The DNSSEC Root Signing Ceremony

The root DNS zone contains information about how to query the top-level domain (TLD) name servers (.com, .edu, .org, etc). It enables Internet users to access domain names in all TLDs, even brand new ones like .software and .bank, making it an integral part of the global Internet.

In How DNSSEC Works, we explained how trust in DNSSEC is derived from the parent zone's DS resource record. However, the root DNS zone has no parent, so how can we trust the integrity and authenticity of its information?

ĆḎṙ Ấ ừṙ ẮẃĜẎă ṙ Ḃừ fi !

That's the purpose of the Root Signing Ceremony—a rigorous procedure around signing the root DNS zone's public keying information for the next few months. The private signing key used in this process is quite literally the key to the entire DNSSEC-protected Internet. A public, audited, and tightly controlled ceremony around accessing this key is a necessity for DNSSEC to succeed as a global standard.

Ólafur Guðmundsson, an engineering manager at Cloudflare and Crypto Officer at ICANN, participated in the ceremony this August. These are his reflections on the Root Signing

DNSSEC articles

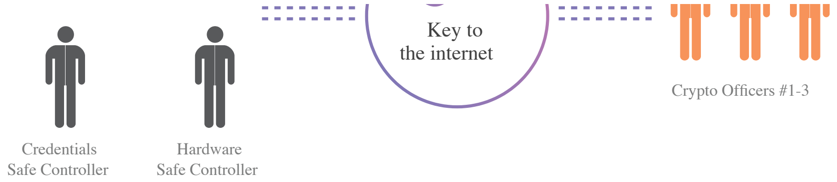
Where Is the Root-Signing Key?

There are two geographically distinct locations that safeguard the root key-signing key: El Segundo, CA and Culpeper, VA. Both are secure facilities, and they contain redundant copies of the key. The ceremony alternates between the El Segundo and Culpeper locations.

Ceremony Participants

- The Ceremony Administrator
- An Internal Witness
- The Credentials Safe Controller
- The Hardware Safe Controller
- Crypto Officer #1
- Crypto Officer #2
- Crypto Officer #3

Each of these participants can only perform certain parts of the ceremony. Their roles are divided in a way that ensures less than a 1:1,000,000 chance that a group of conspirators could compromise the root-signing key, assuming a 5% dishonesty rate (yes, that’s formally in the specification) amongst these individuals.



The first four of these individuals are ICANN staff members, while the three crypto officers are trusted volunteers from the Internet community. Verisign also plays an important role, as they are the root zone maintainer responsible for generating the root zone-signing key that is signed during the ceremony. In addition, the entire procedure is audited by two Big Four auditing firms that are not associated with either Verisign or ICANN.

Ceremony Preparations

There are only 14 available Crypto Officers in the world (7 are affiliated with each location), and at least three of them must attend the ceremony. So, the first step is to poll the Crypto Officers to find a two-day window when 4-5 of them can attend. We usually try to find a period where more than the minimum three are available, as emergencies or travel problems can cause a ceremony cancellation.

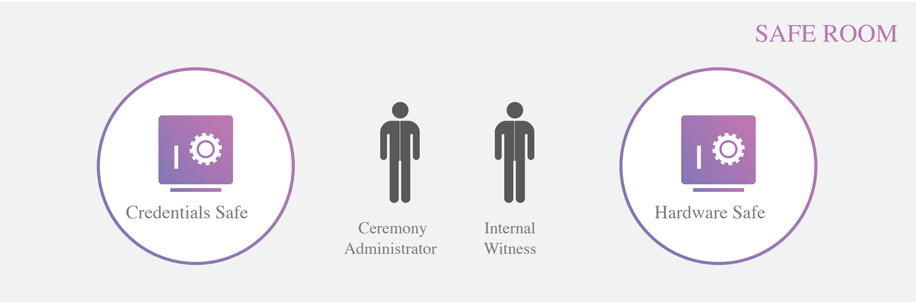
The last ceremony took place on August 13th at the El Segundo facility. To get into the facility, I had to show a government issued ID and show the contents of my bag. In return, I got an ID strip attached to my shirt. Then, I waited for an ICANN staffer to escort me inside. To get through the door, he had to swipe an access card and place his hand on a scanner.

The first stop was a conference room where lunch was being served. We mingled there while waiting for the rest of the ceremony participants to arrive. Being Crypto Officers, most of the small talk revolved around trying to steal root-signing key. We figured it would only take a half hour or so to blast a hole in the wall and walk out with the safe; however, that would probably trip the seismic sensors, so we would know that the key was compromised.

staffer.

