Business Certificate Publisher

Specification

DIFI OFFENTLIGE ANSKAFFELSER

11. september 2017
Skrevet av: Erlend K. Bergheim og Olav A. Kristiansen

Contents

Business Certificate Publisher

Specification

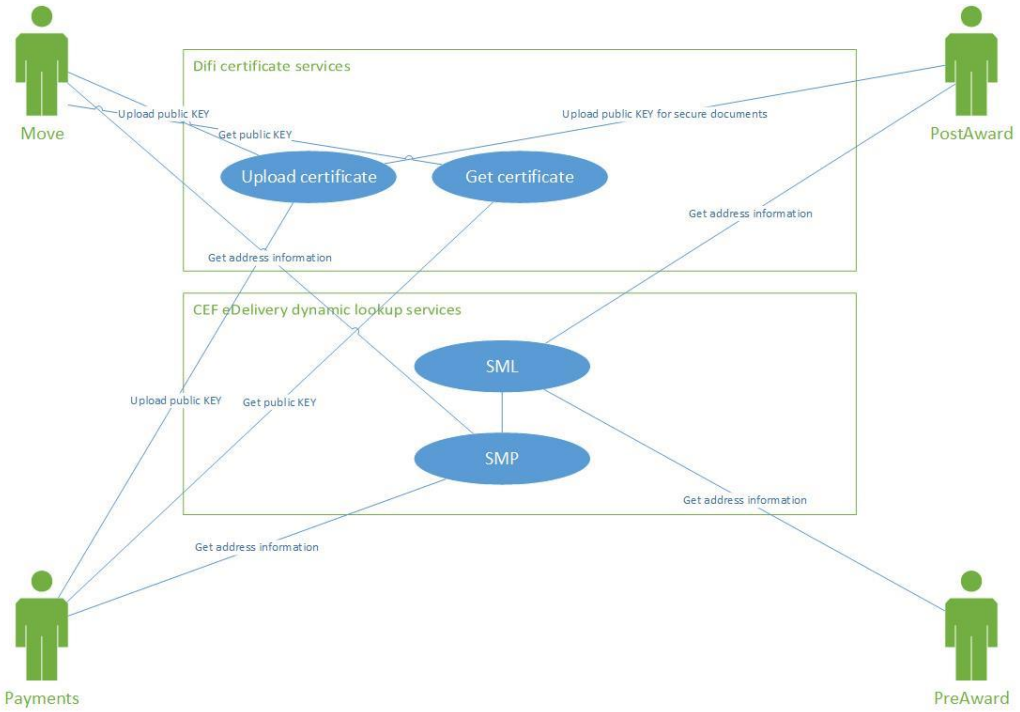
Background

Requirements to information security are increasing in most aspects of society.

Difi has a key management role for security in transaction based systems in different sectors. This is transaction systems like public-to-public, health, invoicing, payments and other systems that are based on Enhanced PEPPOL eDelivery network.

The assumption is a rapidly increased number of services and data transfers will need information security. We have identified a need to establish an infrastructure or a chain of trust.

This infrastructure will make existing PKI trust chains provided by the market available upon request. At the same time a considerable number of services between the public or private sector, seem to have a comparable need for data protection and security. This emphasizes the demand for a scalable trust architecture and allow easy access to encryption certificates when needed in business process inside many industries.



Objective

The purpose of this document is to specify requirements to Business Certificate Publisher (BCP). BCP supports various business level processes were information protection is needed in the four corner model i.e. Enhanced PEPPOL eDelivery network.

Functionality

The BCP will make the business certificate available for solutions that seeks to encrypt a document for one or more given receivers. The entity who want to receive encrypted documents are responsible for making the business certificate available in a structured manner in the BCP. An entity can have many business certificates, organisations numbers and many profiles. When fetching a certificate for encryption a combination of organization number and process is provided.

Description

The first version of BCP is used to make available certificates for use in Enhanced PEPPOL eDelivery network. The certificate is stored at the server for an organisation number and a given process. Process in this context is processes within i.e. payments, public-to-public document exchange and secure post-award (i.e. secured invoice).

The document receiver is responsible for having a correct and valid business certificate in the BCP issued by one of the trusted CA. A receiver may make available multiple certificates, and the same certificate can be used in many processes.

