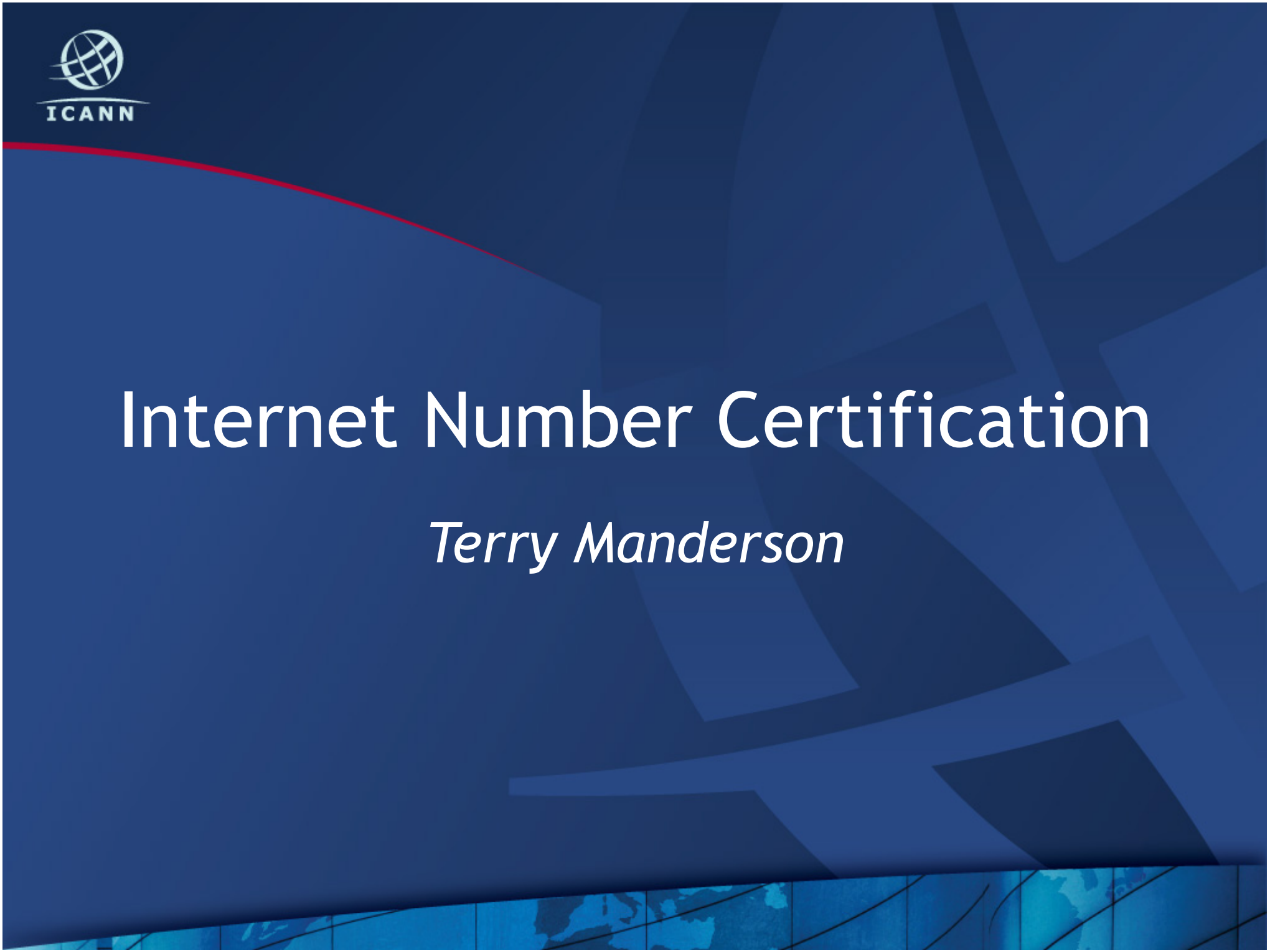


Internet Number Certification

Terry Manderson

ICANN involvement

In response to requests from the Internet community

What you are about to see…

- Possibilities of Implementation
- Technical manifestation of some high level discussions
- Any and all ideas here could change
- Seeking feedback to guide requirements
  - Use this as a catalyst for thought!

