

DMS Connectivity Guide



How to establish connection to AS4 gateway

Indholdsfortegnelse

Introduction	3
Checklist for establishing connectivity	4
1. Get approved to use DMS.....	5
1.1 Get approved to use DMS.....	6
2. Acquire OCES certificate	7
2.1 Acquire OCES certificate	8
2.2 Certificates supported	8
2.2.1 MitID Organisation certificate (Organisationscertifikat) – VOCES3	8
2.2.2 MitID System certificate (Systemcertifikat) – FOCES3.....	8
2.2.3 MitID Employee certificate (Medarbejdercertifikat) – MOCES3.....	9
3. Setting up a system user	10
3.1 Setting up a system user	11
3.1.1 System user for TFE-environment.....	11
3.1.2 System user for PROD environment	11
3.1.3 DMS Online access	11
3.1.4 DMS System-to-System access	12
3.1.5 If your company lodge declarations using a SE-number rather than CVR-number....	12
4. Register client certificate	13
4.1 Register client certificate	14
5. Network connection	16
5.1 AS4 gateway server details.....	17
5.2 Verifying network access	17
5.2.1 Unix	17
5.2.2 Windows.....	18
6. Introduction to AS4.....	20
6.1 AS4 message structure.....	21
6.1.1 AS4 services	21
6.1.2 Submitter	21
6.1.3 Security.....	22
6.1.4 Complete AS4 payload samples	22
6.1.5 AS4 push header.....	23
6.2 Notification.....	25
7. Using the simple AS4 client	26
7.1 Using the simple AS4 client made by the IT and Development Agency	27
8. Appendices	28
8.1 Install certificate	29
8.1.1 Verifying correct certificate.....	33
8.1.2 Troubleshooting certificates in the browser.....	34
8.2 Technical overview of system-to-system.....	38

- 8.3 Examples of synchronous answers 38
 - 8.3.1 Approved messages 38
 - 8.3.2 Unapproved messages 39
- 8.4 Error resolution..... 39
- 8.5 DMS fails to authenticate user..... 39

Introduction

This document is a guide on how to establish access to the AS4 gateway for delivering files to the new declaration management system DMS. It describes server details and the process of setting up and verifying the connection to DMS System-to-system.

As the system uses the AS4 standard, this document describes the general aspects of AS4, the needed AS4 header, security, attachment setup, common errors, and their resolutions.

The guide will refer to two agencies under the Danish Ministry of Taxation: the IT and Development Agency (Udviklings- og Forenklingsstyrelsen) and the Danish Customs Agency (Toldstyrelsen). The guide will also refer to the Danish Customs and Tax Administration (Skatteforvaltningen) which both agencies, together with five other agencies in the Ministry, are a part of. Until 2018 'Skatteforvaltningen' was called 'SKAT'.

The term 'company' corresponds to the term *economic operators* in the Union Customs Code (EU-toldkodeksen).

Checklist for establishing connectivity

Follow the steps below to connect to the AS4 gateway. Make sure to successfully complete each step before moving on to the next.

Step	Description
1	Get approval to use DMS
2	Acquire OCES3 certificate
3	Setting up roles for system users
4	Register client certificate and acquire username and password
5	Setting up network connection

As a supplement to help with integration to the AS4 gateway, a user-friendly AS4 client has been prepared. You’ll find further information in chapter 7.

Get approved to use DMS

1

1.1 Get approved to use DMS

DMS is accessible through two primary channels. Either

1. through DMS Online, or
2. through DMS System-to-System.

Either option requires approval by the Danish Customs Agency which can be obtained by applying for access to DMS on toldst.dk

Acquire OCES certificate

2

2.1 Acquire OCES certificate

System-to-system access is especially suitable for companies with a high volume of declarations. Access requires a valid OCES3 certificate issued by mitid-erhverv.dk

Please note that this document only includes examples of OCES3 certificate usage as OCES2 certificates cannot be used after 31 October 2023 as informed by Digitaliseringsstyrelsen (DIGST).

Companies that are already using OCES2 certificates on the AS4 gateway should note that using an OCES3 requires registration as a new/first time user. It is NOT possible to upload an OCES3 certificate within an OCES2 user account. After registering the OCES3 certificate you will no longer be able to log in to DMS using the existing OCES2 certificate. This will break already functional integrations to DMS.

Please observe that OCES certificates issued for the following systems can be reused:

- eKapital
- Told Manifest
- Told ICS

Please note that neither the IT and Development Agency or the Danish Customs Agency can issue or lookup the relevant OCES certificate. Acquiring and keeping track of certificates is the responsibility of each company and will thus not be covered by this guide. If you have an existing certificate but cannot locate it a new can be issued by MitID Erhverv.

OBS! Having a new certificate issued should be considered a last resort, since this will invalidate the existing certificate and break already functional integrations towards the Danish Customs and Tax Administration (Skatteforvaltningen).

There are different types of OCES3 certificates. The three relevant here are: VOCES (MitID organisationscertifikat) FOCES (MitID Systemcertifikat) and MOCES (MitID Brugercertifikat). We recommend using a FOCES or VOCES certificate. FOCES are supported on the AS4 gateway from 17 May 2023.

All certificates are identified by an UUID (called UI in short) consisting of 36 characters.

2.2 Certificates supported

Below is listed the types of certificates that the AS4-gateway support and which we recommend.

2.2.1 MitID Organisation certificate (Organisationscertifikat) – VOCES3

Represents the organization. Includes the name of the organization, CVR-number and an e-mail. See more under www.mitid-erhverv.dk/avanceret/certifikater<http://www.mitid-erhverv.dk/avanceret/certifikater>

Recommended for connectivity to DMS.

2.2.2 MitID System certificate (Systemcertifikat) – FOCES3

Note that FOCES2 certificate policies are discontinued and in the OCES3 infrastructure FOCES is just a profile under the VOCES certificate policy.

A FOCES certificate is a specialization of an organisationscertifikat and represents a specific system in your organization. The certificate is issued to and used by the system to identify itself when it is in contact with internal or external systems.

Recommended for connectivity to DMS.

2.2.3 MitID Employee certificate (Medarbejdercertifikat) – MOCES3

An individual employee's MOCES certificate can be used instead of a VOCES or FOCES certificate. However, using MOCES certificates for system-to-system communication is advised against for multiple reasons. For example, since the certificate is personal, you would be required to get a new one if the person in question leaves your company, where a VOCES/FOCES certificate only needs renewal.

Not recommended for connectivity to DMS.

Setting up a system user

3

3.1 Setting up a system user

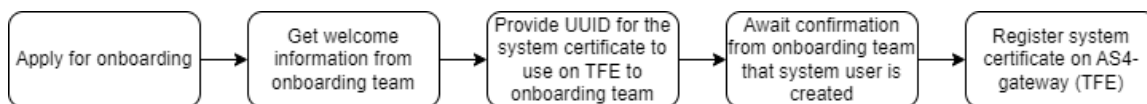
Once you have been approved by the Danish Customs Agency to use DMS, the next step is to have a system user created and appropriate roles assigned to it.

Important! See section 3.1.5 if your company uses SE-number rather than CVR-number when sending in declarations.

3.1.1 System user for TFE-environment

For the test environment, TFE, the system user must be created by Udviklings- og Forenklingsstyrelsen. It is not possible to lodge declarations through the AS4 gateway before the system user is properly set up. After being approved, you will be asked for the UUID/UI of the oces3 certificate you wish to use for the AS4 gateway. **The UUID/UI can be found by the method described in section 8.1.1.**

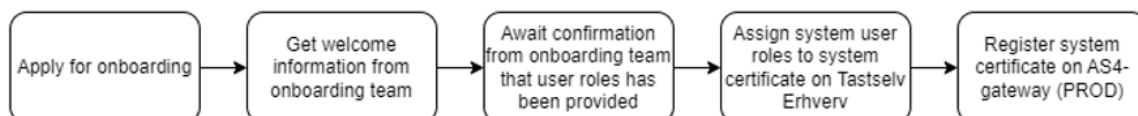
The process can be illustrated like this:



3.1.2 System user for PROD environment

The process for the production environment is almost the same as for the TFE environment, with the difference that your company's MitID Erhverv -administrator directly can give employees access to DMS Online and give the system user access to DMS System-to-System. This is done via Tastselv Erhverv, <https://www.tastselv.skat.dk/>. However, this requires that Udviklings- og Forenklingsstyrelsen has given your company the necessary roles.

The process for PROD environment can be illustrated like this:



Details on how those roles are assigned to system certificate on Tastselv Erhverv can be found in the document DMS [Vejledning til roller og rettigheder](#).

3.1.3 DMS Online access

If your company has applied for access to DMS Online your company's MitID administrator can grant roles to the employees.

Most companies with DMS System-to-System access will likely also want access to DMS Online in order to be able to check declaration statuses. Visit oldst.dk to find links for DMS Online. Here you can also find links for login to DMS Online and guides on how to grant roles to employees.

3.1.4 DMS System-to-System access

Establishing DMS System-to-System access is covered throughout the rest of the guide.

3.1.5 If your company lodge declarations using a SE-number rather than CVR-number

If your company, when sending in declarations, wishes to do this by using one or more SE-numbers rather than a CVR-number you must register a certificate for each SE-number in question. You can not use the same certificate for several SE-numbers. The reason is that DMS sees a SE-number as a separate entity of the company and the system user (the certificate) can only belong to one entity.

