

T2. Validatie token

Vraagstelling

Welke optionele validatie token data zijn voor het beleid van ENUM NL noodzakelijk om een goede validatie te kunnen garanderen en welke kunnen worden weggelaten?

Welke algoritmes moet de Registry definiëren en welke key sizes moet zij accepteren voor de handtekeningen in het validatie token?

Mag de Registry zelf certificaten uitdelen en welke certificaten mag zij accepteren?

Een voorstel voor de beantwoording van deze vraagstelling vindt u hieronder. U kunt op dit voorstel reageren via het online forum of via de fysieke discussiebijeenkomsten. Uw input wordt zeer gewaardeerd en meegenomen bij de operationalisering van ENUM.

Achtergrond

Een ENUM-domeinnaam wordt afgeleid van een onderliggend E.164 telefoonnummer. Validatie is het proces dat controleert of de registrant van de ENUM-domeinnaam ook de gebruiker is van het corresponderende E.164 telefoonnummer. Deze validatie wordt uitgevoerd door een gecertificeerde Validatie Agent. In het voorstel voor een validatiearchitectuur die uitgaat van [RFC 4725](#) wordt aanbevolen dat de validatiedata van de Validatie Agent door de Registrar worden meegestuurd met de registratie aan de Registry. Eveneens wordt aangegeven dat een specifieke validatietechniek vooraf geregistreerd moet zijn. Dit voorstel gaat dieper in op de syntax van de validatiedata die in dit proces worden gebruikt.

Belangrijk in het proces is dat bij de registratie van een ENUM-domein kan worden beoordeeld door welke Validatie Agent en volgens welke methode de validatie heeft plaatsgevonden. Ook dient te worden aangegeven dat de data die dit aantonen integer zijn.

Data die integer aantoont dat en hoe een validatie heeft plaatsgevonden, wordt een "validatie token" genoemd. Een validatie token bestaat uit de relevante validatiedata en wordt door de Validatie Agent van een digitale handtekening voorzien, zodat de integriteit van de data door andere partijen, zoals de Registry, kan worden beoordeeld.

Een voorstel voor de syntax en encryptie van een dergelijke validatie token is inmiddels goedgekeurd door de IETF en zal binnenkort als RFC worden gepresenteerd. Het voorstel is voorlopig te vinden als Internet Draft op <http://tools.ietf.org/id/draft-ietf-enum-validation-token-04.txt>.

Het voorstel gaat ervan uit dat het validatie token moet kunnen worden gebruikt in het standaard Registry-Registrar Extensible Provisioning Protocol (EPP) en is daarom gebaseerd op XML. Voor de encryptie wordt XML-DSIG volgens RFC 3275 gebruikt. ENUM NL zal in haar registratie systeem voor ENUM EPP ondersteunen en zal voor het validatie token ook deze nieuwe standaard gebruiken.

