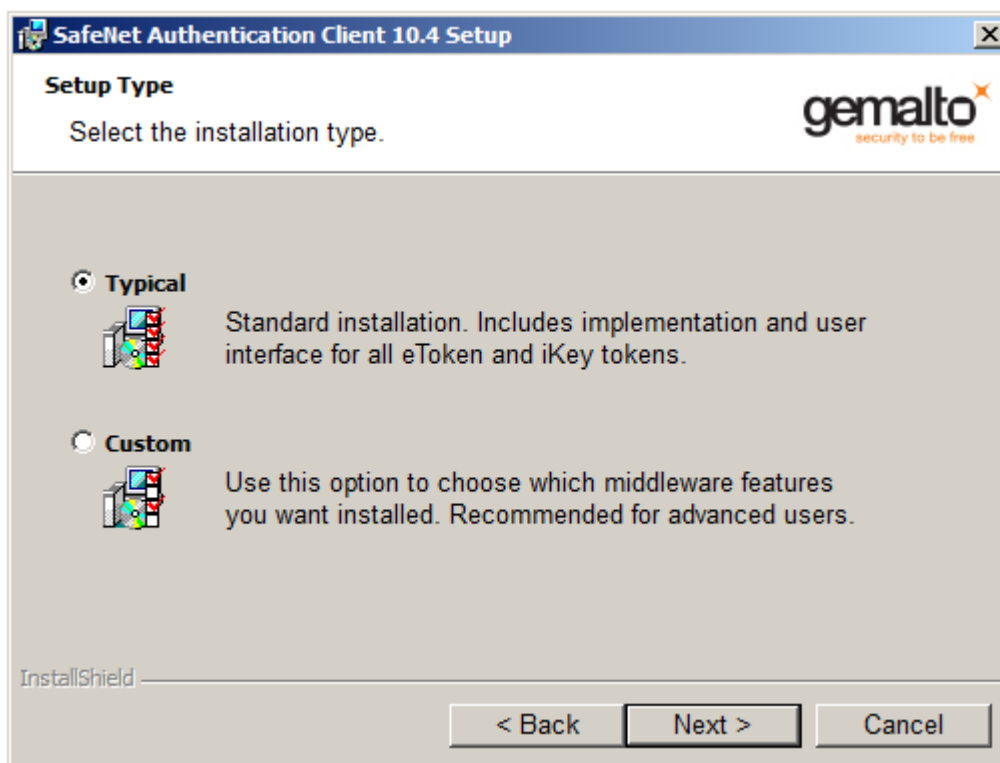
Potrdite licenčno izjavo in kliknite "Next >":



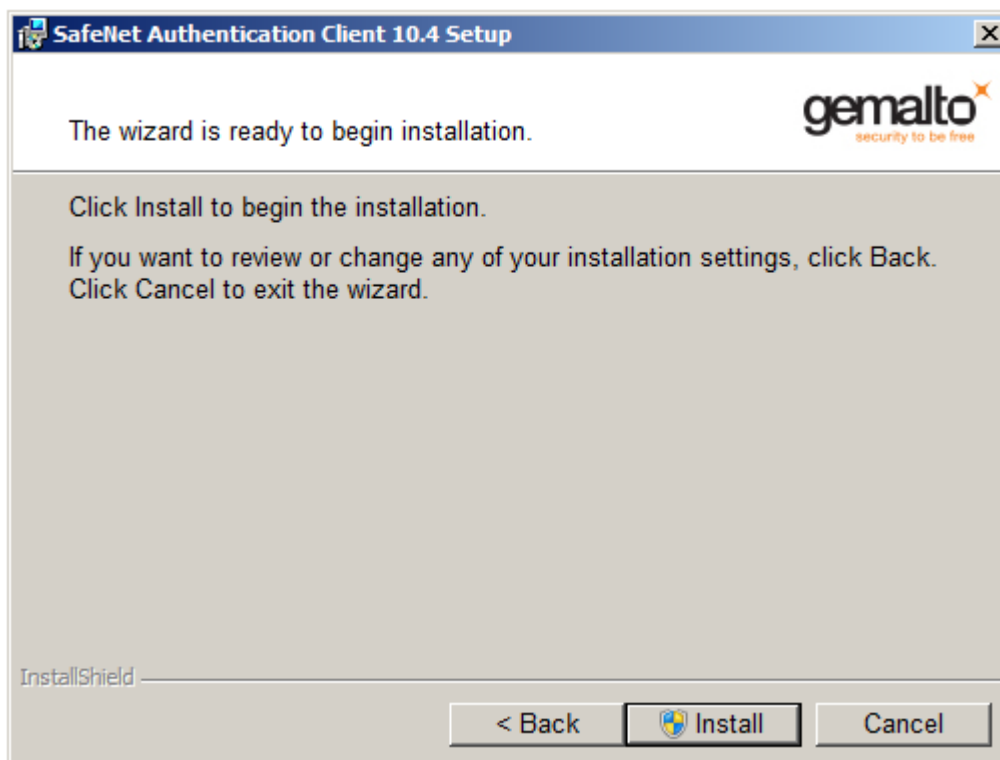
Potrdite privzeto namestitveno mapo "c:\Program Files\SafeNet\Authentication\" s klikom na "Next >":



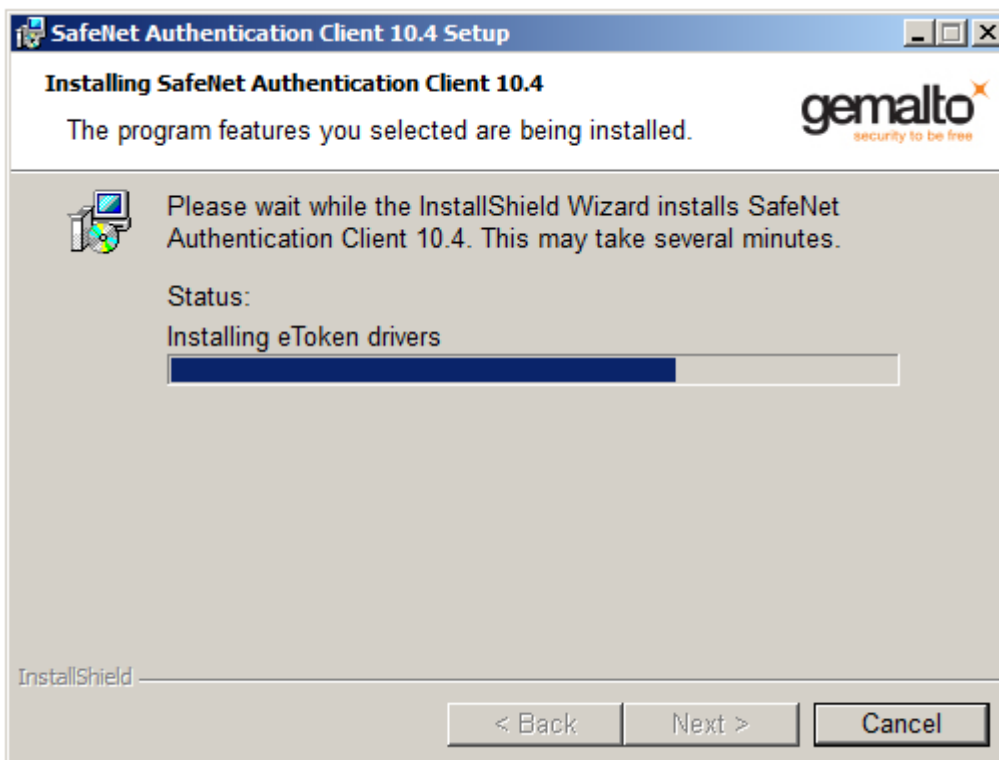
Potrdite način namestitve »Typical«, kliknite »Next>«:



Potrdite začetek namestitve, kliknite »Install«:



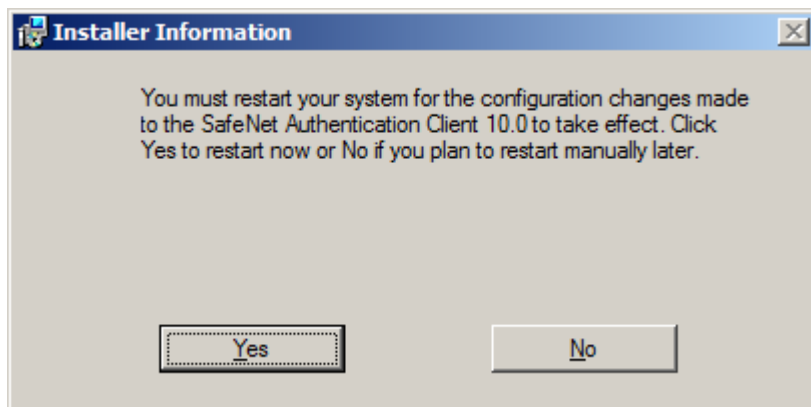
Sledijo okna z obvestili o poteku namestitve. Počakajte, da se namestitev konča:



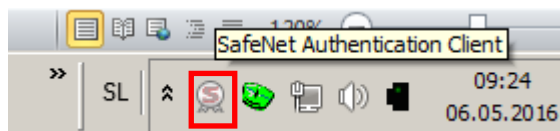
S klikom "Finish" zaključite nameščanje:



Potrdite poziv k ponovnemu zagonu računalnika, kliknite »Yes«:



Po namestitvi se v orodni vrstici pojavi nova ikono z imenom " SafeNet Authentication Client":



Do programa pridete tudi z zaporednimi kliki na "Start", "All Programs", "SafeNet" in " SafeNet Authentication Client ".

1.3 Namestitev programa za upravljanje z digitalnimi potrdili Entrust Entelligence Security Provider

Entrust Entelligence Security Provider je program za upravljanje z digitalnimi potrdili. Omogoča prevzem digitalnih potrdil (Entrust Entelligence, Enroll for Entrust Digital ID), obnovo digitalnih potrdil (Entrust Entelligence, Recover for Digital ID) in avtomatsko ponovno izdajo digitalnih potrdil (Entrust Digital ID Update).

Vsebuje tudi iskalnik digitalnih potrdil (Entrust Entelligence, Entrust Certificate Explorer) in orodje za šifriranje in digitalno podpisovanje datotek.

Namestitev programa zaženemo s klikom na " Entrust Enhanced Security Provider X.X¹"; glede na vrsto operacijskega sistema izberemo 32-bitno ali 64-bitno verzijo:



The screenshot shows a web browser window displaying the website for the Ministry of Defense of the Republic of Slovenia, specifically the SIMoD-PKI infrastructure page. The page is titled "Izdajatelj SIMoD-CA-Restricted" and provides information about digital certificates and software for physical users. A red box highlights the download links for the Entrust Enhanced Security Provider software, including versions for 32-bit and 64-bit systems.

Izdajatelj SIMoD-CA-Restricted

Prezem in uporaba digitalnih potrdil za fizične osebe

Za prevzem digitalnega potrdila za fizično osebo potrebujete referenčno številko in avtorizacijsko kodo. Referenčno številko ste prejeli po elektronski pošti, avtorizacijsko kodo pa skupaj s pametno kartico v kuverti po pošti. Pred pričetkom uporabe je potrebno na delovno postajo namestiti čitalec pametnih kartic in programsko opremo in sicer v naslednjem vrstnem redu:

- čitalec pametnih kartic z gonilnikom,
- program za upravljanje z uporabniškimi parametri pametne kartice (*SafeNet Authentication Client* ali *GemaltoNet.Tool*) in
- program za upravljanje z digitalnimi potrdili, podpisovanje in šifriranje datotek (*Entrust Enhanced Security Provider*).

Za namestitev programske opreme so potrebne administratorske pravice na delovni postaji. Namestitvene programe v komprimirani obliki prenesite na delovno postajo, jih dekomprimirajte in namestite.

Namestitveni programi za potrdila za fizične osebe

Gonilniki za čitalec pametnih kartic:

- ▶ [DKR 730](#) za Win XP
- ▶ [Omnikey 3121](#) za Win XP
- ▶ [DKR 730](#) - ZIP za Win7 32 bit (preberi [navodilo za namestitve](#))
- ▶ [Omnikey 3121](#) za Win7 32 bit
- ▶ [Omnikey 3121](#) za Win7 64 bit
- ▶ [Gemalto](#)

Podpora za pametne kartice DATAKEY 330 in GEMALTO IDPrime MD 840:

- ▶ [SafeNet Authentication Client](#) 10.4 32 bit 29AVG17 **NOVO**
- ▶ [SafeNet Authentication Client](#) 10.4 64 bit 29AVG17 **NOVO**

Podpora za pametne kartice DATAKEY 330:

- ▶ [SafeNet Authentication Client](#) 10.0 32 bit 10AVG16
- ▶ [SafeNet Authentication Client](#) 10.0 64 bit 10AVG16
- ▶ [SafeNet Borderless Security](#) 7.3

Podpora za pametne kartice GEMALTO .NET:

- ▶ [IDGo800](#) - minidriver 32 bit
- ▶ [IDGo800](#) - minidriver 64 bit
- ▶ [MS Base Smart Card Crypto Provider](#) za Win XP
- ▶ [GemaltoNet.Tool.exe](#) (preberi [opombe](#))

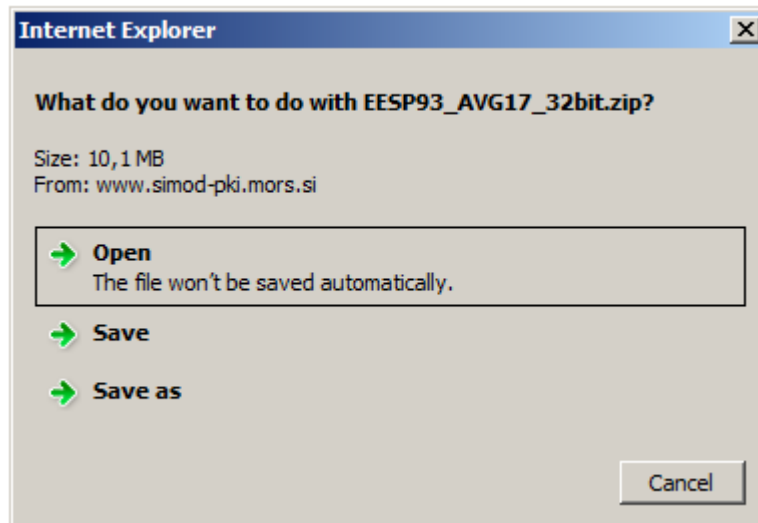
Programska oprema za upravljanje z digitalnimi potrdili:

- ▶ [Entrust Enhanced Security Provider](#) 9.3 ZIP 32 bit 31AVG17 **NOVO**
- ▶ [Entrust Enhanced Security Provider](#) 9.3 ZIP 64 bit 31AVG17 **NOVO**
- ▶ [Entrust Enhanced Security Provider](#) 9.3 ZIP 32 bit
- ▶ [Entrust Enhanced Security Provider](#) 9.3 ZIP 64 bit
- ▶ [Entrust Enhanced Security Provider](#) 9.2 ZIP 32 bit
- ▶ [Entrust Enhanced Security Provider](#) 9.2 ZIP 64 bit

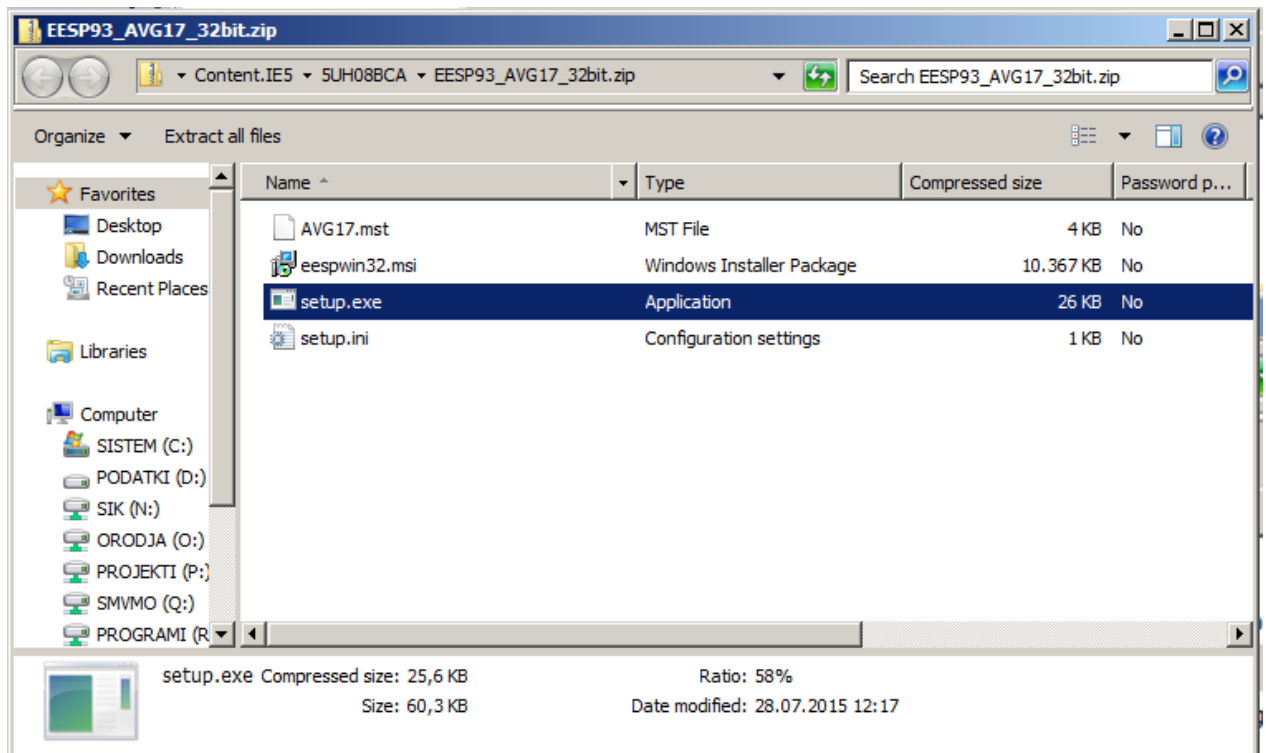
Za pomoč pri namestitvi se obrnite na **storitveni center**. Postopek namestitve čitalca pametnih kartic in programske opreme, postopek prevzema in nekateri načini uporabe digitalnega potrdila za fizične osebe so opisani v [Navodilu za uporabnike digitalnih potrdil - PDF](#).

