# 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 kartic2
	1.2	Namestitev programa za podporo pametne kartice SafeNet Authentication Client8
	1.3	Namestitev programa za upravljanje z digitalnimi potrdili Entrust Entelligence Security Provider
2.		Prevzem digitalnega potrdila
	2.1	Preverjanje delovanja čitalca pametne kartice in pametne kartice
	2.2	Pravilna nastavitev programa za podporo pametne kartice SafeNet Authentication Client
	2.3	Začetna določitev gesla za pametno kartico DATAKEY 33022
	2.4	Določitev gesla za pametno kartico GEMALTO IDPrime MD 840
	2.5	Prevzem digitalnega potrdila25
	2.6	Inicializacija pametne kartice DATAKEY 33029
	2.7	Odklepanje pametne kartice GEMALTO IDPrime MD 840 in ponastavitev pozabljenega gesla
3.		Obnova digitalnega potrdila
4.		Šifriranje in podpisovanje datotek ter elektronskih sporočil
	4.1	Digitalno podpisovanje elektronskih sporočil v Outlooku 201043
	4.2	Šifriranje elektronskih sporočil v Outlooku 201044
	4.3	Šifriranje in podpisovanje elektronskih sporočil v Outlooku 2010
	4.4	Šifriranje in podpisovanje datotek45

# 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 <u>http://www.simod-pki.mors.si/index.php?id=36</u>, Infrastruktura javnih ključev SIMoD-PKI, Prevzem in uporaba digitalnih potrdil:



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 <u>http://www.simod-pki.mors.si/index.php?id=36</u>, *Infrastruktura javnih ključev SIMoD-PKI*, *Prevzem 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:



Infrastruktura javnih ključev na MO, Navodilo za namestitev strojne in programske opreme ter uporabo osnovnih storitev Ver. 1.3, 28. Septemeber 2017 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 >":

🖁 HID OMNIKEY 3x21 PC/SC Driver - 🛛	InstallShield Wiz	ard		×
License Agreement Please read the following license agree	ment carefully.		HIII	D
End User License Agreement				-
IMPORTANT - CAREFULLY CONDITIONS OF THIS LICE "AGREEMENT") BEFORE INS CLICKING "I ACCEPT" AND INSTALLATION OF THE SOI THAT YOU HAVE READ, UN AGREEMENT, AND THAT YO	READ ALL TH NSE AGREEN STALLING TH PROCEEDIN FTWARE YOU DERSTAND A OU AGREE TO	HE TERMS AN MENT (THIS E SOFTWAR G WITH THE J ARE INDIC AND ACCEPT D BE BOUND	ND E. BY ATING I THIS BY ITS	T
I accept the terms in the license agree     I do not accept the terms in the license     InstallShield	agreement < <u>B</u> ack	<u>N</u> ext >	Print Cance	

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

🙀 HID OMNIKEY 3x21 PC/SC Driver - InstallShield Wizard	×
Ready to Install the Program The wizard is ready to begin installation.	HID
Click Install to begin the installation.	
If you want to review or change any of your installation settings, click E exit the wizard.	ack. Click Cancel to
InstallShield	
< Back	Cancel

Počakajte, da se namestitev konča:

🙀 HID OMN	IKEY 3x21 PC/SC Driver - InstallShield Wizard	(
Installing The prog	HID OMNIKEY 3x21 PC/SC Driver         gram features you selected are being installed.	
P	Please wait while the InstallShield Wizard installs HID OMNIKEY 3x21 PC/SC Driver. This may take several minutes.	
	Status:	
InstallShield –	< Back Next >	-

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 incializacijo pametne kartice.

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

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



#### Ignorirajte varnostno opozorilo, kliknite »Run«:

~	The publisher of SAC_29AVG17-x32-10.4.msi couldn't be verified. Are you sure you want to run the program Learn more	?	;	×
8		Run	View downloads	

Sledite postopku namestitvenega programa. Kliknite "Next >":



Izberete žaljeni jezik. Kliknite "Next >":

🙀 SafeNet Authentication Client 10.4	Setup		×
Interface Language Select the interface language.			gemalto <sup>×</sup>
English	-		
1 3	_		
InstallShield	< Back	Next >	Cancel

Potrdite licenčno izjavo in kliknite "Next >":

🙀 SafeNet Authentication Client 10.4 Setup	×
License Agreement Please read the following license agreement carefully.	gemalto security to be free
SAFENET SOFTWARE LICENSE TERMS SafeNet Authentication Client	
Legal notice: SafeNet software is not sold; rather, copies of SafeNet softw licensed all the way through the distribution channel to the UNLESS YOU HAVE ANOTHER AGREEMENT DIRECTLY WITH SA CONTROLS AND ALTERS YOUR USE OR DISTRIBUTION OF THE S SOFTWARE, THE TERMS AND CONDITIONS OF THE APPLICABL	vare are end user. FENET THAT SAFENET E LICENSE
I accept the license agreement     I do not accept the license agreement InstallShield	Cancel

