

Onderwerp: Technische Richtlijnen voor User ENUM in Nederland

Datum: 5 november 2007

Versie: 0.2b (levend document)

Auteurs: Deelnemers aan het ENUM Innovatie Platform

Contact: <http://www.enuminnederland.nl/>

Classificatie: Openbaar

Samenvatting

Dit document bevat technische richtlijnen voor ...
<<Editor's Note: meer samenvattingtekst nodig>>

Dit document is opgesteld door de deelnemers aan de Technische Werkgroep van het ENUM InnovatiePlatform Nederland.

Disclaimer

<<Disclaimer tekst, indien gewenst>>

Inhoudsopgave

1	Inleiding	3
1.1	Business rollen	3
1.2	Terminologie	4
1.3	Afkortingen	4
2	Technische eisen registrant (T1)	5
3	Opbouw en uitwisseling validatietoken (T2)	6
3.1	Vraagstelling	6
3.2	Voorstel ter beantwoording van de vraagstelling	6
3.3	Achtergrond van Opbouw en uitwisseling validatietoken	6
3.4	Scope Kader van de discussie	8
3.5	Onderbouwing van het voorstel	8
3.6	Voor- en nadelen van het voorstel	8
3.7	Impact	9
3.8	Referentiemateriaal	9
4	Geschikte validatietechnieken (T3)	10
4.1	Vraagstelling	10
4.2	Voorstel ter beantwoording van de vraagstelling	10
4.3	Achtergrond van validatietechnieken	11
4.4	Scope Kader van de discussie	12
4.5	Onderbouwing van het voorstel	12
4.6	Voor- en nadelen van het voorstel	13
4.7	Impact	13
4.8	Referentiemateriaal	13
5	Beschrijving registry / registrar interface (T4)	15
6	Hoofdprocessen te ondersteunen door Registry en Registrar (T5)	16
6.1	Vraagstelling	16
6.2	Voorstel ter beantwoording van de vraagstelling	16
6.3	Achtergrond van door Registry en Registrar te ondersteunen processen	16
6.4	Scope Kader van de discussie	17
6.5	Onderbouwing van het voorstel	17



6.6	Impact van het voorstel.....	17
6.7	Referentiemateriaal	18
7	IS en WHOIS voor ENUM (T6).....	19
7.1	Vraagstelling.....	19
7.2	Voorstel	19
7.3	Achtergrond IS en WHOIS voor ENUM	19
7.4	Scope Kader van de discussie	19
7.5	Onderbouwing van voorstel	20
7.6	Alternatieven voor het voorstel	20
7.7	Voor- en nadelen van het voorstel.....	20
7.8	Impact van het voorstel.....	20
7.9	Referentiemateriaal	21
8	DNSsec voor ENUM (T7)	22
9	Technische eisen Registry (T8).....	23
9.1	Inleiding	23
9.2	Begrippen	23
9.3	Operationeel beheer van de Name servers	23
9.4	Bereikbaarheid	23
9.5	Organisatorische eisen	23
10	DDI, Delegatie, nummerblokken en nummerextensies (T9).....	24
10.1	Introduction	24
10.2	Number Blocks	24
10.3	DNS delegation.....	24
10.4	Number extensions.....	24
10.5	Number Blocks and DDI	25
11	Referenties	26
12	BIJLAGEN	27
12.1	Mogelijke scenario's voor het gebruik van ENUM.....	27

1 Inleiding

Het ENUM Innovatie Platform Nederland is ...
<< Editor's Note: placeholder for scoping section >>

1.1 Business rollen

De volgende businessrollen worden binnen Public User ENUM onderscheiden (onderstaande rolbeschrijvingen zijn algemene beschrijvingen en geen formele beschrijvingen van rechten en plichten):

Registry

De Registry beheert de ENUM zone en de authoritative nameservers hiervan voor een land. Voor Nederland wordt deze rol ingevuld door ENUM NL. Deze partij beheert de nameservers voor de zone 1.3.e164.arpa. De Registry registreert ENUM registraties die onder haar domein vallen, en neemt de delegaties naar die zones op in de DNS.

Registrar

Een Registrar vraagt ENUM domeinregistraties aan bij de Registry uit naam van een nummergebruiker. Deze rol is vergelijkbaar met de rol die Registrars hebben in de wereld van ccTLD's en gTLD's. Directe registraties door nummergebruikers bij de Registry zijn niet mogelijk. Alle domeinregistraties verlopen via een Registrar.

Registrant

De ENUM Registrant is de "houder" van een ENUM-domein: De persoon of organisatie op wiens naam het domein geregistreerd is. De Registrant bepaalt waar het domein geregistreerd staat (bij welke Registrar en via welke nameservers) en welke verwijzingen (NAPTR records) in de zonefile opgenomen zijn. Alleen de nummergebruiker van het telefoonnummer waarop het ENUM-domein gebaseerd is, kan registrant zijn van dat ENUM-domein.

Nummerhouder

Nummerhouders zijn partijen die direct via de OPTA beschikking hebben over (blokken) telefoonnummers. Dit kunnen nummers voor eigen gebruik zijn (bijv. 0900 nummers) of nummers die doorgegeven worden aan eindgebruikers van telefoniediensten (bijv. mobiele of geografische telefoonnummers).

Nummergebruiker

De nummergebruiker is de persoon of organisatie die een telefoonnummer uit het Nederlandse nummerplan in gebruik heeft. Een ENUM-registratie voor een telefoonnummer kan enkel worden aangevraagd op naam van de gebruiker van dat telefoonnummer.

Validatieagent

Een Validatieagent valideert dat de aanvrager van een ENUM-registratie de nummergebruiker is van het telefoonnummer op basis waarvan de registratie wordt aangevraagd. Deze rol kan door verschillende partijen worden ingevuld en is niet gelimiteerd tot één agent. Afhankelijk van het type partij dat deze rol invult, kunnen verschillende validatiemethoden worden gebruikt (bijv: een nummerhouder kan in de rol van validatieagent interne validatiemethoden ontwikkelen voor eigen nummers, andere partijen kunnen call-back of sms-validaties opzetten. NB. validatie-methoden worden door het Innovatieplatform besproken, dit zijn slechts voorbeelden.)

DNS-Serviceprovider

Een DNS-Serviceprovider beheert de nameservers voor de ENUM DNS zones waarin de NAPTR records zijn opgenomen. Deze rol heeft een directe relatie met de Registrant en Registrar. De Registrant besteedt het technisch beheer van zijn ENUM zone vaak uit aan een DNS-Serviceprovider. De Registrar heeft de rol om bij registratie te controleren of de DNS-Serviceprovider voldoet aan de technische eisen. Vaak zijn Registrar en DNS-Serviceprovider dezelfde partij, soms zijn Registrant en DNS-Serviceprovider één en dezelfde, maar ook situaties met 3 afzonderlijke partijen komen voor.



1.2 Terminologie

1.3 Afkortingen



2 Technische eisen registrant (T1)

Uitwerking van dit onderdeel volgt op een later tijdstip

3 Opbouw en uitwisseling validatietoken (T2)

3.1 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?

