DMS Connectivity Guide

How to establish connection to AS4 gateway

UDVIKLINGS OG FORENKLINGS STYRELSEN

Indholdsfortegnelse

Introduction

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

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 VOCES 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

The 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 following the process described on
https://skat.dk/skat.aspx?oid=2305068 (in Danish).

Acquire VOCES certificate

2

2.1 Acquire VOCES certificate

System-to-system access is especially suitable for companies with a high volume of declarations. Access requires a valid VOCES certificate issued by NETS. Please observe that VOCES certificates issued for the following systems can be reused:

- eKapital
- Offentlig Inddrivelse (PSRM)
- Told Manifest
- Told ICS
- Moms via accounting software: https://skat.dk/skat.aspx?oid=2244392

Please note that you must use the same certificate as on the FTPS gateway.

Please note that neither the IT and Development Agency or the Danish Customs Agency is able to issue or lookup the relevant VOCES certificate. Acquiring and keeping track of certificates is the responsibility of each company and will thus not be covered by this guide. If you cannot locate your existing certificate, a new can be issued by NETS through the following link:

https://www.medarbejdersignatur.dk/produkter/nemid_medarbejdersignatur/nemid_selvbetjening/oevrige_signaturer/virksomhedssignatur/bestil_virksomhedssignatur

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).

2.2 Optional: Acquire MOCES certificate

Alternatively, an individual employee's MOCES certificate could be used instead of a VOCES. However, using MOCES for 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 questions leaves your company.

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.

3.1.1 System user for TFE-environment

For the test environment, TFE, the system user must be created by Udviklings- og Forenklingsstyrelsen. It's 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 UID of the system certificate you wish to use for the AS4 gate-way. The UID can be found by the method described in section 8.1.1.

The process can be illustrated like this:
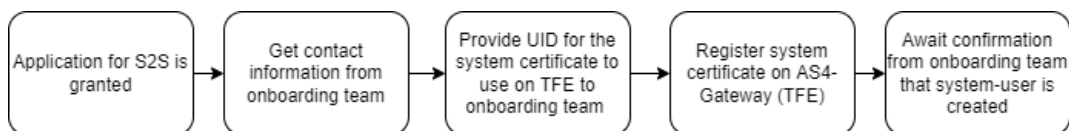
3.1.2 System user for PROD environment

The process for the production environment is almost the same as for the TFE environment, with the difference that your company's NemID administrator (LRA) directly can give DMS Online access to employees and DMS System-to-System access to your system user. This is done via Tastselv Erhverv, https://www.tast-selv.skat.dk/. However, this requires that UFST has given your company the nec-essary roles.

The process can be illustrated like this:
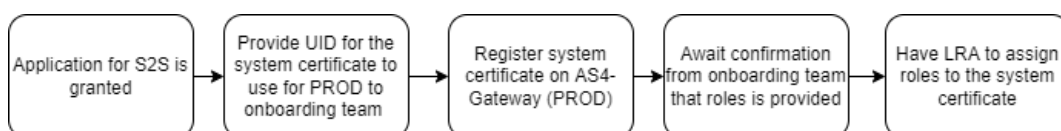
Details on how those roles are assigned to system certificate on Tastselv Erhverv can be found in the document Vejledning til roller i DMS. https://github.com/skat/dms-public/blob/master/Onboarding Docu-ments/VejledningRollerTilTP.pdf

3.1.3 DMS Online access

TastSelv features the ability to grant DMS Online access to the test system, TFE. Companies with DMS System-to-System access can also use the DMS Online to search and check declaration statuses. Users can login on the following ad-dresses:

Test environment (TFE01)	https://tfe.toldsystemet.toldst.dk/swp.trader.customs
Production environment (PROD)	https://toldsystemet.toldst.dk/swp.trader.customs

Your company's LRA can assign roles to the employees that need access to DMS Online via Tastselv Erhverv as described above. The LRA can assign roles for both TFE and PROD users.