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

🙀 SafeNet	Authentication Client 10.4	Setup	×
Destinati Click N a differe	i <b>on Folder</b> ext to install to this folder, ent folder.	or click Change to instal	to genalto
	Install SafeNet Authentio C:\Program Files\SafeN	ation Client 10.4 to: et\Authentication\	Change
InstallShield -		< Back Next	> Cancel

Infrastruktura javnih ključev na MO, Navodilo za namestitev strojne in programske opreme ter uporabo osnovnih storitev Ver. 1.3, 28. Septemeber 2017 Potrdite način namestitve »Typical«, kliknite »Next>«:



Potrdite začetek namestitve, kliknite »Install«:

🕞 SafeNet Authentication Client 10.4 Setup	×
The wizard is ready to begin installation.	gemalto security to be free
Click Install to begin the installation.	
If you want to review or change any of your installation Click Cancel to exit the wizard.	settings, click Back.
InstallShield	
< Back 🛞	Install Cancel

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

🙀 SafeNet /	Authentication Client 10.4	Setup		
<b>Installing</b> The pro	SafeNet Authentication Cl gram features you selecte	ient 10.4 ed are being installe	d. <b>g</b> e	security to be free
1	Please wait while the Ins Authentication Client 10.	stallShield Wizard in .4. This may take se	stalls SafeNet everal minutes.	
	Status: Installing eToken drivers			
InstallShield -				
2172 Sound) (1216)		< Back	Next >	Cancel

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.X<sup>1</sup>"; glede na vrsto operacijskega sistema izberemo 32-bitno ali 64-bitno verzijo:



<sup>1</sup> Praviloma namestimo zadnjo verzijo programske opreme, objavljeno na spletni strani.

Infrastruktura javnih ključev na MO, Navodilo za namestitev strojne in programske opreme ter uporabo osnovnih storitev

in nato kliknemo "Open":

Inter	net Explorer	×
Wha	it do you want to do with EESP93_AVG17_32bit.zip?	
Size: From	10,1 MB : www.simod-pki.mors.si	
•	<b>Open</b> The file won't be saved automatically.	
•	Save	
•	Save as	
	Cancel	

Z dvoklikom na "setup" zaženite nameščanje programa:

EESP93_AVG17_32bit.zip					
Content.IE5 • 5UH08BCA • EESP93_AVG17_32bit.zip • 🚱 Search EESP93_AVG17_32bit.zip					
Organize 👻 Extract	all files				- 🔳 🔞
🛧 Favorites 🔺	Name ^	-	Туре	Compressed size	Password p
🧾 Desktop	AVG17.mst		MST File	4 KB	No
Downloads	🕞 eespwin32.msi		Windows Installer Package	10.367 KB	No
Recent Places	💷 setup.exe		Application	26 KB	No
🥞 Libraries	📰 setup.ini		Configuration settings	1 KB	No
Normal Computer					
SISTEM (C:)					
PODATKI (D:)					
PROJEKTI (P:)					
SMVMO (Q:)					
🖵 PROGRAMI (R 💌					Þ
setup.e	Xe Compressed size: 25,6 KB		Ratio: 58%		
	Size: 60,3 KB	[	Date modified: 28.07.2015 12:17		





Potrdite licenčno izjavo in kliknite "Next >":

🙀 Entrust Entelligence Security Provider 9.3 for Windows	_ 🗆 🗙
End-User License Agreement	$\bigcirc$
ATTENTION: THIS IS A LICENSE, NOT A SALE. THIS SOFTWAR IS PROVIDED UNDER THE FOLLOWING LICENSE THAT DEFINES WHAT YOU MAY DO WITH THE SOFTWARE AND CONTAINS LIMITATIONS ON REPRESENTATIONS, WARRANTIES, CONDITIONS, REMEDIES, AND LIABILITIES. IF YOU OBTAINED THIS SOFTWARE IN THE UNITED STATES, "ENTRUST" SHALL MEAN ENTRUST, INC. IF YOU OBTAINED THIS SOFTWARE OUTSIDE OF THE UNITED STATES, "ENTRUST" SHALL MEAN ENTRUST LIMITED. "AFFILIATES" OF ENTRUST SHALL MEAN ALL CORPORATIONS CONTROLLED DIRECTLY OR INDIRECTLY	E A
Print Back Next C	Cancel

Izberite običajno namestitev "Typical" :

🖶 Entrust Entelligence Security Provider 9.3 for Windows	
Choose Setup Type Choose the setup type that best suits your needs	Ø
Typical Installs the most common program features. Recommended for most users. Custom	
Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users. Complete All program features will be installed. Requires the most disk space.	
Back Next Cancel	

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



Počakajte, da se namestitev konča:



ter s klikom "Finish" zaključite nameščanje programa:



# 2. Prevzem 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. Prevzem 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 nastavitev 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 ":

	Tools About
	Change Token Password Certificate Information
Ś	Exit

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 nastavitev shranimo z pritiskom na gumb "Save".

