

AD CS

9. PREDAVANJE



- Kratak pregled PKI
- Implementacija CA
- Implementacija i upravljanje predlošcima certifikata
- Distribucija i povlačenje certifikata iz uporabe
- Povrat izgubljenih certifikata



Kratki pregled PKI

- Što je PKI?
- Komponente PKI rješenja
- Što su CA?
- Pregled AD CS uloge u Windows Server 2012
- Što je novo u AD CS u Windows Server 2012
- Javni vs. Privatni CA
- Što je Cross-Certifikacijska hijerarhija?



Algebra

visoka škola za
primijenjeno računarstvo

Što je PKI?

PKI :

- Je standardizirani pristup sigurnosno baziranim alatima, tehnologijama, procesima, i servisima koji se koriste da bi povećali sigurnost komunikacije, aplikacija i poslovnih transakcija
- Zasniva se na razmjeni digitalnih certifikata između autenticiranih korisnika i resursa kojima vjerujemo

PKI provides:

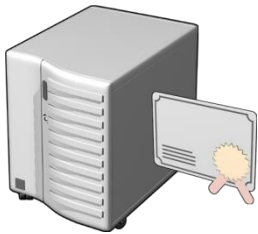
- Confidentiality (povjerljivost)
- Integrity (integritet)
- Authenticity (izvornost)
- Non-repudiation (neodbijanje (načelo prema kojemu primatelj poruke ne može tvrditi da poruku nije primio, niti pošiljatelj može tvrditi da poruku nije poslao))



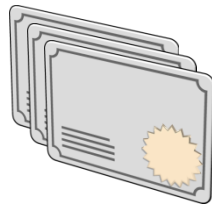
Algebra

visoka škola za
primijenjeno računarstvo

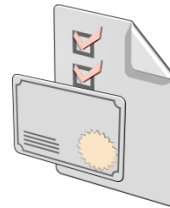
Komponente PKI rješenja



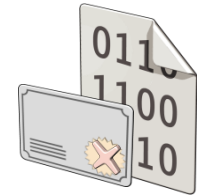
CA



Digital Certificates



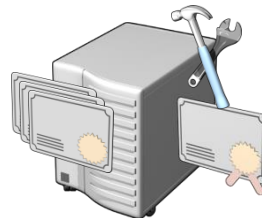
Certificate Templates



CRLs and Online Responders



Public Key-Enabled Applications and Services



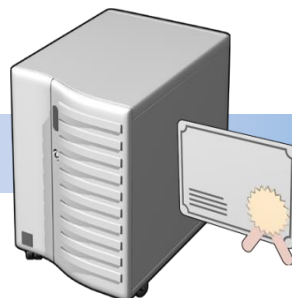
Certificates and CA Management Tools



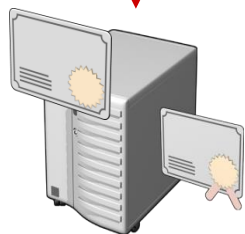
AIA and CDPs



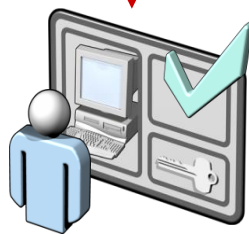
Što su CA?



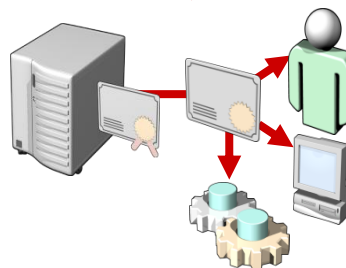
Root CA



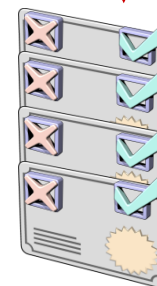
Izdaje certifikat
sam sebi



Provjerava identitet
tražioca certifikata



Izdaje certifikate
korisnicima, računalima i
servisima



Upravlja
povlačenjem
certifikata iz
uporabe

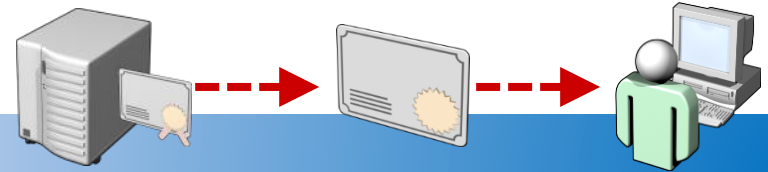


Algebra

visoka škola za
primijenjeno računarstvo

Pregled AD CS uloge u Windows Server 2012

CA



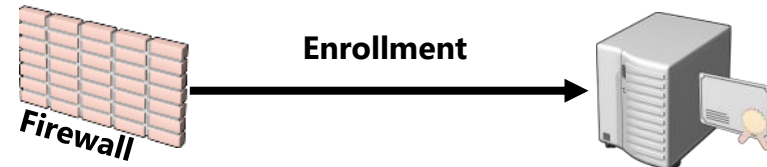
CA Web Enrollment



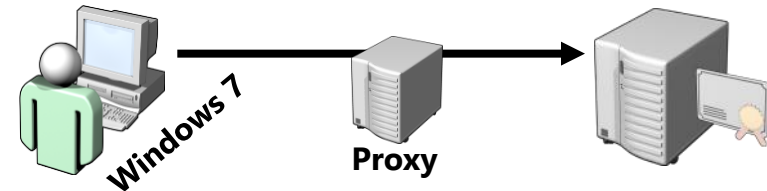
Online Responder



Network Device Enrollment Service



Certificate Enrollment Web Service



Certificate Enrollment Policy Web Service



Što je novo u AD CS u Windows Server 2012

- Sve AD CS uloge rade na svim Windows Server verzijama
- Integracija s Server Manager konzolom
- Upravljanje putme Windows PowerShell
- Nova verzija predloška certifikata (v4)
- Podrška za automatsko obnavljanje certifikata računala koji nisu članovi domene
- Prisilna obnova certifikata s istim ključem
- Dodatna sigurnost prilikom traženja certifikata
- Podrška za virtualne pametne kartice