3.1.4   DMS System-to-System access

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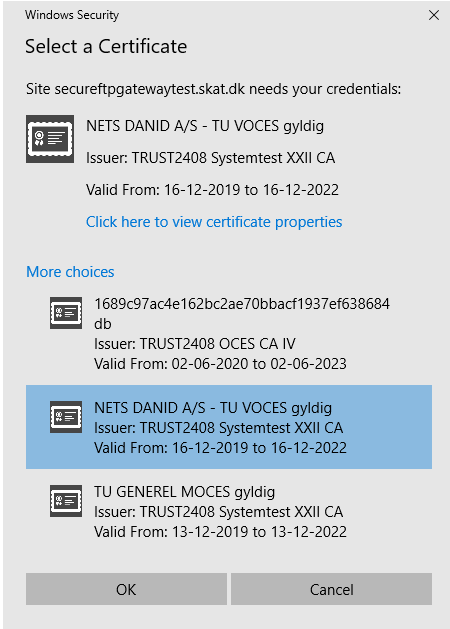
Register client certificate

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

The VOCES certificate must be installed on the machine. For details on how to install a certificate, see appendix 9.1 Install certificate. You are required to use the same certificate as for the FTPS gateway.

Registering certificate for system-to-system usage

1. In this example, multiple certificates have been imported to the browser. Here we select a NETS test certificate and enter the logon page of the certificate portal.	Windows Security ✕ Select a Certificate Site secureftpgatewaytest.skat.dk needs your credentials: NETS DANID A/S - TU VOCES gyldig Issuer: TRUST2408 Systemtest XXII CA Valid From: 16-12-2019 to 16-12-2022 Click here to view certificate properties More choices 1689c97ac4e162bc2ae70bbacf1937ef638684db Issuer: TRUST2408 OCES CA IV Valid From: 02-06-2020 to 02-06-2023 NETS DANID A/S - TU VOCES gyldig Issuer: TRUST2408 Systemtest XXII CA Valid From: 16-12-2019 to 16-12-2022 TU GENEREL MOCES gyldig Issuer: TRUST2408 Systemtest XXII CA Valid From: 13-12-2019 to 13-12-2022 OK Cancel
2. The CVR and UID/RID information is extracted from the certificate. In this example, you are identified as user: CVR_30808460_UID_25351738. **Important:** The first time you log in, the default password is your user ID. You can therefore simply copy and paste, and proceed to log in. **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.	**UFST Managed File Transfer -** Selected certificate is for user: CVR_30808460_UID_25351738 Log on using your password for the Certificate Portal app. Password [••••••••••••••••••••• 👁] Log on UDVII FORE STYRI

3. The first time you log in you are required to change password. You may use the password for your certificate or any other.

Change password

You must change the default password!   ✕

Current password	••••••••••••••••••••••
New password	••••••••
Confirm password	•••••••• 👁

Change password   Cancel

---

4. The certificate is not registered in the self-service portal, which would therefore reject any logon attempt. Proceed 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

---

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.

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

---

6. The certificate is now registered. Check the AS4 box in the interface section and click "Update interfaces".

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	do-not-write@skat.dk Update e-mail
Interfaces	☑ FTPS ☐ AS4 ⟵ Update interfaces
Gateway user	CVR_30808460_RID_45490598
Gateway password	******** 👁

7. Note down your username and password, which will be used for setting up your AS4 session.

UFST Managed File Transfer - Certificate/User overview

Your certificate is registered and ready for use.

Common name	CVR:30808460-UID:25351738
Expiry date	16-12-2022
Type	CVR
Legal identifier	CVR_30808460
Account	UID_25351738
E-mail	do-not-write@skat.dk [Update e-mail] E-mail is updated.
Interfaces	☑ FTPS ☑ AS4
Gateway user	CVR_30808460_UID_25351738
Gateway password	******** 👁

7. 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).