¹ Praviloma namestimo zadnjo verzijo programske opreme, objavljeno na spletni strani.

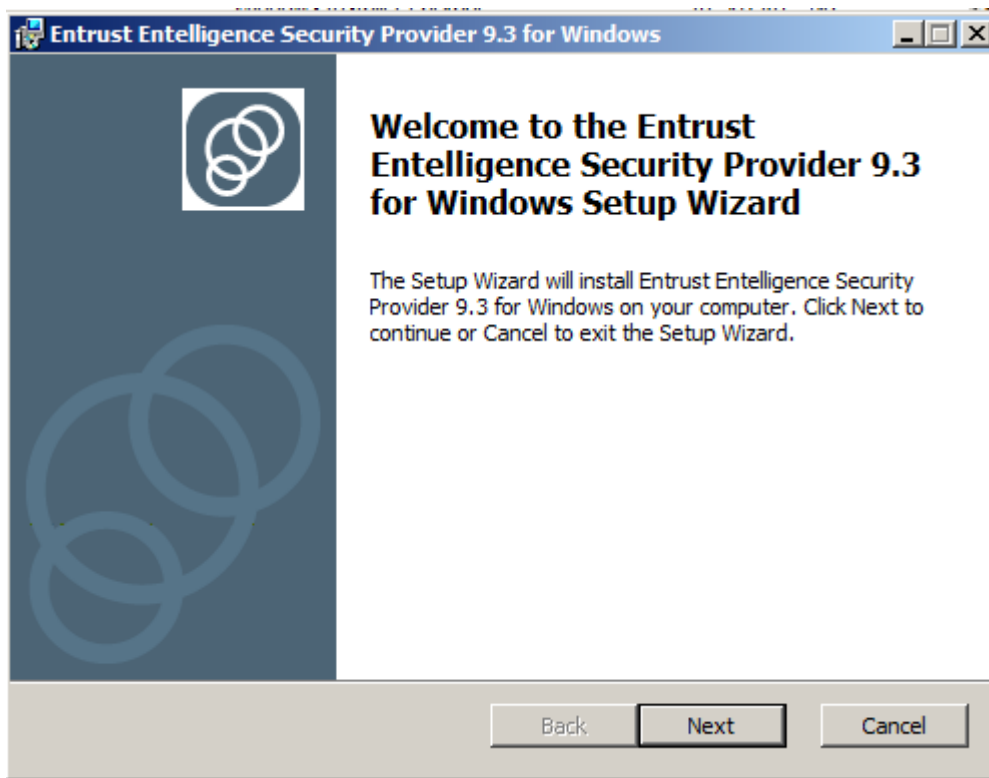
in nato kliknemo "Open":



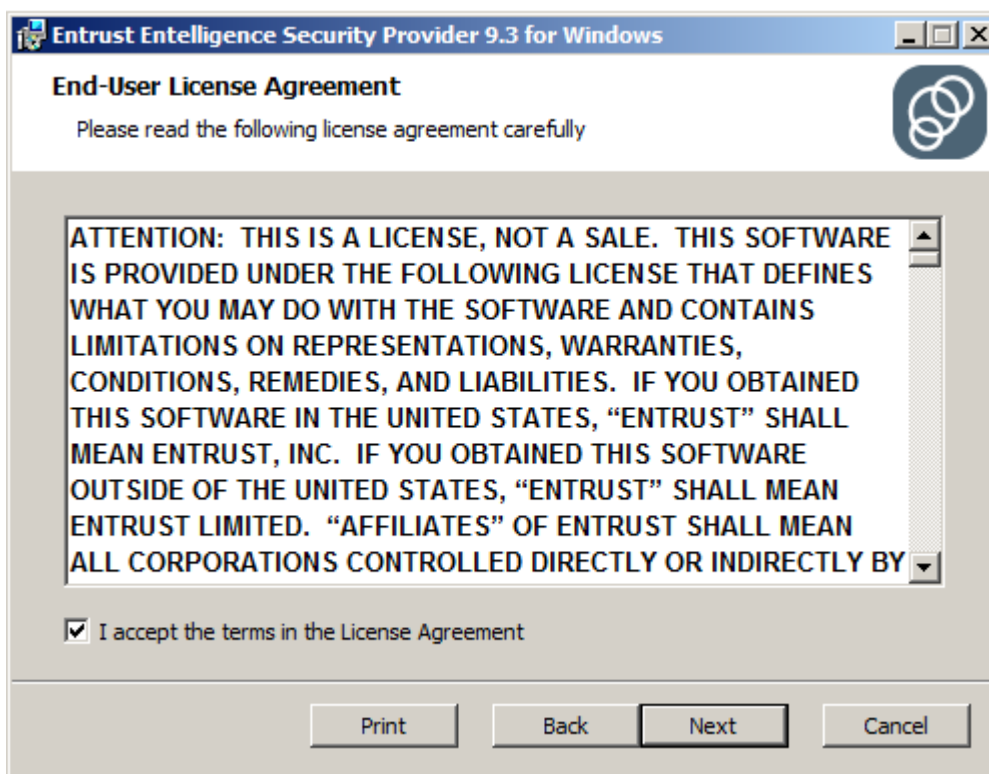
Z dvoklikom na "setup" zaženite nameščanje programa:



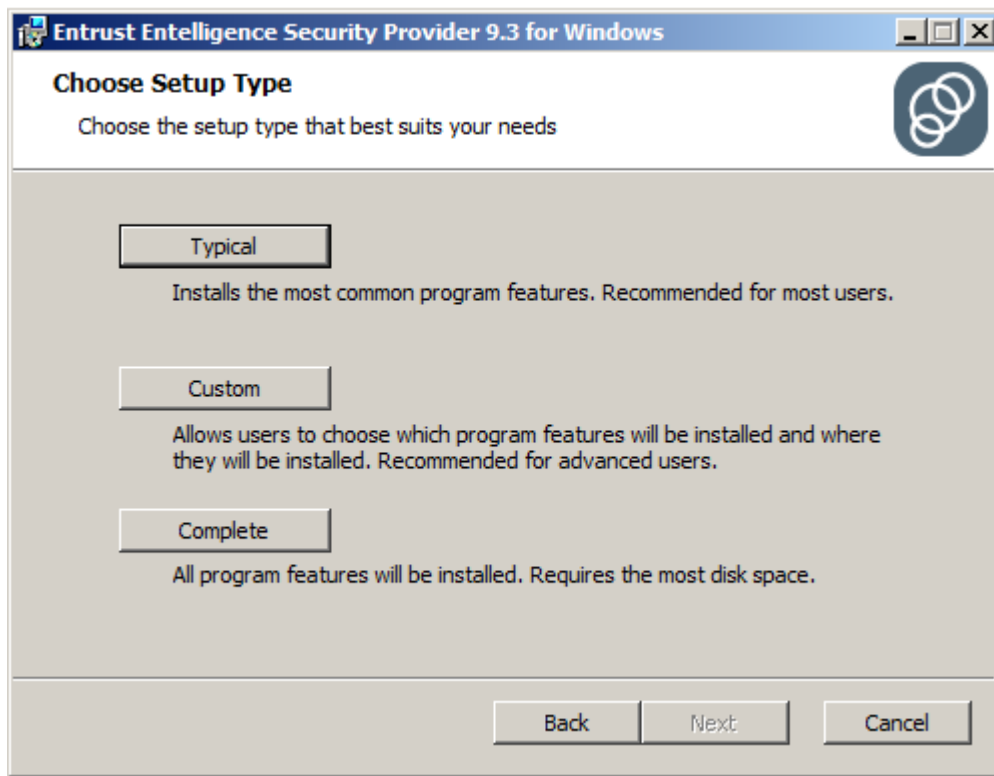
Sledite postopku namestitvenega programa. Kliknite "Next >":



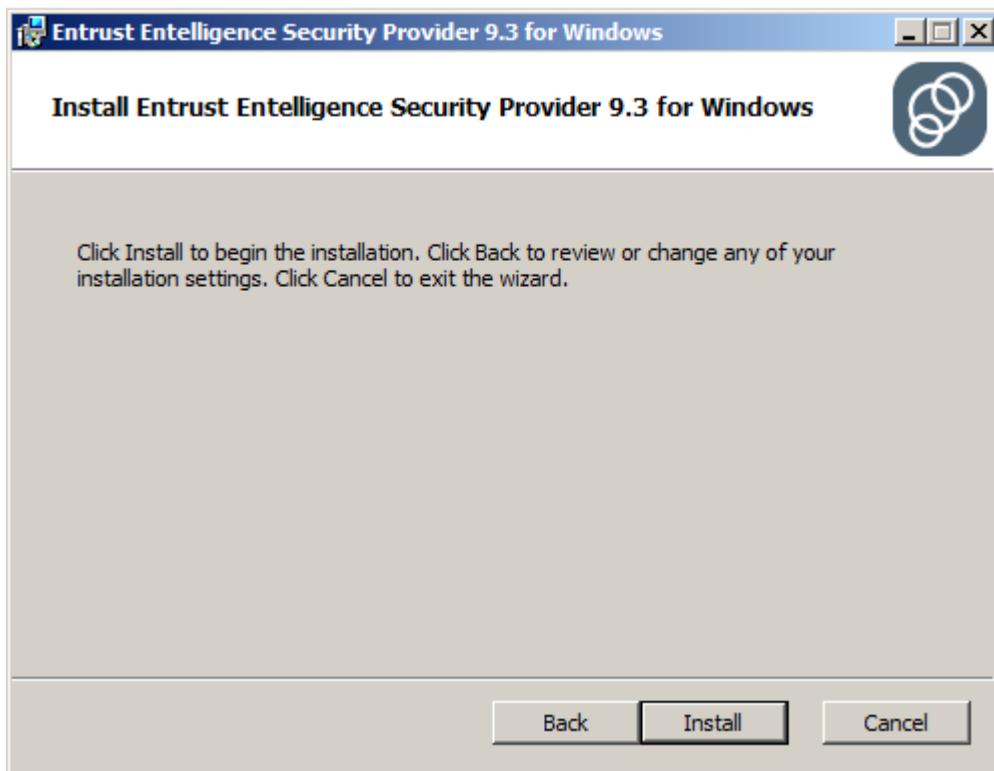
Potrdite licenčno izjavo in kliknite "Next >":



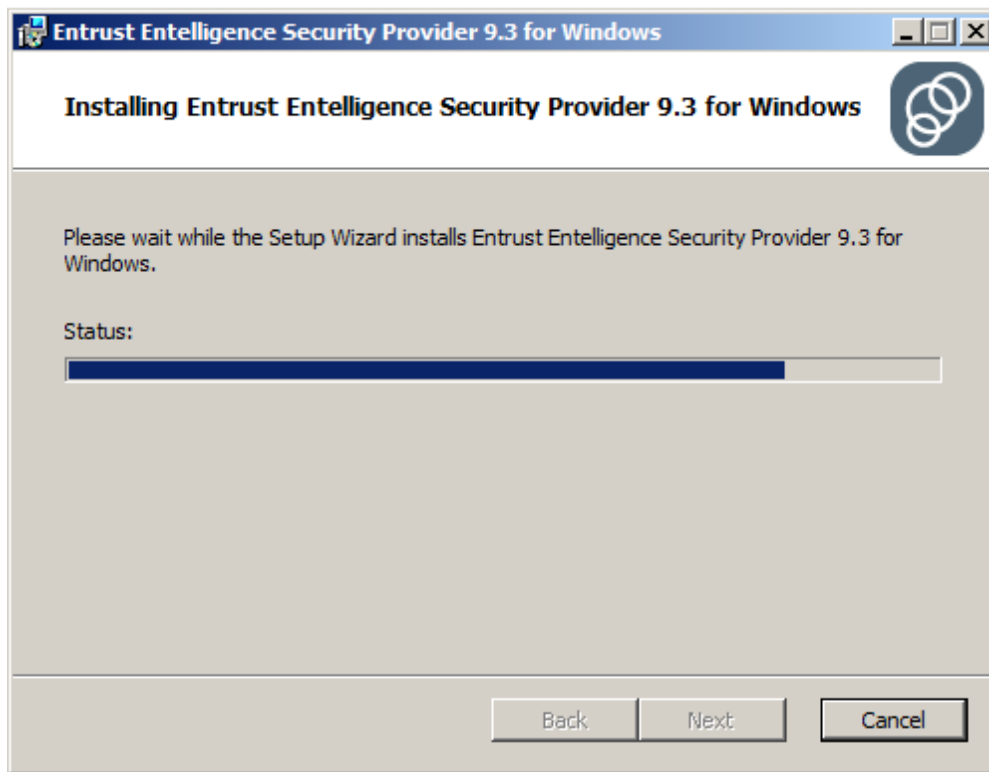
Izberite običajno namestitev "Typical" :



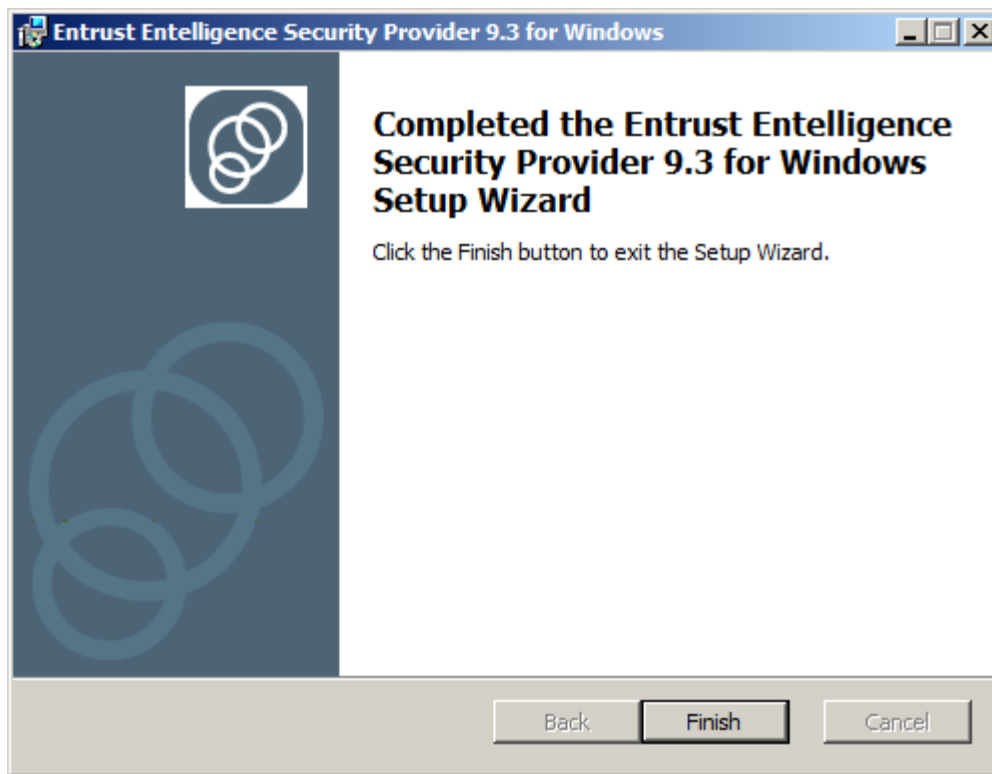
S klikom "Install" boste dejansko sprožili nameščanje programskih datotek:



Počakajte, da se namestitev konča:



ter s klikom "Finish" zaključite nameščanje programa:



2. Prezem digitalnega potrdila

2.1 Preverjanje delovanja čitalca pametne kartice in pametne kartice

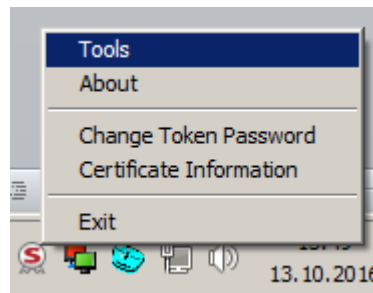
Digitalno potrdilo lahko prevzamete, ko po navadni pošti prejmete avtorizacijsko kodo, po elektronski pošti pa referenčno številko. Prezem digitalnega potrdila mora biti izveden v uporabniškem okolju, to pomeni, da morate imeti na delovni postaji nameščeno namensko programsko opremo iz poglavja 1 Namestitev strojne in programske opreme.

