A MITEL
PRODUCT
GUIDE

OpenScape Business V3

Whitepaper SSL certificate handling

Release Number 09/2024

Mitel
Powering connections

Content

History of change

V1.0	Initial Creation	21/11/2023
V1.1	Editorial changes	30/09/2024

Disclaimer

This document is intended for trained OpenScape Business technicians.

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of the contract.

Availability and technical specifications are subject to change without notice.

The following description refers to OpenScape Business V3R3 and above.

1 Introduction

1.1 What are SSL certificates?

TLS/SSL certificates are used to protect data during communication between servers such as OpenScape Business and web-based clients by means of encryption and to verify the identity of the company belonging to the website so that the user can be sure that he is really communicating with the real server.

OpenScape Business issues itself a temporary ("self-signed") SSL certificate during the initial system installation or upon change of the LAN IP address, but this certificate does not contain sufficient data for identity verification apart from the user's own LAN IP address.

Such a certificate does not comply with current security standards and must be replaced by a trustworthy, individual SSL certificate issued by an official Certificate Authority (CA) as soon as possible after the initial installation of OpenScape Business. This is the only way to meet the minimum standards of current client operating systems and web browsers for secure Internet communication.

CA's usually offer SSL certificates with different trust levels: Domain Validation (DV), Organization Validation (OV) and Extended Validation (EV). For OpenScape Business, domain validated certificates are sufficient. This is usually the cheapest option, with some CA's even free of charge.

1.2 For which web services does OpenScape Business use the SSL certificate?

The active SSL certificate is used for administrator access via the Admin Portal as well as for various other web-based applications (e.g. key programming) and WSI-based UC clients such as myPortal @work, myPortal to go, Application Launcher, myContacts and myPortal for Teams.

1.3 Where can I get a trusted SSL certificate from?

To obtain an SSL certificate, you must contact a certification authority. You must verify the domain name used to reach OpenScape Business in order to create a Certificate Signing Request (CSR), which is then sent to the CA for validation.

It should be noted that CA issued, trusted SSL certificates only have a limited validity period of a few months to a few years to ensure that they comply with current security standards. It is important to keep an eye on the expiration date and to renew SSL certificates before the expiration date is reached.

Failure to renew SSL certificates can result in the client environment classifying the website as "insecure" and preventing communication with the server.

Please note that some client environments have special requirements for SSL certificates, which may not be met by every CA. Such special requirements are linked further down in the section „client side considerations". When selecting your CA, please follow the corresponding instructions.

1.4 Why has the certificate issue become so important?

The use of trustworthy, customer or server-specific SSL certificates is extremely important and is increasingly being enforced by the major operating system and browser manufacturers. Security, professionalism, integrity and confidentiality when handling personal data are the key arguments for this.

Due to the increasing use of web-based services and clients, including via the Internet, the permanent use of the temporary, self-signed (and therefore insecure) default SSL certificate of OpenScape Business is out of the question.

In addition, the temporary, self-signed certificate of OSBiz has a multi-year validity, while some client environments have started restricting the certificate validity – sometimes to not more than one year.

Moreover, in many customer installations that were originally set up with older software releases prior to V3R2.1, the validity of these temporary, self-signed certificates expires on January 1, 2024.

The Admin Portal of OpenScape Business provides a range of tools for generating and managing SSL certificates and also supports the system administrator in creating certificate signing requests. The most important functions in this regard are explained below.

2 SSL format requirements

2.1 Requirements for SSL certificates to be used in OpenScape Business

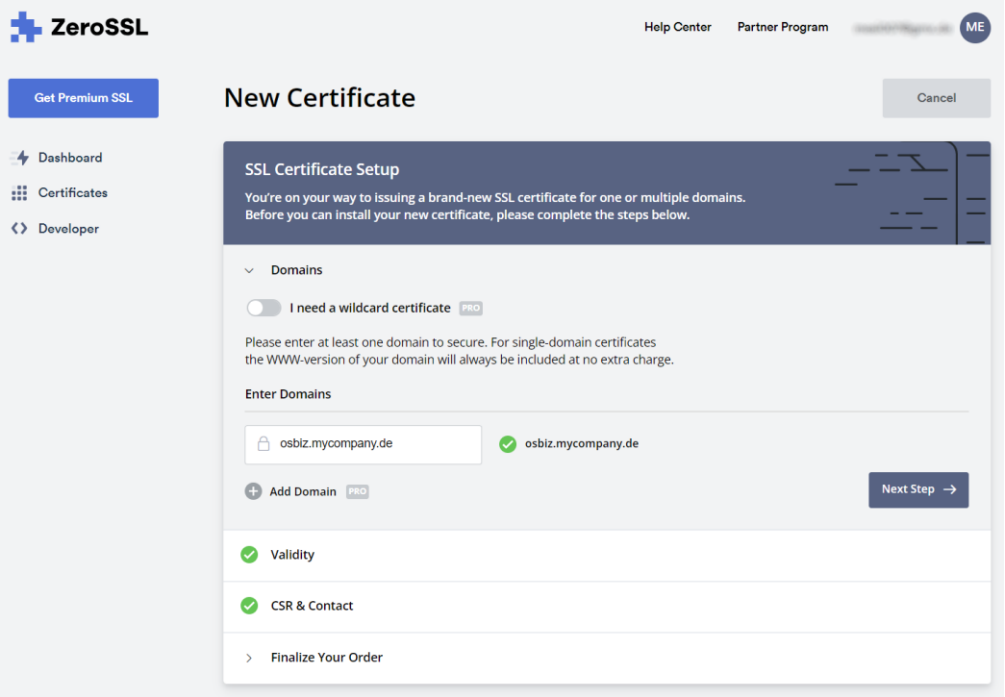
- OSBiz requires an TLS/SSL server certificate according to the International Telecommunication Union (ITU) standard X.509
- Supported signature algorithms: sha256RSA, sha384RSA, sha512RSA
- Supported certificate file format: PKCS #12 or PEM format
- Public key length: 2048