Algebra

visoka škola za
primijenjeno računarstvo

Interni privatni CA:

- Zahtjeva veću administraciju nego eksterni javni CA
- Košta manje nego eksterni CA i nudi veću kontrolu nad izdavanjem certifikata
- Inicijalno mu ne vjeruju vanjski klijenti
- Nudi mogućnost prilagodbe predložaka certifikata i automatsko izdavanje

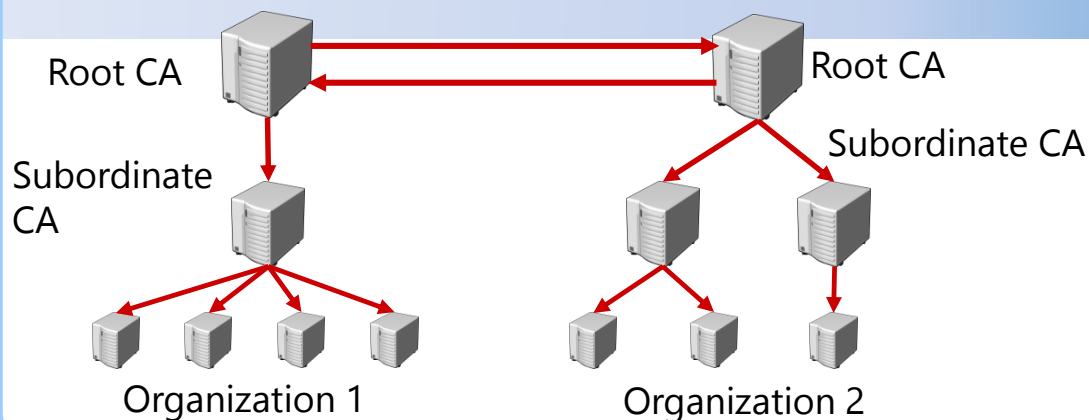
Eksterni javni CA:

- Vjeruju im mnogi klijenti (web preglednici, aplikacije, operativni sustavi)
- Sporije izdaju certifikate

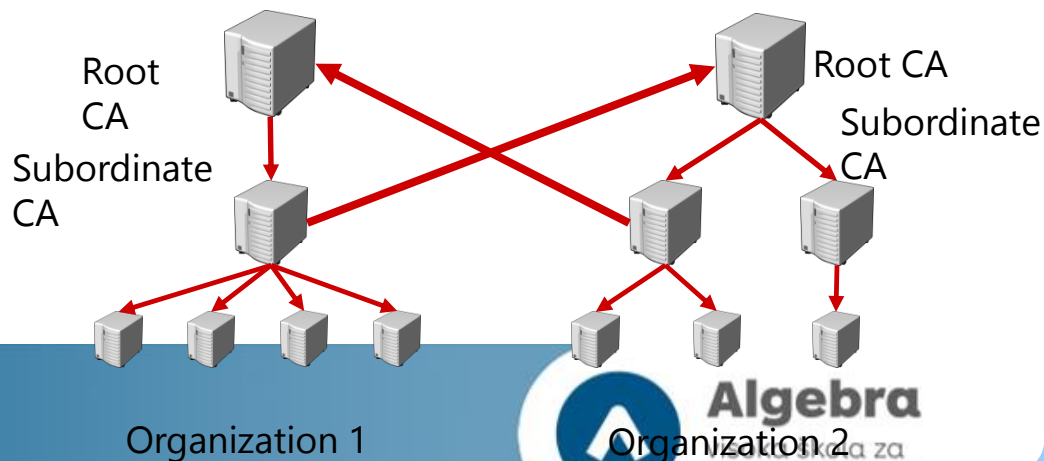


Što je Cross-Certifikacijska hijerarhija?

Cross-Certification na razini Root CA



Cross-Certification Subordinate CA prema Root CA



Implementacija CA

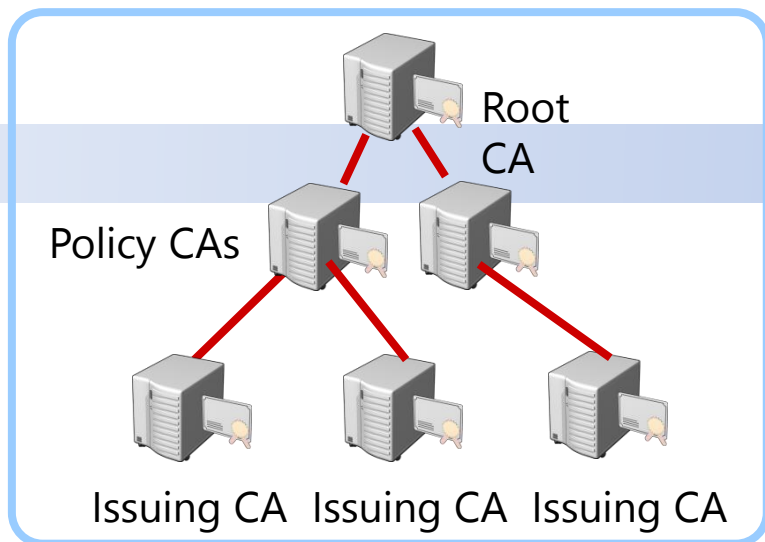
- Opcije za implementaciju CA hijerarhije
- Standalone vs. Enterprise CA
- Implementacija Root CA
- Implementacija Subordinate CA
- Kako koristiti CAPolicy.inf datoteku za instalaciju



