



# **SECIR WG: Status Update**

**Secure Email Communication for ccTLD Incident Response**

**February 10, 2015**  
**ccNSO Members Day 1**  
**ICANN52, Singapore**

Cristian Hesselman, .nl (chair)

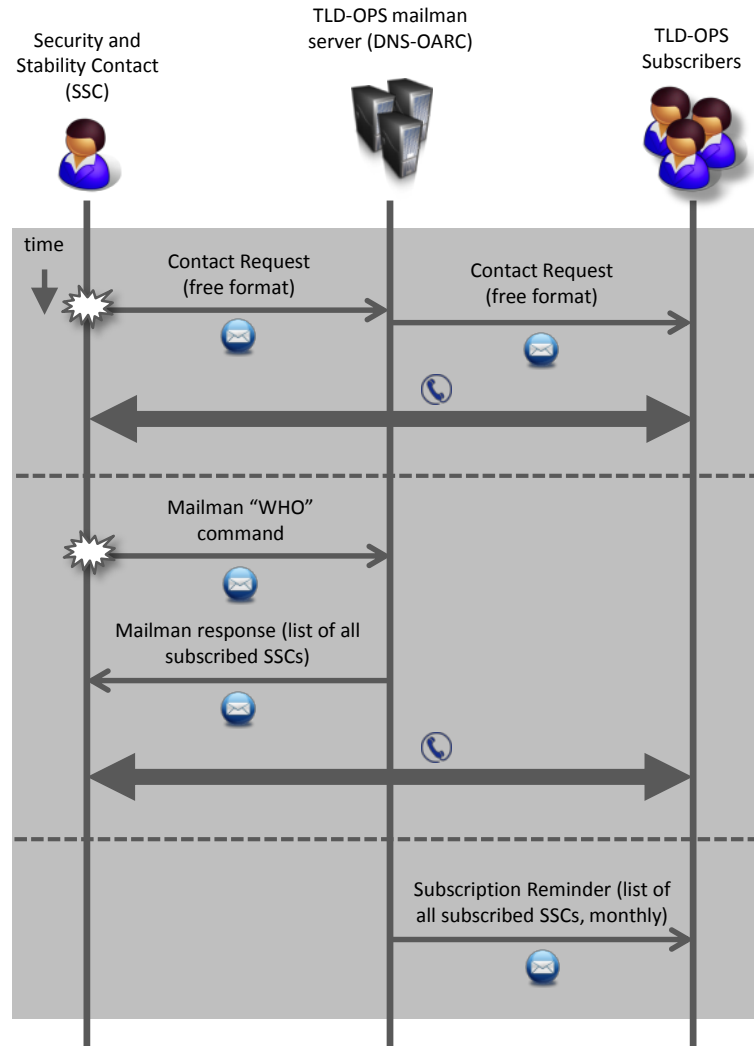
## WG Objectives

- Implement version 1.0 of a ccTLD Contact Repository
  - Enable ccTLDs to quickly and easily obtain each other's contact details
  - Exchange rudimentary incident messages
- Based on a mailing list
  - Globally accessible and easy to use
  - Development and operational costs near zero (CRI survey, Dec 2013)
  - Possibility to interface with similar systems at Regional Organizations
- Expected impact
  - Improved handling of incidents that require a coordinated response of ccTLDs at the global level
  - Such as targeted attacks on or malfunctions of registration systems, the DNS, or the Internet at large
- Contact Repository explicitly open to non-ccNSO members

