MoSAPI TLS Client Authentication

Gustavo Lozano

vTechDay ICANN 73

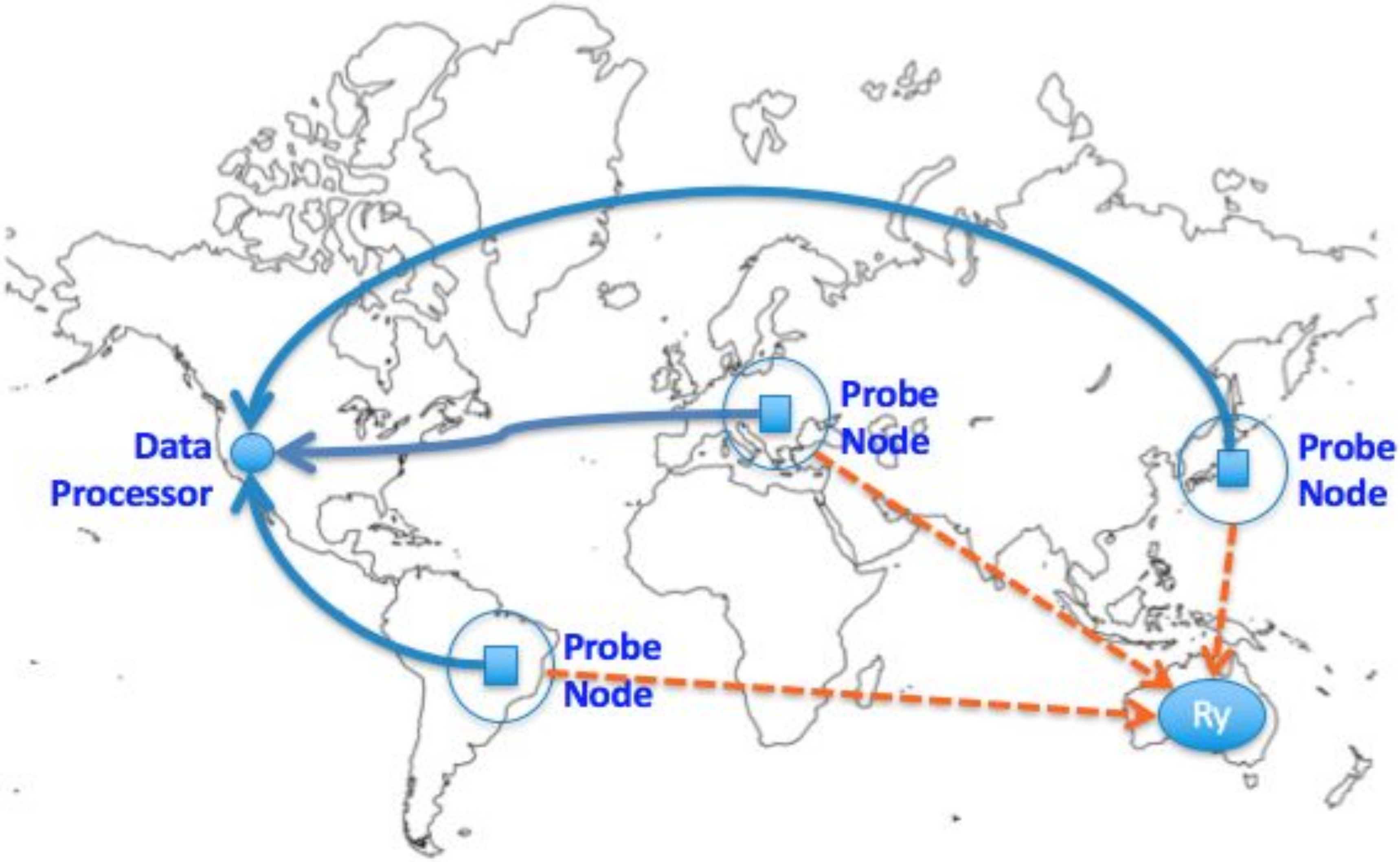
07 March 2022

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

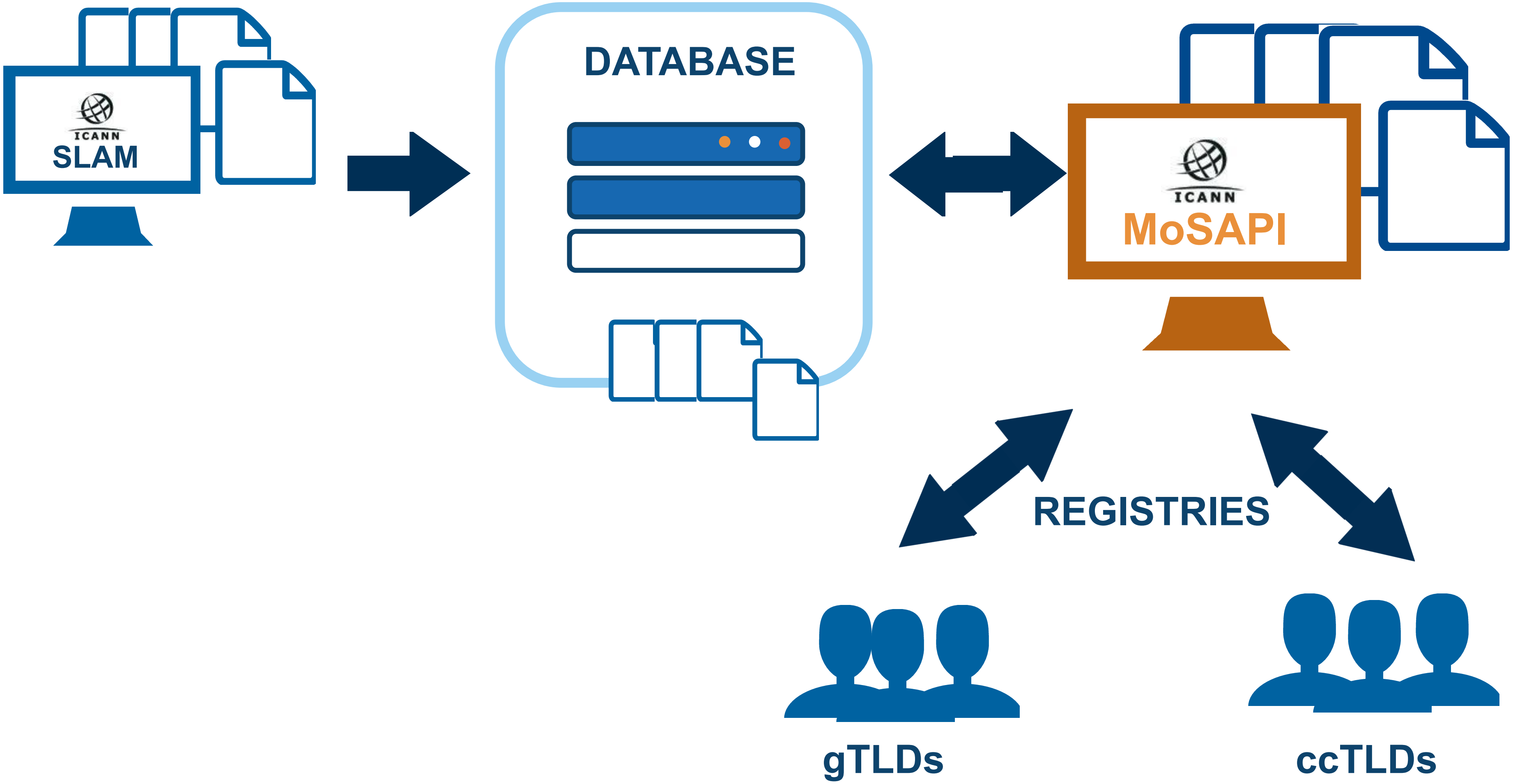
Critical Function	Emergency Threshold
DNS Service	4-hour total downtime / week
DNSSEC proper resolution	4-hour total downtime / week
EPP*	24-hour total downtime / week
RDDS	24-hour total downtime / week

* 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?

