



**Technical Operations for Registries**  
a.k.a.  
**Registry Wellness Program**

# Agenda

---

- Registry Data Escrow
- Monthly Reports
- Zone File Access
- BRDA
- SLA Monitoring System
- Arringo Game

# Question to the Audience

**What has been most technically challenging for Registries?**

# Registry Data Escrow

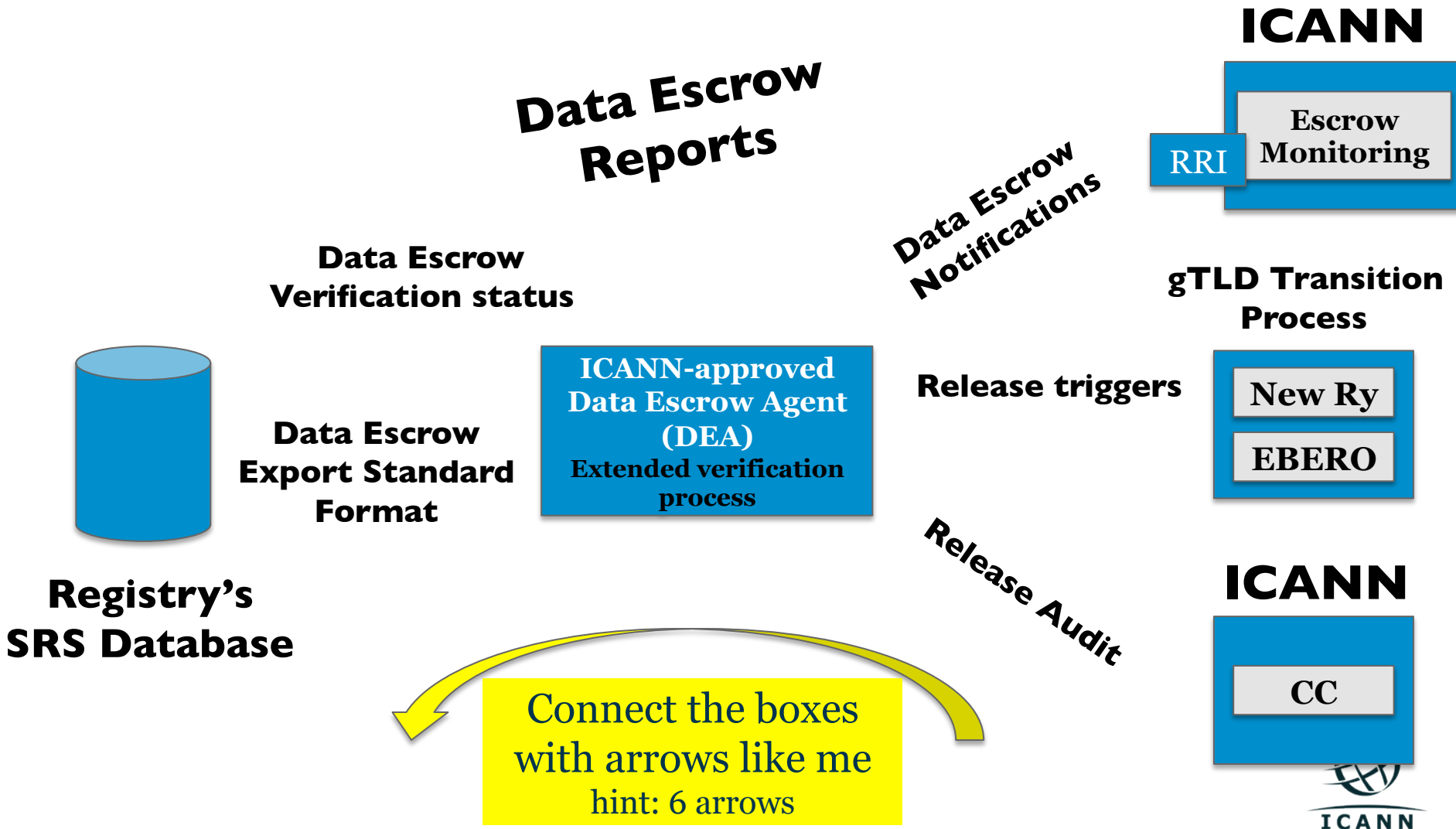
# Data Escrow - Overview

---

- Data Escrow is like an insurance policy.
- Data Escrow is the last resort in case of a TLD emergency.
- The EBERO process require the Data Escrow Deposits for a successful TLD transition.

# Data Escrow – High level view of the process


## Connect the Boxes Arringo Game



# Data Escrow – High level view of the process

## Connect the Boxes Arringo Game

**Yell Out **Arringo!****  
**When you are done**  
**Bring your up your completed**  
**sheet for verification and Win!**



