

Connectivity Guide



Establish connection to AS4 Gateway

Table of Contents

Introduction	3
Checklist for establishing connectivity	4
1. Get approved to use DMS system	5
1.1 Get approved to use DMS system	6
1.1.1 UI Access	6
1.1.2 System to System access	6
2. Acquire VOCES Certificate	8
2.1 Acquire VOCES certificate	9
2.1.1 Setup of certificate for usage towards DMS	9
2.1.2 Acquire username and password needed for the AS4 header	9
2.1.3 Acquire S2S password	11
3. Acquire Server Certificate	12
3.1 Acquire Server Certificate	13
3.1.1 Verifying network access	13
3.1.2 Verifying correct certificate	18
4. Register Client Certificate	20
4.1 Register Client Certificate	21
5. System to System Server details	24
5.1 System to System Server details	25
5.1.1 AS4 End Point	25
6. Setting up Roles for System User	26
6.1 Setting up Roles for System User	27
7. Verify AS4 setup	28
7.1 Verify AS4 setup	29
7.1.1 AS4 Header	30
7.1.2 AS4 Services	32
7.1.3 Submitter	33
7.1.4 Security	33
7.1.5 Complete AS4 Payload Samples	33
8. Using the Simple AS4 Client made by SKAT	35
8.1 Using the Simple AS4 Client made by SKAT	36
9. Appendices	37
9.1 System to System – Technical overview	38
9.2 Synchronous answers example	38
9.2.1 Approved message	38
9.2.2 Unapproved message	39
9.3 Error resolution	39
9.4 DMS Fails to Authenticate User	39

9.5 Certificate Errors..... 39

Introduction

This document describes in overall details how to establish access to the AS4 Gateway for delivering files to the new Import declaration system - Toldsys-temet.

The document describes server details, and tests steps to confirm a working connection towards the system. The system accepts messages following the AS4 standard. This document describes the general aspects of AS4, the needed AS4-header, security, and attachment setup. Eventually follows common errors, and their resolution

Checklist for establishing connectivity

This Guide is structured to follow the steps below in order to have a fully established connectivity to the AS4 Gateway. Be sure to successfully test and pass a step before you move on to the next step.

Step	Description
1	Get approval to use DMS system
2	Acquire VOCES Certificate
3	Acquire Server Certificate
4	Register Client Certificate
5	System to System Server details
6	Setting up Roles for System user
7	Verify AS4 setup

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 10.

**Get approved to use DMS
system**

1

1.1 Get approved to use DMS system

The DMS Import and Export system is accessible through two primary channels. Either

1. through the User Interface (UI)
2. through the system-to-system interface (S2S).

Either option requires you have filled out, submitted application for, and obtained approval for access to the system. Access grant to DMS can be obtained by following the process described on <https://skat.dk/skat.aspx?oid=2305068>.

Once the above mentioned application has been approved, your company's NemID administrator has the ability to assign access for either employees for UI access, or for your system user for S2S access through Tastselv Erhverv. <https://www.tastselv.skat.dk/>

Details on how those access/roles are assigned can be found here:

<https://github.com/skat/dms-public/raw/master/dokumenter/VejledningRollerTilTP.docx>

1.1.1 UI Access

TastSelv features the ability to grant UI access to the test system, Test for Erhverv (TFE). Many companies with S2S access also have access to the UI in order to use its search feature and to check declaration statuses. When granted, users can login without further setup on the following addresses:

Test environment (TFE)	https://tfe.toldsystemet.toldst.dk/swp.trader.customs
Production environment	https://toldsystemet.toldst.dk/swp.trader.customs

1.1.2 System to System access

System to System (S2S) accesses are most suitable for companies with a high volume of declarations. Access requires a valid VOCES certificate issued NETS and a working AS4 client. This guide has multiple sections on how certificates are obtained and managed, as well as details on how AS4 is setup.

Shortly summarized, **Udviklings- og Forenklingsstyrelsen (UFST), Toldstyrelsen (TOLDST) or SKAT do not possess the ability to issue or locate the relevant VOCES certificate**. This is entirely delegated to either the NemID responsible within the company or to the maintainers of the company's IT solution. This guide can therefore not provide details on how to locate the relevant certificate as it entirely depends on who is NemID responsible, and possibly whether and where a certificate has been used before. Most S2S solutions within SKAT require a VOCES, so most likely the correct VOCES can be located within one of the running solutions. The following systems within SKAT are known to require VOCES authentication:

- eKapital
- Offentlig Inddrivelse (PSRM)
- Told Manifest
- Told ICS
- Moms via accounting software: <https://skat.dk/skat.aspx?oid=2234574>

Please refer to the above checklist in Section 2: *Checklist for establishing connectivity* for an index of detailed description of the steps that is needed to follow in order to establish connectivity.

Acquire VOCES Certificate

2

2.1 Acquire VOCES certificate

As UFST/TOLDST or SKAT do not possess the ability to issue or locate the relevant VOCES certificate, this guide will not provide details on this. This is delegated to the NemID responsible within the company. If all fails in locating an existing certificate, a new can be issued within NETS: https://www.medarbejdersignatur.dk/produkter/nemid_medarbejdersignatur/nemid_selvbetjening/oevrige_signaturer/virksomhedssignatur/bestil_virksomhedssignatur.

This should be considered a last resort, since this will invalidate the existing certificate and break already functional integrations towards SKAT.