SafeNet Authentication Client Tools		
SafeNet Authen	tication Client	🏶 😳 1 ? 🔒
SafeNet Authentication Client Tools Tokens BIT4ID miniLector EVO 0 SIMoD-PKI pametna kartica, 10.4 User cettificates CC certificates CC certificates CC certificates CC certificates	Password Quality       Advanced         Image: Copy user certificates to the local store.         Image: Copy CA certificates to the local store.         Image: Enable single logon.         Image: Enable single logon for PKCS#11.         Image: Allow password quality configuration on token after initialization         Image: Allow only an administrator to configure password quality or         Show application tray icon:         Automatic logoff after token inactivity (in minutes):         Enable Logging	tion. h token. Always V Always V Save Discard
		⊖ GEMALTO.COM

#### 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«:

Password Security: SIMOD-PKI pametna kartica		
For security reasons, you must change the Token Password.		
	OK Cancel	

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.

Schange Password: SIMOD-P	KI pametna kartica	×
SafeNet Authenticat	tion Client	gemalto <sup>×</sup>
Current Token Password:	•••••	]
New Token Password:		
Confirm Password:		0%
The new password must comply wit	h the quality settings defined on the to	ken.
A secure password has at least 8 cl numerals, and special characters (s	naracters, and contains upper-case let uch as !, \$, #, %).	ters, lower-case letters,
Current Language: SL		
The password must comply with the	quality settings.	
		OK. Cancel

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":

Ľ	Tools	
	About	
	Change Token Pas Certificate Informa	sword
_	Exit	-
S		13.10.2016

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

SafeNet Authentication Client Tools		
		gemalto security to be free
SafeNet Authen	ticati	on Client 🛛 🛯 🐲 💁 🔒
BIT4ID miniLector EVO 0	1	Rename Token
SIMoD-PKI pametna kartica, 10.4	****	Change Token Password
		Unlock Token
	$\otimes$	Delete Token Content
	Q	View Token Info
		Disconnect SafeNet Virtual Token
4		

Pojavi se pojavno okno:

S Change Password: SIMoD-P	KI pametna kartica, 10.4	×		
SafeNet Authentication Client		gemalto <sup>×</sup>		
Current Token Password:	1			
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 cl numerals, and special characters (s	naracters, and contains upper-case let uch as !, \$, #, %).	ters, lower-case letters,		
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«.

Uporabr	niško geslo mora biti dolg	o vsaj 6 znakov.		
	S Change Password: SIMoD-PKI pametna kartica, 10.4			
	SafeNet Authenticat	gemalto recurity to be free	×	
	Current Token Password:	•••••		
	New Token Password: Confirm Password:	••••••		
	The new password must comply with	the quality settings defined on th	e token.	
	A secure password has at least 8 ch numerals, and special characters (su	aracters, and contains upper-case ich as !, \$, #, %).	e letters, lower-case letters,	
	Current Language: SL			
			OK Cancel	

Infrastruktura javnih ključev na MO, Navodilo za namestitev strojne in programske opreme ter uporabo osnovnih storitev Ver. 1.3, 28. Septemeber 2017

#### 2.5 Prevzem digitalnega potrdila

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

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



Pojavi se okno pozdravno okno programa za prevzem 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>":

都 Enroll for Entrust Digital	ID	×		
<b>Specify your activation codes</b> 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 nu	imber and authorization code:			
<u>R</u> eference number:	58681473			
Authorization code:	NIZE-Q9A6-DLZA			
Your administrator reference number.	should have provided these values to you (for example, 91480170 and authorization code: CRTJ-8V0R-VFNS).			
	< <u>B</u> ack <u>N</u> ext > C	ancel		

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	×
<b>Specify a smart card</b> The wizard needs to know which smart card it should use to store your Entrust digital ID.	Ø
Choose a smart card from the following list:	
OMNIKEY CardMan 2020 0> Datakey M 330	•
One of the smart card names in this list should match the smart card you wish to use. If not, please insert smart card.	
< <u>B</u> ack <u>N</u> ext >	Cancel

Infrastruktura javnih ključev na MO, Navodilo za namestitev strojne in programske opreme ter uporabo osnovnih storitev Ver. 1.3, 28. Septemeber 2017 Še enkrat potrdite namero za prevzem digitalnega potrdila z"Next >":

