



ENUM & DNSSEC

- (inter)nationales -

Peter Koch <koch@denic.de>

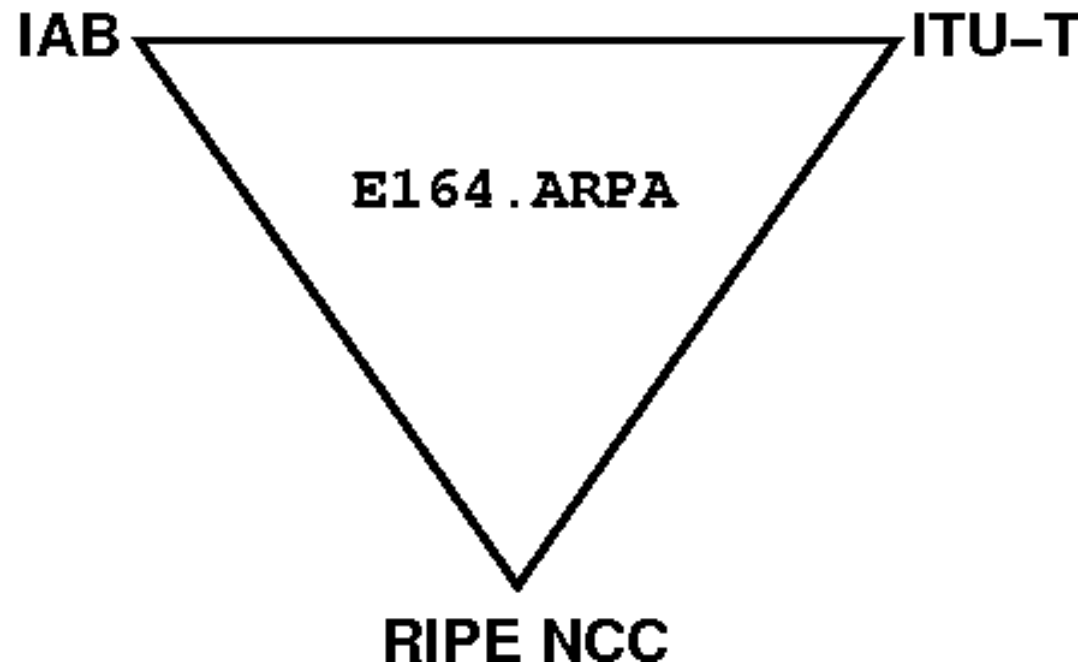
Frankfurt, 3. September 2007

- „Eine Nummer für alle Dienste“
- Rufnummer --> Domain
- „Ländervorwahl“ entspricht (in etwa) TLD
 - +49 für Deutschland -> 9.4.e164.arpa
 - DENIC betreibt Tier1-Registry für +49

RFC 3761 (Security Considerations):

Because of these threats, a deployed ENUM service SHOULD include mechanisms which ameliorate these threats. Most of these threats can be solved by verifying the authenticity of the data via mechanisms such as DNSSEC [8] once it is deployed.

- NAPTR-RRs bilden (ENUM-)Domain auf URIs ab
- ==> NAPTR-Records führen weitere Indirektionsebene ein
- SSL/TLS kein probates Mittel zur NAPTR-Sicherung (kein Endpunkt, der authentisiert werden könnte)
- DNSSEC liefert *data origin authentication* und *data integrity*
- Wichtig ohne NAPTR: *authenticated denial*
- ENUM ist Dienst mit eigenem Namensraum!



- IAB (Internet Architecture Board)
- ITU-T
- RIPE NCC (als Tier0 Registry)
- DENIC (als eine Tier1 Registry)
- ...
- Tier 2: Registranten

- 2007-07-05: RIPE NCC meldet E164.ARPA „DNSSEC ready“
- 2007-07-24: IAB informiert ITU-T
- 2007-08-23: DENIC unterstützt IAB-Plan
- 2007-1?-??: DNSSEC in E164.ARPA
- Tier1 Registrars aktivieren DNSSEC
 - +48 (PL) hat bereits begonnen
 - +49 (DE) in Planung und Vorbereitung
- IANA bereitet Signierung von ARPA vor

- Zweistufiger Ansatz
- Start mit Signierung von 9.4.E164.ARPA
 - ermöglicht *authenticated denial*
 - Registrierung des *Key Signing Key* (KSK) bei Tier0
 - transparent für Tier2 (Registrar und Registrant)
- Später: signierte DS-RRs für ENUM-Delegationen
 - Authentisierung & Integrität



Vielen Dank!

Peter Koch, DENIC eG

<koch@denic.de>

<<http://www.denic.de/de/enum/>>