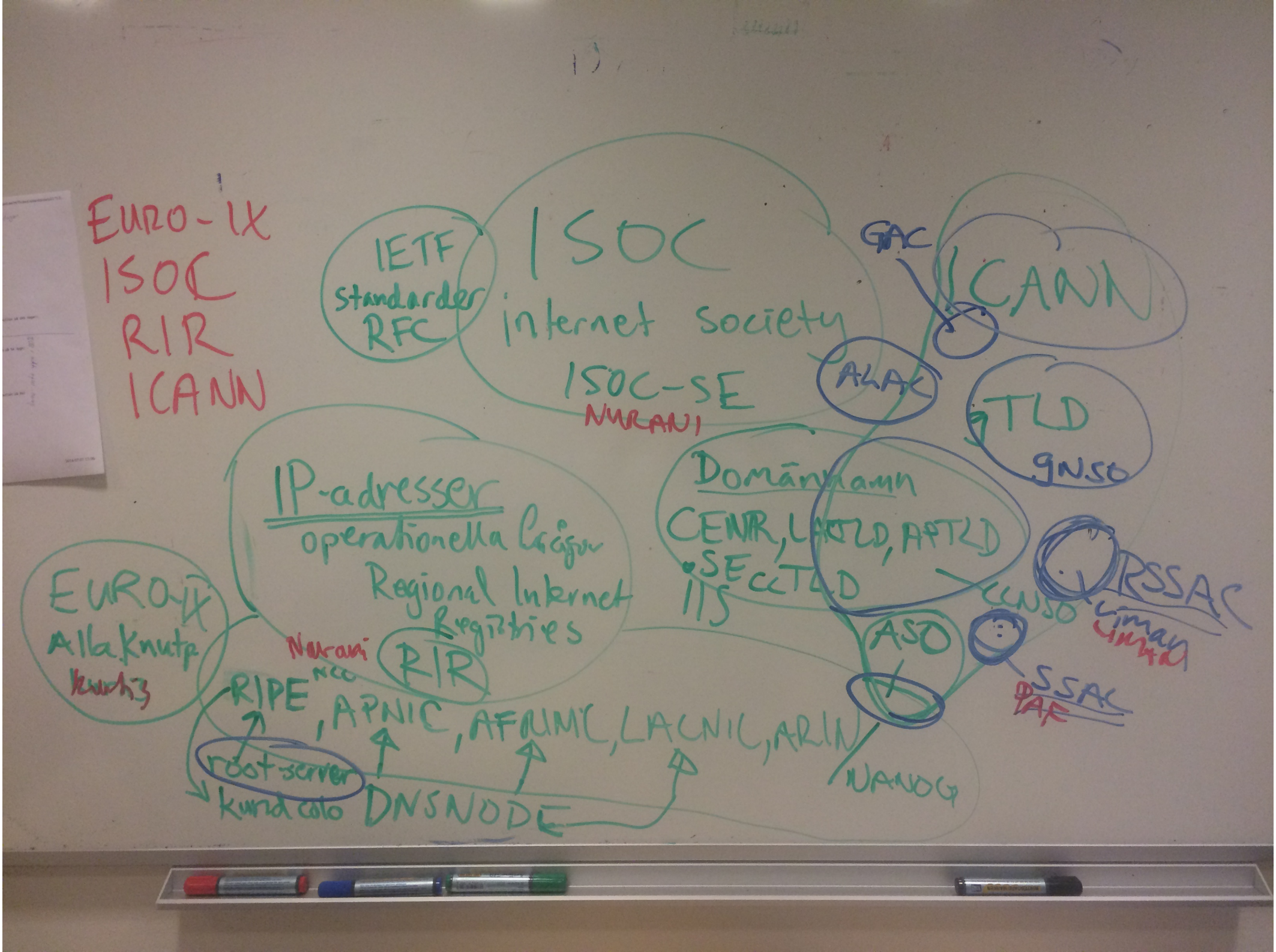