Connect the boxes  
with arrows like me  
hint: 6 arrows

# Data Escrow – High level view of the process

**Data Escrow Reports**

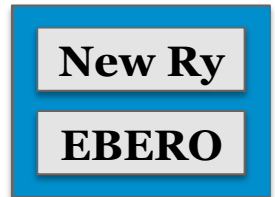
**ICANN**



**Data Escrow Notifications**

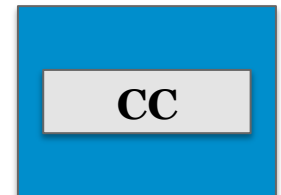
**gTLD Transition Process**

**Release triggers**



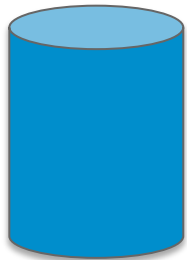
**Release Audit**

**ICANN**



**Data Escrow Verification status**

**Data Escrow Export Standard Format**



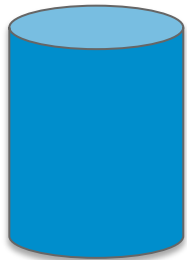
**Registry's SRS Database**



# Data Escrow – High level view of the process

## Data Escrow Reports

Data Escrow  
Verification status



Data Escrow  
Export Standard  
Format

ICANN-approved  
Data Escrow Agent  
(DEA)  
Extended verification  
process

Data Escrow  
Notifications

Release triggers

Release Audit

ICANN

RRI

Escrow  
Monitoring

gTLD Transition  
Process

New Ry

EBERO

ICANN

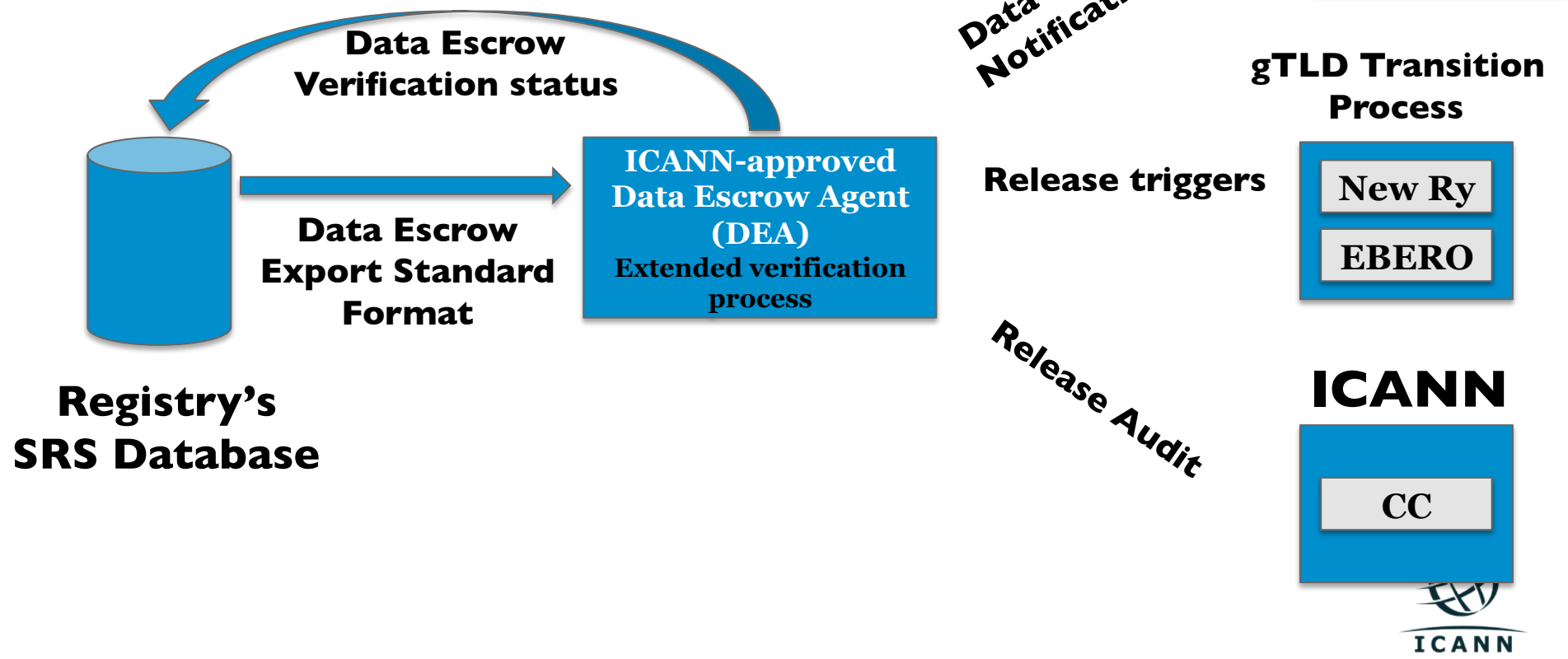
CC



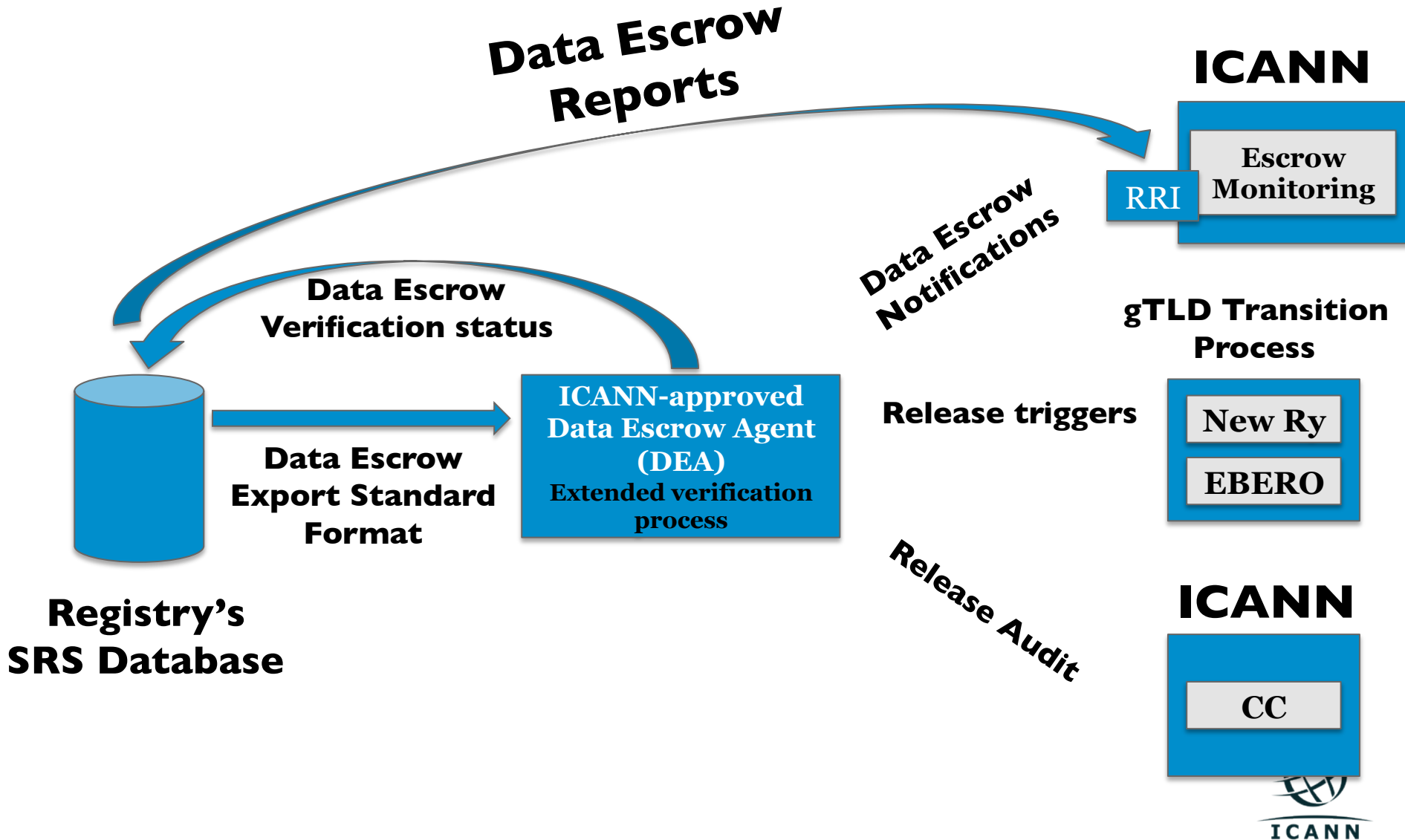
Registry's  
SRS Database

# Data Escrow – High level view of the process

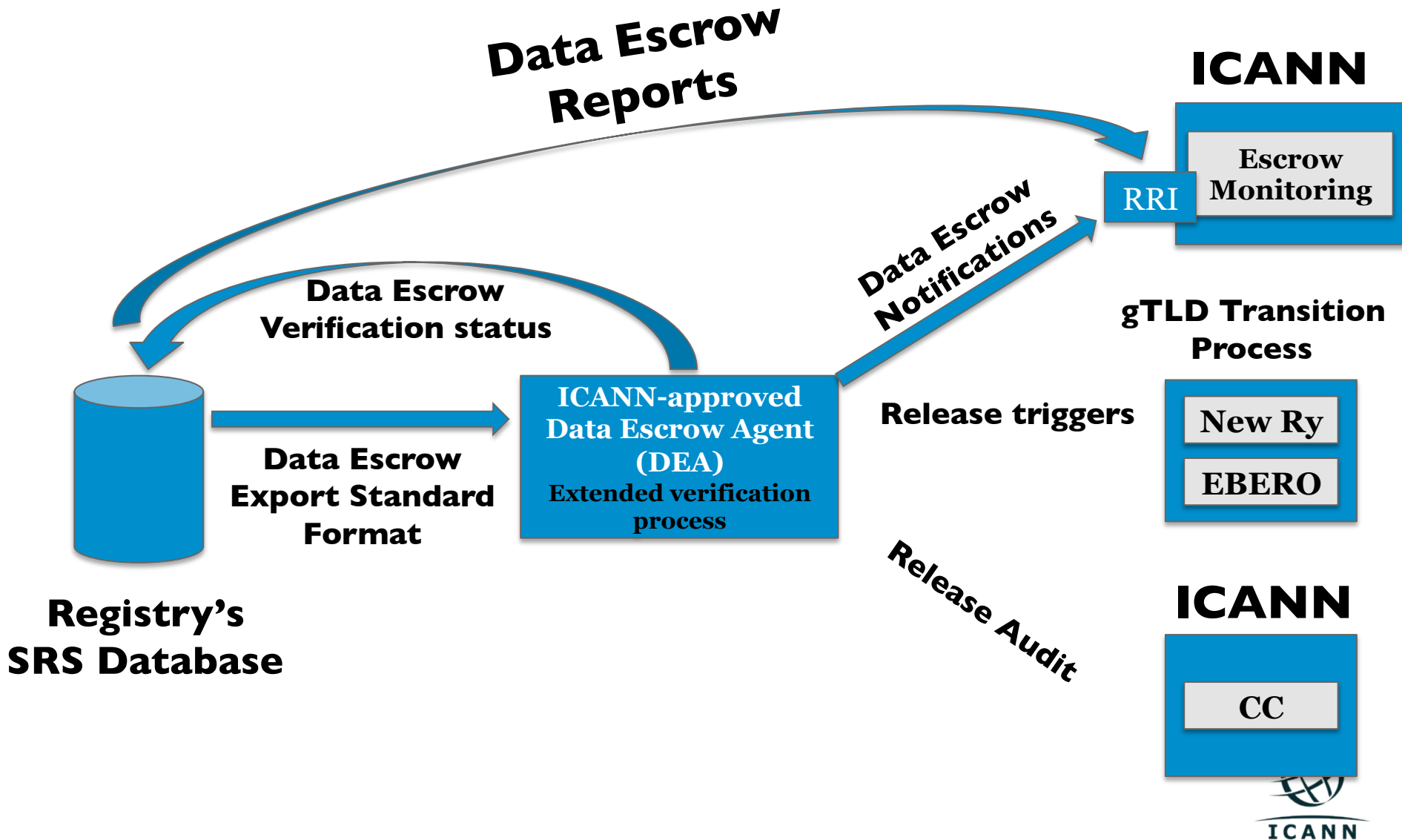
## Data Escrow Reports



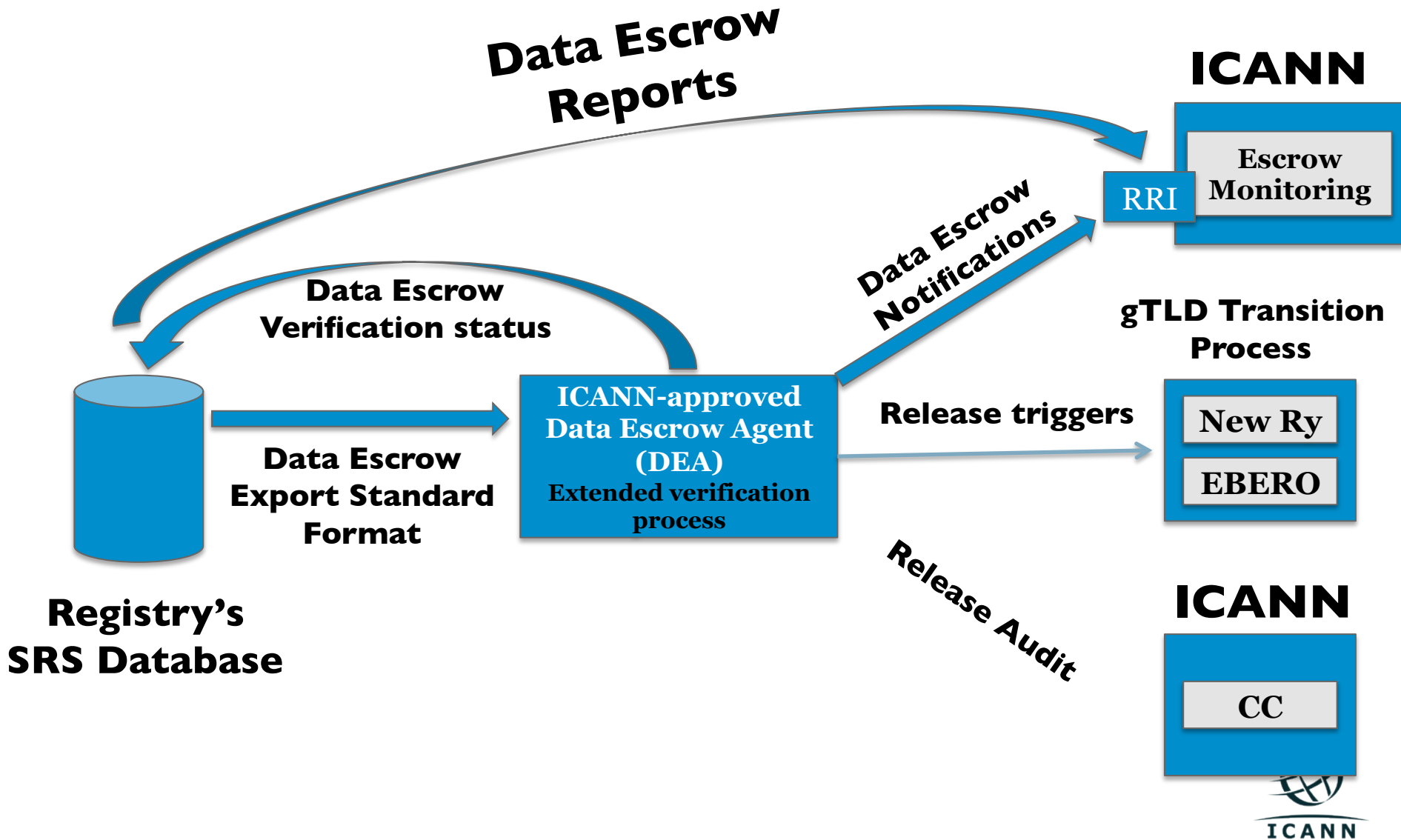
# Data Escrow – High level view of the process



