Enable-U
Dé Integratiespecialist

eHerkenning rapport Enable-u

Enable-U 2Secure

Auteur: Kevin Rijs
Plaats en Datum: Amsterdam, 03-10-2016
Versie: 1.0

1. Inhoudsopgave

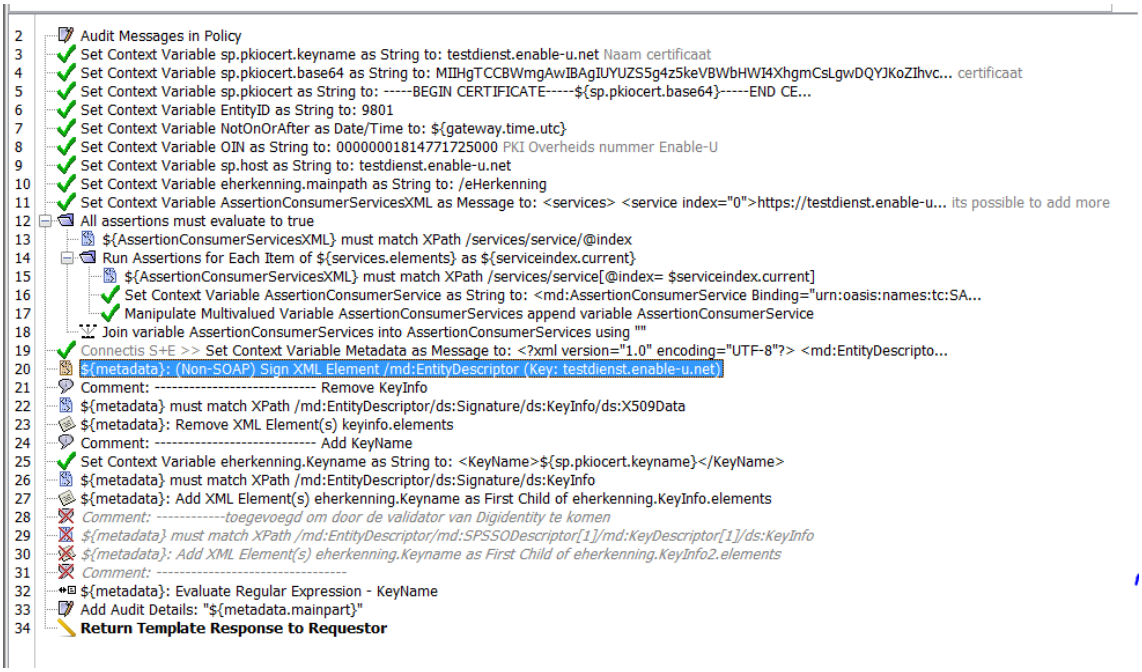
2. eHerkenning aansluiting Enable-u

De eHerkenning aansluiting van Enable-u wordt gerealiseerd door Enable-u2Secure (powered by CA API Management Gateway). De belangrijkste stappen in het authenticatie proces van de dienstverlener worden gerealiseerd in de zogehete 'policies' van Enable-u 2Secure waar verschillende stappen worden afgedwongen en gevalideerd. De stappen in de eHerkenning policy bestaan uit individuele regels die van boven naar onder worden gelezen.

Hieronder worden kort de belangrijkste stappen van het Eherkenning inlog proces beschreven.

2.1 Genereren en signen metadata Dienstverlener

Hieronder is een screenshot van de policy aanwezig die laat zien hoe de XML van de metadata van de Dienstverlener wordt opgebouwd (regel 2-19) op het moment dat deze wordt aangeroepen. Nadat deze is gegenereerd wordt deze gesigned met het private key van de klant (regel 20) en de signature in de metadata geplaats (regel 21-32). Daarna wordt de volledig gegenereerde metadata aan de requestor getoond (regel 34).



2.2 Versturen en signen Saml/Authn Request

Hieronder is een screenshot van de policy aanwezig die laat zien hoe een Authn/Saml request wordt opgebouwd. Als eerst wordt de relaystate en het samlrequest message gemaakt (regel 63-70). Hierna wordt de samlRequest gesigned (regel 71), waarna de signature in het saml

request wordt geplaatst (regel 73-82). Als laatste wordt de gebruiker geredirect naar de Herkennings Makelaar (regel 83-87).

2.3 Ontvangen en valideren Saml/Authn Response

Hieronder is een screenshot van de policy aanwezig die laat zien hoe een ontvangen Authn/Saml response wordt gevalideerd en gelezen. Als eerst wordt er gezocht naar de signature van de herkenningsmakelaar (regel 129-132), waarna deze controleerd wordt tegen het desbetreffende certificaat van de herkennings makelaar (regel 133). Daarna wordt het saml response gevalideerd op structuur (regel 136) en wordt er gekeken of het betrouwbaarheidsniveau overeenkomt met het benodigde niveau (regel 137-141). Is dit het geval dan worden alle meegestuurde attributen van de gebruiker uitgelezen (regel 142-165) en later aangeboden aan de backend applicatie.