3.2 Voorstel ter beantwoording van de vraagstelling

- Voor de optionele data wordt voorgesteld om alle adresgegevens niet verplicht te stellen in het validatie token. Ook het "<commercialregisternumber>" heeft geen waarde in de ENUM NL context.
- Als algoritmes mogen alleen SHA256 of hoger worden gebruikt en geen SHA1 met key sizes van 2048 of hoger.
- Voorgesteld wordt dat de Registry werkt met voorgeregistreerde certificaten die in het accreditatie proces door een validatie agent out of band aan de Registry worden aangeboden. De certificaten hoeven niet noodzakelijkerwijs door een certificate authority te worden uitgegeven, maar kunnen door de validatie agent zelf worden gegenereerd.

3.3 Achtergrond van Opbouw en uitwisseling validatietoken

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/xmenc#sha256"/>
<DigestValue
>VxqsBxSNPFwPAUICHTs3g3DehcxnB1dqUz+GypLZ0k=</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>
QKqphKRNPokVZFbenje+HZZV+RLrNweGnlWBw7ngAtH+rtuslR8LhLmC4DIBb9V
HvKlti+7zLm3vgYsqfHH8q3jC1mF XUluLlPqtpJs+xAHAJDzZ+vmsF/q2lgrS
K0uMmKuU5V1gydDBOvlpcJx+PrPYyXYZSjQXkWknK8=</SignatureValue>
<KeyInfo>
<X509Data>
<X509Certificate>
MIIDZCCAs+gAwIBAgIBBDANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJBVDEP
MA0GA1UEBxMGVmlbm5hMRQwEgYDVQQKEwTC0ZIIENlcnRzLjEhMBkGA1UEAxMS
Q0VSVFUyYm9maC5wcm12LmF0MSEwHwYJKoZIhvcNAQkBFhJjZjJ0c0Bib2Z0LnBy
aXYuYXQwHhcNMjQwNzIwMTMxNTA5WWhcNMDUwNzIwMTMxNTA5WjB/MQswCQYDVQQG
EwJBVDEDEKMAgGA1UECBMBLETPMA0GA1UEBxMGVmlbm5hMR0wGwYDVQQKExRBY2I1
IEVOU0ogVmFsaWRhdGlvbjeQMA4GA1UEAxMHYWNtZS1WRTEIMCAGCSqSb3DQeJ
ARYTbm9ib2R5SQGVudW0tYWwNtZS5hdDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEArlPcjMFC54/zwtzsdQXGxUtodJT9r1qGI2IQPNjLvtPjg93+7o5SIOsZGSpg
zWbtDAV5qc7PHZUWUlyf6MbM5qSgQDVrjNRhTosNtyqmwi23BH52SKkX3P7eGit
LmqEKiUZRxZz6upRbtcpvKSwmXitW4zXZnkVHYJZ2HuMcAwaEAaOB/DCB+TAJ
BgNVHRMEAJAAMCwCGWCGSAGG+EIBDQqFh1PcGVuU1NMIEdlbmVyyXRIZCBBDXJ0
aWZpY2F0ZTAdBgNVHQ4EFQYUyK4otQtv6KdSIBMOPT5Ve18JgwgZ4GA1UdIwSB
IjCBk4AUvFpadpm0HhmZx2iAVumQTWgnG2ehEKr2MHQxCzAJBgNVBAYTAkFUMQ8w
DQYDVQQHEwZwaWVubmExFDASBgNVBAoTC0JPRkkgQ2VydHMuMRswGQYDVQQDEwJX
RVJUU5ib2Z0LnByaXYuYXQwIHRlZjBkqhkiG9w0BQCQEWEmNlcnRzQjGvZmgucHJp
di5hllIBADANBgkqhkiG9w0BAQQFAAOBqCB9CHBnlUhrdic4h5Ar4hdXjHSQkDH
sJWd+MYrNcuSrv3TIOsUkUgNpNNhmKZPtXqfy3388IRdJtJiLWXSOB/xIZHOM9I
MwvKYwhcpQ9UdM/w7VpXQqf+CEjOXSyqxGw65UsHIOijgiG/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.

3.4 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.

3.5 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

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.

3.6 Voor- en nadelen van het voorstel

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.

3.7 Impact

Het voorstel heeft de volgende impact op de verschillende rollen:

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.
VALIDATIEAGENT:	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.

3.8 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

- RFC 4725, Validatie architectuur
- Validatie token
- RFC 4930, EPP
- RFC 3275 XML-DSIG

4 Geschikte validatietechnieken (T3)

4.1 Vraagstelling

Op welke manier kunnen validatietechnieken worden ontwikkeld, en hoe dienen voorstellen voor nieuwe validatietechnieken te worden beoordeeld? Hoe kan een naar later blijkt mogelijk ondeugdelijke validatietechniek worden ingetrokken zonder dat dit gevolgen heeft voor andere validatietechnieken of validatieagenten?

4.2 Voorstel ter beantwoording van de vraagstelling

Iedere Validatie Agent dient vooraf een validatietechniek te registreren bij de Registry. In de registratie van een validatietechniek dient te worden opgenomen:

- De Validatie Agent die de techniek toepast.
- Een unieke code voor de specifieke validatie techniek van die validatie agent.
- Nummerreeksen waarop de validatie techniek van toepassing is.
- Een omschrijving van de validatie techniek, met daarin de handelingen die worden gedaan, de specifieke gegevens die worden gecontroleerd, de manier waarop de partijen die betrokken zijn en de relatie daartussen, de gegevens van de validatie die worden gearhiveerd of herleidbaar zijn en de criteria voor een succesvolle validatie.

De Registry zal een eerste evaluatie doen van de techniek. De volgende uitkomsten zijn hierbij mogelijk:

- De validatietechniek is voorlopig betrouwbaar en wordt geaccepteerd. Bijvoorbeeld in geval van validatie via COIN
- De validatietechniek is overduidelijk onbetrouwbaar of voldoet niet aan de eisen en wordt afgewezen.
- De validatietechniek is onvolledig of onvolledig beschreven en wordt voorlopig afgewezen.
- De Registry heeft twijfels over de validatietechniek en legt, na toestemming van de agent, de techniek ter evaluatie voor aan een ENUM consultatieplatform.

Indien de Registry de validatietechniek als voorlopig betrouwbaar aanmerkt, zal de validatietechniek in het registratiesysteem worden opgenomen. Vanaf dat moment kunnen er registraties worden gedaan die zijn gevalideerd door de gespecificeerde Validatie Agent volgens de gespecificeerde techniek.

Indien later blijkt dat een geregistreerde techniek heeft geleid tot een onjuiste validatie, of aangetoond wordt dat de techniek kan leiden tot een onjuiste validatie, hetzij, maar niet alleen doordat bijvoorbeeld:

- Het nummerplan is gewijzigd.
- De techniek niet meer kan worden uitgevoerd.
- De Validatie Agent zich niet houdt aan de door hem omschreven procedure.
- Betrokken partijen hebben aangegeven de techniek niet langer te ondersteunen.
- De Validatie agent geen geldig contract met de Registry meer heeft, failliet is, of niet meer bestaat.
- De procedure tot fouten kan leiden die bij acceptatie nog niet bekend waren.
- De procedures voor ENUM registraties gewijzigd zijn.

dan kan de Registry overgaan tot:

- intrekken van de specifieke validatietechniek voor de specifieke validatie agent
- intrekken van alle validatietechnieken voor de specifieke validatie agent, en opzeggen van het validatie agent contract
- intrekken van alle vergelijkbare validatietechnieken voor alle validatie agenten.