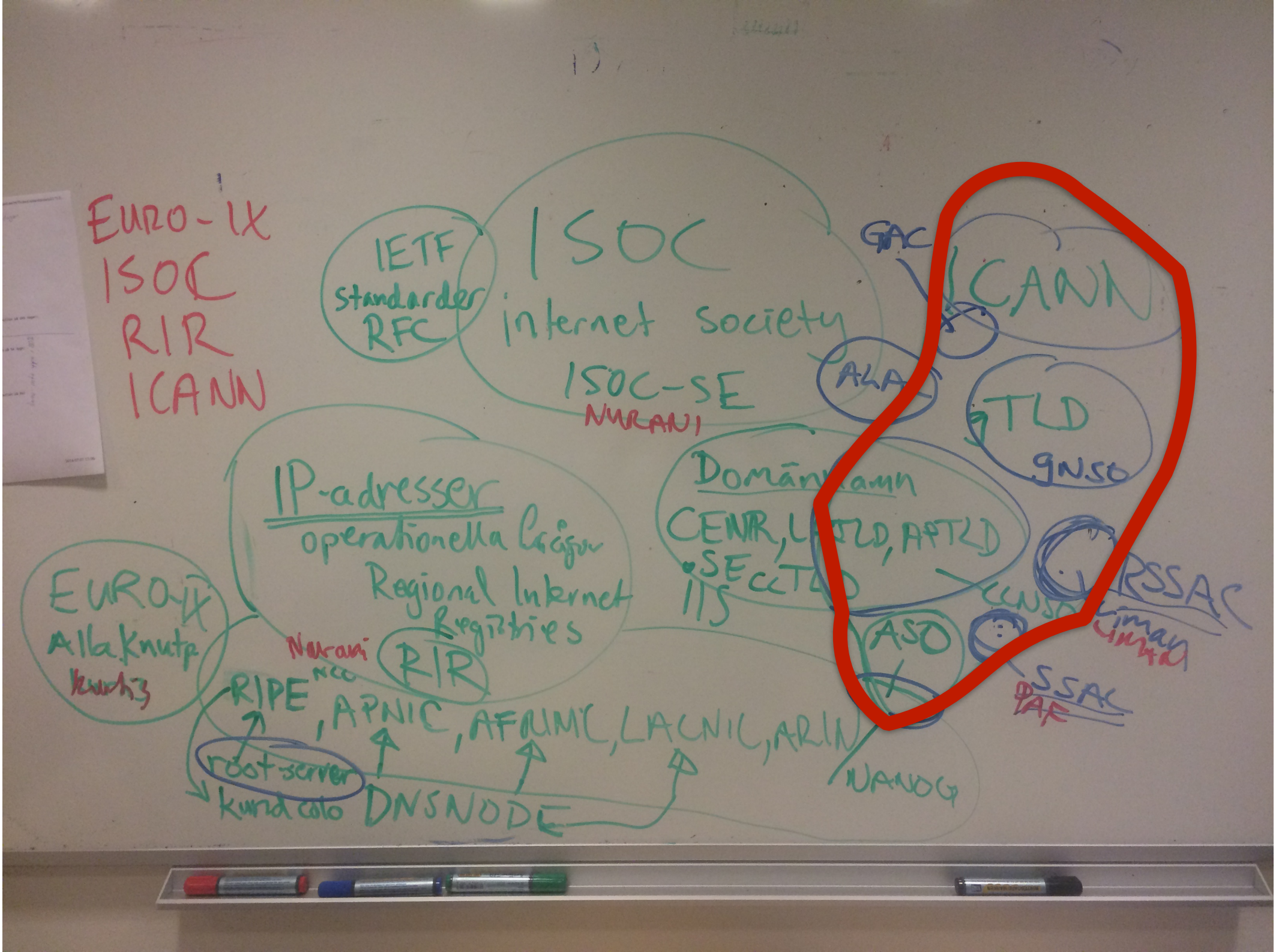

