MoSAPI and RRI TLS Client Authentication

Gustavo Lozano

ROW 11

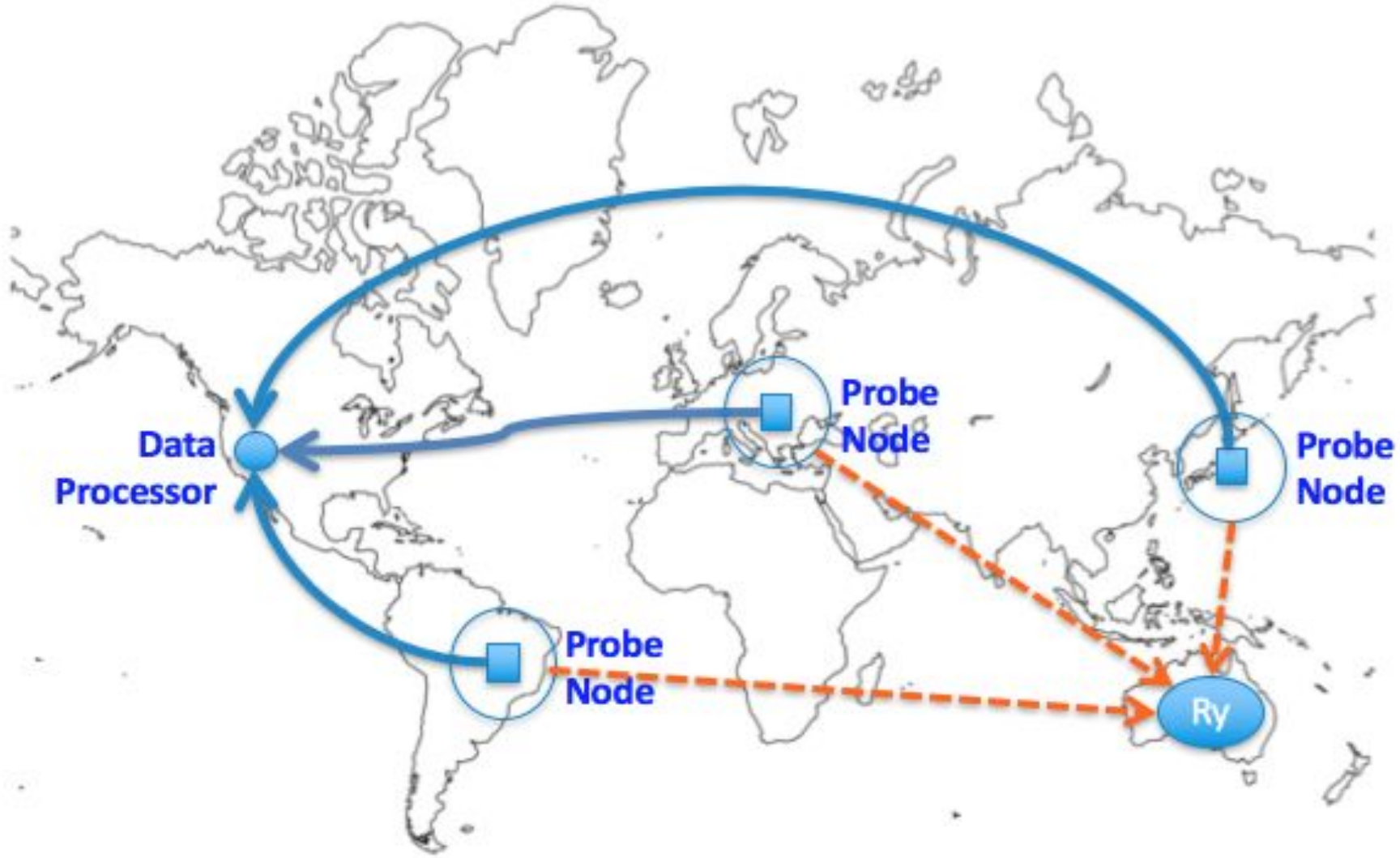
21 June 2022

SLA Monitoring (SLAM)

What is SLAM?