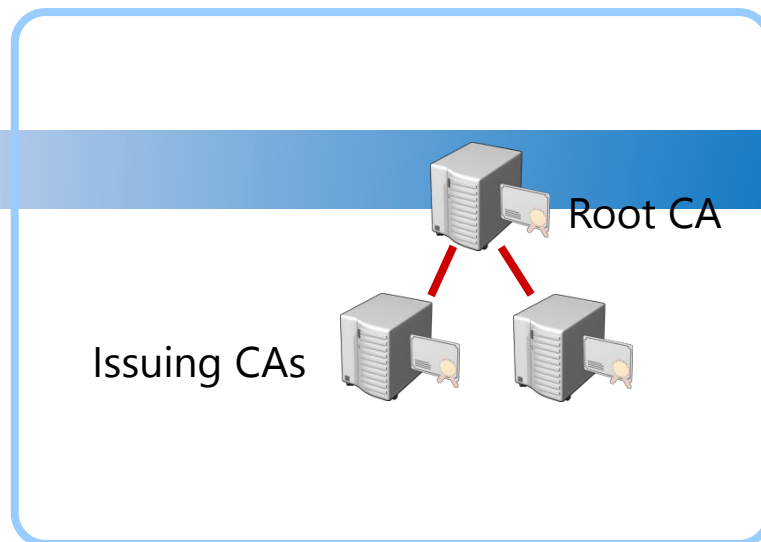
Algebra

visoka škola za
primijenjeno računarstvo

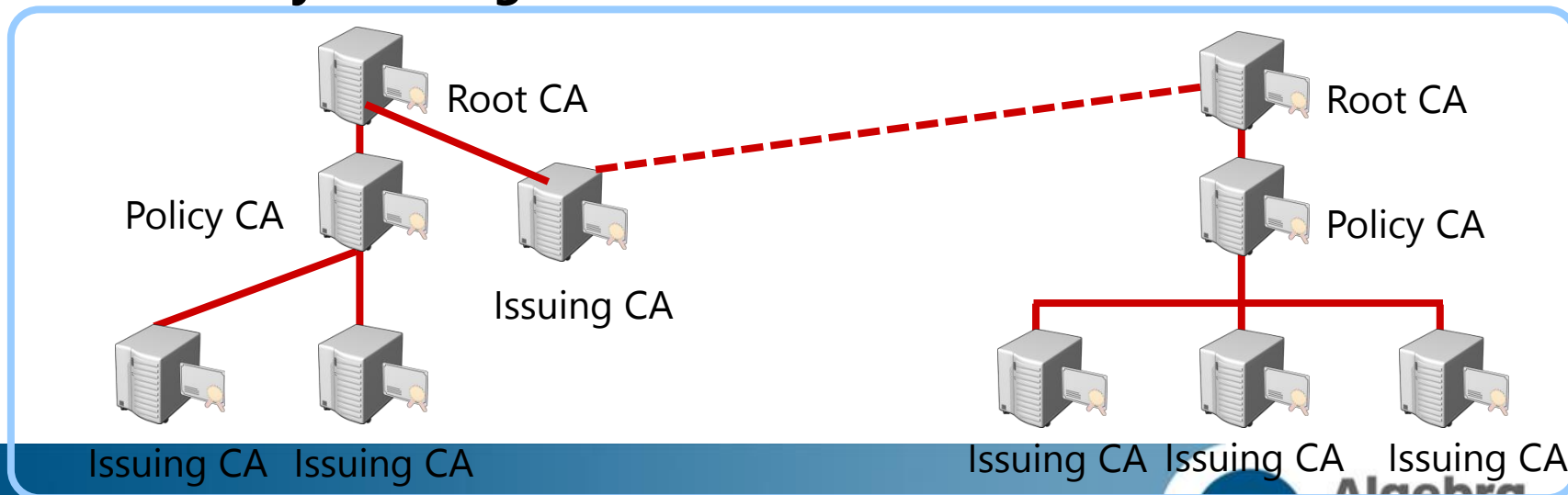
Opcije za implementaciju CA hijerarhije



Policy CA Usage




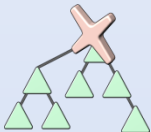

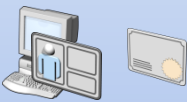
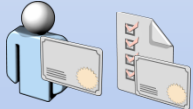




Two-Tier Hierarchy



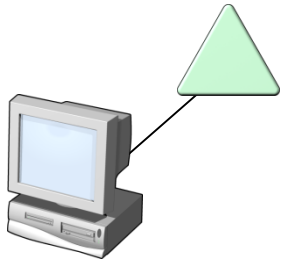
Cross-Certification Trust



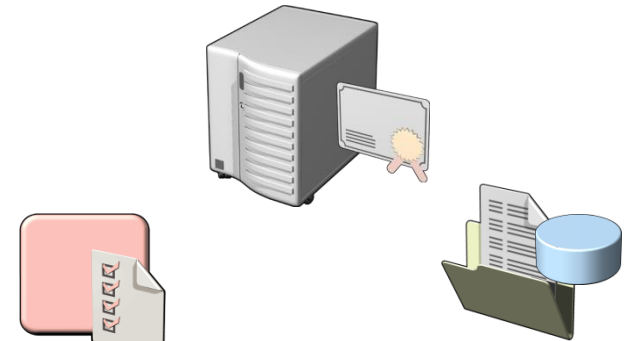
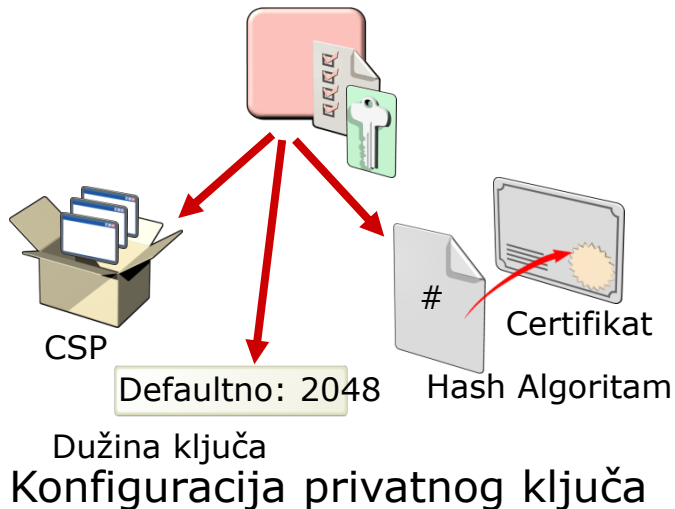
Standalone vs. Enterprise CA

