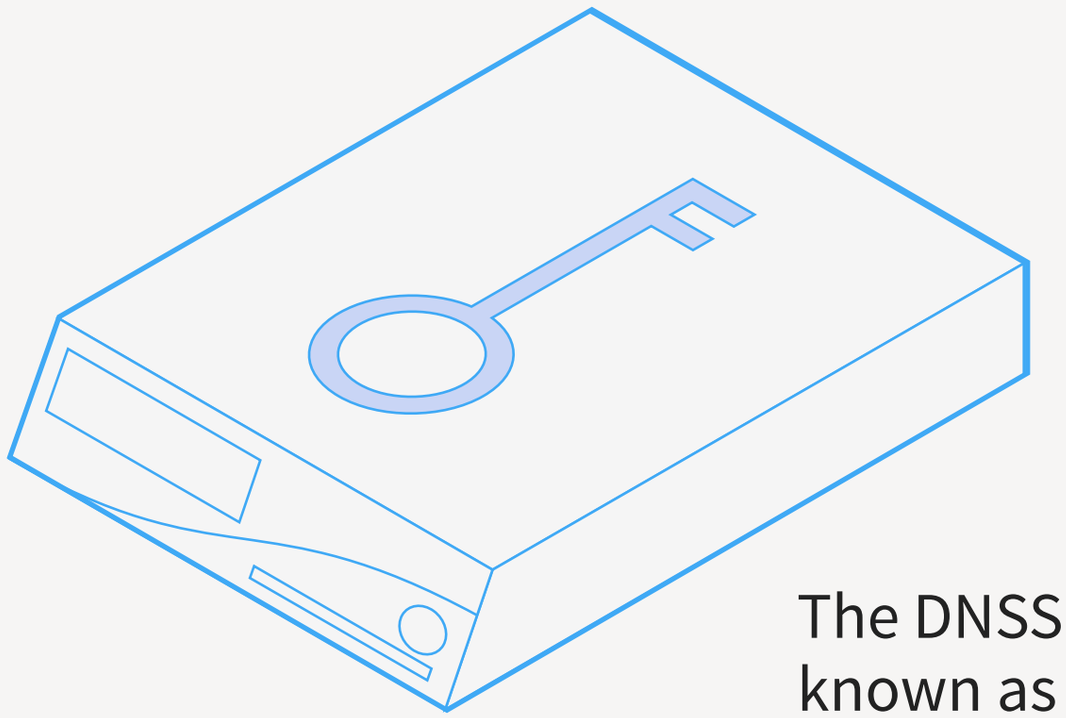
Root KSK Protection and Key Ceremonies

ICANN DNS Symposium: Madrid, Spain
13 May 2017

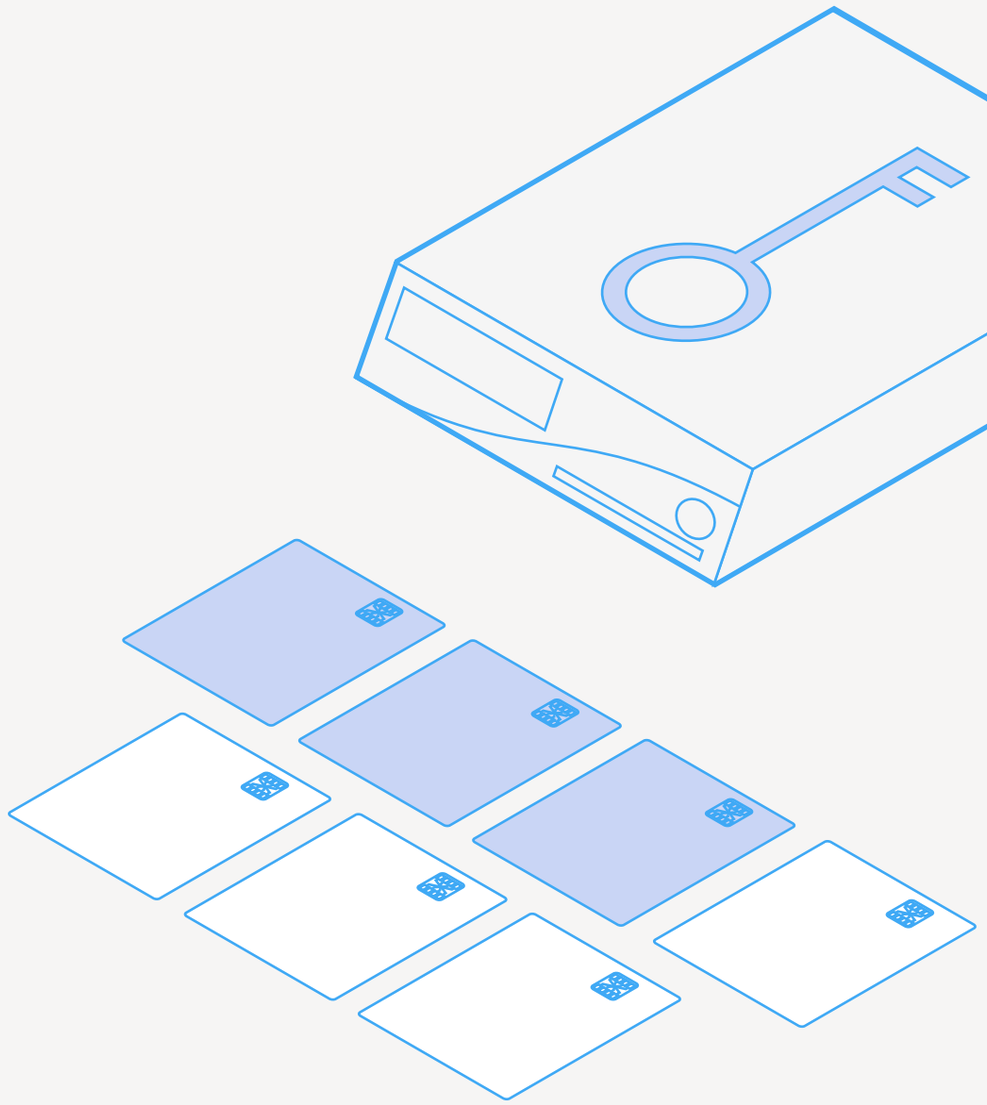
PTI | An ICANN Affiliate

The Root Key Signing Key