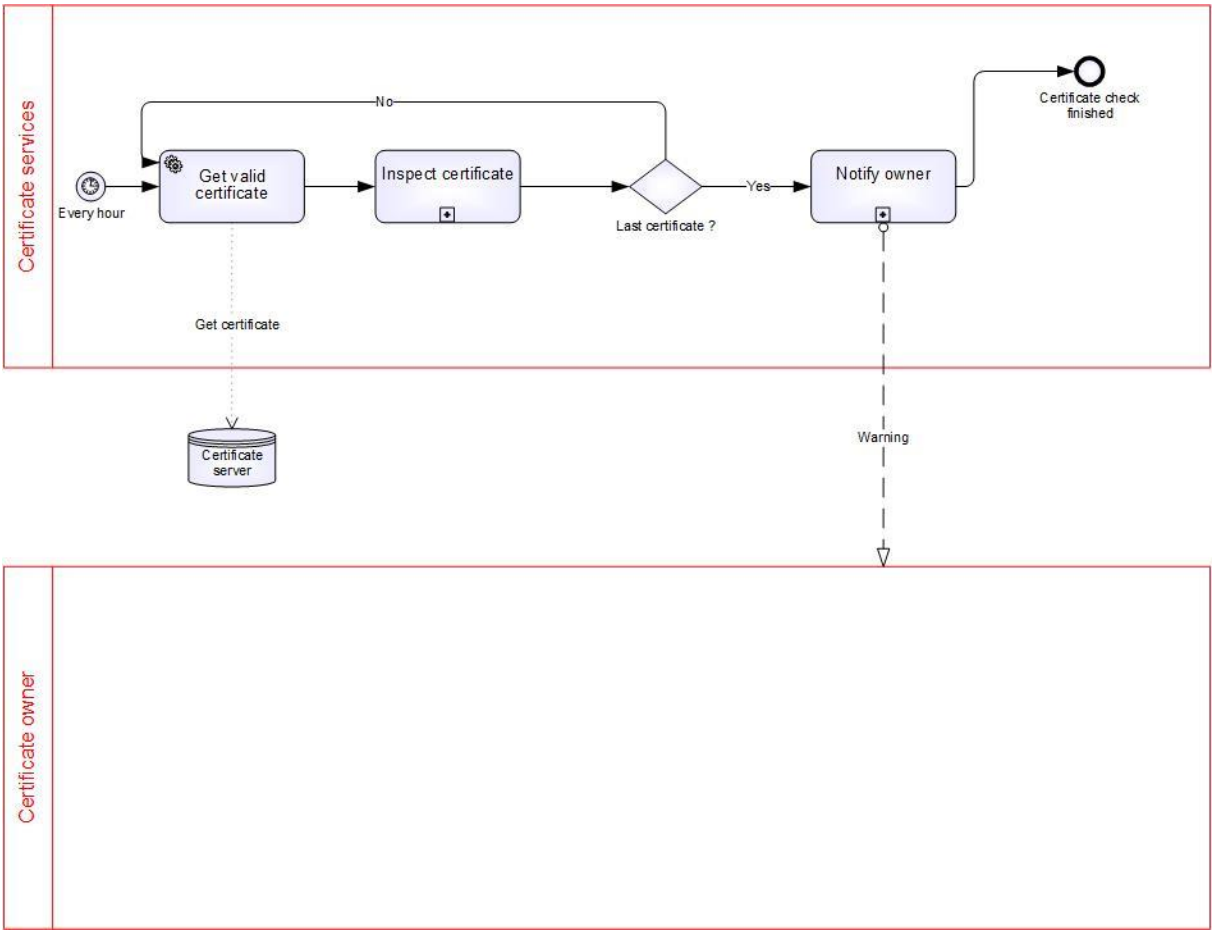
Uploaded certificates must be issued by a trusted certificate authority (CA) and in first phase only certificates from Commfides and Buypass are approved. All approved CA will be listed on https://vefa.difi.no/.

Control mechanism

The BCP is mainly a service for publishing business certificate in a structured manner. The service will verify registered business certificates on given intervals to make sure revoked and expired certificates are removed from use. It is still important and necessary for users to verify each certificate upon use.