Stand-Alone CA		Enterprise CA	
	<p>Stand-alone CA se mora koristiti ako je ijedan CA (root ili intermediate / policy) nedostupan, zbog toga što stand-alone CA nije dio AD domain</p>		<p>Zahtjeva postojanje domene</p>
			<p>Može pomoću Group Policya propagirati certifikate u Trusted Root Certificate Store na klijentima</p>
	<p>Korisnici sami upisuju podatke o sebi i o tipu certifikata koji im treba</p>		<p>Objavljuje korisničke certifikate i CRL u AD</p>
	<p>Ne zahtjeva postojanje predložaka za certifikate</p>		<p>Kreira i izdaje certifikate na osnovu predložaka</p>
	<p>Svi certifikati su na čekanju dok ih administrator ne odobri</p>		<p>Ima podršku za autoenrollment</p>

Implementacija Root CA



Ime računala i članstvo
u domeni



Ime i konfiguracija

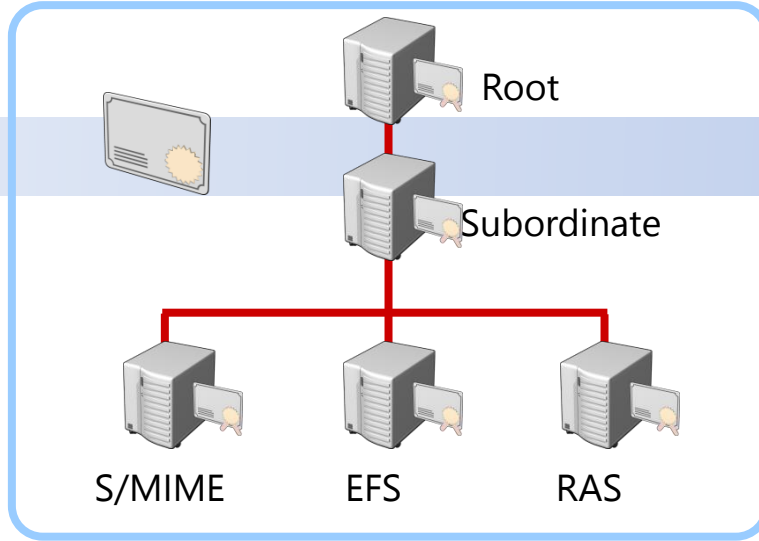
Lokacija baza i logova



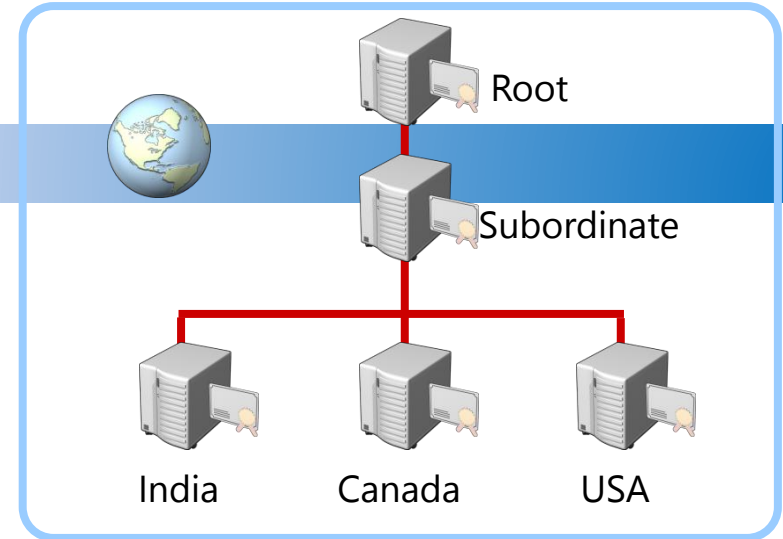
Trajanje certifikata

Plamiranje Root CA

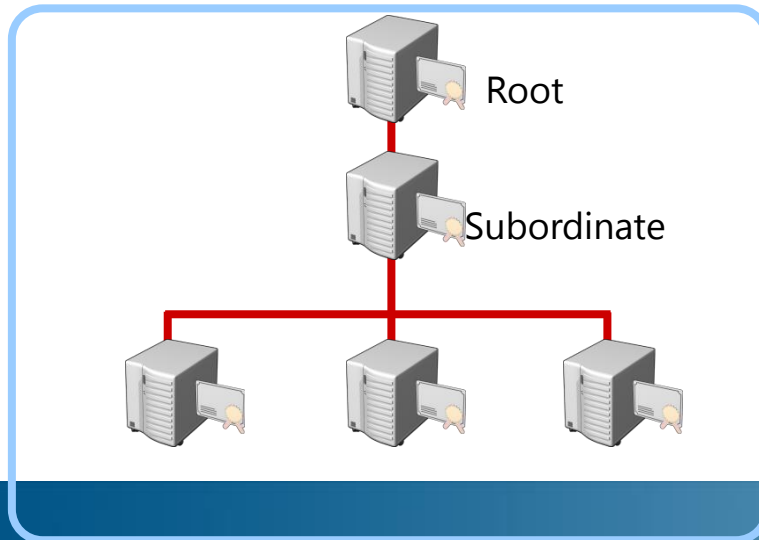
Implementacija Subordinate CA



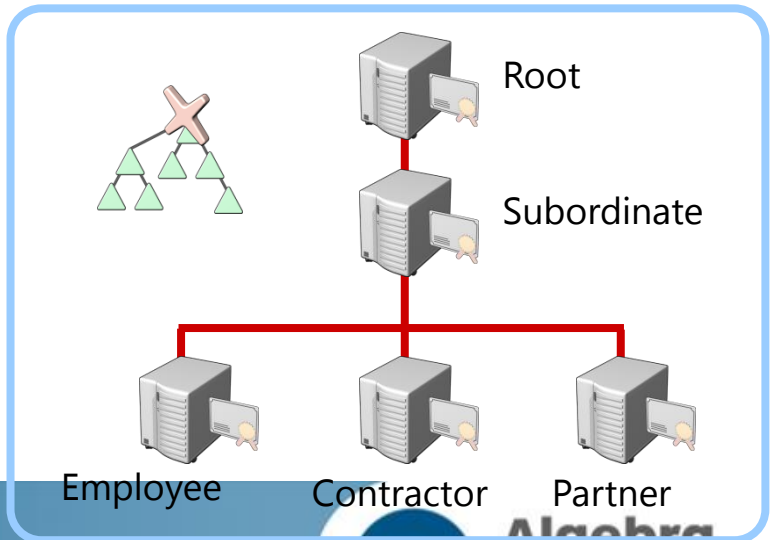
Certificate Uses



Locations



Load Balancing



Kako koristiti CAPolicy.inf datoteku za instalaciju

CAPolicy.inf je spremljen u direktoriju %Windir% subordinate CA. Ova datoteka definira sljedeće:

- CPS
- Object Identifier
- CRL publication intervals
- CA renewal settings
- Key size
- Certificate validity period
- CDP and AIA paths



Algebra

visoka škola za
primijenjeno računarstvo

Implementacija i upravljanje predlošcima certifikata

- Što su predlošci certifikata?
- Verzije predložaka u Windows Server 2012
- Konfiguracija dozvola za predloške
- Konfiguracija postavki predložaka
- Opcije za nadogradnju predložaka certifikata



Algebra

visoka škola za
primijenjeno računarstvo

Što su predlošci certifikata?

Predložak certifikata definira:

- Format i sadržaj certifikata
- Proces za kreiranje i izdavanje certifikata
- Sigurnosne principale koji mogu read, enroll, ili koristiti Autoenroll za sve certifikate bazirane na tom predlošku
- Dozvole koje definiraju tko može modificirati predložak certifikata



Algebra

visoka škola za
primijenjeno računarstvo

Verzije predložaka u Windows Server 2012

Version 1:

- Introduced in Windows 2000 Server, provided for backward compatibility in newer versions
- Created by default when a CA is installed
- Cannot be modified (except for permissions) or removed, but can be duplicated to become version 2 or 3 templates (which can then be modified)

Version 2:

- Default template introduced with Windows Server 2003
- Allows customization of most settings in the template
- Several preconfigured templates are provided when a CA is installed

Version 3:

- Supports advanced Suite B cryptographic settings
- Includes advanced options for encryption, digital signatures, key exchange, and hashing
- Only supports Windows Server 2008 and Windows Server 2008 R2 servers
- Only supports Windows Vista and Windows 7 client computers

Version 4:


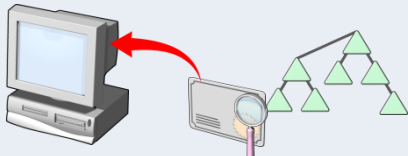
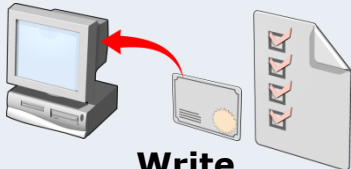
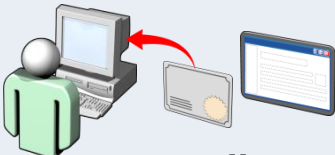
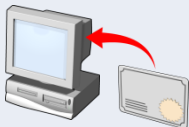
- Available only for Windows Server 2012 and Windows 8 clients
- Supports both CSPs and KSPs
- Supports renewal with the same key



Algebra



visoka škola za
primijenjeno računarstvo

Konfiguracija dozvola za predloške

Dozvola	Opis
 Full Control	Omogućava modificiranje svih atributa predloška uključujući i vlasništvo i dozvole drugih korisnika
 Read	Omogućava čitanje informacija iz predloška prilikom kreiranja zahtjeva za predložak
 Write	Omogućava modifikaciju svih atributa predloška osim dozvola
 Enroll	Omogućava kreiranje zahtjeva za izdavanje certifikata prema odabranom predlošku
 Autoenroll	Omogućava izdavanje certifikata korištenjem Autoenrollment procesa

Konfiguracija postavki predložaka

Za svaki predložak možemo prilagoditi neke od postavki, kao što su: vrijeme trajanja, svrha, CSP, eksportiranje privatnog ključa i zahtjevi za izdavanje certifikata

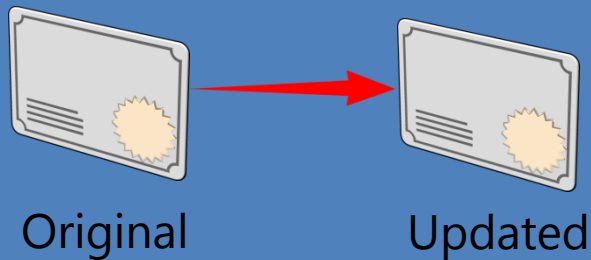
Kategorija	Primjer jedne svrhe	Primjer više svrha
 Korisnici	<ul style="list-style-type: none">• Basic EFS• Authenticated session• Smart card logon	<ul style="list-style-type: none">• Administrator• User• Smart card user
 Računala	<ul style="list-style-type: none">• Web server• IPsec	<ul style="list-style-type: none">• Computer• Domain controller



Algebra

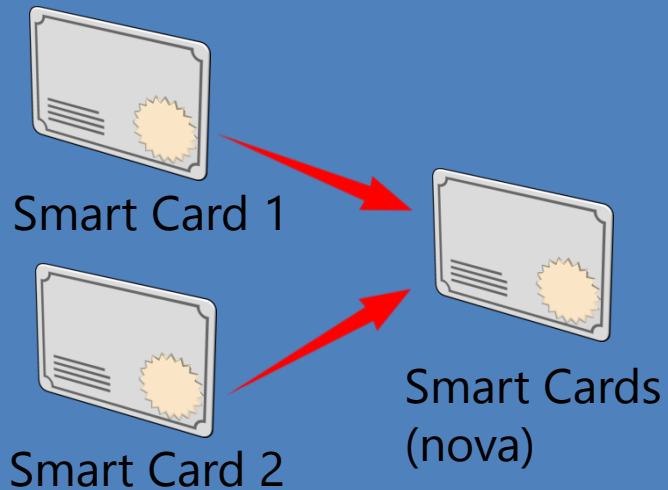
visoka škola za
primijenjeno računarstvo