Pametno kartico vstavite v čitalec tako, da je čip obrnjen navzgor. Kartico v režo potisnite do konca. Ko jo čitalec zazna, lučka izmenično utripa zeleno in rdeče (pri nekaterih čitalcih je indikacija lahko drugačna).

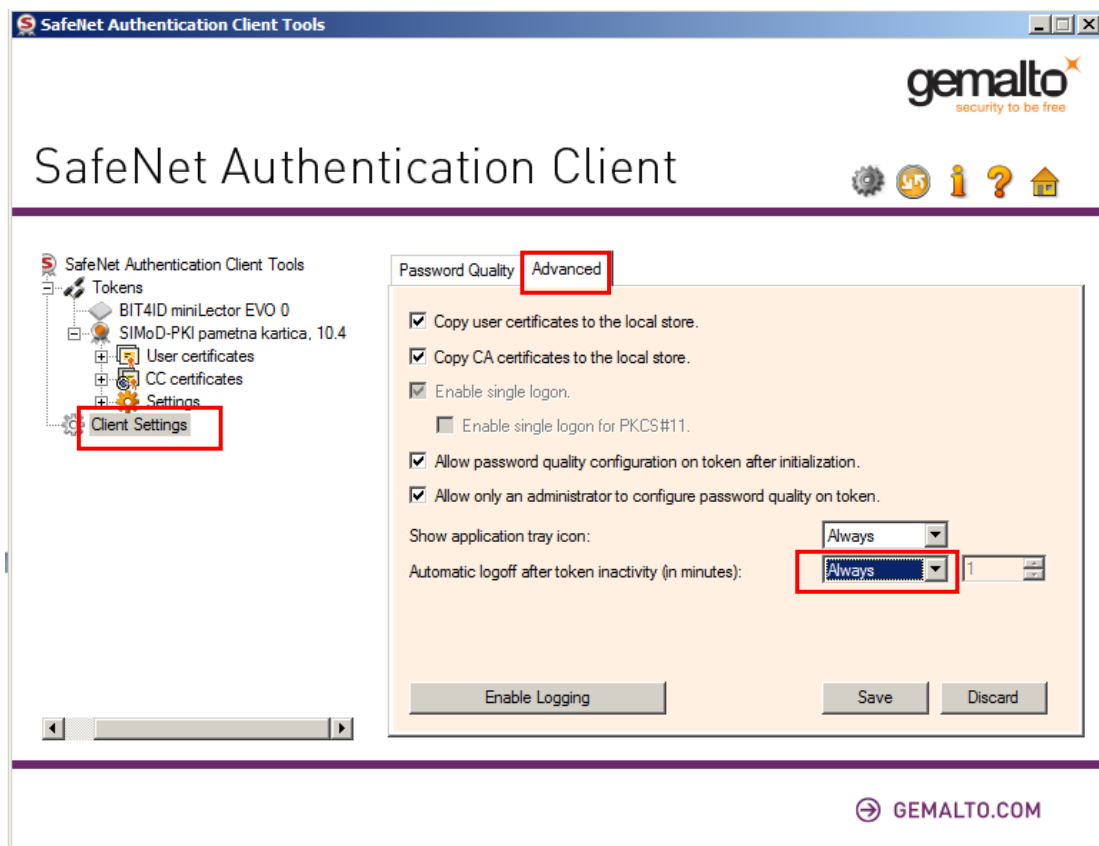


2.2 Pravilna nastavitve programa za podporo pametne kartice SafeNet Authentication Client

Pred prevzemom in uporabo digitalnega potrdila je potrebno preveriti parameter "**SAC, Tools, Client Settings, Advanced, Automatic logoff after token inactivity (in minutes): Always**". To storimo npr. z desnim klikom po ikoni " SafeNet Authentication Client ", " Tools ":

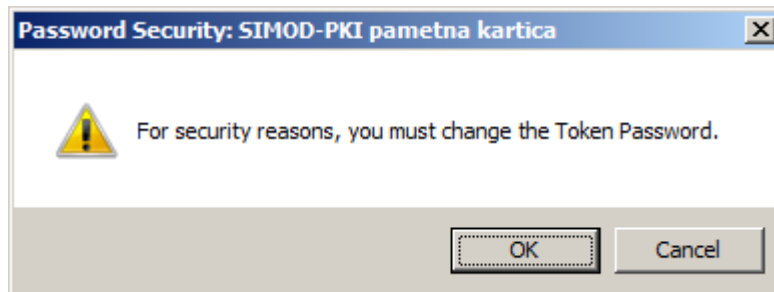


nato kliknemo na "**Client Settings**" in na novem pogledu izberemo zavihek "**Advanced**". Parameter "**Automatic logoff after token inactivity (in minutes)**": mora biti nastavljen na "**Always**". V primeru, da ni nastavljen na "**Always**" parameter nastavimo na "**Always**" in nastavitve shranimo z pritiskom na gumb "**Save**".



2.3 Začetna določitev gesla za pametno kartico DATAKEY 330

Od overitelja digitalnih potrdil na MO ste prejeli inicializirano pametno kartico s privzetim geslom, ki ga morate ob prvi uporabi spremeniti. Ko prvič vstavite pametno kartico v čitalec, se pojavi poziv k spremembi privzetega gesla, kliknite »OK«:



V polje "New Token Password:" vnesite geslo, ki ga boste uporabljali za aktivacijo pametne kartice, potrdite v polju "Confirm Password:". Uporabniško geslo mora zadostiti zahtevam:

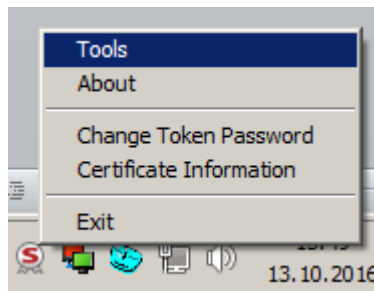
- dolžina mora biti od 8 do 20 znakov,
- vsebovati mora vsaj eno veliko in eno malo črko,
- vsebovati mora vsaj eno število in vsaj en znak.

Kliknite »OK«.

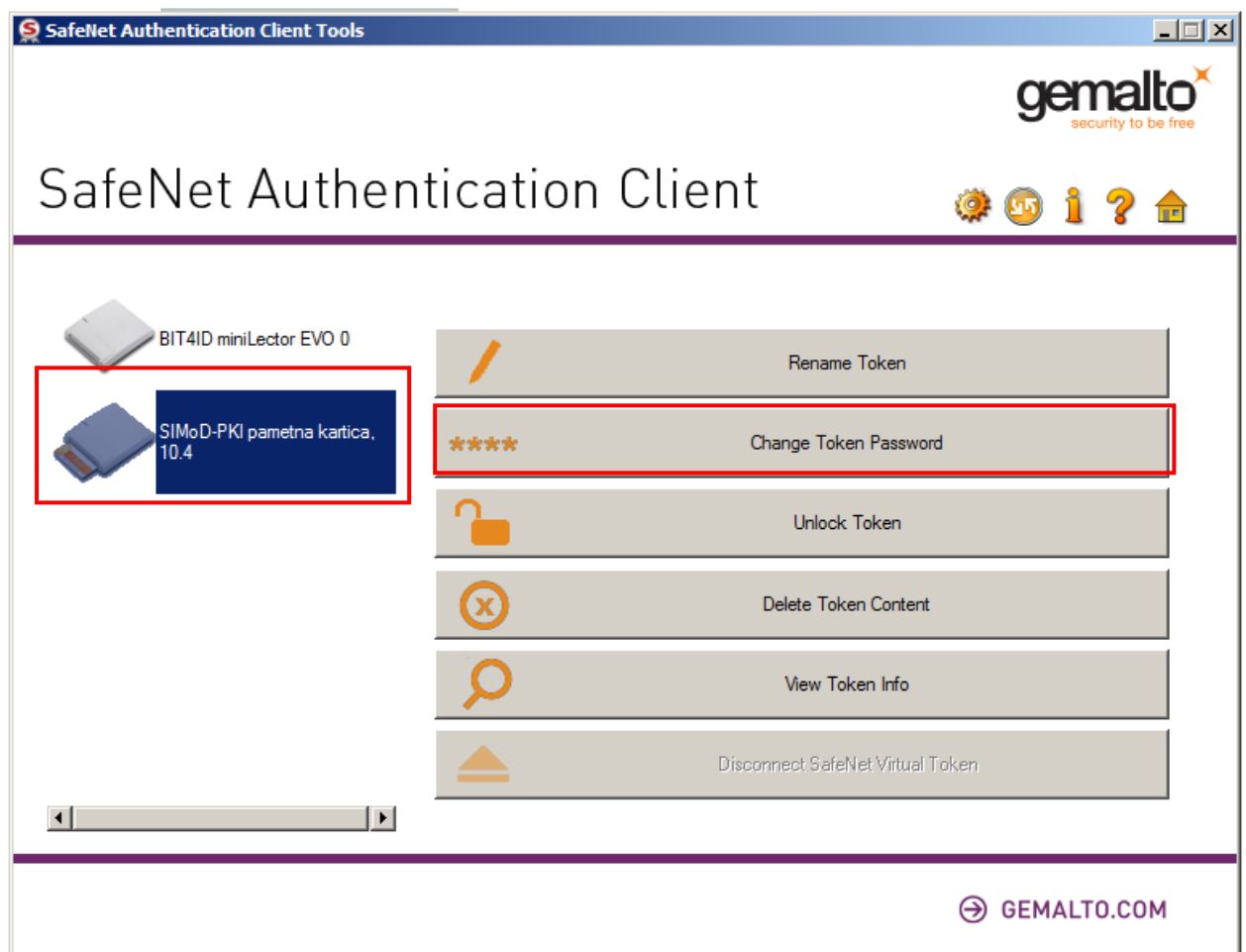
2.4 Določitev gesla za pametno kartico GEMALTO IDPrime MD 840

Od overitelja digitalnih potrdil na MO ste prejeli inicializirano pametno kartico z naključnim geslom, ki ga morate ob prvi uporabi spremeniti.

Do funkcij upravljanja s pametno kartico pridemo z desnim klikom po ikoni " SafeNet Authentication Client " in izberemo "Tools":



Odpre se okno SafeNet Authentication Client. Označite pametno kartico in kliknite »Change Token Password« :



Pojavi se pojavno okno:

Change Password: SIMoD-PKI pametna kartica, 10.4

SafeNet Authentication Client **gemalto**
security to be free

Current Token Password:

New Token Password:

Confirm Password:

The new password must comply with the quality settings defined on the token.

A secure password has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, \$, #, %).

Current Language: **SL**

Enter your current password.

OK Cancel

V polje »**Current Token Password**« vpišite trenutno geslo. V polje "**New Token Password:**" vnesite geslo, ki ga boste uporabljali za aktivacijo pametne kartice. Geslo potrdite v polju "**Confirm Password:**". Zaključimo s klikom na »OK«.

Uporabniško geslo mora biti dolgo vsaj 6 znakov.

Change Password: SIMoD-PKI pametna kartica, 10.4

SafeNet Authentication Client **gemalto**
security to be free

Current Token Password:

New Token Password:

Confirm Password:

The new password must comply with the quality settings defined on the token.

A secure password has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, \$, #, %).

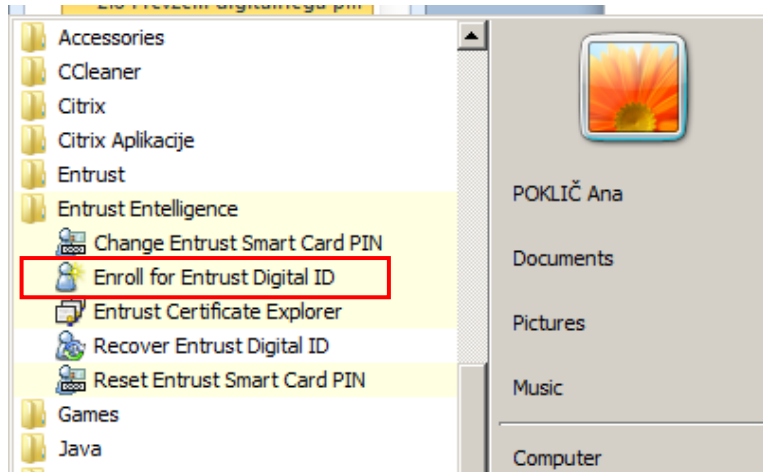
Current Language: **SL**

OK Cancel

2.5 Prezem digitalnega potrdila

Za prezem digitalnega potrdila potrebujete referenčno številko in avtorizacijsko kodo. Referenčno številko ste prejeli po elektronski pošti, po navadni pošti pa ste prejeli avtorizacijsko kodo.

Prezem pričnite s klikom na "Start", "Programs", "Entrust Entelligence" in dvoklikom na vrstico "Enroll for Entrust Digital ID":



Pojavi se okno pozdravno okno programa za prezem digitalnega potrdila. Za nadaljevanje postopka kliknite "Next >":



V oknu za vnos prevzemnih podatkov v polje "Reference Number" vpišite referenčno številko, v polje "Authorization code" pa avtorizacijsko kodo. Kliknite "Next>":

Enroll for Entrust Digital ID

Specify your activation codes

The wizard needs to know your activation codes so that it can enroll for an Entrust digital ID that is right for you.

Enter your reference number and authorization code:

Reference number: 58681473

Authorization code: NIZE-Q9A6-DLZA

i Your administrator should have provided these values to you (for example, reference number: 91480170 and authorization code: CRTJ-8V0R-VFNS).

< Back Next > Cancel

Namestitveni program vam ponudi pametno kartico, na katero boste prevzeli digitalno potrdilo. V primeru, da imate na računalnik priključen samo en čitalec in eno pametno kartico, kliknite "Next >"; če imate več čitalcev in več pametnih kartic, pa preverite izbiro in po potrebi zamenjajte ponujeno pametno kartico in kliknite "Next >":

Enroll for Entrust Digital ID Wizard

Specify a smart card

The wizard needs to know which smart card it should use to store your Entrust digital ID.

