HCL Software Academy
for Digital Solutions

HCL

Domino V12.0.1 Certificate Management

Daniel Nashed
HCL Lifetime Ambassador

HCL SOFTWARE

Improvements

DSAPI Filter Logic moved to HTTP Task

- **V12.0 - DSAPI filter was used for incoming ACME HTTP-01 challenge verification**
- The functionality is now part of the HTTP task and enablement by default
  - Disable via notes.ini: **HTTP_CertMgr_Disable=1**
- **V12.0.1 - No DSAPI filter configuration needed** in server doc or internet site document
  - Remove existing DSAPI filter (n)certmgrdsapi
- **ACME HTTP-01 challenges now also available on AIX and OS400**
  - Tip: You can always create redirects to have challenges processed on other servers
    - Check: https://blog.nashcom.de/nashcomblog.nsf/dx/using-acme-http-01-challenges-redirected-to-other-servers.htm
- Diagnostic parameters now use the HTTP_ prefix
  - HTTP_CertMgr_Verbose=1
  - HTTP_CertMgr_Debug=1

“PublicKey” Field

- **PrivateKey is always written encrypted**
- In some special cases having access to the public key can be helpful
  - e.g. when building your own integration/flow on top
- **“PublicKey” field is written in parallel to the encrypted PrivateKey field**
  - PEM formatted
  - Field is not shown in the UI
  - Mainly important for TLS Credentials documents, but also written for the ACME account documents
  - Only written when the key changes, not for existing keys

Configurable Follow Redirects for Curl Requests

- LibCurl requests by default do not follow redirects
- ACME challenge verification in V12.0 used an own logic to follow redirects
  - Changed to use core LibCurl functionality to follow redirects
  - Default: **5 redirects per request**
  - Notes.ini: **CertMgr_MaxRedirHTTPChallenge=n** (can be also set to zero)
- New Optional redirects parameter for DNS TXT record HTTP/HTTPS requests
  - Default: No redirects
  - Notes.ini: **CertMgr_MaxRedirDNSProvide=n**
- ACME communication by default allows not redirects
  - In some very special cases this might be useful
  - Notes.ini: **CertMgr_MaxRedirACME=n**

Disable ACME HTTP-01 Challenge Verification

- By default CertMgr verifies **ACME HTTP-01** challenges before confirming them in ACME flow
  - In some special cases (even following with redirects) a challenge cannot be verified from internal
    - But can be verified by the ACME provider from external
  - In 12.0 disabling the verification was only possible via load certmgr **-g**
- New Notes.ini parameter:
  - **CertMgr_NoVerifyHTTPChallenge=1**
- **New troubleshooting living document with many tips to troubleshoot**
  - https://github.com/HCL-TECH-SOFTWARE/domino-cert-manager/blob/main/docs/troubleshooting_acme_challenges.md
  - A must read before calling support!

TLS Cache Select Criteria

- **V12.0**
  - Only “**issued”** or “**pending**” TLS Credentials with “**green**” or “**yellow**” **certificate status** are loaded
- **V12.0.1**
  - Ensure that TLS Cache loads TLS Credentials also in **transient** or **renew error state**
  - TLS Credentials with **certificate status** of “**yellow**” **and** “**green**” with the following status are loaded
    - Issued
    - Pending
    - Renew
    - Waiting
    - Error
    - Expired
    - Update Server List

TLS Credentials Import & Export

Use cases for import & export

- **Import existing X.509 certificates**
  - Use existing PEM (.pem), PKCS12 (.p12 / .pfx) and keyring-files (.kyr)
  - For example wild card certificates already available in your organization
  - Support for password protected PEM and PKCS12 with current crypto standards