The IAB principles

IAB statement on the RPKI.

- *To*: IETF Announcement list <ietf-announce at ietf.org>
- *Subject*: IAB statement on the RPKI.
- *From*: IAB Chair <iab-chair at ietf.org>
- *Date*: Fri, 12 Feb 2010 02:55:43 -0800 (PST)

1. the RPKI should have a single authoritative trust anchor

2. this trust anchor should be aligned with the registry of the root of the allocation hierarchy

Internet number resource. Consequently, before originating, propagating, or accepting an IP address prefix, each routing domain must individually assess the consistency of that prefix with whatever information can be obtained about actual allocations. This loose "routing by rumor" approach provides considerable flexibility to each routing domain, but the negative consequences are severe. The global routing system is vulnerable to large-scale disruptions through both misconfiguration and malice. These vulnerabilities can be substantially reduced through the use of an RPKI. Through proper design and wide-scale deployment, an RPKI enables network operators to generate their routing policies from securely verifiable allocation data, providing much higher confidence in the authenticity of routing information.

= Technical considerations with respect to the design of the PKI

IETF requests

RPKI Architecture

RFC-Editor's Queue:

draft-ietf-sidr-arch	-13	2011-05-23	RFC Ed Queue	3/3
draft-ietf-sidr-cp	-17	2011-04-19	RFC Ed Queue	1/1
draft-ietf-sidr-iana-objects	-03	2011-05-11	RFC Ed Queue	

AS0 ROAs for IETF IPv4 assignments

The NRO

The Number Resource Organization (NRO)
www.nro.net

The NRO would like to enter into discussions with ICANN, conducting also proper talks with IAB, for a global trust anchor (GTA) to be operational in the near future. The NRO would be interested to task ICANN with the management of the GTA as a supplemental technical activity

Chair

ICANN Support

Security and Stability Plan

- http://forum.icann.org/lists/ssr-plan-fy11/
- RPKI addressed!

RPKI

- Resource Public Key Infrastructure.
- An X.509 PKI used to attest to the validity of Internet number resource (IPv4/IPv6, ASNs) allocations.
  - uses RFC3779 extensions
- Provides first step in adding a layer of routing security - tells us 'who has what' in a way that a machine can validate using cryptography (if desired).