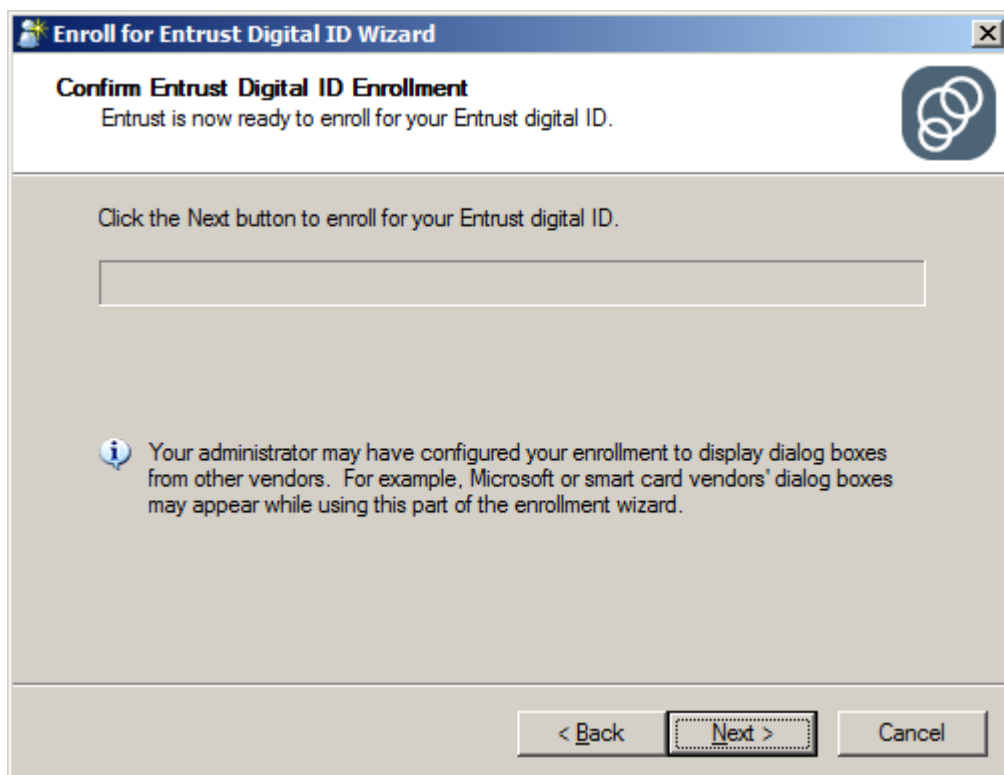
Choose a smart card from the following list:

OMNIKEY CardMan 2020 0 -> Datakey M 330

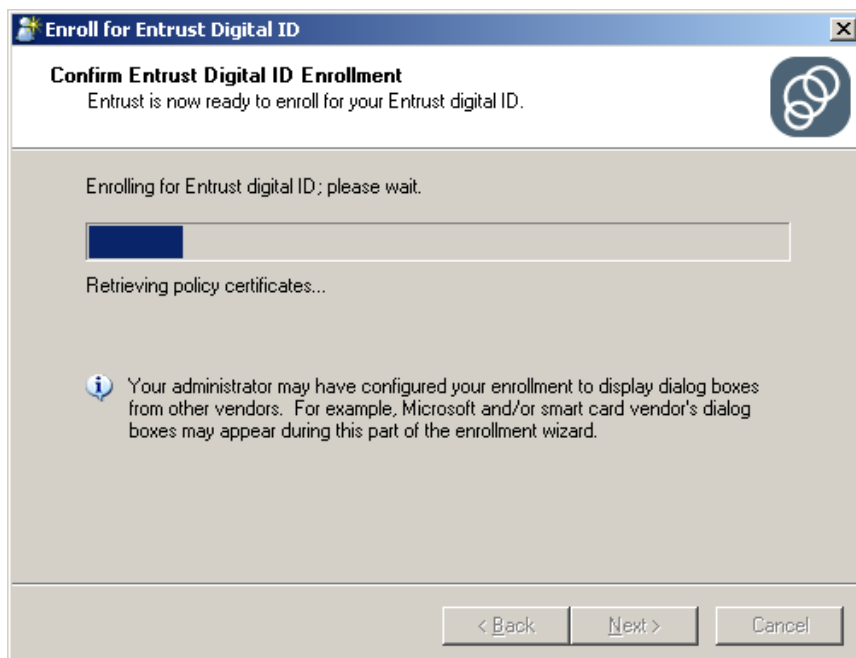
i One of the smart card names in this list should match the smart card you wish to use. If not, please insert smart card.

< Back Next > Cancel

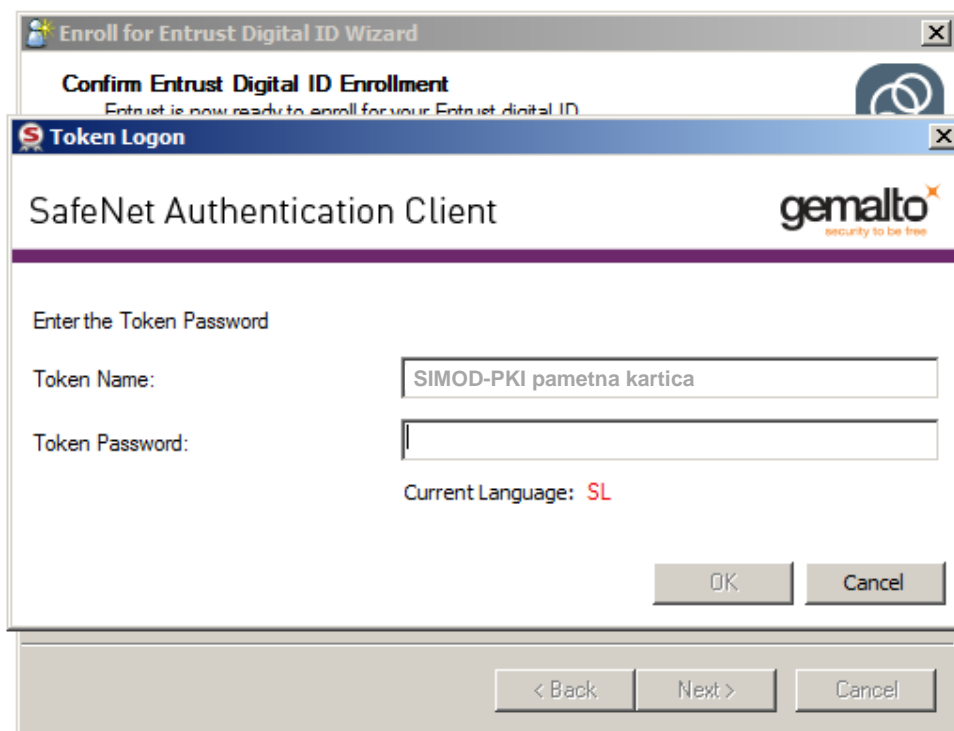
Še enkrat potrdite namero za prevzem digitalnega potrdila z"Next >":



Namestitveni program si z izdajateljem digitalnih potrdil izmenja določene podatke, zato počakajte na naslednji korak.



Ko se pojavi okence "Token Logon", vpišite vaše uporabniško geslo za dostop do pametne kartice in pritisnite "OK":



Začne se postopek vpisovanja digitalnih potrdil na pametno kartico, ki lahko traja nekaj minut.

Ko je zapisovanje digitalnih potrdil na pametno kartico končano, kliknite "Finish":






2.6 Inicializacija pametne kartice DATAKEY 330

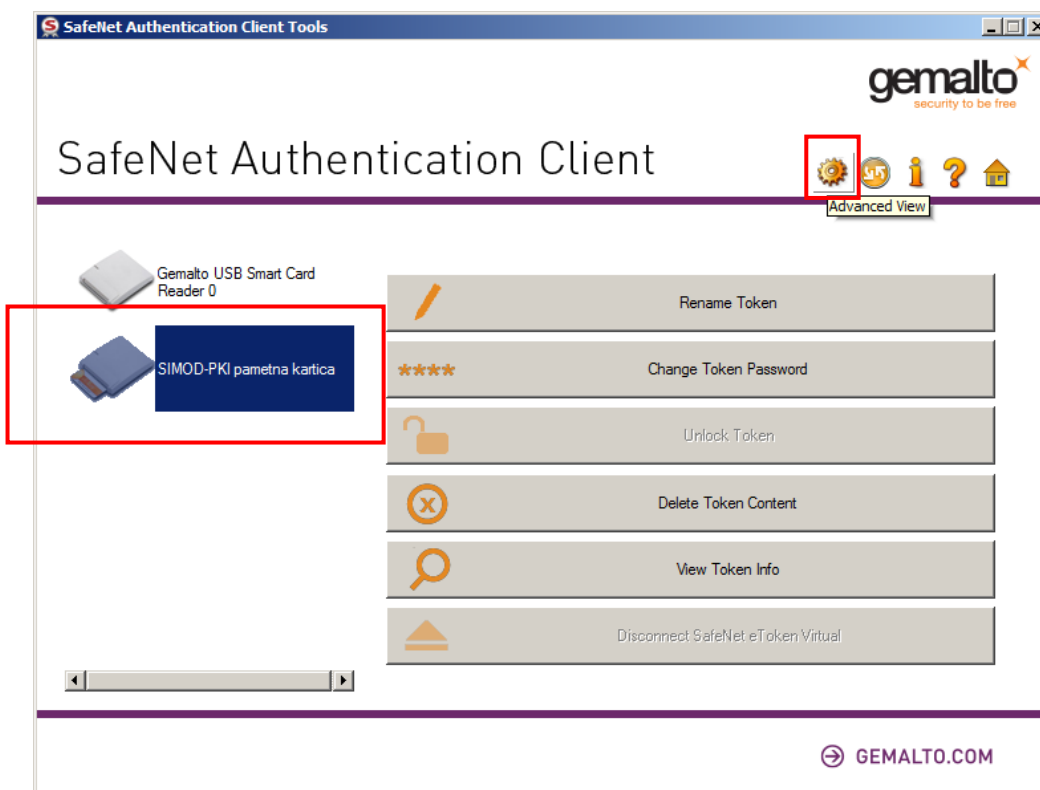
Ob inicializaciji pametne kartice določimo njene parametre in ponovno nastavimo geslo za njeno aktivacijo. Inicializacijo običajno naredimo, če smo pozabili geslo za aktivacijo pametne kartice. Inicializacijo izvedemo samo za pametne kartice DATAKEY 330.

OPOZORILA: Ob inicializaciji se vsebina pametne kartice zbriše – digitalna potrdila in zasebni ključi se nepovratno izgubijo!

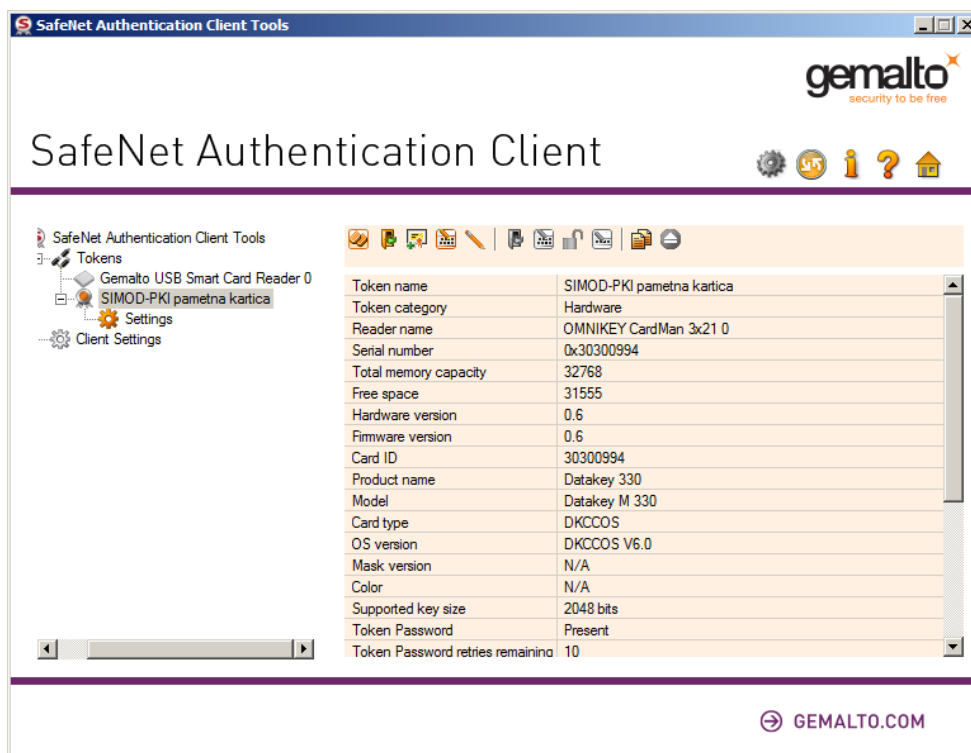
Inicializacijo naj uporabniki izvedejo samo v izjemnih okoliščinah po navodilu Storitvenega centra ali osebja overitelja digitalnih potrdil.



Zaženite program SafeNet Authentication Client, Tools (Start, All Programs, SafeNet, SafeNet Authentication Client, SafeNet Authentication Client Tools ali z dvojnim klikom po ikoni  ali desnim klikom po ikoni  nato izberite Tools).

Izberite čitalec z vstavljeno pametno kartico, nato kliknete na ikono , "Advanced View":

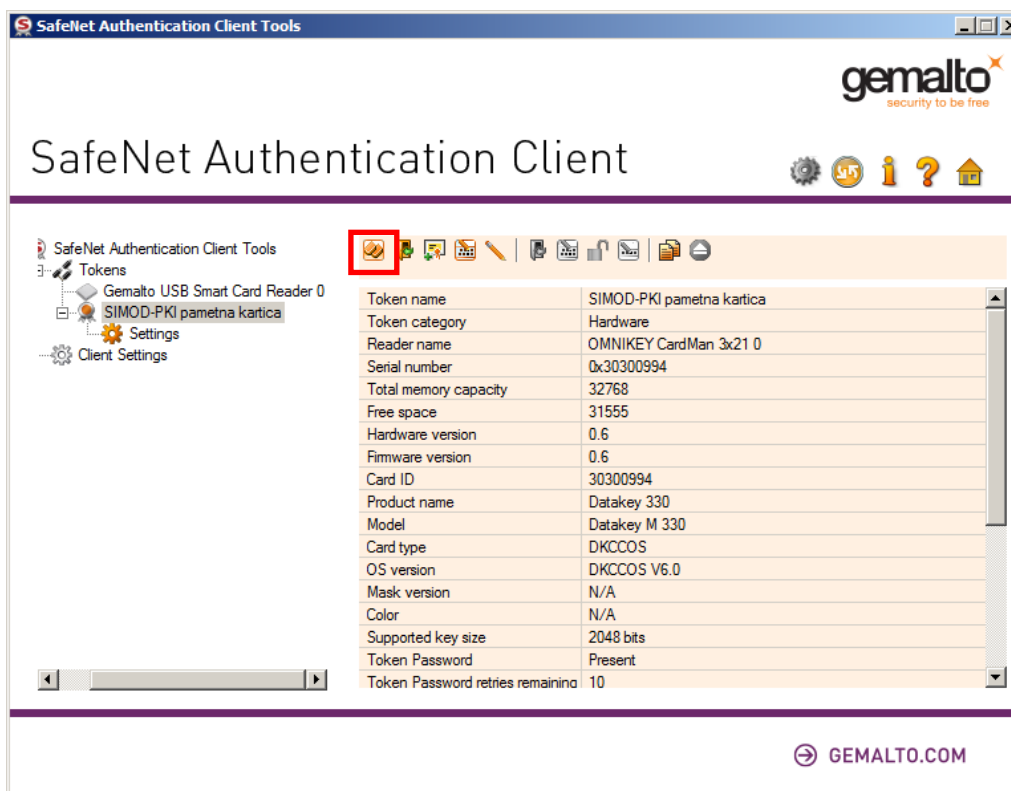


Odpre se nov pogled:

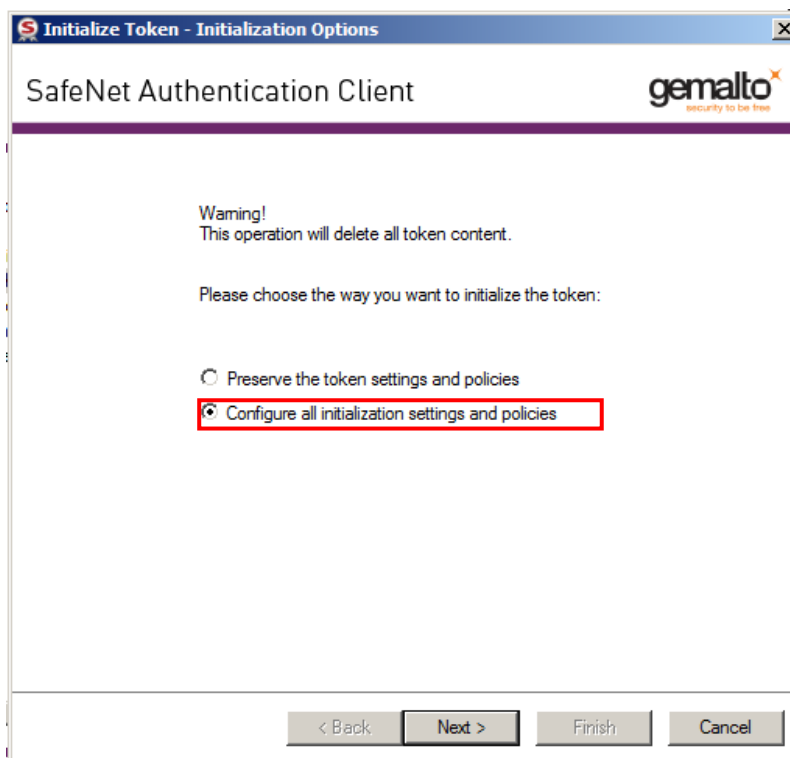


S klikom na plus  ali minus  razširjamo in zožujemo pogled. Razširite pogled tako, da bo vidno čim več podatkov. Iz slike je razvidno, da imamo pametno kartico z imenom "SIMOD-PKI pametna kartica". Predefinirana imena pametnih kartic DATAKEY so tudi "Token" ali "Dkccos 6.0 Token" ali kaj drugega.