Opcije za nadogradnju predložaka certifikata



Modifikacija

Modifikacija postojećeg predloška
da bi se dodale nove opcije



Superseding

Zamjena jednog ili više predložaka s
novim predloškom

Distribucija i povlačenje certifikata iz uporabe

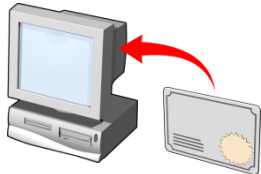
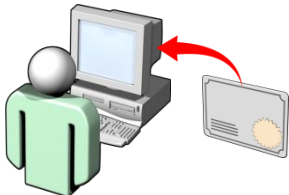
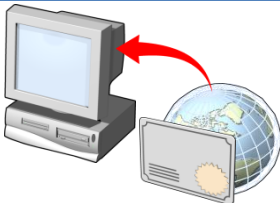
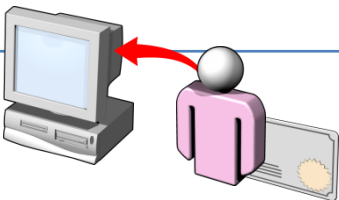
- Opcije za izdavanje certifikata
- Kako radi Autoenrollment proces?
- Što je Restricted Enrollment Agent?
- Što je Network Device Enrollment Service?
- Kako funkcionira prijevremeno povlačenje certifikata?
- Objavljivanje AIAs i CDP
- Što je Online Responder?



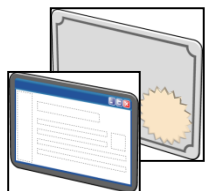
Algebra

visoka škola za
primijenjeno računarstvo

Opcije za izdavanje certifikata

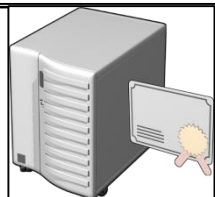
Metoda	Koristi se
 Autoenrollment	<ul style="list-style-type: none">• Automatizaciju zahtjeva, instaliranja, i spremanja certifikata za domenska računala
 Manual enrollment	<ul style="list-style-type: none">• Zahtjevanje certifikata korištenjem MMC konzole ili Certreq.exe naredbe, kada tražitelj ne može komunicirati direktno s CA
 CA Web enrollment	<ul style="list-style-type: none">• Zahtjevanje certifikata s web servera na CA serveru (http://ServerName/certsrv)• Da bi se izdali certifikat kada autoenrollment nije dostupan
 Enroll on behalf	<ul style="list-style-type: none">• Da bi dali CA administratoru da zatraži certifikat u ime drugog korisnika (Enrollment Agent)

Kako radi Autoenrollment proces?



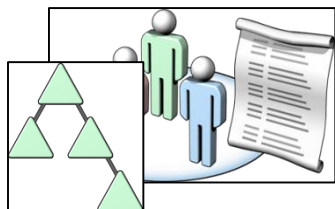
Certificate template

Predložak certifikata se konfigurira da omogući, enroll i autoenroll dozvole za korisnike koji traže ovaj certifikat.



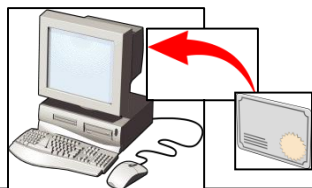
Certification authority

CA je konfiguriran da izda prije definirani predložak.



Group Policy Object

Active Directory Group Policy Object (GPO) se kreira i konfigurira za autoenrollment. GPO je linkan na odgovarajući site, domenu, ili organizacijsku jednicu.



Client machine

Klijentsko računalo dobije certifikat prilikom sljedećeg obnavljanja GP objekata.

Što je ograničeni Enrollment Agent?

Ograničeni Enrollment Agent:

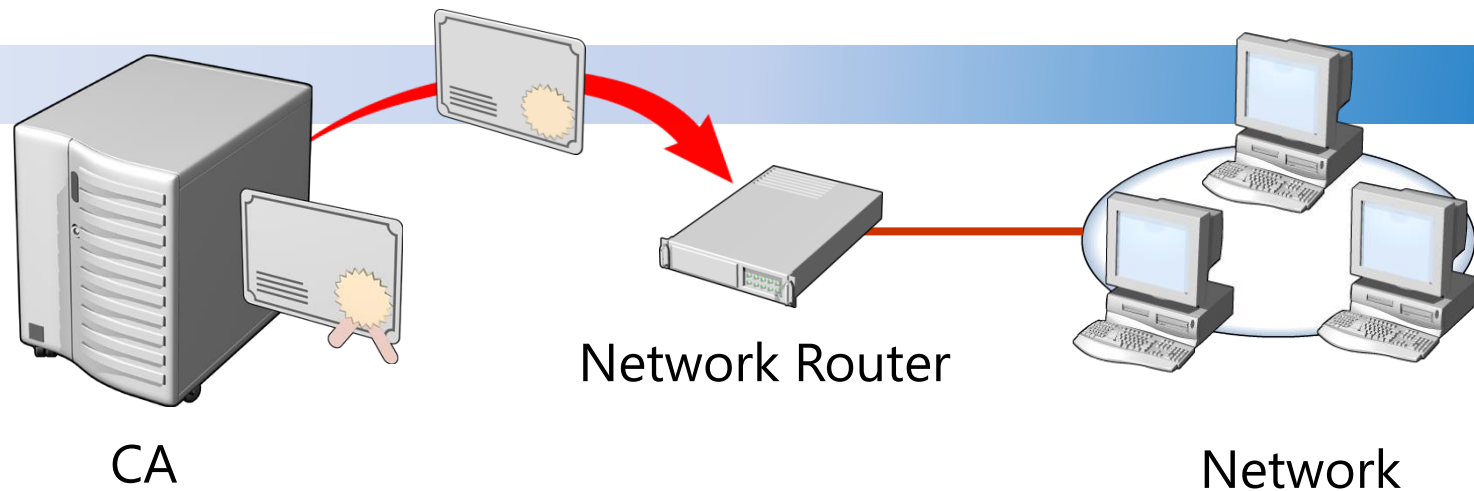
- Ograničava dozvole za enrollment agenta
- Zahtjeva Windows Server 2008 Enterprise ili Windows Server 2012 CA
- Koristi verziju 3 ili 4 predložaka



Algebra

visoka škola za
primijenjeno računarstvo

Što je Network Device Enrollment Service?