4.3 Achtergrond van validatietechnieken

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 zal worden uitgevoerd door een partij die de rol als Validatie Agent op zich neemt.

Dit kan een partij zijn die ook eveneens Registrar of nummerhouder is, maar het zou ook een partij kunnen zijn die enkel deze rol aanneemt om deze dienst aan te bieden aan meerdere Registrars of zelfs aan Registranten.

Dit voorstel kijkt naar een aantal mogelijke technieken waarmee een validatie gedaan kan worden. Echter, het is, voornamelijk op zoek naar een framework waarbij een Validatie Agent zelf ook andere validatietechnieken kan ontwikkelen.

De rol van validatie Agent zit op hetzelfde niveau als de Registrars, en is niet noodzakelijkerwijs een rol die door een specifieke partij moet worden vervuld. Ook moet worden voorkomen dat Validatie Agenten onderling de markt van Registrars verdelen, of een voorkeur uitspreken voor een bepaald type Registrar. De overheid wil de markt voor ENUM Registrars zo open en transparant mogelijk houden om concurrentie te bevorderen. Het is dan vanzelfsprekend om de Registrars een vrije keuze te geven in de validatie agent die zij wensen te gebruiken. De verwachting is dat Validatie Agenten onderling met elkaar concurreren in het aanbieden van een zo efficiënt mogelijk validatieproces. Het blijft daarbij belangrijk dat de validatie zelf nog steeds betrouwbaar en correct plaatsvindt.

Voor de validatie van verschillende telefoonnummers kunnen verschillende validatietechnieken meer of minder geschikt zijn. Zo kan een geografisch nummer zeer efficiënt worden gevalideerd door de nummerhouder die de nummergebruiker als eigen klant heeft. Deze methode zal echter niet werken voor telefoonnummers die zijn uitgegeven voor prepaid mobiele SIM-kaarten, of nummers en waarvan de nummerhouder de gegevens van de klant niet kent. Omgekeerd zal een SMS-validatie wel geschikt zijn voor mobiele nummers, maar geografische nummerblokken weer niet ondersteunen. Tevens is het van belang dat er meerdere validatie technieken bestaan om te voorkomen dat een individuele partij een validatie kan blokkeren en daarmee de open en transparante markt en de vrije keuze van een Registrant voor een Registrar kan frustreren.

Onderstaand worden een aantal voorgestelde validatie technieken kort beschreven.

1. Validatie via COIN

In Nederland zijn alle telecomoperators aangesloten bij de vereniging COIN, de instelling die onder andere porteringsverzoeken voor nummerbehoud faciliteert. Een operator die aangesloten is bij COIN kan zo de nummerhouder informatie van een telefoonnummer laten controleren door een porteringverzoek te doen. Enkele kleine operators zijn niet zelf aangesloten bij COIN, maar maken gebruik van een intermediair die wel is aangesloten bij COIN.

In plaats van een porteringsverzoek zou COIN ook een ENUM-validatieverzoek kunnen ondersteunen, zodat aangesloten leden direct, en niet aangesloten leden via een intermediair, de validatie van een telefoonnummer kunnen uitvoeren. Dit is een betrouwbare vorm van validatie, die direct bij de nummerhouder die het nummer onder zijn/haar beheer heeft, wordt gedaan. Nummerhouders hebben zelf een groot belang bij een juiste validatie.

Deze techniek van validatie zal niet voor alle nummers werken, waardoor dit niet de enig toegestane vorm van validatie kan zijn.

2. Validatie door nummerhouder

Een nummerhouder die tegelijkertijd validatie agent is, zou voor haar eigen klanten een validatie kunnen verzorgen. Hetzij omdat zij eveneens ENUM Registrar zijn voor eigen klanten, hetzij zij dit willen aanbieden als (betaalde of gratis) dienstverlening richting eigen klanten. Een dergelijke validatie tegen de eigen gegevens is een betrouwbare validatie. Een nummerhouder kan aan haar eigen klanten een validatie token uitdelen waarmee de nummergebruiker vervolgens bij een willekeurige Registrar zijn ENUM registratie kan doen. Een dergelijk validatie token kan op verzoek worden verstrekt aan de nummerhouder via bijvoorbeeld e-mail, of standaard worden aangeboden op bijvoorbeeld een online portal of online gepubliceerde telefoonrekening.

3. Algemene validatie

In het geval de gegevens van de nummergebruiker niet bekend zijn bij een nummerhouder of als de nummerhouder niet kan of wil meewerken aan een validatie, omdat deze bijvoorbeeld geen validatie agent is, bestaan er technieken die betrouwbaar genoeg zijn voor validatie zonder tussenkomst van de nummerhouder.

Allereerst kan een handmatige controle via een originele, recente telefoonrekening of een telecommunicatie contract dat door de nummergebruiker aan een validatie agent beschikbaar wordt gesteld, voldoende betrouwbaar zijn voor validatie.

Ten tweede kan bij mobiele nummers een validatie via SMS uitstekend betrouwbaar worden uitgevoerd. Net als bij online bankieren via een TAN-code, kan een Validatie Agent bij een verzoek tot validatie per SMS een code sturen naar het mobiele nummer. Na invoering en controle van de gegevens en de code op een website geeft deze een validatie token.

Dit zijn slechts enkele voorbeelden van validatie technieken die gebruikt zouden kunnen worden.

De Registry bevindt zich echter niet in een positie om voor deze markt implementeerbare oplossingen te ontwikkelen.

Wel heeft de Registry als taak om te bewaken of de validatietechnieken die door Validatie Agenten worden gebruikt voldoende betrouwbaar zijn en in geval van klachten over onjuiste validatie een agent daarop aan te spreken of de technieken die niet betrouwbaar zijn gebleken te verbieden. De Registry heeft echter geen voorkeur voor één specifieke validatietechniek of Validatie Agent.

Tenslotte kan gemeld worden dat er in de telecommunicatie-industrie vaker behoefte is aan eenduidige validatie van nummergebruikers bij telefoonnummers. Ook bij bijvoorbeeld DSL, of micropayments (betalen via mobiel) bestaat de behoefte om een nummergebruiker of contractant van een telefoonnummer te kunnen valideren. Een goede validatietechniek moet dus ook algemener en met andere business cases in gedachten, ontwikkeld worden.

4.4 Scope | Kader van de discussie

In het afgesloten convenant tussen de Nederlandse overheid en ENUM NL, als ook in het achterliggende NLEG rapport staat een voorgesteld registratiemodel beschreven. Hierin is eveneens de voorwaarde opgenomen dat een registrant vrij moet zijn in de keuze van zijn (ENUM) Registrar. Deze voorwaarde staat niet ter discussie, net als de bepaling wie als Registrar of Validatie Agent mag optreden.

De vraag of er zondermeer gevalideerd moet worden, staat eveneens niet ter discussie. Het NLEG rapport stelt validatie verplicht, maar laat de keuze hoe deze validatie wordt belegd nog vrij.