- Zabbix monitoring platform plus custom code
- Other parts of the code developed internally
- Probe node network consists of ≈ 40 probe nodes distributed globally
- Centralized servers that compile, analyze and act on the data collected by the probe nodes
- A Network Operations Center operating 24/7
- ICANN staff on-call 24/7

What is SLAM?



gTLDs SLA

gTLD's SLA

	Parameter	SLR (monthly basis)
DNS	DNS service availability	0 min downtime = 100% availability
	DNS name server availability	≤ 432 min of downtime (≈99%)
	TCP DNS resolution RTT	≤ 1500 ms, for at least 95% of queries
	UDP DNS resolution RTT	≤ 500 ms, for at least 95% of queries
	DNS update time*	≤ 60 min, for at least 95% of probes
RDDS	RDDS availability	≤ 864 min of downtime (≈98%)
	RDDS query RTT	≤ 2000 ms, for at least 95% of queries
	RDDS update time*	≤ 60 min, for at least 95% of probes
EPP	EPP service availability*	≤ 864 min of downtime (≈98%)
	EPP session-command RTT*	≤ 4000 ms, for at least 95% of commands
	EPP query-command RTT*	≤ 2000 ms, for at least 95% of commands
	EPP transform-command RTT*	≤ 4000 ms, for at least 95% of commands

* Not implemented yet

Emergency Thresholds

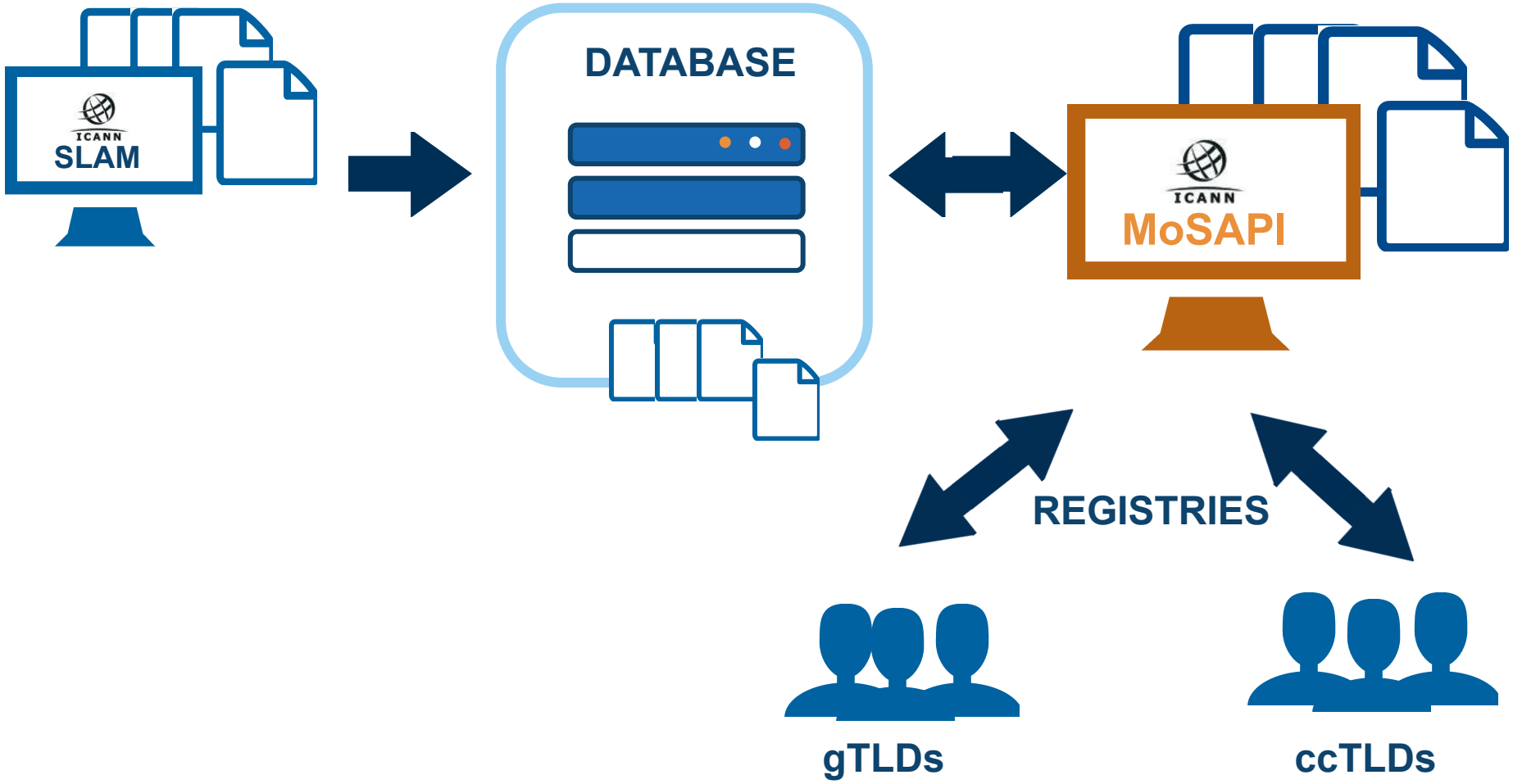
Critical Function	Emergency Threshold
DNS Service	4-hour total downtime / week
DNSSEC proper resolution	4-hour total downtime / week
EPP*	24-hour total downtime / week
RDDS	24-hour total downtime / week

