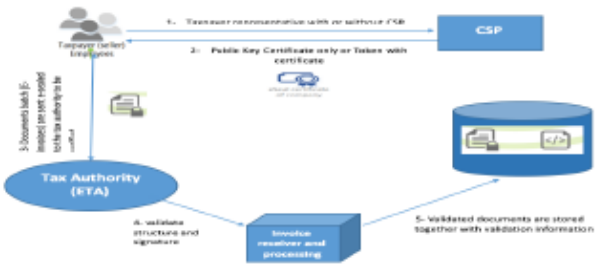
Introduction

- As an introduction to the scenario, a large or mid-size taxpayer submits a document batch from its ERP systems which calls APIs of the solution to submit digitally signed document batch to the tax authority. These documents have to be signed or Electronically sealed by such taxpayer entity using the e-sealing certificate which have to be issued by the CSPs. These signed documents are then sent to ETA to be validated and stored
- E-sealing certificates actually resemble any other certificate issued for a person, but the only difference is that it is issued for an entity or company and therefore contains an additional field with a certain technical structure called the TAX ID which is required to differentiate a taxpayer company from the others within the tax system

Detailed Scenario



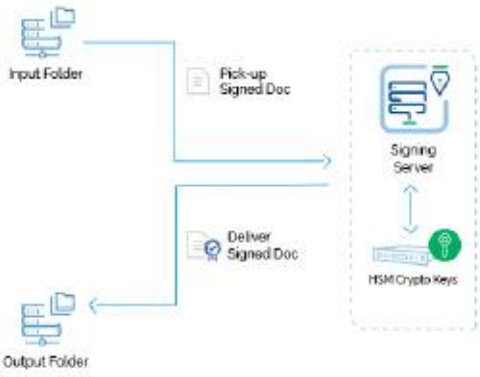
- For the scenario shown in the above figure, a taxpayer can request an e-sealing certificate through one of the below steps:
  - The Key pair (public and private key that will be used in digital signing and verification process) will be generated from the taxpayer's side through HSM device that will be supported by HSM Vendor, then taxpayer will create CSR (Certificate Signing Request that consists of public key and data of taxpayer's organization) by using the HSM device and send it to CSP (Egypt Trust / MCDR) to sign it and issue digital certificate for the taxpayer. Then taxpayer will receive the certificate from CSP (Egypt Trust / MCDR) on a portable media to import it back to the HSM device
  - The Key pair is generated from the CSP's side on a secure media e.g. Token which is given back to the taxpayer to be directly used in sealing documents. This is for small size taxpayers which do not require HSM device

E-invoice process flow

Steps1: the ERP system will put the JSON (final format of e-invoice) file in the input folder

Step2: the Front-End APP will take this file to sign it through the signing service and place it in the output folder

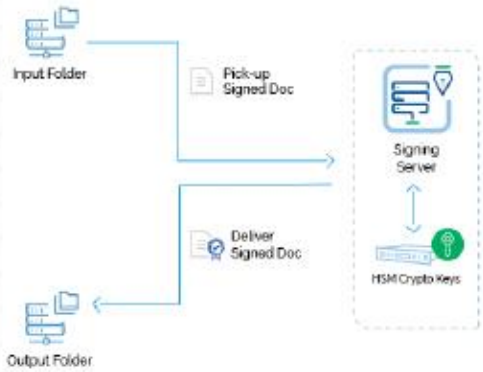
Step3: the taxpayer ERP system will take this signed document (JSON file) and submit it to ETA e-invoice system



Taxpayer Responsibilities

Taxpayer will perform the following tasks:

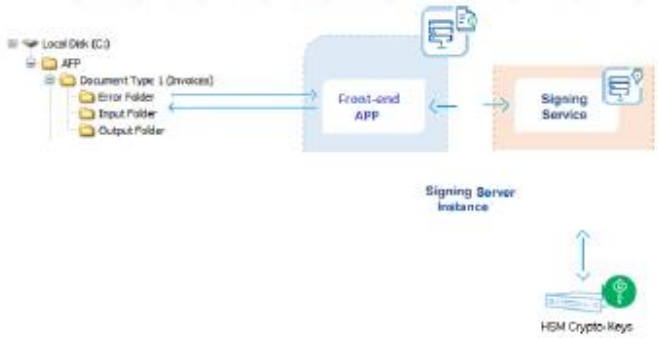
- Install Operating System on Signing Server
- Install HSM driver on Signing Server
- Configure HSM to be connected with Signing server
- Generate Keys on HSM and Create CSR using HSM tools, send CSR to CSP
- Import digital Certificate in HSM after CSP (Egypt Trust / MCDR) sign the CSR and issue the taxpayer's digital certificate
- Develop, install and configure Front-End APP on signing server
- Develop Signing Service based on ITIDA's SDK (Software Documentation Kit), install and configure it on signing Server



Front-End APP

- Front-end application for signing Server to monitor multiple input folders and processes batches of files
- It selects a batch of files to process, removes these from the input folder, processes them and then places the output files in their specified output folder locations

Signing Service



- Signing service profiles define the type of signature to produce, including:

The format of the document to sign (PDF, XML, files… etc.).

- E-invoice backend system is expecting a basic signature type in format of CAdES object RFC5126
- Define signing key to use (a default key can be used) which information to include in the signature (e.g. signing reason, signer's location, signing policy etc.)
- Digital signature is not visible as it's a complicated mathematical computations on the data/files using cryptography algorithms

Thank You