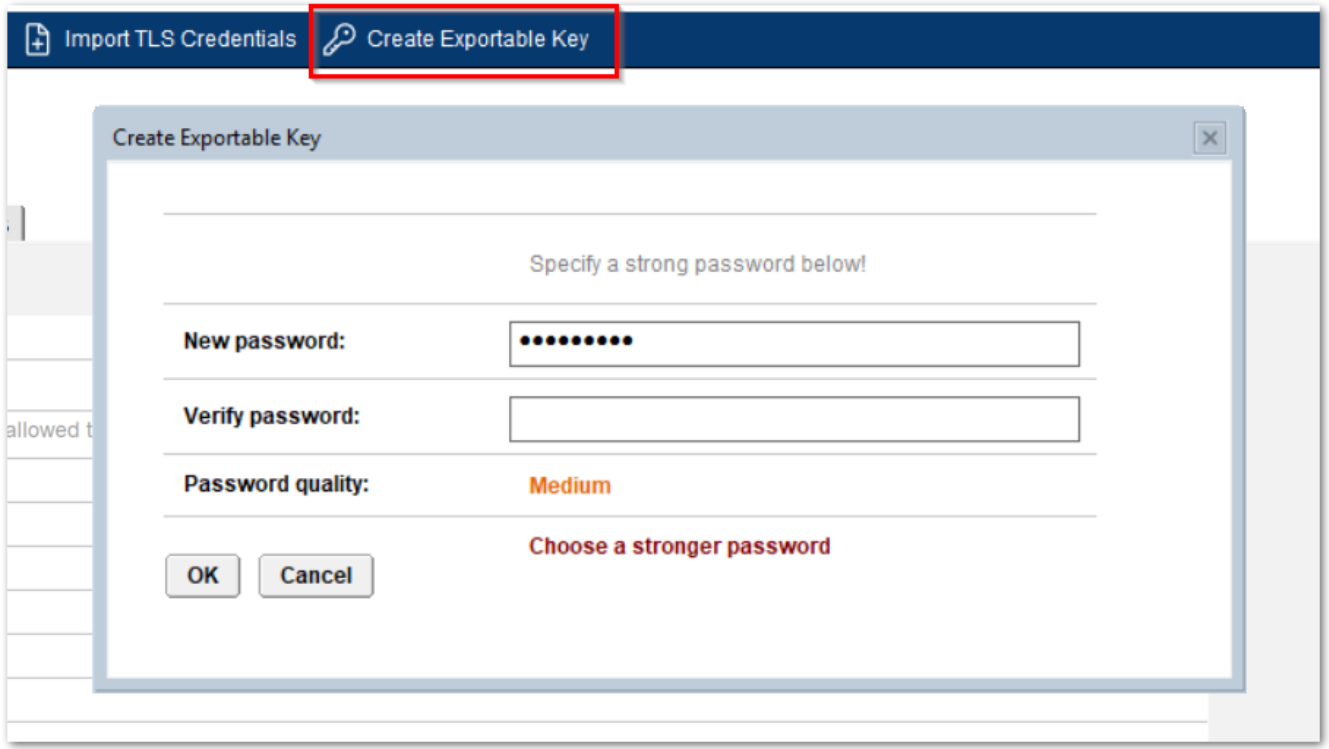
- **Export CertMgr TLS Credentials to be used on other environments**
  - Export to encrypted PEM and PKCS12 files
  - Exported keys are required to be password protected with a “secure” password
  - Useful to export for Sametime, SafeLinx any type of load-balancer etc.

Concept of “exportable keys”

- **The private key is always encrypted for server only and can be only decrypted by**
  - CertMgr server
  - All servers listed in “Servers with access”
- Beginning with Domino 12.0.1 private keys can be created or imported as “**exportable**”
  - Either create an “**exportable private**” key for ACME and manual certificate flows
  - Or import x.509 certificates marking them exportable
- Exportable keys are protected with a password/passphrase
  - Stored as **AES 256 encrypted PEM** in a visible field in the form
- Export functions use the **Exportable key** field to create files containing the complete TLS credentials information (key + cert + chain + root)