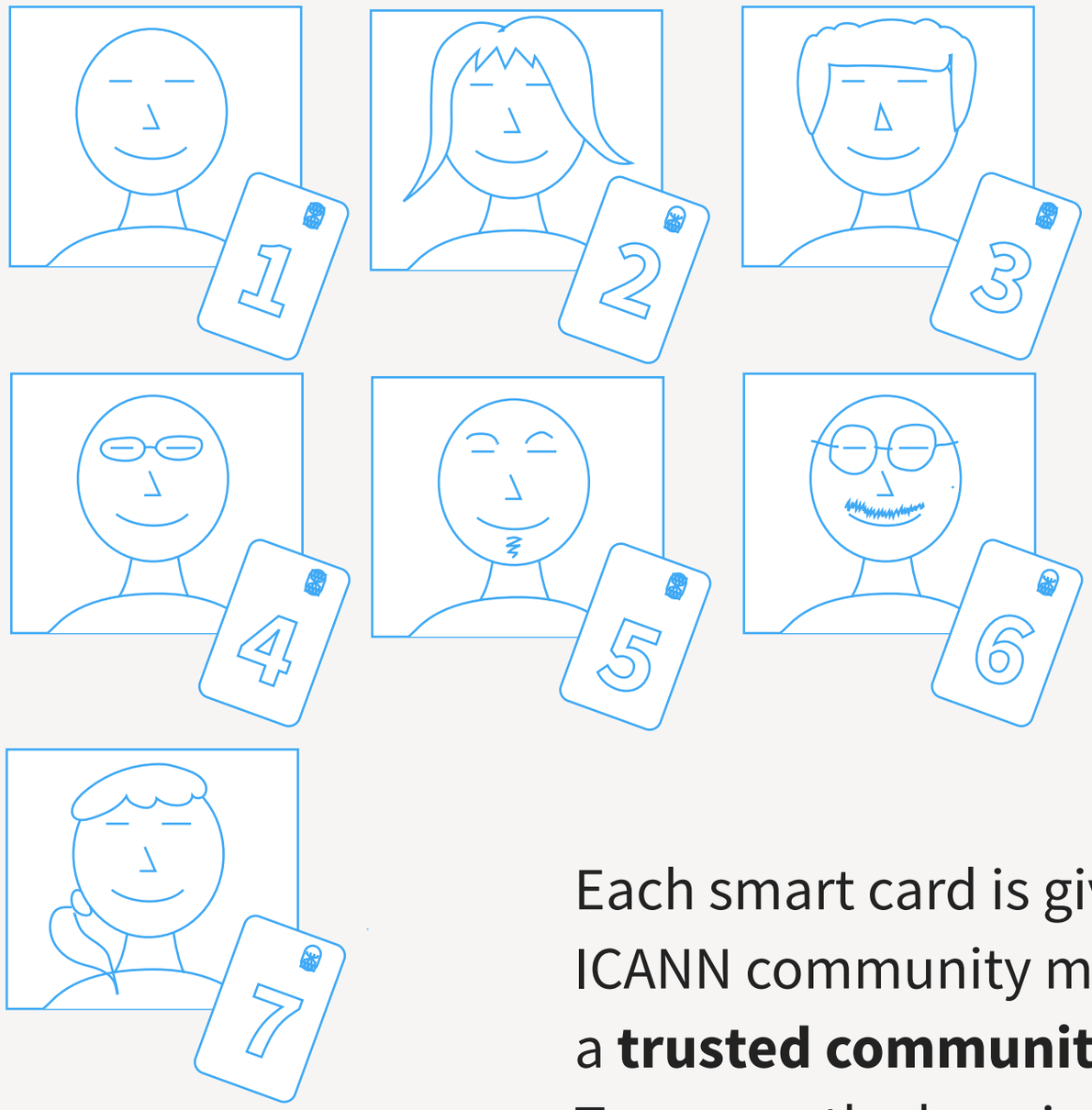
- As part of its root zone related functions, the IANA services team manages the **key signing key**, used to secure the DNS with the DNSSEC protocol.
- The key signing key is the **trust anchor** for the DNS, making its role especially unique.
- An auditable process of performing **key signing ceremonies** to use this key is conducted using members of the community as key participants.