Example:

Acme Industries – CVR 12345678 has 2 divisions with each its own SE-number as well as a headquarter.

- Division East – SE 44444444 lodges declaration on that SE-number. A specific certificate needs to be registered for this entity.
- Division West – SE 88888888 lodges declaration on that SE-number A specific certificate needs to be registered for this entity.
- Headquarter – No SE-number. Lodges declarations on CVR-number. A specific certificate needs to be registered for this entity

In all 3 certificates need to be registered for this company. One for Division East, One for Division West and one for Headquarter. All certificates are issued for CVR 12345678.

See section 4 on how to register the certificates.

Register client certificate

4

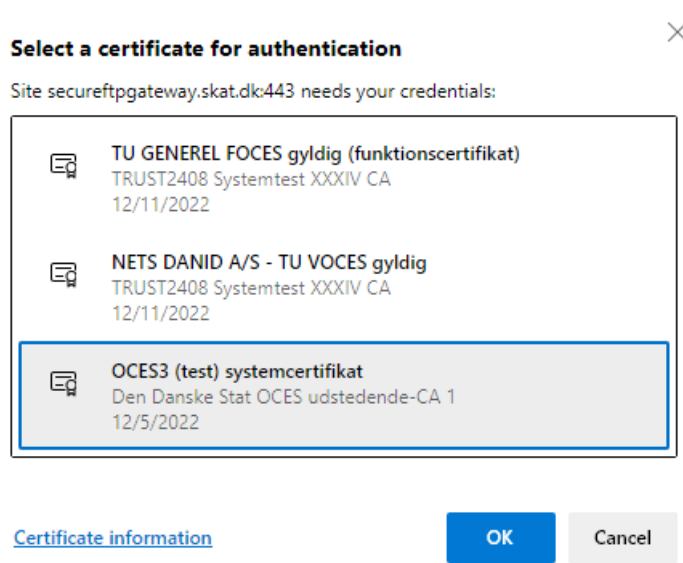
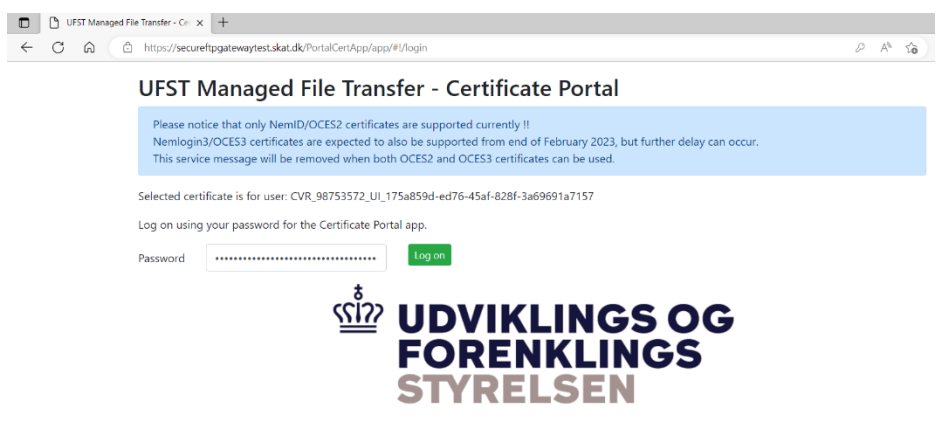
4.1 Register client certificate

The certificate portal provides self-service for pre-registration of certificates.

TFE: secureftpgatewaytest.skat.dk

PROD: secureftpgateway.skat.dk

The OCES certificate must be installed on the local computer. For details on how to install a certificate, see appendix 8.1 Install certificate and 8.1.2 on how to add the certificate to the web-browser.

Registering certificate for system-to-system usage	
<p>1. In this example, multiple certificates have been imported to the browser.</p> <p>Here we select a MitID Erhverv test certificate and enter the logon page of the certificate portal.</p>	
<p>2. The CVR and UUID information is extracted from the certificate. In this example, you are identified as user: CVR_98753572_UI_175a859d-ed76-45af-828f-3a69691a7157.</p> <p>Important: The first time you log in, the default password is <u>your user ID</u>. You can therefore simply copy and paste, and proceed to log in.</p> <p>Note: Your email address is extracted from the certificate (if present). Please make sure you have a valid and relevant email address for your certificate as this could be used to contact you later.</p>	

<p>3. The first time you log in you are required to change password. This password is used for logging in to the registration self-service portal. Changing this password does not change the password of the certificate used when connecting to the gateway.</p> <p>You can use the same password used for your certificate or select a new password.</p>	<div><div>Change password</div><div>You must change the default password!</div><div>Current password<div>.....</div></div><div>New password<div>.....</div></div><div>Confirm password<div>.....</div></div><div>Change passwordCancel</div></div>
<p>4. At this moment the certificate is not yet registered in the self-service portal. The AS4 gateway will therefore reject any logon attempt at this time.</p> <p>If you lodge declarations using a SE-number and not just the CVR fill out the field “<i>SE-number</i>” with the SE-number used for this certificate. Otherwise leave it empty. See section 3.1.5 of this guide.</p> <p>Check the AS4 box in the interface section.</p> <p>Proceed to press: “register certificate”.</p>	<div>UFST Managed File Transfer - Certificate/User overview</div> <div>Your certificate is not registered in UFST MFT. Press 'Register Certificate' in order to update the certificate in UFST MFT.</div> <div><div>Common name</div><div>OCE33 (test) systemcertifikat</div></div> <div><div>Expiry date</div><div>04-12-2025</div></div> <div><div>Type</div><div>CVR</div></div> <div><div>E-mail</div><div></div></div> <div><div>Legal identifier</div><div>CVR_98753572</div></div> <div><div>Account</div><div>UL_175a859d-ed76-45af-828f-3a69691a7157</div></div> <div><div>SE-number</div><div></div></div> <div><div>Interfaces</div><div><input type="checkbox"/> FTPS <input checked="" type="checkbox"/> AS4</div></div> <div>Register certificate</div> <div>Refresh</div>
<p>5. The registration process starts and should be completed within a few minutes. Use the refresh button to verify that the registration has been completed.</p>	<div><div>Register certificate</div><div>Refresh</div><div>Certificate has been registered. It can take a few minutes for the registration process to complete. Press 'Refresh' after a few minutes to see the updated status.</div></div>
<p>6. The certificate is now registered.</p> <p>Note down your username and password, which will be used for setting up your AS4 session.</p>	<div>UFST Managed File Transfer - Certificate/User overview</div> <div>Your certificate is registered and ready for use.</div> <div><div>Common name</div><div>OCE33 (test) systemcertifikat</div></div> <div><div>Expiry date</div><div>04-12-2025</div></div> <div><div>Type</div><div>CVR</div></div> <div><div>Legal identifier</div><div>CVR_98753572</div></div> <div><div>Account</div><div>UL_175a859d-ed76-45af-828f-3a69691a7157</div></div> <div><div>SE-number</div><div></div><div>Update SE-number</div></div> <div><div>E-mail</div><div>do-not-write@skat.dk</div><div>Update e-mail</div></div> <div><div>Interfaces</div><div><input type="checkbox"/> FTPS <input checked="" type="checkbox"/> AS4</div><div>Update interfaces</div></div> <div><div>Gateway user</div><div>CVR_98753572_UL_175a859d-ed76-45af-828f-3a69691a7157</div></div> <div><div>Gateway password</div><div>.....</div></div>
<p>7. Finish by selecting “Log out”.</p>	

Network connection

5

5.1 AS4 gateway server details

Environment	Hostname	Port	IP
Test/TFE	secureftpgatewaytest.skat.dk	6384	195.85.251.85
PROD	secureftpgateway.skat.dk	6384	195.85.251.102

The client needs access to this server, on the correct port.

OBS! Neither the IT and Development Agency or the Danish Customs Agency can help with opening the correct ports for access. Confirm access to the non-standard ports with your maintenance vendor.

As far as possible, the client needs to resolve the host name on suitable name server. The IP listed above is the currently active IP at the time of writing. The given IPs are likely to change.

A complete list of services and actions on the AS4 gateway can be found in the appendix of the [DMS System Guide](#) document found Github.

5.2 Verifying network access

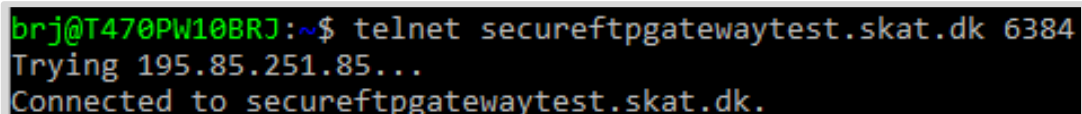
The following section describes various methods for verifying connectivity from the client towards the DMS System-to-System solution. Which method to use is determined by the availability of tools on the client setup.

5.2.1 Unix

This section describes ways to test the connectivity on Unix-style servers, using common connectivity testing tools.