Security and Stability Advisory Committee
Internetdagarna
November 2014
ICANN


EURO-IX
ISOC
RIR
ICANN
IETF
Standarder
RFC
ISOC
internet society
ISOC-SE
NURANI
GAC
ICANN
ALAC
TLD
GNSO
IP-adresser
operationella frågor
Regional Internet
Registries
RIR
Nurani
NCC
RIPE, APNIC, AFRINIC, LACNIC, ARIN
Domännamn
CENTR, LACTLD, APTLD
SE ccTLD
IIS
ASO
CCNSO
RSSAC
SSAC
IAF
NANOG
root-server
kund colo
DNSNODE
EURO-IX
Alla knutpunkter


EURO-IX
ISOC
RIR
ICANN
IETF
Standarder
RFC
ISOC
internet society
ISOC-SE
NURANI
GAC
ICANN
ALAC
TLD
GNSO
IP-adresser
operationella frågor
Regional Internet
Registries
Domännamn
CENTR, LACTLD, APTLD
SE ccTLD
IIS
EURO-IX
Alla knutpunkter
RIPE NCC
Nurani
RIR
APNIC, AFRINIC, LACNIC, ARIN
ASO
RSSAC
ICANN
SSAC
IAF
root-server
kund colo
DNSNODE
NANOG

Security and Stability Advisory Committee (SSAC)

- 2001: SSAC initiated; 2002: Began operation.
- Provides guidance to ICANN Board, Supporting Organizations and Advisory Committees, staff and general community.
- Charter: To advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems.
- Patrik Fältström, Chair; Jim Galvin, Vice Chair (re-elected to 3-year terms beginning 2015); Ram Mohan, Board Liaison (3-year term ending 31 December 2015).
- Members as of October 2014: 40; appointed by ICANN Board for 3-year terms.