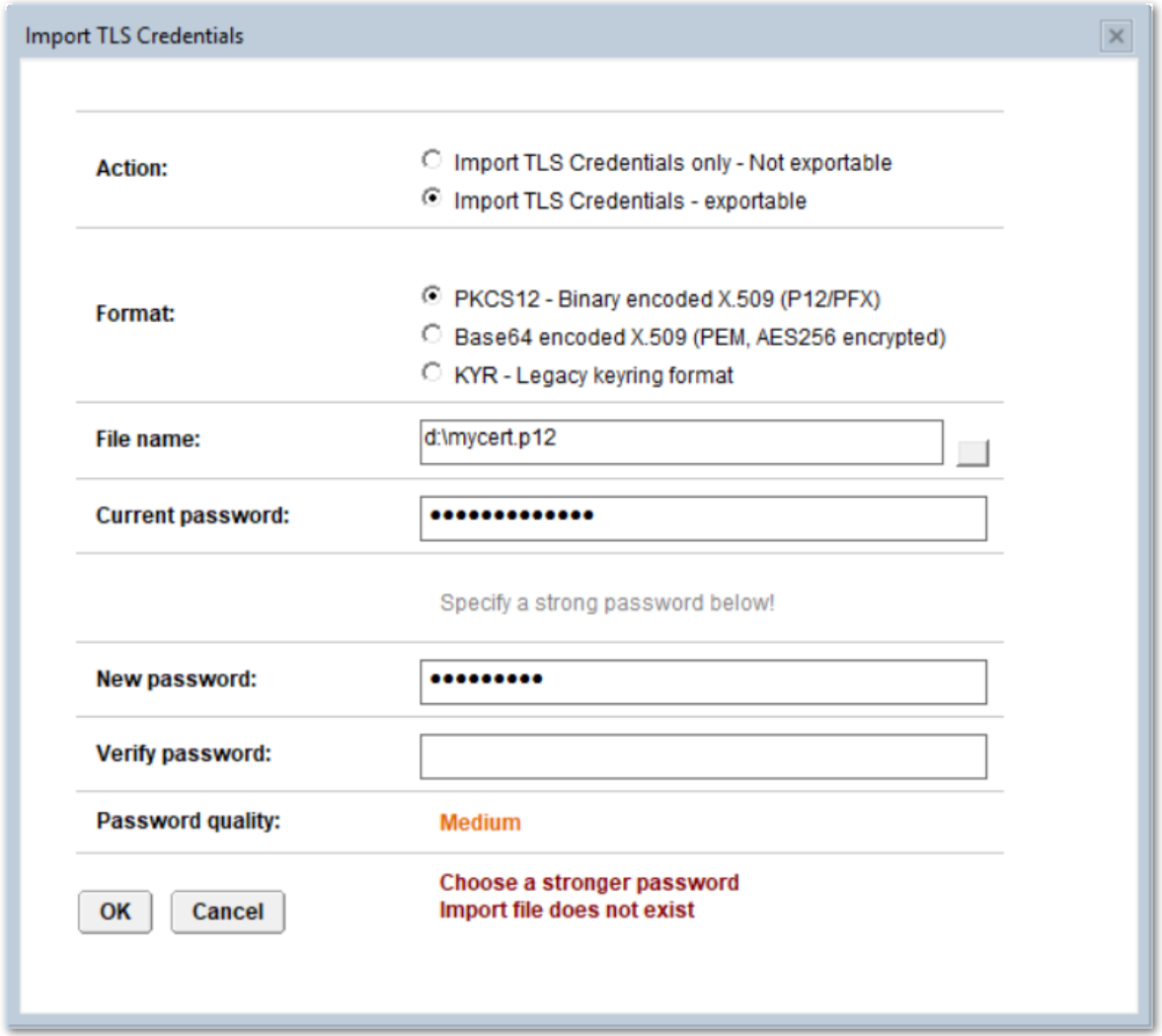
Create Exportable Key

- **Create key and specify a secure password**
  - The export function ensures the password quality checking the entropy
- Private key type and size/curve is created based on the settings in the TLS Credentials document
- Created key can be used for ACME and manual flows