Method #1 – telnet

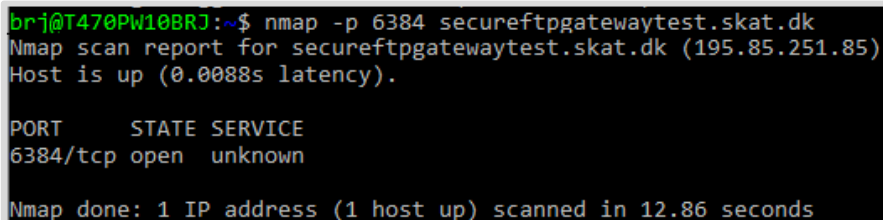
```
telnet <Hostname> 6384
```



```
brj@T470PW10BRJ:~$ telnet secureftpgatewaytest.skat.dk 6384
Trying 195.85.251.85...
Connected to secureftpgatewaytest.skat.dk.
```

Method #2 – nmap

```
nmap -p 6384 <Hostname>
```



```
brj@T470PW10BRJ:~$ nmap -p 6384 secureftpgatewaytest.skat.dk
Nmap scan report for secureftpgatewaytest.skat.dk (195.85.251.85)
Host is up (0.0088s latency).

PORT      STATE SERVICE
6384/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 12.86 seconds
```

Method #3 – openssl

```
openssl s_client -connect <Hostname>:443 -showcerts
```

```

prj@1470PW108R3:~$ openssl s_client -connect secureftpgatewaytest.skat.dk:443 -showcerts
CONNECTED(00000003)
depth=2 OU = GlobalSign Root CA - R3, O = GlobalSign, CN = GlobalSign
verify return:1
depth=1 C = BE, O = GlobalSign nv-sa, CN = GlobalSign RSA OV SSL CA 2018
verify return:1
depth=0 C = DK, ST = Copenhagen, L = Copenhagen Oe, O = Skatteforvaltningen, CN = secureftpgatewaytest.skat.dk
verify return:1
139743226499712:error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake failure:../ssl/record/rec_layer_s3.c:1543:SSL alert number 40
...
Certificate chain
 0 s:C = DK, ST = Copenhagen, L = Copenhagen Oe, O = Skatteforvaltningen, CN = secureftpgatewaytest.skat.dk
 1 C = BE, O = GlobalSign nv-sa, CN = GlobalSign RSA OV SSL CA 2018
-----BEGIN CERTIFICATE-----
MIIGqjCCBZKgAwIBAgITMdnh1InSQ0EDNYMGVMA0GCSqG5Ib3Q0EBCwUAMFAx CzA3
BgNVBAYTAkFRKwFuYDVOQQkxExBHBG91YXkTaWduIG51ZCXXNhM5YyJAYDVOQQkxEx
bG91YXkTaWduIFJ1TSBpbnV1BU0wQ0Q0BgMjAxODAwFw0xOTExMTM0MDAwFw0y
MjAxMDQwMDExMDAwMDE4MDE4CzA3BgNVBAYTAkRHRmRwEYDVQQEYwV3B1b2hhbmhZ2Vv
MRYyYFAYDVOQQHEwIDB3B1b2hhbmhZ2VvIE91RmRwEYDVQQKEwNtX2F0dG9mb332YVw0
bm1uZ2VvM5U0YVYDVOQQDEkxzZWNIc3VmndHMhYXR1d2F5dGVZdC52aF08LnRrMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsxOn1pL26S3H9VAP1PJDzJK9
4gSB/PfPVVc5s1F8eb6KqKQA8M47LXqeIz9+q6vqh4o+WAhgZqU5Q0b7TFysIBR
Dep1F8CtB3UG/c3ypbz+X00Q5Ux2y3stQ06vD12GNpct4w0/HCF9ZwK1AxKdke7w
t8hwYzamao3w0Wdd5x0QKSU8rdogqx+ZJb1+o1cFegqazh18n2ke1oFRZrygl
vP1SEU/YZT2ZQuwSdqtUTrFhAZHfPeSf1H2P1Rp33yAq3Kt08PAKGRNMST190uD
hqq6mG71CRTC1zq7aEYXpWxyR8QC07ySME51fmgU304c096051QFzwh2K5wD
A0Kp41D1uCCAB8BgNVBAYTAkFRKwFuYDVOQQkxExBHBG91YXkTaWduIG51ZCXXNhM5YyJAYDVOQQkxEx
bG91YXkTaWduIFJ1TSBpbnV1BU0wQ0Q0BgMjAxODAwFw0xOTExMTM0MDAwFw0y
MjAxMDQwMDExMDAwMDE4MDE4CzA3BgNVBAYTAkRHRmRwEYDVQQEYwV3B1b2hhbmhZ2Vv
MRYyYFAYDVOQQHEwIDB3B1b2hhbmhZ2VvIE91RmRwEYDVQQKEwNtX2F0dG9mb332YVw0
bm1uZ2VvM5U0YVYDVOQQDEkxzZWNIc3VmndHMhYXR1d2F5dGVZdC52aF08LnRrMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsxOn1pL26S3H9VAP1PJDzJK9
4gSB/PfPVVc5s1F8eb6KqKQA8M47LXqeIz9+q6vqh4o+WAhgZqU5Q0b7TFysIBR
Dep1F8CtB3UG/c3ypbz+X00Q5Ux2y3stQ06vD12GNpct4w0/HCF9ZwK1AxKdke7w
t8hwYzamao3w0Wdd5x0QKSU8rdogqx+ZJb1+o1cFegqazh18n2ke1oFRZrygl
vP1SEU/YZT2ZQuwSdqtUTrFhAZHfPeSf1H2P1Rp33yAq3Kt08PAKGRNMST190uD
hqq6mG71CRTC1zq7aEYXpWxyR8QC07ySME51fmgU304c096051QFzwh2K5wD
A0Kp41D1uCCAB8BgNVBAYTAkFRKwFuYDVOQQkxExBHBG91YXkTaWduIG51ZCXXNhM5YyJAYDVOQQkxEx
bG91YXkTaWduIFJ1TSBpbnV1BU0wQ0Q0BgMjAxODAwFw0xOTExMTM0MDAwFw0y
MjAxMDQwMDExMDAwMDE4MDE4CzA3BgNVBAYTAkRHRmRwEYDVQQEYwV3B1b2hhbmhZ2Vv
MRYyYFAYDVOQQHEwIDB3B1b2hhbmhZ2VvIE91RmRwEYDVQQKEwNtX2F0dG9mb332YVw0
bm1uZ2VvM5U0YVYDVOQQDEkxzZWNIc3VmndHMhYXR1d2F5dGVZdC52aF08LnRrMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsxOn1pL26S3H9VAP1PJDzJK9
4gSB/PfPVVc5s1F8eb6KqKQA8M47LXqeIz9+q6vqh4o+WAhgZqU5Q0b7TFysIBR
Dep1F8CtB3UG/c3ypbz+X00Q5Ux2y3stQ06vD12GNpct4w0/HCF9ZwK1AxKdke7w
t8hwYzamao3w0Wdd5x0QKSU8rdogqx+ZJb1+o1cFegqazh18n2ke1oFRZrygl
vP1SEU/YZT2ZQuwSdqtUTrFhAZHfPeSf1H2P1Rp33yAq3Kt08PAKGRNMST190uD
hqq6mG71CRTC1zq7aEYXpWxyR8QC07ySME51fmgU304c096051QFzwh2K5wD
A0Kp41D1uCCAB8BgNVBAYTAkFRKwFuYDVOQQkxExBHBG91YXkTaWduIG51ZCXXNhM5YyJAYDVOQQkxEx
bG91YXkTaWduIFJ1TSBpbnV1BU0wQ0Q0BgMjAxODAwFw0xOTExMTM0MDAwFw0y
MjAxMDQwMDExMDAwMDE4MDE4CzA3BgNVBAYTAkRHRmRwEYDVQQEYwV3B1b2hhbmhZ2Vv
MRYyYFAYDVOQQHEwIDB3B1b2hhbmhZ2VvIE91RmRwEYDVQQKEwNtX2F0dG9mb332YVw0
bm1uZ2VvM5U0YVYDVOQQDEkxzZWNIc3VmndHMhYXR1d2F5dGVZdC52aF08LnRrMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsxOn1pL26S3H9VAP1PJDzJK9
4gSB/PfPVVc5s1F8eb6KqKQA8M47LXqeIz9+q6vqh4o+WAhgZqU5Q0b7TFysIBR
Dep1F8CtB3UG/c3ypbz+X00Q5Ux2y3stQ06vD12GNpct4w0/HCF9ZwK1AxKdke7w
t8hwYzamao3w0Wdd5x0QKSU8rdogqx+ZJb1+o1cFegqazh18n2ke1oFRZrygl
vP1SEU/YZT2ZQuwSdqtUTrFhAZHfPeSf1H2P1Rp33yAq3Kt08PAKGRNMST190uD
hqq6mG71CRTC1zq7aEYXpWxyR8QC07ySME51fmgU304c096051QFzwh2K5wD
A0Kp41D1uCCAB8BgNVBAYTAkFRKwFuYDVOQQkxExBHBG91YXkTaWduIG51ZCXXNhM5YyJAYDVOQQkxEx
bG91YXkTaWduIFJ1TSBpbnV1BU0wQ0Q0BgMjAxODAwFw0xOTExMTM0MDAwFw0y
MjAxMDQwMDExMDAwMDE4MDE4CzA3BgNVBAYTAkRHRmRwEYDVQQEYwV3B1b2hhbmhZ2Vv
MRYyYFAYDVOQQHEwIDB3B1b2hhbmhZ2VvIE91RmRwEYDVQQKEwNtX2F0dG9mb332YVw0
bm1uZ2VvM5U0YVYDVOQQDEkxzZWNIc3VmndHMhYXR1d2F5dGVZdC52aF08LnRrMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsxOn1pL26S3H9VAP1PJDzJK9
4gSB/PfPVVc5s1F8eb6KqKQA8M47LXqeIz9+q6vqh4o+WAhgZqU5Q0b7TFysIBR
Dep1F8CtB3UG/c3ypbz+X00Q5Ux2y3stQ06vD12GNpct4w0/HCF9ZwK1AxKdke7w
t8hwYzamao3w0Wdd5x0QKSU8rdogqx+ZJb1+o1cFegqazh18n2ke1oFRZrygl
vP1SEU/YZT2ZQuwSdqtUTrFhAZHfPeSf1H2P1Rp33yAq3Kt08PAKGRNMST190uD
hqq6mG71CRTC1zq7aEYXpWxyR8QC07ySME51fmgU304c096051QFzwh2K5wD
A0Kp41D1uCCAB8BgNVBAYTAkFRKwFuYDVOQQkxExBHBG91YXkTaWduIG51ZCXXNhM5YyJAYDVOQQkxEx
bG91YXkTaWduIFJ1TSBpbnV1BU0wQ0Q0BgMjAxODAwFw0xOTExMTM0MDAwFw0y
MjAxMDQwMDExMDAwMDE4MDE4CzA3BgNVBAYTAkRHRmRwEYDVQQEYwV3B1b2hhbmhZ2Vv
MRYyYFAYDVOQQHEwIDB3B1b2hhbmhZ2VvIE91RmRwEYDVQQKEwNtX2F0dG9mb332YVw0
bm1uZ2VvM5U0YVYDVOQQDEkxzZWNIc3VmndHMhYXR1d2F5dGVZdC52aF08LnRrMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsxOn1pL26S3H9VAP1PJDzJK9
4gSB/PfPVVc5s1F8eb6KqKQA8M47LXqeIz9+q6vqh4o+WAhgZqU5Q0b7TFysIBR
Dep1F8CtB3UG/c3ypbz+X00Q5Ux2y3stQ06vD12GNpct4w0/HCF9ZwK1AxKdke7w
t8hwYzamao3w0Wdd5x0QKSU8rdogqx+ZJb1+o1cFegqazh18n2ke1oFRZrygl
vP1SEU/YZT2ZQuwSdqtUTrFhAZHfPeSf1H2P1Rp33yAq3Kt08PAKGRNMST190uD
hqq6mG71CRTC1zq7aEYXpWxyR8QC07ySME51fmgU304c096051QFzwh2K5wD
A0Kp41D1uCCAB8BgNVBAYTAkFRKwFuYDVOQQkxExBHBG91YXkTaWduIG51ZCXXNhM5YyJAYDVOQQkxEx
bG91YXkTaWduIFJ1TSBpbnV1BU0wQ0Q0BgMjAxODAwFw0xOTExMTM0MDAwFw0y
MjAxMDQwMDExMDAwMDE4MDE4CzA3BgNVBAYTAkRHRmRwEYDVQQEYwV3B1b2hhbmhZ2Vv
MRYyYFAYDVOQQHEwIDB3B1b2hhbmhZ2VvIE91RmRwEYDVQQKEwNtX2F0dG9mb332YVw0
bm1uZ2VvM5U0YVYDVOQQDEkxzZWNIc3VmndHMhYXR1d2F5dGVZdC52aF08LnRrMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsxOn1pL26S3H9VAP1PJDzJK9
4gSB/PfPVVc5s1F8eb6KqKQA8M47LXqeI
```