🎥 Enroll for Entrust Digital ID Wizard	×
Confirm Entrust Digital ID Enrollment Entrust is now ready to enroll for your Entrust digital ID.	Ø
Click the Next button to enroll for your Entrust digital ID.	
Your administrator may have configured your enrollment to display dialog boxes from other vendors. For example, Microsoft or smart card vendors' dialog boxes may appear while using this part of the enrollment wizard.	
< <u>B</u> ack <u>Next</u> > Cance	el

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":

Enroll for Entrust Digital ID Wi Confirm Entrust Digital ID Enro Entrust is now ready to enroll for	zard rollment	×
🤶 Token Logon		×
SafeNet Authenticatio	on Client	gemalto security to be tree
Enter the Token Password		
Token Name:	SIMOD-PKI pametna kartic	а
Token Password:		
	Current Language: SL	
		OK. Cancel
	< Back.	Next > Cancel

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":



Infrastruktura javnih ključev na MO, Navodilo za namestitev strojne in programske opreme ter uporabo osnovnih storitev Ver. 1.3, 28. Septemeber 2017

#### 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:

SafeNet Authentication Client Tools			ç	<b>jen</b>	na surity to	
SafeNet Authen	tication Clie	ent	ی چې	1	?	
≷ SafeNet Authentication Client Tools	2 F II 1 1 1 1 1 1	n 🖻 🗐 🖨				
Gemalto USB Smart Card Reader 0	Token name	SIMOD-PKI pametoa kartica				
🖃 🤵 SIMOD-PKI pametna kartica	Token category	Hardware				_
Settings	Reader name	OMNIKEY CardMan 3x21.0				
Client Settings	Serial number	0x30300994				
	Total memory capacity	32768				
	Free space	31555				
	Hardware version	0.6				
	Firmware version	0.6				
	Card ID	30300994				
	Product name	Datakey 330				
	Model	Datakey M 330				
	Card type	DKCCOS				
	OS version	DKCCOS V6.0				
	Mask version	N/A				
	Color	N/A				
	Supported key size	2048 bits				
	Token Password	Present				
	Token Password retries remaining	10				<b>•</b>
			⊖ gei	IALT	0.00	М

S klikom na plus <sup>•</sup> ali minus <sup>•</sup> 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":

SafeNet Authentication Client Tools			g	en	na urity to	
SafeNet Authen	tication Clie	ent	۵ 🖗	1	?	
SafeNet Authentication Client Tools ∃-∽ Tokens	🧶 🖡 🐺 🛍 🔨 🖡 🛍	n 🖻 👌 🔿				
Gemalto USB Smart Card Reader 0	Token name	SIMOD-PKI pametna kartica				
SIMOD-PKI pametna kartica	Token category	Hardware				
Settings	Reader name	OMNIKEY CardMan 3x21 0				
	Serial number	0x30300994				
	Total memory capacity	32768				
	Free space	31555				
	Hardware version	0.6				
	Firmware version	0.6				
	Card ID	30300994				
	Product name	Datakey 330				
	Model	Datakey M 330				
	Card type	DKCCOS				
	OS version	DKCCOS V6.0				
	Mask version	N/A				
	Color	N/A				
	Supported key size	2048 bits				
	Token Password	Present				
₹ Þ	Token Password retries remaining	10				-
			⊖ gem	ALT	0.C0	М

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

S Initialize Token - Initialization Options	×
SafeNet Authentication Client	gemalto <sup>×</sup>
Warning! This operation will delete all token content. Please choose the way you want to initialize the token: Preserve the token settings and policies Configure all initialization settings and policies	
< Back, Next > Finish	Cancel

Odpre se okno za določitev gesla:

S Initialize Token - Password Settings	×
SafeNet Authentication Client	gemalto <sup>×</sup>
Token Name: SIMOD-PKI pametna kartica	
Create Token Password	•••••
Confirm Password:	•••••
Logon retries before token is locked:	10
Token password must be changed on first	t logon
Create Administrator Password:	
Create Administrator Password:	
Confirm Password:	
Logon retries before token is locked:	10
	Current Language: SL
< <u>B</u> ack	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«:

S Initialize Token - Password Quality Settings	×
SafeNet Authentication Client	gemalto <sup>×</sup>
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 character	ers: Mandatory
< <u>B</u> ack <u>N</u> ext >	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:

🤶 Initialize Token	×
Initializing token	
	52%
Warning: Do not remove the token. Removing the token during this operation will damage it.	