Kartico inicializirate tako, da kliknete na ikono "Initialize Token":



Prikaže se opozorilo, da bo vsebina pametne kartice izbrisana. Potrebno je spremeniti način inicilizacije na • *Configure all initialization setting and policies*, nato kliknete »«Next«>:



Odpre se okno za določitev gesla:

Initialize Token - Password Settings

SafeNet Authentication Client

gemalto
security to be free

Token Name: SIMOD-PKI pametna kartica

Create Token Password:

New Token Password: [masked]

Confirm Password: [masked]

Logon retries before token is locked: 10

Token password must be changed on first logon

Create Administrator Password:

Create Administrator Password: [empty]

Confirm Password: [empty]

Logon retries before token is locked: 10

Current Language: SL

< Back Next > Finish Cancel

V polju "Token Name:" lahko spremenite ime pametne kartice; predlagamo vaše ime in priimek, a brez uporabe šumnikov.

V polje "New Token Password:" vnesite geslo, ki ga boste uporabljali za aktivacijo pametne kartice. Izbiro gesla potrdite v polju "Confirm Password:". Uporabniško geslo mora zadostiti zahtevam:

- dolžina mora biti od 8 do 20 znakov,
- vsebovati mora vsaj eno veliko in eno malo črko,
- vsebovati mora vsaj eno število in vsaj en znak.

Predlagamo, da ne spreminjate izbire pred "Token Password must be changed on first logon". Nato lahko kliknete »Finish«, če pa želite pregledati ali spremeniti nastavitve kvalitete gesla, kliknete "Next >".

V oknu z nastavitvami kvalitete gesla ne zmanjšujte zahtev za geslo, kliknite »Finish«:

Initialize Token - Password Quality Settings

SafeNet Authentication Client

gemalto
security to be free

Enforce password quality settings (recommended)

Minimum length (characters): 8

Maximum length (characters): 16

Minimum usage period (days): 0

Maximum usage period (days): 0

Expiration warning period (days): 0

History size: 10

Maximum consecutive repetitions: 0

Must meet complexity requirements: Manual

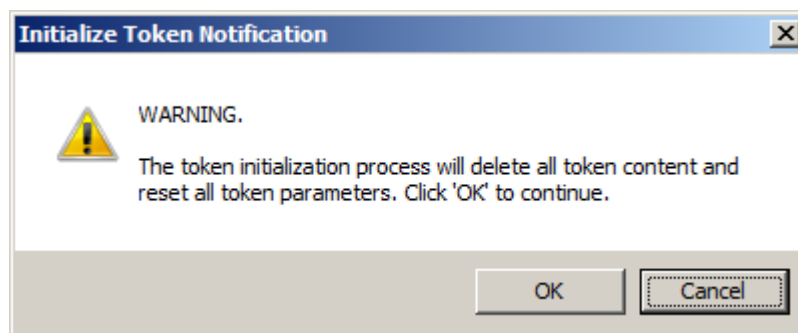
Manual Complexity Rules

Upper-case letters: Mandatory Numerals: Mandatory

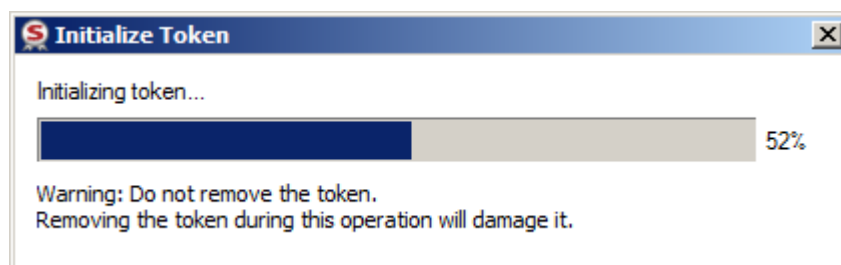
Lower-case letters: Mandatory Special characters: Mandatory

< Back Next > Finish Cancel

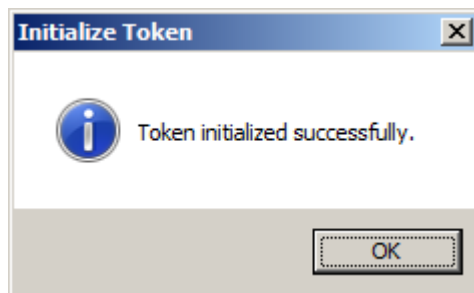
Sledi opozorilo, da bo inicializacija izbrisala vsebino pametne kartice. Potrdite z »OK«:



Počakajte, da se izvede postopek inicializacije. Potek je predstavljen z indikatorjem:



Po uspešni inicializaciji se pojavi obvestilo: "Token initalization successfully.", ki ga potrdimo z na »OK«:



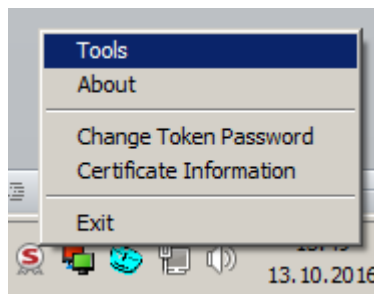
Pametna kartica je pripravljena za prevzem digitalnega potrdila.

2.7 Odklepanje pametne kartice GEMALTO IDPrime MD 840 in ponastavitev pozabljenega gesla


OPOZORILO: Pametna kartica GEMALTO IDPrime MD 840 se po **treh nepravilnih** poskusih vnosa gesla **zaklene**.

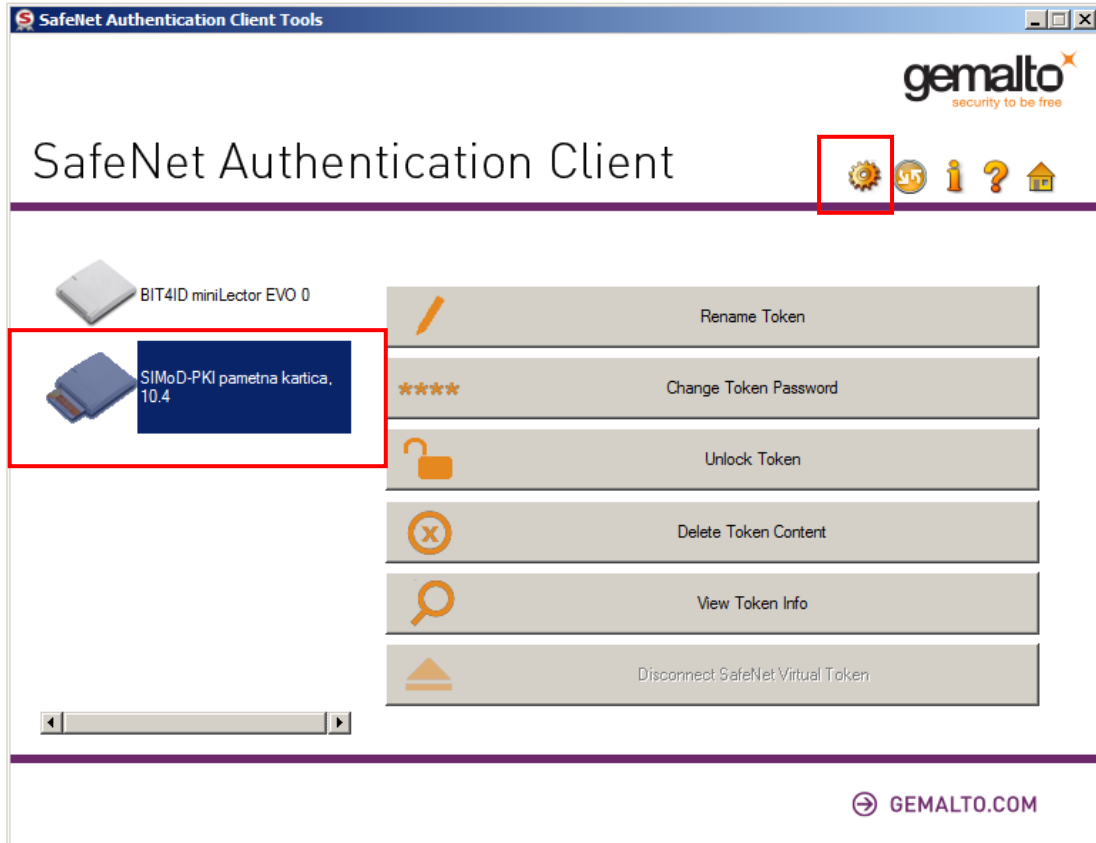
Za odklepanje pametne kartice morate poznati administratorsko geslo ("Administrator Password"), ki ste ga dobili po pošti skupaj s pametno kartico.

Z desnim klikom po ikoni , "SafeNet Authentication Client" in izberemo "Tools".

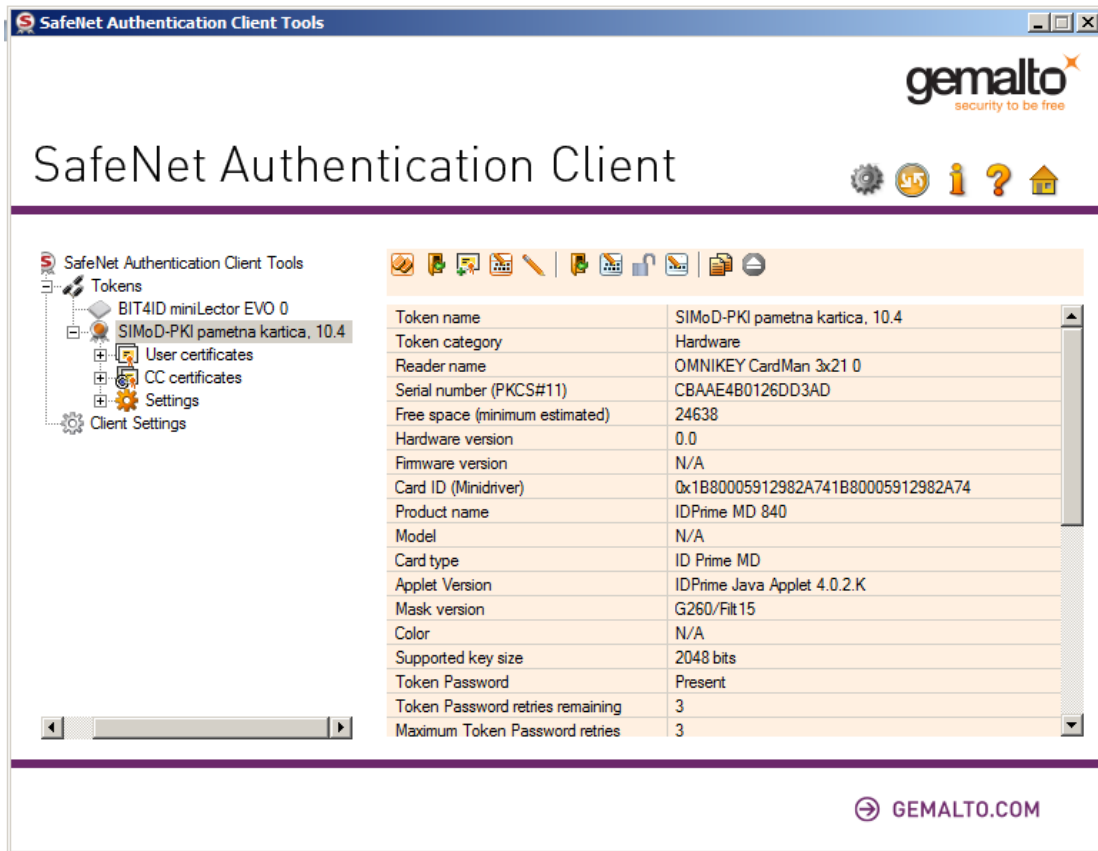



Odpre se "SafeNet Authentication Client". Izberemo pametno kartico in kliknemo na

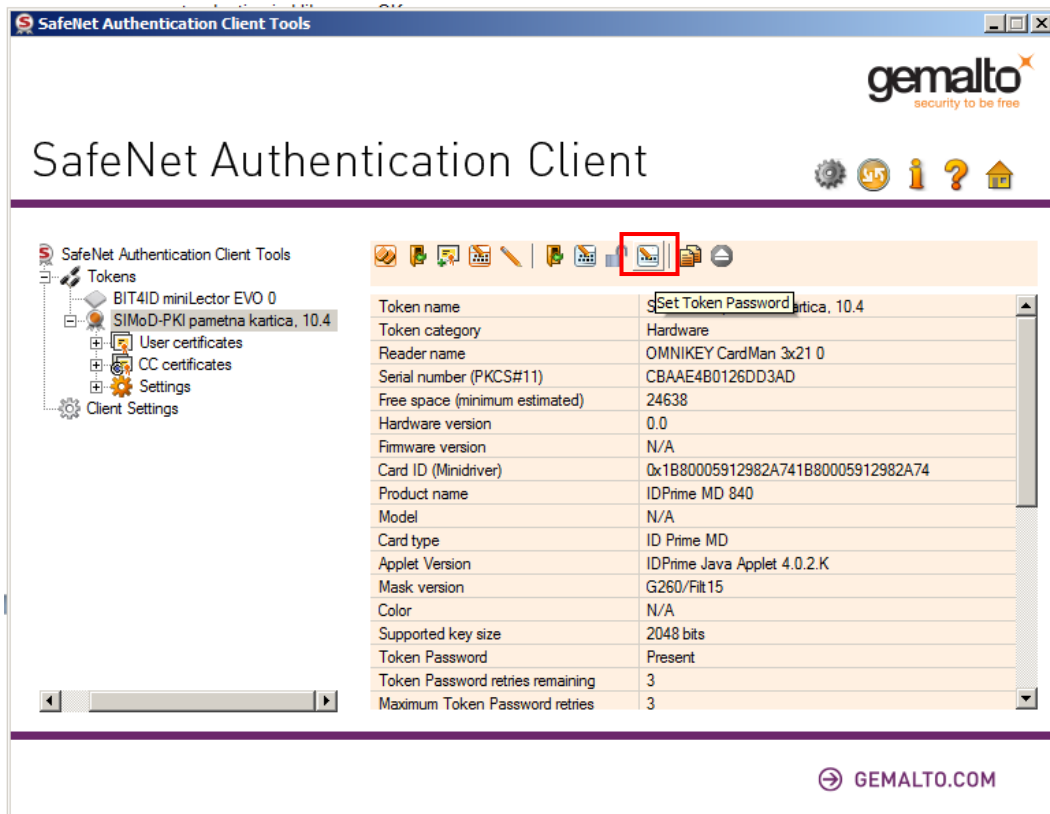
ikono , "Advanced View":



