The Keys to the Internet Names As Global Critical Infrastructure

Oleksandr Tsaruk, Ph.D.
Chief adviser, Committee on ICT,
Parliament of Ukraine

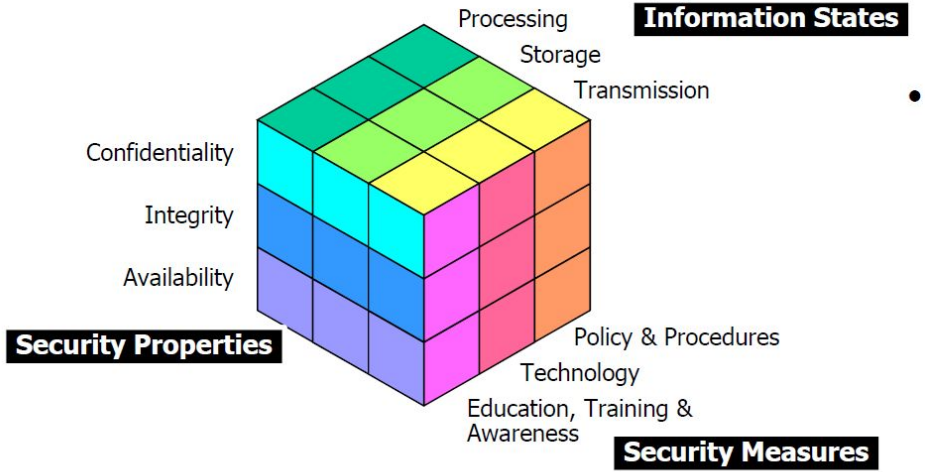
Key Prediction, 2010

The root anchors were first published on 15 July 2010 by ICANN.

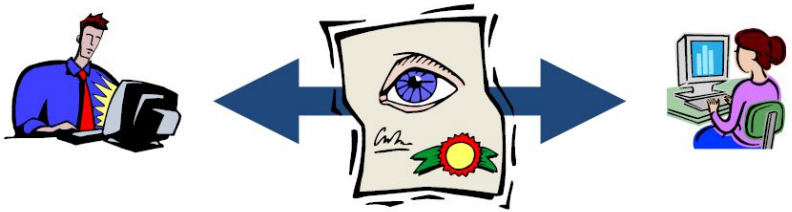
Vinton Cerf (aka “Father of Internet”) said about this event: “I would predict that although we started out putting this system together to assure that the domain name lookups return valid Internet addresses that in the long run this hierarchical structure of trust will be applied to a number of other functions that require strong authentication and so you will have seen a new major milestone in the internet story.”

Digital signature as key element of internet security

- **Information Security**



- **Electronic Signature**
  - It is a unique information which identifies a person who made an electronic document and confirms whether the electronic document has been modified or not. The electronic document has functions such as self-identification, secret protection and prevention of tampering, forging document and denying himself.

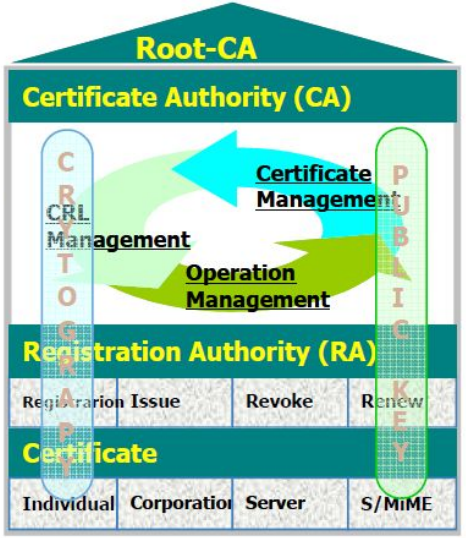


Private Key Infrastructure

- **PKI**
  - A system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

Security Services	Threat	Solution
Authenticity	Unauthorized User	Digital Signature
Confidentiality	Data Leakage	Encryption
Integrity	Data Forgery	Digital Signature
Non-repudiation	Repudiation	Digital Signature