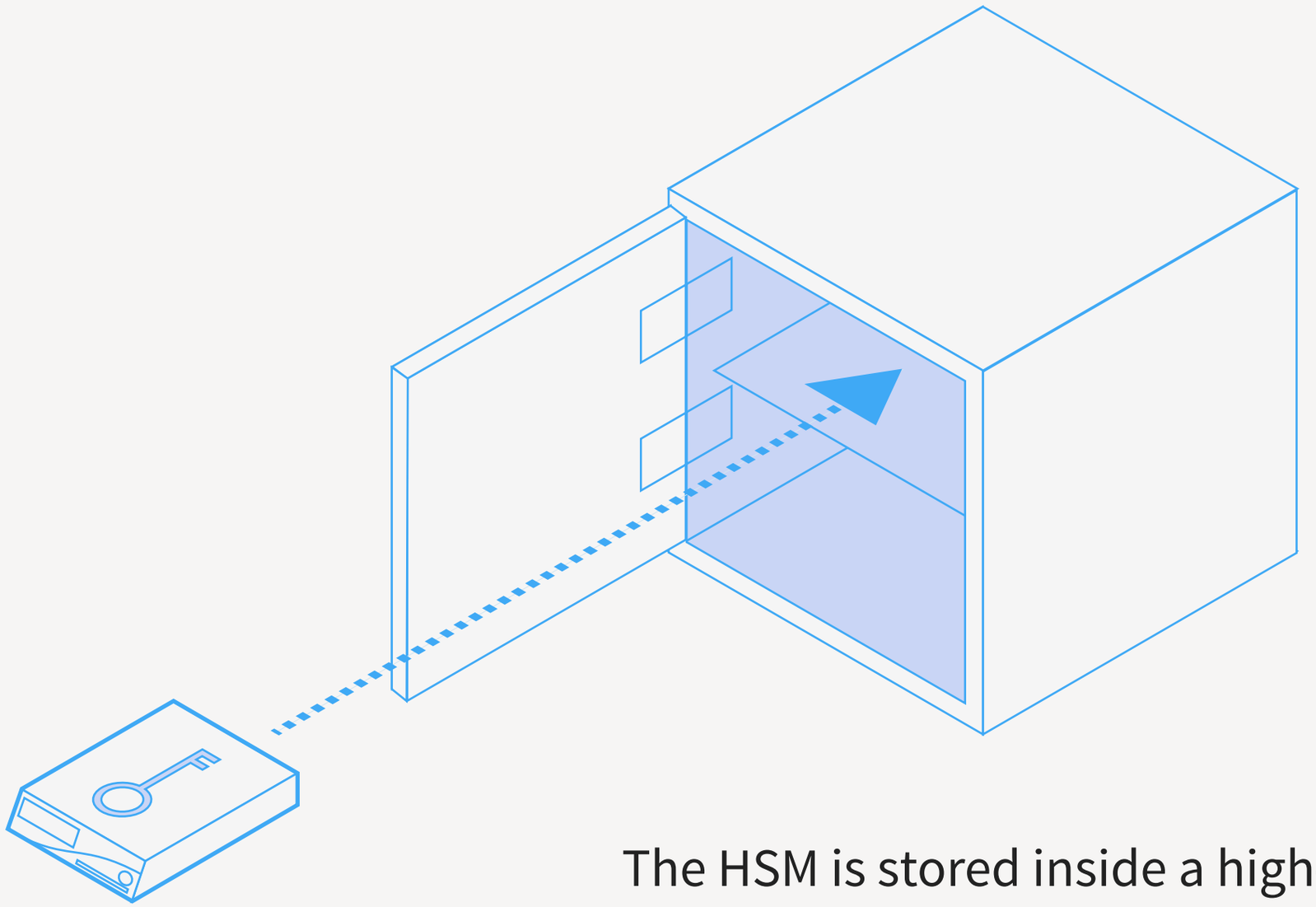
The DNSSEC root key is stored in a device known as a **hardware security module** (HSM) whose sole purpose is to securely store cryptographic keys. The device is designed to be tamper proof. If there is an attempt to open it, the contents will self-destruct.



Seven smart cards exist that can turn on each device. The device is configured such that **3 of the 7** smart cards must be present to make it useable.