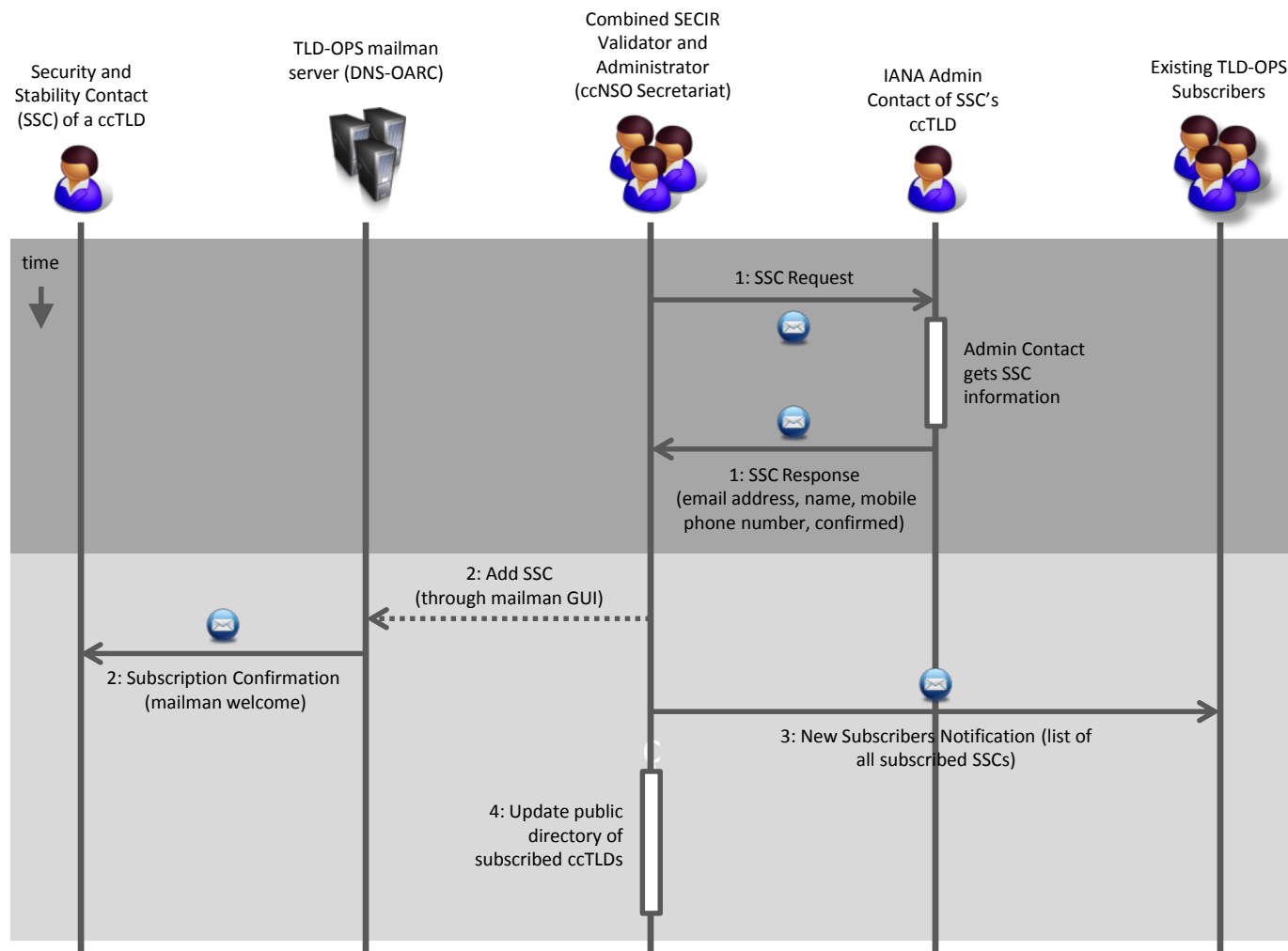
## TLD-OPS Mailing List

- Address: [tld-ops@lists.dns-oarc.net](mailto:tld-ops@lists.dns-oarc.net)
- Set up back in 2004 for similar purposes, but mostly dormant
- Members: “Security and Stability Contacts” (SSCs) of ccTLDs
- IANA Admin Contact appoints/authenticates SSCs
- May be used to exchange incident info, but not recommended
- ccNSO Secretariat is the Administrator
- DNS-OARC hosts the server (“neutral ground”)