* Not implemented yet

Monitoring System API (MoSAPI)

What is MoSAPI?

- REST API that allows Registries to retrieve information collected by the SLAM.



Benefits

Almost real time data*

Access to continuously test data of the DNS

Access to DAAR statistics for your TLD

Proactive monitoring

Who can use MoSAPI?

gTLD Registry Operators

&

ccTLD Registry Operators

Registration Reporting Interfaces (RRI)

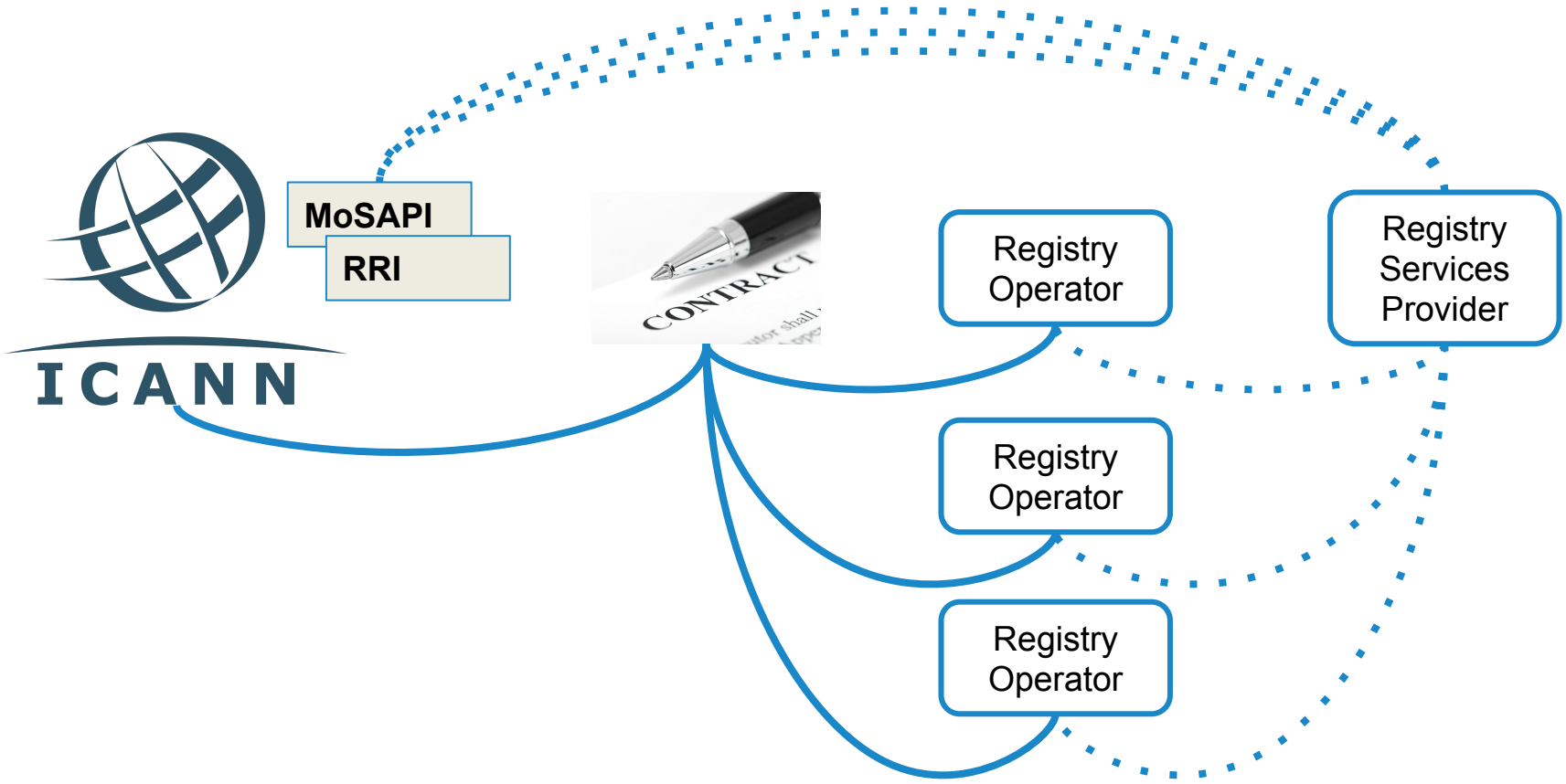
RRI

The Registration Reporting Interfaces (RRI) system is a set of interfaces provided by ICANN to contracted parties including Registry Operators and Data Escrow Agents (DEA) to fulfill and monitor their applicable reporting requirements, including:

- Per-registrar transaction reports
- Registry functions activity report
- Data escrow deposits reports
- Data escrow deposits notifications
- Registry Services – maintenance window management
- SLA Monitoring (SLAM) – probe node list retrieval

The problem

The problem


MoSAPI
RRI
ICANN
CONTRACT
Registry Operator
Registry Operator
Registry Operator
Registry Services Provider

Background

MoSAPI and RRI used to only offer HTTP Basic Authentication:

- The credentials (i.e., username and password) for the authentication are managed by the registries and need to be shared with RSPs, if shared at all
- A set of credentials is required for accessing the data of each TLD
- Only one set of credentials is allowed per TLD
- Multiple connections and login requests are required to get the information of several TLDs
- Once authenticated, the user has access to all datasets

Solution: TLS Client Authentication

How it works?

How to configure TLS Client Authentication?