2.1.1 Setup of certificate for usage towards DMS

To setup certificates for usage towards DMS, the following must be completed:

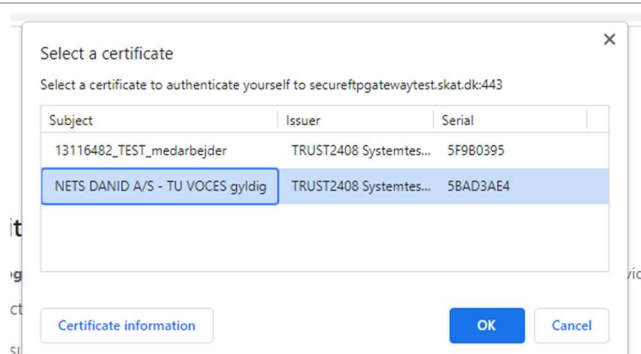
- 1) Register certificate within the gateway solution. See Section [4 Register Client Certificate](#) for details.
- 2) Configure your client to use certificate. This entails placing the certificate on a server/filesystem the client has access to and setting up the software to access the certificate with a correct password. Details for this depends entirely on the used software, and the software vendor can provide details on how to perform this step.

2.1.2 Acquire username and password needed for the AS4 header

Access the Gateway portal through:

Environment	Hostname
Test/TFE	https://secureftpgatewaytest.skat.dk
Prod	https://secureftpgateway.skat.dk

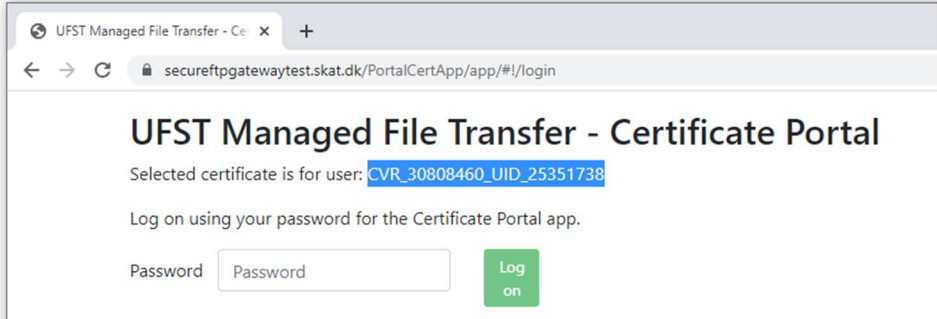
1) When entering these sites, you should be prompted to select a certificate.



<p>2) Select the one that is a valid VOCES certificate. This is determinable via the Certificate Information Button in Chrome.</p>	
<p>3) Certificate Properties in IE.</p> <p>Login with credentials. See below for default credentials.</p>	
<p>4) Once in, you must copy the password listed under Gateway password.</p>	

2.1.3 Acquire S2S password

If you don't have the password for the certificate portal.

<p>The default is the username listed upon the login page. In this example, the password is CVR_30808460_UID_25351738.</p>	
--	--

Acquire Server Certificate

3

3.1 Acquire Server Certificate

The following sections are not a step by step guide, but rather a reference guide that an implementer can use to lookup details and successfully implement an integrated solution.

3.1.1 Verifying network access

The following section describes various tools and methods for verifying connectivity from the client towards the DMS S2S solution. Availability of tools on the client setup will determine the method for testing

3.1.1.1 Unix

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

Method #1 – telnet

```
telnet <Hostname> 6384
```

Example:

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

Method #2 – nmap

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

Example:

```
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
```

Example:

```
rj9t470PWU68Rr: $ 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 Øe, O = Skatteforvaltningen, CN = secureftpgatewaytest.skat.dk  
verify return:1  
139743226499712:error:14094410:SSL routines:ssl_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 Øe, O = Skatteforvaltningen, CN = secureftpgatewaytest.skat.dk  
   1:C = BE, O = GlobalSign nv-sa, CN = GlobalSign RSA OV SSL CA 2018  
-----BEGIN CERTIFICATE-----  
MIIGGqJCcBZKgaWIBAgIMdnhIlnSQQOENYGMVAOGCSQgSIb3DQEBCwUA MFaxCzAJBgNVBAYTAkFRMRkwFwYDVQQKEXBhbG91YmVtaWRudGVzZXNhdnVndydzLXNldHJlcHRucyMxMDAwMTA1OTcwODExLnVxwTAdUFIJTGF3BPBVBU0uWGQGegqEgJAxoDAEAFew0XTotMTMOXIzdMaHFawByMJAXMQdxMQDEAsMZAMHBxCzAJBgNVBAYTAklRMRRMEQYDVQDEWEpDB3Blbmhhf2ZVuMRywFAFYDVQQHEHDb3Blbmhhf2ZVUEI9EIHMwwGUVDOVKXEKXntA2FdgdGmb3J2YWVsbnluZWVMSUJwInVyDVQQDESxxZWNIcmVmMHBNXRllIDZF5dGVzcDIzMzaFlmrMRIIBIJANBgkqhkiG9w0BAQEFAAACOA8AMIIBCgCAEQASxOnplZ6SJN9VAP1PJdJK9AGSB/PVPVynwsBFReb6KRqQA8NA7LXqeIt+qvgho4+wHAhg=qUSQB07TFYSIRBRDepIF8CBTZag/Cjypbz+xODFXzy2jyoQgeDVOl2GNpfcto/O/HCF9ZNwkIAxdke7wtShmyZmauoG3w0iddqsJFOQSkuendoggs+zjb1+clPcfaggzhIH8nzgeioFRZRryglVPISEUT/YztzvowSDltqr-fhzahFs5fhzpRItpZYngSKTK68PAAR-nMSTLoPdAQABggGECEPT-Ifxz7AEysvBfywRB0Co7YSH5SiAIIUDatcp0AESIQfnhaKSwIDAAQABADIUCCIACCA8NhdyVR0Rpqa/BACQAgkgHG0GBgrgnBEFFRoBaQS8gtB/MEOGCCsgGAOUFBzAcchJhedRWoi8vc2vjDXJJmdsbz2bhHpzz2AuY29LI2NHyz2lydc9nc33=Yv92cz3Ny2YeYMdeALmltyda3bggerBFQCwaYYrahlROcdovLL29icz3AuZZcxYmfsc21nbis5jb2bvZH3yc2FvdnlznBGniHfAxODBWgbGWLSAEST-BNMIEEGCsGaQSY0DiBFDADMNDIOGCCGsGaBYBTfiZodHRwczoVL3dd3y5nbG91YmxzaWduMLNBvaQ9YZXBvc2lob3J5SLZA7BgZngOWBagTWCOVDVR8TBAtWA/BgnVNRHREODAZMDSgmGAWhi5pd4RWoi8vyZ3slmgdsbt2bbHNznZ2AUvZ9T1tdzcrnNbHzrrzsvITVMtlpjY3Is
```

