

# Domeny – główna domena

Domeny zapewniają logiczny podział DPG, administracyjny i developerski.

- Główna/Podstawowa domena: *default*
- Ustawienia dostępne tylko w domenie *default*
  - interfejsy sieciowe
  - użytkownicy, grupy i kontrola dostępu
  - domeny aplikacyjne

# Katalogi plików - konfiguracje

Store	Scope	Usage
<b>config:</b>	Per application domain; not shared	Stores configuration files for the current application domain
<b>export:</b>	Per application domain; not shared	Holds any exported configuration that is created with the Export Configuration operation
<b>local:</b>	Per application domain; <i>possibly visible to other domains</i>	Storage space for files that local services use, including XML style sheets, XML schemas, and WSDL documents <ul style="list-style-type: none"><li>• Use the <b>visible domains</b> setting to view the local file store of other application domains</li></ul>
<b>store:</b>	<i>System-wide</i> ; shared	Sample and default style sheets that DataPower services use <ul style="list-style-type: none"><li>• A common practice is to copy these style sheets into your local directory before you change them</li></ul>
<b>temporary:</b>	Per application domain; not shared	Temporary disk space that document processing rules and actions use, and is cleared on an appliance restart

# Katalogi plików - bezpieczeństwo

Store	Scope	Usage
<b>cert:</b>	Per application domain; not shared	Location to store private keys and digital certificates <ul style="list-style-type: none"><li>• System automatically encrypts all files in this store</li><li>• After being added, files cannot be copied or modified</li><li>• You can delete digital certificates and private keys</li></ul>
<b>sharedcert:</b>	<i>System-wide</i> ; shared between application domains	Stores digital certificates to be shared with business partners <ul style="list-style-type: none"><li>• System automatically encrypts all files in this store</li></ul>
<b>pubcert:</b>	<i>System-wide</i> ; shared between application domains	Provides security certificates for root certificate authorities, such as the ones used by web browsers <ul style="list-style-type: none"><li>• System automatically encrypts all files in this store</li><li>• Files cannot be modified, but they can be copied</li></ul>

# Katalogi plików - logowanie

Store	Scope	Usage
<b>logtemp:</b>	Per application domain; not shared	Default location of log files, such as the system-wide default log <ul style="list-style-type: none"><li>• The file store size is fixed at 13 MB</li></ul>
<b>logstore:</b>	Per application domain; not shared	Long-term storage space for log files

# Katalogi plików - reszta

Store	Scope	Usage
<b>audit:</b>	default domain	Stores the audit log Available from the CLI in the default domain only
<b>checkpoints:</b>	Per application domain; not shared	Contains the checkpoint configuration files
<b>dpcert:</b>	default domain	Encrypted directory that contains files that the appliance uses for processing Available from CLI in the default domain only
<b>image:</b>	default domain	Contains the primary and rollback firmware
<b>tasktemplates:</b>	default domain	XSL files that the WebGUI uses

# Domeny aplikacyjne

- "partycja" dla dewelopmentu i usług
- użytkownicy mogą mieć dostęp tylko do konkretnej domeny
- mogą być restartowane niezależnie od innych domen
  - restart wczytuje zapisaną konfigurację domeny, która może być różna od konfiguracji działającej (cli: write memory, gui: save configuration)

# Widoczność domen

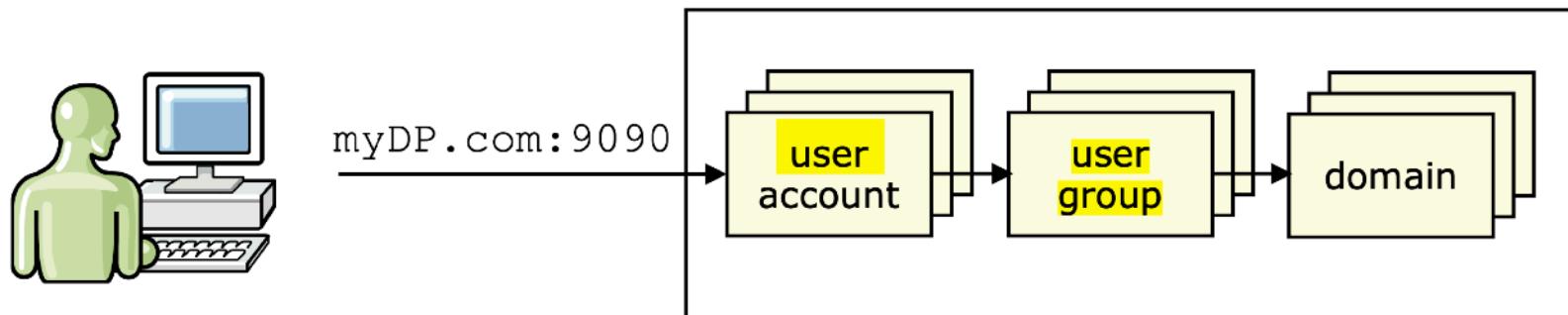
Domeny mogą być “widoczne” dla innych (widoczność nie może być zapętlona)

