

DS Automation - current work

Shumon Huque
ICANN DNSSEC & Security Workshop
ICANN 77; Washington, D.C.
June 12th 2023

DS Automation

- **DS: Delegation Signer** record ([RFC 4034](#)) - a signed record in the parent zone that indicates that a child zone is signed, and also indicates which key (SEP/KSK/CSK) is valid for the child zone.
- Establishing a new or updated DS record (e.g. when a child zone is newly signed or changes its SEP key) requires **coordination with the parent zone, and the goal is to smoothly automate this interaction.**
- The main mechanism to do so is the use of **CDS and/or CDNSKEY records** ([RFC 8078](#) - “Managing DS Records from the Parent via CDS/CDNSKEY”)
- These are published in the child and signal to the parent that a key change for the zone has happened and the DS record (set) needs to be updated.

To Scan or Not?

- How does parent detect the new CDS/CDNSKEY records?
 - Dominant method today: **Polling the child zone**.
 - Doing this comprehensively at a registry means periodically scanning all the secure delegations and querying each of them.
 - **Scanning is time consuming & inefficient**. Some have argued that it may not scale well at large registries, or as DNSSEC deployment truly ramps up.
-
- An explicit notification based system would be more efficient.
 - Under development: see Peter Thomassen's presentation on **Generalized Notifications later** in the panel.

Bootstrapping: strongly authenticated or not

- Enabling DNSSEC for the first time?
 - The signed CDS/CDNSKEY records in the child cannot be trusted, because there is no pre-established secure chain of trust.
- RFC 8078 permits weak forms of initial validation. Some have adopted additional methods: multi-vantage point confirmation of responses, etc. But ideally, we should have strongly authenticated bootstrapping.
- See “Authenticated Bootstrapping” presentation coming up, which can solve this problem in many configurations (where the DNS operator manages the nameserver names in a signed zone).

(ccTLD) DNSSEC Deployment Maps

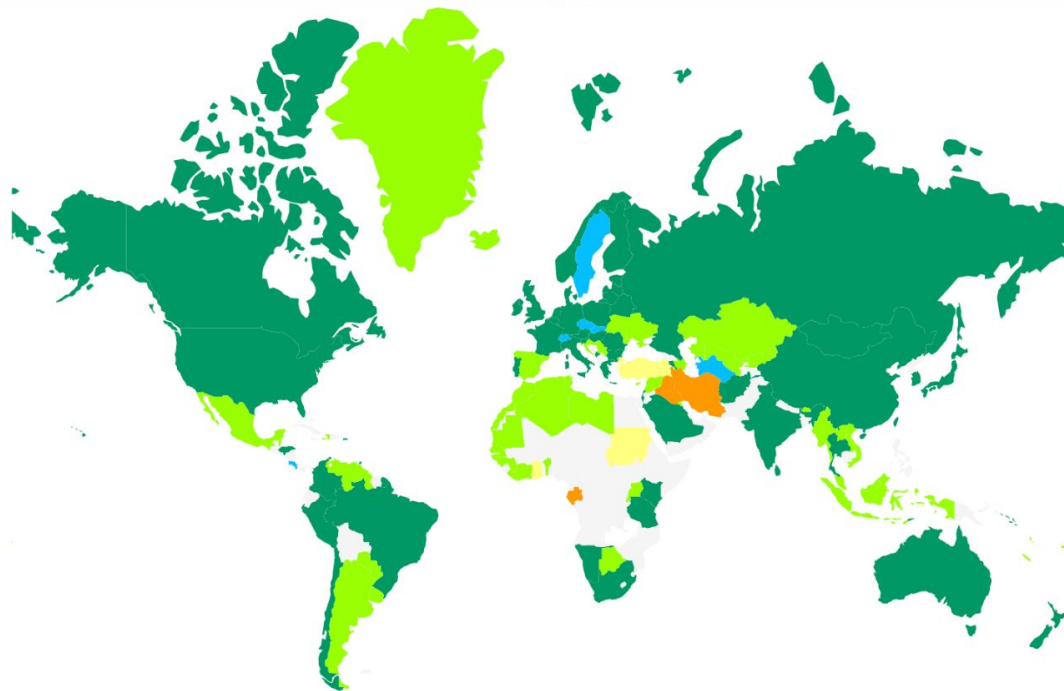
<https://maps.dnssec.gmu.edu/>

General Statistics

Total ccTLD's

160

Experimental	8	5%
Announced	4	3%
Partial	0	0%
DS in Root	69	43%
Operational	69	43%
DS Automation	8	5%