3 How to request and install trusted SSL certificates

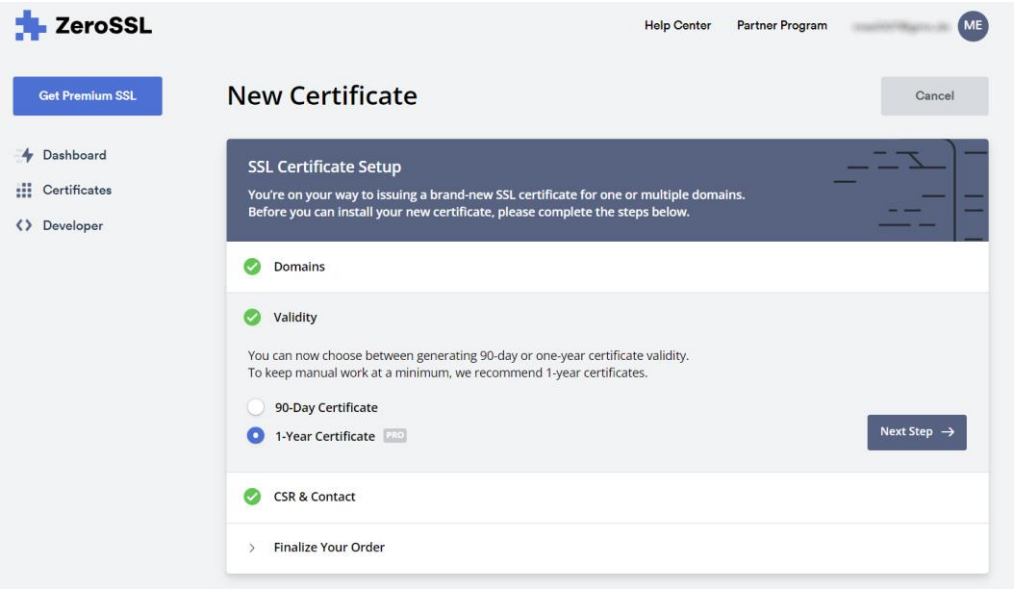
Dependent on the certificate authority (CA) of your choice, there are different options, in particular:

1) Using the web portal of the certificate authority to request a certificate for your domain. You will have to provide some basic data like the domain name which you own and you intend to use to access the OSBiz system.
Also you may have to choose a certificate validation method. Once you have made your choice – for example DNS validation – the CA will give you a challenge which you have to fulfill according to the guidelines of your CA. Example (CA Provider ZeroSSL):

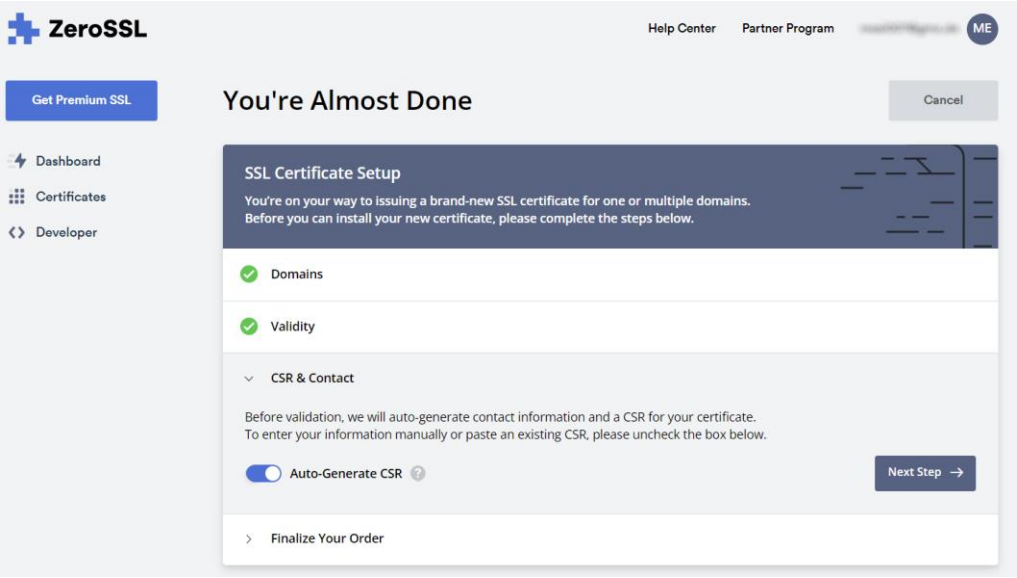
   Define the certificate content (configurable scope depends on the chosen CA):



2) Define further certificate properties:

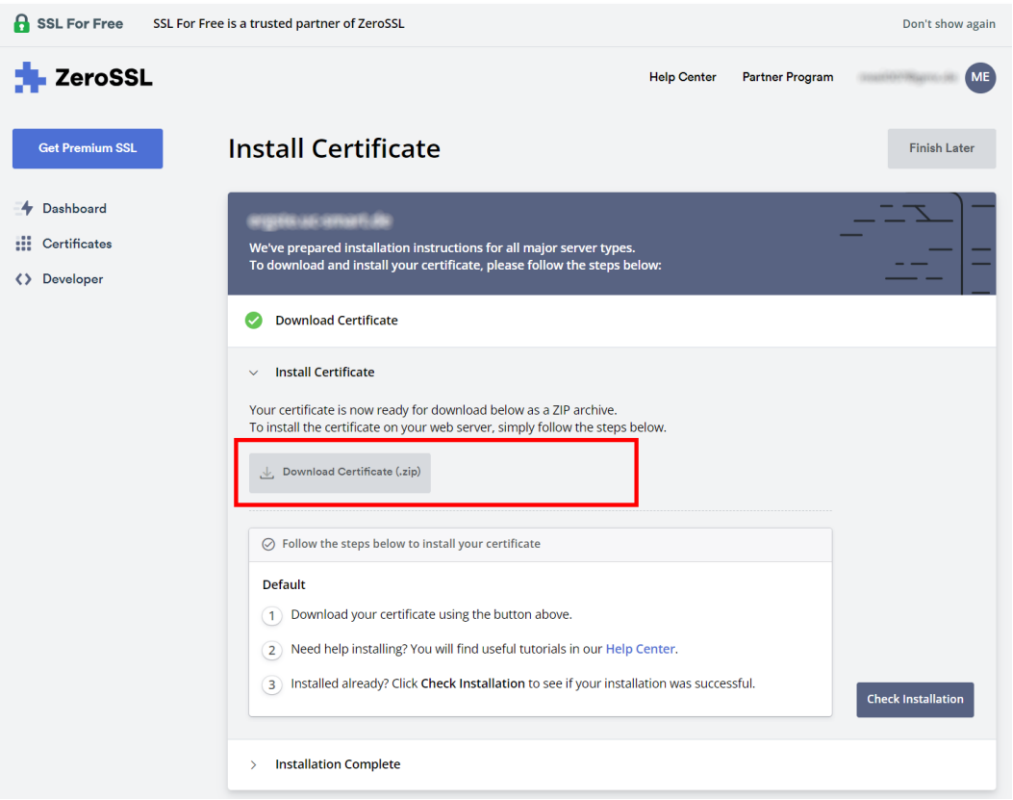


3) Auto-Generate the CSR:



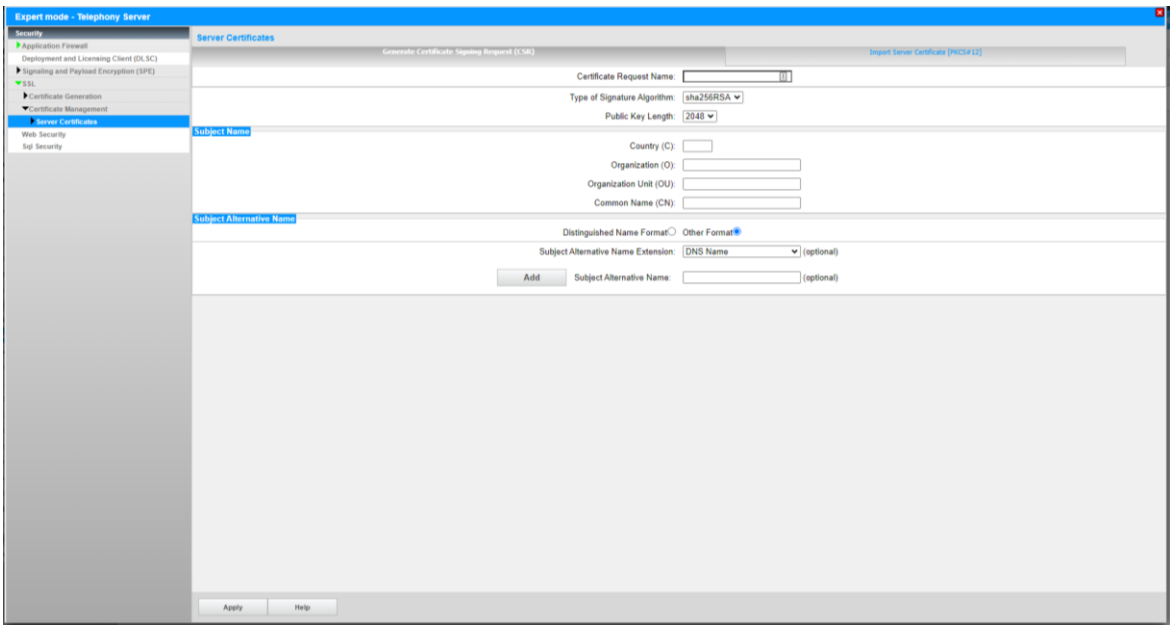
Next, the Certificate Authority needs to verify that you are the domain owner. This will be done via a specific challenge that only the domain administrator can fulfill. For example, a DNS server challenge will ask you to create a specific DNS entry for your domain.

After this is done and the CA confirms successful domain validation, you will be able to download the certificate and key file, which you then import and activate via OSBiz Admin Portal.



4) Using OSBiz Admin Portal to create a Certificate Signing Request (CSR).

Navigate to Expert Mode -> Security -> SSL -> Certificate Management -> Server Certificate



In Generate Certificate Signing Request (CSR) page, the following fields must be filled in order to generate the key and csr files

General:

- Certificate Request Name: A name for the CSR which will be used in the name of the file that will be downloaded.
- Type of Signature Algorithm: Select between sha256RSA and sha512RSA
- Public Key Length: The only option is 2048

Subject Name:

- Country (C): Use a two letter country code e.g. DE
- Organization (O): denotes the formal name of the overarching entity or company to which the certificate is assigned.
- Organization Unit (OU): designates a specific subunit or department within an organization, offering additional granularity to identify the organizational structure
- Common Name (CN): a vital identifier, usually representing the domain name for which the certificate is issued, providing a key element for verifying the certificate holder identity.

Subject Alternative Name (Optional):

The Subject Alternative Name (SAN) extension is a feature of X.509 certificates used in the field of cryptography. X.509 is a standard that defines the format of public-key certificates. The SAN extension allows additional identities, such as host names, IP addresses, or email addresses, to be associated with a single X.509 certificate. This is particularly useful in scenarios where a server may be accessed by different names or addresses.

Distinguished Name Format: Information similar to the Subject name such as Country (C), Organization (O), Organization Unit (OU), Common Name (CN) must be filled.

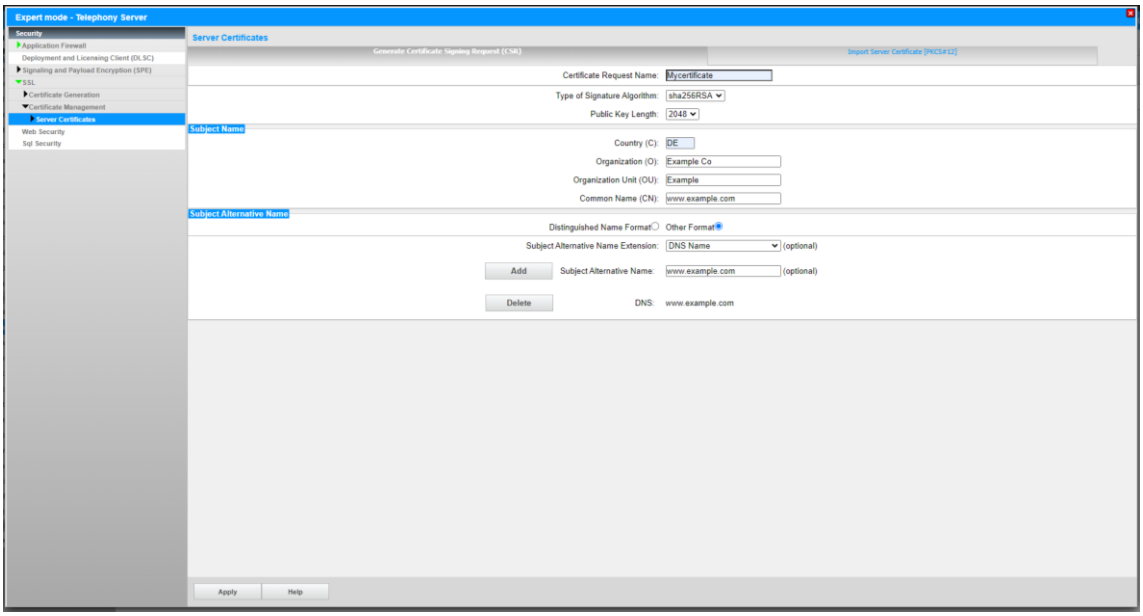
Other Format:

- Subject Alternative Name Extension: Option are DNS, IP Address, Email Address, Uniform Resource Indicator
- Subject Alternative Name: The SAN extension helps address limitations in cases where a single common name is insufficient or when there is a need to include multiple identities within a single certificate. This is important for modern web services, where a server might be accessible through multiple domain names or IP addresses.

Here's an example of how the SAN extension might look in a certificate:

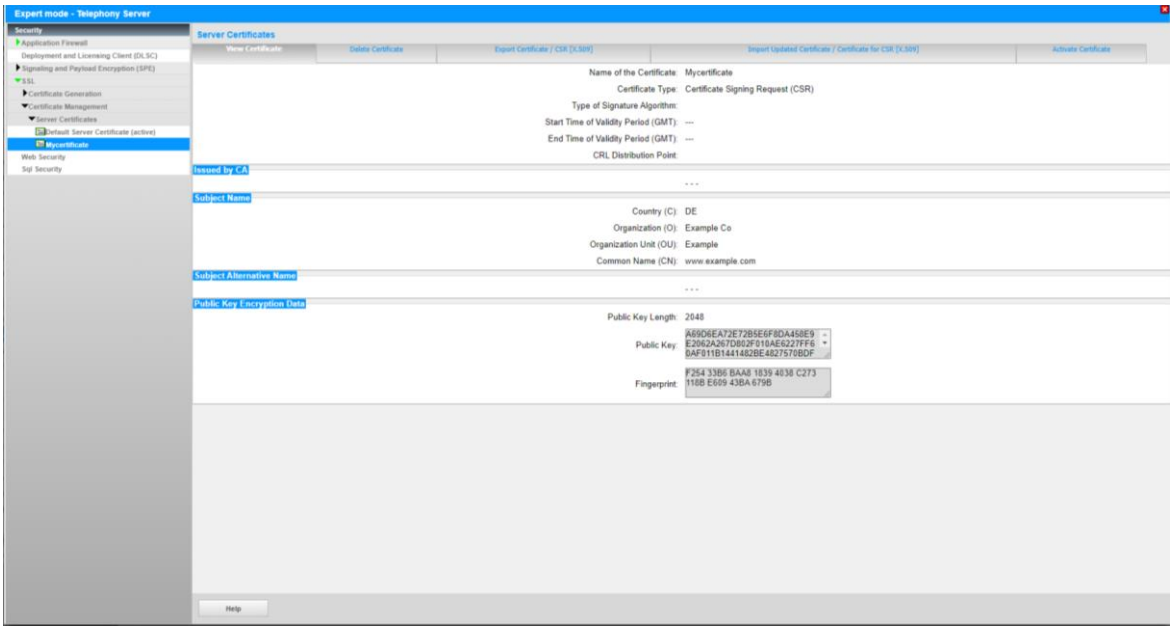
Subject Alternative Name:
DNS:www.example.com
DNS:mail.example.com
IP Address:192.168.1.1
Email:admin@example.com

when Subject Alternative Name option has been filled the Add button must be used in order to be included in the CSR.



By applying the information two files will be generated and downloaded "Certificate_Name".csr and key_csr.pem

The generated CSR can be seen under the list of Server Certificates



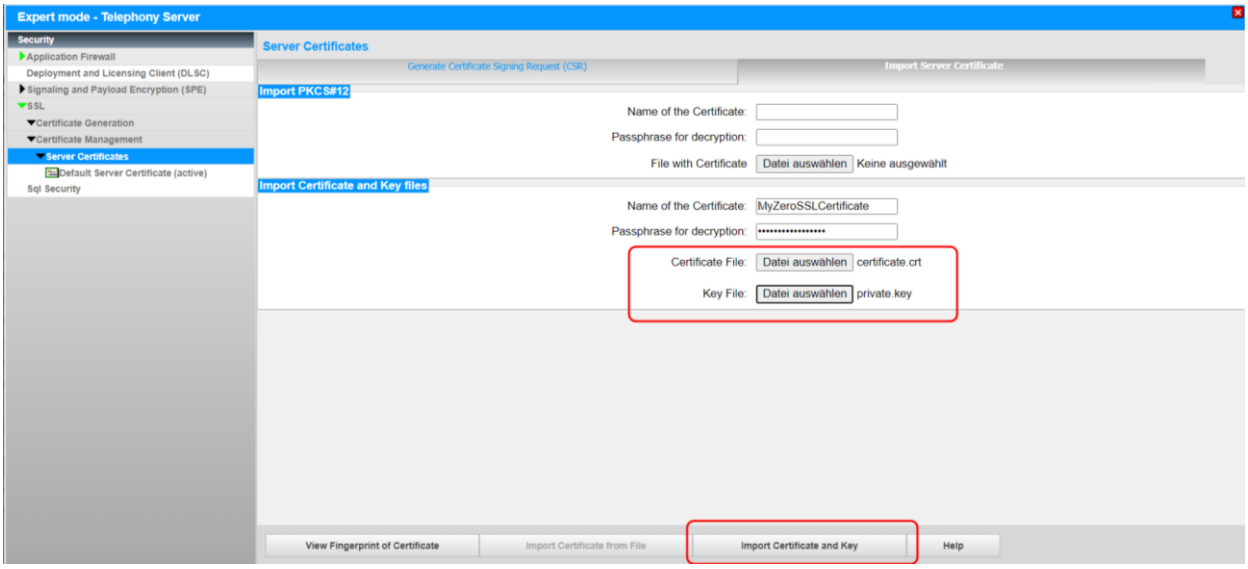
5) Using 3rd party tools (usually based on OpenSSL) to create a Certificate Signing Request (CSR) and provide this to the Certificate Authority (CA) of your choice.
Again you will have to fulfill a challenge given by the CA to verify that you are the owner of the domain which is covered by the trusted SSL certificate.
After you have received the certificate from your CA, you can install and activate it via OSBiz Admin Portal.