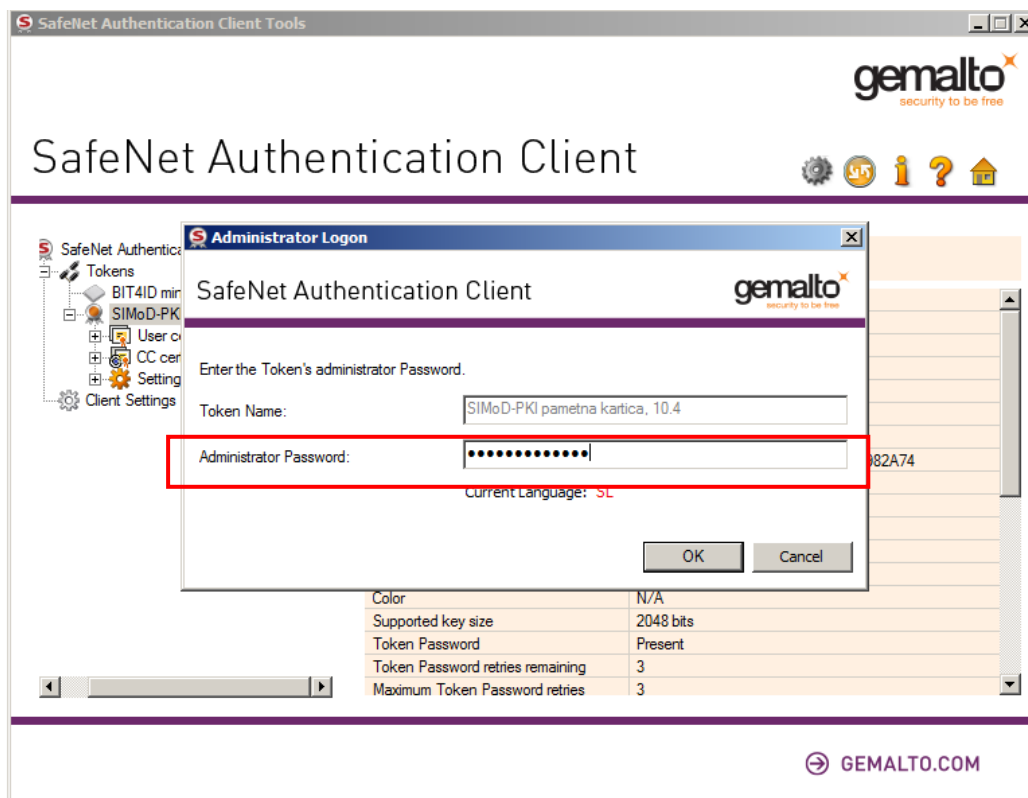
Odpre se nov pogled:



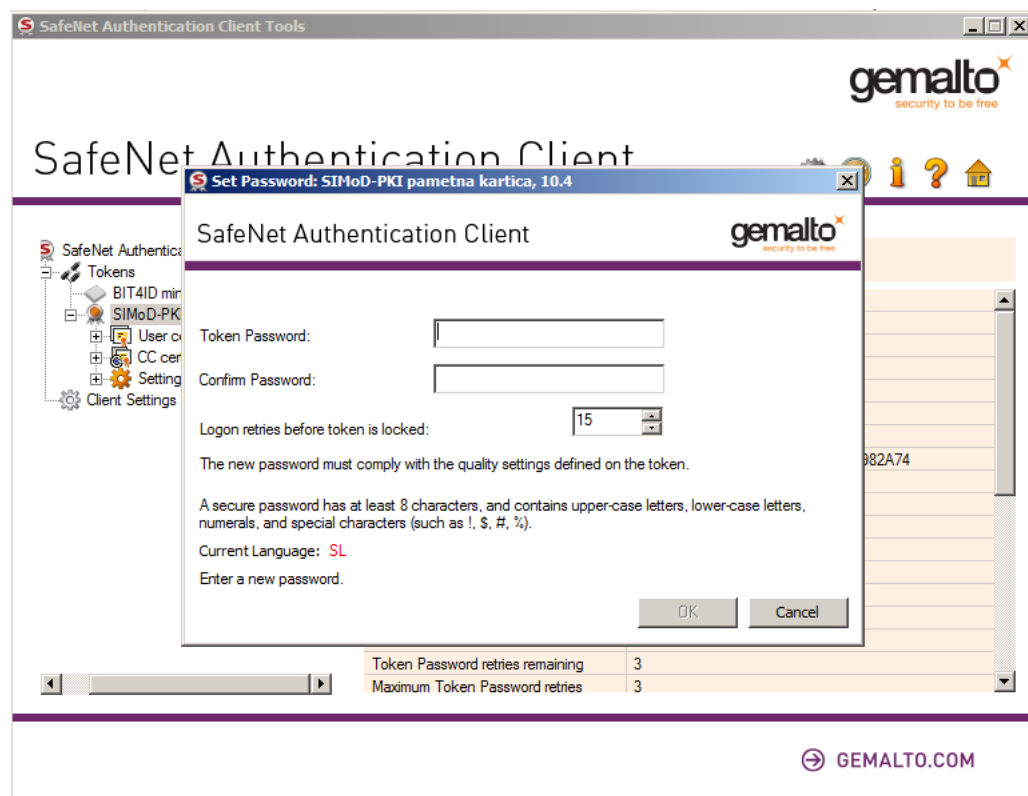
Kliknemo na ikono , »Set Token Password« :



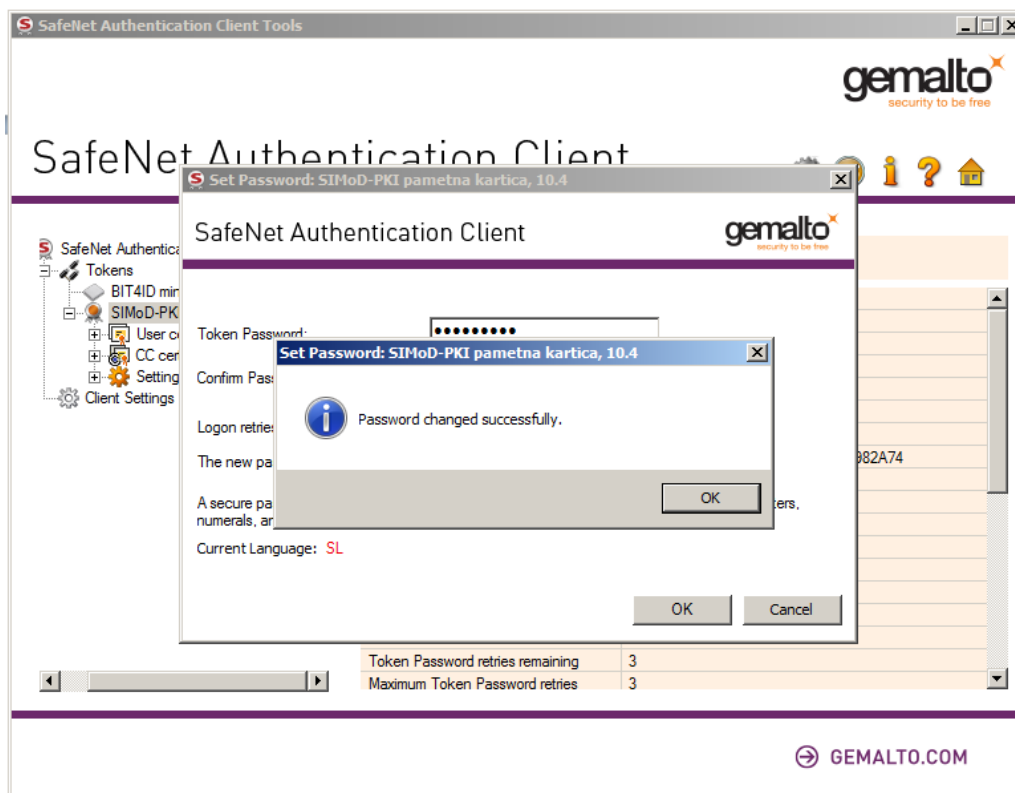
V polje »Administrator Password« vpišemo administratorsko geslo, ki smo ga dobili po pošti skupaj s pametno kartico in kliknemo »OK«:



V polje »Token Password« vpišemo novo geslo za pametno kartico in potrdimo v polju »Confirm Password«:



Kliknemo »OK« in pojavi se nam okno za uspešno odklepanje pametne kartice:



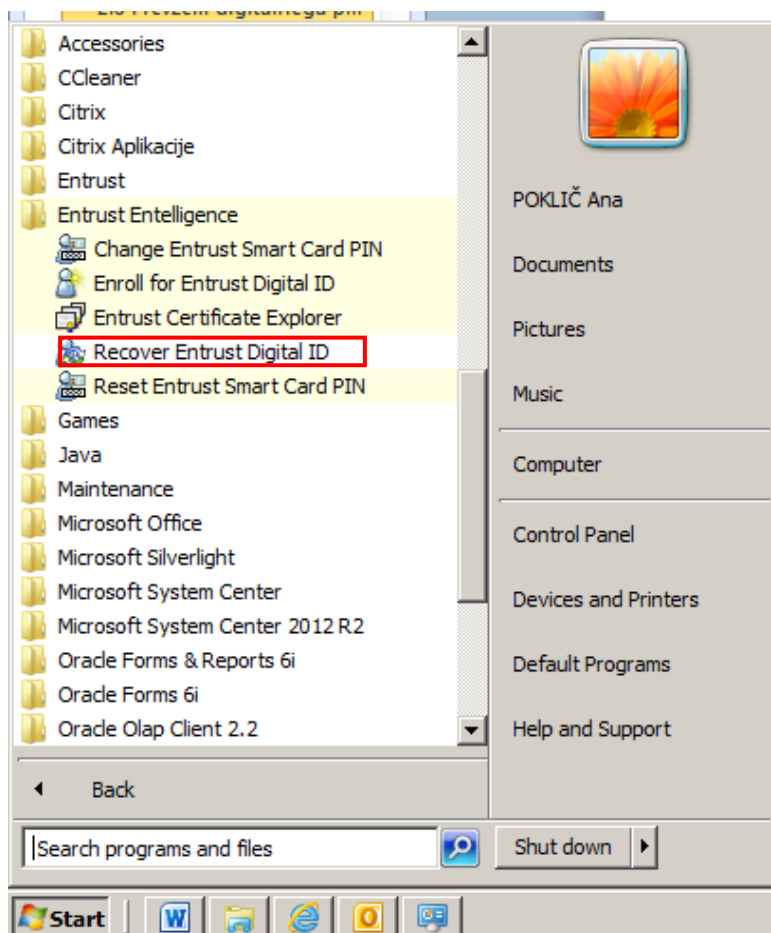
Še enkrat potrdimo z »OK«. Pametna kartica je uspešno odklenjena.

3. Obnova digitalnega potrdila

Uporabnik lahko po izgubi, poškodbi ali če je pozabil geslo za dostop do pametne kartice, zahteva obnovo digitalnega potrdila. Obnova digitalnega potrdila pomeni ponovno izdajo zasebnega ključa za ustvarjanje digitalnega podpisa in digitalnega potrdila za preverjanje digitalnega podpisa, v zvezi z digitalnim potrdilom za šifriranje pa se izvede povrnitev zasebnih ključev za dešifriranje in digitalnih potrdil za šifriranje (z vso zgodovino).

Uporabnik mora za obnovo oziroma ponovno izdajo digitalnega potrdila v prijavno službo oddati enak zahtevek kot za prvo pridobitev digitalnega potrdila. Po tem uporabnik prejme novo referenčno številko in avtorizacijsko kodo, s katerima obnovi digitalno potrdilo.

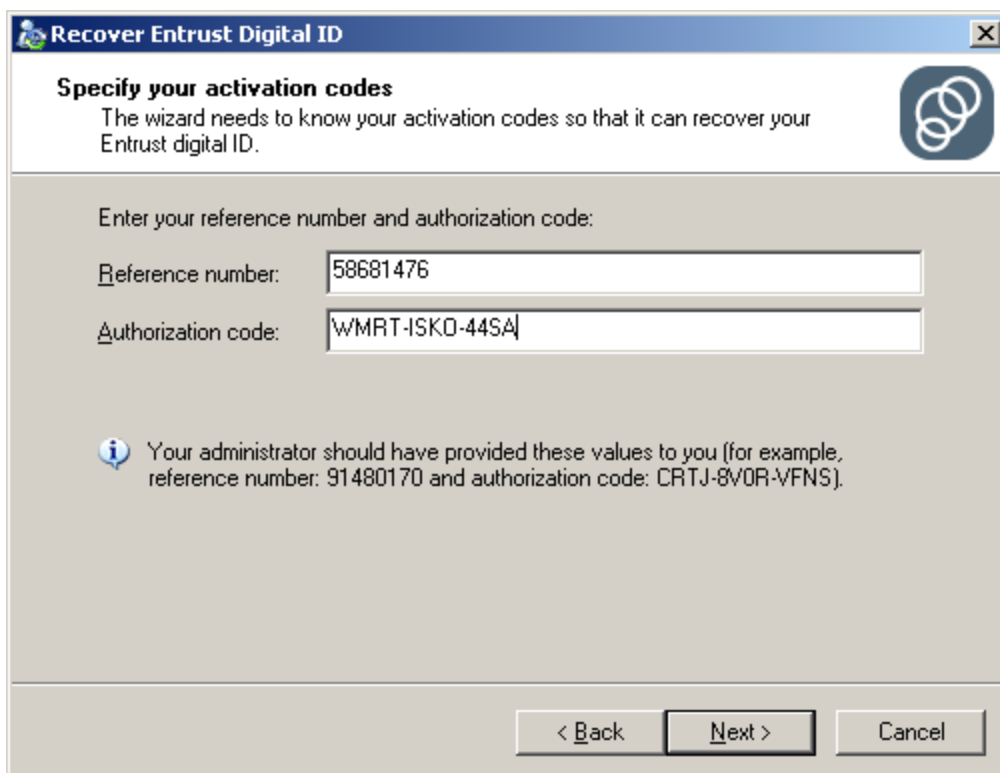
Za začetek obnove digitalnega potrdila kliknite "Start", "Programs", "Entrust Entelligence" in "Recover Entrust Digital ID":



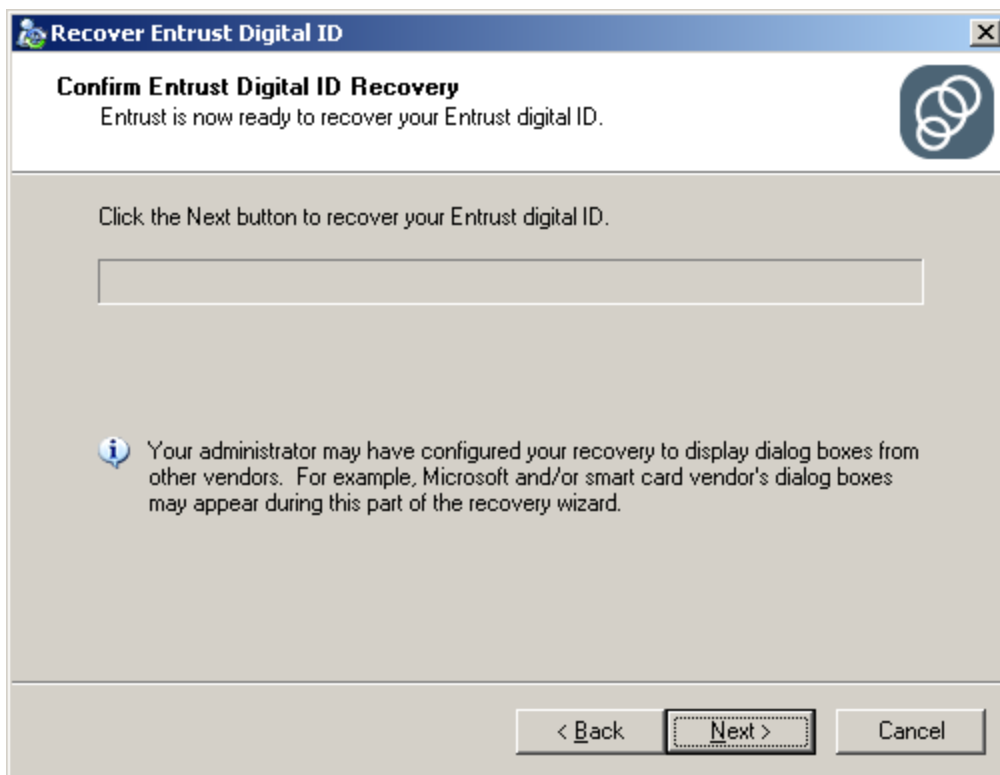
V oknu namestitvenega programa kliknite "Next >":