Ascension Isl...	ARUBA	BRAZIL	COTE D'IVOIRE	DENMARK	FRANCE	GREECE	INDONESIA	JERSEY	LAO PEOPLE...	LIBYAN ARAB ...	MONTserrat	NIUE	REUNION	SWEDEN	FRENCH SOU...	TAIWAN, PRO...	VIET NAM
ANDORRA	ALAND ISLAN...	BHUTAN	CHILE	DOMINICA	GABON	SOUTH GEOR...	IRELAND	JAPAN	LEBANON	MOROCCO	MAURITIUS	NEW ZEALAND	ROMANIA	SINGAPORE	THAILAND	TANZANIA, U...	VANUATU
AFGHANISTAN	AZERBAIJAN	BOUVET ISLA...	CHINA	ALGERIA	UNITED KING...	GUINEA-BISS...	ISRAEL	KENYA	SAINT LUCIA	MONACO	MEXICO	PERU	SERBIA	SAINT HELEN...	TIMOR-LESTE	UKRAINE	WALLIS AND ...
ANTIGUA AN...	BELGIUM	BOTSWANA	COLOMBIA	ESTONIA	GRENADA	GUYANA	INDIA	KYRGYZSTAN	LIECHTENSTE...	MOLDOVA, RE...	MALAYSIA	POLAND	RUSSIAN FED...	SLOVENIA	TURKMENIST...	UGANDA	SAMOA
ANGUILLA	BULGARIA	BELARUS	COSTA RICA	SPAIN	GUERNSEY	HONG KONG	BRITISH INDI...	KIRIBATI	SRI LANKA	MONTENEGRO	NAMIBIA	SAINT PIERRE...	RWANDA	SVALBARD A...	TUNISIA	UNITED STAT...	MAYOTTE
ARMENIA	BAHRAIN	BELIZE	CHRISTMAS I...	FINLAND	GHANA	HONDURAS	IRAQ	KOREA, REPU...	LIBERIA	MADAGASCAR	NEW CALEDO...	PUERTO RICO	SAUDI ARABIA	SLOVAKIA	TONGA	URUGUAY	SOUTH AFRICA
ARGENTINA	BENIN	CANADA	CYPRUS	FIJI	GIBRALTAR	CROATIA	IRAN, ISLAMI...	KUWAIT	LITHUANIA	MYANMAR	NORFOLK ISL...	PORTUGAL	SOLOMON IS...	SENEGAL	TURKEY	UZBEKISTAN	ZAMBIA
AUSTRIA	BERMUDA	COCOS (KEEL...	CZECH REPU...	MICRONESIA, ...	GREENLAND	HAITI	ICELAND	CAYMAN ISL...	LUXEMBOURG	MONGOLIA	NETHERLANDS	PALAU	SEYCHELLES	SINT MAARTE...	TRINIDAD AN...	SAINT VINCE...	
AUSTRALIA	BRUNEI DARU...	SWITZERLAND	GERMANY	FAROE ISLAN...	GUINEA	HUNGARY	ITALY	KAZAKHSTAN	LATVIA	MAURITANIA	NORWAY	PARAGUAY	SUDAN	SYRIAN ARAB...	TUVALU	VENEZUELA, ...	

General Statistics

Total ccTLD's

160

Experimental	8	5%
Announced	4	3%
Partial	0	0%
DS in Root	69	43%
Operational	69	43%
DS Automation	8	5%