- The registry provides the following information to enable TLS Client access:
  - Domain name(s) for TLS client access (e.g. rsp1.nic.example)
  - Roles that provide access to the relevant datasets:
    - SLAM - TLD SLAM Data
    - SLAM - TLD DAAR Data
    - RRI - TLD Maintenance Window
    - RRI - SLAM Probe Node List
    - RRI - TLD Monthly Reporting
    - RRI - TLD Data Escrow Daily Reporting
    - RRI - TLD Data Escrow Agent Notification

How it works?

- MoSAPI and RRI use a domain name to find one or more TLSA RR(s) that are used to authenticate the client certificate provided in the TLS connection
- An RSP may use the end-points for any TLD for which the domain name is authorized for
- Any and all the TLDs having the same domain name for TLS Client authentication can be accessed using the same certificate

Example - managing multiple TLDs

TLD	Domain Name	Roles
example01	rsp1.nic.example	SLAM Data, DAAR, TLD maintenance window
example02	rsp1.nic.example	SLAM Data, DAAR, Probe node list, TLD maintenance window
example03	rsp1.nic.example	SLAM Data, Probe node list, TLD maintenance window
example04	rsp1.nic.example	SLAM Data, Probe node list, TLD maintenance window

TLS Client Authentication benefits

- No sharing credentials between the registry and RSP
- No need to manage passwords
- Ability to obtain data for multiple TLDs using one connection
- No need for multiple credentials for several TLDs
- Multiple parties can have the same role for a given TLD (e.g., registry, RSP)
- Once the registry has set the configuration, the RSP can manage their credentials (the certificate) without having to interact with ICANN or the registry