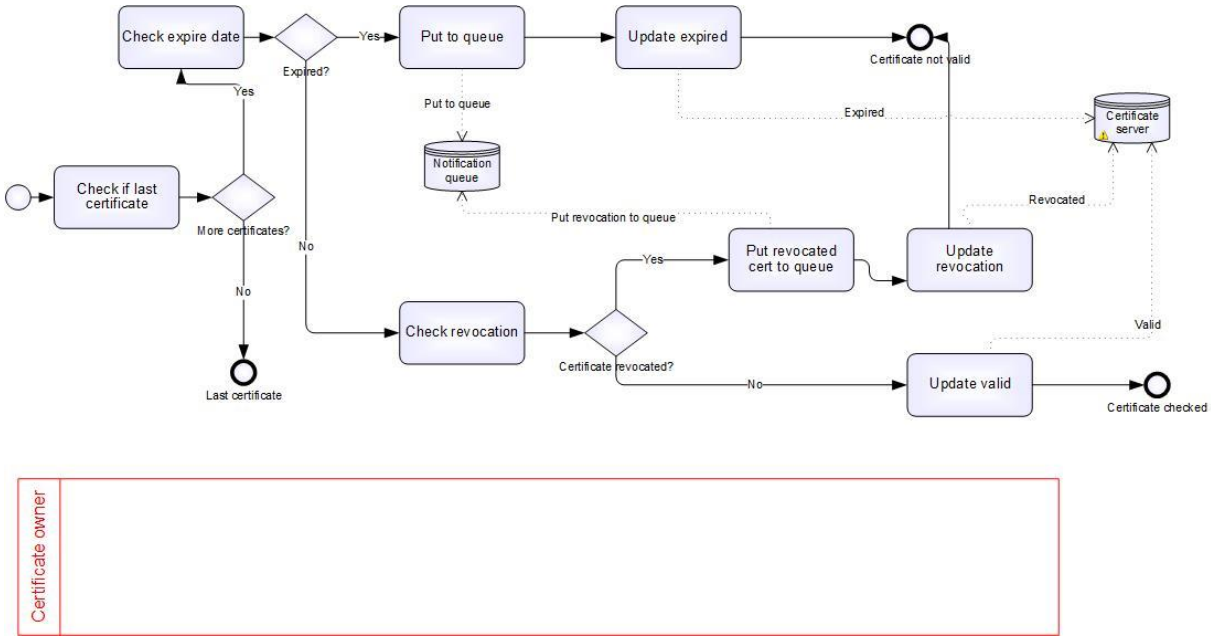
Process: Hourly control of certificates and expiry dates

The services will verify each registered certificate for expiration date and revocation. Notification about upcoming expiration and revocation is sent to registered users.



Process: Verify certificate

This sub-process will check if the certificate is valid.



The sub-process starts with a check if there are more certificates to verify.

The following steps are performed during validation of a given certificate:

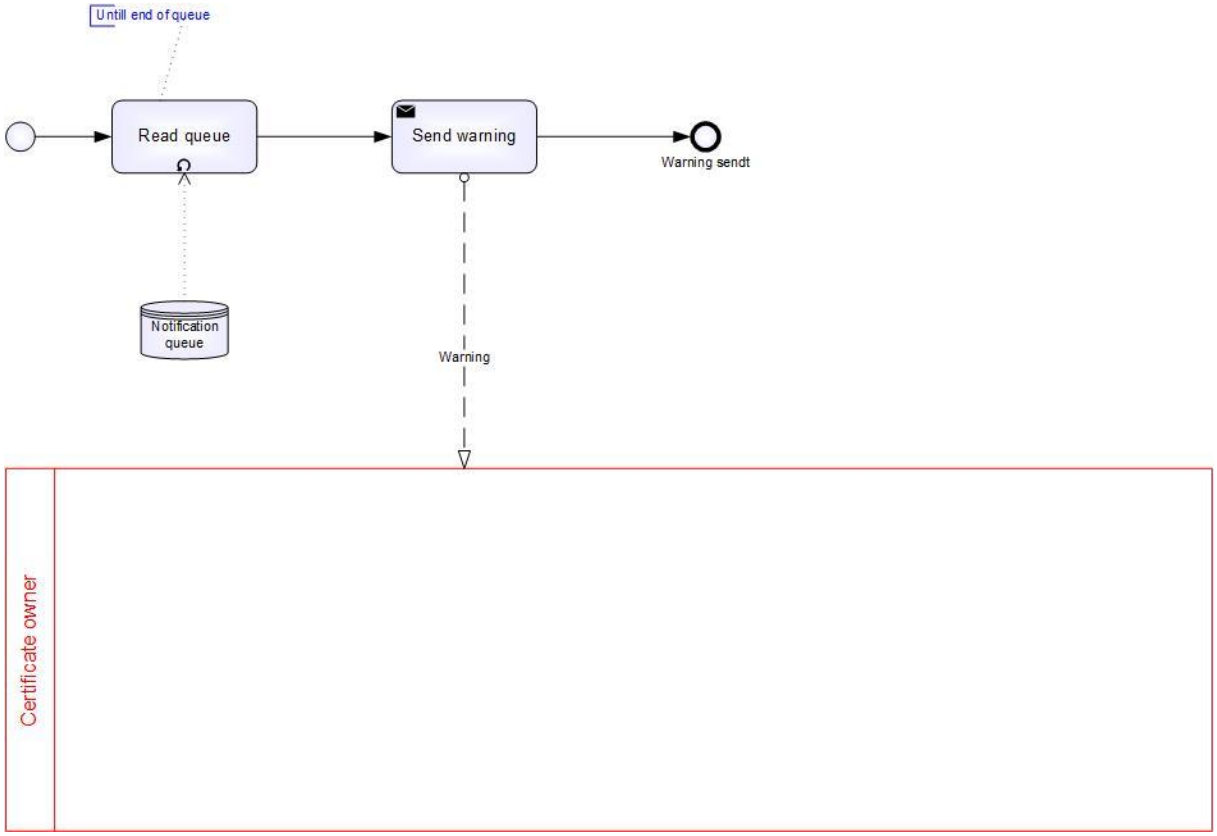
- Verify the certificate is not expired.
- Verify the certificate is not revoked.