3.1 How to install a trusted SSL certificate

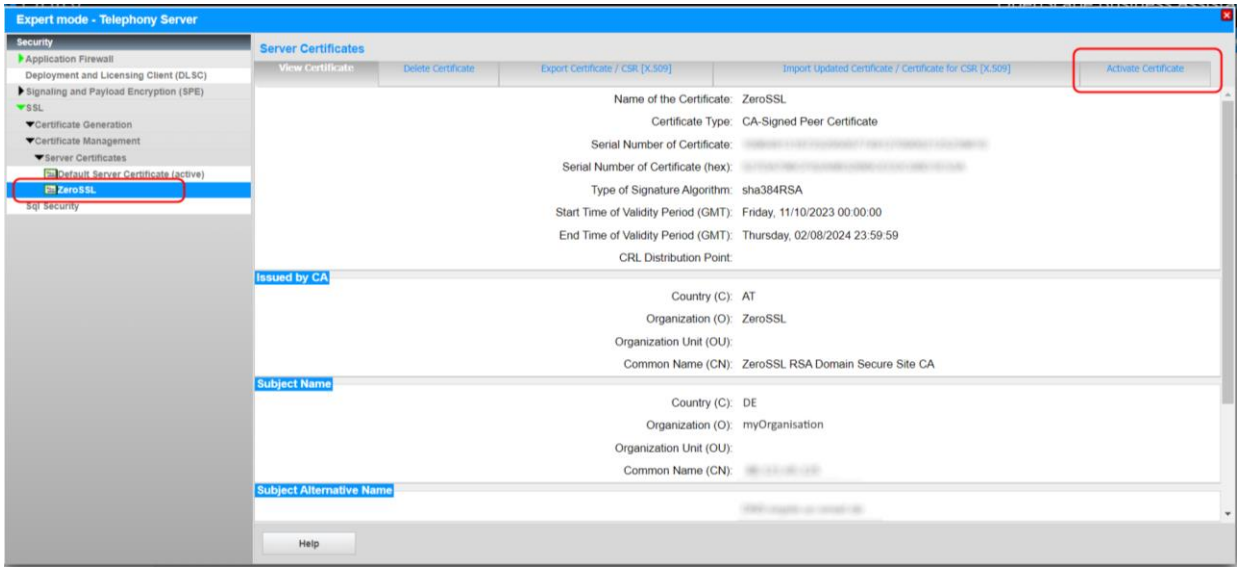
Dependent on your certificate authority, you may receive SSL certificates in different formats.
The Admin Portal of OpenScape Business supports two options for the import of SSL certificates:

1. Import in **PKCS #12** format (file extension*.p12). PKCS is an archive file format for storing multiple cryptography objects as a single file. It is commonly used to bundle a private key with its certificate.
2. Import in **PEM** format, where certificate and private key as separate files (file extension *.cer and *.key).

Both import options are offered in Admin Portal under
Expert Mode – Telephony Server – Security – SSL – Server Certificates – Import Server Certificates.
Example using option 2:
1. Enter a name and a passphrase for the certificate you import. The passphrase requires at least 7, at maximum 32 characters.
2. Select the certificate file and key file as obtained by your certificate authority.
3. Press the button „*Import Certificate and Key*“



After successful import, you will see the new certificate in the list of Server Certificates, showing the name that you have defined in the previous step.



4. New certificates are not automatically activated upon import. Please navigate to the *Activate Certificate* tab to activate the new certificate.
Please note that the integrated web server of OpenScape Business will restart upon certificate activation. This means that for approx. 2-3 minutes, the Admin Portal and any other web services will not be reachable.

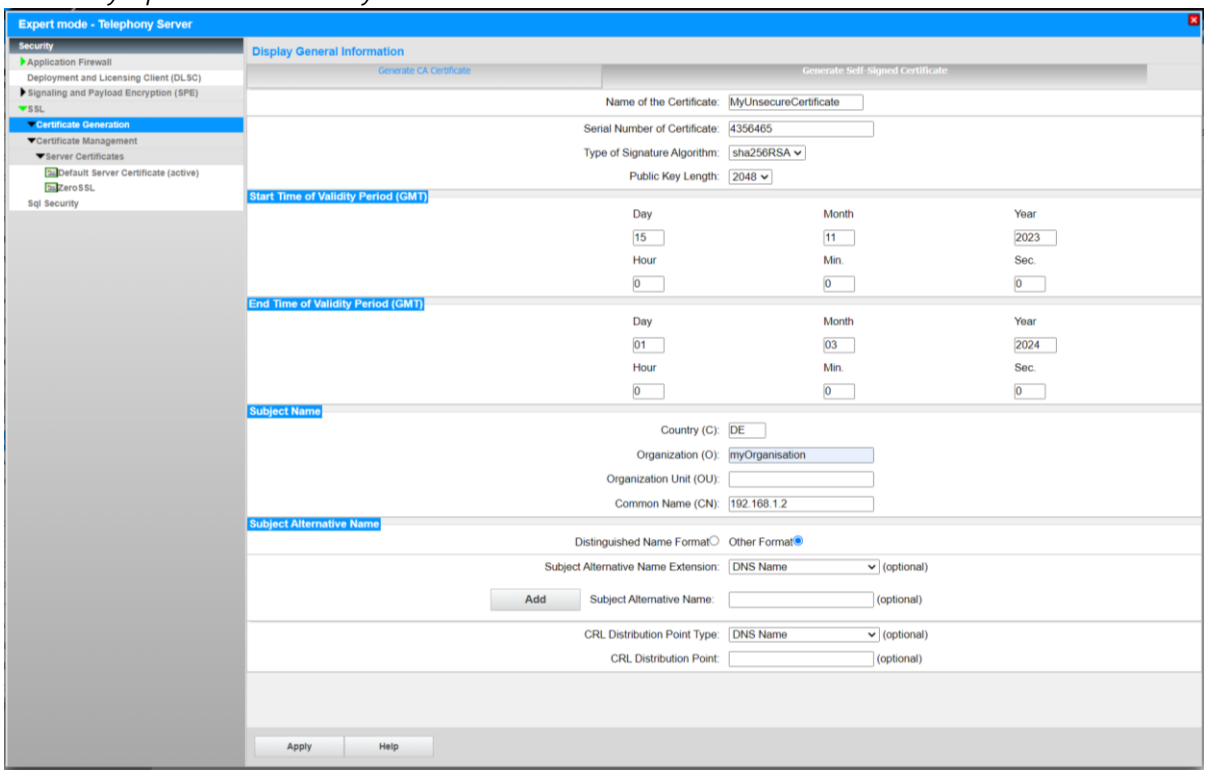
4 Renew of a temporary self-signed SSL certificate