- widoczność domeny ”default” udostępnia zasób “store:” tylko do odczytu
- widoczność domeny aplikacyjnej udostępnia “local:” tylko do odczytu

# Użytkownicy i grupy

Konta (użytkowników) tworzy administrator

- użytkownik przypisany jest do jednej grupy
- grupa definiuje uprawnienia do zasobów i domeny/domen





# Uwierzytelnienie

- Custom
- LDAP server
- Local user
- RADIUS server
- SAF
- SPNEGO (deprecated)
- TLS user certificate
- XML file

# Mapowanie uwierzytelnienia

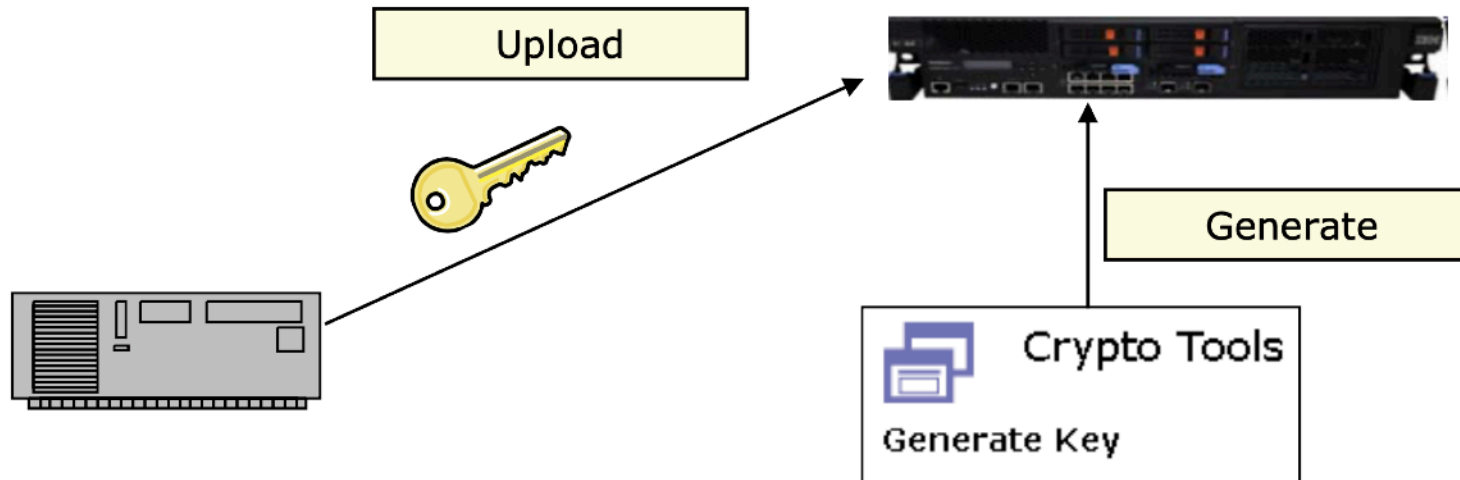
- Custom
- Local user group
- XML file

*Table 1. Authentication methods and supported credential mapping methods*

Authentication method	Mapping with a local user group	Mapping with an XML file	Custom mapping
Custom	No	Yes	Yes
LDAP	No	Yes	Yes
Local user	Yes	Yes	Yes
RADIUS	No	Yes	Yes
SAF	No	Yes	Yes
TLS user credential	No	Yes	Yes
XML file	Yes	Yes	Yes