ICANN

2014 Achievements

Publications Since ICANN-50 London:

- [SAC068]: SSAC Report on the IANA Functions Contract – 13 October 2014
- [SAC067]: Overview and History of the IANA Functions – 15 August 2014

Publications Since ICANN-49 Singapore:

- [SAC066]: SSAC Comment on JAS Phase I Report on Mitigating the Risk of DNS Namespace Collisions – 06 June 2014

Publications since ICANN-48 Buenos Aires:

- [SAC065]: SSAC Advisory on DDoS Attacks Leveraging DNS Infrastructure – 18 February 2014
- [SAC064]: SSAC Advisory on DNS “Search List” Processing – 13 February 2014

IANA Functions Stewardship Transition

Background

- On 14 March 2014, the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) announced its intention to transition out of its current role with respect to the Internet Assigned Numbers Authority (IANA) Functions.
- NTIA called on ICANN to "convene global stakeholders to develop a proposal to transition the current role played by NTIA in the coordination of the Internet's domain name system (DNS)."

ICANN

Background, Cont.

- IANA is a traditional name used “to refer to the technical team making and publishing assignments of Internet protocol technical parameters.”
- This technical team performs a set of tasks that involve the administration or coordination of many of the identifiers that allow the global Internet to operate.

Background, Cont.

- As described in the current IANA Functions contract between ICANN and NTIA, the IANA Functions are:
  - Domain Name System (DNS) Root Zone Management;
  - Internet Numbers Registry Management;
  - Protocol Parameter Registry Management, including management of the “Address and Routing Parameter Area” (.ARPA) TLD; and
  - Management of the “INTernational treaty organizations” (.INT) top-level domain.

Overview and History of the IANA Functions

- SAC067 was published on 15 August 2014. The report:
  - Establishes a baseline of understanding for those interested in how the upper-most level of the Internet's system of unique identifiers is managed;
  - Describes the activities included in the IANA Functions contract; and
  - Describes the functions performed under the IETF MoU.
- The report focuses on:
  - The IANA Functions contract; and
  - Describes all of the activities related to the IANA Functions as they are currently performed, including those that lie outside of the IANA Functions contract.

ICANN

Report on the IANA Functions Contract

SAC068 was published on 13 October 2014:

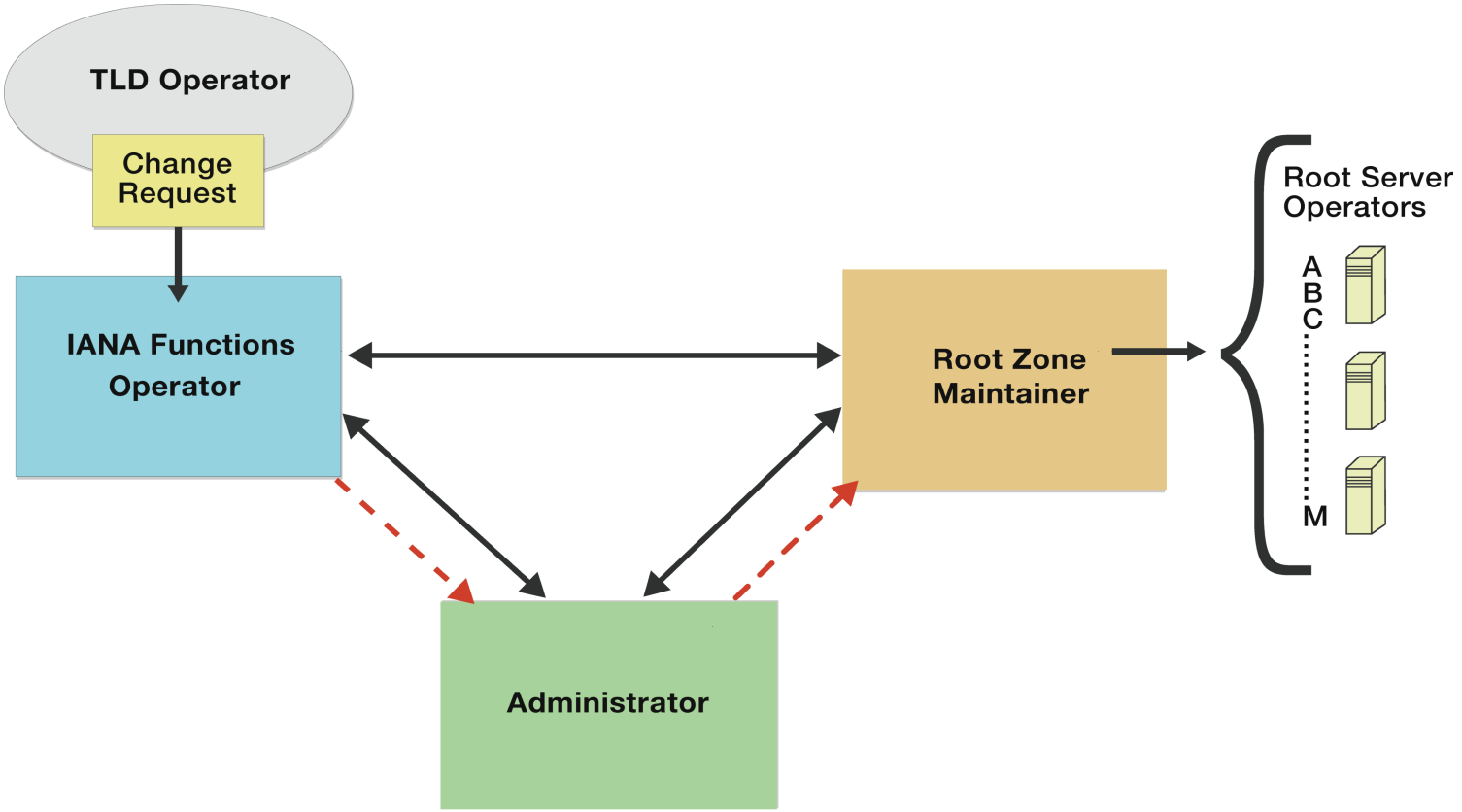
- In this report the SSAC:
  - Provides an overview of the key elements of the IANA Functions contract; and
  - Documents the role that NTIA currently plays with respect to the IANA Functions based on current public contractual information.