Welke validatietechnieken geschikt zijn voor validatie is afhankelijk van de validatie-architectuur, het validatie token en de voorwaarden waaraan een Validatie Agent moet voldoen. Geprobeerd wordt een framework te presenteren dat deze afhankelijkheid zo klein mogelijk maakt en de mogelijkheid biedt om meerdere validatietechnieken en Validatie Agenten in de markt te laten opereren.

Voorts zijn specifieke validatie technieken afhankelijk van het Nederlandse nummerplan, de toegestane nummers voor gebruik in ENUM en de manier waarop nummers door de nummerhouder worden uitgegeven.

4.5 Onderbouwing van het voorstel

De Registry kan onmogelijk vooraf alle denkbare validatietechnieken in kaart brengen. Validatie is een taak die ook aan de markt kan worden overgelaten, hetgeen weer kan zorgen voor een vrije markt onder Registrars. De mogelijkheid tot het intrekken van een validatietechniek zorgt voor een betrouwbare validatie. In combinatie met hervalidatie leidt dit tot uitsluitend correct gevalideerde ENUM-registraties op termijn. Constatering van een onjuist gevalideerd nummer zal onmiddellijk leiden tot doorhaling van een op dat nummer gebaseerde ENUM-registratie, maar ook andere nummers die volgens dezelfde techniek zijn gevalideerd mogen bij hervalidatie niet meer door middel van deze desbetreffende techniek worden gevalideerd.

Alternatieven

Sommige validatie technieken kunnen centraal worden georganiseerd en bij één partij worden ondergebracht. Denk hierbij aan een validatie via COIN of het valideren van mobiele nummers via SMS.

ENUM NL ziet het niet als haar taak om de rol van validerende partij te vervullen, daar hier mogelijk concurrerende validatie technieken tegenover kunnen staan. Zij heeft echter geen bezwaar wanneer andere marktpartijen deze rol op zich nemen.

Een andere mogelijkheid zou zijn om enkel telecom operators, eventueel verplicht opgelegd door de OPTA, als validatie agent te laten optreden. Naast de vraag of telecom operators daar welwillend tegenover staan, rest de vraag of er voldoende concurrentie mogelijkheden blijven bestaan.

4.6 Voor- en nadelen van het voorstel

Voordelen

- Het registreren van validatietechnieken zorgt ervoor dat de Registry een specifieke validatietechniek of Validatie Agent als ongeldig kan verklaren zonder dat andere valide technieken of agenten daardoor worden beïnvloed.
- Het vooraf moeten registreren van een voorgestelde validatietechniek door een Validatie Agent zorgt ervoor dat een duidelijk foute validatietechniek niet kan worden gebruikt voor een registratie.
- Het is voor een Registrar en Validatie Agent duidelijk welke validatietechnieken geldig zijn en gebruikt kunnen worden.
- Het toepassen van meerdere validatietechnieken en agenten zorgt ervoor dat bij het wegvallen van een techniek of agent alternatieven blijven bestaan.

Nadelen

- Een voorgestelde validatietechniek moet vooraf worden beoordeeld en goedgekeurd door de Registry, eventueel na consultatie van het ENUM platform. Tijdens deze evaluatie kan een voorgestelde techniek nog niet worden gebruikt voor registraties.
- Er moeten proces worden afgesproken tussen de Registry en Validatie Agenten om een validatietechniek te registreren. De Registry zal expertise moeten inzetten om een techniek te evalueren, hetgeen, een handmatig, dus tijdrovend en kostbaar proces is.
- Er is vooraf geen eenduidige definitie te geven van een betrouwbare validatietechniek en uitvoering.

4.7 Impact

Het voorstel heeft de volgende impact op de verschillende rollen:

REGISTRY:	De Registry moet extra expertise en processen inzetten om een validatietechniek te evalueren en registreren.
REGISTRAR:	De Registrar moet vooraf één of meerdere geschikte Validatie Agenten kiezen die voor zijn markt de validatie kunnen verzorgen.
REGISTRANT:	De Registrant moet op de hoogte zijn van het validatieproces. Afhankelijk van de gebruikte validatietechniek en validatieagent kan dit een ander proces zijn. Vooraf is het voor de Registrant niet duidelijk welk proces er voor een ENUM registratie geldt. Dit proces is namelijk afhankelijk van de Registrar die wordt gekozen.
NUMMERHOUDER:	Een nummerhouder kan mee werken aan de validatie van zijn nummers. Dit is echter niet verplicht.
VALIDATIEAGENT:	De Validatie Agent moet een voorgestelde validatietechniek vooraf aanmelden bij de Registry,. Vervolgens moet de Registry zich aan die omschrijving blijven houden. Een verandering in handelswijze moet door een Validatie Agent opnieuw worden aangemeld bij de Registry.
OVERIGE BETROKKENEN:	Nummergebruikers zonder ENUM registratie worden beter beschermd tegen een foute validatie. Bovendien wordt de integriteit tussen de ENUM Registrant en nummergebruiker versterkt.

4.8 Referentiemateriaal

Buitenlandse implementaties:

Een vergelijkbaar model voor registratie van validatie technieken wordt al 2 jaar in productie gebruikt door de ENUM Registry in Oostenrijk. Groot verschil is dat een twijfelachtige validatie techniek standaard wordt geaccepteerd tot bewezen is dat deze niet werkt. Gedurende deze twee jaar is nog geen enkele techniek ingetrokken.

Bronmateriaal:

- RFC 4725 - <http://www.ietf.org/rfc/rfc4725.txt>
- Validatie token - <http://tools.ietf.org/id/draft-ietf-enum-validation-token-04.txt>
- NLEG rapport - <http://www.enumnederland.nl/files/ENUMinNederland.pdf>
- Convenant EZ - ENUM NL - <http://www.ez.nl/dsc?c=getobject&s=obj&objectid=151281&ldsname=EZInternet&isapidir=/gvisapi/>



5 Beschrijving registry / registrar interface (T4)

Uitwerking van dit onderdeel volgt op een later tijdstip

6 Hoofdprocessen te ondersteunen door Registry en Registrar (T5)

6.1 Vraagstelling

Welke hoofdprocessen dienen te worden ondersteund door Registry en Registrar?

6.2 Voorstel ter beantwoording van de vraagstelling

Een limitatief voorstel voor in de te richten processen is:

Registrars

- Aanmelding nieuwe Registrar
- Wijziging gegevens Registrar
- Opheffing Registrar / Beëindiging overeenkomst

Validatie (verder uit te werken na uitkomst van de discussie t.a.v. de inrichting van Validatie – dit gebeurt binnen een separaat thema):

- Validatieagent:
 - Aanmelding Validatieagent
 - Wijziging gegevens Validatieagent
 - Opheffing Validatieagent
- Validatiemethode:
 - Aanmelding validatiemethode
 - Opheffing/blokkering validatiemethode

ENUM-domein

- Registratie nieuwe domeinnaam:
 - Identificatie van de Registrant door Registrar
 - Validatie nummer en nummergebruiker
- Wijziging bestaande registratie:
 - Nameservers
 - Contactgegevens Registrant (m.u.v.registrant naam)
- Verhuizing naar andere Registrar
- Opheffing registratie
- Omzetting/overdracht registratie naar nieuwe Registrant
- Hervalidatie / verlenging
- Quarantaine registratie

Registry

- Periodieke facturering aan Registrars
- Levering rapportages/overzichten domeinen en mutaties aan Registrars
- Afhandeling support en storingsmeldingen

6.3 Achtergrond van door Registry en Registrar te ondersteunen processen

ENUM is een dienst die in samenwerking tussen (voornamelijk) Registry en Registrars geleverd wordt. Daarbij is het van belang afstemming te bereiken over de processen die ingericht moeten worden voor het operationaliseren van de dienst.