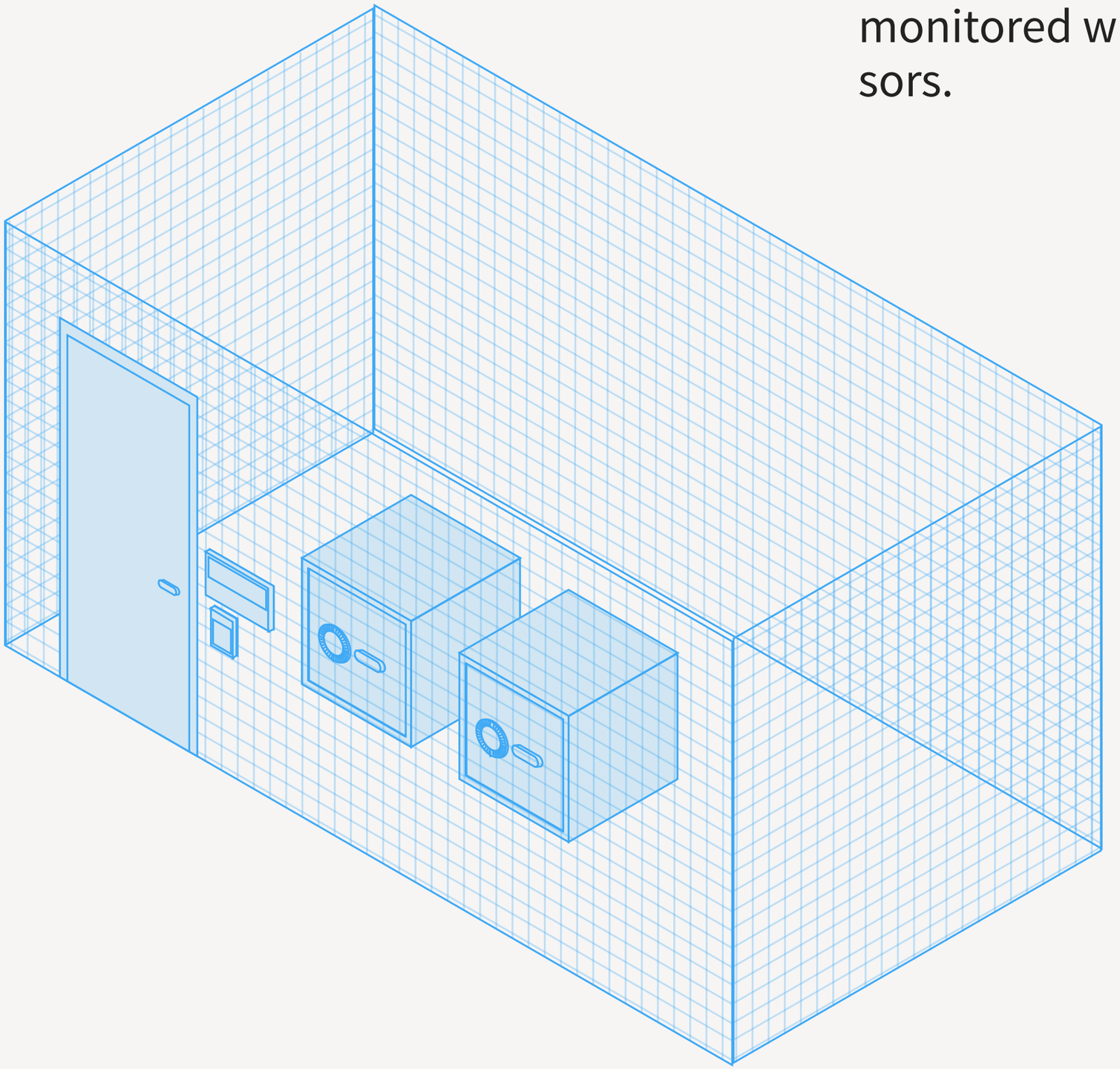


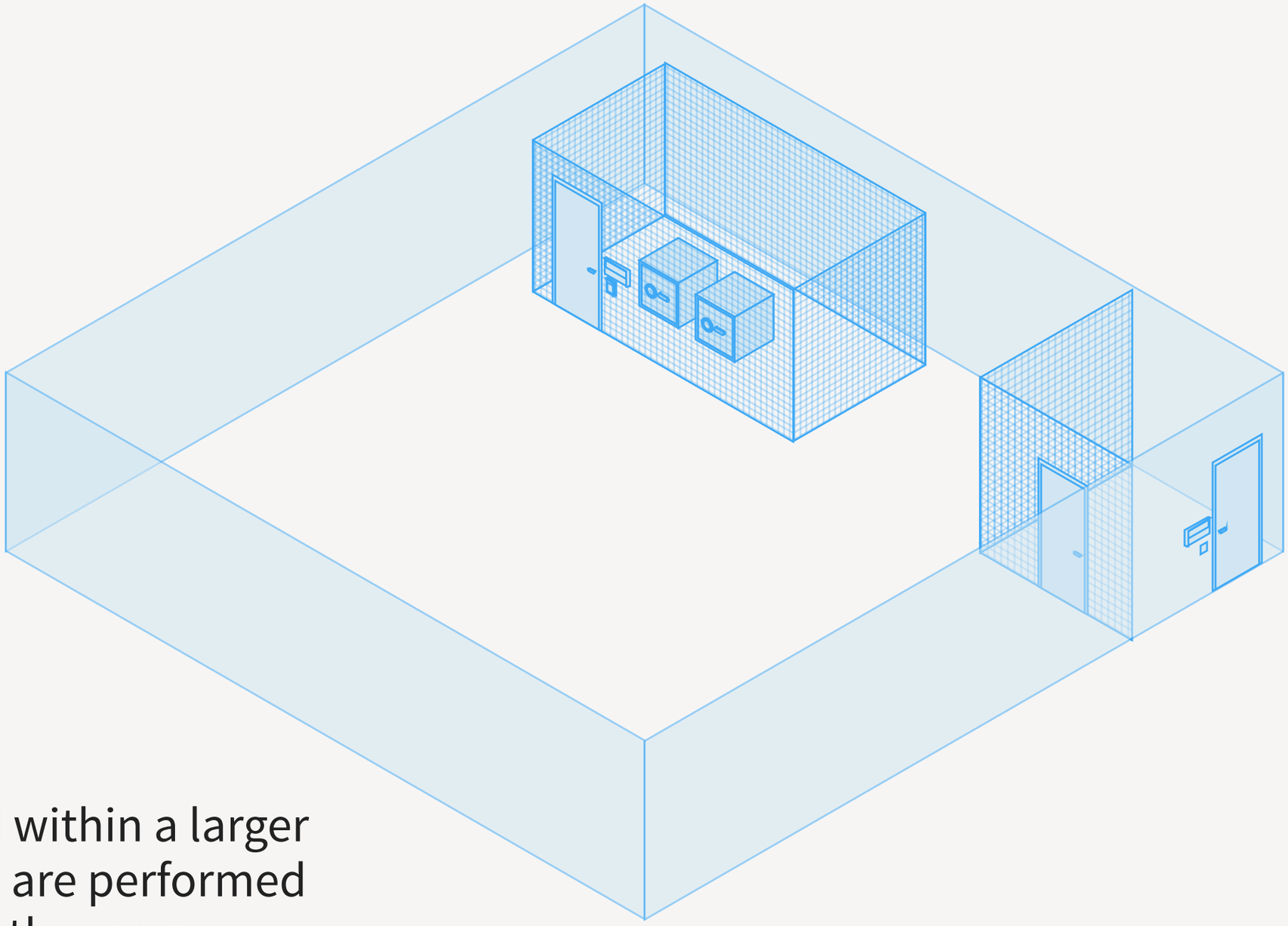
Each smart card is given to a different ICANN community member, known as a **trusted community representative**. To access the key signing key, therefore, at least three of these TCRs need to be present.