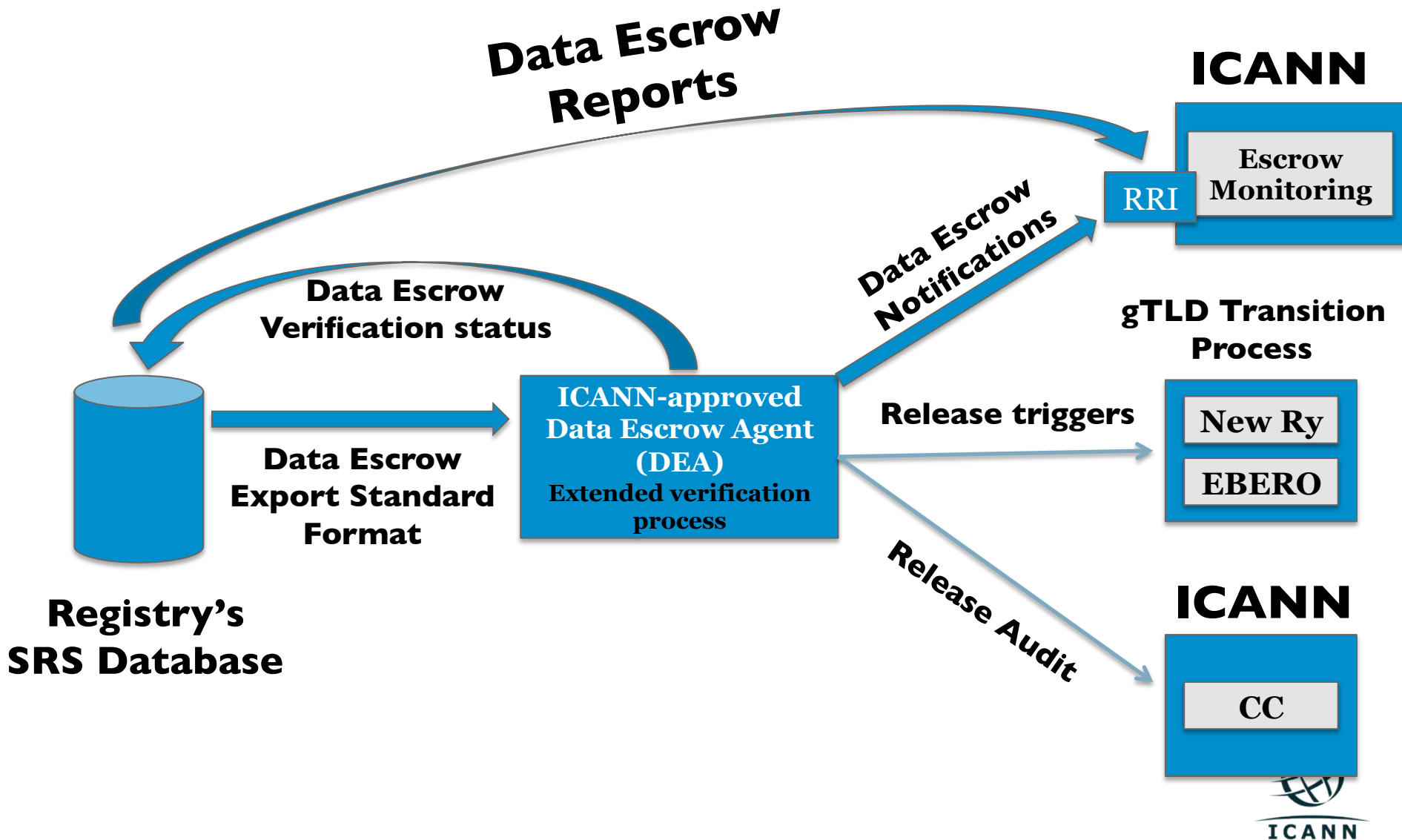
# Data Escrow – High level view of the process



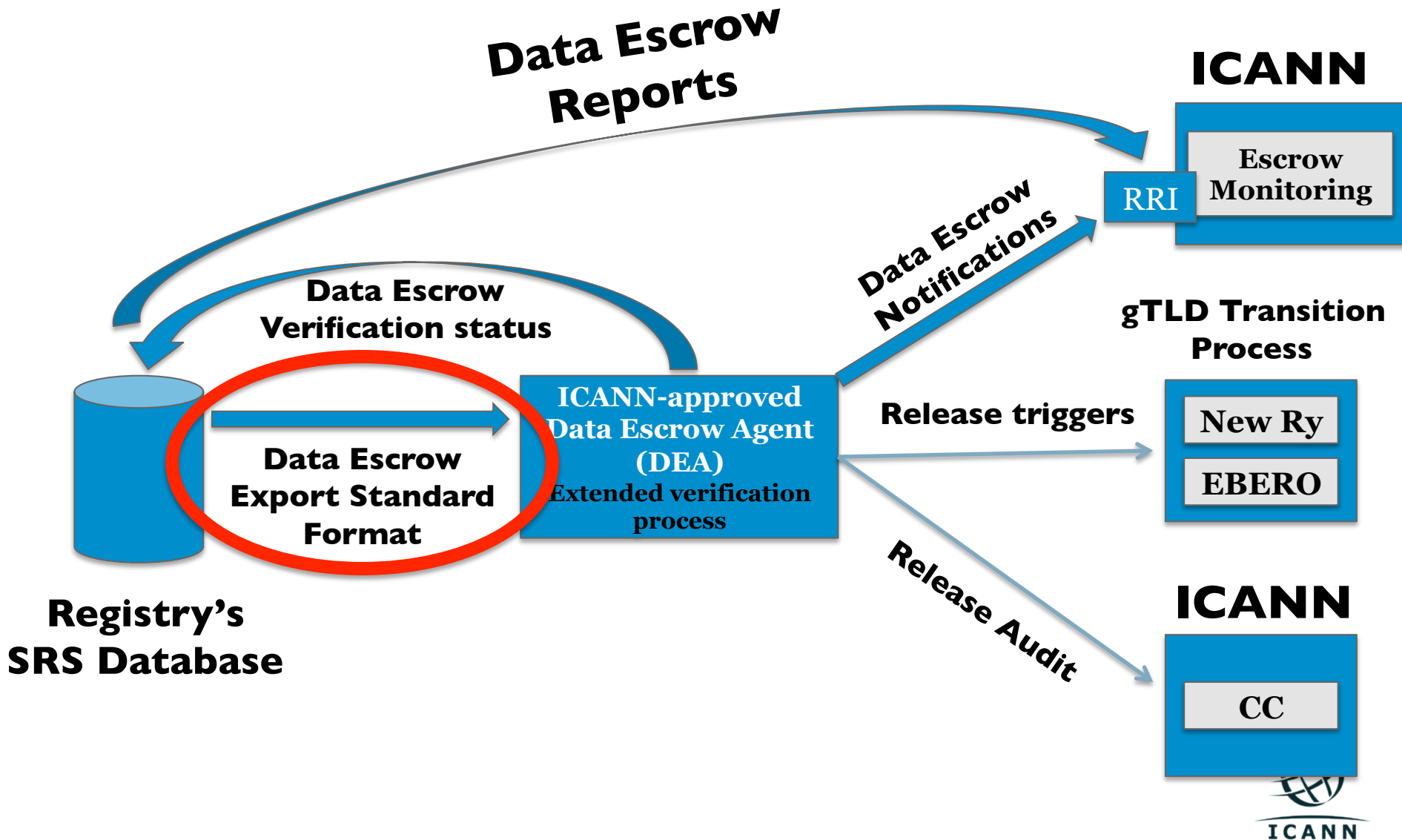
# Data Escrow – High level view of the process



# Data Escrow – High level view of the process



# Data Escrow – High level view of the process



# Data Escrow – Format

---

- Two internet drafts are being developed:
  - <http://tools.ietf.org/html/draft-arias-noguchi-registry-data-escrow>
  - <http://tools.ietf.org/html/draft-arias-noguchi-dnrd-objects-mapping>
- The first draft defines the escrow deposit container.
- The second draft defines how the SRS objects are escrowed.



# Data Escrow – Format

---

- <http://tools.ietf.org/html/draft-arias-noguchi-registry-data-escrow>

**Container**

**Escrow  
Deposit**

# Data Escrow – Format

---

- <http://tools.ietf.org/html/draft-arias-noguchi-dnrd-objects-mapping>
- This draft defines how to escrow the objects used by Domain Name Registries.
- Objects escrowed:
  - Domains
  - Hosts
  - Contacts
  - Registrars
  - NNDN (reserved domain names)
  - IDN practices
  - ...

# Data Escrow – Format

---

- A standard set of data elements was defined with the technical community per object.
- The standard set of data elements should be enough for the customary services + IDNs, but the format is extensible.
- If a Registry is going to provide Registry Services different from the customary services, the Registry and ICANN need to agree on the data escrow extensions.