3.1.1.2 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.skat.dk -Port 6384

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

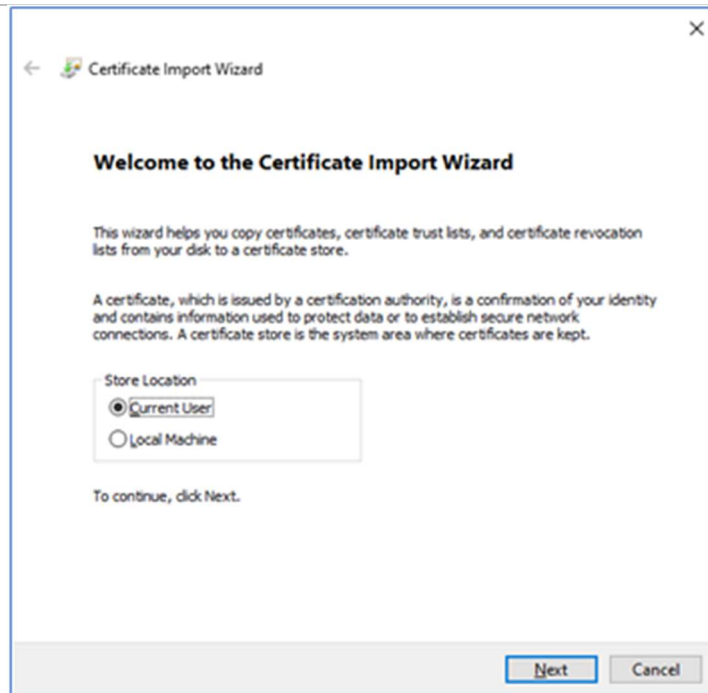
Method #2 – Browser

Requires valid VOCES (or similar trusted client certificate in testing clients truststore). Installation of client certificate on client PC:

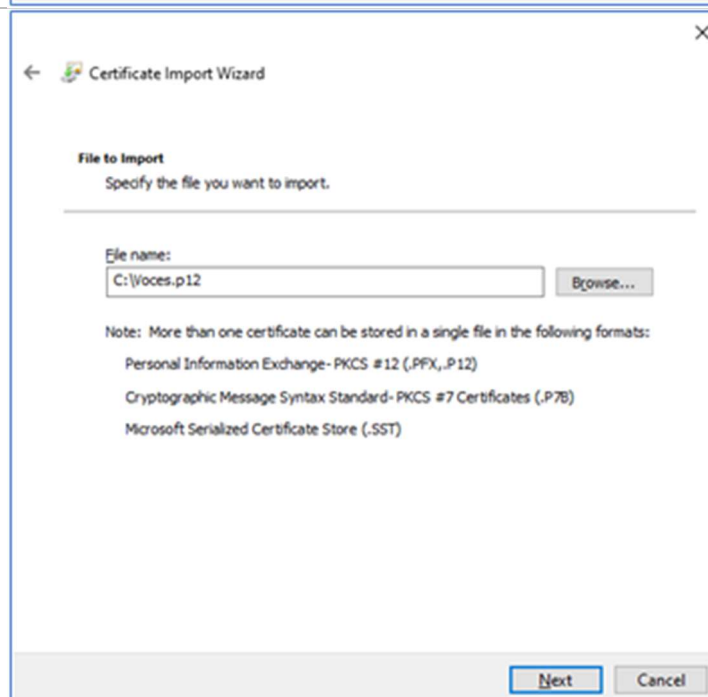
Install the certificate	
1) Locate suitable certificate.	See details section 2.

Install the certificate

2) Install certificate in truststore – if access is allowed, double-click the pfx/p12 file and see this menu.

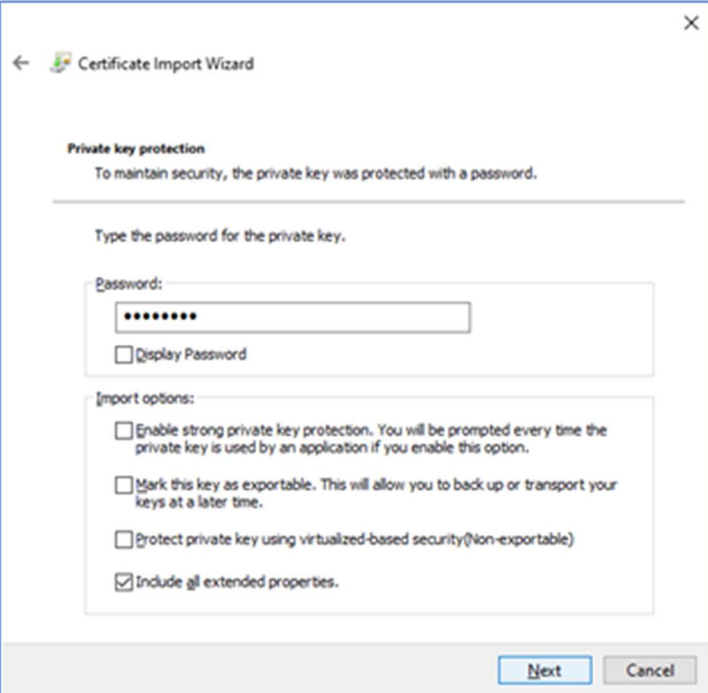


3) Select the VOCES certificate.



