At-Large Summit Workgroup 5
DNS Security Issues within ICANN's Remit
Parties involved in Signing the Root

In order to understand the political implications, some technical terms needs to be clearly understood. Technically speaking the root zone is signed in the same way as any ordinary zone, but each step might be strictly separated to be executed by independent parties. For this overview, the details of data flow between the parties is ignored.

A **KSK** (*key signing key*) is used to sign all keys together, all ZSKs and all other KSKs. There is no way for signing only a subset of those keys. Because the keyset can't be split, all keys needs to have place in a single EDNS0 answer packet. Therefore the total number of keys is limited to less than 10.

Each KSK is important, because it has to be distributed all over the world, implemented into the resolvers, and is very likely to be hardcoded into a lot of devices. Root KSKs as the primary trust anchors are very hard to change. Starting from any locally known KSK, all other keys are trusted using the existing signatures. Every party able to make signatures with a KSK is called **RKO** (*root key operator*). An RKO has the power to add, remove, or recertify ZSKs, that is hire or fire the RZS.

A **ZSK** (*zone signing key*) is used sign the real zone data. The **RZS** (*root zone signer*) possesses a ZSK, signed by some KSK. In other words the RZS need to be accepted by an RKO. An RZS has the power to add, remove, and redirect top level domains, as well as answering arbitary DNS questions.

Zone data comes from the *top level domain administrators*. ICANN preprocesses the updates and the **Auditor** decides which update is to be applied or rejected. The **RZM** (*root zone maintainer*) compiles a new root zone from the approved updates, cooperates with a RZS to get it signed, and send it to the **RZD** (*root zone distributors*) to load it onto the productive root servers. Currently VERISIGN is the only contractor for RZM and RZD and the US DEPARTMENT OF COMMERCE is the auditor.

For the comparsion of the various proposals, access to private key material is the main focus, i.e. if a organisation generated zone keys on behalf of a RZS, the organisation is listed as a RZS, simply because they can do the job. The audit column shows if public key material needs to be approved by the auditor.

Date	Proposal	RKO	RZS	RZM	Audit	KSKs	Comment
Jun 00	IETF	IANA	IANA	RZM	No	1	RFC 2870
Oct 06	US DHS	RKO	RZM	RZM	Yes	1–3	Option 1
	"	RKO	RKO, RZM	RZM	Yes	1–2	Option 2
	"	RKO	RKO	RZM	Yes	1–2	Option 3
May 07	IGF	RKO	RKO	RZM	No	2	NGO based
Oct 07	Nominum	IANA	IANA, RZM	RZM	No	1	
Jul 08	ICANN	any	any	RZM	Yes	1	
Sep 08	ICANN	ICANN	ICANN	ICANN	Yes	1	
Sep 08	Verisign	RS Ops@Verisign	Verisign	Verisign	No	1	N-of-M
Oct 08	US DoC	RKO	RZM	RZM	Yes	1	Proposal 1
	NTIA	RKO	RKO, RZK	RZM	Yes	1	Proposal 2
	"	RKO	RKO	RZM	Yes	1	Proposal 3
	"	IANA	IANA	IANA	Yes	1	Proposal 4
	"	RZM	RZM	RZM	Yes	1	Proposal 5
	"	N-of-M	RZM	RZM	Yes	1	Proposal 6