NDES:

- Koristi SCEP za komunikaciju s mrežnim uređajima
- Funkcionira kao servis uloge AD CS
- Zahtjeva IIS

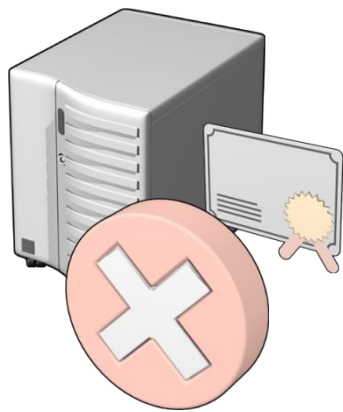


Algebra

visoka škola za
primijenjeno računarstvo

Kako funkcionira prijevremeno povlačenje certifikata?

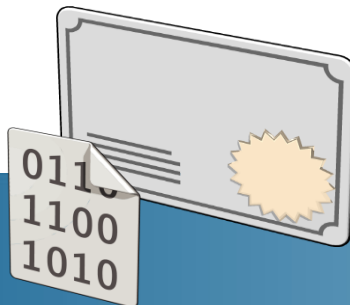
1 Certifikat je povučen



2 Objavljuje se povlačenje certifikata



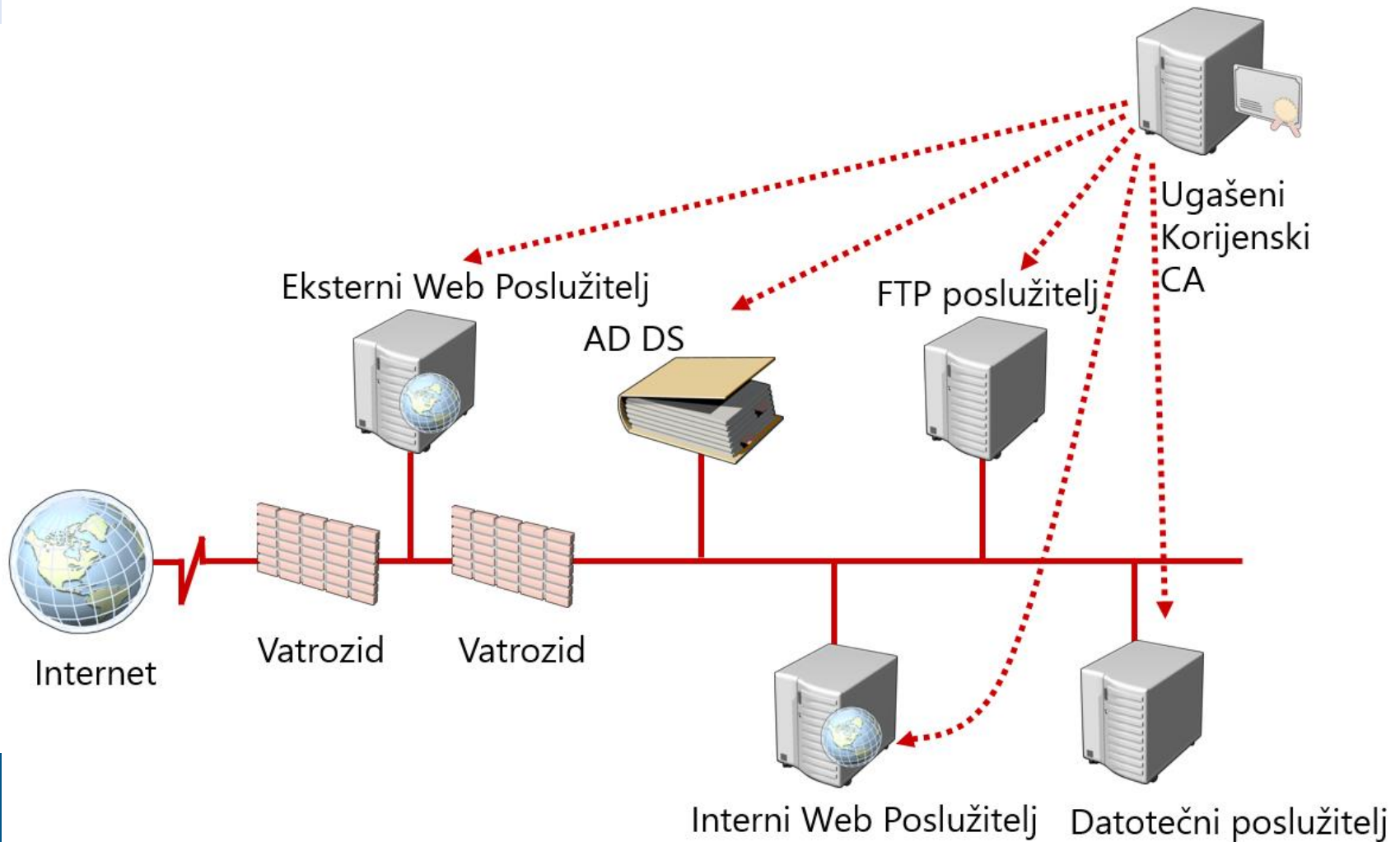
3 Klijentsko računalo provjerava ispravnost certifikata



Algebra

visoka škola za
primijenjeno računarstvo

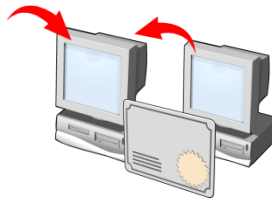
Objavljivanje AIA i CDP



Što je Online Responder?