5.2.2 Windows

This section describes ways to test the connectivity on Windows-style servers using common connectivity testing tools.

Method #1 - Test-NetConnection [Requires execution in Powershell]

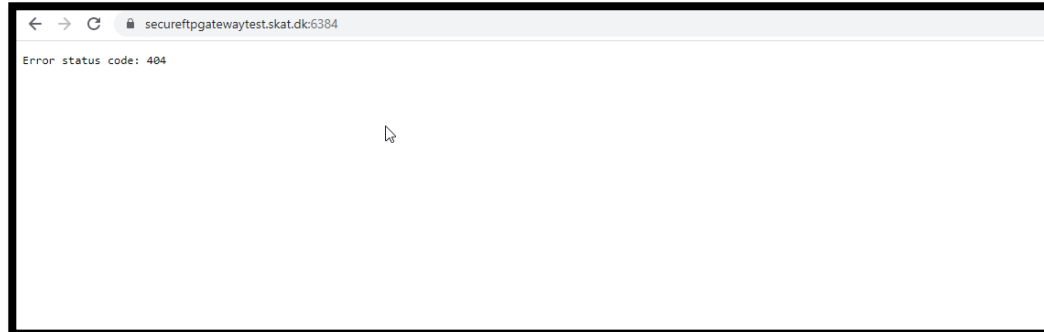
```
Test-NetConnection <Hostname>-Port 6384
```

```
PS Z:\> Test-NetConnection secureftpgatewaytest.skate.dk -Port 6384

ComputerName      : secureftpgatewaytest.skate.dk
RemoteAddress     : 195.85.251.85
RemotePort        : 6384
InterfaceAlias    : Ethernet 67
SourceAddress     : 192.168.146.12
TcpTestSucceeded  : True
```

Method #2 – Browser

Open <https://<Hostname>:6384> in a browser that has access to the internet - on a client setup that the internal network is set up as the accessing system. If it works, you will receive a 404 error.



Introduction to AS4

6

6.1 AS4 message structure

AS4 is a standard describing various fields related to the message transfer – described in a header. AS4 furthermore standardises encryption and signing of the payload, using the WS-* standard. AS4 is closely related to SOAP, in that it utilizes the soap-envelope for defining headers and payload elements. The main difference from AS4 to SOAP, is that there is no SOAP-WSDL describing the service. This means that there is not a single file to help define the complete service schemas and endpoints. Therefore, the following must be defined:

- AS4 header XSD
- Payload XSD (either declaration or notification)
- Endpoint
- Encryption settings

6.1.1 AS4 services

The following section describes the available services provided by AS4. The parameters `UserMessage.CollaborationInfo [Service]` and `UserMessage.CollaborationInfo [Action]` in the AS4 header allows setting which service the AS4 message is destined for.

A full list of environment specific services and actions is available in the appendix of the [DMS System Guide](#), in the section titled **AS4 Services**, which is available on [Github](#).

```
<eb3:CollaborationInfo>
  <eb3:Service type="string">DMS.Export</eb3:Service>
  <eb3:Action>Notification</eb3:Action>
  <eb3:ConversationId>placeholder</eb3:ConversationId>
</eb3:CollaborationInfo>
```

6.1.2 Submitter

A submitter needs to be provided in the payload and AS4 header of every call to the AS4 gateway. For all companies, the submitter reference must be either the CVR-number of the company **or** the SE-number for which the certificate was registered for in the certificate portal (See section 3.1.5 and section 4).

For example, if a company has the CVR number “CVR_98753572” then the submitter reference will be “98753572”. This CVR must match the CVR in the OCES certificate used. A SE number can also be used and must match the SE-number for which the certificate was registered for.

For Export and Import the submitter field then looks as follows:

```
<ns2:Submitter>
  <ns2:Name>98753572</ns2:Name>
  ...
</ns2:Submitter>
```

For transit declarations and IE-messages related to export and transit the CVR/SE number registered in the certificate needs to be placed in the `messageSender` field:

```
<messageSender>98753572</messageSender>
```

For Exit declarations the submitter field looks as follows:

```
<ns2:Submitter>
  <ns2:name>
    <ns2:Text.Content>98753572</ns2:Text.Content>
  </ns2:name>
  ...
</ns2:Submitter>
```

For more information on the Submitter element, see the XML Guides on [Skatteforvaltningen's GitHub](#).

6.1.3 Security

The following webpage describes detailed the security aspects about AS4: [eDelivery AS4 - 1.15 \(europa.eu\)](#)

In general, the DMS solution expects the following elements being signed:

- Body
- Messaging
- cid:Attachments

The solution has been tested using hash-function/digest-method: xmenc#sha256 – and signature Algorithm: xmldsig-more#rsa-sha256.

OBS! The solution does not (!) encrypt XML messages. However, the data stream itself is of course encrypted through TLS.

