DNSSEC allgemein

Ist die Signierung der Root-Zone Voraussetzung für DNSSEC?

Nein, Vertauensketten können auch in Unterzonen beginnen wenn deren DNSKEYs im Resolver hinterlegt sind oder aus einem vertrauenswürdigen Repository bezogen werden. So könnte beispielsweise in der Konfiguration eines Resolvers der von der DENIC für die .de-Zone verwendete DNSKEY als vertrauenswürdig hinterlegt sein. Damit wäre für alle signierten .de Zonen und deren Subzonen eine Validierung möglich, da die Vertrauenskette bei einem DNSKEY beginnt, der als vertrauenswürdig eingestuft ist. Ein Wechsel des Schlüssels bei der DENIC würde in diesem Beispiel allerdings auch ein Update der Konfiguration des Resolvers erfordern, da er ansonsten den neuen Schlüssel nicht als vertrauenswürdig einstuft und somit keine Validierung möglich ist oder im schlimmsten Fall eine Nichterreichbarkeit von signierten Zonen entsteht. Falls die DeNic ihren DNSKEY über ein DLV-Repository verfügbar macht, ist sie selbst für die Aktualität des Schlüssels und dessen Austausch verantwortlich.

Eindeutige ID: #1009
Verfasser: Thomas Klute
Letzte Änderung: 2010-04-29 11:47