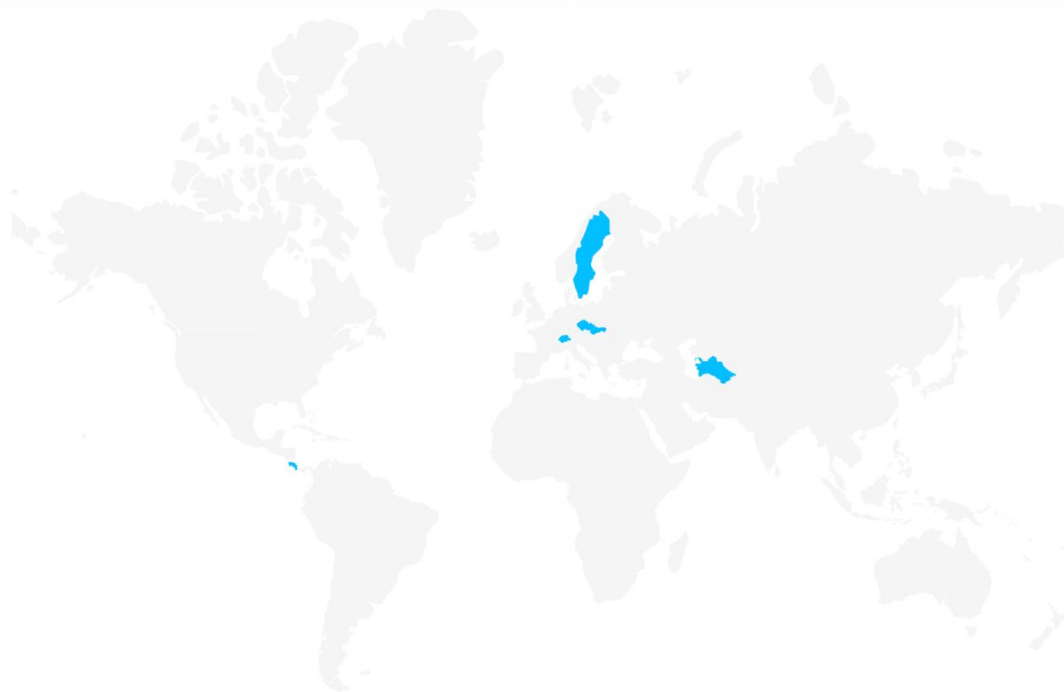
Ascension Isl...	CANADA	FRANCE	BRITISH INDI...	LATVIA	POLAND	SEYCHELLES	TAIWAN, PRO...
AFGHANISTAN	CHILE	UNITED KING...	ITALY	MONTENEGRO	SAINT PIERRE...	SAINT HELEN...	TANZANIA, U...
ARMENIA	CHINA	GREECE	JAPAN	MONGOLIA	PUERTO RICO	SLOVENIA	UNITED STAT...
AUSTRIA	COLOMBIA	SOUTH GEOR...	KENYA	NAMIBIA	PORTUGAL	SINT MAARTE...	WALLIS AND ...
AUSTRALIA	CHRISTMAS I...	HONDURAS	KIRIBATI	NORFOLK ISL...	REUNION	FRENCH SOU...	MAYOTTE
BELGIUM	GERMANY	HUNGARY	KOREA, REPU...	NETHERLANDS	ROMANIA	THAILAND	SOUTH AFRICA
BULGARIA	DENMARK	IRELAND	SRI LANKA	NORWAY	RUSSIAN FED...	TIMOR-LESTE	
BRAZIL	ESTONIA	ISRAEL	LITHUANIA	NEW ZEALAND	SAUDI ARABIA	TRINIDAD AN...	
BELARUS	FINLAND	INDIA	LUXEMBOURG	PERU	SOLOMON IS...	TUVALU	

General Statistics

Total ccTLD's

160

Experimental	8	5%
Announced	4	3%
Partial	0	0%
DS in Root	69	43%
Operational	69	43%
DS Automation	8	5%



SWITZERLAND
COSTA RICA
CZECH REPU...
LIECHTENSTE...
NIUE
SWEDEN
SLOVAKIA
TURKMENIST...

ccTLD deployments of DS automation

- Currently operational
 - .CH - Switzerland
 - .LI - Lichtenstein
 - .CZ - Czech Republic
 - .SK - Slovakia
 - .SE - Sweden
 - .NU - Niue
 - .CR - Costa Rica
 - .TM - Turkmenistan
 - Also ZA (alt.za, edu.za) - South Africa [Not yet on DNSSEC maps]
- Upcoming/In progress
 - .CL - Chile
 - Any others?

Recap of some past ccTLD DS automation talks

- ICANN 76, March 2023
 - [CDS Scanning Rollout at CentralNIC](#) - Gavin Brown
- ICANN 72, October 2021
 - [Recent DNSSEC Automation Developments in .CZ](#) - Jaromir Talir
- ICANN 71, June 2021
 - [CDS Scanning at RIPE NCC](#) - Ondrej Caletka
- ICANN 68, June 2020
 - [Support for and adoption of CDS in .CH and .LI](#) - Oli Schacher

What about gTLDs?

- Is a GTLD registry allowed to scan & take action on CDS/CDNSKEY records in registrant zones directly?
- Lack of clarity around possible ICANN contractual impediments.
- Are formal RSEP (Registry Services Evaluation Policy) requests required?
- See ICANN 69, October 2020
 - [DS Automation - Non Technical Considerations](#) - Jim Galvin
- Also ICANN 76, March 2023
 - [DNS Child Updates in the gTLD Space](#) - Francisco Arias
 - [CDNSKEY in Tango Registry Services](#) - Michael Bauland
- Let's try to clear up the confusion and allow progress in this space.