# Certyfikaty

- Generowane przez DPG korzystając z Crypto Tool
- Wgrane na Datapower






# Certyfikaty – zabezpieczanie ruchu

## SSL (TLS) Profile - deprecated

 Configure SSL Proxy Profile

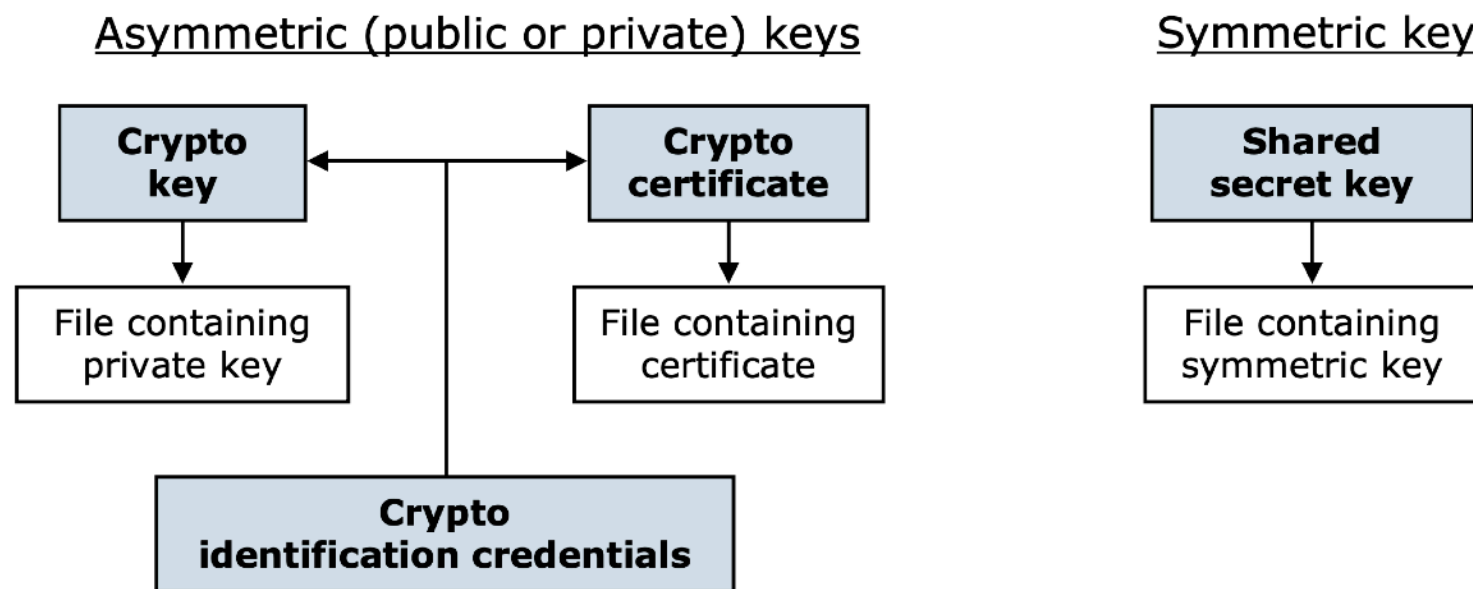
Refresh

Name	Status	Op-State	Logs	Direction	Forward (Client) Crypto Profile	Reverse (Server) Crypto Profile
MyBasicFirewall	saved	up		forward	StudentClientCP	
MyTransformFirewall	saved	up		reverse		StudentServerCP
TwoWayDemo	new	up		two-way	StudentClientCP	StudentServerCP

Add

# Klucze i certyfikaty – obiekty

- The key and certificate objects point to the files on the appliance that are the actual key or certificate
  - Certificate contains the public key



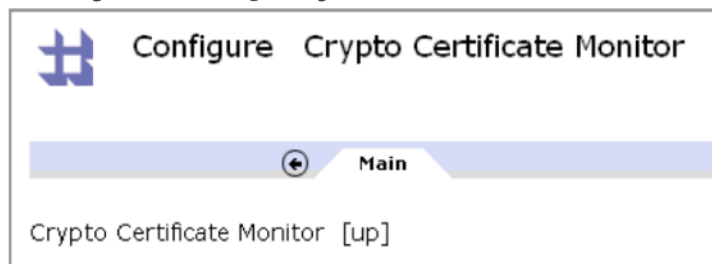
- The **crypto identification credentials** object maintains the relationship between the private key object and its related certificate (public key) object

# Wygasanie certyfikatów i CRL



**Valid until  
02-14-2015**

- Certificates are valid only for a certain length of time *and can expire*
- A certificate monitor can constantly check certificates that are stored on the appliance and warn before expiration invalidates the certificate
  - This object is **up** by default



- Certificates can also be revoked by issuing authority
- The appliance can check certificate revocation lists (CRL) for revoked certificates