6.1.4 Complete AS4 payload samples

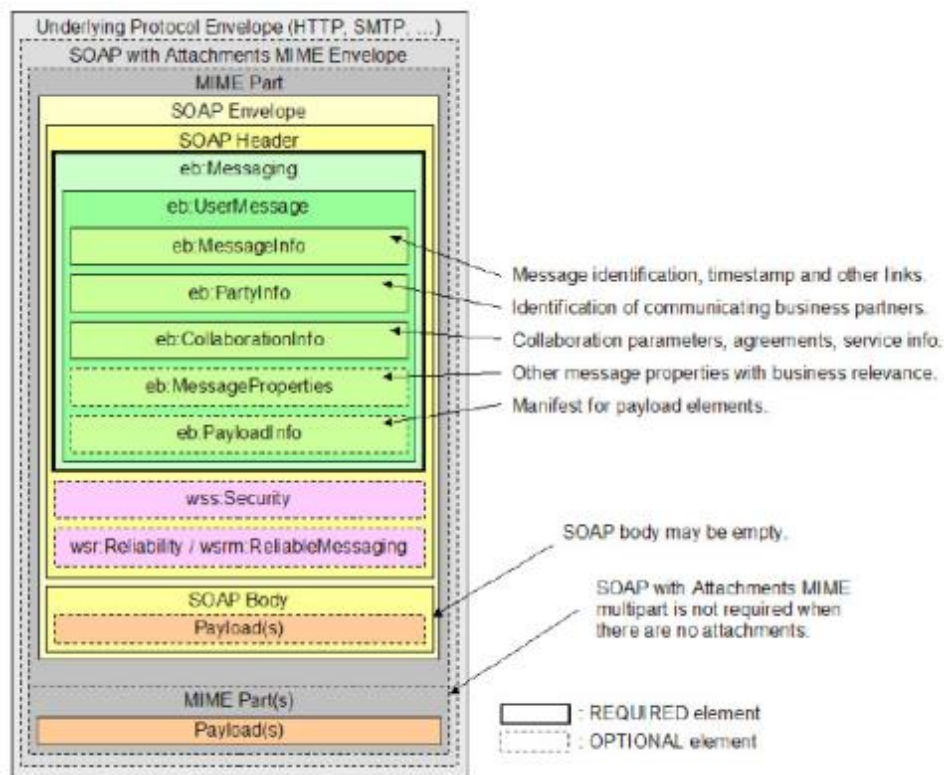
This section contains a few examples of properly formatted XML messages, with their AS4 headers, sent to DMS, with the replies received included. Fully signed message, with username and password is available as an appendix which can be found on [Github](#).

The setup of the following depends wholly on the client setup. There exist many implementations of AS4 clients and how these settings are applied is determined by the client. A list of existing open source AS4 clients can be found on following sites:

- <https://peppol.eu/downloads/peppolimplementations/>
- <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4+conformant+solutions>

The Holodeck AS4 solution has been used internally at the IT and Development Agency for testing the AS4 delivery method.

An AS4 message allows sending of a payload only as an attachment to the message, and not in the body. In DMS the main payload – the declaration, or request for notification – is therefore set to be delivered in the attachment. The message structure is shown here below:



6.1.5 AS4 push header

The AS4 header XSD can be downloaded from this URL: https://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/ebms-header-3_0-200704.xsd

Some clients come with this header preloaded.

This section contains information about what information should be contained in the AS4 header for submitting a declaration.

OBS! The following attributes must be provided. The bolded values must not be changed. The rest depends on the client certificate and user.

Attribute	Value	Example
MessageInfo.Timestamp	YYYY-MM-DDTHH:MI:ss.SSSZ	2021-01-19T15:24:37.376Z
MessageInfo.MessageId	GUID@CVR_<CVR>_UI_<UUID>	d4872030-3862-4e7b-9754-17a98523e826@CVR_98753572_UI_175a859d-ed76-45af-828f-3a69691a7157
PartyInfo.From.PartyId	CVR_<CVR>_UI_<UUID>_AS4	CVR_98753572_UI_175a859d-ed76-45af-828f-3a69691a7157_AS4
PartyInfo.From.Role	AS4 Initiator role	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/initiator
PartyInfo.To.PartyId	AS4 receiver	SKAT-MFT-AS4

Attribute	Value	Example
PartyInfo.To.Role	AS4 Responder role	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/responder
CollaborationInfo. Service	Service prefix	DMS.Import2 (se AS4 service section for details)
CollaborationInfo. Action	Service postfix (action)	Declaration.Submit (se AS4 service section for details)
CollaborationInfo. ConversationId	GUID	f411f3b5-26ff-4207-baf9-a50526d9063f
MessageProperties. Property[lang]	Language	EN
MessageProperties. Property[procedureType]	Procedure type	H7 (se AS4 service section for details)
PayloadInfo.PartInfo. PartProperties.Property[original-file-name]	File name	im_decl_01.01.2021_0001.xml

A full XML example of the messaging header is shown below:

```
<eb3:Messaging xmlns:mustUnderstand="http://www.w3.org/2003/05/soap-envelope" xmlns:eb3="http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" mustUnderstand:mustUnderstand="true" wsu:Id="id-4b2850335f374e5-f471-4f64-9e3d-elb845277dd9">
  <eb3:UserMessage>
    <eb3:MessageInfo>
      <eb3:Timestamp>2021-01-19T15:24:37.376Z</eb3:Timestamp>
      <eb3:MessageId>d4872030-3862-4e7b-9754-17a98523e826@CVR_98753572_UI_175a859d-ed76-45af-828f-3a69691a7157</eb3:MessageId>
    </eb3:MessageInfo>
    <eb3:PartyInfo>
      <eb3:From>
        <eb3:PartyId type="string">CVR_98753572_UI_175a859d-ed76-45af-828f-3a69691a7157 AS4</eb3:PartyId>
        <eb3:Role>http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/initiator</eb3:Role>
      </eb3:From>
      <eb3:To>
        <eb3:PartyId type="string">SKAT-MFT-AS4</eb3:PartyId>
        <eb3:Role>http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/responder</eb3:Role>
      </eb3:To>
    </eb3:PartyInfo>
    <eb3:CollaborationInfo>
      <eb3:Service type="string">DMS.Import2</eb3:Service>
      <eb3:Action>Declaration.Submit</eb3:Action>
      <eb3:ConversationId>f411f3b5-26ff-4207-baf9-a50526d9063f</eb3:ConversationId>
    </eb3:CollaborationInfo>
    <eb3:MessageProperties>
      <eb3:Property name="lang">EN</eb3:Property>
      <eb3:Property name="procedureType">H7</eb3:Property>
    </eb3:MessageProperties>
    <eb3:PayloadInfo>
      <eb3:PartInfo>
        <eb3:PartProperties>
          <eb3:Property name="original-file-name">im_decl_01.01.2021_0001.xml
        </eb3:Property>
        </eb3:PartProperties>
      </eb3:PartInfo>
    </eb3:PayloadInfo>
  </eb3:UserMessage>
</eb3:Messaging>
```

6.2 Notification

Notifications from DMS are received from the AS4 gateway via a push-pull model. Pushing means requesting specific notifications to be added to the message queue and pulling means receiving the oldest messages from the message queue.

The recommended use of the notification service is to push a notification request every five minutes, asking for all notifications from previous seven minutes. Then the user's service should pull from the default message topic until the topic is empty.

Since it can take minutes to generate a response to your request, you may not necessarily get a reply to your latest request before you have emptied the topic. If you do not receive a response to a particular request within 10 minutes you should resend it.

The notifications in DMS received from the AS4 gateway are covered extensively in the System Guide, in the chapter **Requesting Notifications**, which is available on [GitHub](#).

Using the simple AS4 client

7

7.1 Using the simple AS4 client made by the IT and Development Agency

During earlier onboarding we observed **significant** difficulty with creating AS4 communication programming. Therefore, a simple to use package has been made. The goal of this package is to speed up the onboarding of companies and their service providers.

A Java based simple AS4 client is available through the link below. There, you can also find further references to the documentation, and advice for implementation:

<https://github.com/skat/simple-as4-client>

This package aims to facilitate developing a client which can communicate with the AS4 portal, and through it, the DMS import system. It covers the following:

- Converting an XML format declaration to an AS4 message
- Handles connectivity to the AS4 gateway
- Encryption and signing of AS4 messages
- Sending AS4 messages to AS4 gateway
- Receiving replies from AS4 gateway

The package is written in Java and provided as Java dependency. Integration with .NET based projects is therefore not as simple. For .NET based projects we recommend building a small Java based communication middleman REST API, which utilizes the simple AS4 client, that the existing .NET code can communicate with.

Appendices

8

8.1 Install certificate


Install certificate	
1. Locate the certificate you wish to install. It should be a file in .pfx/.p12 format. Double click the file.	See details chapter 2. Adding the certificate to the web-browser see section 8.1.2 Troubleshooting.
2. You should be presented with this menu. Click Next.	<div><div>← Certificate Import Wizard</div><div><div>×</div></div><div><div>Welcome to the Certificate Import Wizard</div><div><p>This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.</p><p>A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.</p><div><div>Store Location</div><div><div><input checked="" type="radio"/> Current User</div><div><input type="radio"/> Local Machine</div></div></div><div>To continue, click Next.</div><div><div>Next</div><div>Cancel</div></div></div></div></div>
3. Select the OCES certificate.	<div><div>← Certificate Import Wizard</div><div><div>×</div></div><div><div>File to Import</div><div>Specify the file you want to import.</div><div><div>File name:</div><div><div>C:\oces3_-test-_systemcertifikat.p12</div><div>Browse...</div></div></div><div><div>Note: More than one certificate can be stored in a single file in the following formats:</div><div><div>Personal Information Exchange- PKCS #12 (.PFX,.P12)</div><div>Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)</div><div>Microsoft Serialized Certificate Store (.SST)</div></div><div><div>Next</div><div>Cancel</div></div></div></div></div>

