

## T7. DNSSEC voor ENUM

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 Public keys provided to the registry that are not in the DNS at the time of the data exchange MUST not be published in the DNS.