De processen die gebruikt worden voor TLD-domeinnaamregistraties vormen hiervoor de basis. Deze processen kunnen echter niet zonder meer worden overgenomen; er bestaan wel degelijk verschillen. Een ENUM-domeinnaam is in tegenstelling tot een TLD-domeinnaam geen vrij te kiezen naam: Een registratie kan enkel gedaan worden op basis van een telefoonnummer uit een bestaand nummerplan en

enkel door de gebruiker van dat telefoonnummer. De registratie-aanvraag van een domein moet hierop gevalideerd worden.

Zie 1.1. Business Rollen voor rolbeschrijvingen van de verschillende partijen.

6.4 Scope / Kader van de discussie

Doel van deze discussie is consensus te bereiken in de keuze van de in te richten processen. De invulling hiervan (de daadwerkelijke inrichting, de interface-definities en procedures, de opzet van voorwaarden en reglement en handhaving hiervan) valt buiten de scope van dit thema. Wanneer deze 'invulling' op bepaalde onderdelen discussie behoeven, dan worden separate thema's ter discussie aangeboden.

De processen die zich zuiver tussen Registrar en Registrant afspelen worden in dit thema niet expliciet genoemd. Deze processen zijn vrijelijk in te vullen door de Registrar (met inachtnaam van de voorwaarden en het reglement van de Registry).

De processen die door de Validatieagent ondersteunt dienen te worden zijn niet binnen dit thema opgenomen. (De opzet en inrichting van Validatie is nog geen helder gegeven – zie "afhankelijkheden".)

Afhankelijkheden

- Validatie: Validatie, hervalidatie en technieken hiervoor worden in een apart thema besproken. De uitkomsten van die discussie zijn nodig om tot verdere uitwerking van de processen over te gaan.
- Functionaliteit registratie-software: Bij de beschrijving van de in te richten processen wordt aangenomen dat de registratiesoftware deze ondersteunen (op basis van de operationele status van andere registries die van identieke software gebruik maken). Deze aanname kan pas na implementatie en configuratie van de software op de systemen definitief worden gestaafd.
- Geschillenregeling: Bij bepalen van de geschillenregeling (separaat discussiethema) kunnen mogelijk additionele processen aangedragen worden.

6.5 Onderbouwing van het voorstel

Onderstaande processen worden niet ingericht:

- Actieve verlenging van registratie. Dit kan worden ingevuld op basis van periodieke hervalidatie.
- Wijziging domeinnaam ENUM-registratie. Dit komt neer op het registreren van een nieuwe domeinnaam en het opheffen van de bestaande domeinnaam.

Het inrichten van deze processen vraagt relatief veel aanvullende regulering en voorwaarden, terwijl de uitkomst via andere processen ook verkregen kan worden.

Verhuizing naar een andere Registrar kan op basis van deze argumenten ook worden vervangen door een opheffing i.c.m. nieuwe registratie. Dit proces wordt wel separaat ingericht om continuïteit van registratie en bereikbaarheid te kunnen leveren.

Om deze reden wordt de omzetting van een bestaande registratie naar een nieuwe Registrant ook gefaciliteerd. Voorwaarde daarbij is wel dat de nieuwe Registrant een geldige validatie overlegt tijdens de aanvraag.

Een domeinregistratie moet in quarantaine gezet kunnen worden bij de uitvoering van een geschillenregeling (zie ook discussiethema geschillenregeling): Nadat een registratie opgeheven wordt als gevolg van een (terecht) bezwaarschrift geldt een quarantaineperiode voor een nieuwe registratie (om te voorkomen dat de valide gebruiker van het telefoonnummer op kosten gejaagd wordt door nieuwe, onterechte, registratie-aanvragen op basis van datzelfde nummer).

6.6 Impact van het voorstel

Het voorstel heeft de volgende impact op de verschillende rollen:

REGISTRY: Biedt hiermee voldoende mogelijkheden voor het aanvragen en beheren van

	ENUM-domeinen aan Registrars. De registry zal bovenstaande processen moeten ondersteunen.
REGISTRAR:	Kan met behulp van bovenstaande processen ENUM-domeinen beheren voor Registrants.
REGISTRANT:	n.v.t.: Document beschrijft processen tussen Registrar en Registry
NUMMERHOUDER:	n.v.t.: Document beschrijft processen tussen Registrar en Registry
VALIDATIEAGENT:	n.v.t.: Document beschrijft processen tussen Registrar en Registry
OVERIGE	n.v.t.: Document beschrijft processen tussen Registrar en Registry
BETROKKENEN:	

6.7 Referentiemateriaal

Referentie Buitenlandse implementaties:

Het Registrar-model is generiek identiek aan buitenlandse toepassingen. De relaties met de Validatieagent worden wisselend ingevuld en zijn voor Nederland nog nader te bepalen.

Bronmaterialen:

- RFC 4725 - <http://www.ietf.org/rfc/rfc4725.txt>
- NLEG rapport - <http://www.enuminnederland.nl/files/ENUMinNederland.pdf>
- Convenant EZ - ENUM NL - <http://www.ez.nl/dsc?c=getobject&s=obj&objectid=151281&ldsname=EZInternet&isapidir=/qvisapi/>

7 IS en WHOIS voor ENUM (T6)

7.1 Vraagstelling

Welke gegevens van een ENUM registratie dienen publiek gepubliceerd te worden, en is een whois interface wenselijk voor ENUM ?

7.2 Voorstel

De Registry zou geen gegevens van de ENUM registratie openbaar moeten maken anders dan voor de volgende doelen:

- Eventuele technische problemen betreffende de werking van het Internet op te lossen
- De geldigheid(sduur) van een validatie te kunnen achterhalen

Gegevens die hiervoor gepubliceerd kunnen worden zijn:

- Een technisch contactpersoon van de ENUM zone
- De gegevens van de Registrar die de registratie heeft uitgevoerd
- De vervaldatum van de huidige validatie

Niet gepubliceerd mogen worden:

- Gegevens van de Registrant van de ENUM zone

De gegevens zouden gepubliceerd moeten worden via een techniek die geautomatiseerd verzamelen van die gegevens verhindert, maar individuele bevraging toestaat.

Een whois interface voor ENUM registraties is daardoor niet wenselijk.

7.3 Achtergrond IS en WHOIS voor ENUM

Het grote verschil tussen een gewone domeinnaam en een ENUM domeinnaam is de wijze van uitgifte. Waar een gewone domeinnaam normaliter wordt uitgegeven op basis van first-come-first-serve wordt een ENUM domeinnaam slechts uitgegeven op basis van een bestaand gebruikersrecht van het reeds uitgegeven E.164 telefoonnummer. Bij een gewone domeinnaam wordt het gebruikersrecht dus bepaald door de registratie bij de registry, waar bij een ENUM domeinnaam dit gebruikersrecht al door de E.164 nummer uitgever wordt bepaald.