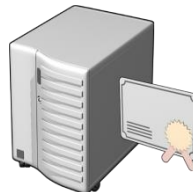
Koristi OCSP validaciju i provjeru pomoću HTTP



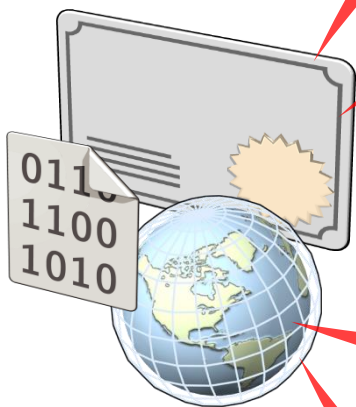
Zaprema i odgovara dinamički na upite



Podržava samo Windows Server 2008, Windows Vista, i novije Windows operative sustave



Funkcionira kao responder za više CA



Povrat izgubljenih certifikata

- Pregled arhiviranja i povrata ključeva
- Konfiguracija automatskog arhiviranja ključeva
- Povrat izgubljenih ključeva



Algebra

visoka škola za
primijenjeno računarstvo

Pregled arhiviranja i povrata ključeva

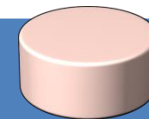
Ključeve možemo izgubiti kada:

- Obrišemo korisnički profil
- Reinstaliramo OS
- Disk se ošteti
- Računalo je ukradeno



Metode povrata podataka uključuju:

- Arhiviranje ključeva i KRA
- Ručno arhiviranje ključeva i povrat



Algebra

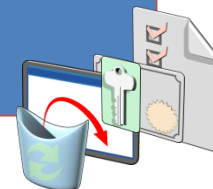
visoka škola za
primijenjeno računarstvo

Konfiguracija automatskog arhiviranja ključeva

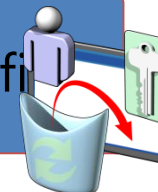
Koraci za automatsko arhiviranje ključeva:



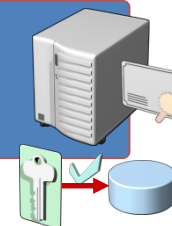
Konfigurirajmo i izdajmo KRA predložak



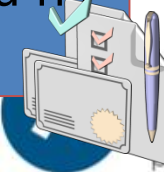
Odredimo tko će biti KRA i dodijelimo mu certifikat



Omogućimo arhiviranje ključeva na CA



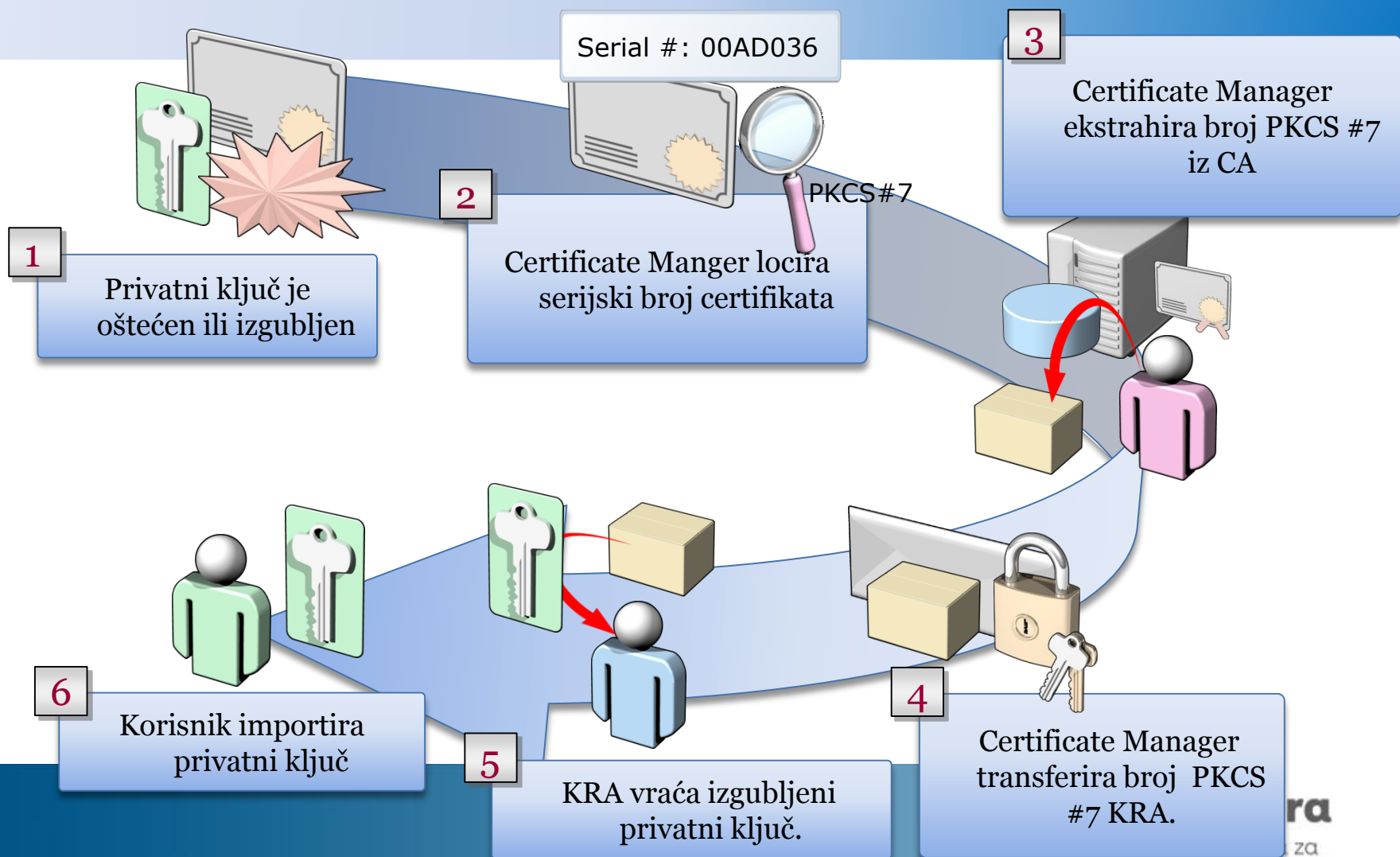
Modificirajmo i omogućimo arhiviranje ključeva na predlošku



Algebra

soka škola za
primijenjeno računarstvo

Povrat izgubljenog ključa





Algebra

visoka škola za
primijenjeno računarstvo