NTIA and IANA Functions

IANA Functions	Involved Parties	NTIA Role
DNS Root Zone Management	ICANN, NTIA and Verisign	IANA Functions Contract Administrator and Root Zone Management Process Administrator
Internet Numbers Registry Management	ICANN under authority of Regional Internet Registries and their communities	IANA Functions Contract Administrator
Protocol parameter registry management	ICANN under authority of The Internet Engineering Task Force (IETF) / Internet Architecture Board (IAB)	IANA Functions Contract Administrator
.ARPA and .INT management	ICANN under authority of IETF/IAB and other existing processes	IANA Functions Contract Administrator

ICANN

NTIA and Root Zone Management



Use of unallocated TLDs

How do we know what is in use?

Look at root servers and resolvers?

- **We had a look at i-root during 24 hours**

162 million unique TLDs queried for
65 million are 10 characters long
Created real problems even counting the counters...memory issues...

- **Easy to look at the most common ones**

What do the long tail say?
Look at RD flag and QType?
Other things?

com	298667604
net	170919539
local	115912656
home	45600753
org	43616366
internal	42269815
localdomain	27669054
arpa	27178051
localhost	22019549
lan	18476248
domain	17505162
ru	17424736

Example: Internal Server Names

Designed for “internal only” type applications.

- **Often used by Microsoft Exchange, Active Directory:**

www.corp, www.accounting, mail.test

Doesn’t end in a TLD

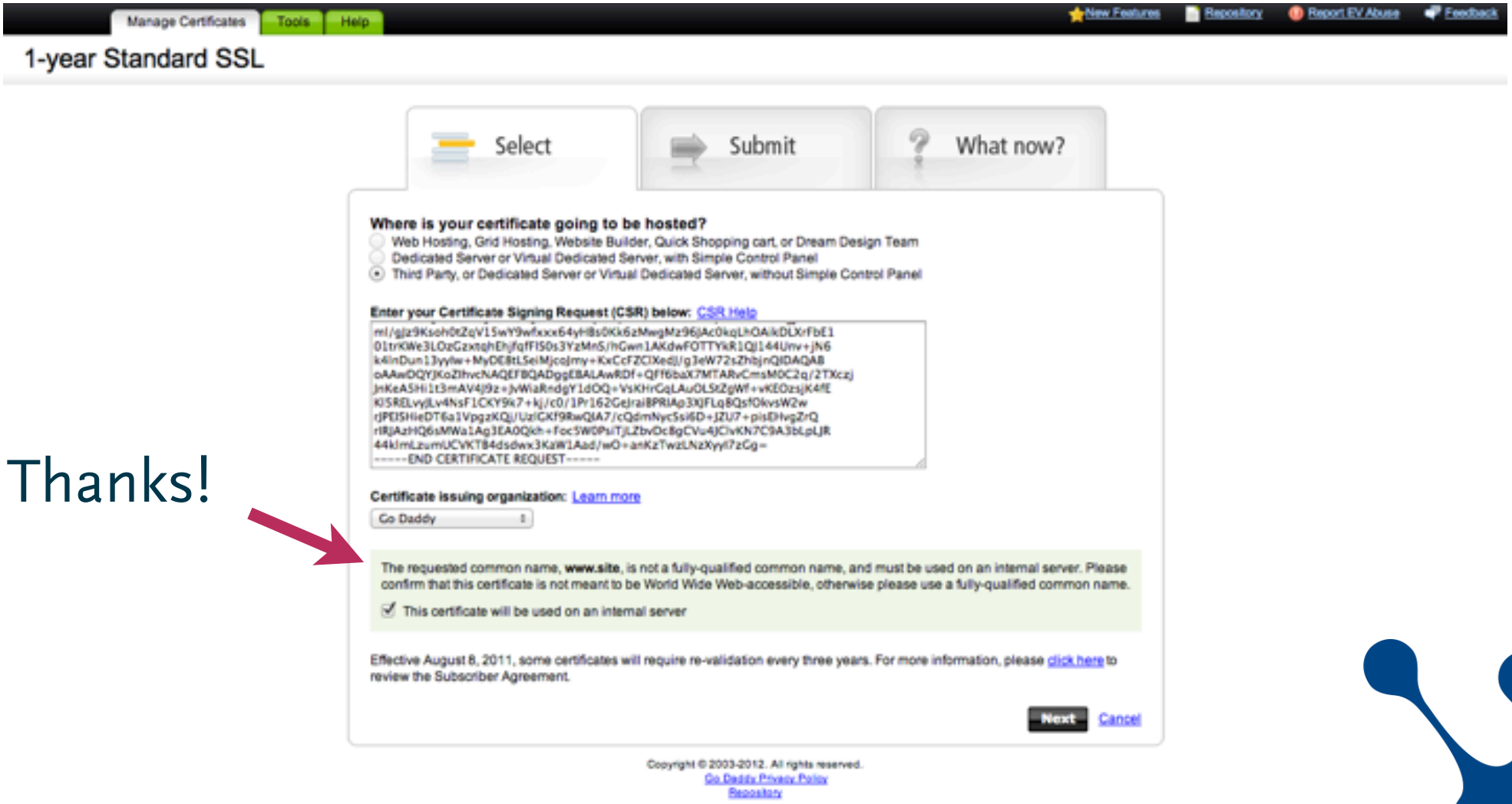
- **Can’t be used on the Internet**
- **Nowhere to send the validation email**

Until a TLD is created with that name

Certificate request

```
Data:
 Version: 0 (0x0)
  Subject: C=US, ST=VA, L=Dulles,
      O=Dulles Steel and Forge Supplies,
      OU=IT - Internal WWW Site.,
      CN=www.site/emailAddress=warren@kumari.net
    Subject Public Key Info:
     Public Key Algorithm: rsaEncryption
     RSA Public Key: (2048 bit)
     Modulus (2048 bit):
      00:da:ef:bd:d0:ee:db:...
```

Helpful...



Thanks!

Issued Certificate

Certificate:

Version: 3 (0x2)
Serial Number:
27:e7:22:63:59:11:b0
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, ST=Arizona, L=Scottsdale,
O=GoDaddy.com, Inc., OU=http://certificates.godaddy.com/repository,
CN=Go Daddy Secure Certification Authority/serialNumber=07969287
Validity
Not Before: Oct 2 23:56:35 2012 GMT
Not After : Oct 2 23:56:35 2013 GMT
Subject: O=**www.site**, OU=Domain Control Validated,
CN=**www.site**
X509v3 Subject Alternative Name:
DNS:**www.site**, DNS:**site**