<div data-bbox="180 286 395 320" data-label="Section-Header"><h2>Install certificate</h2></div> <div data-bbox="180 365 616 421" data-label="Text"><p>4. Fill out the password and check the box to include all extended properties.</p></div>	<div data-bbox="655 342 1385 1048" data-label="Form"><div><div>←</div><div>Certificate Import Wizard</div><div>×</div></div><div><div>Private key protection</div><div>To maintain security, the private key was protected with a password.</div></div><div>Type the password for the private key.</div><div><div>Password:</div><div><div>••••••••••</div></div><div><input type="checkbox"/> Display Password</div></div><div><div>Import options:</div><div><div><input type="checkbox"/> Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.</div><div><input type="checkbox"/> Mark this key as exportable. This will allow you to back up or transport your keys at a later time.</div><div><input type="checkbox"/> Protect private key using virtualized-based security(Non-exportable)</div><div><input checked="" type="checkbox"/> Include all extended properties.</div></div></div><div><div>Next</div><div>Cancel</div></div></div>
<div data-bbox="180 1077 608 1133" data-label="Text"><p>5. Choose to automatically select the certificate store based on the type of certificate.</p></div>	<div data-bbox="655 1059 1385 1767" data-label="Form"><div><div>←</div><div>Certificate Import Wizard</div><div>×</div></div><div><div>Certificate Store</div><div>Certificate stores are system areas where certificates are kept.</div></div><div>Windows can automatically select a certificate store, or you can specify a location for the certificate.</div><div><div><input checked="" type="radio"/> Automatically select the certificate store based on the type of certificate</div><div><input type="radio"/> Place all certificates in the following store</div></div><div><div>Certificate store:</div><div><div></div><div>Browse...</div></div></div><div><div>Next</div><div>Cancel</div></div></div>

Install certificate

6. Click the finish button. The certificate will be imported.

←

 Certificate Import Wizard

×

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by the wizard
Content	PFX
File Name	C:\oces3_test-systemcertifikat.p12

<

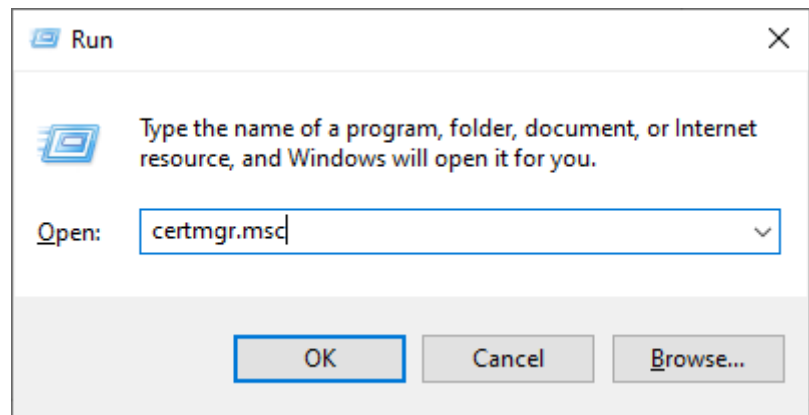
>

Finish

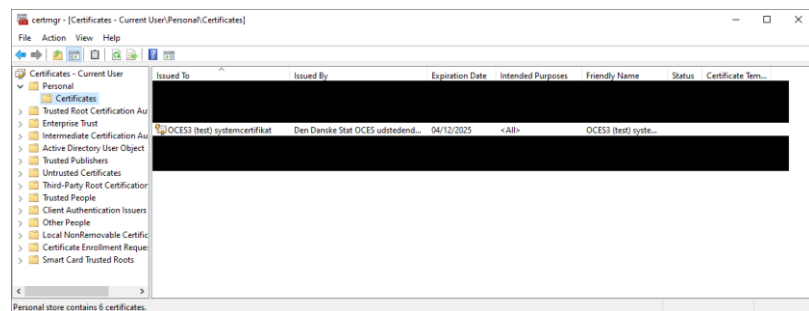
Cancel

Verify installation in Windows certificate manager

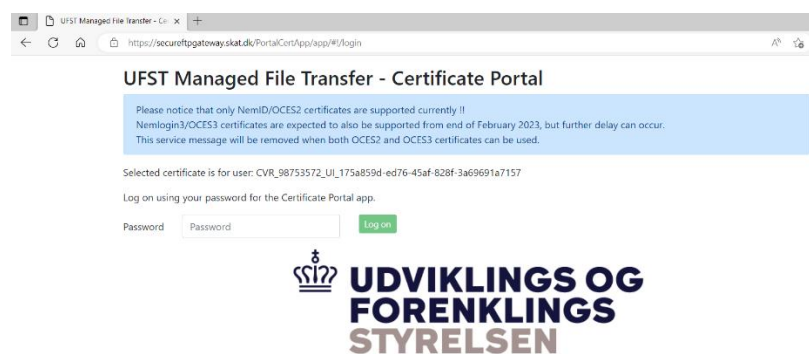
1. Open the Run app (found by searching in the start menu). Open the certificate manager by typing “certmgr.msc” and clicking OK.



2. Locate the certificate. The certificate store and naming of client certificate depends on your client setup.



3. Go to <https://secureftpgatewaytest.skat.dk> in a client with access to certificate



8.1.1 Verifying correct certificate

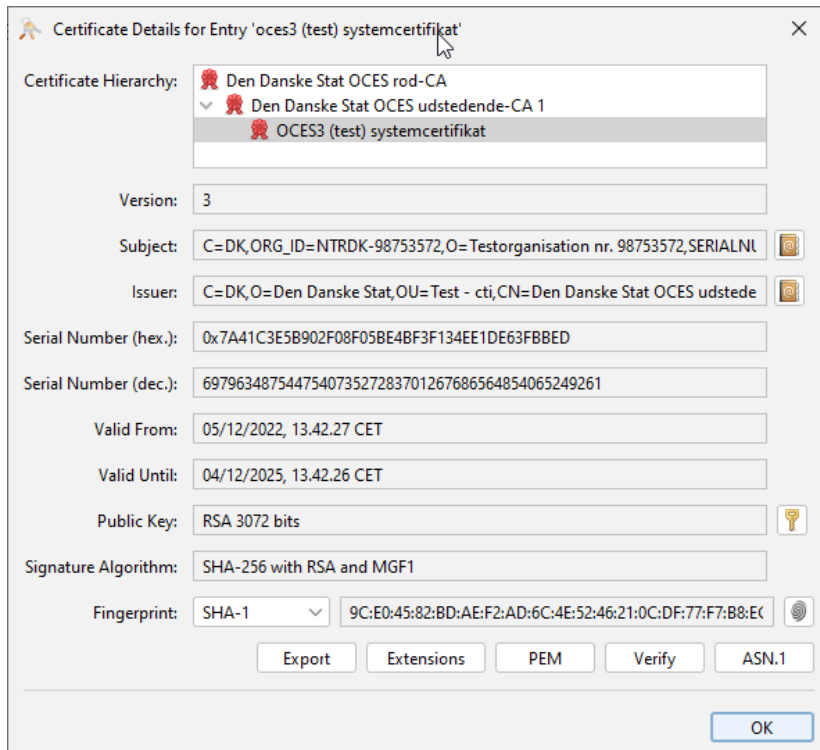
Certificates must be of the OCES format, which contains a unique UUID as well as the CVR or SE-number of the submitting company.

OBS! The CVR or SE-number given in the certificate is not used for any monetary processes, such as processes related to VAT or customs debt. It is a purely technical and identifying CVR to ensure only trusted companies have access.

Verify correct certificate

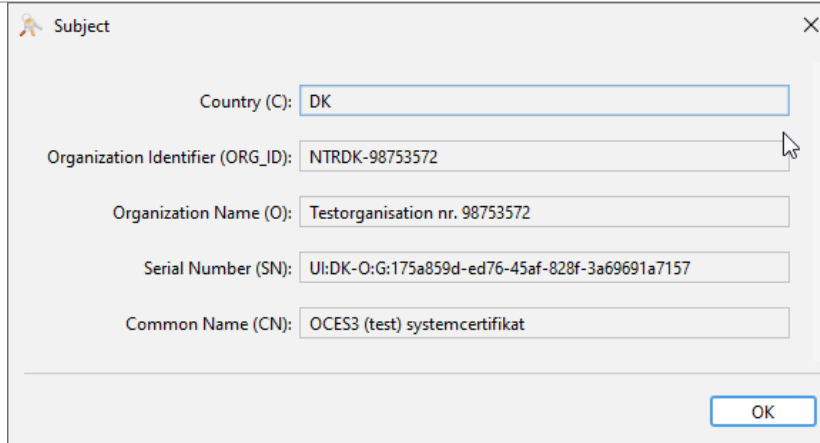
1. Download and install KeyStone Explorer. <http://keystore-explorer.org/>

2. Start KeyStone Explorer and open the certificate by dragging and dropping the relevant jks/pfx/p12 file into the window.



The screenshot shows the 'Certificate Details for Entry 'oces3 (test) systemcertifikat'' window. The 'Certificate Hierarchy' shows 'Den Danske Stat OCES rod-CA' expanded to 'Den Danske Stat OCES udstedende-CA 1', with 'OCES3 (test) systemcertifikat' selected. The details include: Version: 3; Subject: C=DK,ORG_ID=NTRDK-98753572,O=Testorganisation nr. 98753572,SERIALN1; Issuer: C=DK,O=Den Danske Stat,OU=Test - cti,CN=Den Danske Stat OCES udstede; Serial Number (hex.): 0x7A41C3E5B902F08F05BE4BF3F134EE1DE63FBBED; Serial Number (dec.): 697963487544754073527283701267686564854065249261; Valid From: 05/12/2022, 13.42.27 CET; Valid Until: 04/12/2025, 13.42.26 CET; Public Key: RSA 3072 bits; Signature Algorithm: SHA-256 with RSA and MGF1; Fingerprint: SHA-1, 9C:E0:45:82:BD:AE:F2:AD:6C:4E:52:46:21:0C:DF:77:F7:B8:EC. At the bottom are buttons for Export, Extensions, PEM, Verify, ASN.1, and an OK button.