# Data Escrow – Format

---

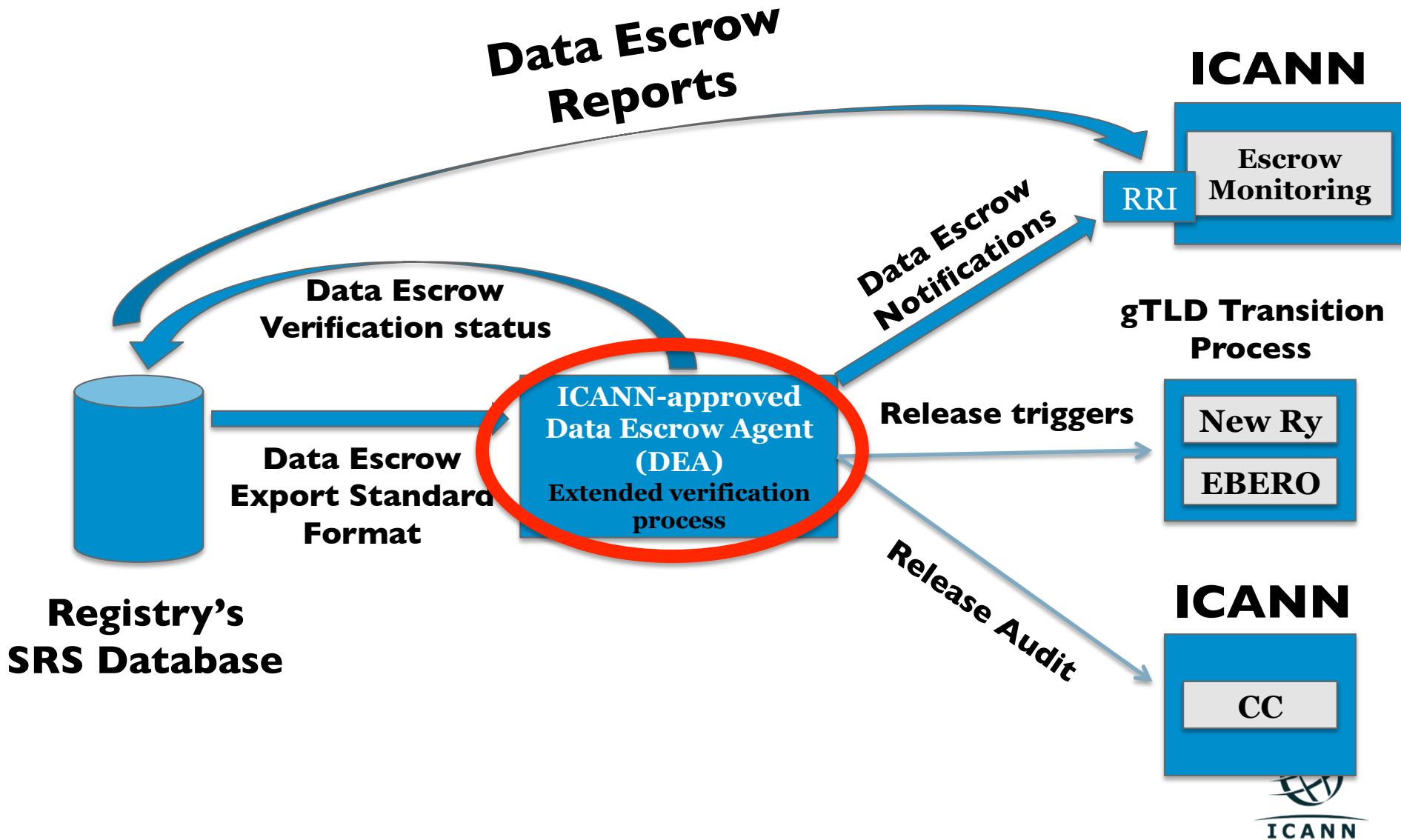
- Two kinds of deposits can be used by Registries as specified in the Registry Agreement:
  - Full
  - Differential
- Full: All objects must be escrowed.
- Differential: Delta between the escrowed watermark and the previous watermark.

# Data Escrow – Format

---

- Two sub-formats are supported:
  - XML
  - XML+CSV
- XML and CSV data elements have been normalized.
- EBEROs and DEAs **MUST** support both formats.

# Data Escrow – High level view of the process



# Data Escrow – Extended Verification Process

---

## Upon reception of a deposit, the DEA:

- The Data Escrow Agent **MUST** perform an extended verification process using the contents of data escrow deposits to a point in time (watermark) or last full deposit plus all differential deposits.

# Data Escrow – Extended Verification Process

---

## Upon reception of a deposit, the DEA validates:

- The escrow deposits using the definition agreed with the Registry.
- The number of objects is equal to the number of objects reported in the <header> element of the escrow deposit of that point in time (watermark).
- All contacts linked to domain names are present.
- All registrars linked to other objects are present.
- A name exists only as a domain name or NNDN.
- The elements listed in the <policy> element are present.
- All idnTableRef definitions linked from other objects are present.



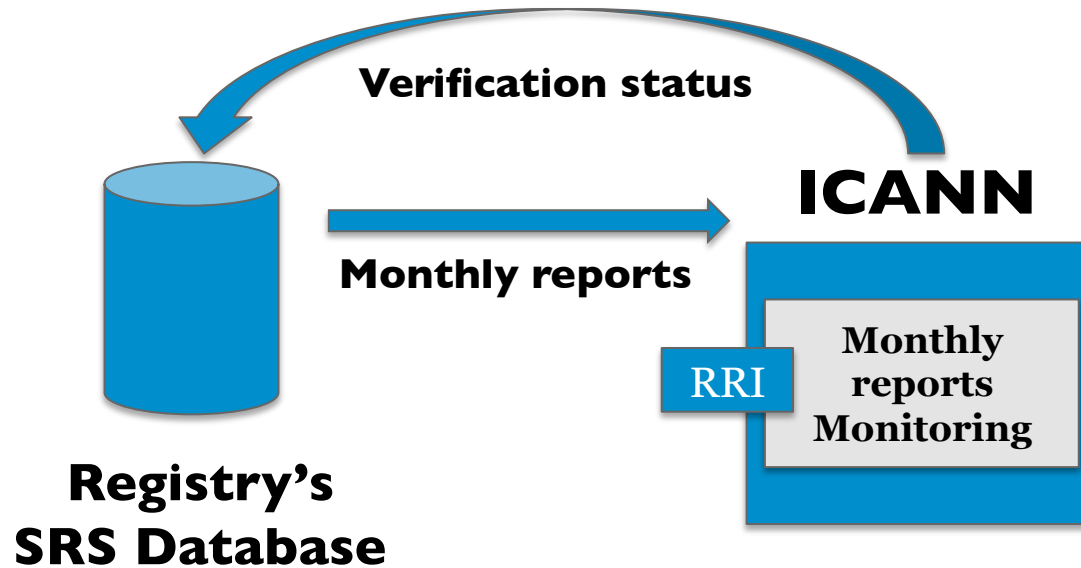
# Monthly Reports

# Monthly Reports – Overview

---

- There are two monthly reports defined in the Registry Agreement:
  - Per-Registrar Transactions Report
  - Registry Functions Activity Report
- Per-Registrar Transactions Report: this report contains the number of transactions per Registrar.
- Registry Functions Activity Report: this report contains the different operational statistics from the Registry.

# Monthly Reports – High level view of the process



# Monthly Reports – Format

---

- The format of the monthly reports is defined in Specification 3 of the Registry Agreement (<http://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm>).
- The format of the reports is CSV.
- Note: the design principle of the **Per-Registrar Transactions Report** is to report the transaction once the related grace period is over. For example, once the AGP is over or once the domain is purged.

# Registry Reporting Interface

# Registry Reporting Interface

---

- Software platform that allows automation of the following operational tasks:
  - Daily escrow notifications from DEA
  - Daily escrow reports from Registry Operator
  - Monthly reports
- API defined in:
  - <http://tools.ietf.org/html/draft-lozano-icann-registry-interfaces>

# I am a Registry, How to comply with Data Escrow?

# Data Escrow / Monthly Reports, How to comply?

---

## Onboarding:

1. **(OPTIONAL)**, Test your implementation in the RRI OTE. Open a case with ICANN's CSC in order to obtain access to the RRI OTE.
2. Create credentials (**per TLD**) for you and your Data Escrow Agent in RRI.

## What information is required:

- a. The password that you will use to connect to the RRI (talk to your IT guys).
- b. The list of IP addresses from which you will connect to the RRI (talk you your IT guys).
- c. The password that the DEA will use to connect to the RRI (talk to your DEA).
- d. The list of IP addresses from which the DEA will connect to the RRI (talk to your DEA)



# Data Escrow / Monthly Reports, How to comply?

## Onboarding:

3. Submit credentials (per TLD) for you and your Data Escrow Agent in RRI.

Registry Reporting Interface (RRI)

	RRI Registry Username :	xn--test-a212_ry
a	RRI Registry Password :	<input type="password"/>
	Confirm Password :	<input type="password"/>
b	RRI Registry IP Address Block :	<input type="text"/>
	RRI DEA Username :	xn--test-a212_dea
c	RRI DEA Password :	<input type="password"/>
	Confirm Password :	<input type="password"/>
d	RRI DEA IP Address Block :	<input type="text"/>

# Data Escrow / Monthly Reports, How to comply?

---

## Data Escrow (**daily basis**):

Once your TLD is delegated in the root, you need to start doing Data Escrow.

1. Generate your data escrow deposit.

More information:

- Specification 2 of the Registry Agreement (<http://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.docx>)
- <http://tools.ietf.org/html/draft-arias-noguchi-registry-data-escrow>
- <http://tools.ietf.org/html/draft-arias-noguchi-dnrd-objects-mapping>

# Data Escrow / Monthly Reports, How to comply?

---

## Data Escrow (**daily basis**):

2. Once your Data Escrow Agent receives your Data Escrow deposit, you need to send a Registry Data Escrow Report to ICANN through the RRI (use your credentials).

## More information:

- Specification 2 of the Registry Agreement (<http://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm>)
- <http://tools.ietf.org/html/draft-lozano-icann-registry-interfaces> (section 2.1)

# Data Escrow / Monthly Reports, How to comply?

---

## Data Escrow (**daily basis**):

3. Your Data Escrow Agent will verify your Data Escrow deposit, and the result (Data Escrow Notification) will be sent to ICANN through the RRI (DEA must use its credentials).

## More information:

- Specification 2 of the Registry Agreement (<http://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.htm>)
- <http://tools.ietf.org/html/draft-lozano-icann-registry-interfaces> (section 2.2)

# Data Escrow / Monthly Reports, How to comply?

---

## Monthly reports (**monthly basis**):

Once your TLD is delegated in the root, you need to start sending monthly reports (**i.e. Per-Registrar Transactions and Registry Functions Activity Reports**) to ICANN.

Registry Operator must send the two monthly reports for each month by the 20th of the following month.

# Data Escrow / Monthly Reports, How to comply?

---

## Monthly reports (**monthly basis**):

1. Generate your monthly reports.

More information:

- Specification 3 of the Registry Agreement (<http://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-09jan14-en.docx>)

2. Send your monthly reports to ICANN.

More information:

- <http://tools.ietf.org/html/draft-lozano-icann-registry-interfaces> (section 3)

# Service Level Agreement monitoring system

# What is the SLA monitoring system?

---

- The SLA monitoring system is a real-time monitoring system used to answer the following question:
  - **Is the contracted party operating according to the SLA (Specification 10 of the Registry Agreement)?**
- The SLA monitoring system validates that:
  - DNS/DNSSEC is working.
  - SRS (EPP interface) is working.
  - RDDS is working.
  - Updates to the SRS are being propagated to DNS and RDDS (a.k.a. Whois).