Network connection

5

5.1 AS4 gateway 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.

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.

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
```


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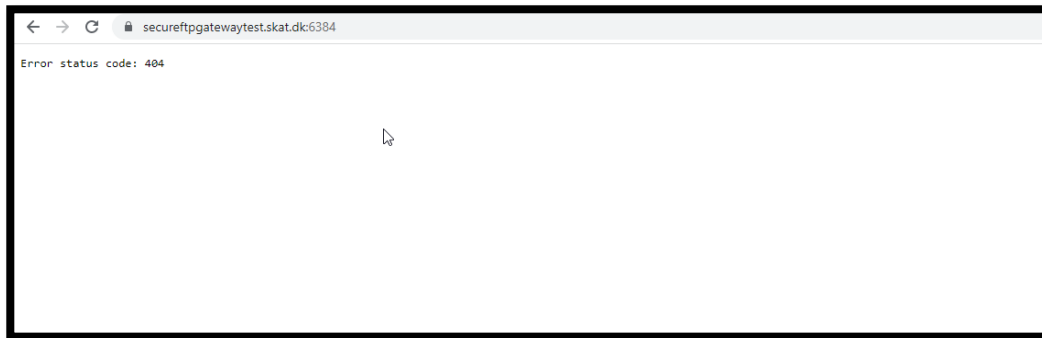
```
Test-NetConnection <Hostname>-Port 6384
```

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. The list of environment specific services and actions is available under AS4 services in the system guide on GitHub.

```
<eb3:CollaborationInfo>
        <eb3:Service type="string">DMS.Import2</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 or AS4 header of every call to the AS4 gateway. For all companies, the submitter reference should be the numbers in their CVR or EORI number. For example, if a company has the CVR number "CVR_30808460" then the submitter reference will be "30808460". The submitter field then looks as follows:

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

6.1.3   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: xmlenc#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: AS4 payload sample

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 set to be delivered in the SOAP body. The message structure is shown here below:
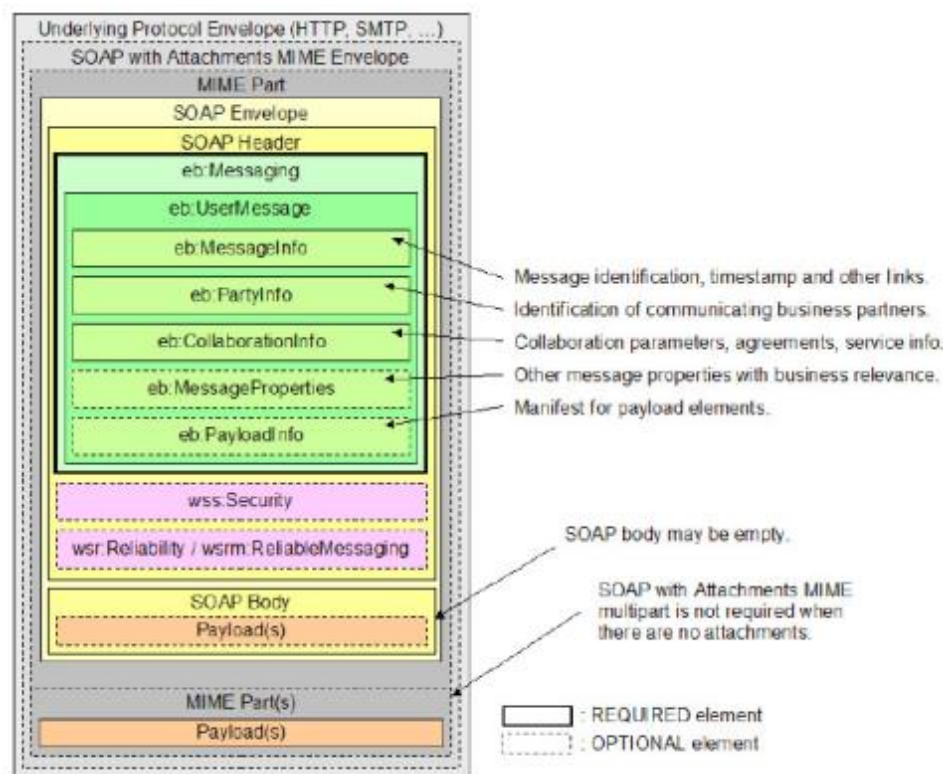
The soap attachments are planned to be used for amendments in a later release and will not be covered by the testcases described here.