A Guy Walks Into a Room with Two Safes...

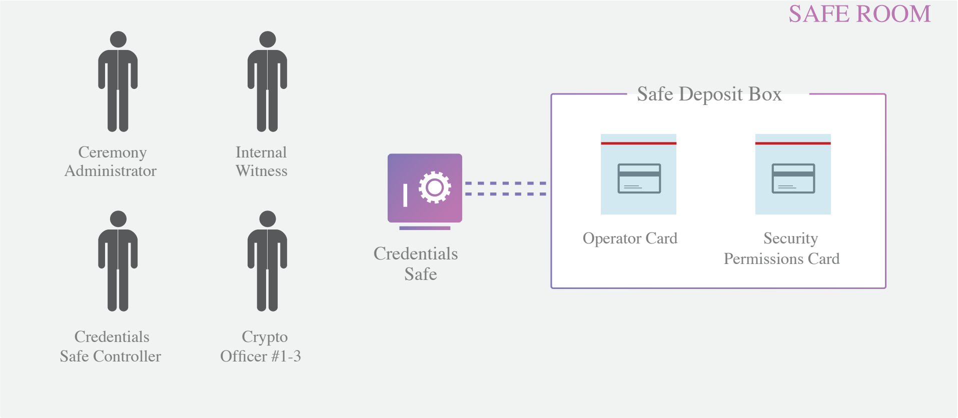
The ceremony room has a cage on the side of it that contains two safes. These safes store all of the sensitive material used during the ceremony. The cage can only be entered in the presence of the Ceremony Administrator and an Internal Witness. This is enforced by a second retina scan and access cards from both the Ceremony Administrator and Internal Witness.



However, neither the Ceremony Administrator or Internal Witness can actually open the safes. For that, we need the Safe Controllers

The Credentials Safe

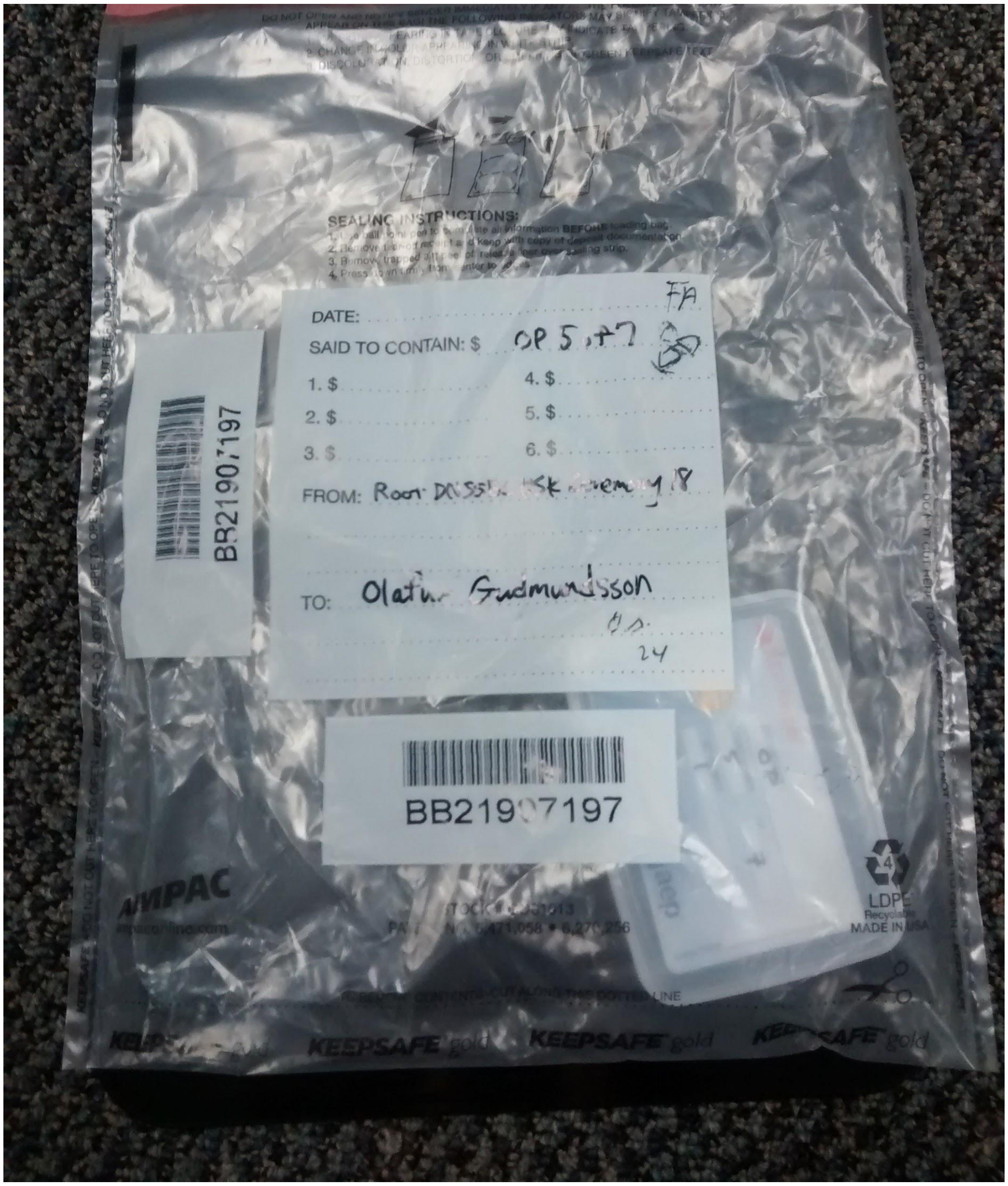
The Credentials Safe Controller opens the first safe, and inside we find several safe deposit boxes, each requiring two keys. The Ceremony Administrator has one of those keys, and each of the Crypto Officers has a key to a different box. Together (and in the



