DNSSEC für Registrare

Wie werden Schlüssel erzeugt?

Die Schlüsselerzeugung sollte von der von Ihnen verwendeten DNSSEC-Software geleistet werden. Eine händische Schlüsselerzeugung ist möglich, es wird aber davon abgeraten, solange man nicht über tiefergehendes Detailwissen im DNSSEC-Bereich verfügt. Grundsätzlich wird empfohlen, für DNSSEC RSA/SHA-1- oder RSA/SHA-256-Schlüssel mit entsprechender Schlüssellänge (siehe Schlüssellängen) zu erzeugen. DNSKEY-Einträge enthalten den verwendeten Algorithmus für die Schlüsselerzeugung, näheres siehe RFC4034 bzw. RFC5702 RFC4641 empfiehlt SHA-256 zu verwenden, sobald die aktuell verwendete Hardware/Software SHA-256 unterstützt.

DENIC hat sich für das .de-DNSSEC-Testbed entschieden, SHA-256 zu verwenden, um spätere Migrationsprobleme ggf. in produktivem Betrieb vorwegzunehmen. Eine zum aktuellen Zeitpunkt konservative und auf Kompatiblität fokussierte Empfehlung würde SHA-1 den Vorzug geben, und zu SHA-256 zu wechseln, sobald es flächendeckend erprobt und verfügbar ist, da SHA-1 inzwischen als anfällig betrachtet werden muss.

Eindeutige ID: #1036
Verfasser: Thomas Klute
Letzte Änderung: 2010-04-29 13:16