3. Verify that the subject field corresponds to your company.



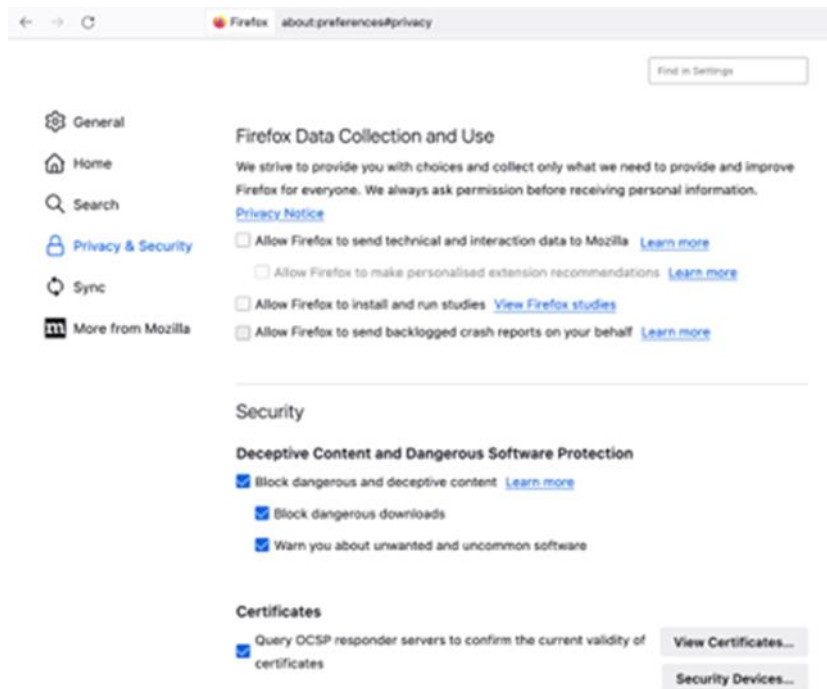
The screenshot shows the 'Subject' field details window. It contains the following information: Country (C): DK; Organization Identifier (ORG_ID): NTRDK-98753572; Organization Name (O): Testorganisation nr. 98753572; Serial Number (SN): UI:DK-O:G:175a859d-ed76-45af-828f-3a69691a7157; Common Name (CN): OCES3 (test) systemcertifikat. An OK button is at the bottom right.

8.1.2 Troubleshooting certificates in the browser

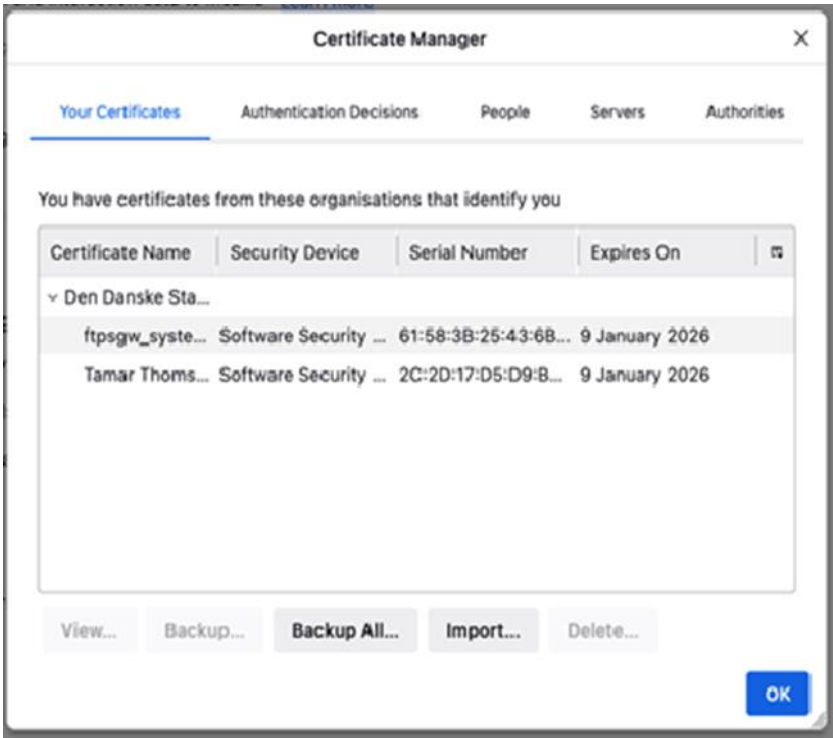
In certain instances, after installing a new certificate, it may not immediately appear in the browser's dropdown list of installed certificates within the certificate portal. To ensure that the newly added certificates are visible in the web browser, it's necessary to clear the links to the old certificates. The following steps demonstrate how to achieve this for various web browsers:

Firefox

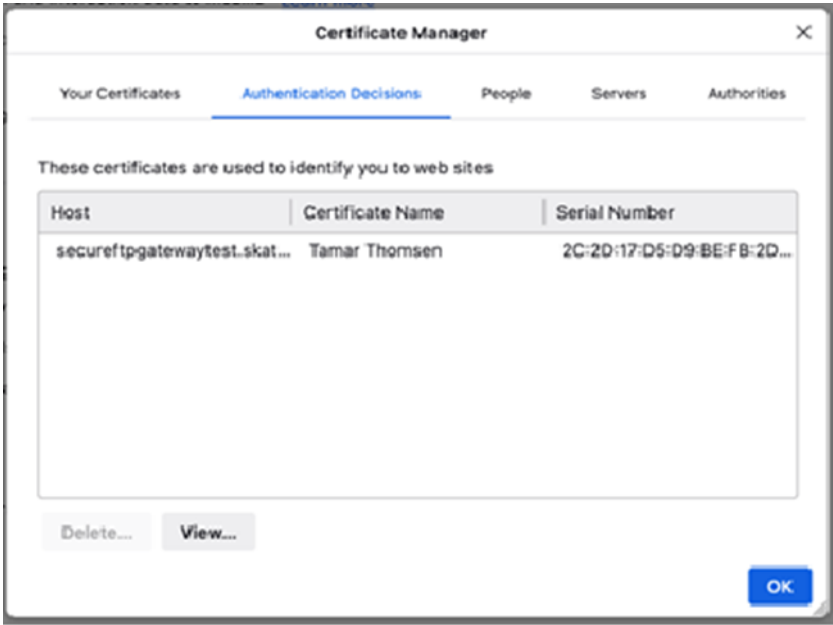
3. Open the browser and find the Settings menu item.
4. Choose **“Privacy & Security”** and go to **“Security”** section.
5. Press the button **“View Certificates.”**



6. In the Certificate Manager window press Import and locate your certificate. It will probably ask for the password for the certificate.

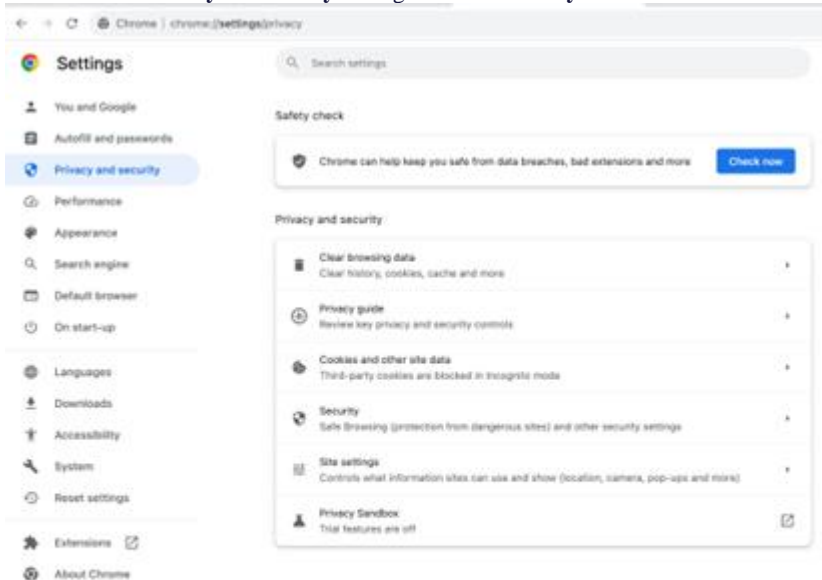


7. Go to the Tab “**Authentication Decisions**” and delete previous entries related to the Certificate Portal URL <https://secureftpgateway.skat.dk> (Production) or <https://secureftpgatewaytest.skat.dk> (TFE). Choose the URL that match the system you want to register either TFE or Production.

