DNSSEC im Detail

Was ist ein ZSK, was ist ein KSK?

Ein ZSK (Zone-Signing-Key) ist ein DNSSEC-Schlüssel, der verwendet wird, um die Einträge innerhalb einer DNS-Zone zu signieren. Der KSK (Key-Signing-Key) ist ein DNSSEC-Schlüssel, der ausschließlich verwendet wird, um den ZSK zu signieren.

Die Schlüssellänge des ZSK ist kürzer als beim KSK, was den ZSK kryptografisch schwächer macht als den KSK. Aus diesem Grund wird der ZSK üblicherweise häufiger gewechselt als der KSK. Eine signierte Zone enthält somit mindestens einen KSK und mindestens einen ZSK, der durch den KSK signiert ist, und wiederum alle Zoneneinträge signiert.

Falls eine Vertrauenskette mit einer übergeordneten Zone gebildet werden soll, wird der öffentliche Teil des KSK durch die übergeordnete Zone signiert und die Signatur dort veröffentlicht.

Eindeutige ID: #1013
Verfasser: Thomas Klute
Letzte Änderung: 2010-04-29 11:55