Each safe deposit box contains an operator card and a security permissions card for the Hardware Security Module (HSM), which we'll discuss in the next section. Three operator cards are required to unlock the HSM, which is why three Crypto Officers must attend the ceremony. The security permissions cards are only used when we need to transfer the root-signing key, so we usually leave those in the safe deposit box.

Both cards are stored inside plastic cases wrapped in tamper-evident bags (most of the ceremony revolves around detecting foul-play, if you couldn't tell already). These cards stay in the safe when not in use, which means the last time someone touched them was at the previous Root Signing Ceremony. The tamper-evident bags help ensure that they haven't been altered in the interim.

The plastic cases are also very important, as someone discovered that it was possible to manipulate the cards by poking needles through the tamper evident bag, which would not necessarily be noticeable when inspecting the bag. This is a good example of how the security procedures around the ceremony are constantly evolving.



DATE: FA

SAID TO CONTAIN: $ OP 5, #7

1. $

2. $

3. $

4. $

5. $

6. $

FROM: Root DNSSEC KSK Ceremony 18

TO: Olafur Gudmundsson

O.G.

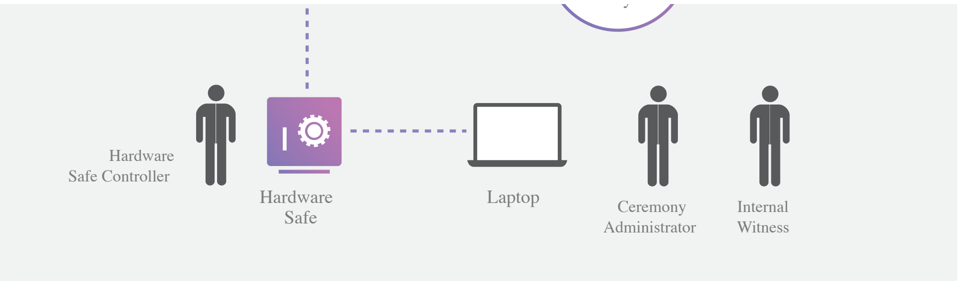
24

BB21907197

BB21907197

The Hardware Safe

The Hardware Safe Controller then enters the safe room and opens up the second safe, which contains a tamper-proof hardware security module (HSM). The HSM is a physical computing device designed specifically for working with sensitive cryptographic material. You can think of it as a digital lock-box for the root-signing key. It can only be accessed with the three operator cards that we collected from the credentials safe.



The HSM can’t be operated without an external interface, so the hardware safe also contains a special laptop that can send commands to the HSM. This laptop has no battery, hard disk, or even a clock backup battery, and thus can’t store state once it’s unplugged. The goal is to eliminate any possibility of the root-signing key leaving the HSM after the ceremony ends.