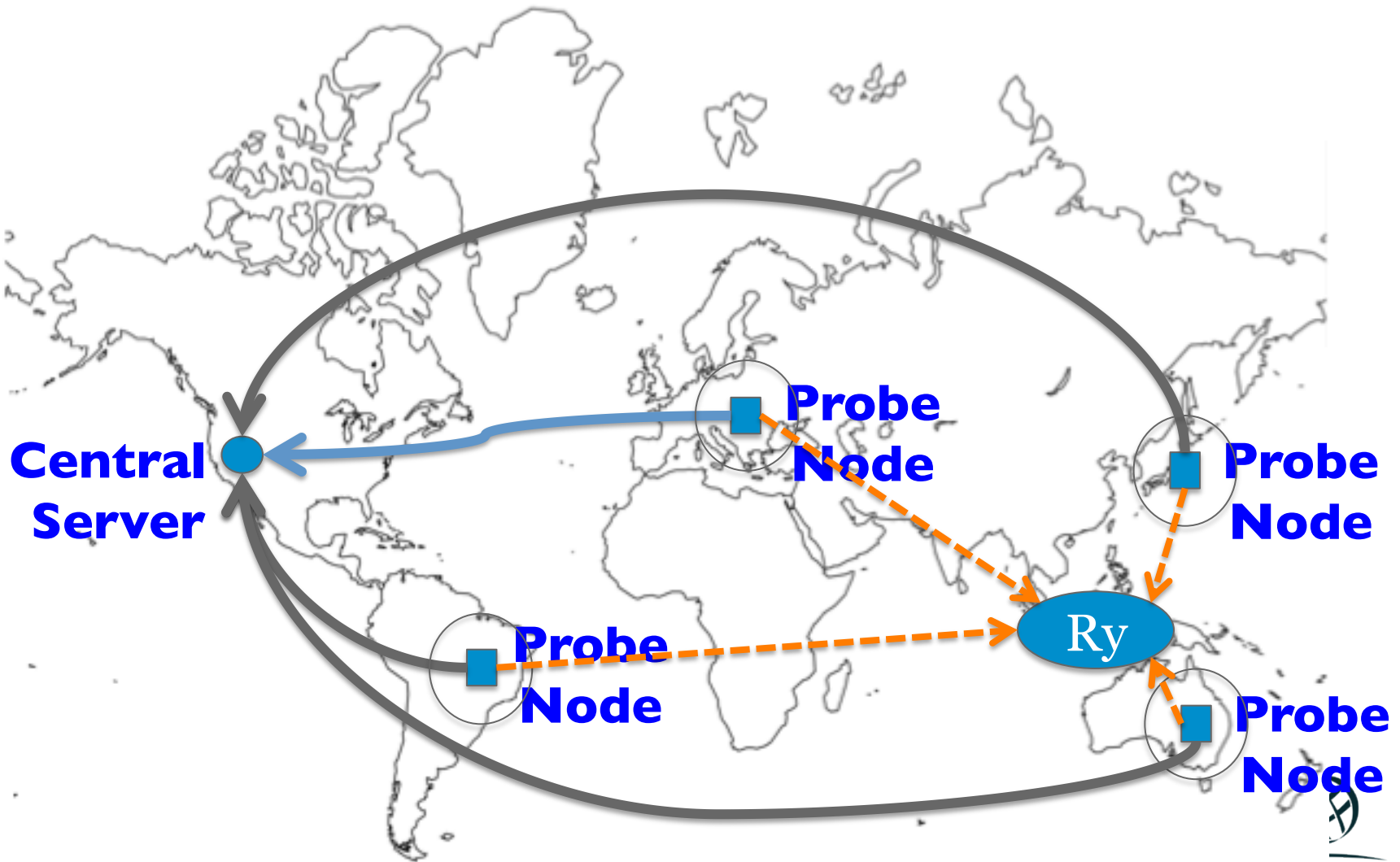
# What is the SLA monitoring system?

---

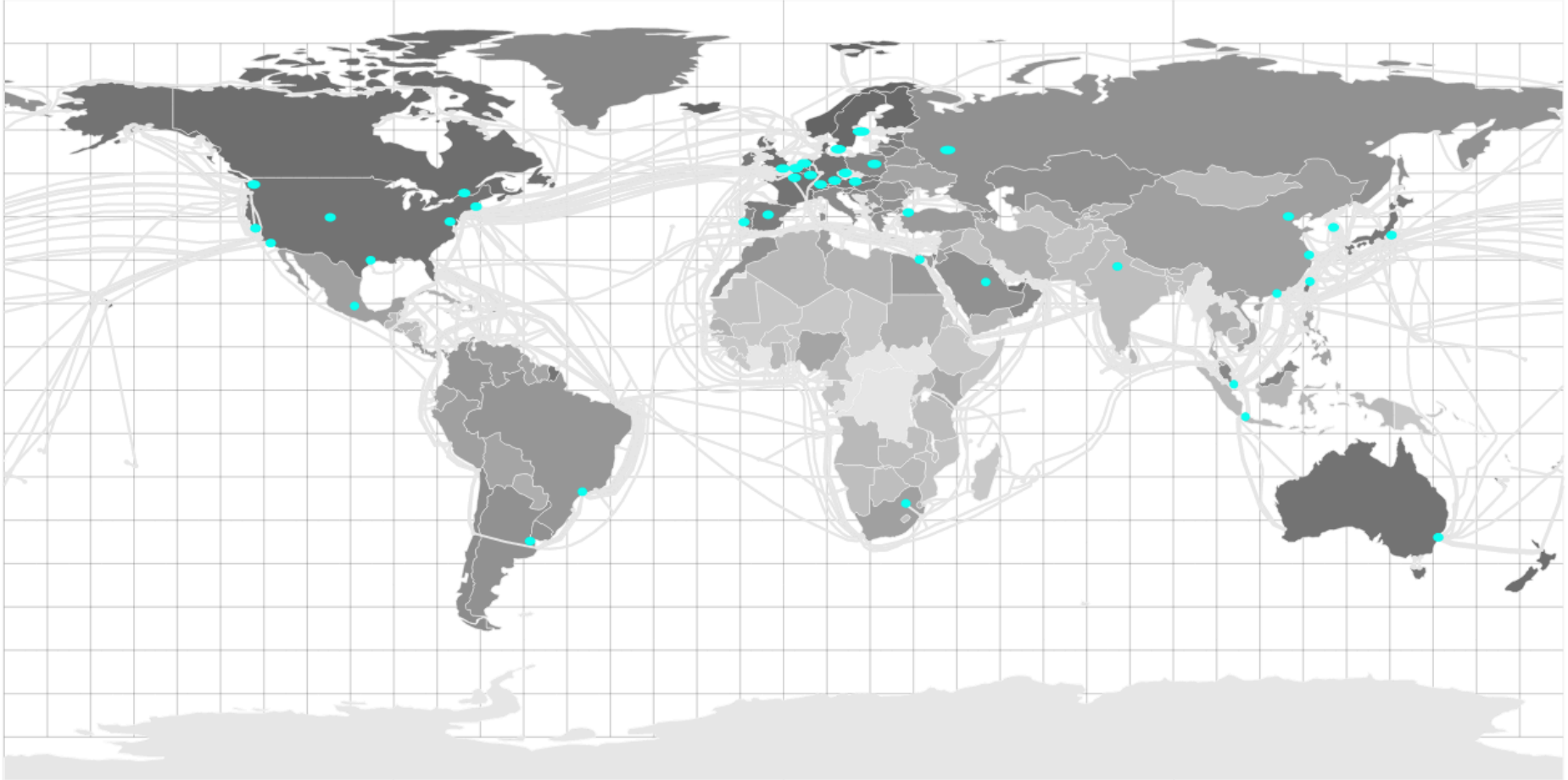
The SLA monitoring system design principles:

- Several probe nodes must agree that the service is not working (test are done concurrently).
- What is verified in a test (e.g. DNS query) depends on the result of another test (e.g. domain name created via EPP).
- Real-time: DNS every minute and EPP/WHOIS every 5 minutes.

# Central servers and probe nodes



# Current probe node network



# Monitoring platform

TLD Rolling week status [re x]

https://tld-monitor.icann.org/rsm.rollingweekstatus.php?sid=d9a3c68c013dcd27&form\_refresh=1&filter\_search=&filter\_dns=1&filter\_dnssec=1&filter\_rdds...

History: History » Latest data » History » Latest data » TLD Rolling week status

### TLD Rolling week status

Displaying 1 to 9 of 9 found

Filter

TLD:

DNS  DNSSEC  RDDS  EPP [All/Any](#) Exceeding or equal to: 5% Current status: all

ccTLD  gTLD  otherTLD  testTLD [All/Any](#)

[Filter](#) [Reset](#)

TLD	Type	DNS (4Hrs)	DNSSEC (4Hrs)	RDDS (24Hrs)	EPP (24Hrs)
		8.750% <a href="#">graph</a>	0.000%		
		10.417% <a href="#">graph</a>			
		10.833% <a href="#">graph</a>			
		13.750% <a href="#">graph</a>			
		17.500% <a href="#">graph</a>			
		55.417% <a href="#">graph</a>			
		152.083% <a href="#">graph</a>			
		417.500% <a href="#">graph</a>			
		4185.833% <a href="#">graph</a>			