6.1.5   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.

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>_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 Initator 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 Initator 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. Conversation Id	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:

```xml
<eb3:Messaging xmlns:mustUnderstand="http://www.w3.org/2003/05/soap-enve-
lope" 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/oa-
sis-200401-wss-wssecurity-utility-1.0.xsd" mustUnderstand:mustUnder-
stand="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/ini-
tiator</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/re-
sponder</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>
```

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 five 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 chapter 4.

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 was made by the IT and Development Agency. The goal of this package is to speed up the onboarding of new economic operators 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
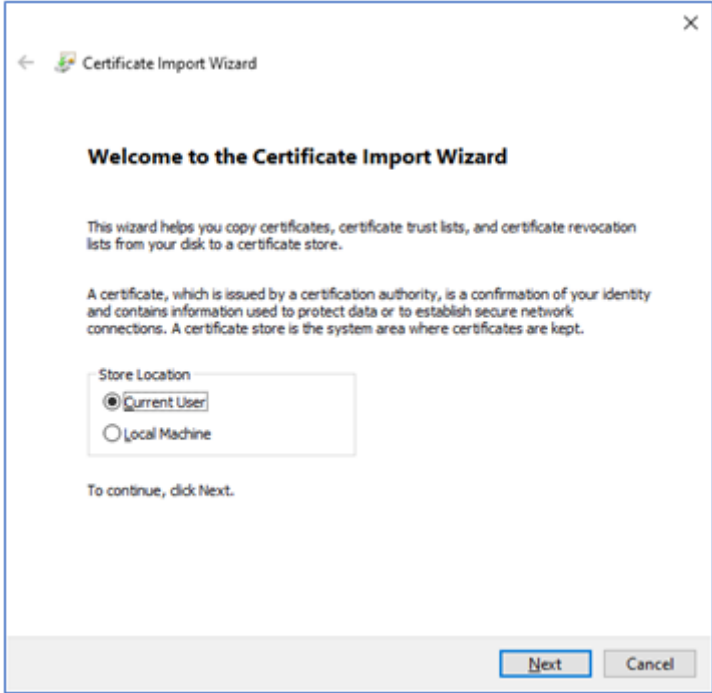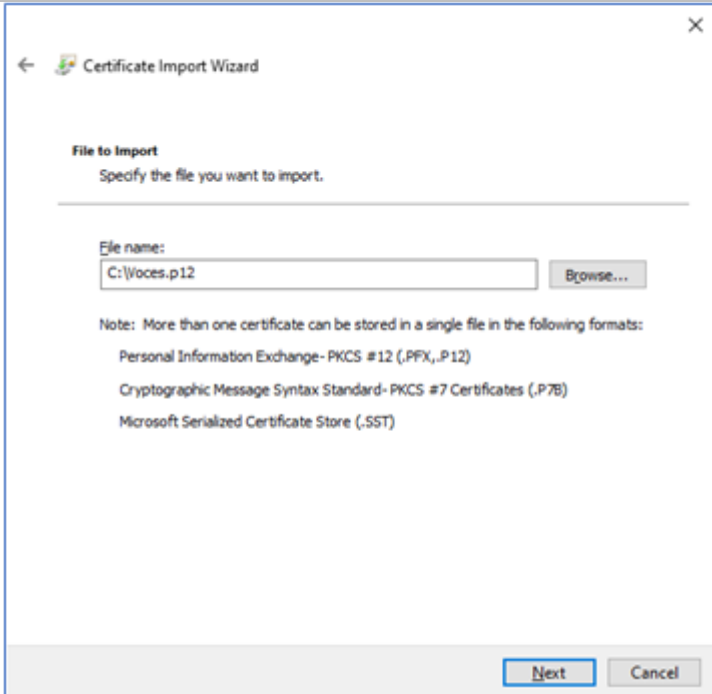
The package is written in Java and provided as Java dependency. Integration with .NET based projects is therefore not as simple. For .NET based projects we recommend building a small Java based communication middleman REST API, which utilizes the simple AS4 client, that the existing .NET code can communicate with.
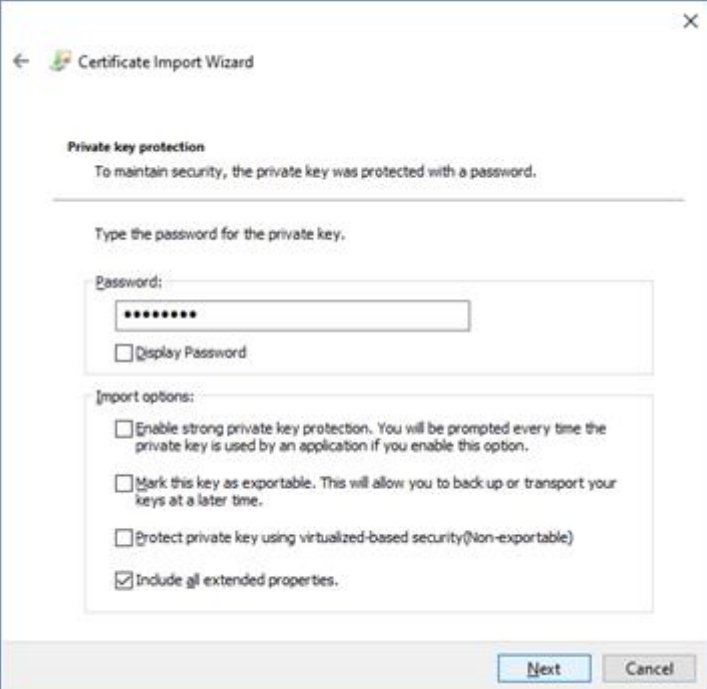
Appendices

