# GYTPOL Validator

## PEM Certificate setup

**Doc: GYT-TEC-012**
**Release: 1**
**Date: 28th February 2023**

| | |
|---|---|
| **Total pages:** | 3 |

| | |
|---|---|
| **Doc. Title:** | GYTPOL Validator<br>PEM Certificate setup |

| | | | |
|---|---|---|---|
| **Doc. No.:** | GYT-TEC-012 | **Classification:** | Confidential |
| **Revision:** | 2 | **Restriction:** | GYTPOL and approved recipients |
| **Date:** | 28th Feb 2023 | **Customer:** | |

| | | | |
|---|---|---|---|
| **Owner:** | Mark Zuk | **Reviewers/ Approvers:** | Matthew Album<br>Gilad Raz<br>Tal Kollender |
| **Author:** | Mark Zuk | | |

# Introduction

The purpose of this document is to provide instructions to create a certificate supported by GYTPOL in PEM format.

# Workflow

To create a PEM certificate - use a third-party software or install OpenSSL (free) and turn your PFX certificate to PEM format.

In case of using OpenSSL, please use the following steps:

## Creating the right format of certificate (OpenSSL)

1. Open a **CMD as Admin** window and change to the directory where you installed OpenSSL, i.e. **c:\program files\OpenSLL-Win64\bin\**

2. Run the following command to extract the private key and save it to a new file:

```
openssl pkcs12 -in yourpfxfile.pfx -nocerts -out client-key.pem -nodes
```

(You will be asked for the PFX password if there is one)

- If there is PEM Password/Phrase - run the following instead of the above **#2**:

```
openssl pkcs12 -in yourpfxfile.pfx -nocerts -out client-key-temp.pem
```

(You will be asked for the PFX password + PEM password)

```
openssl rsa -in client-key-temp.pem -out client-key.pem
```

(You will be asked for the PFX password if there is one)

3. Now run the following command to also extract the public cert and save it to a new file:

```
openssl pkcs12 -in yourpfxfile.pfx -nokeys -out client-cert.pem -nodes
```

(you will be asked for the PFX password if there is one)

## Changing within the server

Copy the files created on the first step (**client-key.pem** and **client-cert.pem**) into the following location on Gytpol server: ***gytpolInstalDrive*:\gytpol\data\websrv** (backup and then replace the existing files).

Next, restart the service "**Gytpol WebUI Service**" and open again the console with the FQDN of the server (or Netbios name - depends on the certificate you generated).

## Troubleshooting

If webUI service is unable to start, please rollback the **client-key.pem** and **client-cert.pem** using the original files you backed up and start the webUI service.
Please open Event Viewer and look for any errors related to webUI and make sure the steps above were followed correctly.
Please contact support@gytpol.com for any assistance needed.