One World

One Internet

Everyone

Connected

Resource Certification Discussions

Discussion group formed

- Staff from all RIRs
- IETF Chair
- IAB Chair
- ICANN Staff

Opening discussions

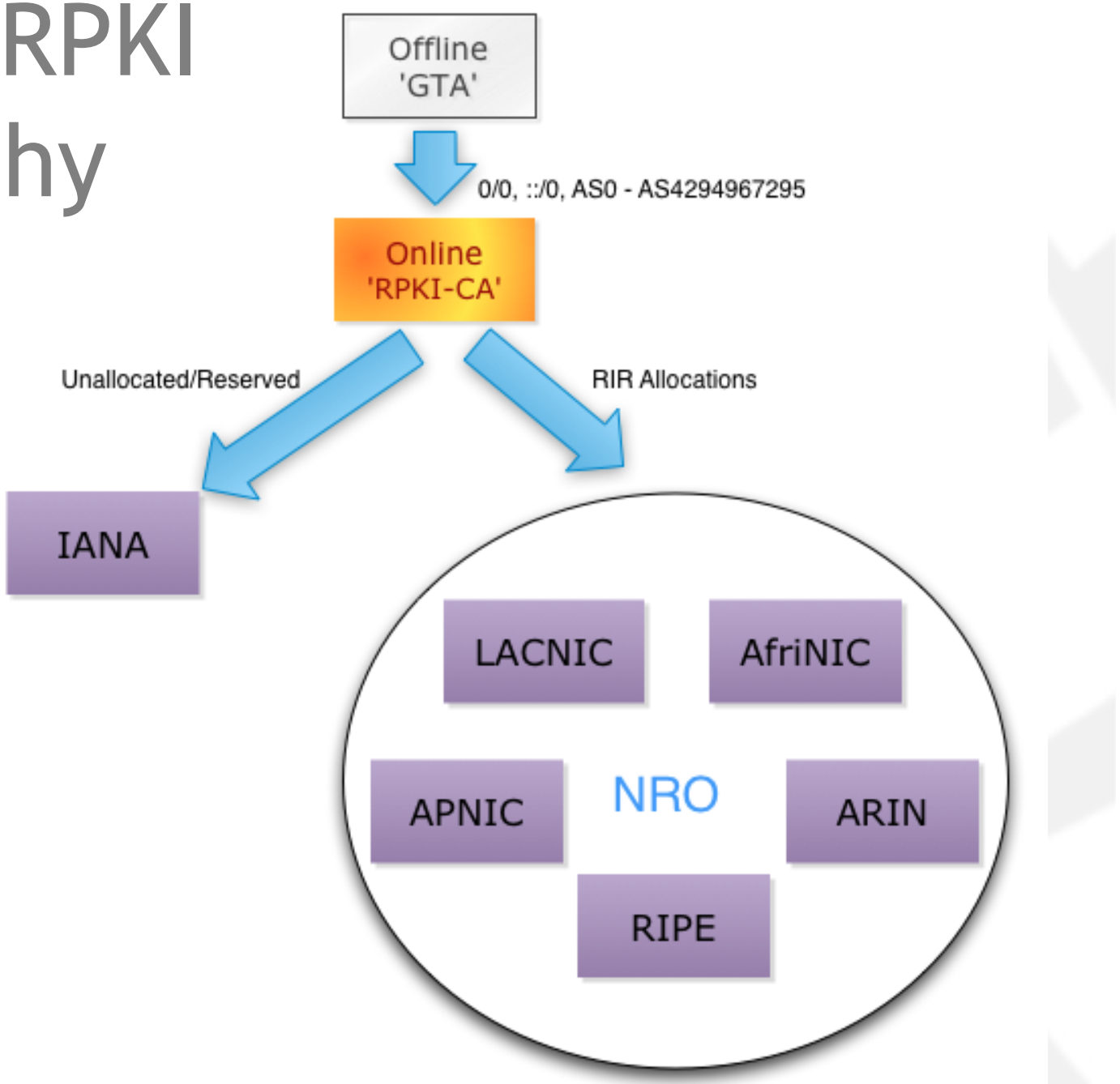
- At IETF 80 March 2011
- Meeting of minds
- Established a shared vision for discussion
- Started the search for requirements

Second discussion

- At IETF 81 in July 2011
- Agenda limited to requirements discussion
- For next meeting
  - —A plan for exploratory ICANN-RIR testing
  - —More requirements building

Some Thoughts on Technical Parts…

A Possible RPKI CA Hierarchy



Idea 1:
What a GTA might look like

Global (single) Trust Anchor (GTA)

- Self signed certificate
- RFC 3779 extensions
  - sbgp-autonomousSysNum: critical
    - 0-4294967295
  - sbgp-ipAddrBlock: critical
    - IPv4
      - » 0/0
    - IPv6
      - » ::/0
- Validity
  - 30 years (long-lived and stable)
- Offline
- Signs An Online RPKI Certification Authority (CA) Certificate Signing Request (CSR)
- See draft-ietf-sidr-ta-07 for TAL format

Idea 2: How the online portion might appear

Online 'RPKI CA'