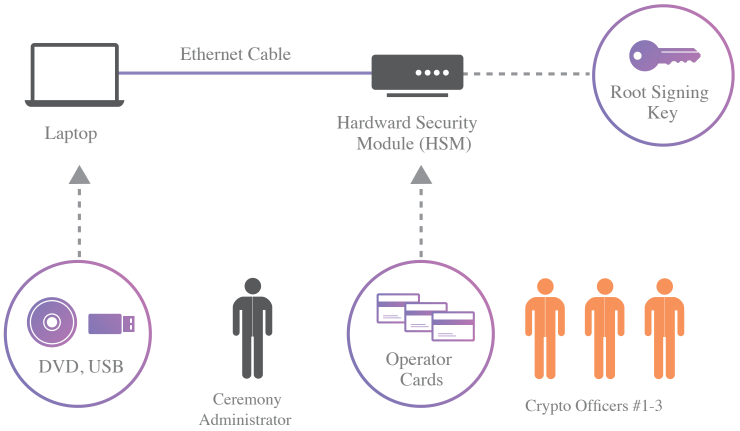
We now have the hardware to perform the Root Signing Ceremony. Notice that the presence of all 7 participants is required to physically access the materials for the ceremony. Again, the idea is to minimize the risk of malicious conspirators by separating access to the HSM from access to the operator cards that activate the HSM.

A USB containing logs from each of the prior ceremonies and a DVD used to boot the laptop (both in their own tamper-evident bags) are also removed from this safe.

Equipment Setup

We’re now ready to perform the actual Root Signing Ceremony. All of the equipment is laid out on a table in full view of all those attending, as well as the camera used to audit the proceedings.

Ceremony Administrator is allowed to touch the card.



The Ceremony Administrator boots the laptop from a DVD and initializes the USB that records the ceremony logs. Remember that the laptop has no clock battery backup, which means the time needs to be set manually from a special wall clock in the ceremony room. It’s the same clock used since the first ceremony five years ago, and it’s completely isolated from the rest of the world. It’s drifted slightly, but that’s fine, as it’s only used for logging purposes.

ǪǴẃǴŅ̂ ṙ Ȫă Ấ ǘ ḵǴūǘ Ǵḃ ẃǴ ǴẂẪệ̩ Ņ̂ ǴȪẤŸǴẪẏ

Next, the Ceremony Administrator needs to activate the HSM by placing the three operator cards collected from the Crypto Officers into the machine. Then, the HSM is connected to the laptop via ethernet cable. The Ceremony Administrator now has access to the root-signing key.

Signing the Root DNS Keys

There are two geographically distinct locations that safeguard the root key-signing key: El Segundo, CA and Culpeper, VA. Both are secure facilities, and they contain redundant copies of the key. The ceremony alternates between the El Segundo and Culpeper locations.

Public KSK
Sign with Private KSK
DNSKEY

The laptop/HSM system is air-gapped, meaning it is physically isolated from any potentially insecure computer networks (e.g., the Internet). The only way to move information from the outside world into the laptop/HSM is via USB drive. Accordingly, the key-signing request is loaded into the laptop via USB. To ensure that the correct key is being signed, a PGP hash of the key-signing request is computed, and Verisign verifies that it is identical to the one they provided.