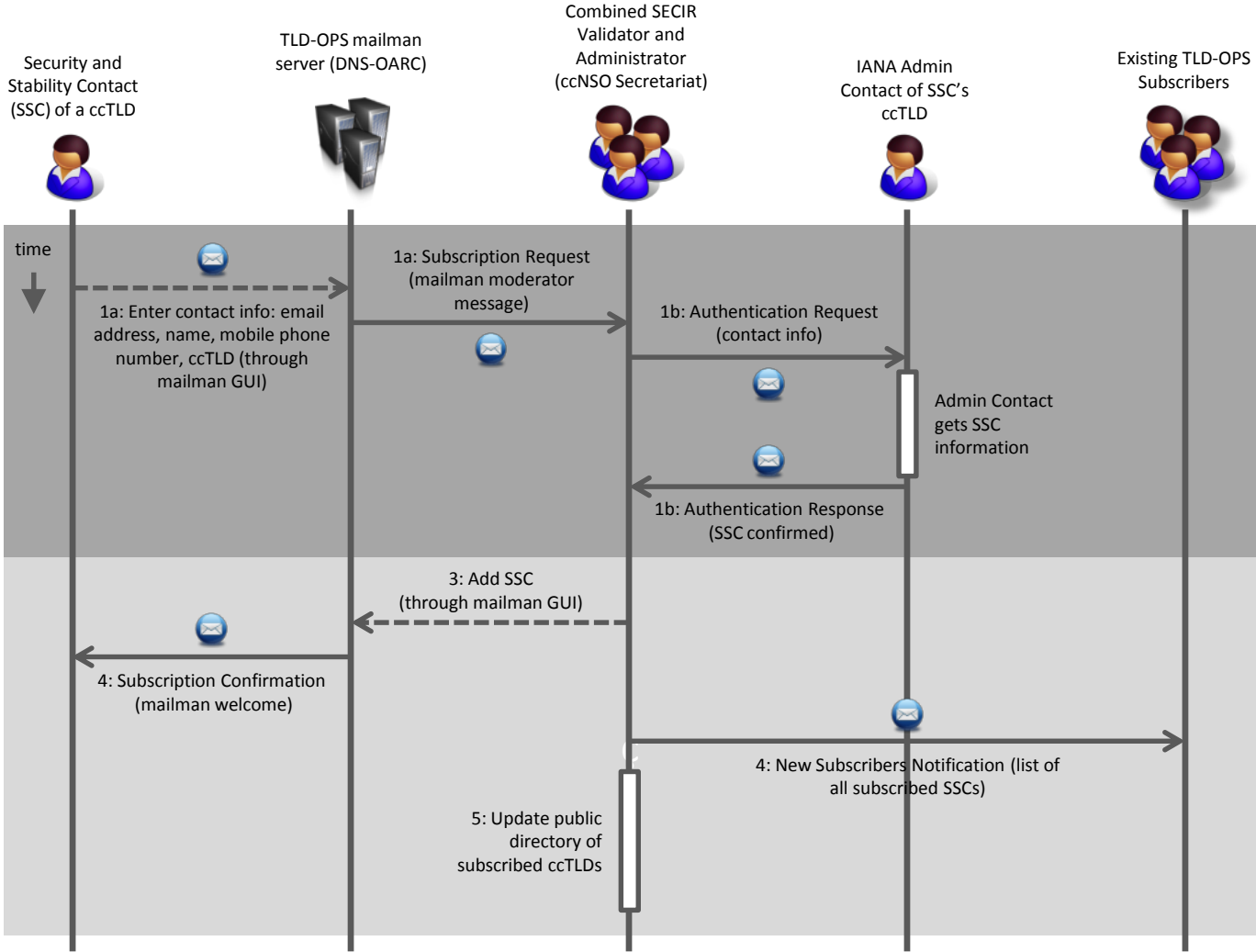
# TLD-OPS Usage



# TLD-OPS Subscription Procedure

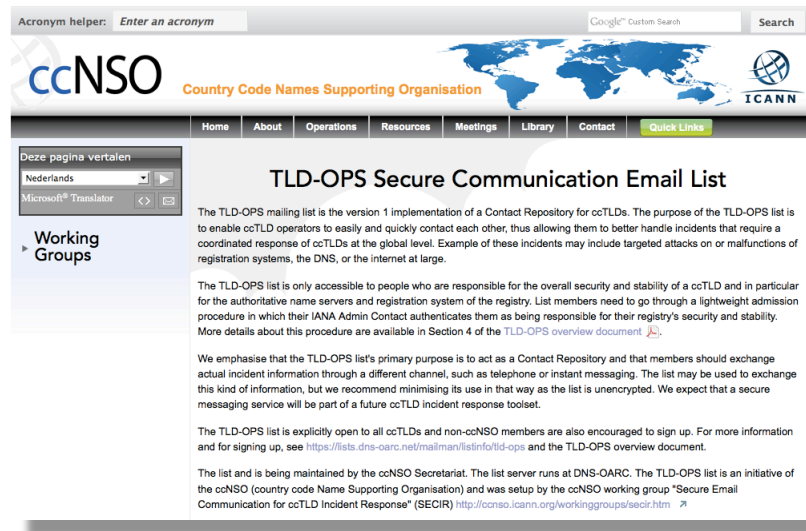


# TLD-OPS Subscription Procedure (SSC-initiated)



# Status

- Invited first batch of ccTLDs to evaluate subscription procedure
  - WG members: **.br**, **.ca**, **.dk**, **.nl**, **.tw**, and **.tz**
  - And five more, with one ccTLD per region: **.co**, **.jp**, **.uk**, **.us**, and **.za**
- TLD-OPS page on ccNSO site available
  - <http://ccnso.icann.org/resources/tld-ops-secure-communication.htm>
  - Links to TLD-OPS overview document with more info



The screenshot shows the ccNSO website with the following elements:

- Header: "Acronym helper: Enter an acronym" and "Google Custom Search Search".
- Logo: "ccNSO Country Code Names Supporting Organisation" and "ICANN".
- Navigation: "Home", "About", "Operations", "Resources", "Meetings", "Library", "Contact", "Quick Links".
- Left sidebar: "Deze pagina vertalen" (Microsoft Translator) and "Working Groups".
- Main content: "TLD-OPS Secure Communication Email List".

**TLD-OPS Secure Communication Email List**

The TLD-OPS mailing list is the version 1 implementation of a Contact Repository for ccTLDs. The purpose of the TLD-OPS list is to enable ccTLD operators to easily and quickly contact each other, thus allowing them to better handle incidents that require a coordinated response of ccTLDs at the global level. Example of these incidents may include targeted attacks on or malfunctions of registration systems, the DNS, or the internet at large.

The TLD-OPS list is only accessible to people who are responsible for the overall security and stability of a ccTLD and in particular for the authoritative name servers and registration system of the registry. List members need to go through a lightweight admission procedure in which their IANA Admin Contact authenticates them as being responsible for their registry's security and stability. More details about this procedure are available in Section 4 of the [TLD-OPS overview document](#).