- Signed by GTA
- RFC 3779 extensions (full allocation)
  - sbgp-autonomousSysNum: critical
    - 0-4294967295
  - sbgp-ipAddrBlock: critical
    - IPv4
      - » 0/0
    - IPv6
      - » ::/0
- Validity
  - 15 years
- Issues RPKI certificates to RIRs and IANA
  - According to allocations
  - Based on an Online Certificate Practices Statement (CPS)
  - 10 year validity
  - No policy exists to not renew nor to revoke certificates unless requested by the RIR through global policy

Implied Goal

The GTA discussion team and ICANN takes all efforts in the security and stability of the internet seriously

ICANN Goal

ICANN will support the Global Trust Anchor (GTA) activity to the best of its ability

- Collaborating on the design of a trustworthy process
- Communicating its actions with the community, incorporating community input, and ensuring transparency

More '*reaching*' Goals

Transparency

Audited

High Security

True Community Involvement (TCI)

Ideas on how to get there…

Auditing and Transparency

- Third-party auditor to check that the GTA operator operates as described in the CPS and all other documented procedures
- Other external witness may also attend the ceremonies

Transparency: Certificate Practices Statement (CPS)

- Encoded in the GTA CPS as an X.509 Certification Authority (CA)
- Published

TCI: Selecting Trusted Community Representatives (TCRs)

- Crypto Officers (COs)
- Backup TCRs

TCI: Selecting TCRs

- Where do we invite TCRs from?
- One organisation? eg ITAC?
- Other/Multiple Organisations?
  - Maybe just ask on all NOG lists?

TCI: Selecting TCRs

- Question to you!
  - No more than 2 COs based in the same country?

TCI: Backup TCRs

- Are backup TCRs important?
  - Is the process important enough to have them?
- If so, what is a sane number?

Security and TCI: GTA Process

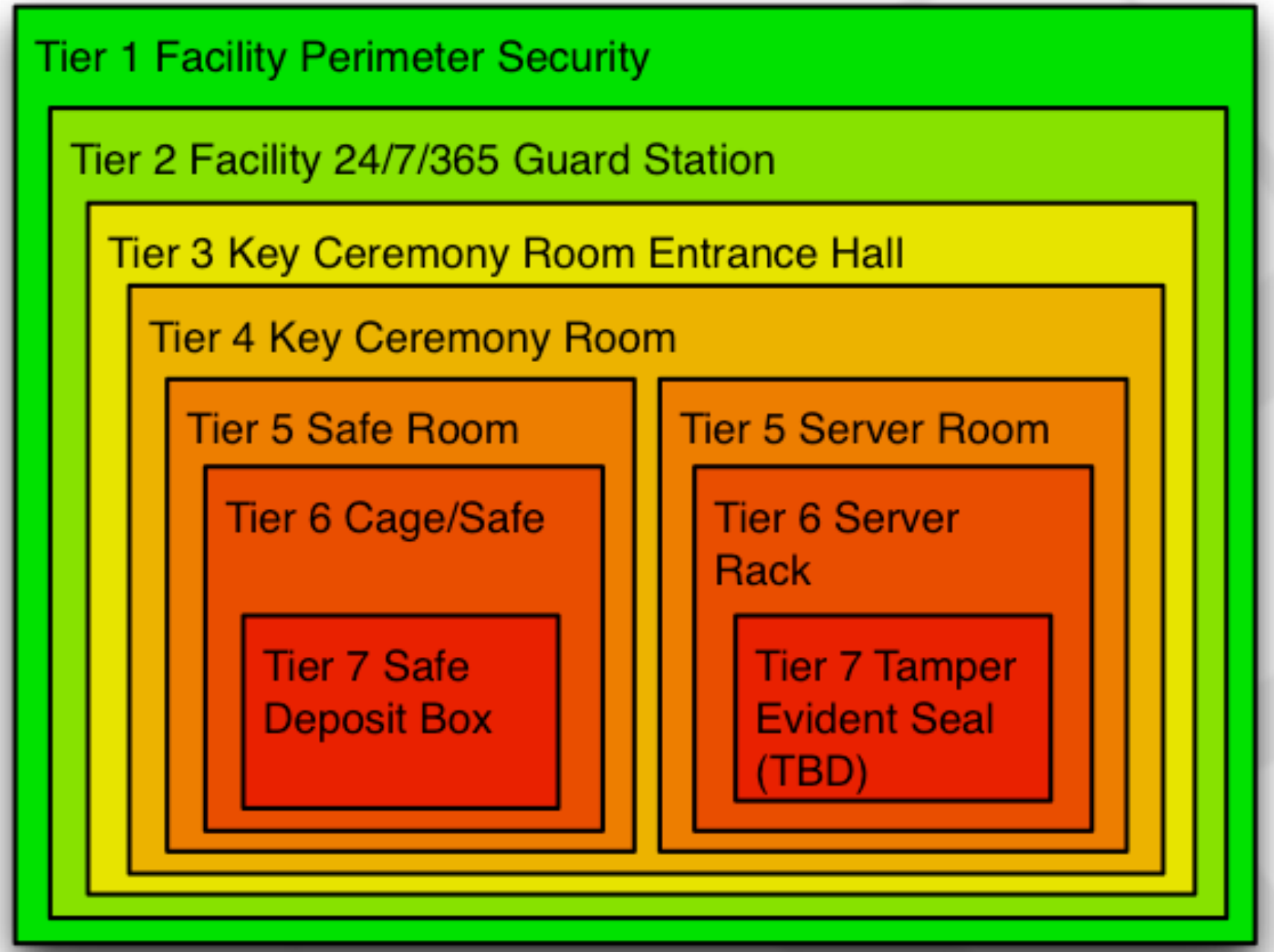
- Key Creation
  - M of N? What is “M”.. what is “N”
    - 3 of 7 COs required to generate new GTA key?
    - 5 of 9 COs required to generate new GTA key?
- Travel to designated GTA KMF once every three?, five?, seven? years to sign the next online RPKI CA cert
  - Assuming all TCRs MUST arrange their own travel funding..