PKI

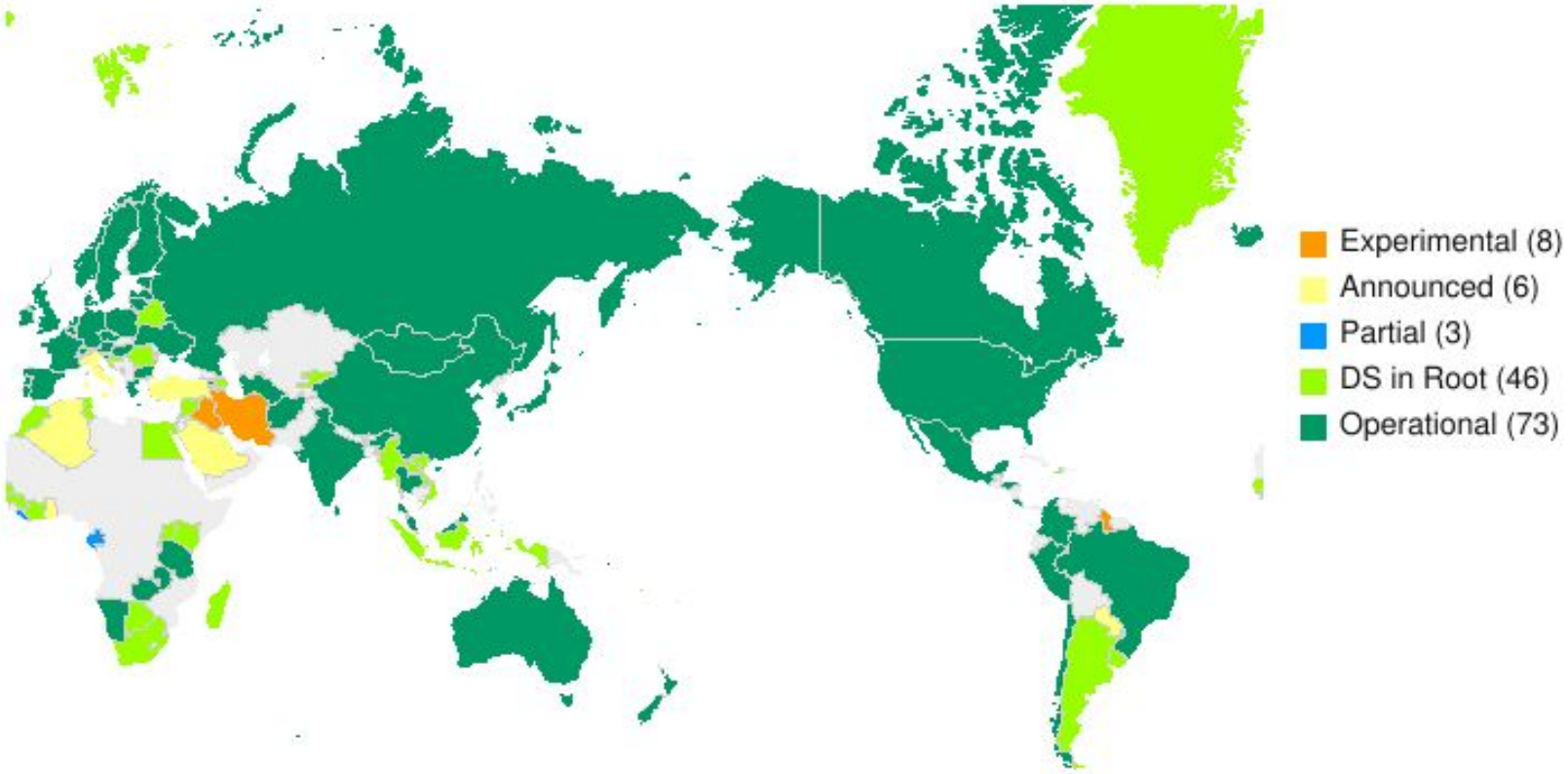


DNSSEC Deployment, 2016

Signing of domains with DNSSEC:

- 89% of top-level domains (TLDs) zones signed.
  - ~47% of country-code TLDs (ccTLDs) signed.
- Second-level domains (SLDs) vary widely:
  - Over 2.5 million .nl domains signed (~45%) (Netherlands).[1]
  - ~88% of measured zones in .gov are signed.
  - Over 50% of .cz (Czech Republic) domains signed.
  - ~24% of .br domains signed (Brazil).[2]
  - While only about 0.5% of zones in .com are signed, that percentage represents ~600,000 zones.

DNSsec in ccTLD, 2017



Distribution of Key Algorithms, 2016

Number	Algorithm	# Keys	%
1	RSA/MD5 (Deprecated)	21	0.0%
3+6	DSA/SHA-1	218	0.0%
5+7	RSA/SHA-1	1,548,639	36.4%
8	RSA/SHA256	2,453,608	57.6%
10	RSA/SHA512	13,929	0.4%
12	ECC/GOST	89	0.0%
13	ECDSA Curve P-256 with SHA-256	211,078	5.6%
14	ECDSA Curve P-384 with SHA-384	484	0.0%

Root Key Signing Key Rollover

- **February 2017**: New KSK published in Trust Anchor XML file at http://data.iana.org/root-anchors/
- **July 2017**: New KSK published in root zone as part of DNSKEY RRset signed by the old KSK.
- **September 2017**: Size increase for DNSKEY response from root name servers.
    - Root name servers include both old and new KSK DNSKEY in responses
- **October 2017**: Begin signing the root zone DNSKEY RRset with new KSK (Actual rollover event).
- **January 2018**: Old KSK is published in root zone DNSKEY RRset with revoked bit set. DNSKEY RRset includes new KSK.
- **March 2018**: Remove old KSK from the root zone.
- **May/August 2018**: Old KSK and all backups deleted

EdDSA in DNSSEC?

EdDSA has very recently been standardised for use in DNSSEC

RFC 8080 standardises two curves:

- Ed25519 (algo 15) 256-bit curve, 128-bit security, highly attractive, keys only require 32 bytes in a DNSKEY record
- Ed448 (algo 16) 448-bit curve, 224-bit security, high security

EdDSA in DNSSEC?

EdDSA support is (virtually) non-existent in software

There are good reasons to push for support:

- EdDSA is much faster
- EdDSA keys require only half the space of an equivalent ECDSA key in a DNSKEY record
- EdDSA has better security properties (see https://safecurves.cr.yp.to)

Developers are pushing for our HSM vendors to support EdDSA

Formula of Safer Internet

Safer Internet = (TSL(HTTPS) ∩ (TLS (DNSsec)))* EdDSA (1)

The formula (1) states that Transport Layer Security will be applied for HTTPS and DNSsec queries with Edwards-curve Digital Signature Algorithm. Such End-to-End trust with most advanced cryptographic encryption will guaranty that end-user traffic will be routed to real source and even in a case of interception (legal or illegal) it would not be decrypted.

Outcome

Such cryptographic improvements also needs regulatory frameworks update basing on mutistakeholder model of policy development and implementation that is widely in use inside global Internet Governance eco-system.

Q&A

Oleksandr Tsaruk, Ph.D.

https://www.facebook.com/tsaruk