Het validatie token bestaat uit verplichte data, optionele data, een handtekening en een certificaat. Onderstaand treft u een voorbeeld van een validatie token.

```
<?xml version="1.0" encoding="utf-8" standalone="no" ?>
<token xmlns="urn:ietf:params:xml:ns:enum-token-1.0" Id="TOKEN"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation=
    "urn:ietf:params:xml:ns:enum-token-1.0 enum-token-1.0.xsd">
  <validation serial="acmeve-000001">
    <E164Number>+442079460123</E164Number>
    <validationEntityID>ACME-VE</validationEntityID>
```

```

    <registrarID>reg-4711</registrarID>
    <methodID>42</methodID>
    <executionDate>2007-05-08</executionDate>
</validation>
<tokendata xmlns="urn:ietf:params:xml:ns:enum-tokendata-1.0"
  xsi:schemaLocation=
    "urn:ietf:params:xml:ns:enum-tokendata-1.0 enum-tokendata-
1.0.xsd">
  <contact>
    <organisation>Example Inc.</organisation>
    <commercialregisternumber>4711</commercialregisternumber>
    <title>Dr.</title>
    <firstname>Max</firstname>
    <lastname>Mustermann</lastname>
    <address>
      <streetName>Main</streetName>
      <houseNumber>10</houseNumber>
      <postalCode>1010</postalCode>
      <locality>London</locality>
      <countyStateOrProvince>London</countyStateOrProvince>
      <ISOcountryCode>GB</ISOcountryCode>
    </address>
    <phone>+442079460123</phone>
    <email>mm@example.com</email>
  </contact>
</tokendata>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod
      Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    <SignatureMethod
      Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256" />
    <Reference URI="#TOKEN">
      <Transforms>
        <Transform Algorithm=
          "http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        <Transform
          Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
          <InclusiveNamespaces
            xmlns="http://www.w3.org/2001/10/xml-exc-c14n#"
            PrefixList="enum-token enum-tokendata" />
          </Transform>
        </Transforms>
        <DigestMethod
          Algorithm="http://www.w3.org/2001/04/xmldsig#sha256" />
        <DigestValue
          >VxqsBxSNPFwPAU1CHts3g3DehcexnB1dqUz+GypLZ0k=</DigestValue>
        </Reference>
      </SignedInfo>
      <SignatureValue>
        QKqphKRNpOkVZFbenje+HZZV+RLrNweGnlWBw7ngAtH+rtuslR8LhMLmC4D1Bb9V
        HvKI1l+7zLGm3VgYsqfHH8q3jC11mFxiUuLlIPqtpJs+xAHAJDzZ+vmsF/q2IgrS
        K0uMmKuU5V1gydDBOvIipcJx+PrPYyXYZSjQXkWknK8=</SignatureValue>
      <KeyInfo>
    <X509Data>
    <X509Certificate>

```

```
MIIDZjCCAs+gAwIBAgIBBDANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJBVDEP
MA0GA1UEBxMGVml1bm5hMRQwEgYDVQQKEwtCT0ZIIENlcnRzLjEhMBkGA1UEAxMS
Q0VSVFMuYm9maC5wcm12LmF0MSEwHwYJKoZIhvcNAQkBFhJjZXJ0c0Bib2ZoLnBy
aXYuYXQwHhcNMDQwNzIwMTMxNTA5WhcNMDUwNzIwMTMxNTA5WjB/MQswCQYDVQQG
EwJBVDEKMAgGA1UECBMlTEPMA0GA1UEBxMGVml1bm5hMR0wGwYDVQQKEwRBY211
IEVOVU0gVmFsaWRhdGlvb2ZlbnR5b250b291b291b291b291b291b291b291b291
ARYTbm9ib2R5QG9w0BAQEFAAOBjQAwgYKC
gYEAJPCjMfc54/zwztSdQXGxUtodJT9r1qGI2lQPNjLvtPJg93+7o5SIOsZGSpg
zWbztDAV5qc7PHZWUVIyf6MbM5qSgQDVRjNRhTosNtyqmwi23BH52SKkX3P7eGit
LmqEkiUZRxZhZ6upRbtCqvKSwmXitvW4zXZkhVHYJZ2HuMcCAwEAAaOB/DCB+TAJ
BgNVHRMEAjAAMCwGCWCGSAGG+EIBDQqFh1PcGVuU1NMIEdlbmVyYXRlZCZBDXJ0
aWZpY2F0ZTA0BGNVHQ4EFgQUyK4otTQtvv6KdS1MBOPT5Ve18JgwgZ4GA1UdIwSB
1jCBk4AUvfPadpm0HhmZx2iAVumQTWgnG2eheKR2MHQxCzAJBgNVBAYTAKFUMQ8w
DQYDVQQHEwZwZWVubmExFDASBgNVBAoTC0JPRkkgQ2VydHMuMRswGQYDVQQDEwJD
RVJUUy5ib2ZoLnByaXYuYXQwITAfBgkqhkiG9w0BCQEWEmNlcnRzQGJvZmgucHJp
di5hdIIBADANBgkqhkiG9w0BAQQFAAOBQCB9CHBnIUhrdic4h5Ar4hdxjHSQkDH
sJWd+MYrNcuSrv3TIOsUkUgNpNNhmKzPtiXqfy3388IRdJtJiLWXSOb/XLZHOM9I
MvwKYwhcpQ9UdM/w7VpXQqf+CEj0XSyqxGw65UsHIOijgiG/WyhSj+Lzriw7CTge
P2iAJkJVC4t2XA==
</X509Certificate>
</X509Data>
</KeyInfo>
</Signature>
</token>
```