Po uspešni incializaciji 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":						
SafeNet Authentication Client Tools						_ 🗆 X
			g		nal arity to	to be free
SafeNet Authen	ticatior	n Client 🛛 🧔	9	1	?	
BIT4ID miniLector EVO 0	/	Rename Token	-			
SIMoD-PKI pametna kartica, 10.4	****	Change Token Password				
		Unlock Token				
	$\odot$	Delete Token Content				
	Q	View Token Info				
		Disconnect SafeNet Virtual Token				
		9	GEM	ALT	0.CO	м

Odpre se nov pogled:

		dema
		security
afaNlat Author	tication Olia.	<b>a</b> t
alemet Auther	incation Uter	່ 🔅 💁 🧎 💈
SafeNet Authentication Client Tools	🐼 🖪 🗔 🖓 🔪 🗏 🖪 🕅	
Tokens	🐼 k 🚧 🧰 🥖 k 📾 I	
BIT4ID miniLector EVO 0	Token name	SIMoD-PKI pametna kartica, 10.4
SilvioD-PKi pametna kartica, 10.4	Token category	Hardware
	Reader name	OMNIKEY CardMan 3x21 0
	Serial number (PKCS#11)	CBAAE4B0126DD3AD
Client Settings	Free space (minimum estimated)	24638
-0+	Hardware version	0.0
	Firmware version	N/A
	Card ID (Minidriver)	0x1B80005912982A741B80005912982A74
	Product name	IDPrime MD 840
		IV/A
	Cara type	
	Applet version	G260/File15
	Color	N/A
	Supported key size	2048 hits
	Token Password	Present
	Token Password retries remaining	3
	Maximum Token Password retries	3
emo na ikono 脑 , »Se	et Token Password« :	⊖ GEMALTO.C
emo na ikono 📔 , »Se	et Token Password« :	⊖ GEMALTO.C
emo na ikono 🕥 , »Se SafeNet Authentication Client Tools	et Token Password« :	⊖ GEMALTO.C
emo na ikono 🔛 , »Se SafeNet Authentication Client Tools	et Token Password« :	
emo na ikono 🕥 , »Se SafeNet Authentication Client Tools	et Token Password« :	GEMALTO.C     GEMALTO
emo na ikono 🕥 , »Se SafeNet Authentication Client Tools	et Token Password« :	
emo na ikono 🔛 , »Se SafeNet Authentication Client Tools SafeNet Auther	et Token Password« :	GEMALTO.C     Gemal     Gemal     Security to 1     O     Security to 1     Security to
emo na ikono 🕥 , »Se SafeNet Authentication Client Tools SafeNet Auther	et Token Password« :	Э GEMALTO.C Genal Security to 1 nt ŵ ŵ 1 ?
emo na ikono 🔊 , »Se SafeNet Authentication Client Tools	et Token Password« :	GEMALTO.C     GEMALTO.C     Gemal     Gemal     Security to     security to     security to     t     @      @     1     ?
emo na ikono in , »Se SafeNet Authentication Client Tools SafeNet Authentication Client Tools SafeNet Authentication Client Tools	et Token Password« :	GEMALTO.C Genal Security to At I I I I I I I I I I I I I I I I I I I
emo na ikono in , »Se SafeNet Authentication Client Tools SafeNet Authentication Client Tools SafeNet Authentication Client Tools SafeNet Authentication Client Tools	et Token Password« :	GEMALTO.C General Security to Nt @ @ 1 ?
emo na ikono , »Se SafeNet Authentication Client Tools SafeNet Authentication Client Tools SafeNet Authentication Client Tools SafeNet Authentication Client Tools BIT4ID miniLector EVO 0 BIT4ID miniLector EVO 0	et Token Password« :	GEMALTO.C
emo na ikono , »Se SafeNet Authentication Client Tools SafeNet Authentication Client Tools User certificates SimoD-PKI pametna kartica, 10.4	et Token Password« :	GEMALTO.C
emo na ikono , »Se SafeNet Authentication Client Tools SafeNet Authentication Client Tools SafeNet Authentication Client Tools Tokens BITAID miniLector EVO 0 SIMOD-PKI pametra kartica, 10.4 SIMOD-PKI pametra kartica, 10.4	et Token Password« :	GEMALTO.C
emo na ikono , »Se SafeNet Authentication Client Tools SafeNet Authentication Client Tools SafeNet Authentication Client Tools Tokens BIT4ID miniLector EVO 0 SIMOD-PKI pametna kartica, 10.4 User certificates Settings CC certificates Settings	et Token Password« : Token Dication Clier	GEMALTO.C
emo na ikono , »Se SafeNet Authentication Client Tools SafeNet Authentication Client Tools Cocertificates Settings Client Settings	et Token Password« :	GEMALTO.C
emo na ikono , »Se SafeNet Authentication Client Tools SafeNet Authentication Client Tools	et Token Password« :	GEMALTO.C       GEMALTO.C
emo na ikono (), »Se SafeNet Authentication Client Tools SafeNet Authentication Client Tools	et Token Password« :	GEMALTO.C       GEMALTO.C
emo na ikono (), »Se SafeNet Authentication Client Tools SafeNet Authentication Client Tools Control Client Settings	et Token Password« : Token Clien Noten ame Token category Reader name Serial number (PKCS#11) Free space (minimum estimated) Hardware version Firmware version Card ID (Minidriver) Product name Model	
emo na ikono (), »Se SafeNet Authentication Client Tools SafeNet Authentication Client Tools Coefficient Settings	et Token Password« :	GEMALTO.C       GEMALTO.C
emo na ikono (), »Se SafeNet Authentication Client Tools SafeNet Authentication Client Tools Coefficient Settings	et Token Password« : Token Clier Noten ante Token category Reader name Token category Reader name Serial number (PKCS#11) Free space (minimum estimated) Hardware version Card ID (Minidriver) Product name Model Card type Applet Version	GEMALTO.C       GEMALTO.C
emo na ikono (), »Se SafeNet Authentication Client Tools SafeNet Authentication Client Tools SafeNet Authentication Client Tools SafeNet Authentication Client Tools (), %Simode Client Setting (), %Simode Client Settin	et Token Password« : Token Clier Noten anne Token category Reader name Serial number (PKCS#11) Free space (minimum estimated) Hardware version Firmware version Card ID (Minidriver) Product name Model Card type Applet Version Mask version	GEMALTO.C       GEMALTO.C
emo na ikono (), »Se SafeNet Authentication Client Tools SafeNet Authentication Client Tools SafeNet Authentication Client Tools Tokens BITAID miniLector EVO 0 SIMOD-PKI pametra kartica, 10.4 SIMOD-PKI pametra kartica, 10.4 SiMoD-PKI pametra kartica, 10.4 Simod-PKI pametra kartica, 10.4 Settings	et Token Password« :	GEMALTO.C       GEMALTO.C
emo na ikono (), »Se SafeNet Authentication Client Tools SafeNet Authentication Client Tools SafeNet Authentication Client Tools Tokens BIT4ID miniLector EVO 0 SIMOD-PKI pametna kartica, 10.4 User certificates CC certificates Settings	et Token Password« : Token Clier Version Clier Version Clier Version Clier Version Clier Version Card ID (Minidriver) Product name Model Card type Applet Version Mask version Color Supported key size	
emo na ikono (), »Se SafeNet Authentication Client Tools SafeNet Authentication Client Tools SafeNet Authentication Client Tools SafeNet Authentication Client Tools () SafeNet Authentication Client Tools () SafeNe	et Token Password« : Token Clier Version Clier Version Clier Version Clier Version Clier Version Card ID (Minidriver) Product name Model Card type Applet Version Mask version Color Supported key size Token Password	GEMALTO.C         GEMALTO.C         Cont         Image: Set Token Password Intica, 10.4         Hardware         OMNIKEY CardMan 3x21 0         CBAAE480126DD3AD         24638         0.0         N/A         Drime MD 840         N/A         ID Prime MD 840         N/A         ID Prime MD         ID Prime MD         ID Prime MD         N/A         Present