Voor het achterhalen van het gebruikersrecht en de verantwoordelijkheid voor een domeinnaam stelt een registry vaak een openbare whois interface beschikbaar, die enkel voor specifieke doelen geraadpleegd mag worden. Voor de .nl registry volgen die doelen bijvoorbeeld uit de WBP regeling van SIDN, artikel 2.1.e:

- de oplossing van eventuele technische problemen betreffende de werking van het Internet;
- de aanvraag van (nog vrije) domeinnamen;
- de bescherming van intellectuele eigendomsrechten, en;
- de voorkoming en bestrijding van illegale en schadelijke op inhoud op het Internet.

Op een ENUM domeinnaam zijn een aantal van deze doelen niet toepasbaar.

Het is voor een registry niet verplicht om een dergelijke openbare whois interface aan te bieden. Het is een best practice die door veel registries wordt gevolgd, en als deze wordt gevolgd dan voldoet de interface aan het standaard whois protocol. Of en welke gegevens worden gepubliceerd is een individuele keuze van de registry, die daarmee een geautomatiseerde oplossing biedt voor talloze vragen die zij anders afhankelijk van lokale wetgeving op een andere manier zou moeten beantwoorden.

7.4 Scope / Kader van de discussie

De discussie beperkt zich tot de vraag voor welk doel, welke gegevens volgens welke interface door de registry gepubliceerd zouden moeten worden voor een ENUM registratie. Niet ter discussie staan de

doelen voor andere domeinnamen, de gegevens of de wijze van publiceren door een uitgever van e.164 nummers of de wettelijke verplichtingen die daarop gelden.

7.5 Onderbouwing van voorstel

De Registrant van een ENUM registratie komt 1 op 1 overeen met de gebruiker van het bijbehorende E.164 telefoonnummer. De gebruiker van het telefoonnummer is de primaire databron waar de gegevens van de ENUM Registrant uit worden herleid. Vragen over de ENUM Registrant zijn dus te herleiden naar de gebruiker van het telefoonnummer. Gegevens die worden gepubliceerd over de gebruiker van een telefoonnummer zijn gebonden aan wettelijke bepalingen, die worden bewaakt door de uitgever van het nummer. Door geen gegevens te publiceren over de ENUM Registrant wordt voorkomen dat deze wettelijke bepalingen worden overtreden, of de bewaking door de nummeruitgever wordt aangetast. Indien iemand gegevens van een ENUM Registrant en dus een nummergebruiker wenst te achterhalen, dan kan dat volgens de geldende regels bij de primaire databron waar de gegevens van de nummergebruikers worden bijgehouden.

Gegevens die specifiek zijn voor de ENUM registratie, die niet door de nummeruitgever worden bijgehouden, en die nodig zijn voor het oplossen van technische of registratie problemen kunnen alleen via de Registry worden achterhaald.

Een whois interface is niet afdoende te beveiligen tegen geautomatiseerde bevraging. Zeker omdat telefoonnummers, en dus ENUM zones, een eindige reeks vormen, zou misbruik door het inzetten van botnets kunnen leiden tot ongewenst verzamelen van alle ENUM registratie data die publiek gesteld wordt voor andere doelen.

Een technisch contactpersoon van een zone kan ook gevonden worden via het RNAME veld van de zone in de DNS.

Een Registrar en vervaldatum van een ENUM registratie zou gepubliceerd kunnen worden op de website van de ENUM registry, met een techniek als Captcha om te zorgen dat alleen menselijke bevragingen mogelijk zijn.

Voor een Registrant kan het wenselijk zijn om de Registrar en vervaldatum van zijn eigen ENUM registratie te kunnen controleren.

7.6 Alternatieven voor het voorstel

Het zou mogelijk zijn om een whois interface beschikbaar te stellen met enkel de gegevens van de Registrar daarin zonder adresgegevens. De meerwaarde van een dergelijke commandline interface voor incidentele bevragingen is echter niet aanwezig.

De Registry zou ook helemaal geen gegevens kunnen publiceren, en vragen rechtstreeks kunnen doorverwijzen naar de nummerhouder van het telefoonnummer.

7.7 Voor- en nadelen van het voorstel

Voordelen:

- De privacy van een ENUM Registrant/nummergebruiker blijft gewaarborgd.
- Problemen met de ENUM registratie kunnen zonder tussenkomst van Registry of nummerhouder worden opgelost.

Nadelen:

- Voor ENUM domeinen wordt een afwijkende interface gebruikt.

7.8 Impact van het voorstel

Het voorstel heeft de volgende impact op de verschillende rollen:

REGISTRY:	De Registry moet de voorgestelde interface beschikbaar stellen.
REGISTRAR:	De gegevens van een Registrar zullen publiek beschikbaar zijn. De Registrar dient zijn medewerking te verlenen bij het oplossen van problemen.
REGISTRANT:	De Registrant kan zijn registratie controleren bij de Registry.
NUMMERHOUDER:	Een nummerhouder blijft het aanspreekpunt voor vragen over de gebruiker van een telefoonnummer.
VALIDATIEAGENT:	Dit vraagstuk heeft geen impact op de validatie agent.
OVERIGE	Rechtspersonen die een klacht willen indienen over een ENUM registratie kunnen via de interface achterhalen wie de registratie heeft verzorgd of wie technisch verantwoordelijk is voor de ENUM zone.
BETROKKENEN:	

7.9 Referentiemateriaal

Buitenlandse ENUM registries publiceren geen gegevens over de Registrant. De Oostenrijkse ENUM registry registreert niet eens gegevens van de Registrant, en verwijst conflicten direct door naar de Registrar. In geval er gegevens worden gepubliceerd betreffen deze enkel de gegevens van de Registrar.

Bronmaterialen

- WBP regeling SIDN - http://www.sidn.nl/ace.php/p,727,2694,18752,Wbp-regeling-SIDN_pdf
- Whois protocol, RFC 3912 - <http://www.ietf.org/rfc/rfc3912.txt>

8 DNSsec voor ENUM (T7)

The ENUM specification [RFC3761, section 6.1] advises the use of DNSSEC to ameliorate a set of threads. DNSSEC allows for verification of authenticity and integrity of the data provided through the DNS. The procedures, described elsewhere in this document, assure the validity of the data that is published in the DNS. The certainty of the correctness of the data due to the registration process and the certainty that data has not been tampered during its way through the DNS, allows for a high trust in the 1.3.e164.arpa domain. In other words deployment of DNSSEC on the ENUM tree improves its reliability, the sense of security for end-users, and may allow for new innovations.

With respect of the operational procedures this document sets a number of prerequisites that will need further expansion by the registry.

