Integracija kIDCA certifikata u domensko okruženje

Zagreb

Verzija 1.3

Sadržaj

1 Integracija 3
1.1 Infrastrukturni preduvjeti 3
1.1.1 SmartCard Infrastructure Requirements 3
1.2 Pretpostavke i potrebne promjene 3
1.2.1 Potrebne promjene i pretpostavke na domenskim servisima 3
How to import third-party certification authority (CA) certificates into the Enterprise NTAuth store 4
Posebno odjeljak: 4
1.2.2 Potrebne promjene na TMG poslužitelju 6
1.2.3 Potrebne promjene na Outlook klijentima 6

1 Integracija

1.1 Infrastrukturni preduvjeti

Da bi se moglo podržati sigurno logiranje smart karticama na domenu te potpisivanje emailova i dokumenata potrebno je napraviti određena podešavanja na infrastrukturnim servisima koji uključuju domenske poslužitelje, Exchange poslužitelje i klijente te TMG poslužitelje i klijente.
U nastavku dokumenta su zbirno navedena potrebna podešavanja uz linkove na službenu Microsoft dokumentaciju(TechNet članke) u kojima su određeni postupci detaljno opisani.

1.1.1 SmartCard Infrastructure Requirements

Smart Card Authentication to Active Directory requires that Smartcard workstations, Active Directory, and Active Directory domain controllers be configured properly. Active Directory must trust a certification authority to authenticate users based on certificates from that CA. Both Smartcard workstations and domain controllers must be configured with correctly configured certificates.

As with any PKI implementation, all parties must trust the Root CA to which the issuing CA chains. Both the domain controllers and the smartcard workstations trust this root.

1.1.1.1 Active Directory and domain controller configuration

- Required: Active Directory must have the third-party issuing CA in the NTAuth store to authenticate users to active directory.
- Required: Domain controllers must be configured with a domain controller certificate to authenticate smartcard users.
- Optional: Active Directory can be configured to distribute the third-party root CA to the trusted root CA store of all domain members using the Group Policy.

1.1.1.2 Smartcard certificate and workstation requirements

- Required: All of the smartcard requirements outlined in the "Configuration Instructions" section must be met, including the text formatting of the fields. Smartcard authentication fails if they are not met.
- Required: The smartcard and private key must be installed on the smartcard.

1.2 Pretpostavke i potrebne promjene

1.2.1 Potrebne promjene i pretpostavke na domenskim servisima

1.2.1.1 Domain kontroler poslužitelji i sva klijentska računala moraju imati pristup internetu do CRL lista koje su objavljene na ID web stranicama na slijedećoj lokaciji:

http://crl1.id.hr/akdcaroot.crl

http://crl2.id.hr/akdcaroot.crl

http://crl1.id.hr/kidca.crl

http://crl2.id.hr/kidca.crl

1.2.1.2 Postupak importanja third-party CA certifikata u Enterprise NTAuth store

Potrebi certifikati za import nalaze se na lokacijama :

- http://id.hr/cert/akdcaroot.crt
- http://id.hr/cert/kidca.crt

How to import third-party certification authority (CA) certificates into the Enterprise NTAuth store

Guidelines for enabling smart card logon with third-party certification authorities

Posebno odjeljak:

To import a CA certificate into the Enterprise NTAuth store, follow these

steps:

1. Export the certificate of the CA to a .cer file. The following file formats are supported:
   ○ DER encoded binary X.509 (.cer) ○
   Base-64 encoded X.509 (.cer)
2. At a command prompt, type the following command, and then press ENTER:
   certutil -dspublish -f *filename* NTAuthCA

The contents of the NTAuth store are cached in the following registry location:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EnterpriseCertificates\NTAuth\Certificates
This registry key should be automatically updated to reflect the certificates that are published to the NTAuth store in the Active Directory configuration container. This behavior occurs when Group Policy settings are updated and when the client-side extension that is responsible for autoenrollment executes. In certain scenarios, such as Active Directory replication latency or when the **Do not enroll certificates automatically** policy setting is enabled, the registry is not updated. In such scenarios, you can run the following command manually to insert the certificate into the registry location:
certutil -enterprise -addstore NTAuth *CA_CertFilename.cer*

1.2.1.3 Uključivanje postavki „Allow certificates with no extended key usage certificate attribute" i „Force the reading of all certificates from the smart card"

U AD Group policy-u Administrative Templates->Windows Components->Smart Card potrebno je omogućiti postavku „Allow certificates with no extended key usage certificate attribute„

Group Policy setting	Registry key	Default	Description

Allow no certificates with extended k usage certificate attribute	AllowCertificatesWithNoEKU	Enabled	This policy setting allows certificates without an enhanced key usage (EKU) set to be used for logon. In versions of Windows prior to Windows Vista, smart card certificates that are used for logon require an EKU extension with a smart card logon object identifier. This policy setting can be used to modify that restriction. **Enabled** Certificates with the following attributes can also be used to log on with a smart card: • Certificates with no EKU • Certificates with an All Purpose EKU • Certificates with a Client Authentication EKU **Disabled** or **Not Configured** Only certificates that contain the smart card logon object identifier can be used to log on with a smart card.
Force the reading of all certificates from the smart card	ForceReadingAllCertificates	Enabled	This policy setting allows you to manage the reading of all certificates from the smart card for logon. During logon, Windows reads only the default certificate from the smart card unless it supports retrieval of all certificates in a single call. This setting forces Windows to read all the certificates from the card. This can introduce a significant performance decrease in certain situations.

			Contact the smart card vendor to determine if your smart card and associated CSP support the required behavior. Enabled Windows attempts to read all certificates from the smart card regardless of the CSP feature set. Disabled or Not Configured Windows only attempts to read the default certificate from smart cards that do not support retrieval of all certificates in a single call. Certificates other than the default are not available for logon.

1.2.2 Potrebne promjene na TMG poslužitelju

How to Support Smart Card Logon for Remote Access VPN Connections

Configuring VPN remote access connections to use NAP based quarantine

Overview of virtual private networks (VPN)

1.2.3 Potrebne promjene na Outlook klijentima

Configure the Address Book for LDAP