Zabbix 2.0.10rc1 Copyright 2001-2013 by Zabbix SIA | Connected as 'Admin'



gTLD Monitor

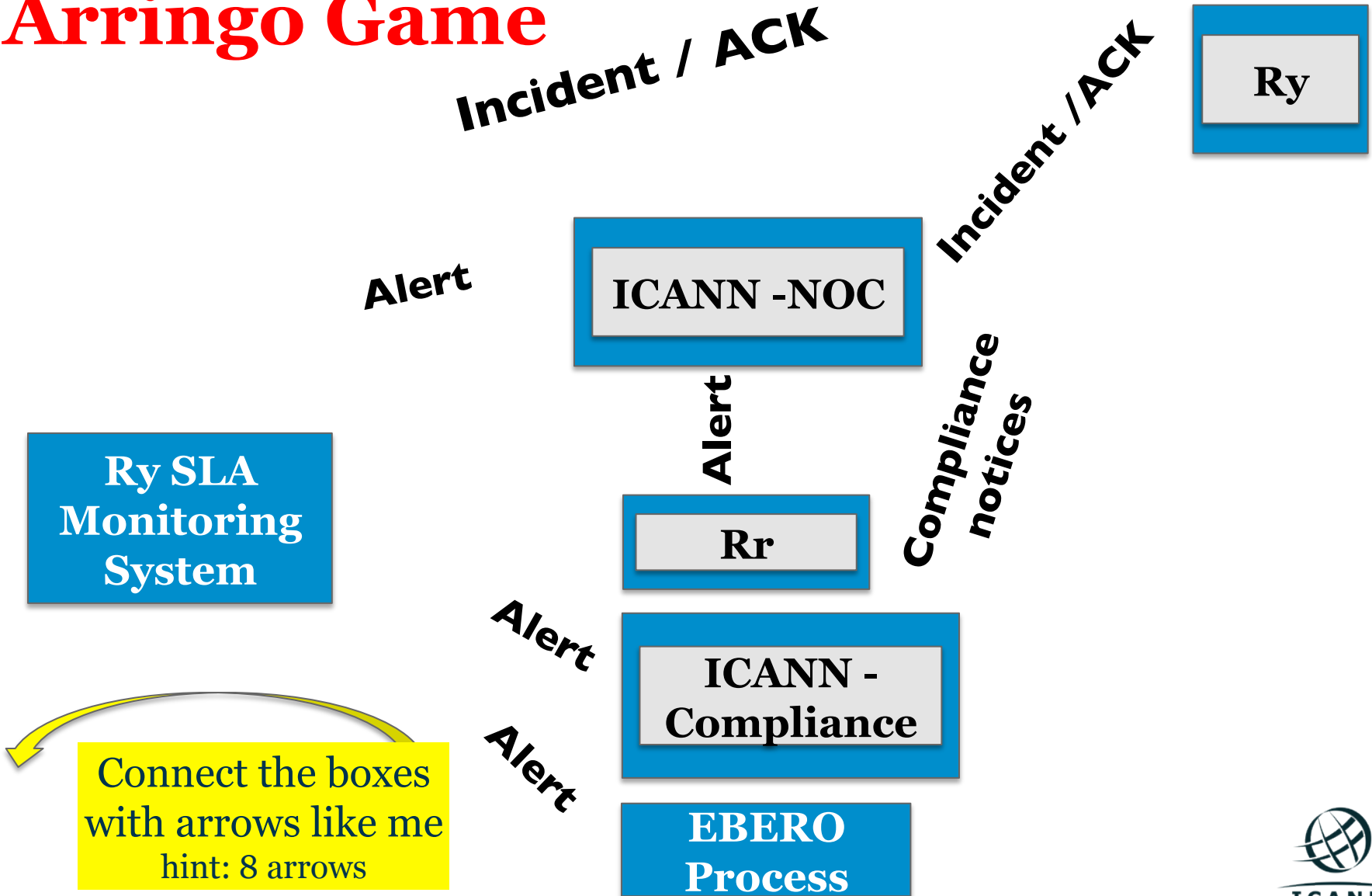
**Ask the Audience**

**Who wants their gTLD tested?**

**Let's Spin up the Globe**

# SLA monitoring system – High level overview

## Arringo Game




# Data Escrow – High level view of the process

## Connect the Boxes Arringo Game

**Yell Out **Arringo!****

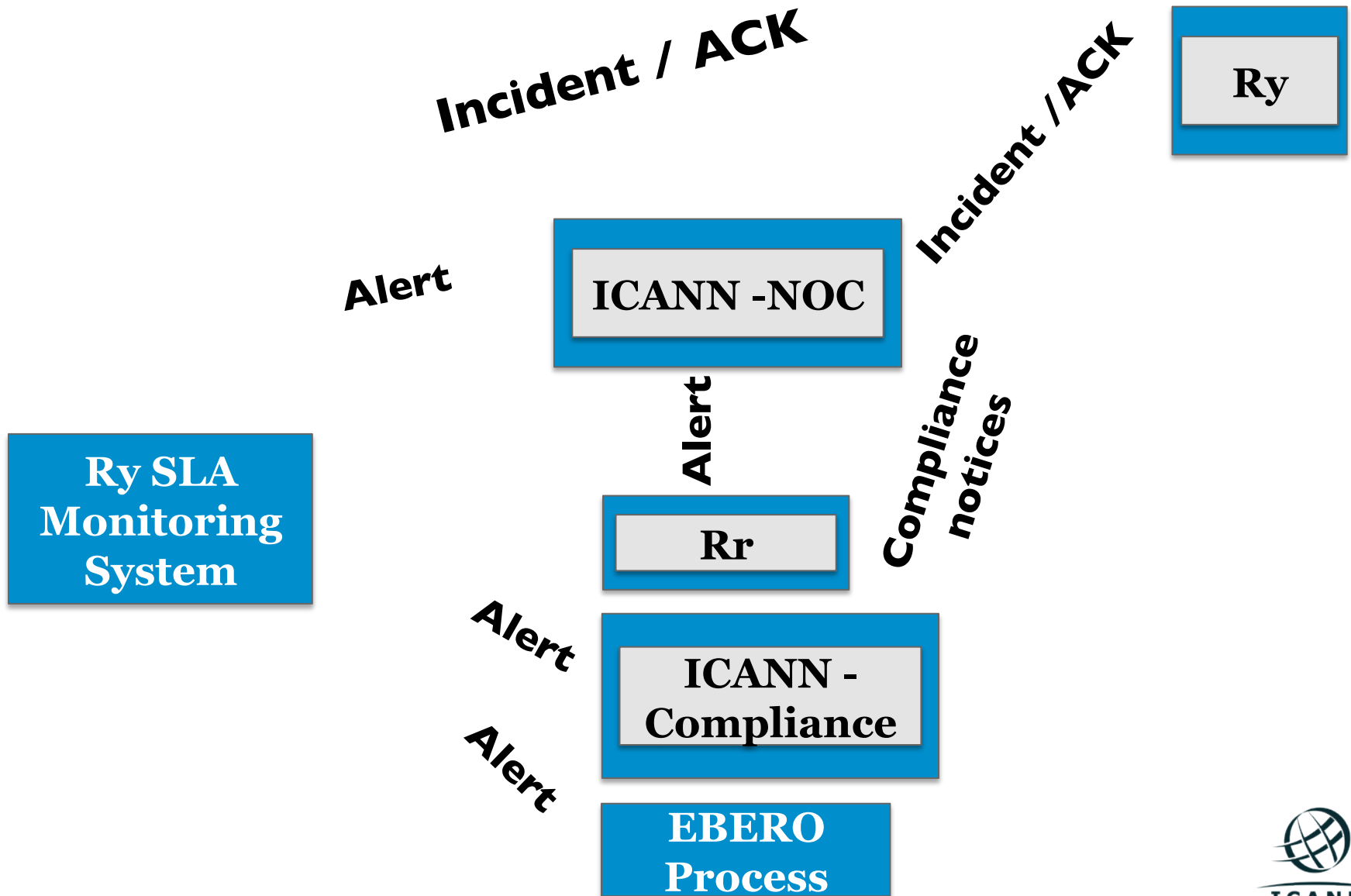
**When you are done**

**Bring your up your completed  
sheet for verification and Win!**



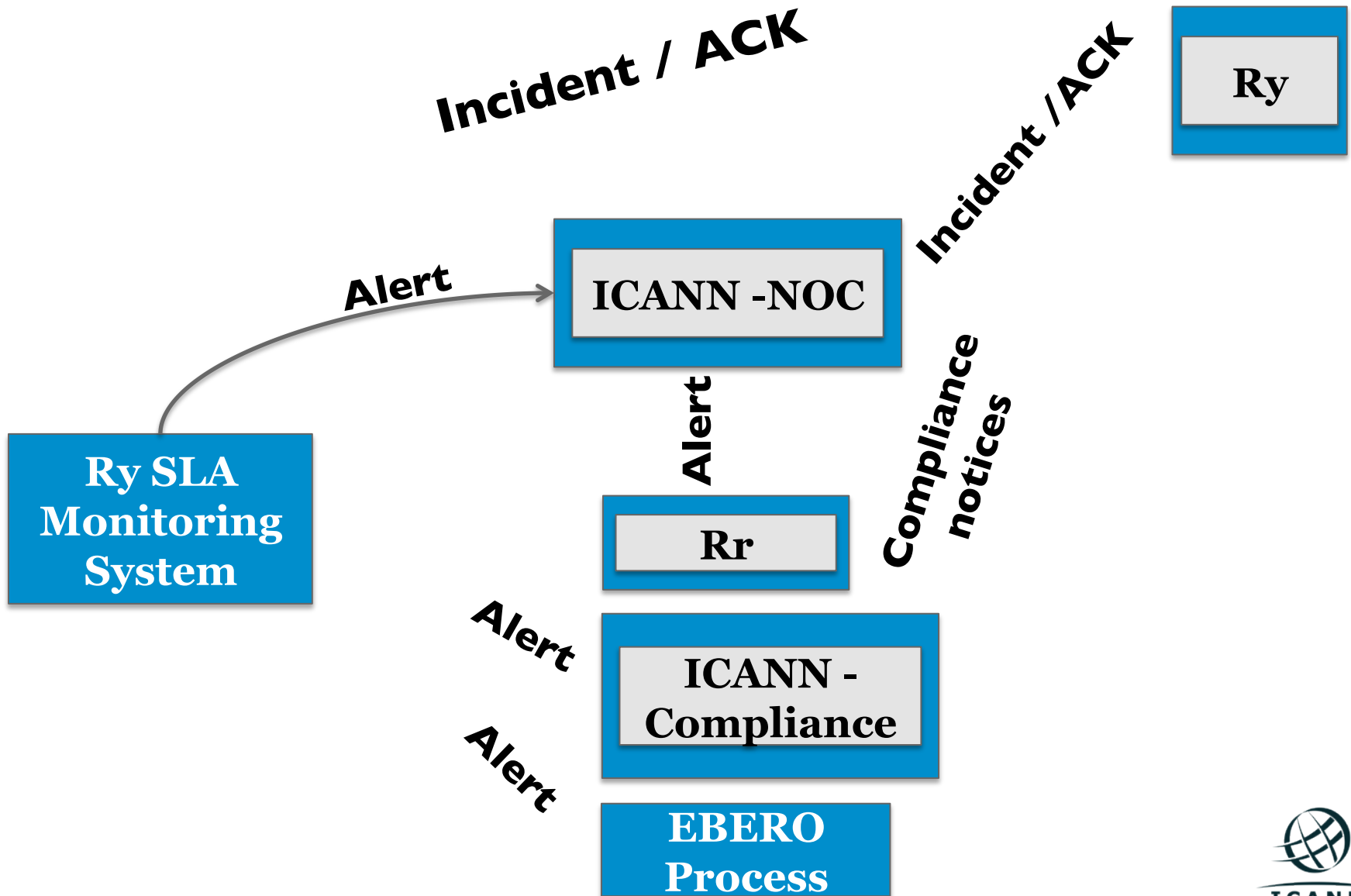
Connect the boxes  
with arrows like me  
hint: 8 arrows