Alle elementen die vallen onder de “<tokendata>” zijn optioneel in dit schema en worden bepaald door het beleid van de ENUM Registry en de toegestane validatiemethoden. Er moet dus bepaald worden welke optionele data voor het beleid van ENUM NL noodzakelijk zijn en welke elementen uit het schema weggelaten kunnen worden om toch een goede validatie te kunnen garanderen.

Daarnaast moet de Registry definiëren welke algoritmes en key sizes ze accepteert voor de handtekeningen in het validatie token. Bovendien moet worden besloten of de Registry zelf certificaten uitdeelt, publieke certificaten accepteert, of dat het alleen met vooraangemelde certificaten werkt en hoe die dienen te worden uitgewisseld.

Scope | Kader van de discussie

De keuzes die moeten worden gemaakt gelden alleen voor het validatie token. Indien een validatie token wordt aanbevolen, kiest ENUM NL voor een implementatie volgens de RFC's. Een andere syntax of encryptie voor het validatie token dan beschreven in de RFC, of een ander Registry-Registrar protocol, staan bij deze vraag niet ter discussie.

De keuze of een validatie token moet worden gebruikt, wordt behandeld in het vraagstuk over de validatie architectuur.

Ook moeten de technische keuzes over de te gebruiken encryptie worden ondersteund door de registratie software van ENUM NL.

Voorstel ter beantwoording van de vraagstelling

1. Voor de optionele data wordt voorgesteld om alle adresgegevens niet verplicht te stellen in het validatietoken. Ook het "<commercialregisternumber>" heeft geen waarde in de ENUM NL context.
2. Een algoritme moet minimaal vertrouwd kunnen worden voor de periode van de registratie, volgens inschattingen die gangbaar zijn onder cryptografen. Deze inschattingen worden gebaseerd op voortgang van zowel computerkracht als kennis over de kraak van concrete technieken; hij zal daardoor aan verandering onderhevig zijn. De registry is verantwoordelijk voor de publicatie van de geaccepteerde ondergrenzen. Op moment van schrijven zouden als algoritmes alleen SHA1 of hoger mogen worden gebruikt. Key sizes zouden 1024 of hoger moeten zijn.
3. Voorgesteld wordt dat de Registry werkt met voorgeregistreerde certificaten die in het accreditatieproces door een validatieagent out-of-band aan de Registry worden aangeboden. De certificaten hoeven niet noodzakelijkerwijs door een certificate authority te worden uitgegeven, maar kunnen door de validatieagent zelf worden gegenereerd.

Onderbouwing van het voorstel

Van de optionele data moet alleen worden gecontroleerd of de Registrant van de ENUM-registratie overeenkomt met de nummerhouder. Adresgegevens of e-mailadressen kunnen wijzigen tijdens een registratie of nog niet gewijzigd zijn in de administratie van de nummerhouder. Het is voldoende de entiteit die als nummerhouder bekend staat, geautomatiseerd te controleren tegen de ENUM Registrant om te waarborgen dat validatie heeft plaatsgevonden. Dat wil niet zeggen dat in het validatieproces adresgegevens niet gecontroleerd hoeven te worden. Het geeft enkel aan dat die gegevens niet in het validatie token hoeven te worden opgenomen.

De keuze van SHA256 komt voort uit een recentelijke aanbeveling van de IETF waarin SHA1 als mogelijk toekomstig kwetsbaar werd bevonden.