- The Tier-1 MUST deploy DNSSEC for 1.3.e164.arpa according to and relying on best practices in the industry. The Tier-1 SHOULD store its Key Signing Key on tamper proof cryptographic hardware devices.
Actual implementation of DNSSEC MAY be delayed until stable operation of the 1.3.e164.arpa is established but not later than the start of 2009.
- The Tier-1 MUST request a secure delegation from the Tier-0 as soon as DNSSEC is available in e164.arpa.
- Tier-2 providers SHOULD deploy DNSSEC on their zones.
- Tier-2 providers that deploy DNSSEC SHOULD use different Key and Zone Signing keys and should set the "SEP" flag on their Key Signing Keys.
- The Tier-1 provider enables key signing key rollovers by Tier-2s.
- In order to allow for regeneration of DS RRs in case new digest algorithms are being made available the Registry will store the public keys (DNSKEY) instead of their digests (DS).
- Exchange of DNSKEY information between registrar and registry will be based on an EPP based interfaces for key-exchanges [RFC4114 and references therein]. [OK: if EPP is used as the exchange mechanism elsewhere]
- The registry will validate if a public key delivered by the registrar is available in the DNS zone. Public keys provided to the registry that are not in the DNS at the time of the data exchange MUST not be published in the DNS.

9 Technische eisen Registry (T8)

9.1 Inleiding

In dit hoofdstuk worden de technische eisen uitgewerkt waaraan de Nederlands ENUM registry moet voldoen. De registry van het Nederlandse deel van ENUM, 1.3.e164.arpa, is de stichting ENUM.

9.2 Begrippen

Registry: de registry van het Nederlandse ENUM deel, 1.3.e164.arpa, momenteel de Stichting ENUM.

Name servers: de nameservers voor de registry van het Nederlandse ENUM deel. Dit is met name de zone 1.3.e164.arpa.

9.3 Operationeel beheer van de Name servers

De Registry wordt geacht het operationeel beheer uit te voeren van de Name servers zoals beschreven in RFC2870 "Root Name Server Operational Requirements" of opvolgers.

9.4 Bereikbaarheid

Algemeen office, werktijden

Registratieproces, 24x7

Storingen en technische ondersteuning, 24x7 voor calamiteiten

9.5 Organisatorische eisen

n/a

Niet in dit hoofdstuk:

- arbitrageregeling
- statuten en organisatiestructuur
- uitwerken van reglementen voor registranten e.d.

10 DDI, Delegatie, nummerblokken en nummerextensies (T9)

10.1 Introduction

The Public User ENUM infrastructure allows the assignee of a public telephone number to publish reachability information for accepting communication services. ASPs, PBXs, Customer Premises Equipment and PC applications ("clients") that support Public User ENUM capabilities can query the Public User ENUM infrastructure to directly route a communication session to the assignee without involvement of a communications service provider.

This chapter provides considerations to the relation between telephone numbers used in the Dutch "Nummerplan telefoon- en ISDN diensten", and equivalent listings in Public User ENUM.

10.2 Number Blocks

The implementation shall facilitate the widest possible range of public telephone numbers for registration within user ENUM. Number ranges that are to be considered are (but not limited to):

- geographic numbers
- mobile numbers
- corporate numbers
- personal numbers
- freephone/premium numbers

Some number series in European harmonized series (like 14XX) have no equivalent in the full E.164 international format. Because user ENUM assumes availability of full E.164 international format, potential conflicts may occur with regular numbers starting with the same digit string.

10.3 DNS delegation

The Public User ENUM infrastructure is using DNS. ENUM provides the assignee of a public E.164 telephone number with a DNS record with URI information associated with the telephone number. A mapping exists between the number in the Dutch "Nummerplan telefoon- en ISDN diensten", and the DNS. The DNS record for +31.14.234.5678 can be retrieved from DNS by resolving 8.7.6.5.4.3.2.4.1.1.3.e164.arpa.

DNS implements a distributed lookup tree in which public root name servers point to other name servers responsible for the top-level domain (.arpa); these servers in turn delegate responsibility to name servers responsible for the sub-domain e164.arpa; thus, 1.3.e164.arpa is the DNS delegation point for telephone numbers in the Netherlands.

Note that DNS provides caching capabilities for optimized performance.

A resolver in a Public User ENUM capable device performs lookups recursively until an authoritative result is obtained from a name server that is responsible for a particular ENUM entry. The authoritative name server for a particular ENUM entry may be hosted anywhere (also outside the Netherlands) and is outside the influence of both Registry and Registrars.

Due to DNS delegation, a single name server may hold just a single ENUM entry. It is also possible to delegate ranges of ENUM entries for consecutive numbers in a block to a single DNS server.

10.4 Number extensions

The Dutch "Nummerplan telefoon- en ISDN diensten" specifies a fixed number depth ("closed numbering plan") for the E.164 numberspace in the ITU assigned country code 31. Communications service providers generally implement facilities to allow end-users to dial and reach destinations in accordance to the numberplan.

Clients that support Public User ENUM capabilities will exist throughout the world, and are not expected to implement the fixed number depth of the Dutch "Nummerplan telefoon- en ISDN diensten". Instead, timeout and end-of-dialing mechanisms will be deployed that will result in ENUM queries of variable length.

Due to the distributed nature of DNS, it is technically not possible for the Registry nor for Registrars to limit the depth of the public DNS tree. A user of a regular 10-digit number in the Dutch Public Numbering who has successfully registered a Public User ENUM entry with an ENUM registrar, may choose to setup DNS such that ENUM queries will not only succeed for the 10-digit number, but also for 11-digit (and more) numbers in which the first 10 digits match the assigned number. This provides the assignee with a virtual pool of unique "number extensions" that can only be reached through Public User ENUM.

A Number Extension is a number that is accessible through public user ENUM, that can be reached through one-stage dialing, but that contains more digits than the number of the assignee allocated in the Dutch national numbering plan

Public User ENUM provides the assignee of a public telephone number in the Dutch "Nummerplan telefoon- en ISDN diensten" with the possibility to define a pool of consecutive number extensions reachable through Public User ENUM (only). No rights should be exercisable towards the bodies responsible for number planning (DGTP), number allocation (OPTA) and for ENUM registration (ENUM NL).

10.5 Number Blocks and DDI

Number block facilities are deployed in PSTN/ISDN networks to deliver all calls for individual numbers in a number block to a single service provider who has been assigned the number block.

Direct Dial-In ("DDI") facilities are deployed in PSTN/ISDN networks to directly terminate calls into extensions connected to a Private Branch Exchange. The DDI configuration consists of a range/ranges of consecutive telephone numbers from the Dutch "Nummerplan telefoon- en ISDN diensten". All numbers in the DDI range correspond to the same (network of) PBX(es).

Two types of assignment for Number Blocks are identified:

- a) Number blocks (generally large) that are assigned through the NRA (OPTA) to operators; these blocks can be distributed by the operator to end-users (both as individual or small groups of numbers (DDI)). In case number portability is enforced on the operator who has been assigned the number block, individual out-ported numbers or DDI groups in the larger number block need to be routed to a different provider that has been assigned the number (block).
- b) Number blocks that are assigned directly to end-users by the NRA (OPTA), or by assigned number holders. No numbers in this block can be individually outported.

It should be technically possible to allow registration of a number (block) provided the aspirant registrant can be validated as the assignee for the number (block). DNS delegation for a block of numbers that has been validated must be possible.