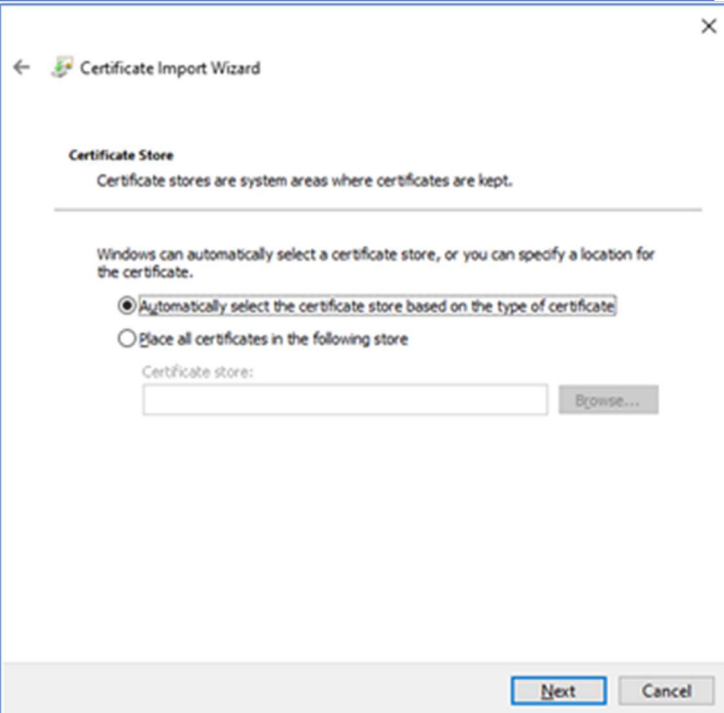
Install the certificate

4) Fill out the password and check off 'Include all extended properties'.



The screenshot shows the 'Certificate Import Wizard' window, step 4. The title bar says 'Certificate Import Wizard'. The main heading is 'Private key protection'. Below it, a message states: 'To maintain security, the private key was protected with a password.' A horizontal line separates this from the next section. The text 'Type the password for the private key.' is followed by a 'Password:' label and a text box containing eight dots. Below the text box is a checkbox labeled 'Display Password'. Another horizontal line separates this from the 'Import options:' section. This section contains four checkboxes: 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.', 'Mark this key as exportable. This will allow you to back up or transport your keys at a later time.', 'Protect private key using virtualized-based security (non-exportable)', and 'Include all extended properties.' The last checkbox is checked. At the bottom right are 'Next' and 'Cancel' buttons.

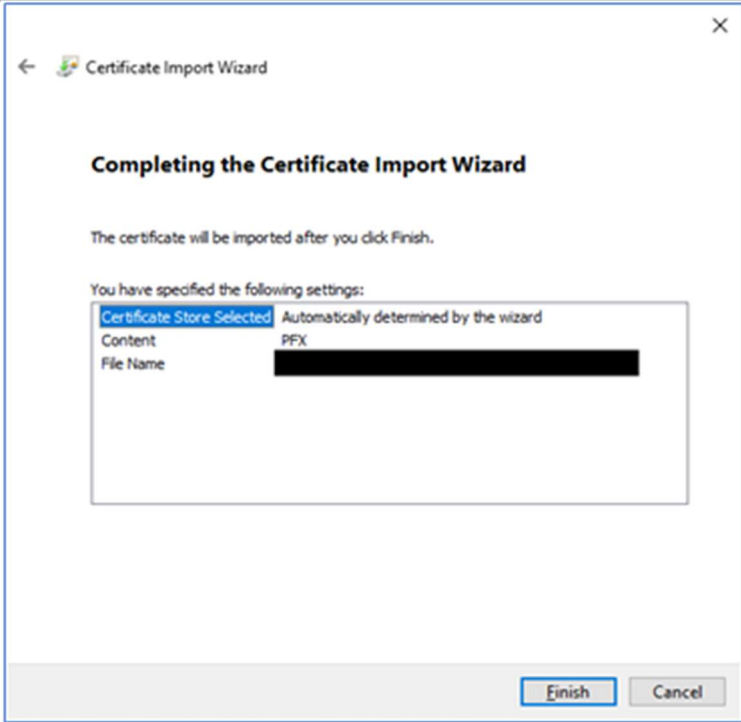
5) Choose to automatically select the certificate store based on the type of certificate.



The screenshot shows the 'Certificate Import Wizard' window, step 5. The title bar says 'Certificate Import Wizard'. The main heading is 'Certificate Store'. Below it, a message states: 'Certificate stores are system areas where certificates are kept.' A horizontal line separates this from the next section. The text 'Windows can automatically select a certificate store, or you can specify a location for the certificate.' is followed by two radio button options: 'Automatically select the certificate store based on the type of certificate' (which is selected) and 'Place all certificates in the following store'. Below the second option is a 'Certificate store:' text box and a 'Browse...' button. At the bottom right are 'Next' and 'Cancel' buttons.

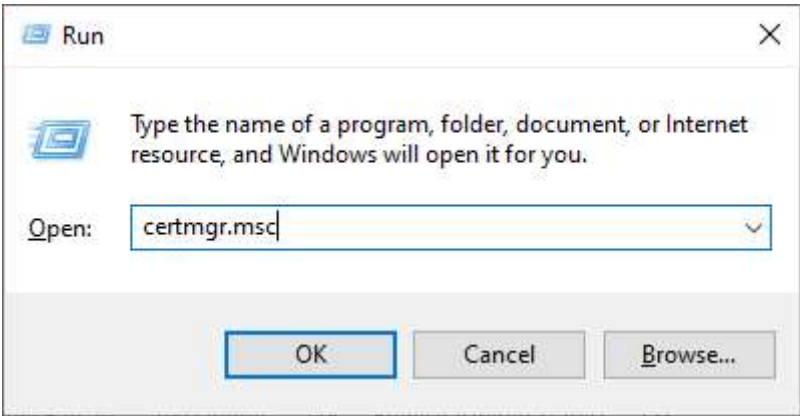
Install the certificate

6) Click 'Finish' and the certificate will be imported.