GEMALTO.COM
 ■

Infrastruktura javnih ključev na MO, Navodilo za namestitev strojne in programske opreme ter uporabo osnovnih storitev Ver. 1.3, 28. Septemeber 2017 V polje »Administrator Password« vpišemo administratorsko geslo, ki smo ga dobili po pošti skupaj s pametno kartico in kliknemo »OK«:

SafeNet Authentica	tion Client Tools			
SafeNe	t Authen	tication Clier	nt 🍘	9 💿 <b>1 ? </b>
SafeNet Authentica	S Administrator Logo	n		X
∃	SafeNet Authe	ntication Client	gemalte security to be t	2 <sup>×</sup>
E - C User o E - C Cer E - C Setting Client Settings	Enter the Token's adminis Token Name:	strator Password. SIMoD-PKI pametna ka	artica, 10.4	
	Administrator Password:	•••••••••		82A74
		Current Language: SL	OK Cancel	
		Color Supported law size	N/A 2049 http://	
		Token Password	Present	
	Þ	Token Password retries remaining Maximum Token Password retries	3 3	<b></b>
			Ð	GEMALTO.COM

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

SafeNet Authentica	tion Client Tools			
SafeNe	t Authant Set Password: SIMo	tication Clien D-PKI pametna kartica, 10.4	†	a 1 ? 🖻
SafeNet Authentica	SafeNet Authe	ntication Client	gemalto <sup>×</sup>	
☐ Tokens BIT4ID mir ☐	Token Password: Confirm Password: Logon retries before toker The new password must of A secure password has at numerals, and special cha Current Language: SL Enter a new password.	n is locked: 15 comply with the quality settings defined or least 8 characters, and contains upper-c racters (such as !, \$, #, %).	The token.	B2A74
•		Token Password retries remaining Maximum Token Password retries	3 3	<b>•</b>
				EMALTO.COM