# SLA monitoring system – High level overview

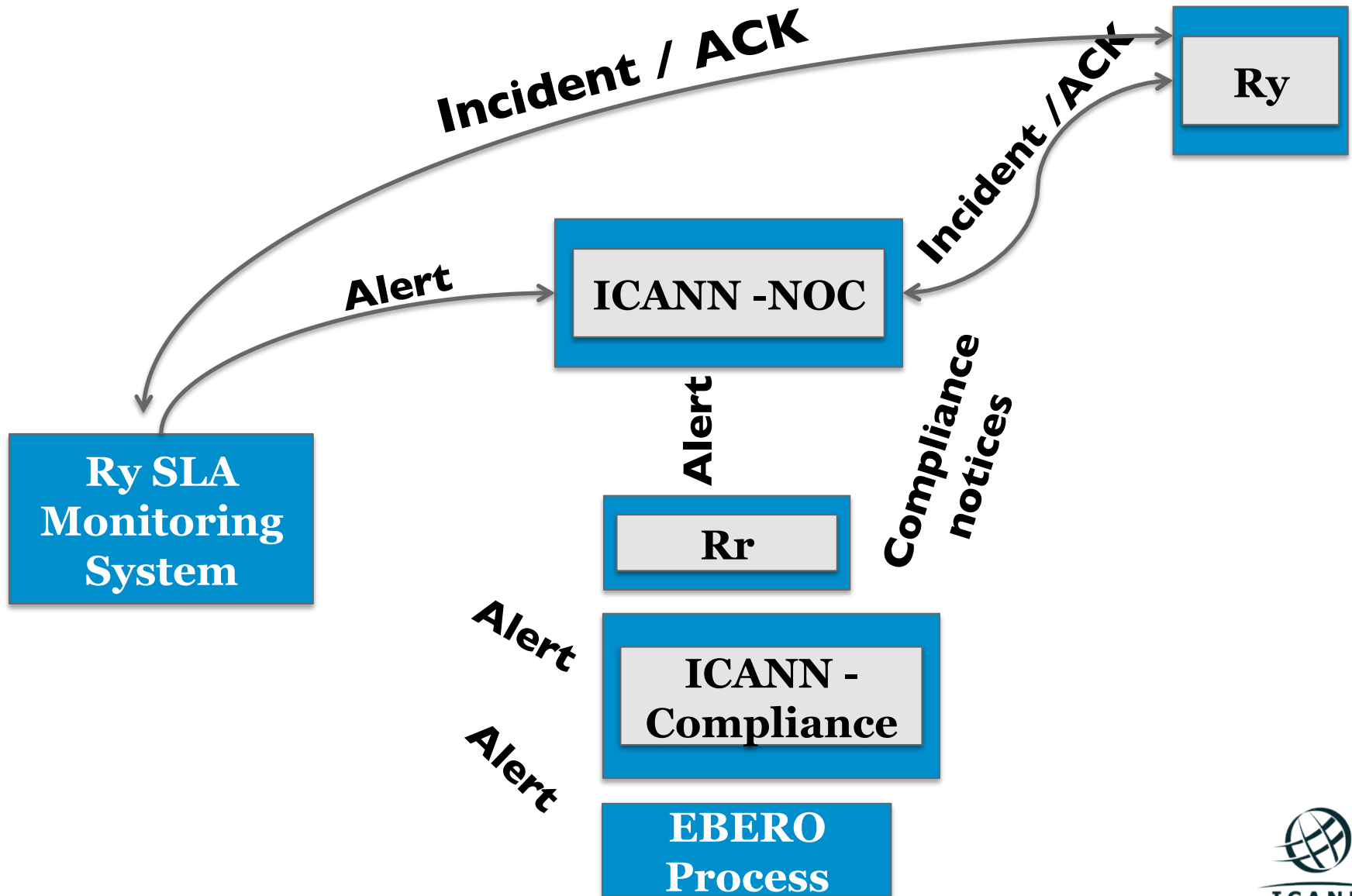




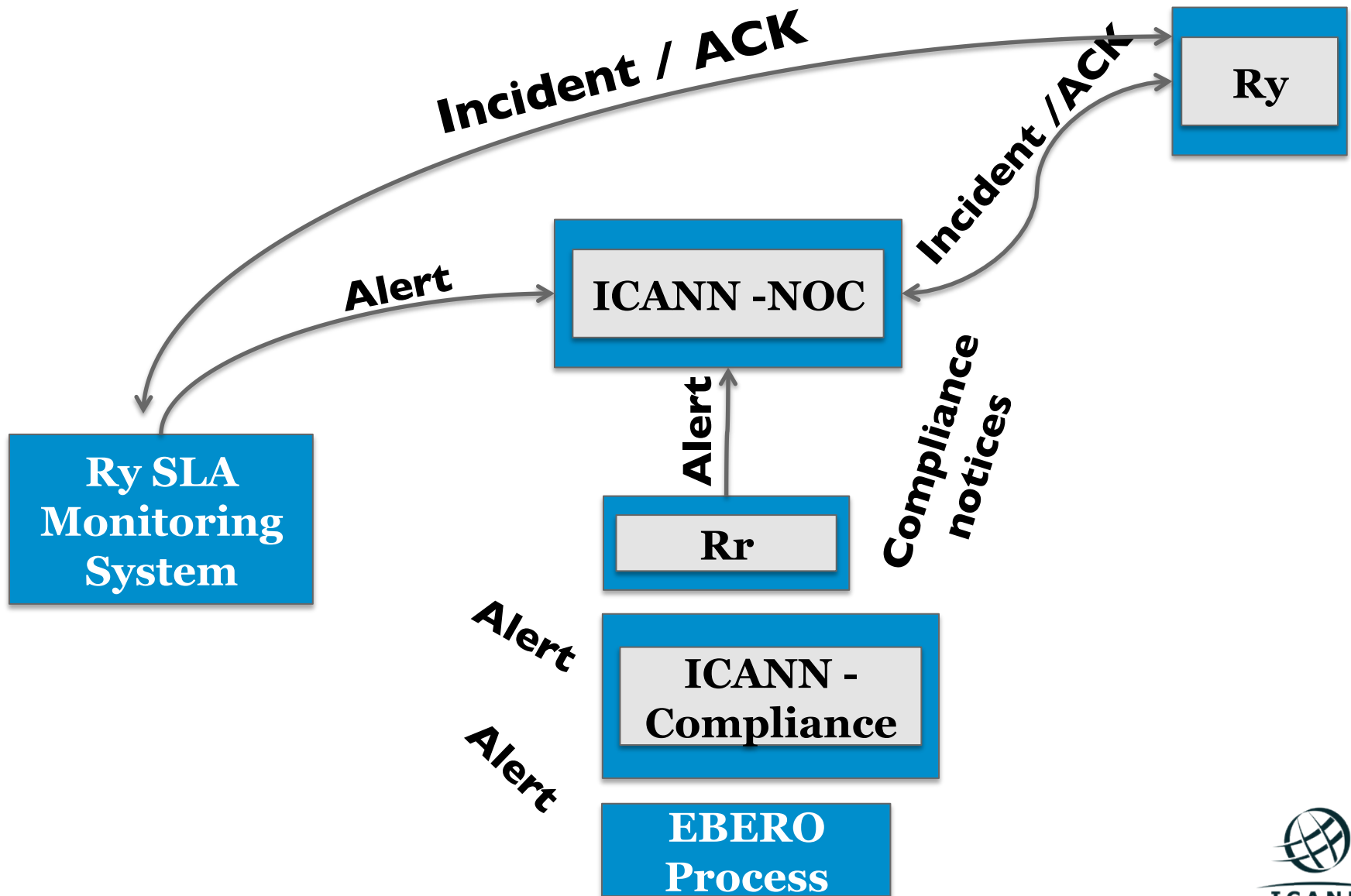
# SLA monitoring system – High level overview