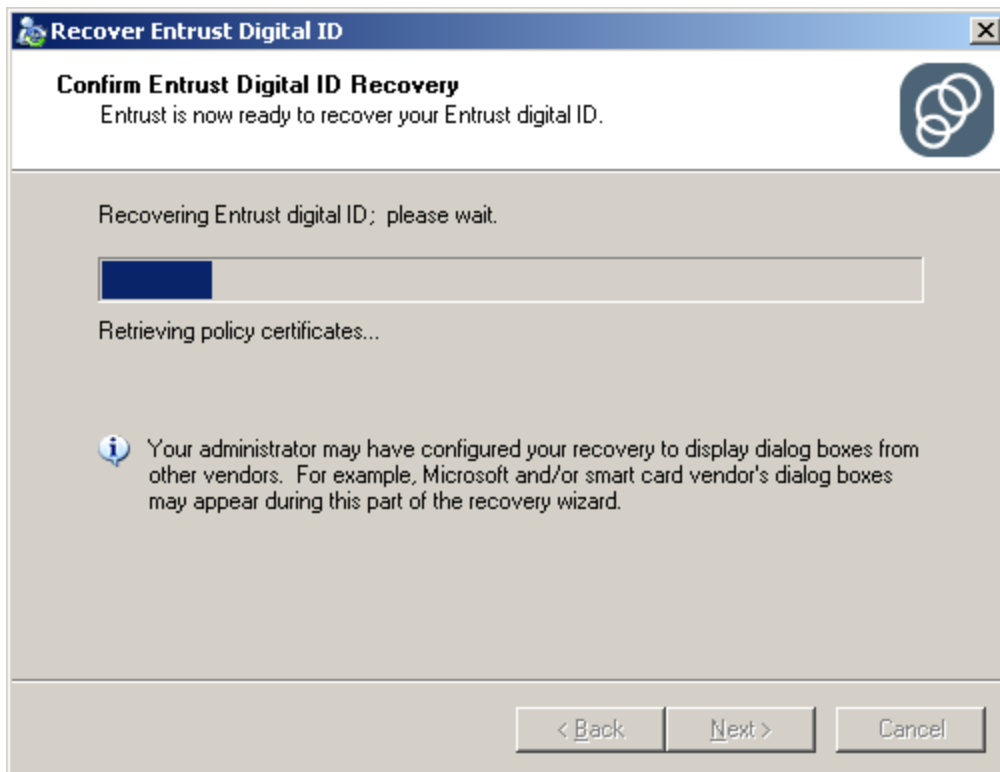
V polje "Reference number: " vpišite referenčno številko, v polje "Authorization code:" pa avtorizacijsko kodo ter kliknite "Next >":



V nadaljevanju postopka vas program opozori, da se bodo med procesom odpirala tudi interaktivna okna drugih proizvajalcev. V tem primeru bo to okno za uporabniško geslo pametne kartice. Kliknite "Next >":



Indikatorna vrstica prikazuje, da se je postopek začel:



V okence vpišite uporabniško geslo pametne kartice:

The screenshot shows a Windows-style dialog box titled "Recover Entrust Digital ID". It contains a sub-window titled "Confirm Entrust Digital ID Recovery" with the text "Entrust is now ready to recover your Entrust digital ID". Below this is another sub-window titled "Token Logon" from the "SafeNet Authentication Client" by Gemalto. The "Token Logon" window has a header with the Gemalto logo and the text "Enter the Token Password". It contains two input fields: "Token Name:" with the value "SIMOD-PKI pametna kartica" and "Token Password:" which is empty. Below the fields, it says "Current Language: SL". At the bottom right of the "Token Logon" window are "OK" and "Cancel" buttons. At the bottom of the main dialog box are "< Back", "Next >", and "Cancel" buttons.

Postopek obnove digitalnih potrdil lahko traja nekaj minut.

Ko je postopek zaključen, kliknite "Finish":

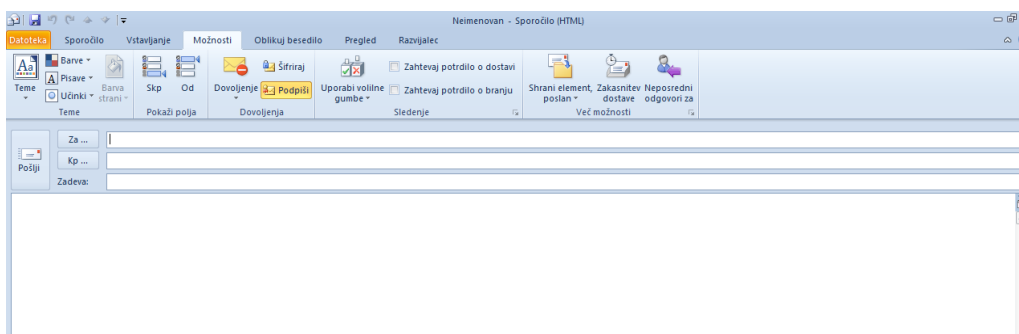
The screenshot shows the final step of the "Recover Entrust Digital ID" wizard. The window title is "Recover Entrust Digital ID". On the left is a dark blue sidebar with the Entrust logo. The main area has the heading "Completing the Recover Entrust Digital ID Wizard". Below the heading, it says "The Recover Digital ID Wizard has completed:" followed by a list: "- recovering your Entrust digital ID" and "- saving the Entrust digital ID on your computer, in a Directory, and/or on a smart card". Below the list, it says "Your Entrust digital ID may now be used to encrypt, digitally sign, and/or authenticate transactions. Your administrator has configured the specific functionality of your Entrust digital ID." At the bottom, it says "To close this wizard, click Finish." At the bottom of the window are "< Back", "Finish", and "Cancel" buttons.

4. Šifriranje in podpisovanje datotek ter elektronskih sporočil

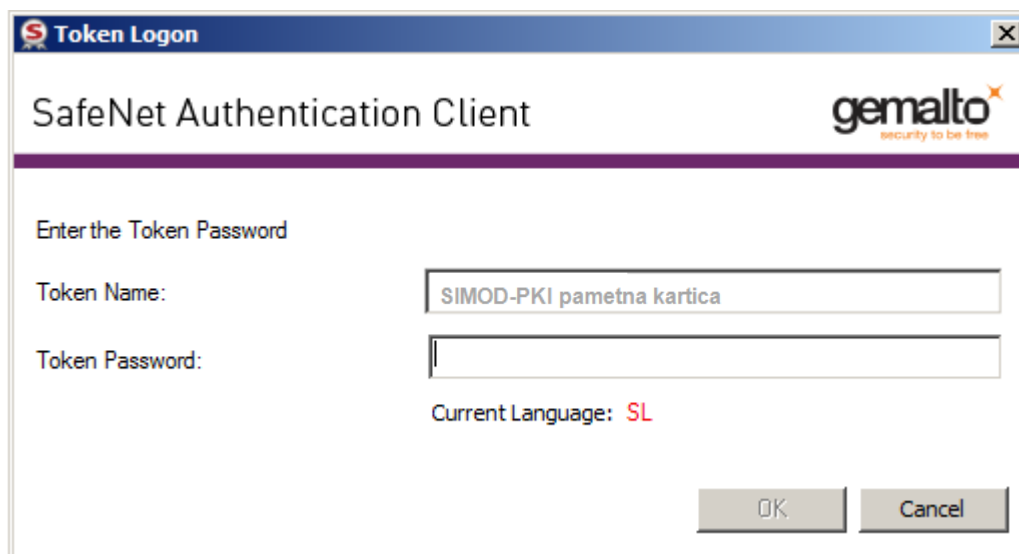
V okviru operacijskega sistema MS Windows so vam na razpolago osnovne varnostne storitve infrastrukture javnih ključev, to sta šifriranje in digitalno podpisovanje. Za uporabo varnostnih storitev mora biti pametno kartico vstavljena v čitalec.

4.1 Digitalno podpisovanje elektronskih sporočil v Outlooku 2010

Postopek pošiljanja digitalno podpisanega sporočila je podoben običajnemu pošiljanju. Odprite okno za izdelavo elektronskega sporočila. Ustvarite novo elektronsko sporočilo kot običajno. Nato izberite zavihek "Možnosti", kjer sta vidni orodji za digitalno podpisovanje in šifriranje. S klikom na gumb "Podpiši", ki se ob aktivaciji obarva rumeno, se elektronskemu sporočilu doda digitalni podpis. Izberite enega ali več naslovnikov, napišite naslov in vsebino sporočila ter kliknite tipko "Pošlji".

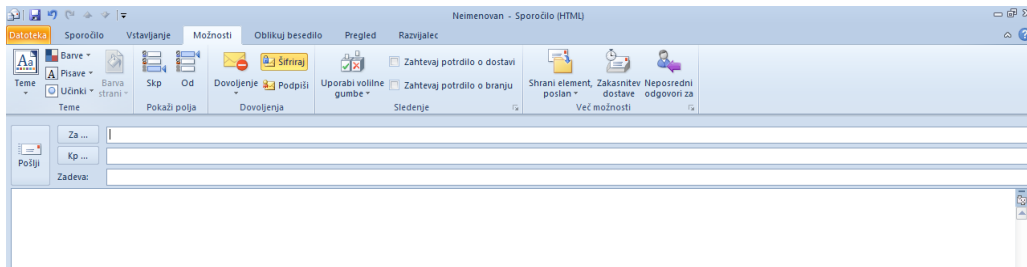


Pojavilo se bo okence za vnos gesla za dostop do pametne kartice, kjer se nahaja vaš ključ za digitalno podpisovanje. S klikom na tipko "OK" bo sporočilo digitalno podpisano in poslano naslovniku:



4.2 Šifriranje elektronskih sporočil v Outlooku 2010

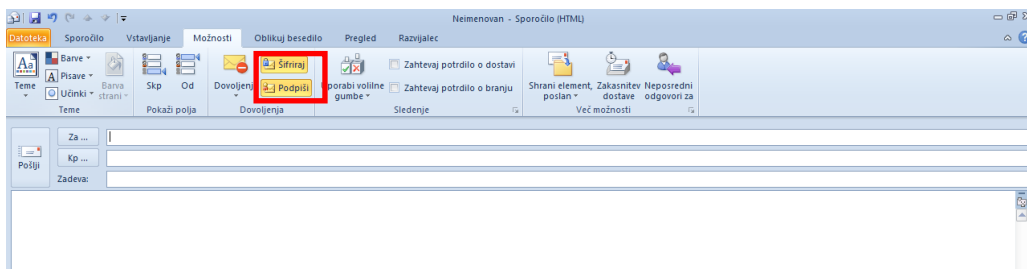
Postopek pošiljanja šifriranega sporočila je podoben običajnemu pošiljanju oziroma pošiljanju podpisanega sporočila. Odprite okno za izdelavo elektronskega sporočila. Ustvarite novo elektronsko sporočilo kot običajno. Nato izberite zavihek "Možnosti", kjer sta vidni orodji za digitalno podpisovanje in šifriranje. S klikom na gumb "Šifriraj", ki se ob aktivaciji obarva rumeno, se elektronsko sporočilo šifrira. V običajnem imeniku izberete enega ali več naslovnikov, napišite naslov in vsebino sporočila ter kliknite tipko "Pošlji":



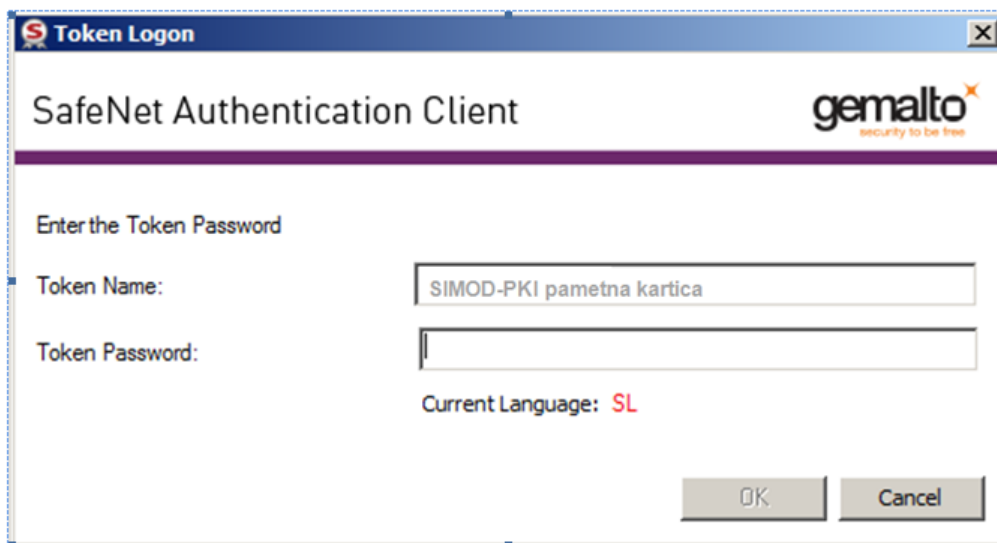
Prejemniku elektronskega sporočila njegova vsebina ni vidna, ker je sporočilo šifrirano. Ob kliku na prejeto elektronsko sporočilo se pojavi okence za vnos gesla za dostop do pametne kartice. S klikom na tipko "OK" potrdite pravilnost gesla, elektronsko sporočilo se bo nato od dešifriralo in bo vidno.

4.3 Šifriranje in podpisovanje elektronskih sporočil v Outlooku 2010

Odprite okno za izdelavo elektronskega sporočila. Ustvarite novo elektronsko sporočilo kot običajno. Nato izberite zavihek "Možnosti" in izberite orodji za digitalno podpisovanje in šifriranje. Naslovnikov je lahko več. Operacija digitalnega podpisovanja in šifriranja se izvede na koncu, ko kliknete tipko "Pošlji".

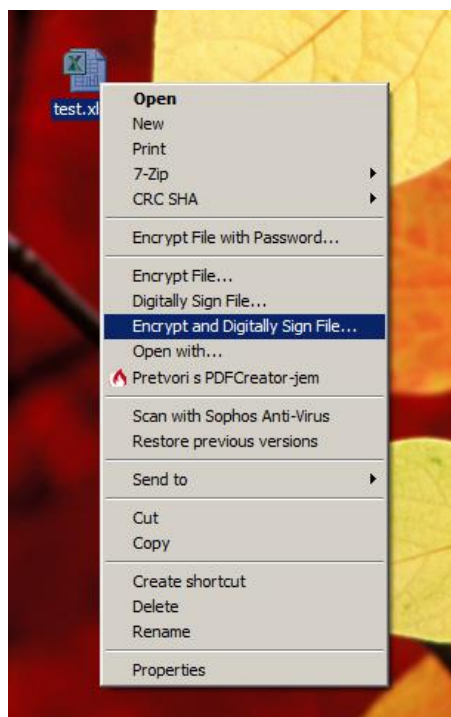


Pojavilo se bo okence za vnos gesla za dostop do pametne kartice, kjer se nahaja vaš ključ za digitalno podpisovanje. S klikom na tipko "OK" bo sporočilo digitalno podpisano in poslano naslovníku:



4.4 Šifriranje in podpisovanje datotek

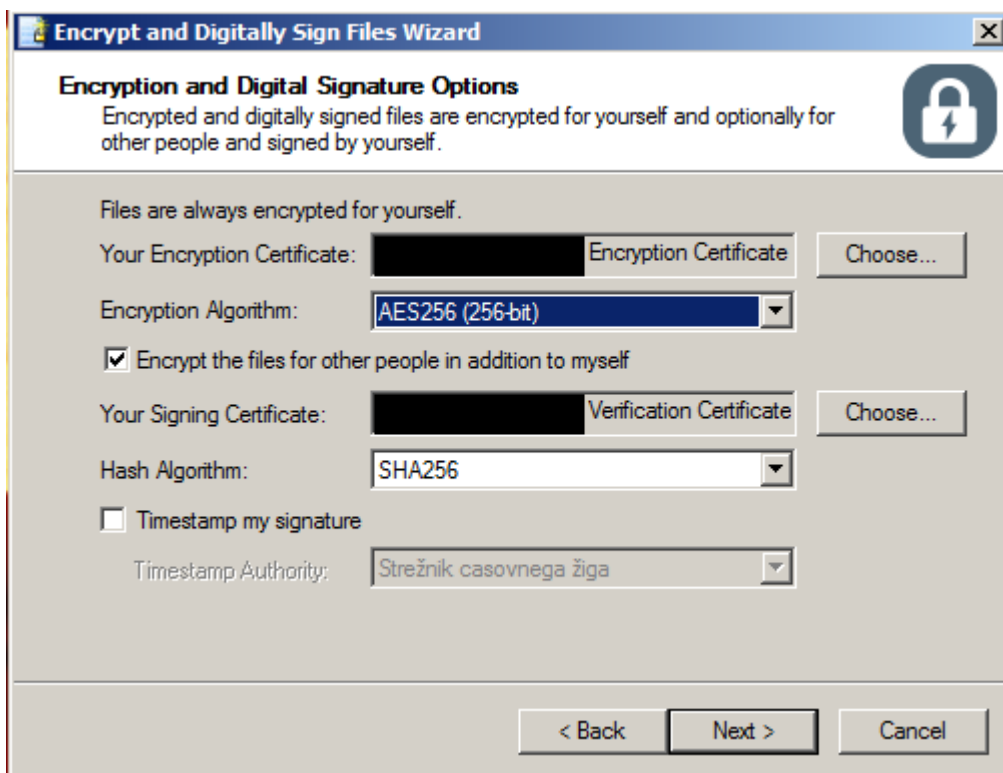
Orodje za podpisovanje in šifriranje datotek je vgrajeno v modulu "Windows Explorer". Z desnim klikom na poljubno datoteko se v drugem segmentu menija prikažejo orodja za šifriranje in digitalno podpisovanje. V navodilu boste sledili primeru šifriranja datoteke "Test.xlsx" za lastnika datoteke in dodatnega uporabnika, poleg tega pa bo datoteka podpisana z lastnikovim digitalnim podpisom.. V meniju kliknite "Encrypt and Digitally Sign File..."