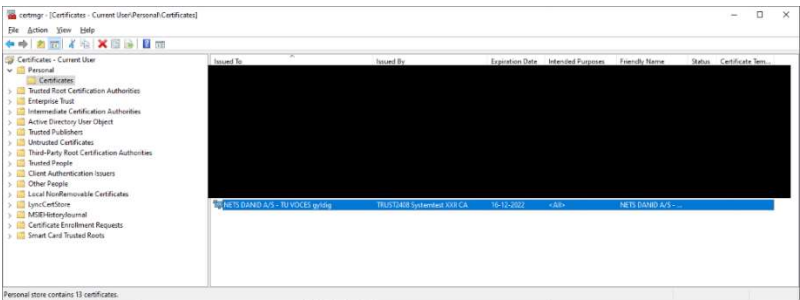


Verify installation in Windows Certificate manager

1) Open Certificate Manager.

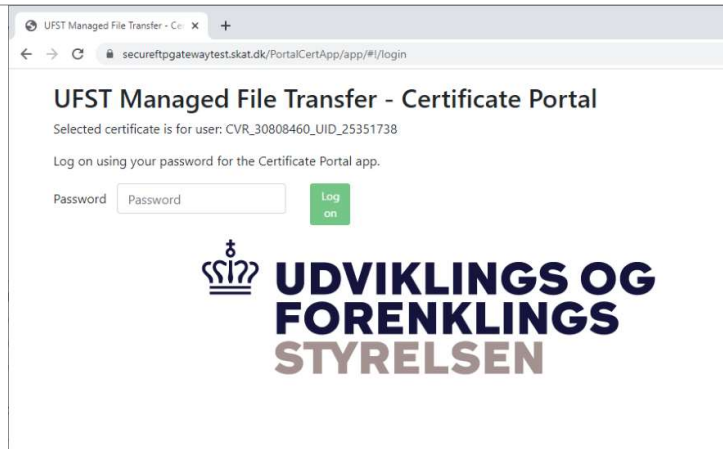


2) Locate certificate.
Certificate Store and naming of client certificate depends on client setup.



Verify installation in Windows Certificate manager

3) Open <https://secureftpgateway.skat.dk> in favourite browser that has access to the internet - on a client setup that the internal network is setup as the accessing system:



3.1.2 Verifying correct certificate

Certificates must be of the VOCES format, which contains a unique UID as well as the CVR/SE-number of the submitting company.

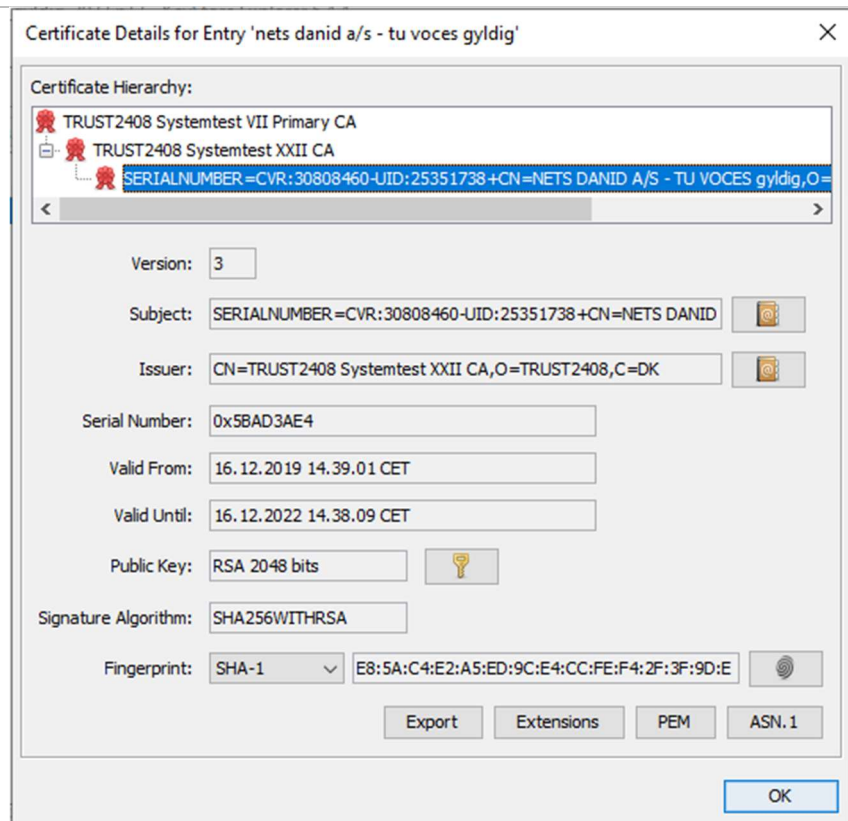
Importantly, the CVR/SE-number given in the certificate is not used for any monetary processes, especially for processes related to VAT or customs debt. It is a purely technical and identifying CVR to ensure only trusted companies have access.

Verify if the certificate is correct by following these steps:

Verify correct certificate

1) Download KeyStone Explorer

2) Open certificate by drag-and-dropping in the relevant jks/pfx/p12 file and verify it is of structure.