All expired and revoked certificates are queued for notification to the registered owner of the certificates.

All valid certificates will be updated in the BCP and all other certificates that are queued is updated whit revoked or expired.

Process: Notify certificate owner

This sub-process notify the certificate owner if the certificate is revoked or the certificate is expired upon detection.



Notify owner

The sub-process starts with reading all certificates from the notification queue and will send a notification to all certificate owners.

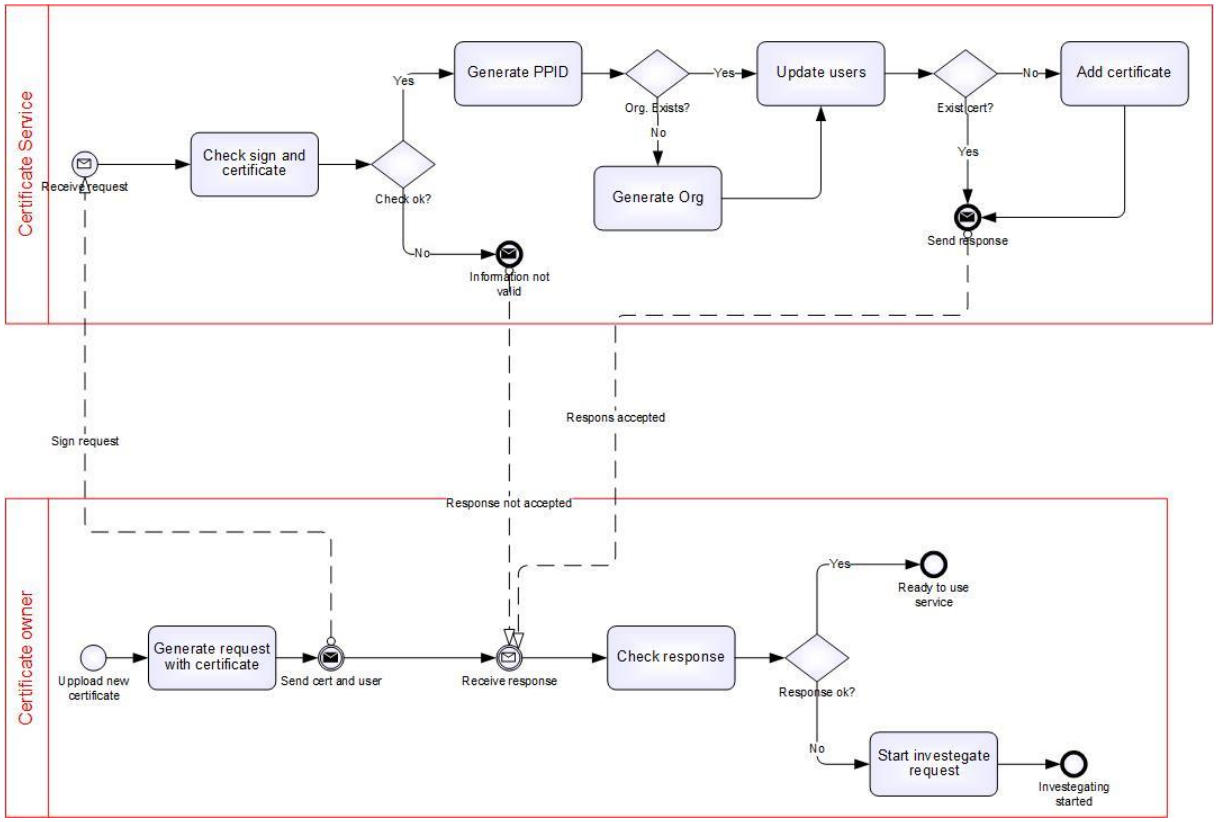
Initiation of a new organization

This process describes how to initiate a new organization into the BCP.

Process: Initiation of a new organization

The main process for approving a new organization with a signed request include the certificate.

The outcome of this process is to ensure that the certificate owner is who he says he is, and register new users and to upload the certificate.



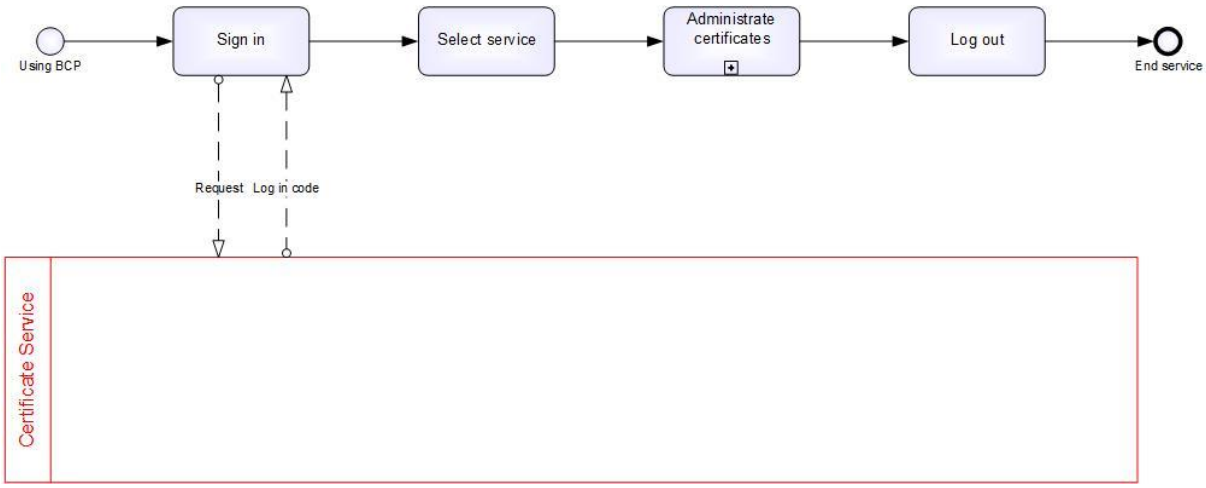
The process is started by the certificate owner wanting to upload a certificate. The certificate owner will make a "file" and sign it and send it to the **certificate service**.

Certificate service will then check the signature and the certificate. If this check is not okay, certificate owner will be notified. If the test is ok, certificate service will generate PPID and the organization if it not exists before the certificate is uploaded. When this is done the certificate owner will be notified.

The certificate owner must handle the response with investigate or ready to use the BCP.

How to use the BCP

This process describes how to use the BCP.



Processes

There are possibilities for entities to upload many company certificates to certificate server. Only certificates associated with one or more processes are made available.

Payments

This profile is for securing payments between banks and payers. Both banks and payers must upload their certificates.

Invoicing

This profile is for securing the content of an invoice. Only the invoice receiver need to upload the certificate.

Ordering

This profile is to secure the content of an order. It is recommended that both the buyer and the supplier upload their certificates.

Catalogue

This profile is to secure the content of a cataloguer. Only the buyer need to upload the certificate.

Archive

This profile is for securing documents between public entities, and it is recommended that all public entities upload their certificates.