We emphasise that the TLD-OPS list's primary purpose is to act as a Contact Repository and that members should exchange actual incident information through a different channel, such as telephone or instant messaging. The list may be used to exchange this kind of information, but we recommend minimising its use in that way as the list is unencrypted. We expect that a secure messaging service will be part of a future ccTLD incident response toolset.

The TLD-OPS list is explicitly open to all ccTLDs and non-ccNSO members are also encouraged to sign up. For more information and for signing up, see <https://lists.dns-oarc.net/mailman/listinfo/tld-ops> and the TLD-OPS overview document.

The list and is being maintained by the ccNSO Secretariat. The list server runs at DNS-OARC. The TLD-OPS list is an initiative of the ccNSO (country code Name Supporting Organisation) and was setup by the ccNSO working group "Secure Email Communication for ccTLD Incident Response" (SECIR) <http://ccnso.icann.org/workinggroups/secir.htm>

## Next Steps

- Invite the rest of the community
- Detail interaction with similar lists at Regional Organizations
- Schedule outreach activities
- SECIR roadmap: our recommendation on how to move forward
- Evaluation (around May)
  - Number of TLD-OPS subscribers
  - Perceived added value of TLD-OPS list
- Write-up of Final Report and closing of the WG (around ICANN53)



## Q&A

### SECIR WG Members

Frederico Neves, .br

Jacques Latour, .ca

Erwin Lansing, .dk

Cristian Hesselman, .nl (chair)

Geng-Da Tsai, .tw

Abibu Ntahigiye, .tz

### ICANN Staff

Gabriella Schitteck

### SECIR Home

[http://ccnso.icann.org/workinggroups/  
secir.htm](http://ccnso.icann.org/workinggroups/secir.htm)

### TLD-OPS Home

[http://ccnso.icann.org/resources/tld-  
ops-secure-communication.htm](http://ccnso.icann.org/resources/tld-ops-secure-communication.htm)

Cristian Hesselman

+31 6 25 07 87 33

[cristian.hesselman@sidn.nl](mailto:cristian.hesselman@sidn.nl)

@hesselma