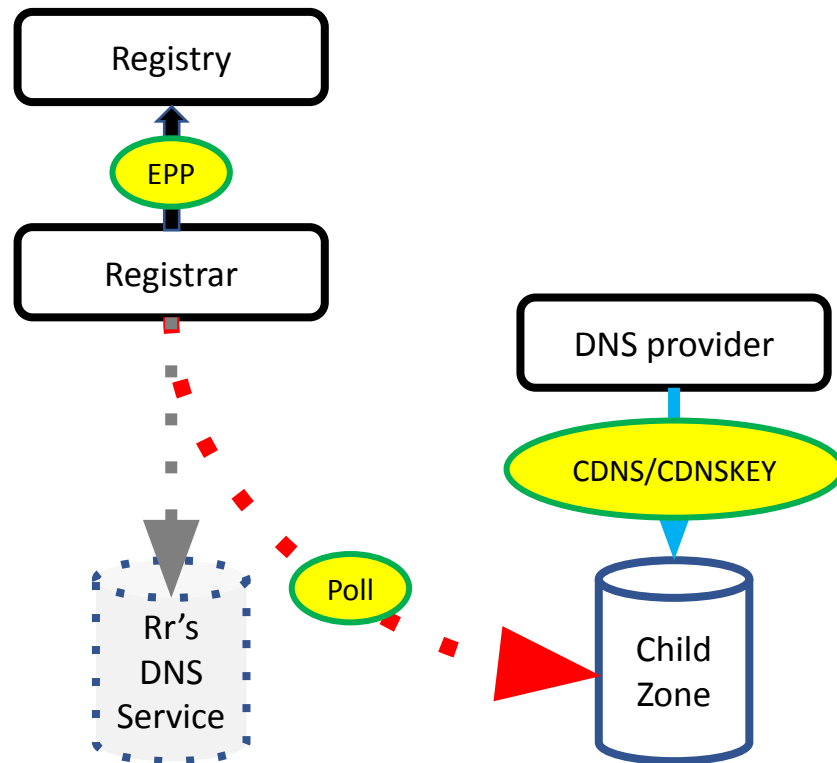
Role of 3rd party DNS operators?

- Presently, DNS operators have no defined role in the registration ecosystem.
- And have no access to the Registry.
- How can we formally recognize their role, and make them more effectively participate in DNSSEC automation efforts?

Scanning by the registrar?

- Can allow easier integration of 3rd party DNS operators.
- Registrar (rather than registry) polls for CDS and CDNSKEY records in domains under their management.
- Automatically updates DS records in the parent registry, via the usual means at their disposal (e.g. EPP or other authenticated channel to registry).
- GoDaddy currently implementing, but there are others ..
- See ICANN 76, March 2023
 - [GoDaddy Current & Proposed DS Update methods](#) - Brian Dickson

Possible Way to Convey the DS key from 3rd party DNS Provider



Registrar polls for CDS/CDNSKEY records.

GoDaddy now testing

from <https://domainname.shop/faq?id=395§ion=7¤cy=USD&lang=en>

Domainnameshop supports CDS/CDNSKEY in two different ways:

1. For domains that use Domainnameshop's nameservers but Domainnameshop is not the registrar, we will automatically publish CDS/CDNSKEY records in DNS to signal to the parent zone which DNSSEC parameters (i.e. DS records) should be active. At the moment, only a handful of TLD operators (.ch, .li, .nu, .se and .sk) periodically check for CDS/CDNSKEY records, but many others (e.g. .no and .dk) have plans to start supporting this soon.
2. For domains that do not use Domainnameshop's nameservers but Domainnameshop is the registrar, we will check daily for any CDS/CDNSKEY records in DNS. If we discover that the nameservers publish CDS/CDNSKEY records that do not match the existing DS/DNSKEY records for the zone, we will automatically update this via EPP and send an email to the domain's administrator, explaining which changes have been made to the domain.

For domains that both use Domainnameshop's nameservers and Domainnameshop is the registrar, CDS/CDNSKEY is not used. Instead, DNSSEC is updated directly via EPP.

DS Automation support in Implementations

- DNS Software Implementations.
 - ISC BIND - see upcoming presentation
 - Knot DNS (“Fully automated KSK rollovers”)
 - PowerDNS (base CDS/CDNSKEY publication support)
- Operators/Managed DNS Providers?
 - For polling based implementations, perhaps nothing needs to be supported, apart from base CDS/CDNSKEY publication support.
 - But base CDS/CDNSKEY support is lacking at many DNS providers.

When the protocol for notifications is fully fleshed out, implementations should plan to support it.

Next up

- Matthijs Mekking on DS Automation support in BIND
- Ondrej Filip on DS Automation in CZ.NIC managed domains