8

8.1 Install certificate

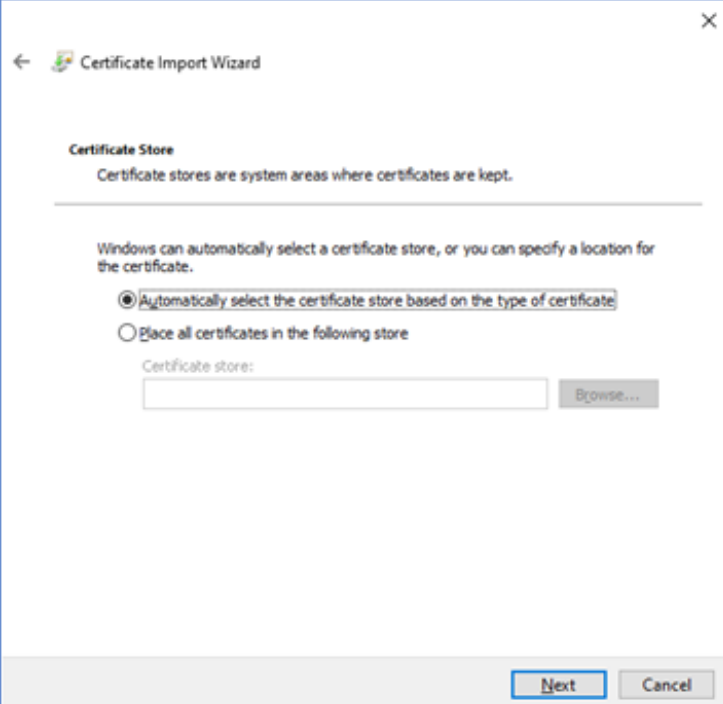| Install certificate	
1. Locate the certificate you wish to install. It should be a file in .pfx/.p12 format. Double click the file.	See details chapter 2.
2. You should be presented with this menu. Click Next.	
3. Select the VOCES certificate.	