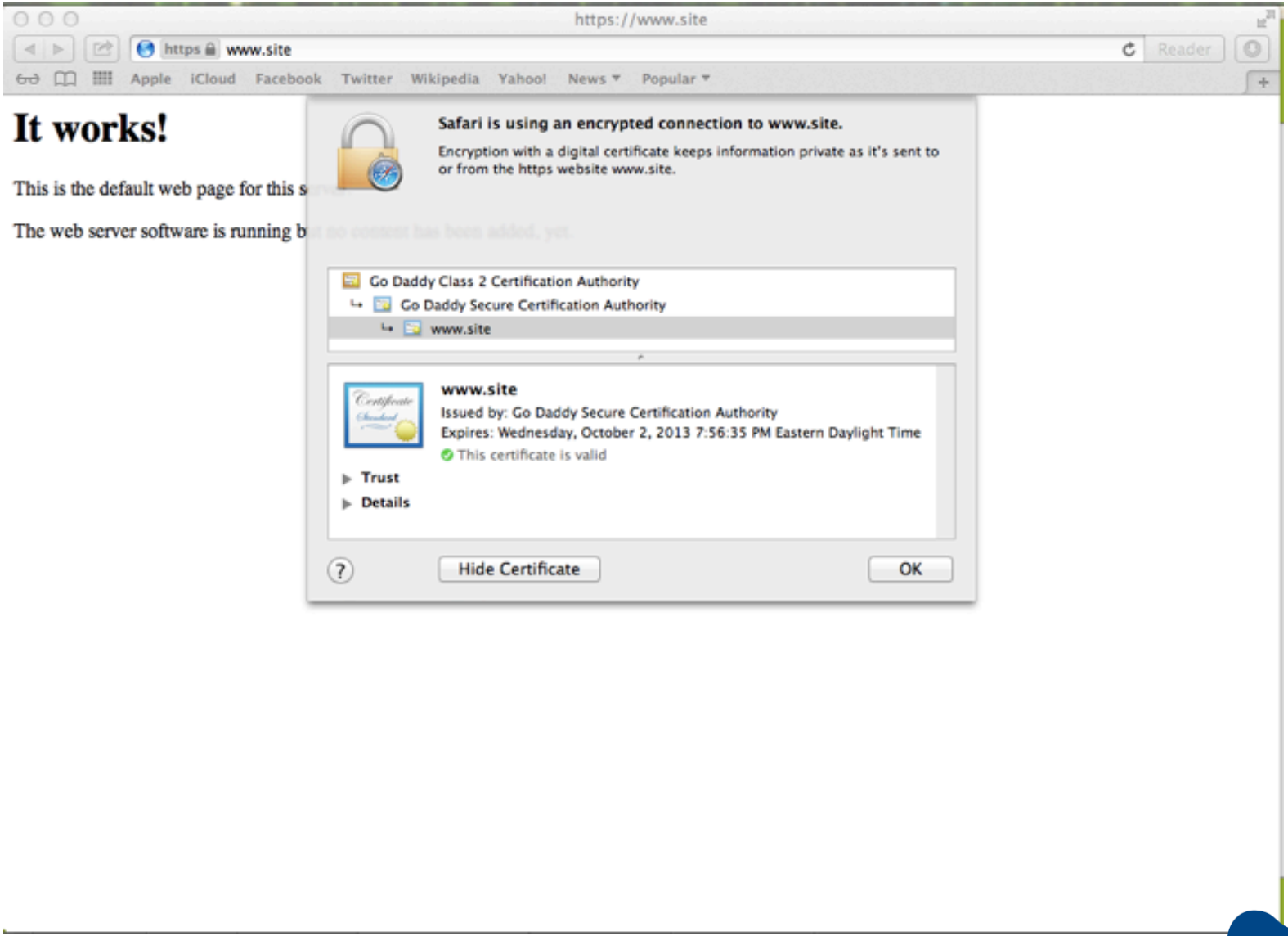
Testing

Setup a fake root

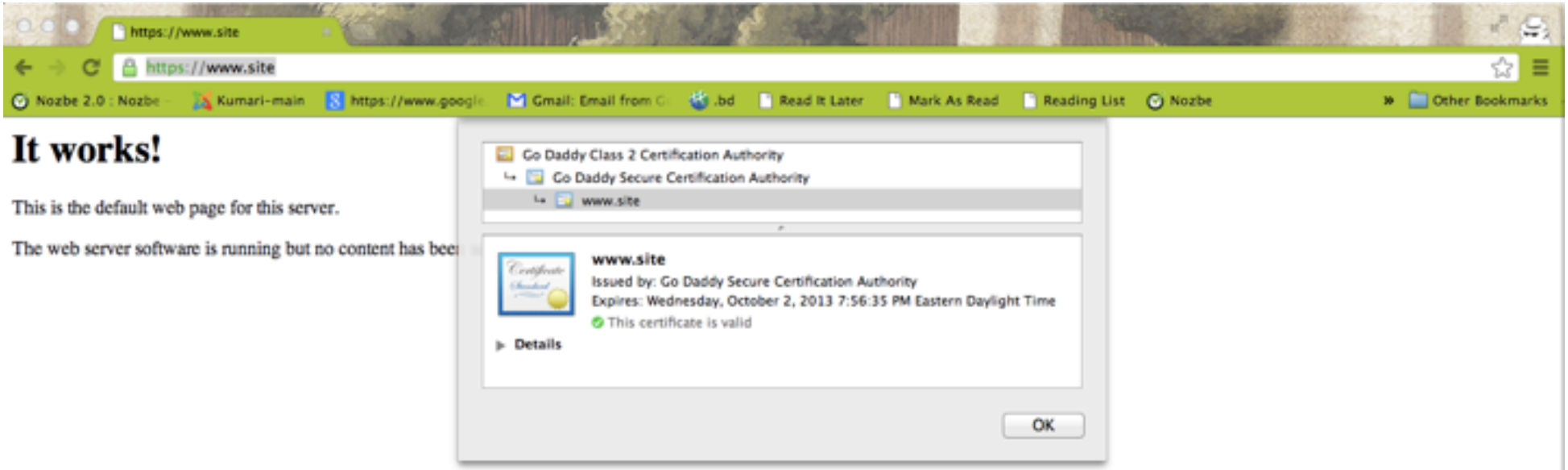
Delegated **.site** to myself

Setup a webserver, serving the cert

Doh!