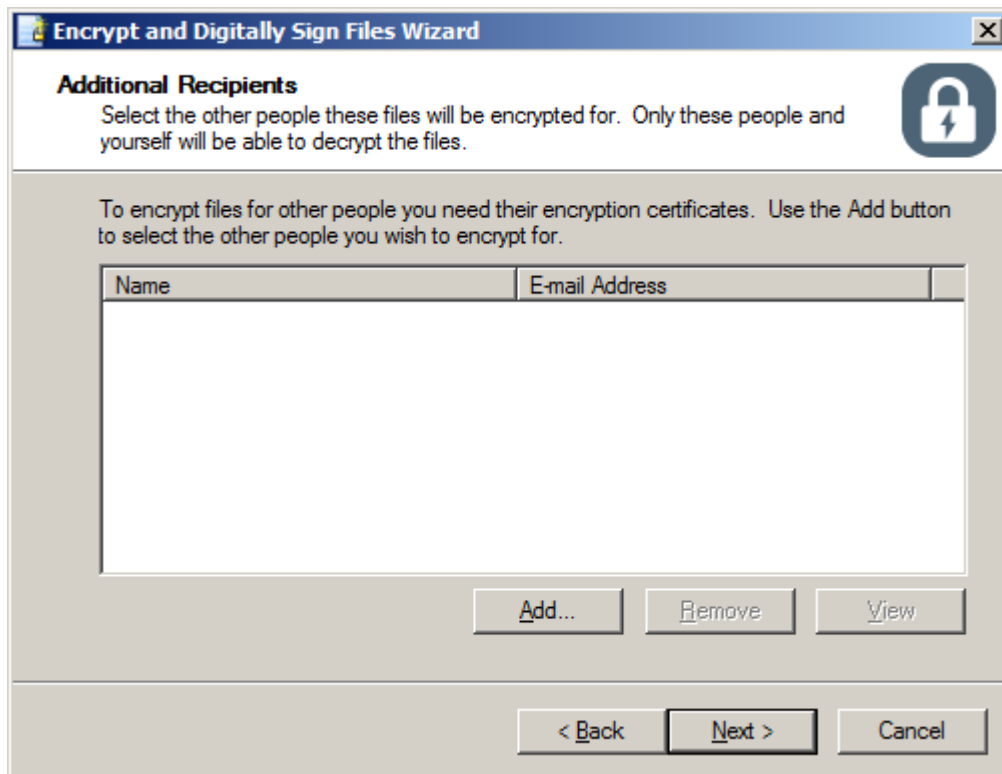
Začetno okno vsebuje ime datoteke, ki bo šifrirana in digitalno podpisana. Za nadaljevanje kliknite "Next >":



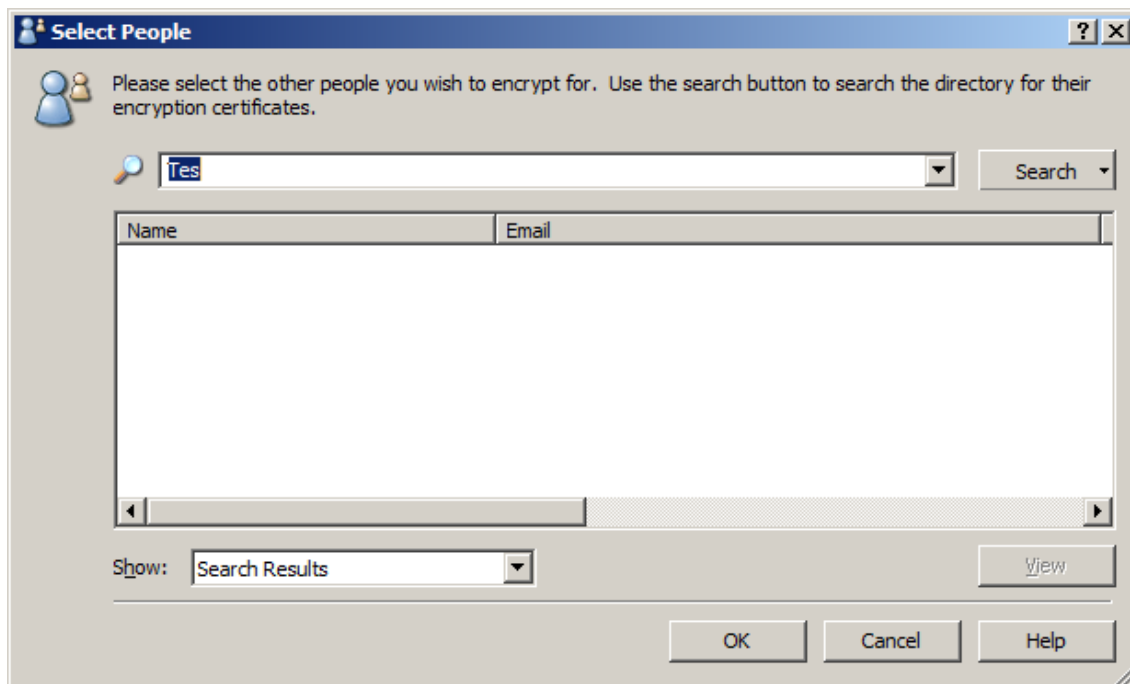
Program vas obvešča, s katerimi digitalnimi potrdili bo datoteka šifrirana in podpisana. Klik "Choose..." za začetnike ni priporočljiv. S kljukico označite možnost "Encrypt the files for other people in addition for myself" in kliknite "Next >":



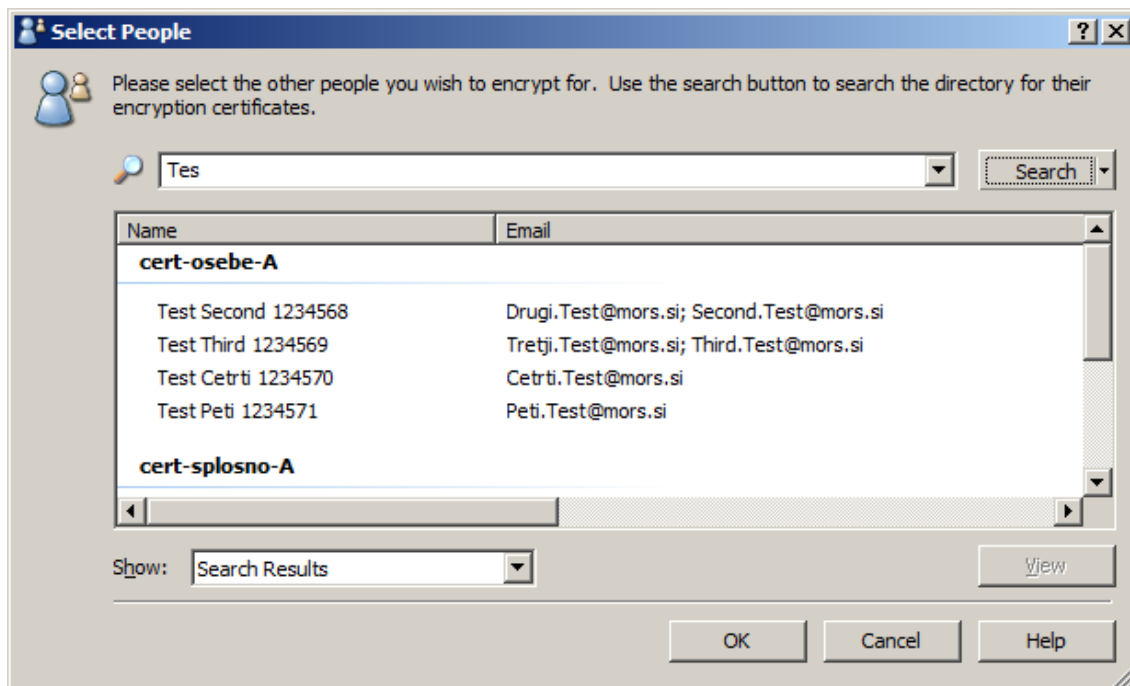
V seznam s klikom "Add..." dodajte še digitalno potrdilo nekoga, ki bo poleg vas lahko dešifriral vsebino datoteke:



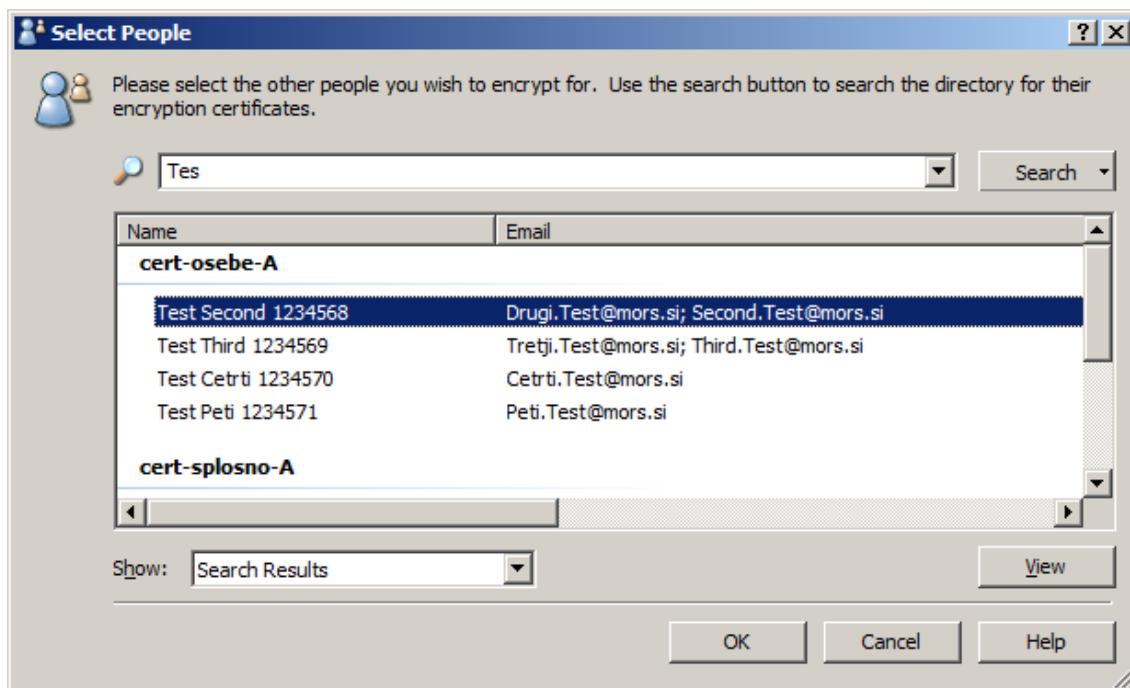
Odpre se okno za iskanje digitalnih potrdil. V zgornje okence vpišite nekaj črk iz imena iskanega uporabnika ter kliknite "Search":



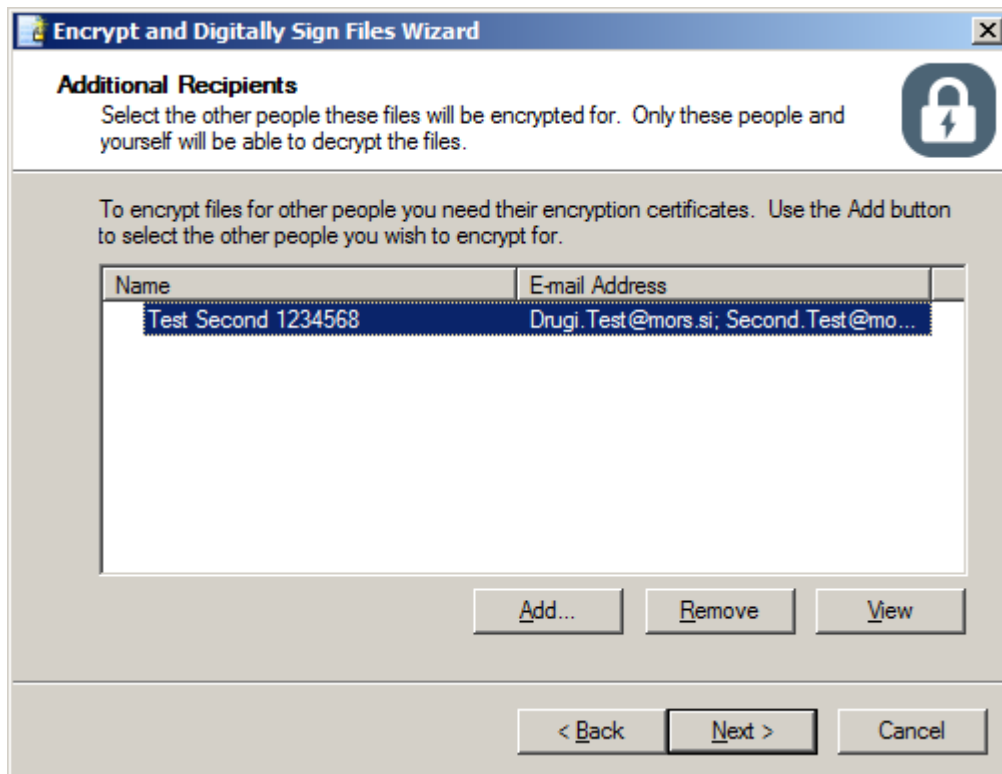
Imenik bo vrnil seznam uporabnikov, ki se vsebujejo niz črk iz iskalnega kriterija:



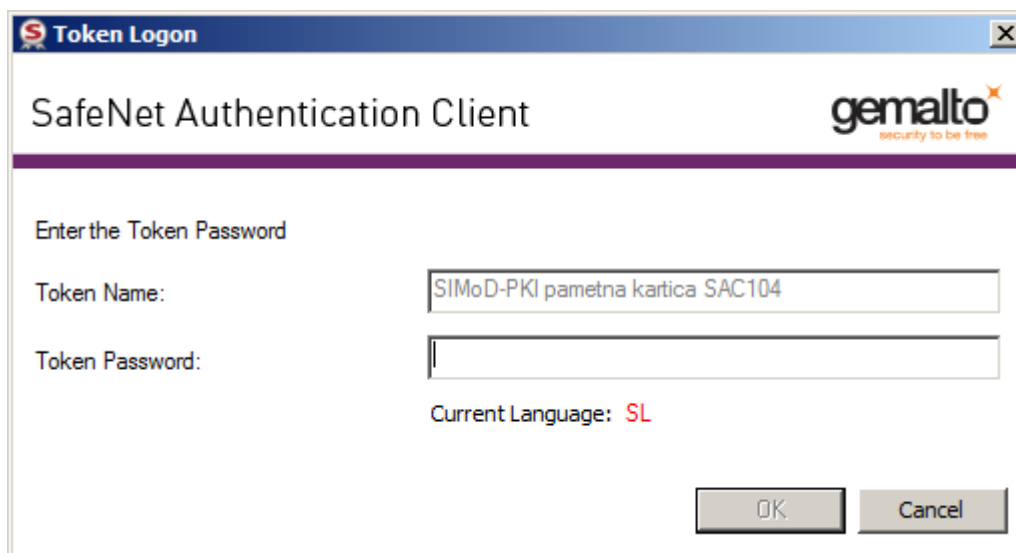
S klikom na uporabnika izberete uporabnikovo digitalno potrdilo, ki se skriva v ozadju. Kliknite "OK":



V oknu je navedeno digitalno potrdilo uporabnika. Njegov javni ključ in javni ključ lastnika bosta uporabljena za šifriranje datoteke "Test.xlsx". Kliknite "Next >":



Poleg šifriranja bo datoteka digitalno podpisana z lastnikovim privatnim ključem za podpisovanje, ki je varno shranjen na pametni kartici. Za dostop do pametne kartice vtipkajte geslo:



Na koncu postopka vas okno obvesti, da je nastala šifrirana datoteka " Test.xlsx.p7m":



Iz varnostnih razlogov je priporočljivo izvorno datoteko "Datoteka.txt" pobrisati, zato odkljukajte okence "Delete the original files on finish". Kliknite "Finish" in postopek je končan.