Install certificate

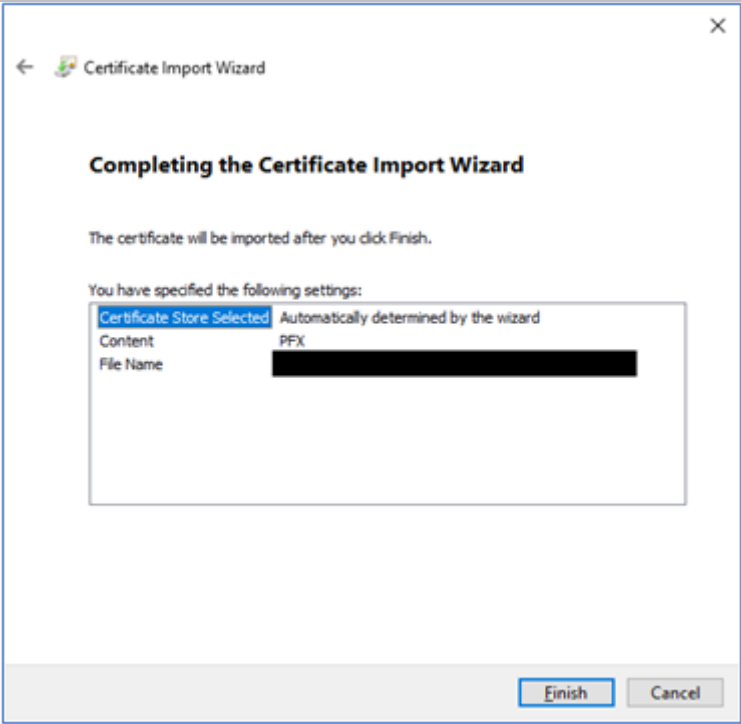|	
4. Fill out the password and check the box to include all extended properties.	
5. Choose to automatically select the certificate store based on the type of certificate.	