https://www.site
https www.site
Reader
Apple iCloud Facebook Twitter Wikipedia Yahoo! News Popular
It works!
This is the default web page for this s
The web server software is running b
Safari is using an encrypted connection to www.site.
Encryption with a digital certificate keeps information private as it's sent to or from the https website www.site.
Go Daddy Class 2 Certification Authority
Go Daddy Secure Certification Authority
www.site
www.site
Issued by: Go Daddy Secure Certification Authority
Expires: Wednesday, October 2, 2013 7:56:35 PM Eastern Daylight Time
This certificate is valid
Trust
Details
Hide Certificate
OK

Doh!


https://www.site
https://www.site
Nozbe 2.0 : Nozbe
Kumari-main
https://www.google
Gmail: Email from
.bd
Read It Later
Mark As Read
Reading List
Nozbe
Other Bookmarks
It works!
This is the default web page for this server.
The web server software is running but no content has bee
Go Daddy Class 2 Certification Authority
Go Daddy Secure Certification Authority
www.site
www.site
Issued by: Go Daddy Secure Certification Authority
Expires: Wednesday, October 2, 2013 7:56:35 PM Eastern Daylight Time
This certificate is valid
Details
OK

Investigations by SSAC

SSAC formed a work party

Researched prevalence of non-FQDN certs

- **Using the EFF SSL Observatory data**
  - **At least 157 CAs have issued such certs**
  - **Lower bounds estimate**
- **CA/B Forum is aware of the issue**
  - **3 year from signing to revocation**

Conclusion:

- **ICANN must immediately do something**

ICANN Actions

ICANN Security Team took the lead

- "Coordinated Vulnerability Disclosure"
- Contacted CA/B Forum Chair Jan 23
- Briefed CA/B Forum Feb 5
- Ballot 96 at CA/B Forum passed Feb 26
  - 30 / 120 day period (instead of 3 years)

SAC057 published Mar 15

- Outreach, outreach and more outreach

Solved? Nope...

Not all CAs are members of the CA/B Forum

- **So not bound by these agreements**
- **But generally trustworthy / follow guidelines**

Revocation ineffective*

- **Blocking CRL / OSCP / air-gapped networks**

* : http://www.imperialviolet.org/2011/03/18/revocation.html

Registrant Protection / Credential Management

Registrant Data/Credential Attacks (Since 2010)

- Passwords (length, complexity, staleness)
- Social Engineering (Registrant and Registrar Support Staff)
- Single Factor Authentication
- Password Reset Process
- Compromised Admin email account
- Failure to Renew
- Employee Turnover (Responsible Contacts)

SSAC Existing Recommendations

Recommended Countermeasures (Summary)	SAC040	SAC044
Password Strength Requirements	✓	✓
Password Rotation	✓	✓
Brute Force Protection Measures	✓	
2FA Deployment	✓	
2FA Implementation	✓	✓
Security Training	✓	
System / Device Verification	✓	
Stronger Alternate Authentication Methods		
Use of Multiple Contact Addresses	✓	✓
Role-based contact addresses	✓	✓
Registrant Education Efforts	✓	✓
Delegated Auth for 3rd parties		✓

Participation in IGF

Key discussion topics

- What are recommendations that small and medium hosting providers could implement as they are often get caught in block lists.
- Role of circumvention tools in Internet blocking.
- Role intermediaries play.
- Need for accountability.
- Block lists should publish annual transparency reports.
- Privacy issue with block lists.
- Recommendations when using blocklists.
- Importance of outreach to judiciary.
- Link to other transparency efforts.
- MLATs are too slow…


9th MEETING OF THE
INTERNET GOVERNANCE FORUM
2-5 September 2014, Istanbul-Turkey
IGF
ISTANBUL
TURKEY
ICTA


9th MEETING OF THE
INTERNET GOVERNANCE FORUM
2-5 September 2014, Istanbul-Turkey
IGF
ISTANBUL
TURKEY
ICTA


Internet Blocking:
When Well Intentioned Measures
Go Too Far
Republic of Turkey
Ministry of Transport Maritime Affairs
and Communications
ICTA
INFORMATION AND COMMUNICATION
TECHNOLOGIES AUTHORITY
9th MEETING OF THE
INTERNET GOVERNANCE FORUM
2-5 September 2014, Istanbul-Turkey
Connecting Continents for Enhanced Multistakeholder Internet Governance
2014
IGF
ISTANBUL
TURKEY
Pendar he
people wh
field and
reputation
It's well s
of other p
of things,
worked, n