Security: Constructing RPKI GTA KMFs

- 2 Locations (??)
  - 1 in USA?
    - Location ideas
      - San Francisco
      - Los Angeles
      - Culpeper
  - 1 outside of USA?
    - Location ideas
      - Sydney
      - Stockholm
      - Brussels

Security: Constructing RPKI GTA KMFs

- Use Intelligence Community Directives as a guideline?
  - Specifically ICS 705
- Inherits
  - Accompanied access
  - Monitored
  - Audited
  - Multiple levels of access control
    - Safe within a safe room
    - Safe room within a cage
    - cage within a tiered facility etc etc


Tier 1 Facility Perimeter Security
Tier 2 Facility 24/7/365 Guard Station
Tier 3 Key Ceremony Room Entrance Hall
Tier 4 Key Ceremony Room
Tier 5 Safe Room
Tier 6 Cage/Safe
Tier 7 Safe Deposit Box
Tier 5 Server Room
Tier 6 Server Rack
Tier 7 Tamper Evident Seal (TBD)

* ICS 705-1

Intended result:

- Trustworthy design and process?
  - Trustworthy enough?
- Do you see anything missing?
  - email me!
  - We want your feedback!

One World

One Internet

Everyone

Connected

ICANN is...

Responding to bottom up process

Used under a CC BY-SA 2.0 license from flickr.com/photos/drb62

- All RIRs are further along the path
- RFCs expected to be published soon
- Collaborating in the discussions

Willing to share progress

- As it develops
- In forums as appropriate or invited

Open for feedback

Used under a CC BY-NC 2.0 license
from flickr.com/photos/glutnix

- Observing most operator forums
- Observing RIR forums
- Direct feedback at terry.manderson@icann.org
- Via any of the RIRs


ICANN
Thank you
terry.manderson@icann.org

One World

One Internet

Everyone

Connected

Questions