Import existing X.509 Certificate and Key

- Supports
  - PEM (.pem)
  - PKCS12 (.p12/.pfx)
  - Keyring files (.kyr)
- Default option: Import only
- Import and mark private key exportable
  - Requires password for exportable key
- Supports password protected files
- Sorting and filtering certificate data
- Auto complete chains

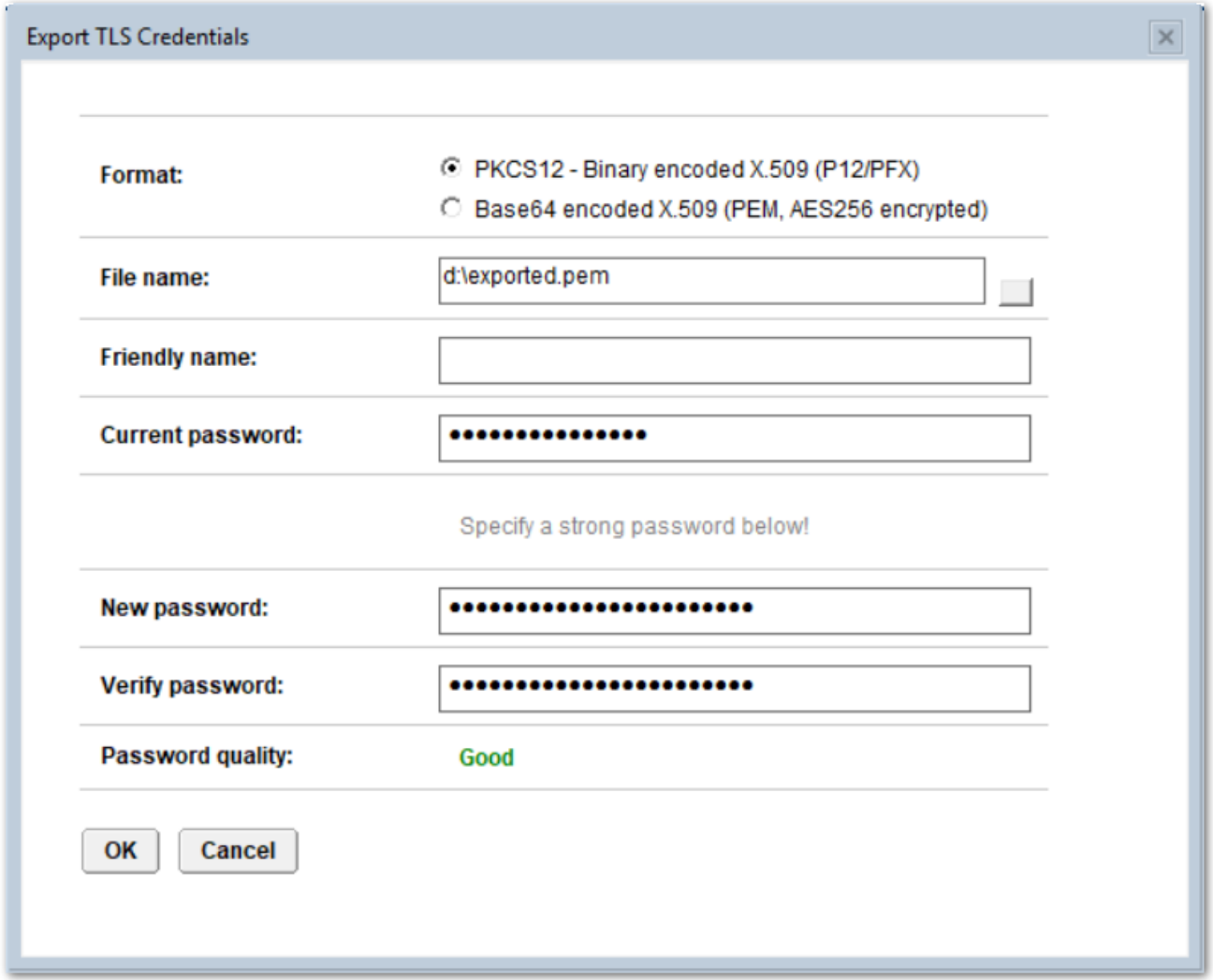


HCL Software Academy for Digital Solutions

HCL SOFTWARE

Export TLS Credentials

- Supports
  - PEM (.pem)
  - PKCS12 (.p12/.pfx)
- Export action is only shown when exportable
- Only password protected / encrypted export with current encryption standards!
  - **PEM: AES 256**
  - **PKCS12: AES 256 / PBES2**
    - See: https://datatracker.ietf.org/doc/html/rfc8018
    - Not all external tools might be able to read it
    - Tip: Use OpenSSL to verify and convert if needed



New algorithms importing/exporting Certificates

- Import now also supports newer **AES-CBC** with **128/192/256 bit** keys.
- For backward compatibility
  - **3DES-CBC, SHA-1** (hmacWithSHA1)
  - **3DES-CBC, SHA-2** (hmacWithSHA256, hmacWithSHA384, and hmacWithSHA512)
- Exporting PEM or PKCS#12 file always use more modern and secure standards
  - **PBES2** with **256 bit AES**, **4096 iterations**, and **HMAC-SHA2**
  - Same standard brand new OpenSSL 3.0 uses (Tip: 3.0 use new **-legacy** option when converting!)
- For older software like Java 8/11 applications (e.g. Sametime 11)
  you will either need to convert via OpenSSL or lower the export security via notes.ini
  - **PKCS12_EXPORT_LEGACY=1**
  - Downgrades all of the PKCS#12 files exported to use **3DES with SHA-1**