11 Referenties

- NLEG rapport
 - <http://www.enumnederland.nl/files/ENUMinNederland.pdf>
- Convenant EZ - ENUM NL
 - <http://www.ez.nl/dsc?c=getobject&s=obj&objectid=151281&ldsname=EZInternet&isapidir=/gvisapi/>
- Notities Min. van EZ n.a.v. herdelegatieproces:
 - <http://www.enumnederland.nl/files/EZ%20notitie%20ENUM%2018%20januari%202007%20openbare%20versie.pdf>
 - <http://www.enumnederland.nl/files/EZ%20notitie%20ENUM%2013%20maart%202007%20openbare%20versie.pdf>
- overzicht lopende implementaties
 - <http://enumdata.org>

- Number Portability in the Global Switched Telephone Network (GSTN): An Overview (RFC 3482)
 - <http://www.ietf.org/rfc/rfc3482.txt>
- enumservice registration for SIP Addresses-of-Record (RFC 3764)
 - <http://www.ietf.org/rfc/rfc3764.txt>
- ENUM Service Registration for H.323 URL (RFC 3762)
 - <http://www.ietf.org/rfc/rfc3762.txt>
- The E.164 to URI DDDS Application (ENUM) (RFC 3761) obsoletes RFC 2916
 - <http://www.ietf.org/rfc/rfc3761.txt>
- Enumservice Registration for Presence Services (RFC 3953)
 - <http://www.ietf.org/rfc/rfc3953.txt>
- IANA Registration for ENUMservices web and ft (RFC 4002)
 - <http://www.ietf.org/rfc/rfc4002.txt>
- E.164 Number Mapping for the Extensible Provisioning Protocol (EPP) (RFC 4114)
 - <http://www.ietf.org/rfc/rfc4114.txt>
- IANA Registration for Enumservices email, fax, mms, ems and sms (RFC 4355)
 - <http://www.ietf.org/rfc/rfc4355.txt>
- IANA Registration for Enumservice Voice (RFC 4415)
 - <http://www.ietf.org/rfc/rfc4415.txt>
- An ENUM Registry Type for the Internet Registry Information Service (IRIS) (RFC 4414)
 - <http://www.ietf.org/rfc/rfc4414.txt>
- IANA Registration for an Enumservice Containing Public Switched Telephone Network (PSTN) Signaling Information (RFC 4769)
 - <http://www.ietf.org/rfc/rfc4769.txt>
- ENUM Validation Architecture (RFC 4725)
 - <http://www.ietf.org/rfc/rfc4725.txt>
- IANA Registration for Enumservice 'XMPP' (RFC 4979)
 - <http://www.ietf.org/rfc/rfc4979.txt>
- IANA Registration for vCard Enumservice (RFC 4969)
 - <http://www.ietf.org/rfc/rfc4969.txt>
- Validation token
 - <http://tools.ietf.org/id/draft-ietf-enum-validation-token-04.txt>

12 BIJLAGEN

(enkel bestemd ter informatie)

12.1 *Mogelijke scenario's voor het gebruik van ENUM*

Bereikbaarheid voor bedrijven

Een bedrijf heeft onlangs een huiscentrale in gebruik genomen die gebruik maakt van VoIP, en wil van buitenaf ook via VoIP bereikbaar zijn. Hiertoe heeft ze een veilige ingang gemaakt in haar netwerk ten behoeve van VoIP (op basis van SIP). Het nummerblok wordt bij een ENUM registrar geregistreerd, waarna een controle plaatsvindt van het feit dat het nummerblok ook daadwerkelijk door het bedrijf wordt gebruikt.

Vervolgens wordt het nummerblok in DNS gedelegeerd aan het bedrijf en wordt de vertaling van het hele nummerblok naar een VoIP domein in de DNS servers van het bedrijf geconfigureerd. Vanaf dat moment kunnen bellers van buiten nummers uit het nummerblok opzoeken via ENUM en het bedrijf via SIP bereiken.

Individuele bereikbaarheid binnen een bedrijf

In een vervolgstap wordt niet meer het hele nummerblok vertaald, maar kan een medewerker zijn eigen nummer zo instellen, dat een gesprek naar dat nummer terechtkomt op het adres van zijn keuze. Dat kan de ene keer zijn mobiel of thuiswerknummer zijn, en de andere keer zijn VoIP toestel. Overloop is uiteraard ook mogelijk.

Nog geavanceerder is de mogelijkheid om het hybride mobiele toestel van de medewerkers te laten reageren op de aanwezigheid van een bluetooth baken, waardoor de routing van het mobiele nummer automatisch in ENUM wordt omgezet naar het VoIP deel van het hybride toestel.

<http://www.denic.de/en/enum/allgemeines/szenarien/bluetooth.html>

Kostenbesparing tussen vestigingen van een bedrijf

Een ander bedrijf heeft meerdere kleine vestigingen en wil onderling bellen via internet laten lopen zonder er meteen een duur IPVPN voor aan te laten leggen. Met ENUM wordt ervoor gezorgd dat wanneer een medewerker op een lokatie belt naar een medewerker op een andere, de internetroute wordt gevolgd in plaats van de route via de telefoonaansluiting.

Thuisgebruik

Een enthousiaste thuisgebruiker maakt gebruik van een kastje (CPE) in zijn meterkast waarop een VoIP account geconfigureerd is dat doorgeschakeld is naar een DECT toestel. Hij wil via VoIP bereikbaar zijn en registreert zijn vaste nummer bij een registrar. Nadat de registrar hem heeft gebeld om te verifiëren of het vaste nummer hem toebehoort, kan hij via het portal van de registrar zijn VoIP account koppelen aan het vaste nummer. Zo is hij bereikbaar op zijn DECT telefoon.

ENUM voor het WWW (09xx nummers)

Een dienstenleverancier die bekend is om zijn 09xx nummer wil een eenvoudig webadres om ook op het web eenvoudig vindbaar te zijn voor haar klanten. Registratie en validatie bij een registrar van het webadres en een koppeling met het betreffende 09xx nummer zorgt ervoor dat klanten alleen nog maar het 09xx nummer in hun adresbalk van de browser hoeven in te typen om op de site van de dienstenaanbieder terecht te komen.

Integratie met (legacy) videocommunicatiesystemen

Wanneer een multinational geïnvesteerd heeft in IP-gebaseerde videoconferencing sets moet het gebruik ervan intuïtief zijn zodat gebruikers ze optimaal gebruiken. Het ligt voor de hand om elke set een telefoonnummer te geven. Het betreft echter geen nummer dat bereikbaar is via het telefoonnetwerk, dus kan ENUM ervoor zorgen dat de nummers vertaald worden naar de internetadressen van de sets. Dat kunnen e-mail achtige adressen zijn, of IP adressen. Het maakt niet uit of de sets nog gebruik maken van het H.323 protocol, of al bereikbaar zijn via SIP.

ENUM voor operatorpeerings

Telefoniebedrijven koppelen niet alleen meer op de traditionele wijze maar ook via VoIP. Nu nog gebeurt dat op speciaal ingerichte knooppunten. Om te bepalen naar welke operator een gesprek gerouteerd moet worden, wordt nu al ENUM gebruikt. Het nummer wordt opgezocht in DNS en het bijbehorende operatordomein komt terug uit DNS, waarna het gesprek naar die operator wordt doorgezet. Op deze wijze is het eenvoudig om op basis van nummerblokken te routeren, en uitzonderingen daarop (bijvoorbeeld als gevolg van nummerporteringen) op een schaalbare wijze in DNS te registreren. Dit ENUM gebruik wordt ook aangeduid met de term 'operator ENUM'.