Verify correct certificate

3) Verify the bottom node is of the format:

SERIALNUMBER=CVR:xxxxx-UID:yyyyy+zzzz

Register Client Certificate

4

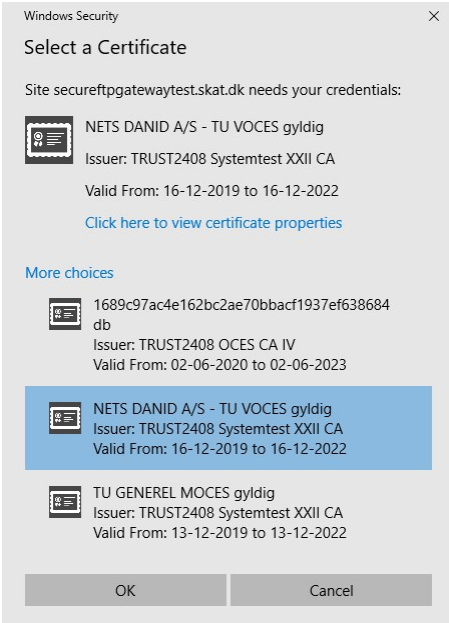
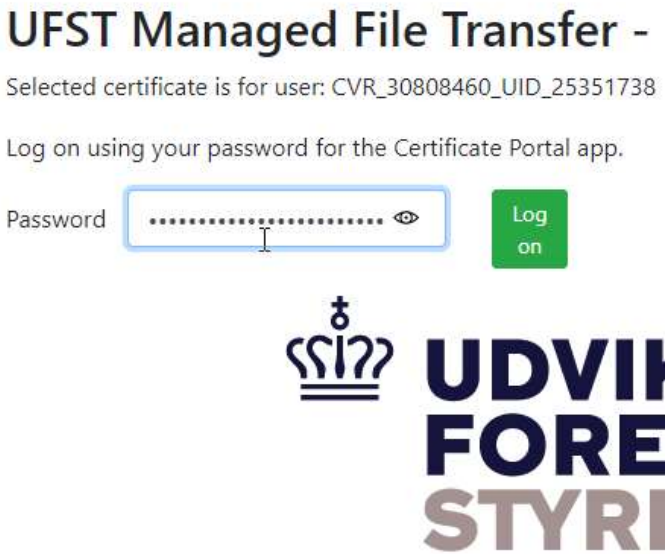
4.1 Register Client Certificate

The Certificate Portal provides self-service for pre-registration of certificates.

TFE: <https://secureftpgatewaytest.skat.dk>

PROD: <https://secureftpgateway.skat.dk>

You are required to use the same certificate as you would use for the FTPS Gateway.

Registering certificate for S2S usage	
<p>1) In this example, you can select from the certificates which have been imported to the browser.</p> <p>Here we select a NETS test certificate and enter the login page of the Certificate Portal.</p>	
<p>2) The CVR and UID/RID information is extracted from the certificate and you are identified as user: CVR_30808460_UID_25351738.</p> <p>Important: The first time you logon the default password <u>is your user identification</u>, and you may thus simply copy/paste and proceed with logon.</p>	

3) The first time you login you are requested to change password. You may use the passphrase for your certificate or any other password, which will thus be required for subsequently logon.

Change password

You must change the default password!

Current password

New password

Confirm password 

Change password

Cancel

In the example below, the Self Service Portal has no previous knowledge of this certificate and would reject any logon attempt. This means that you must choose to “Register Certificate”

UFST Managed File Transfer - Certificate/User overview

Your certificate is not registered in UFST MFT. Press 'Register Certificate' in order to update the certificate in UFST MFT.

Common name CVR:30808460-UID:79909515

Expiry date 16-12-2022

Type CVR

E-mail tu-support@danid.dk

Legal identifier CVR_30808460

Account UID_79909515

Register
certificate

Refresh

The registration process will be initiated and should be completed within a few minutes. Use the “Refresh” to verify when the registration has been completed.

Account UID_79909515

Register
certificate



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.

Refresh

The certificate is now registered, and you view both your username and assigned password which you should record for setup of your AS4 session.

UFST Managed File Transfer - Certificate/User overview

Your certificate is registered and ready for use.

Common name	TU GENEREL MOCES gyldig	
Expiry date	13-12-2022	
Type	CVR	
Legal identifier	CVR_30808460	
Account	RID_45490598	
E-mail	<input type="text" value="do-not-write@skat.dk"/>	Update e-mail
Interfaces	<input checked="" type="checkbox"/> FTPS <input type="checkbox"/> AS4 	Update interfaces
Gateway user	CVR_30808460_RID_45490598	
Gateway password	***** 	

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.

Note: It is important that you checkmark the AS4 part in the interface section and click Update interfaces.

Finish by selecting "Log out". The FTPS Gateway login will be established within 15 minutes from your pre-registration, and you are then ready to upload to the services you have access to (verified with your DCS roles for certificate).

System to System Server details

5

5.1 System to System Server details

Environment	Hostname	Port	IP
Test/TFE	secureftpgatewaytest.skat.dk	6384	195.85.251.58
Prod	secureftpgateway.skat.dk	6384	195.85.251.102

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

Important note: SKAT cannot help with opening the correct ports for access. Ensure access to the nonstandard ports, in due time, with your maintenance vendor.

As far as possible, the client needs to resolve the hostname on suitable nameserver. The IP listed above is the currently active IP at the time of writing. The given IP is suitable for change.

5.1.1 AS4 End Point

The endpoint used depends on the CVR/EORI and UID of the client certificate, the format is described below.