Het gebruik van certificaten die uitgegeven zijn door een officiële certificate authority is een extra kostenpost voor Validatie Agenten. Aangezien er verwacht wordt dat het aantal Validatie Agenten klein blijft en er altijd een directe accreditatie door de Registry plaatsvindt, is het voldoende voor de Registry om direct door Validatie Agenten zelf uitgegeven certificaten te accepteren.

Alternatieven voor het voorstel

Meer optionele gegevens in het validatie token mag. Hetzelfde geldt voor het officieel uitgeven van certificaten. De vraag is dan wel of en welke optionele gegevens verplicht overeen moeten komen met de aanvraaggegevens van de ENUM-registratie. Daarnaast reist de vraag of de Registry naast een eigen controle van een fingerprint ook nog tegen een officiële certificatie autoriteit moet controleren. Indien dit het geval is, moet worden nagegaan welke officiële certificatie autoriteit dit dan moet zijn. Het gebruik van SHA1 kan toegestaan worden.

Voordelen

- Minder optionele gegevens zorgt voor minder kans op moeilijk te herstellen fouten bij een validatie.
- Eigen certificaten zorgen voor minder kosten.
- SHA256 zorgt voor betere beveiliging van het validatie token.

Nadelen

- Hoe minder gegevens tijdens de registratie (nogmaals) moeten worden geverifieerd, hoe zorgvuldiger het validatie proces dient te zijn.
- Eigen certificaten zorgen ervoor dat in het accreditatieproces van een Validatie Agent extra aandacht moet worden besteed aan een out of band uitwisseling van het certificaat.

Impact

REGISTRY:

De registratiesoftware die ENUM NL wil inzetten, ondersteunt het validatie token. De Registry moet een out of band proces afspreken met Validatie agenten om zijn certificaat te verkrijgen en te updaten. De Registry moet een fingerprint van het certificaat opslaan in de registratiesoftware om de validiteit van een validatie token te kunnen toetsen.

REGISTRAR:

De syntax van het validatie token heeft geen invloed op de Registrar. De Registrar moet het doorgegeven bij een registratie in het provisioning proces. Het is dan van belang dat de syntax, signatures en certificaten intact blijven.

REGISTRANT:

De syntax van het validatie token heeft geen invloed op de Registrant. Het kan in sommige validatiemethoden voorkomen dat een Registrant zijn validatie token zelf verkrijgt bij een validatie Agent (bijvoorbeeld bij zijn eigen nummerhouder) en dat hij het token dan moet doorgeven aan zijn Registrar waar hij zijn ENUM-registratie wil laten doen. Het is dan van belang dat de syntax, signatures en certificaten intact blijven.

NUMMERHOUDER:

De syntax van een validatie token heeft geen invloed op een nummerhouder.

VALIDATIE AGENT:

De Validatie Agent moet de hier besproken syntax van het validatie token genereren. Hij moet de besproken technieken ondersteunen. Hiervoor krijgt hij een toolkit ter beschikking.

OVERIGE BETROKKENEN:

De syntax van het validatie token heeft geen impact op overige betrokkenen.

Referentiemateriaal

Buitenlandse implementaties:

Het validatie token zoals beschreven in de uit te komen RFC wordt ondersteund door de registrysoftware van Oostenrijk, die het ook gebruiken voor hun validatieproces. Ook Ierland gaat gebruik maken van dezelfde software.

Bronmateriaal

- Voorstel validatie architectuur (.....)
- RFC 4725, Validatie architectuur (<http://www.ietf.org/rfc/rfc4725.txt>)
- Validatie token (<http://tools.ietf.org/id/draft-ietf-enum-validation-token-04.txt>)
- RFC 4930, EPP (<http://www.ietf.org/rfc/rfc4930.txt/>)
- RFC 3275 XML-DSIG (<http://www.ietf.org/rfc/rfc3275.txt>)