Infrastruktura javnih ključev na MO, Navodilo za namestitev strojne in programske opreme ter uporabo osnovnih storitev Ver. 1.3, 28. Septemeber 2017

Kliknemo »OK« in poja	vi se nam okno za	a uspešno odkl	epanje pametne kartice:
			1 2 1

🤶 SafeNet Authentica	tion Client Tools	
SafeNe	set Password: SIMOD-PKI pametna kartica, 10.4	a) i ? 💼
SafeNet Authentica	SafeNet Authentication Client genalic*	
BIT4ID mir SIMoD-PK SIMoD-PK SIMoD-PK CC cer Setting Client Settings	Token Password: Set Password: SIMoD-PKI pametna kartica, 10.4 X Confim Pass Logon retrie: The new pa A secure pa numerals, ar Current Language: SL	982A74
	OK         Cancel           Token Password retries remaining         3           Maximum Token Password retries         3	
	⊖ G	EMALTO.COM

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 >":

🚵 Recover Entrust Digital 1	ID	×
<b>Specify your activation</b> The wizard needs to kn Entrust digital ID.	codes ow your activation codes so that it can recover your	Ø
Enter your reference nu	mber and authorization code:	
<u>R</u> eference number:	58681476	
Authorization code:	WMRT-ISKO-44SA	
Your administrator reference number:	should have provided these values to you (for example, 91480170 and authorization code: CRTJ-8V0R-VFNS).	
	< <u>B</u> ack <u>N</u> ext > 0	Cancel

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 >":

💩 Recover Entrust Digital ID	×
Confirm Entrust Digital ID Recovery Entrust is now ready to recover your Entrust digital ID.	Ø
Click the Next button to recover your Entrust digital ID.	
Your administrator may have configured your recovery to display dialog boxes from other vendors. For example, Microsoft and/or smart card vendor's dialog boxes may appear during this part of the recovery wizard.	
< <u>B</u> ack <u>Next</u> > Cance	el

Indikatorska vrstica prikazuje, da se je postopek začel:

💩 Recover Entrust Digital ID	×
Confirm Entrust Digital ID Recovery Entrust is now ready to recover your Entrust digital	id.
Recovering Entrust digital ID; please wait.	
Betrieving policy certificates	
Your administrator may have configured your r other vendors. For example, Microsoft and/or may appear during this part of the recovery wi	ecovery to display dialog boxes from smart card vendor's dialog boxes zard.
<]	<u>3</u> ack <u>N</u> ext ≻ Cancel

Infrastruktura javnih ključev na MO, Navodilo za namestitev strojne in programske opreme ter uporabo osnovnih storitev Ver. 1.3, 28. Septemeber 2017

#### 41

V okence vpišite uporabniško geslo pametne kartice:

💩 Recover Entrust Digital ID		×
Confirm Entrust Digital ID Rec Entrust is now ready to recover	overy vour Entrust dinital ID	
S Token Logon		<u> </u>
SafeNet Authenticatio	n Client	gemalto
Enter the Token Password		
Token Name:	SIMOD-PKI pametna kartica	
Token Password:		
	Current Language: SL	
	OK	Cancel
	< <u>B</u> ack. <u>N</u> ext >	Cancel

Postopek obnove digitalnih potrdil lahko traja nekaj minut.

Ko je postopek zaključen, kliknite "Finish":

💩 Recover Entrust Digital ID	×	
Ø	Completing the Recover Entrust Digital ID Wizard	
	The Recover Digital ID Wizard has completed: - recovering your Entrust digital ID - saving the Entrust digital ID on your computer, in a Directory, and/or on a smart card	
	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.	
S	To close this wizard, click Finish.	
	< Back Finish Cancel	

# 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":

🛐 🛃 🖤 (° 🔺 🔶 =		Neimenovan - Sporočilo (HTML)	다 ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~
Datoteka Sporočilo Vstavljanje Mož	osti Oblikuj besedilo Pregled	Razvijalec	~ ⊘
Aa     Barve *     Barve *       A Pisave *     Barva *     Skp       U Ulinki *     Strani *       Teme     Pokaži polja	Dovoljenja	Zahtevaj potrdilo o dostavi Zahtevaj potrdilo o branju Siedenje w Več možnosti	Reportedni odgovori za ra
Za   Połiji Zadeva:			  

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 naslovniku:

🤶 Token Logon		×
SafeNet Authentication	n Client	gemalto <sup>×</sup>
Enter the Token Password		
Token Name:	SIMOD-PKI pametna kartica	•
Token Password:		
	Current Language: SL	
	OK	Cancel

#### 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 >":

Encrypt and Digitally Sign Files Wizard		
	Welcome to the Encrypt and Digitally Sign Files Wizard	
	This wizard will guide you through the process of encrypting and digitally signing files for yourself and others.	
	The files you are encrypting and signing are:	
	Test xlsx	
	To continue, click Next.	
	< Back. Next > Cancel	

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 >":

📑 Encrypt and Digitally Sign F	iles Wizard	
Encryption and Digital Signature Options Encrypted and digitally signed files are encrypted for yourself and optionally for other people and signed by yourself.		
Files are always encrypted	for yourself.	
Your Encryption Certificate:	Encryption Certificate Choose	
Encryption Algorithm:	AES256 (256-bit)	
Encrypt the files for othe	er people in addition to myself	
Your Signing Certificate:	Verification Certificate Choose	
Hash Algorithm:	SHA256	
Timestamp my signature	e	
Timestamp Authority:	Strežnik casovnega žiga 💌	
	< Back Next > Cancel	

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

📑 Enci	ypt and Digitally Sign Files Wizard	2
Add	itional Recipients Select the other people these files will be en yourself will be able to decrypt the files.	crypted for. Only these people and
	To encrypt files for other people you need th to select the other people you wish to encry	eir encryption certificates. Use the Add button ot for.
	Name	E-mail Address
		<u>A</u> dd <u>R</u> emove <u>V</u> iew
		< <u>B</u> ack <u>N</u> ext > Cancel

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

🕌 Selec	t People			<u>? ×</u>
<u> </u>	Please select the other people yo encryption certificates.	ou wish to encrypt for. Use the	e search button to search the direc	tory for their
	🔎 Tes		<b>T</b>	Search 🝷
	Name	Email		
	•			▶
	Show: Search Results	•		⊻iew
			OK Cancel	Help

inienik do vinii sezhani uporadnikov, ki se vsedujejo niz cik iz iskanega kinenja	Imenik bo vrnil seznam ur	porabnikov, ki se	vsebujejo niz	črk iz iskalnega k	riterija:
---	---------------------------	-------------------	---------------	--------------------	-----------

🕌 Selec	t People		? ×
<u>2</u> 8	Please select the other people you wish to encryption certificates.	encrypt for. Use the search button to search the directo	ory for their
	P Tes		Search 🔻
	Name	Email	
	cert-osebe-A		
	Test Second 1234568	Drugi.Test@mors.si; Second.Test@mors.si	
	Test Third 1234569	Tretji.Test@mors.si; Third.Test@mors.si	
	Test Cetrti 1234570	Cetrti.Test@mors.si	
	Test Peti 1234571	Peti.Test@mors.si	
	cert-splosno-A		•
	•		•
	Show: Search Results		⊻iew
		OK Cancel	Help

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

🕌 Selec	ct People	<u>? </u> ×
<u>8</u> ª	Please select the other people you wish to encryption certificates.	encrypt for. Use the search button to search the directory for their
	🔎 Tes	▼ Search ▼
	Name	Email
	cert-osebe-A	
	Test Second 1234568	Drugi.Test@mors.si; Second.Test@mors.si
	Test Third 1234569 Tretji.Test@mors.si; Third.Test@mors.si	
	Test Cetrti 1234570	Cetrti.Test@mors.si
	Test Peti 1234571	Peti.Test@mors.si
	cert-splosno-A	-
	•	
	Show: Search Results	▼ <u>V</u> iew
		OK Cancel Help

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

📑 Encry	pt and Digitally Sign Files Wizard		×
Addit S	tional Recipients elect the other people these files will be en ourself will be able to decrypt the files.	crypted for. Only these people and	
T to	o encrypt files for other people you need th select the other people you wish to encryp	eir encryption certificates. Use the Add button ot for.	
Γ	Name	E-mail Address	
-	Test Second 1234568	Drugi.Test@mors.si; Second.Test@mo	
		<u>A</u> dd <u>R</u> emove <u>V</u> iew	
		< <u>B</u> ack <u>N</u> ext > Cancel	

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:

🤶 Token Logon		×
SafeNet Authenticatio	n Client	gemalto <sup>×</sup>
Enter the Token Password		
Token Name:	SIMoD-PKI pametna kartica SAC104	
Token Password:		
	Current Language: SL	
	OK	Cancel

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

📑 Encrypt and Digitally Sign Files Wizard		
Ģ	Completing the Encrypt and Digitally Sign Files Wizard	
	You have successfully encrypted and signed the following files:	
	test xlsx.p 7m	
	✓ Delete the original files on finish	
	< Back Finish Cancel	

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.