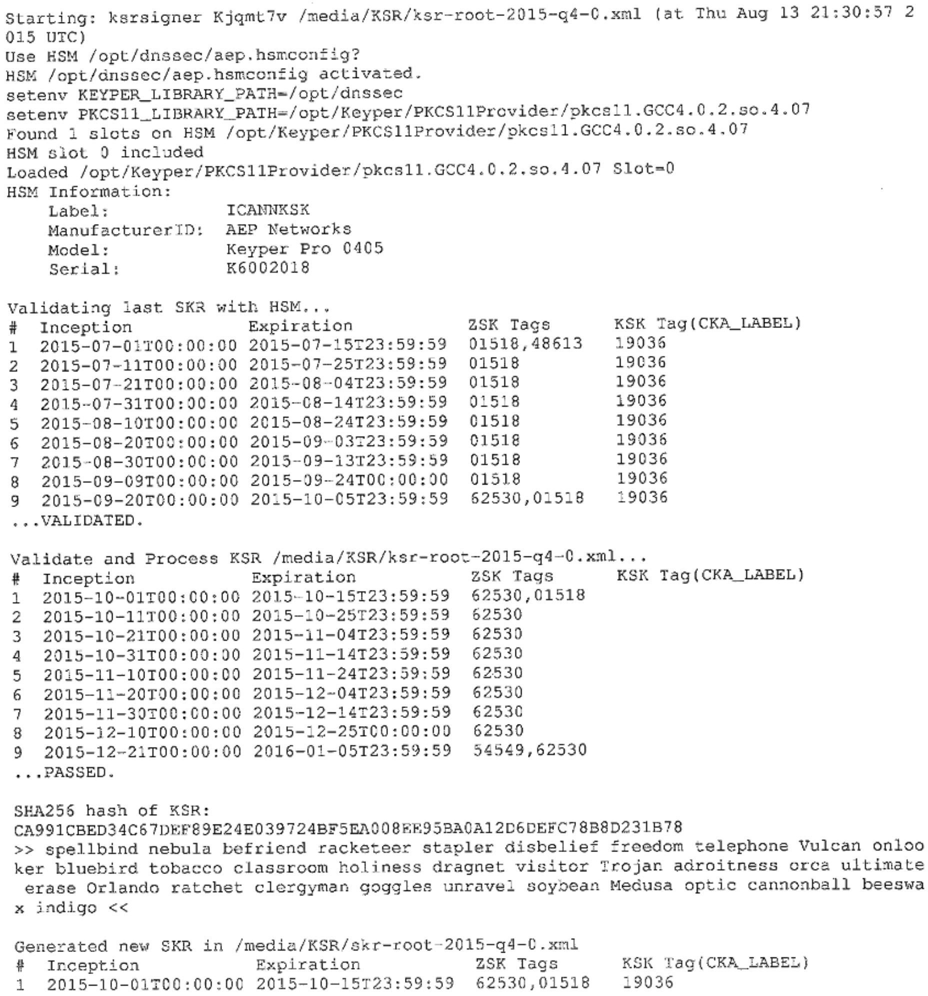
Finally, the Ceremony Administrator can sign the KSR with the private key-signing key. He enters "Y" on a command prompt, and the dramatic portion of the ceremony is complete. The result is a collection of digital signatures, otherwise known in DNSSEC as the RRSIG record, which we'll explore in a moment.

Note that the KSR actually contains a bundle of zone-signing keys that are rotated out every 15-16 days. There are enough keys in the bundle to last until the next Root Signing Ceremony three months from now.

Public Record

Every tiny detail is recorded by auditors and videotaped, making the whole ceremony a matter of public record. This is crucial if the entire DNSSEC-protected Internet is to trust the root name servers' signatures.

This video is streamed live during the ceremony, and we were able to track how many people were watching the ceremony in real time. We had a record-breaking number of



```
Starting: ksrsigner Kjqmt7v /media/KSR/ksr-root-2015-q4-0.xml (at Thu Aug 13 21:30:57 2
015 UTC)
Use HSM /opt/dnssec/aep.hsmconfig?
HSM /opt/dnssec/aep.hsmconfig activated.
setenv KEYPER_LIBRARY_PATH=/opt/dnssec
setenv PKCS11_LIBRARY_PATH=/opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
Found 1 slots on HSM /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07
HSM slot 0 included
Loaded /opt/Keyper/PKCS11Provider/pkcs11.GCC4.0.2.so.4.07 Slot=0
HSM Information:
    Label:            ICANNKSK
    ManufacturerID:   AEP Networks
    Model:            Keyper Pro 0405
    Serial:           K6002018

Validating last SKR with HSM...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2015-07-01T00:00:00 2015-07-15T23:59:59 01518,48613   19036
2  2015-07-11T00:00:00 2015-07-25T23:59:59 01518         19036
3  2015-07-21T00:00:00 2015-08-04T23:59:59 01518         19036
4  2015-07-31T00:00:00 2015-08-14T23:59:59 01518         19036
5  2015-08-10T00:00:00 2015-08-24T23:59:59 01518         19036
6  2015-08-20T00:00:00 2015-09-03T23:59:59 01518         19036
7  2015-08-30T00:00:00 2015-09-13T23:59:59 01518         19036
8  2015-09-09T00:00:00 2015-09-24T00:00:00 01518         19036
9  2015-09-20T00:00:00 2015-10-05T23:59:59 62530,01518   19036
...VALIDATED.

Validate and Process KSR /media/KSR/ksr-root-2015-q4-0.xml...
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2015-10-01T00:00:00 2015-10-15T23:59:59 62530,01518
2  2015-10-11T00:00:00 2015-10-25T23:59:59 62530
3  2015-10-21T00:00:00 2015-11-04T23:59:59 62530
4  2015-10-31T00:00:00 2015-11-14T23:59:59 62530
5  2015-11-10T00:00:00 2015-11-24T23:59:59 62530
6  2015-11-20T00:00:00 2015-12-04T23:59:59 62530
7  2015-11-30T00:00:00 2015-12-14T23:59:59 62530
8  2015-12-10T00:00:00 2015-12-25T00:00:00 62530
9  2015-12-21T00:00:00 2016-01-05T23:59:59 54549,62530
...PASSED.

SHA256 hash of KSR:
CA991CBED34C67DEF89E24E039724BF5EA008EE95BA0A12D6DEFC78B8D231B78
>> spellbind nebula befriend racketeer stapler disbelief freedom telephone Vulcan onloo
ker bluebird tobacco classroom holiness dragnet visitor Trojan adroitness orca ultimate
 erase Orlando ratchet clergyman goggles unravel soybean Medusa optic cannonball beeswa
x indigo <<

Generated new SKR in /media/KSR/skr-root-2015-q4-0.xml
#  Inception           Expiration          ZSK Tags      KSK Tag(CKA_LABEL)
1  2015-10-01T00:00:00 2015-10-15T23:59:59 62530,01518   19036
```