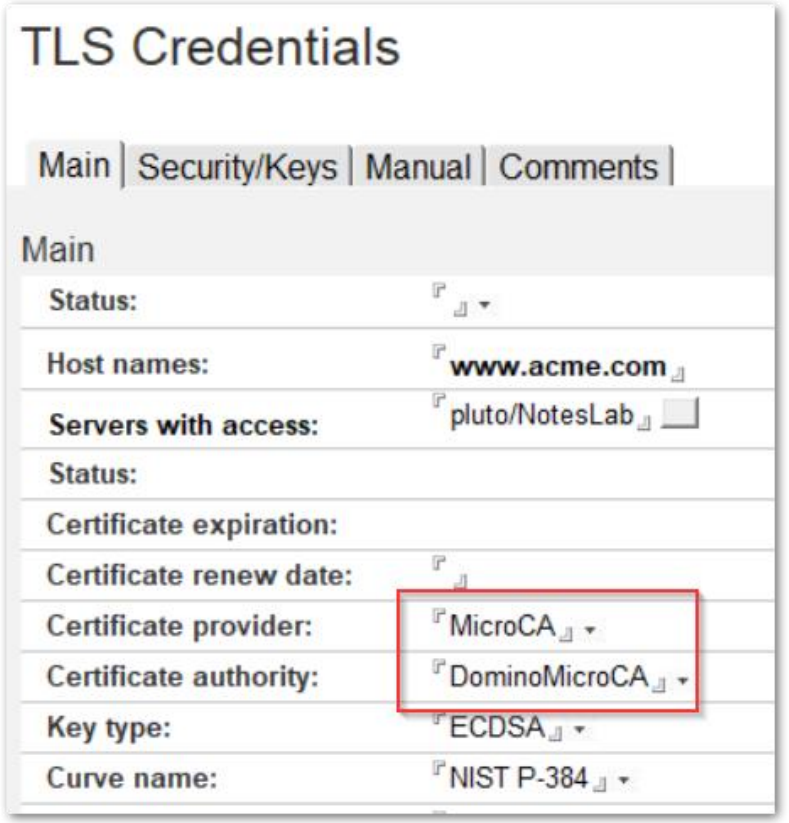
Implementation

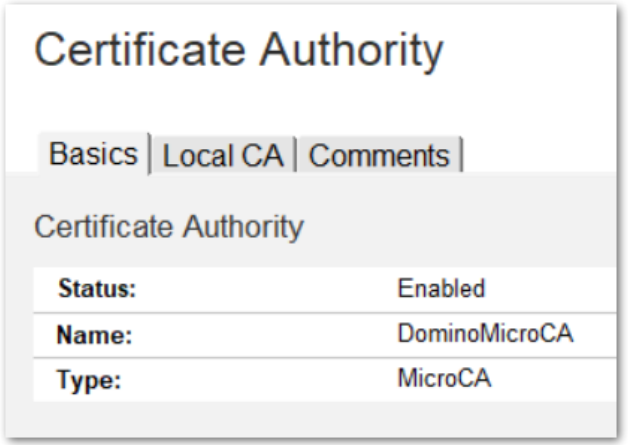
- Single sub-form for export, import and create exportable key
- Designed to use “**Enter**” to validate the form (OK button) for convenience
- Validation is built into the form
  - All errors are shown on the bottom of the dialog box at once
- Script lib encapsulating the functionality
  - Leverages a 12.0.1 C-API call in core
  - New export/import actions are only shown in **12.0.1+** clients
- Central call used for all export and import operations
  - Load certmgr **-importpem** / **-importkyr**
  - One-touch Domino setup: You can now import existing PEM/P12/KYR files!

Micro CA

Simple internal Micro CA

- Sometimes neither Let's Encrypt can be used nor an existing X.509 certificate is available
- But you still want a secure TLS connection for your first server start
- Or you want to use a simple local CA for a test environment …
- Domino 12.0.1 introduces a simple "**Micro CA**" managed by CertMgr.
  - Available via One-touch setup
  - Or directly from certstore.nsf at any time issuing a certificate from the local CA





CertMgr Commands

New CertMgr Commands

- **Tell certmgr show certs**
  - Shows the currently loaded TLS Credentials for this server
  - Each process has it’s own cache
    CertMgr server task is used to show certificate information
  - Also available not CertMgr server and can be invoked via
    load certmgr -showcerts

- **Tell certmgr show ocsp**
  - Checks the OCSP status for all configured TLS Cerdentials