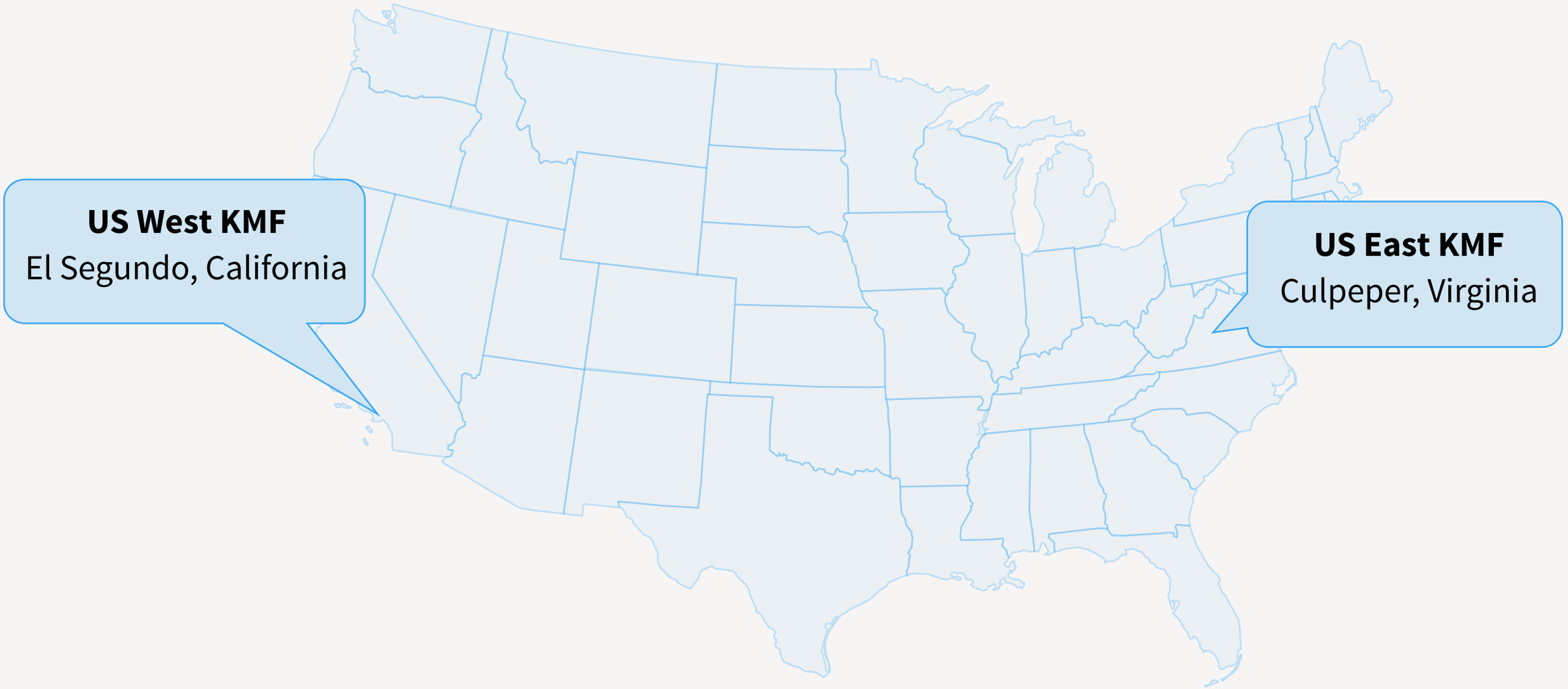
The HSM is stored inside a high-security safe, which can only be opened by a designated person, the **safe security controller**. The safe is monitored with seismic and other sensors.

The safes are stored in a secure room which can only opened jointly by two designated persons, the **ceremony administrator** and the **internal witness**. The room is monitored with intrusion and motion sensors.





The safe room is located within a larger room where ceremonies are performed involving the TCRs and other persons. Ceremonies are recorded on video, witnessed by the participants and others, and audited by a third party audit firm. Access to the room needs to be granted by another designated person, the **physical access control manager**, who is not on-site.



The ceremony rooms, known as **key management facilities**, are located within two guarded facilities, one each on the US West and East coasts.

The ceremonies

- Approximately four times a year, the TCRs and others meet to use the HSMs to sign keys to be used for the root zone.
- The process is streamed and recorded, with external witnesses watching every step. All materials (videos, code, scripts, etc.) are posted online at **iana.org/dnssec**
- The purpose is to ensure **trust in the process**. DNSSEC only provides security if the community is confident the HSMs have not been compromised.

What happens in a ceremony?

- The HSMs and other equipment are retrieved from the safes.
- Three months of ZSK signatures that have been provided by Verisign are signed. (These are used in day-to-day root publication.)
- The **chain of custody** of all the elements is verified throughout the process.

The future

- Current efforts are supporting the key rollover process.
- Ceremony procedures and facility security is regularly enhanced based on experience, community feedback and monitoring of security threats.
- We are enhancing community participation by **calling for new trusted community representatives** for the first time since 2010.

Resources

- TCR criteria and application
  http://iana.org/tcr
- IANA DNSSEC resources
  http://iana.org/dnssec
- Key ceremony primer
  http://kim.id.au/key-ceremony-primer
- Contact for further information
  kim.davies@iana.org