Technical Details

Technical details

- The following combinations of TLSA Certificate Usage, TLSA Selector, and TLSA Matching Type are supported:

TLSA Certificate Usage	TLSA Selector	TLSA Matching Type
3	1	1
		2

Technical details

- The following algorithms are supported on the X.509 certificates:
  - RSA encryption with a key size of 4096 or higher.
  - Elliptic Curve public key
- The following signature algorithms are supported on the X.509 certificates:
  - sha256WithRSAEncryption
  - sha384WithRSAEncryption
  - sha512WithRSAEncryption
  - ecdsa-with-SHA256
  - ecdsa-with-SHA384
  - ecdsa-with-SHA512

Tutorial

Tutorial

1. **openssl req -x509 -newkey ec -pkeyopt ec_paramgen_curve:prime256v1 -sha256 -days 3650 -keyout tls-client.key -subj "/C=US/ST=California/L=Los Angeles/O=ICANN/OU=TS/CN=tls-client-example.example.com " -out tls-client.crt.pem**

2. **danetool --tlsa-rr --host tls-client-example.example.com --load-certificate tls-client.crt.pem**

```
_443._tcp.tls-client-example.example.com. IN TLSA ( 03 01 01
2e472dd954df1c59dfa747a05afb649ff058cbf6ca8aef04f3eb46e9c09326
02 )
```

Tutorial

3. **nsupdate**

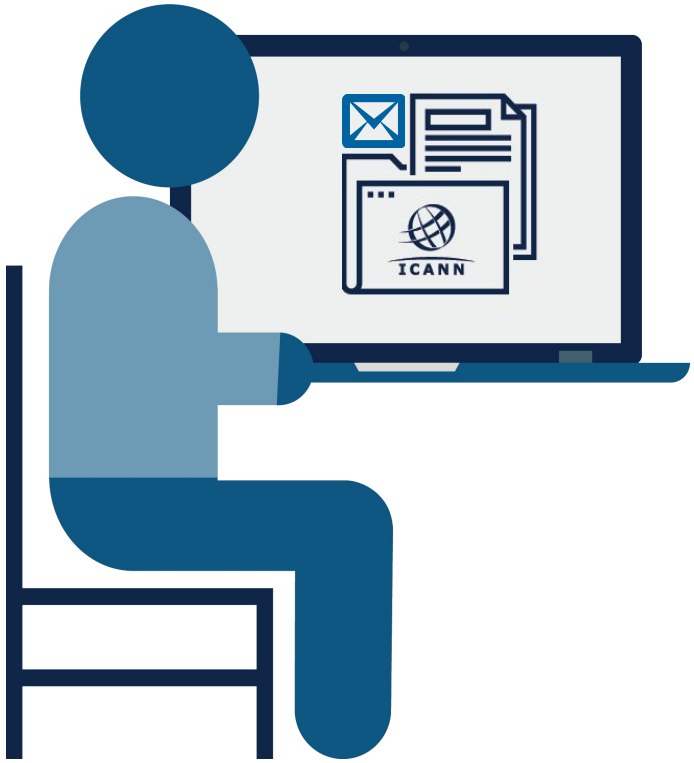
```
> server 127.0.0.1
> zone example.com.
> update add tls-client-example.example.com. 600 in tlsa 3 1 1
2e472dd954df1c59dfa747a05afb649ff058cbf6ca8aef04f3eb46e9c0932602
> send
> quit
```

4. **Configure access to the TLD using the hostname and authorized roles.**

5. **curl --cert tls-client.crt.pem --key tls-client.key https://mosapi.icann.org/mosapi/v1/example/monitoring/state**

Requesting Access

Request access



gTLDs

https://portal.icann.org/

ccTLDs

globalSupport@icann.org

The request will be authenticated with the ccTLD contacts in IANA

Q & A

One World, One Internet

Visit us at **icann.org**

@icann

linkedin/company/icann

facebook.com/icannorg

slideshare/icannpresentations

youtube.com/icannnews

soundcloud/icann

flickr.com/icann

instagram.com/icannorg