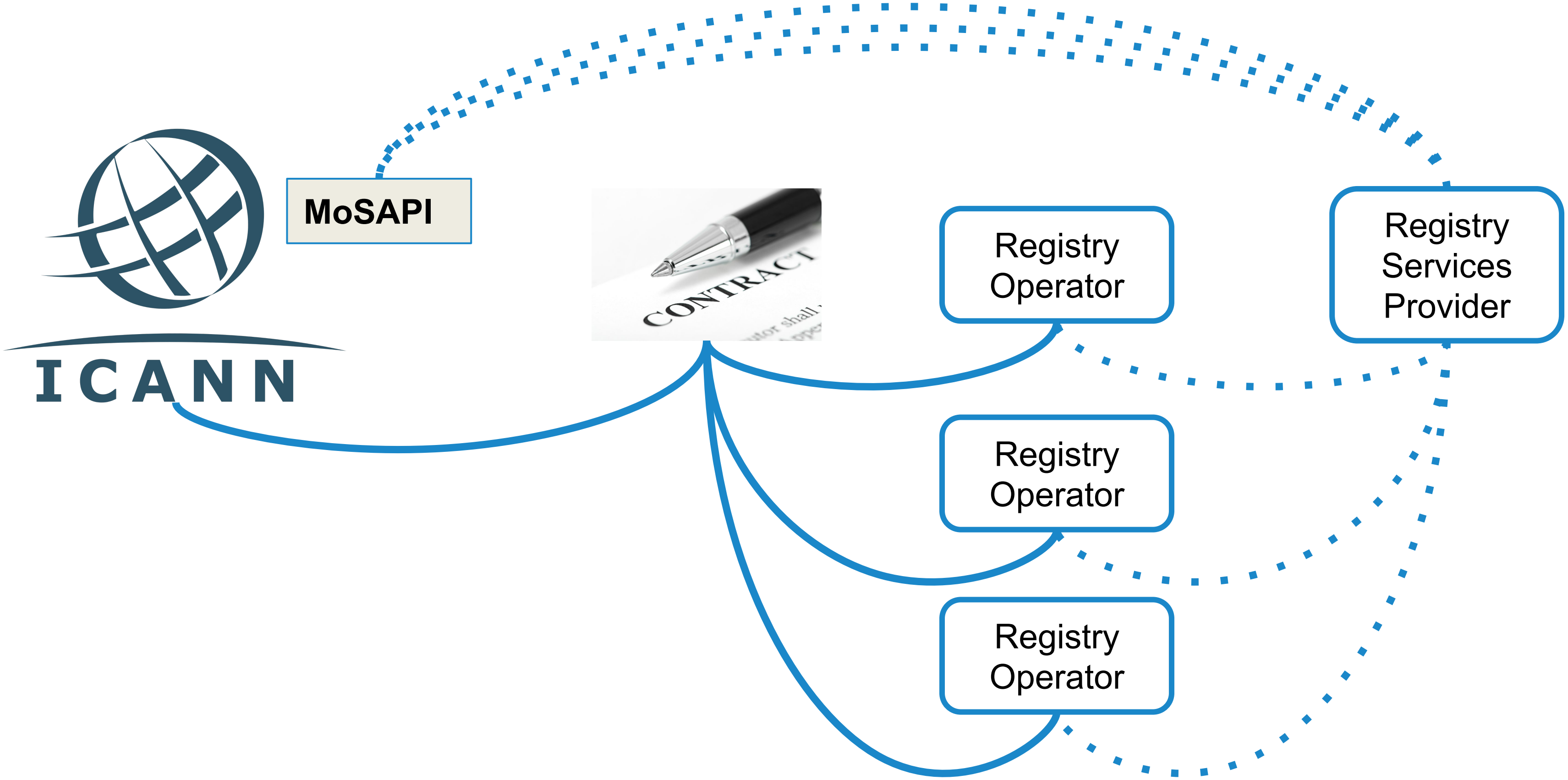
gTLD Registry Operators

&

ccTLD Registry Operators

The problem

The problem



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

Background

- MoSAPI only offered 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 when using HTTP Basic Authentication
- Once authenticated, the user has access to all roles
- 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:
    - SLAM Monitoring Data
    - DAAR

How it works?

- MoSAPI uses a domain name to find one or more TLSA RR(s) used to authenticate the client certificate provided in the TLS connection
- The 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 for TLS Auth	Roles
example01	rsp1.nic.example	mosapi_data
example01	rsp1.nic.example	daar
example01	rsp1.nic.example	mosapi_data, daar
example02	rsp1.nic.example	mosapi_data

TLS Client Authentication Benefits

- No sharing credentials with the registry
- 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 registry can manage their credentials (the certificate) without having to interact with ICANN

Technical Details

Technical details

- The following combinations of TLSA Certificate Usages Registry, TLSA Selectors and TLSA Matching Types are supported:

TLSA Certificate Usages Registry	TLSA Selectors	TLSA Matching Types
3	1	1
		2

Technical details

- The following public key algorithms are supported on the X.509 certificates used for TLS client authentication:
  - 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 used for TLS client authentication:
  - 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
```

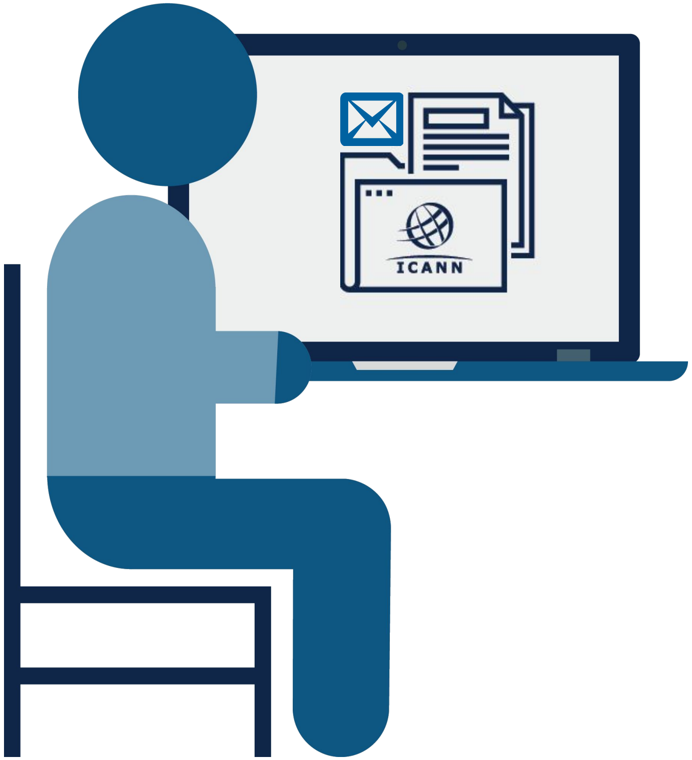
4. **Configure access to the TLD using the hostname and authorized roles.**

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

○ Request authenticated relying on the ccTLD contacts in IANA

✉ globalSupport@icann.org ▶

Q & A

ICANN

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