4.1 How can I renew the temporary, self-signed SSL certificate of OpenScape Business?

As explained above, such a certificate does not comply with current security standards and must be replaced by a trustworthy, individual SSL certificate as soon as possible. If you cannot obtain a trusted SSL certificate in time before the initial self-signed certificate expires, you can create a new temporary self-signed certificate. This happens automatically whenever you change the LAN IP address of an OSBiz X system.

It can also be triggered manually via Admin Portal. Please navigate to:
Expert Mode – Telephony Server – Security – SSL –Certificate Generation – Tab „Generate Self-Signed Certificate"

Here you must specify the name and serial number of the certificate and enter the further certificate properties. Please note that some client environments generally do not trust certificates which have a validity of more than one year.



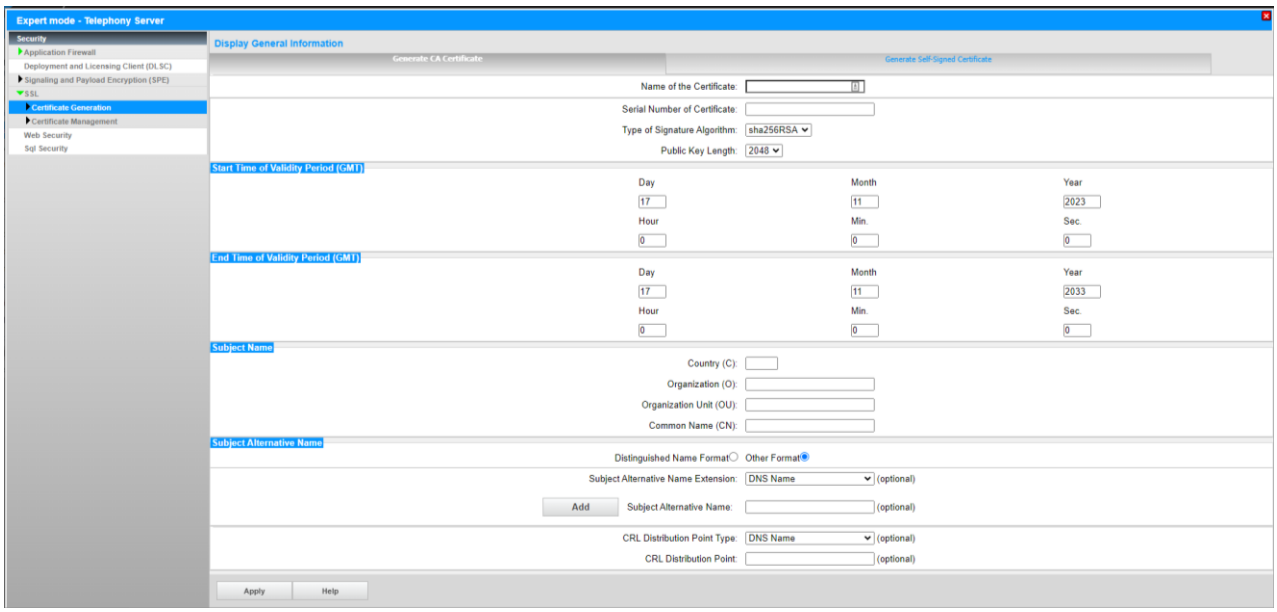
A self-signed SSL certificate also has to be activated manually after creation.

For obvious reason, any web browser will show the connection as untrusted / unsecure when utilizing e.g. Admin Portal with such a certificate.

4.2 Can I create an own certificate and import it on client side to let the web browser trust a specific OSBiz system?

Yes, this is possible. Please note again that such a certificate does not comply with current internet security standards. While it may be applicable when the specific OpenScape Business is accessed only for administration from the internal LAN, such an approach is definitely not recommended if any OpenScape Business Web Services are exposed to the internet.

Navigate to Expert Mode -> Security -> SSL -> Certificate Generation and select the Generate CA Certificate Tab



To proceed with generating the certificate, the following fields must be filled:

General:

- Name of the Certificate: A name for the certificate file
- Serial Number of Certificate: is part of the certificate's metadata and is typically a non-negative integer
- Type of Signature Algorithm: Select between sha256RSA, sha512RSA
- Public Key Length: Only 2048 is supported

Start Time of validity period:

This is the start time of the validity period. The certificate should not be considered valid for use before this date and time. It represents the earliest point in time when the certificate is considered valid.

End Time of Validity Period:

This is the end time of the validity period. The certificate is considered valid up to and including this date and time. After this date, the certificate is no longer considered trustworthy, and clients may reject it.