5.1.1.1 VOCES CVR Users:

https://<hostname>:6384/exchange/CVR_<CVR>_UID_<UID>

Example:

https://secureftpgateway.skat.dk:6384/exchange/CVR_30808460_UID_25351738

5.1.1.2 EORI Users

https://<hostname>:6384/exchange/EORI_<EORI>_RID_<RID>

Example:

https://secureftpgateway.skat.dk:6384/exchange/EORI_SE4445462718_RID_1391404656315

Setting up Roles for System User

6

6.1 Setting up Roles for System User

In order to use Toldsystemet you must have the correct role and rights. It is the company's NemID administrator who can assign roles and rights to you as an employee. Please find the necessary information in this Guide: [Veiledning roller](#).

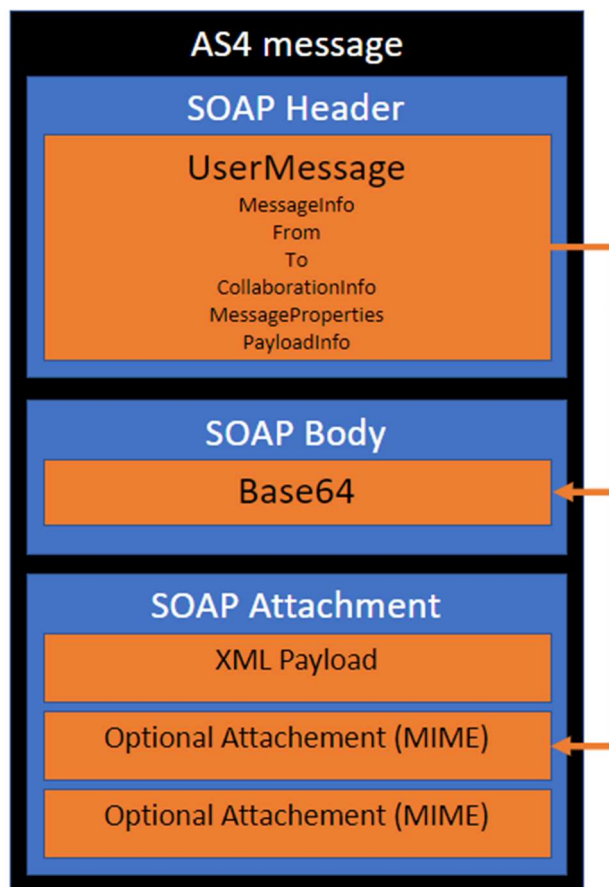
Verify AS4 setup

7

7.1 Verify AS4 setup

AS4 is a standard describing various fields related to the message transfer – described in a header. AS4 furthermore standardizes 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. These settings require manual setup to define the following:

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



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 UFST 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 set to be delivered in the soap-body. The message structure is shown here below:

The soap attachments are planned for usage for amendments in a later release – and will not be tested as part of the testcases described here.

7.1.1 AS4 H7 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 an H7 declaration.

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>_UID_<UID>	d4872030-3862-4e7b-9754-17a98523e826@CVR_30808460_UID_25351738
PartyInfo.From.PartyId	CVR_<CVR>_UID_<UID>_AS4	CVR_30808460_UID_25351738_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
PartyInfo.To.Role	AS4 Initiator 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]	ProcedureType	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-e1b845277dd9">
  <eb3:UserMessage>
    <eb3:MessageInfo>
      <eb3:Timestamp>2021-01-19T15:24:37.376Z</eb3:Timestamp>
      <eb3:MessageId>d4872030-3862-4e7b-9754-17a98523e826@CVR_30808460_UID_25351738</eb3:MessageId>
    </eb3:MessageInfo>
    <eb3:PartyInfo>
      <eb3:From>
        <eb3:PartyId type="string">CVR_30808460_UID_25351738_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.Import</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>
```

7.1.2 AS4 Notification Pull Request Header

This section contains information about what information should be contained in the AS4 header for pulling a notification from a Message Partition Channel (MPC).

The following attributes must be provided:

Attribute	Value	Example
MessageInfo.Timestamp	YYYY-MM-DDTHH:MI:ss.SSSZ	2021-01-19T15:24:37.376Z
MessageInfo.MessageId	GUID@CVR_<CVR>_UID_<UID>	4874bbf7-33c0-49cb-8b98-ca399fccf34a@skdev00ftpsx.dmz23.local
PullRequest.Property[mpc]	Message Partition Channel	urn:fdc:dk.skate.mft.DMS/import2/response

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

```
<eb3:Messaging xmlns:eb3="http://docs.oasis-open.org/ebxml-
msg/ebms/v3.0/ns/core/200704/" xmlns:mustUnder-
stand="http://www.w3.org/2003/05/soap-envelope" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" mustUnder-
stand:mustUnderstand="true" wsu:Id="id-4b28503707cbf61-71e4-43e6-9082-
44ff51d30921">
  <eb3:SignalMessage>
    <eb3:MessageInfo>
      <eb3:Timestamp>2022-02-04T05:09:48.099Z</eb3:Timestamp>
      <eb3:MessageId>4874bbf7-33c0-49cb-8b98-ca399fccf34a@skdev00ftpsx.dmz23.lo-
cal</eb3:MessageId>
    </eb3:MessageInfo>
    <eb3:PullRequest mpc="urn:fdc:dk.skate.mft.DMS/import2/response"/>
  </eb3:SignalMessage>
</eb3:Messaging>
```

7.1.3 AS4 Services

The following section describes the available services provided by AS4. The parameters MessageProperties[procedureType] and Service.Action in the AS4 header allows setting of which service the AS4 message is destined for. The parameters given ensures correct and immediate payload XML Schema validation, as well as ensuring the correct internal flow for processing the file is started upon receipt.

BusinessService	Internal schema and processing engine
DMS.Import2.Declaration.Submit	A create declaration (for now only H7)
DMS.Import2.Declaration.Amend	An amendment for a declaration
DMS.Import2.Declaration.Amend.Goodspresented	I2 declaration message (Only for selected clients)

DMS.Import2.Declaration.Invalidate	Invalidation message
DMS.Import2.Declaration.InvalidateRemissionRepayment	Invalidation and repayment message
DMS.Import2.Notification	Retrieve the latest notifications.

7.1.4 Submitter

In every call to Axway a submitter needs to be filled out in the payload, or in the AS4 header, for all companies the submitter name will be the numbers in their CVR / EORI number, for example, if a company has the following CVR: CVR_ **30808460** then the submitter name will be **30808460**, and will look like this in the payload:

