Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Certificaatgebruik bij het opvragen van statussen (ebMS)

Versie 1.0

Datum 25 mei 2018
Status Definitief

Inhoud

Versie	*Omschrijving/opmerkingen*	*Steller*
1.0	Initiële versie	Logius

1. Certificaatgebruik bij opvragen statussen

Voor het opvragen van de status van een ebMS berichtaanlevering wordt de WUS Statusinformatieservice gebruikt. Om de status op te vragen moet de identiteit van de gebruiker die de status opvraagt overeenkomen met die van berichtaanlevering.

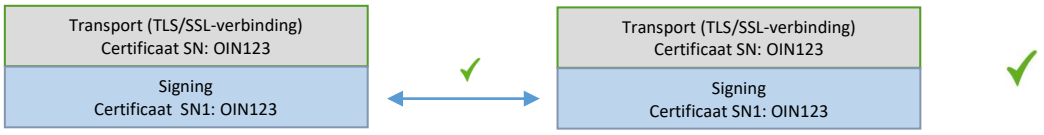
Standaard gebruiken Overheden ebMS met ondertekening (signing) van het bericht en gebruiken ze hetzelfde certificaat voor transport en ondertekenen. Er kunnen situaties zijn dat organisaties verschillende certificaten met hetzelfde OIN of een verschillend OIN willen gebruiken voor transport en ondertekenen. Hieronder zijn de belangrijkste mogelijkheden uitgewerkt en wordt aan gegeven welke opties leiden tot een werkende situatie.

De Statusinformatieservice gebruikt altijd het Organisatie-identificatienummer (OIN) van het certificaat waarmee het statusrequest is ondertekend om de identiteit van de statusaanvrager vast te stellen. Het OIN is in het certificaat opgenomen in het serial number van het onderwerp. Als bij de aanlevering signing is gebruik wordt het OIN van beide handtekeningen met elkaar vergeleken. Bij aanleveringen zonder signing gebruikt de Statusinformatieservice het OIN uit het certificaat dat gebruikt is voor het transspport van de aanlevering.

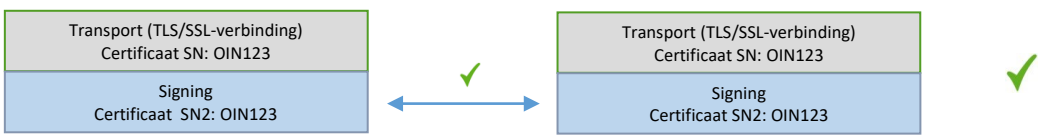
ebMS = ebXML Messaging Service (Electronic Business XML)
WUS = Koppelvlak WUS 2.0 voor Overheden
SN = Serial number van het onderwerp uit het PKI-Overheidcertificaat
SIS = StatusInformatieService

Aanleveren via ebMS	SIS bevragen via WUS	Werkt

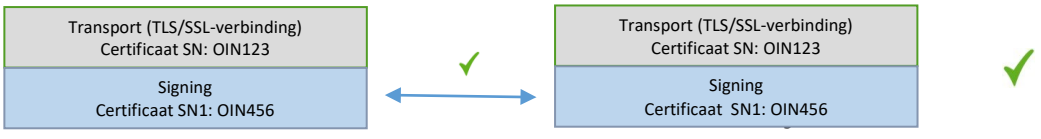
<u>Standaard implementatie</u>: *ebMS en WUS met signing: één certificaat (= één OIN) voor transport en signing*



ebMS en WUS met signing: verschillend certificaat voor transport en signing, beide certificaten hetzelfde OIN



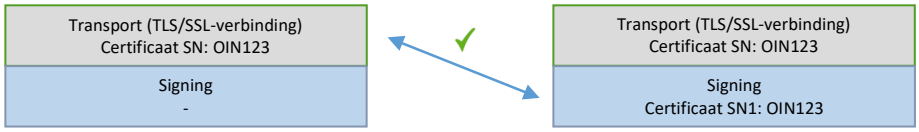
ebMS en WUS met signing: Verschillend certificaat voor transport en signing, certificaten met verschillend OIN



Aanleveren via ebMS	SIS bevragen via WUS	Werkt

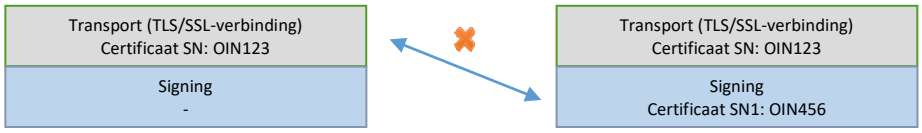
ebMS zonder signing / WUS met signing: één certificaat (= één OIN) voor transport en signing

Bij het ontbreken van signing bij een ebMS aanlevering gebruikt de Statusinformatieservice als identificatie het OIN van het transportcertificaat van de ebMS aanlevering. Als deze overeenkomt kunnen de statussen opgehaald worden.



ebMS zonder signing / WUS met signing: Verschillend certificaat voor transport en signing

Zoals hierboven aangeven zal als signing ontbreekt, de statusinformatie service als identificatie het OIN van het transportcertificaat van de ebMS aanlevering gebruiken. In deze casus is komen de OIN's niet overeen en kunnen de statussen niet worden opgehaald.



ebMS en WUS met signing: Verschillende certificaat voor transport en signing

Mismatch niet door mismatch van certificaat, maar door mismatch van OIN (SSN) tussen de vergeleken (signing) certificaten.