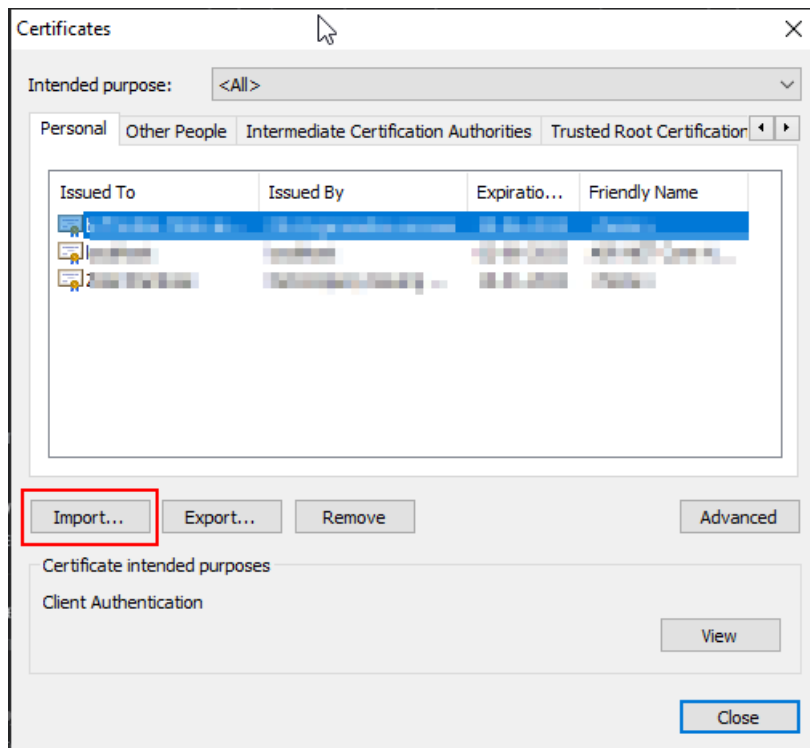


Google Chrome

1. Open the browser and find the Settings menu item.
2. Choose **“Privacy & Security”** and go to the **“Security”** section.

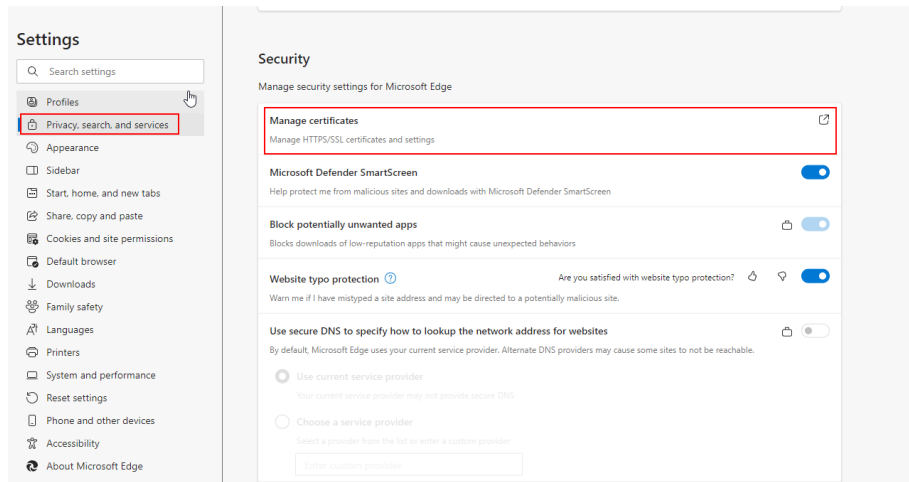


3. Press **“Manage device certificates”** and it will open another window.
4. Press the button **“Import”** to import your certificate. It will probably ask for the certificate password.

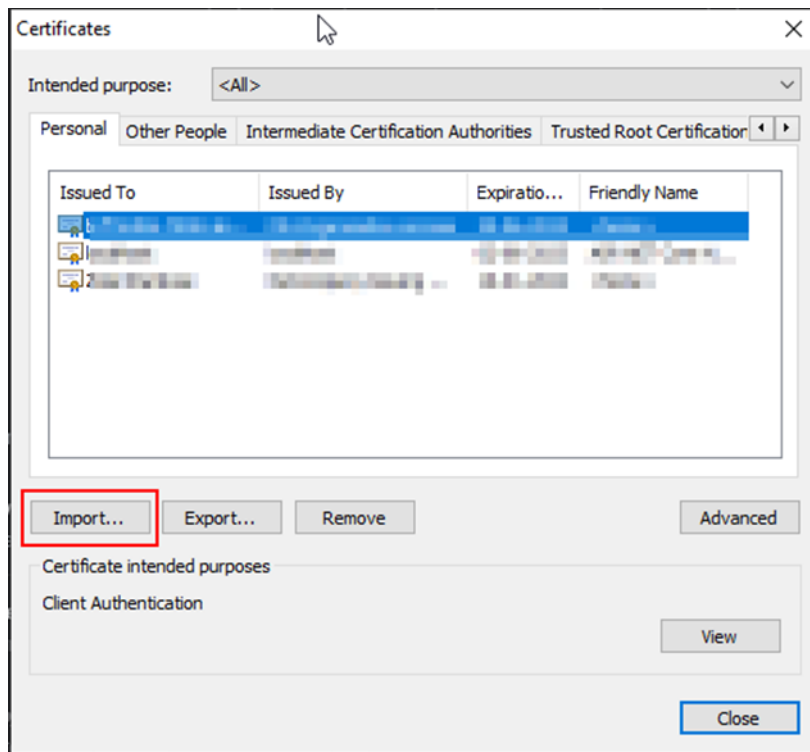


Microsoft Edge

1. Open the browser and find the Settings menu item.
2. Choose **“Privacy, search, and services”** and go to the **“Security”** section.



3. Press **“Manage certificates”** and it will open another window.



4. Press the button **“Import”** to import your certificate. It will probably ask for the certificate password.

8.2 Technical overview of system-to-system

This section provides a brief description of the provided system-to-system solution.

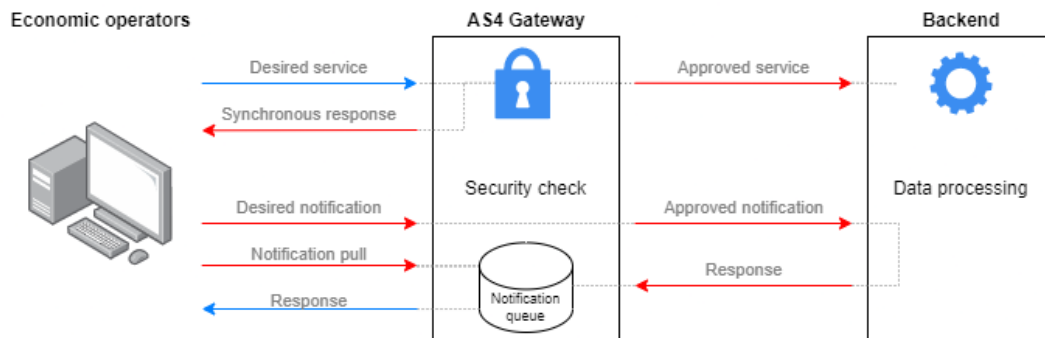


Diagram 1. Overview of services provided by the gateway

All system-to-system operations are performed through the general AS4 gateway, also used for other system-to-system operations within Skatteforvaltningen. Service calls are sent through the AS4 protocol, which is similar in nature to normal SOAP services. AS4 builds upon the technologies within the widespread SOAP landscape, by standardising the exchanged XML formats, describing patterns for push-pull interactivity, and standardising payload signing and encryption. Although AS4 is standardised, some parameters and additional architectural choices have been made to best support the exchange of declaration relevant information. See details on AS4 specific choices in section [6.1](#).

The general flow for interacting with DMS System-to-System is to push a declaration XML to the system, and continually request updates for all declarations, and update when new information arrives. Details on the flow of data as well as an overview of provided notifications can be found in the [DMS System Guide](#) which can be found on Github.

As shown in *Diagram 1*, the gateway exposes multiple services. Most are in an *asynchronous* flow, where the syntax is immediately validated. Further validation steps are performed and reported back via notifications at a later point. All services require the payload to be signed using a OCES certificate. See details on signed payloads in section [6.1.4](#).

8.3 Examples of synchronous answers

8.3.1 Approved messages

The reply contains only a simple code (OK), which means the message is approved and is being handled by the system. To get further information, a notification request should be sent to the gateway. It will then respond with processing notifications from the requested service for the accepted message. See the following examples:

- [Approved message, sample 1](#)
- [Approved message, sample 2](#)

8.3.2 Unapproved messages

In this case, the gateway synchronously responds with all detected XML schema validation errors. See the following examples:

- [Unapproved message, sample 1](#)
- [Unapproved message, sample 2](#)

8.4 Error resolution

This section contains the most common errors that have been reported by partners or observed internally when setting up a connection to DMS.

8.5 DMS fails to authenticate user

Here is a list of possible reasons that DMS fails to authenticate a user:

Failure: EBMS:0004 - Other - Unable to identify Party specified by From PartyId element(s).

- Initiator Party ID is wrong

Failure: EBMS:0004 - Other - Error in getting password for user [USERNAME]. User, password, or policy is not valid or has expired or has been disabled.

- Username is wrong
- Password is wrong

Message failed to send, no Pmode found for message

- Signing Keystore Password is wrong
- Signing KeyReference Method is wrong.
- Keystore Alias is wrong.

Failure: EBMS:0004 - Other - Unable to identify Party specified by To PartyId element(s).

- Responder Party ID is wrong

Message doesn't show up in DMS

- Protocol URL is wrong

Failure: "[ROUTING ID]" is an unknown routing id.

- Routing ID is wrong, right now the standard routing ID is: "DMS.Import.Declaration.Submit"
 - Service is "DMS.Import"
 - Action is "Declaration.Submit"