```
<ns2:Submitter>
  <ns2:Name>30808460</ns2:Name>
</ns2:Submitter>
```

7.1.5 Security

The following webpage describes detailed the security aspects about AS4: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery+AS4+-+1.14#eDeliveryAS4-1.14-Security>

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

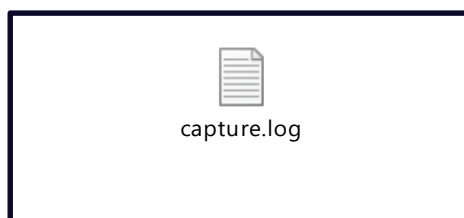
- Body
- Messaging
- cid:Attachments

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

The solution does **not(!)** use encryption for the XML messages..

7.1.6 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:



DoubleClick to open the file

Using the Simple AS4 Client made by SKAT



8.1 Using the Simple AS4 Client made by SKAT

During earlier onboarding we observed **significant** difficulty with creating AS4 communication programming therefore a simple to use package was commissioned.

The goal of this package is to make it faster to onboard new economical operators and those who provides services to economical operators.

A Java based simple AS4 client has been developed which is available here: <https://github.com/skat/simple-as4-client>. This link also contains further references to the documentation, and advice for implementation.

This package aims to make it simple to create a client which can communicate with the AS4 portal and through it the DMS import system, as it handles 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 Axway
- Receiving replies from Axway

The package is written in Java, and provided as Java dependency. Therefore integration with .NET based projects will be less 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

9

9.1 System to System – Technical overview

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

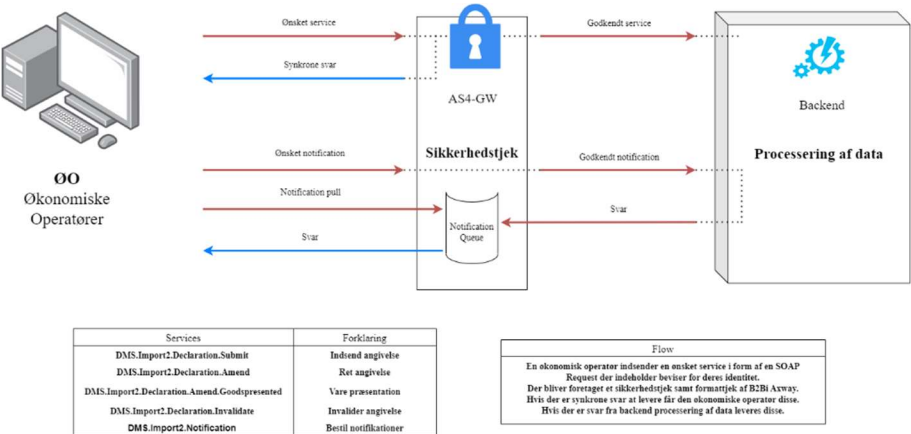


Diagram 1 – Overview of services provided by the gateway

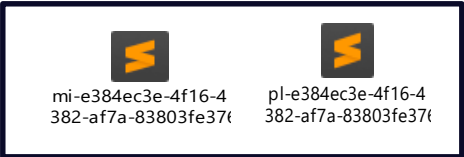
All S2S operations are performed through the general SKAT gateway, also used for other S2S operations. Service calls are sent through the AS4 protocol, which is similar in nature to normal SOAP services. AS4 builds upon the technologies within the widespread SOAP landscape, by standardizing the exchanged XML-formats, describing patterns for PUSH/PULL interactivity, and standardizing payload signing and encryption. Even though AS4 is standardized, 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 7.1](#).

The general flow for interacting with DMS is to push a declaration XML towards the system, and continually request updates for all declarations, and update when new information arrives. Details on the flow of data is described in the [Onboardingguide](#), and an overview of provided notifications can be seen the [Import Systemguide](#). As shown in Diagram 1, the gateway exposes multiple services, most are in an “asynchronous” flow, where an immediate syntax validation is provided, and deeper validation steps are performed upon the declaration, and delivered via notifications at a later point. All services require a signed payload, where the signing must be performed using a VOCES certificate. See details on signed payloads in [Section 7.1.6](#).

9.2 Synchronous answers example

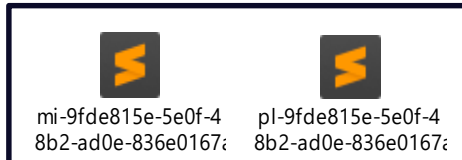
9.2.1 Approved message

This set of replies is for an approved message, this reply only contains a simple code (OK) which means that the message is approved and is currently being handled by the system. For further information a notification request should be sent to the gateway which will then respond with processing notifications from the requested service for the accepted message.



9.2.2 Unapproved message

This set of answers are for an unapproved message, in this case the reply contains information about the semantic mistakes that the gateway detected in the message. The gateway synchronously responds with all detected XML schema validation errors.



9.3 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, with the goal of streamlining the setup as much as possible.

9.4 DMS Fails to Authenticate User

Here is a possible list of reasons this could have happened:

- 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"

9.5 Certificate Errors

These errors were obtained while trying to get a certificate from the [test certificate portal](#):

- "The supplied certificate is not a valid certificate" when accessing certificate portal
 - The certificate is wrong, make sure you are using the correct VOCES certificate.

- “Login failed - verify that your password is correct”
 - Certificate password for VOCES certificate is wrong, make sure you have the correct certificate password.

