

# Life, Universe, and Everything

November 24, 2010

A consistent key(context) is defined as a key that does not introduce internal inconsistencies. A (partially) propagated KSK must have a fully propagated ZSK.

$$\begin{aligned}
 \textit{ConsistentKeys} \equiv \{ & k | k \in \mathbb{K}, \\
 & \textit{Roles}(k) \subseteq \textit{ksk} \rightarrow (\neg H(Ds(k)) \rightarrow O(Dnskey(k))) \wedge \\
 & \neg H(Dnskey(k)) \rightarrow O(Rrsig(k)) \wedge \\
 & ( \\
 & \quad H(Dnskey(k)) \vee \\
 & \quad \textit{ksk} = \textit{Roles}(k) \rightarrow \exists k' \in \mathbb{K} \cdot ( \\
 & \quad \quad \textit{zsk} \in \textit{Roles}(k') \wedge \\
 & \quad \quad \textit{Alg}(k) = \textit{Alg}(k') \wedge \\
 & \quad \quad O(Dnskey(k')) \wedge \\
 & \quad \quad O(Rrsig(k')) \\
 & \quad ) \\
 & ) \\
 & \}
 \end{aligned}$$

SafeKeys are keys that might be internally inconsistent but for which a consistent counterpart exists.

$$\begin{aligned}
 \textit{SafeKeys} \equiv \{ & k | k \in \mathbb{K}, \\
 & k \in \textit{ConsistentKeys} \vee \\
 & \forall r \in \textit{Roles}(k) \cdot ( \\
 & \quad \exists k' \in \mathbb{K} \cdot ( \\
 & \quad \quad \textit{Alg}(k') = \textit{Alg}(k) \wedge \\
 & \quad \quad r \in \textit{Roles}(k') \wedge \\
 & \quad \quad l \in \textit{ConsistentKeys} \wedge \\
 & \quad \quad r = \textit{ksk} \rightarrow (\neg H(Ds(k)) \rightarrow O(Ds(k'))) \wedge \\
 & \quad \quad \neg H(Dnskey(k)) \rightarrow O(Dnskey(k')) \\
 & \quad ) \\
 & ) \\
 & \}
 \end{aligned}$$

A zone is valid if no single key breaks validity and at least one complete chain for any algorithm exists. An insecure zone is represented by a NULL key.

$$\begin{aligned}
Valid(\mathbb{K}) \Leftrightarrow & \\
& \forall k \in \mathbb{K} \cdot k \in SafeKeys \wedge \\
& \exists k \in \mathbb{K} \cdot ( \\
& \quad ksk \in Roles(k) \wedge \\
& \quad O(Ds(k)) \wedge \\
& \quad O(Dnskey(k)) \wedge \\
& \quad O(Rrsig(k)) \wedge \\
& \quad \exists k' \in \mathbb{K} \cdot ( \\
& \quad \quad zsk \in Roles(k') \wedge \\
& \quad \quad O(Dnskey(k')) \wedge \\
& \quad \quad O(Rrsig(k')) \wedge \\
& \quad \quad Alg(k) = Alg(k') \\
& \quad ) \\
& )
\end{aligned}$$