At the end of the ceremony, logs are printed out and given to anybody in the room that wants a copy. Verisign is given a copy of the signed key set on a USB stick, and they will use these signed DNSKEY RRsets in the root zone during Q4 this year. All materials are put back into tamper-evident bags and placed in their respective safes.

Let’s See Those Signed Keys!

There are two geographically distinct locations that safeguard the root key-signing key: El

```
dig . dnskey +dnssec
```

This requests the dnskey records from the root DNS name servers. The interesting part of the response should look something like the following:

```
. 20868 IN DNSKEY 257 3 8

AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF

FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX

bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD

X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz

W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS

Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq QxA+Uk1ihz0= .

20868 IN DNSKEY 256 3 8

AwEAAa67bQck1JjopOOFc+iMISFcp/osWrEst2wbKbuQSUWu77QC9UHL

ipiHgWN7JlqVAEjKITZz49hhkLmOpmLK55pTq+RD2kwoyNWk9cvpc+tS

nIxT7i93O+3oVeLYjMWrkDAz7K45rObbHDuSBwYZKrcSIUCZnCpNMUtn PFl/04cb . 20868 IN

RRSIG DNSKEY 8 0 172800 20150913235959 20150830000000 19036 .

QKU/YSUHNXa0coshORV2r8o0PWZ43dn/u1ml4DglqLXTi2WJh+OyMFgi

w4Xc7cF4T8Eab5TLbwqDHOrE87fmvcdSgQQOVwYN6jwStHAliuEICs6X

rd+sqanyyMpaynLI63Ok5PuuQVOWxHn/Hyn4yFN5MJoQG9Pz+gn8FjCB

oNGs0vu1TQm2m6DSGfjRTd7tRIchXAbOUvEVVnDWaTNPX3c35xqoHlUZ

TaOON9FvKqEwZDjdR1e0BCaDLL/Pk+CRygzOyfSKiuULzKEecsp3jPYY

nXfKZmTuMuaQNRmcyJD+WSFwi5XyRgqrnxWUYmFcum4zw1NXdyp0mlGO slQ6NQ==
```

The first record is the public counterpart to the private key-signing key in the HSM, the second is the zone-signing key provided by Verisign, and the third RRSIG record is what we created during the Root Signing Ceremony. Without that last one, the worldwide DNSSEC system wouldn’t work.

The Root Signing Ceremony turns the root DNS name servers into a trust anchor. Instead of trust being derived from a parent zone, trust is assumed. This whole ceremony is designed to reinforce that trust. It's a very human side of securing the Internet: the reason you can trust the root DNS servers is because you can trust the people signing it. And, the reason you can trust the people signing it is because of the strict protocols they follow while doing so. That's what the Root Signing Ceremony is all about.

CLOUDFLARE

Cloudflare Pricing

Everyone's Internet application can benefit from using Cloudflare.
Pick a plan that fits your needs.

Free $0 /month per website

SELECT

Expand to see more

PRO $20 /month per website

SELECT

Expand to see more

BUSINESS $200 /month per website

SELECT

Expand to see more

Enterprise contact us

SELECT

Expand to see more

Trusted By

CLOUDFLARE

crunchbase

ao com

zendesk

mapbox

log me in

digital ocean

okcupid

montecito

discord

library of congress

udacity

marketo

Sales

Contact Sales:

+1 (888) 99 FLARE

Getting Started

Community

Developers

Support

Company

CLOUDFLARE®