Source address filtering

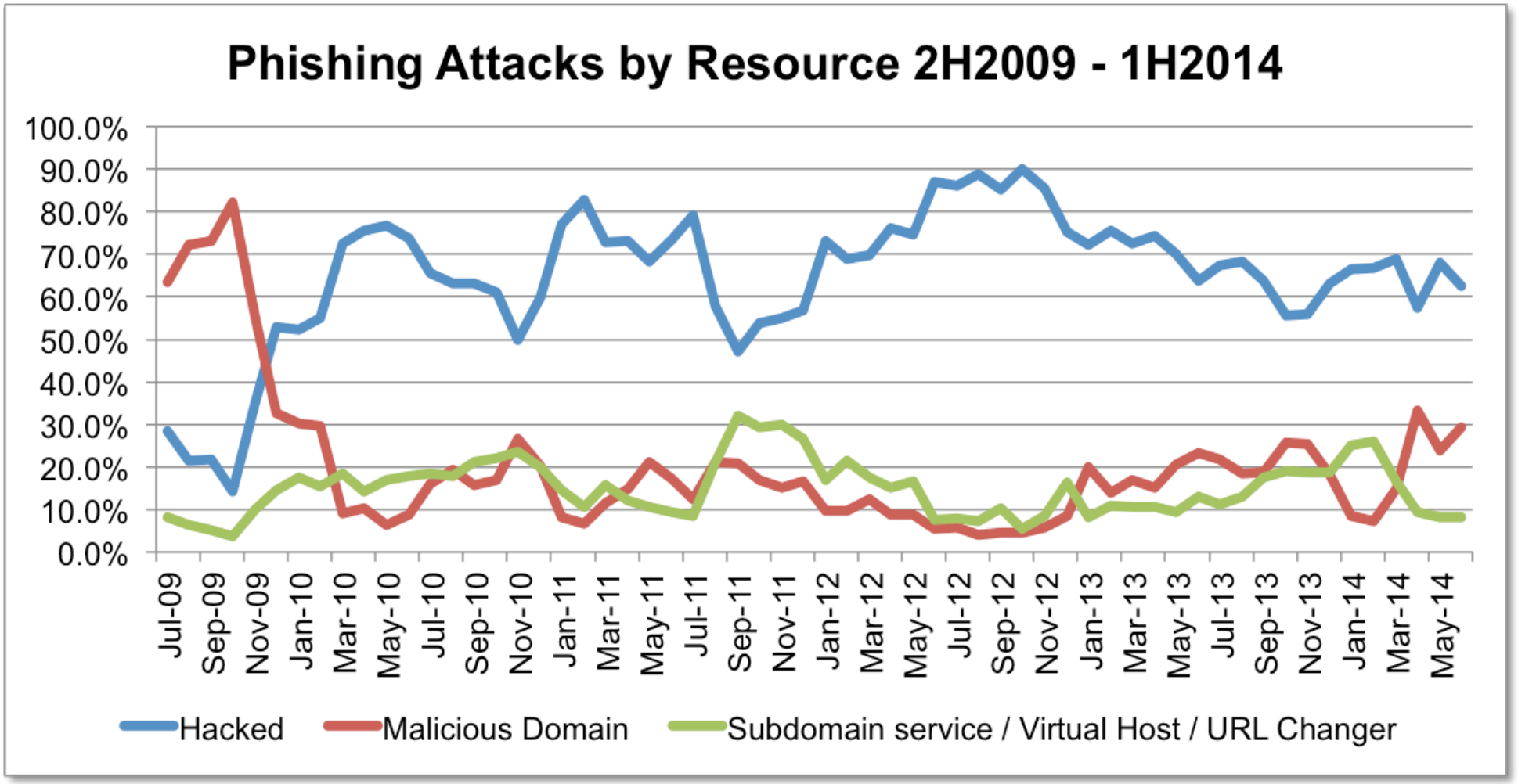
SAC-004

At every edge of the global Internet are the hosts who generate and consume the packet flows which, together, form the overall Internet traffic load. By number, most of these hosts are not secure, leading to dangerous, untraceable traffic flows which can be used to attack other hosts. This memo describes some of the security problems ”at the edge" and makes some recommendations for improvement.

SAC-004

At every edge of the global Internet are the hosts who generate and consume the packet flows which, together, form the overall Internet traffic load. By number, most of these hosts are not secure, leading to dangerous, untraceable traffic flows which can be used to attack other hosts. This memo describes some of the security problems ”at the edge" **and makes some recommendations for improvement**.

Phishing, PSL



Twenty percent of the world's malicious registrations were made in the .TK, .CF, .GA, and .ML registries. Freenom, a Netherlands-based company that offers free domain name


Thank You
ICANN