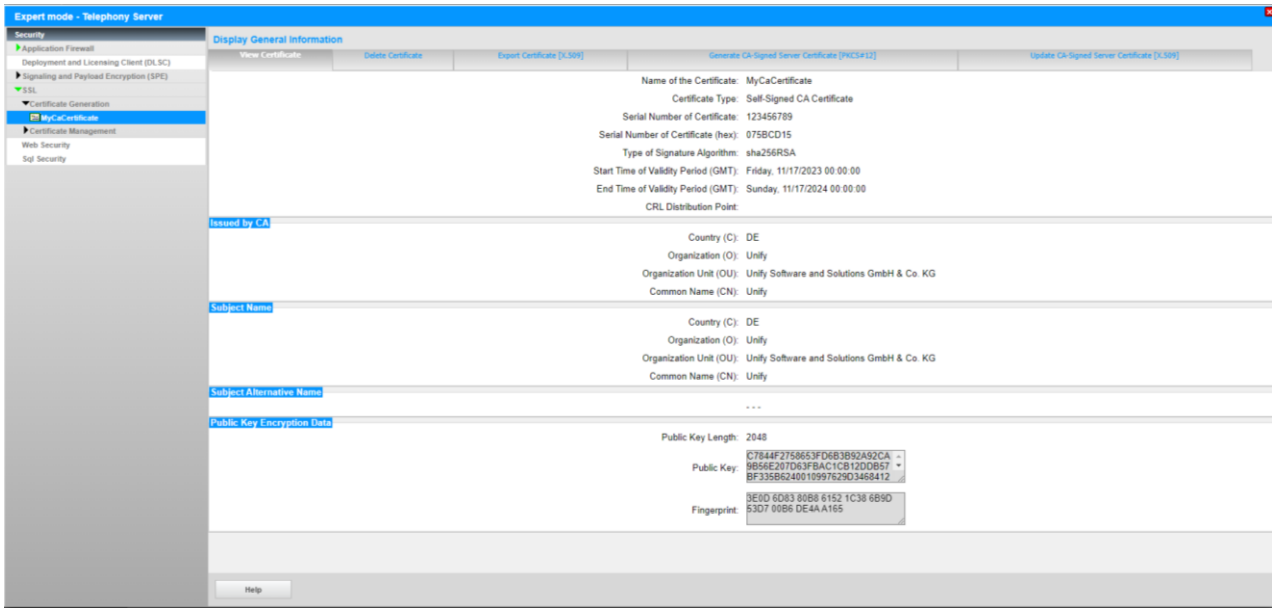
Subject Name:

- Country (C): Use a two letter country code e.g. DE
- Organization (O): entity or company to which the certificate is assigned**.**
- Organization Unit (OU): a specific subunit or department within an organization
- Common Name (CN): a key element for verifying the certificate holder identity.

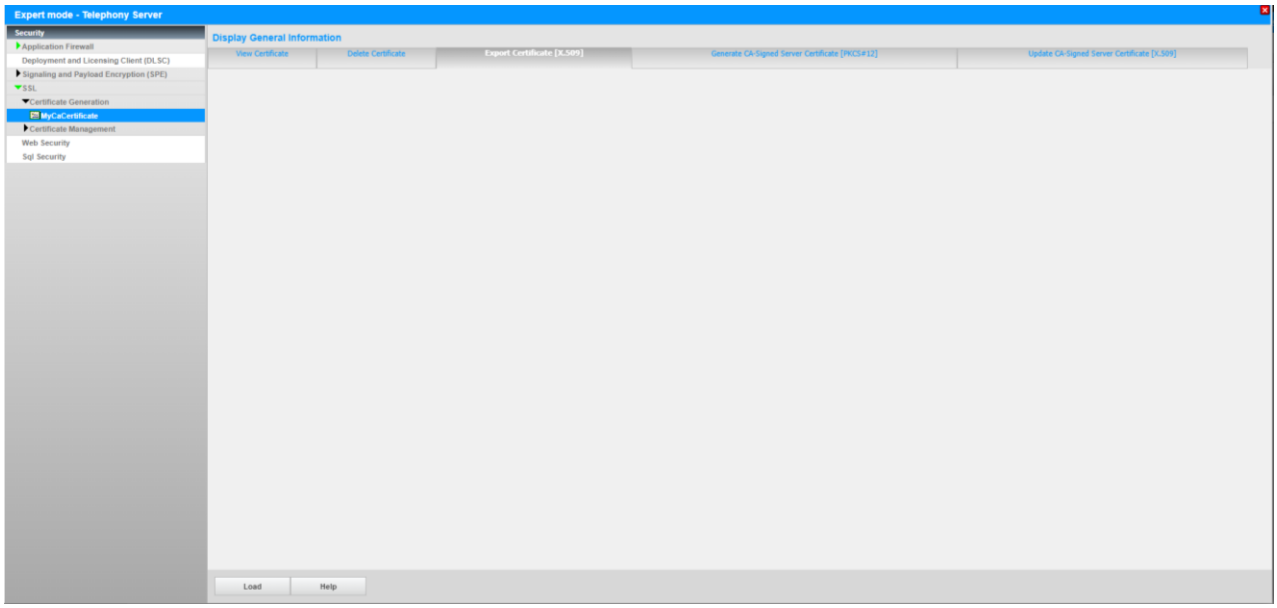
Subject Alternative Name (optional):

Option are DNS, IP Address, Email Address, Uniform Resource Indicator

Once all mandatory fields have been completed, the CA certificates will be listed under the Certificate Generation section.

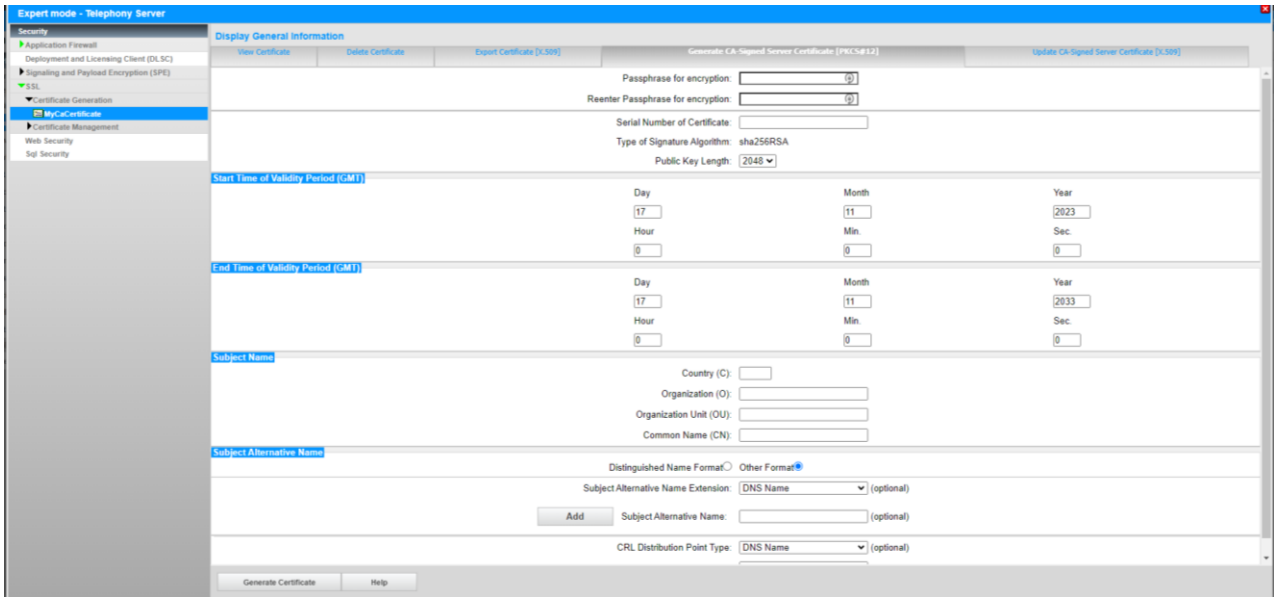


On the designated web page, you can conveniently download the CA (Certificate Authority) certificate. Simply navigate to the "Export Certificate" tab and initiate the download by clicking the "Load" button.