  - Requires OCSP to be enabled
  - Also available via **load certmgr -showocsp**

CertMgr Command Examples

```
Subject key identifier    Key info     Expiration   KeyFile/Tag           Host names (SANs)
-------------------------------------------------------------------------------------------------------
8E1D 5236 BBC1 3A1C ...   NIST P-384    89.7 days   keyfile.kyr           zerossl2.iris.csi-domino.com
0BAE 8710 D30C 1631 ...   RSA 4096      54.3 days                         www.domino-lab.net mail.domino-lab.net
7272 955E 213C D4DD ...   NIST P-384    76.5 days                         *.digitalocean.domino-lab.net
-------------------------------------------------------------------------------------------------------
3 TLS Credentials


Subject key identifier    Key info     OCSP  KeyFile/Tag           Host names (SANs)
-------------------------------------------------------------------------------------------------------
8E1D 5236 BBC1 3A1C ...   NIST P-384   OK    keyfile.kyr           zerossl2.iris.csi-domino.com
0BAE 8710 D30C 1631 ...   RSA 4096     OK                          www.domino-lab.net mail.domino-lab.net
7272 955E 213C D4DD ...   NIST P-384   OK                          *.digitalocean.domino-lab.net
-------------------------------------------------------------------------------------------------------
3 TLS Credentials
```

HCL Domino CertMgr & certstore.nsf

Q&A

HCL

Relationship™

BEYOND THE CONTRACT

$8.4 BILLION ENTERPRISE | **132,000** IDEAPRENEURS | **44** COUNTRIES

WATCH THE **FILM**