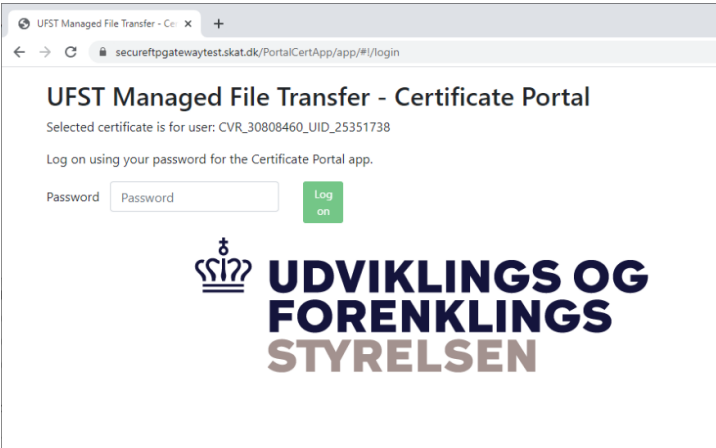## Install certificate

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

Verify installation in Windows certificate manager

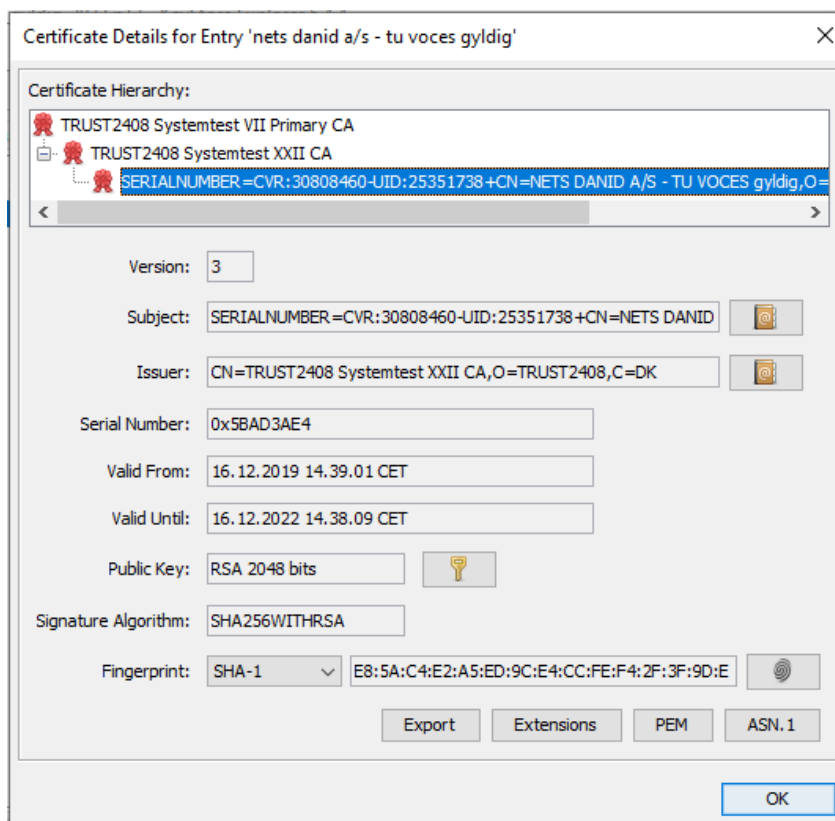|	
1. Open the Run app (found by searching in the start menu). Open the certificate manager by typing "certmgr.msc" and clicking OK.	
2. Locate the certificate. The certificate store and naming of client certificate depends on your client setup.	
3. Go to https://secureftpgateway.skat.dk in a client with access to certificate	

8.1.1   Verifying correct certificate

Certificates must be of the VOCES format, which contains a unique UID 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.
3. Verify that the bottom node is of the following format: SERIALNUMBER=CVR:xxxxx-UID:yyyyy+zzzz

8.2 Technical overview of system-to-system

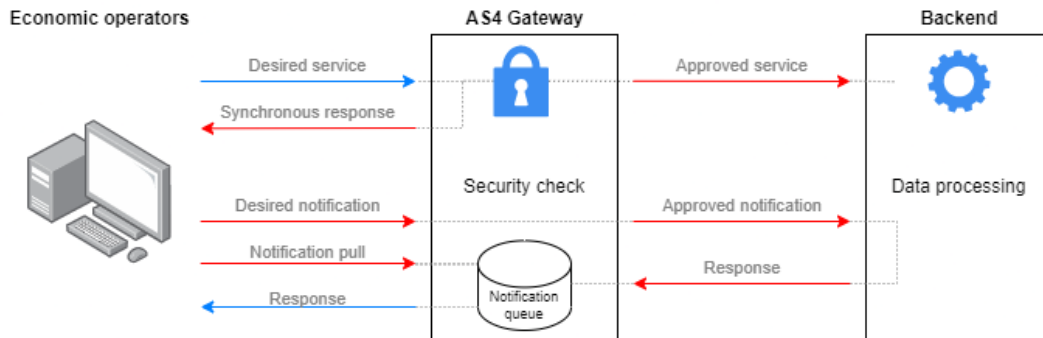This section provides a brief description of the provided system-to-system solution.

*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 in the Danish Customs and Tax Administration. 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 is described in the DMS Onboarding Guide (in Danish), and an overview of provided notifications can be found in the DMS System Guide.

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 VOCES 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

Massage 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"

8.6 Certificate errors

These errors have occurred 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.