The resulting file will be named "Name of the Certificate.crt".

Utilize the "Generate CA-Signed Server Certificate [PKCS#12]" tab to seamlessly create a CA-Signed Server Certificate.



Passphrase for encryption: a passphrase for the certificate with length 7-32 characters

The remaining fields share similarities with those described earlier.

- Serial Number of Certificate:
- Type of Signature Algorithm:
- Start Time of Validity Period
- End Time of Validity Period
- Subject Name
- Subject Alternative Name

Upon clicking the "Generate Certificate" button, a file named "BasedOnName of the Certificate.p12" will be promptly downloaded.

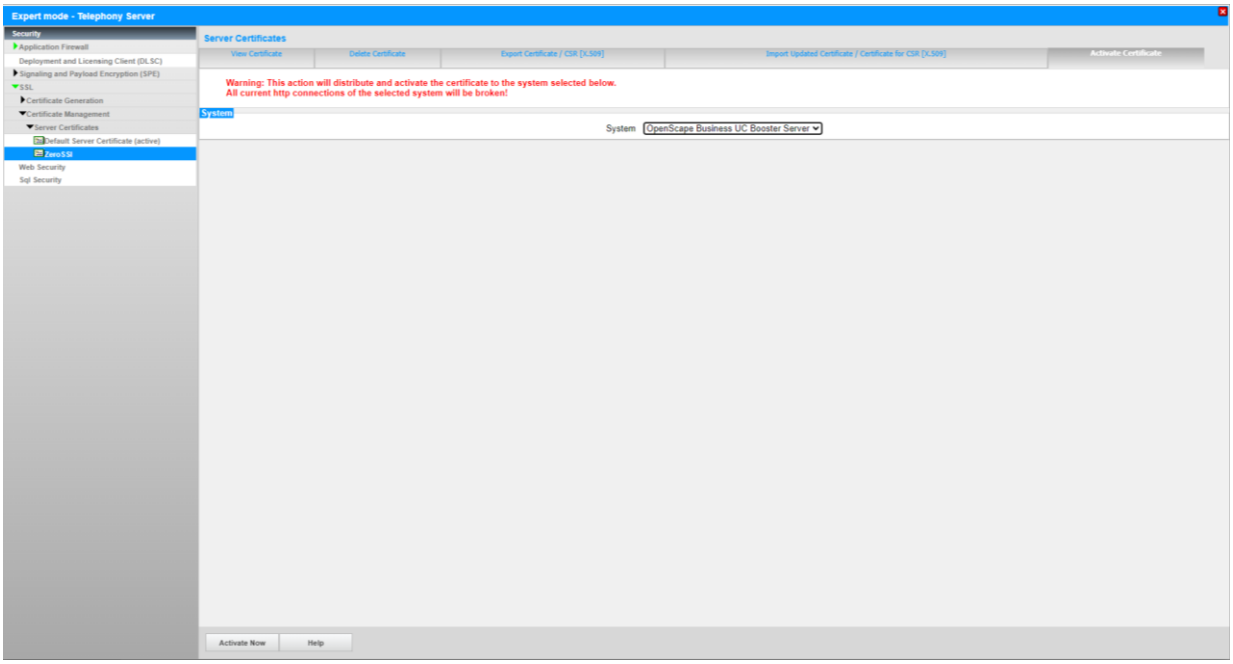
The downloaded certificate can be Imported in the system from Expert Mode -> Security -> SSL -> Certificate Management -> Server Certificate Import Server Certificate Tab

5 Certificate Handling for Booster Server

When initially installing a Booster Server, a certificate is created with the IP address of the booster serving as the common name. The certificate has a 10-year validity period and is issued for the organization "Unify Software and Solutions GmbH & Co. KG," with the organizational unit specified as "Unify."

It is possible to replace the default certificate on the Booster Server by transferring a different certificate through the Web-Based Management (WBM) interface of the system. Once transferred, the new certificate can be activated, providing an alternative security configuration for the Booster Server.

1. Go to Expert Mode.
2. Navigate to Security -> SSL -> Certificate Management -> Server Certificates.
3. Choose one of the imported certificates.
4. Access the "Activate Certificate" tab.
5. From the system drop-down menu, select "OpenScape Business UC Booster Server."
6. Click the "Activate Now" button to apply the selected certificate to the Booster Server.



6 Client side considerations

OpenScape Business clients and devices are in use with many different client environments, operating systems, web browsers etc.

The manufacturers of these environments have different detailed requirements for the format, content and validity period of the server-side SSL certificates. When creating the Certificate Signing Request for your trusted SSL certificate, please follow the relevant guidelines for your client environment.
For example, Apple frequently publishes server certificate requirement updates on their support portal which are relevant for iOS and macOS based client applications:
https://support.apple.com/en-ca/103769
https://support.apple.com/en-us/102028

7 Future plans

Unify is working on the implementation of „Let's Encrypt" in OpenScape Business. Let's Encrypt is a non-profit certificate authority that provides SSL certificates for Transport Layer Security (TLS) encryption at no charge.

With Let's Encrypt, the SSL certificates are handled by an automated process designed to overcome manual creation, validation, signing, installation, and renewal of certificates for secure websites.

© 2024 Mitel Networks Corporation. All Rights Reserved. Mitel and the Mitel logo are trademark(s) of Mitel Networks Corporation. Unify and associated marks are trademarks of Unify Software and Solutions GmbH & Co. KG. All other trademarks herein are the property of their respective owners.