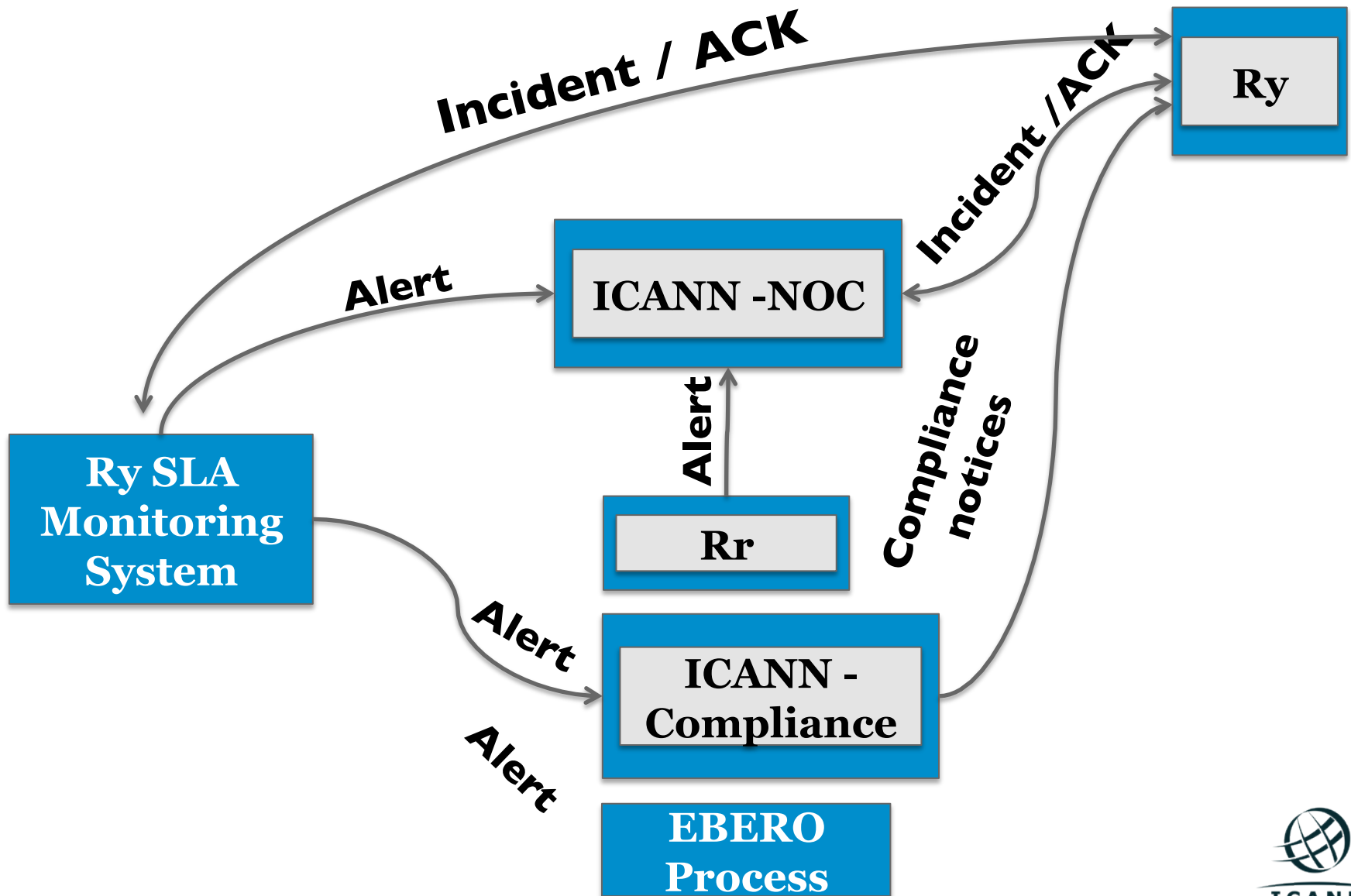
# SLA monitoring system – High level overview



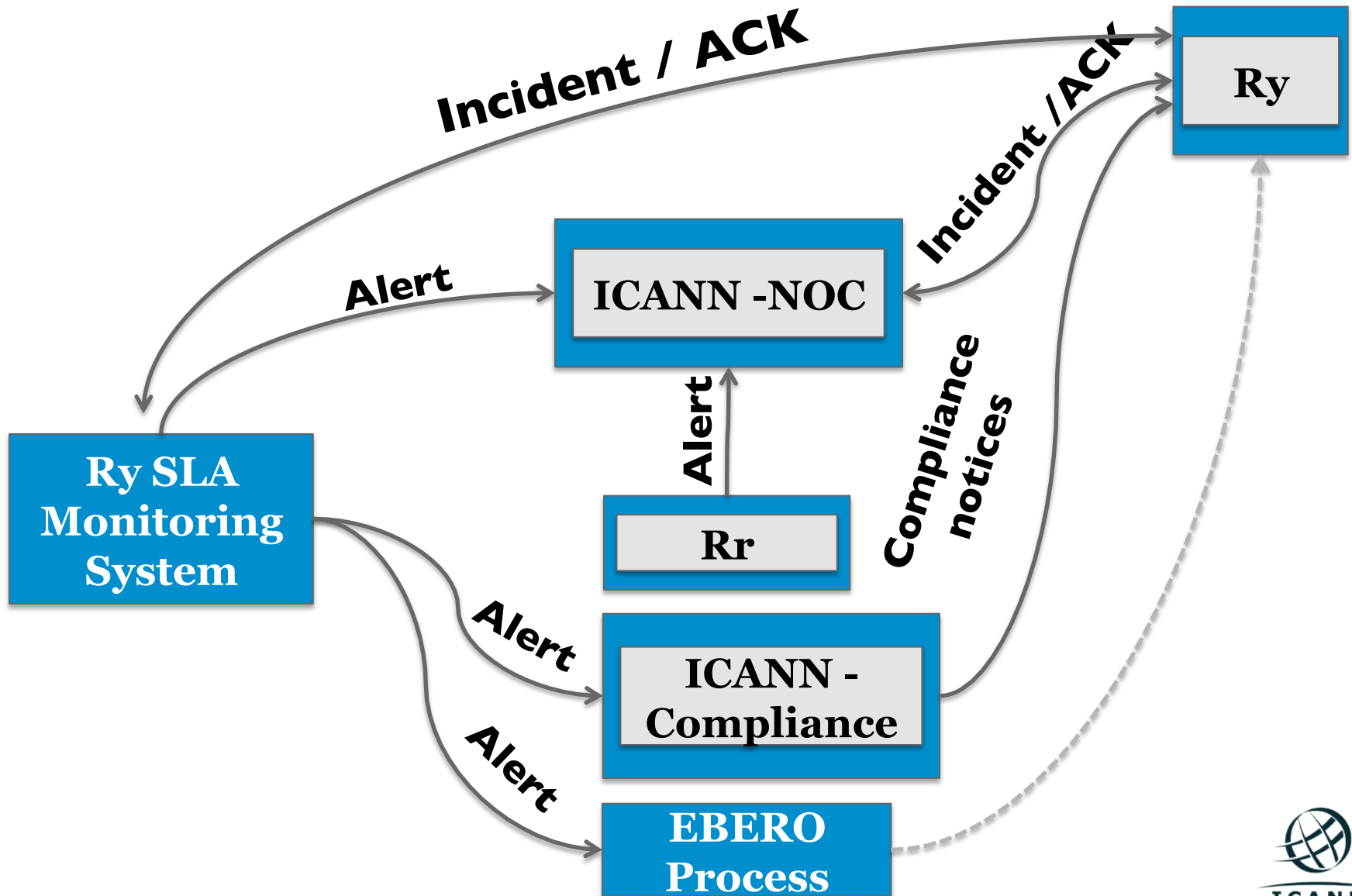
# SLA monitoring system – High level overview



# SLA monitoring system – High level overview



# SLA monitoring system – High level overview



# Emergency threshold:

## Do you know your threshold?

### 1. Emergency Thresholds

The following matrix presents the Emergency Thresholds that, if reached by any of the services mentioned above for a TLD, would cause the Emergency Transition of the Critical Functions as specified in Section 2.13. of this Agreement.

Critical Function	Emergency Threshold
DNS service (all servers)	???? downtime / week
DNSSEC proper resolution	???? downtime / week
EPP	???? downtime / week
RDDS (WHOIS/Web-based WHOIS)	???? downtime / week
Data Escrow	Breach of the Registry Agreement caused by missing escrow deposits as described in Specification 2, Part B, Section 6.

# Emergency threshold:

## 1. Emergency Thresholds

The following matrix presents the Emergency Thresholds that, if reached by any of the services mentioned above for a TLD, would cause the Emergency Transition of the Critical Functions as specified in Section 2.13. of this Agreement.

<b>Critical Function</b>	<b>Emergency Threshold</b>
DNS service (all servers)	4-hour downtime / week
DNSSEC proper resolution	4-hour downtime / week
EPP	24-hour downtime / week
RDDS (WHOIS/Web-based WHOIS)	24-hour downtime / week
Data Escrow	Breach of the Registry Agreement caused by missing escrow deposits as described in Specification 2, Part B, Section 6.

# SLA of new gTLDs:

	Parameter	SLR (monthly basis)
<b>DNS</b>	DNS service availability	0 min downtime = 100% availability
	DNS name server availability	$\leq 432$ min of downtime ( $\approx 99\%$ )
	TCP DNS resolution RTT	$\leq 1500$ ms, for at least 95% of the queries
	UDP DNS resolution RTT	$\leq 500$ ms, for at least 95% of the queries
	DNS update time	$\leq 60$ min, for at least 95% of the probes
<b>RDDS</b>	RDDS availability	$\leq 864$ min of downtime ( $\approx 98\%$ )
	RDDS query RTT	$\leq 2000$ ms, for at least 95% of the queries
	RDDS update time	$\leq 60$ min, for at least 95% of the probes
<b>EPP</b>	EPP service availability	$\leq 864$ min of downtime ( $\approx 98\%$ )
	EPP session-command RTT	$\leq 4000$ ms, for at least 90% of the commands
	EPP query-command RTT	$\leq 2000$ ms, for at least 90% of the commands
	EPP transform-command RTT	$\leq 4000$ ms, for at least 90% of the commands



# Emergency contacts

---

- **Registry emergency contacts:**
  - Receive alerts from the monitoring platform or ICANN's NOC.
  - Communications from ICANN are of technical nature.
  - May be contacted 24x7.

# Emergency contacts

---

- **Escalation process (automatic process):**
  - Send email to three emergency contacts when 10% of the threshold is reached.
- **Escalation process (technical services):**
  - Send email to three emergency contacts (if the 25% threshold is about to be reached, the technical contact also receives the alerts)
  - Contact the emergency contacts by phone.

# ICANN's emergency contact information

---

- **The email address used to send notifications about maintenance window will be published in the GDD portal.**
- **The 24x7 information of our NOC will be published in the GDD portal.**
- **The 24x7 information of IANA's emergency contact will be published in the GDD portal.**

# I am a Registry, How to comply with SLA Monitoring?

# SLA Monitoring, How to comply?

---

## Onboarding:

1. Create a Registrar account for ICANN in your SRS. The IANA Registrar ID 9997 must be used to report the transactions of the ICANN SLA Monitoring System.

Note: By default, ICANN will use a X.509 certificate for establishing TLS with the EPP server, the default certificate is signed by a well-known public CA. The default X.509 certificate can be found here: <http://tld-monitor.icann.org/epp-client-default.crt>.

Note: ICANN will connect from the following IP addresses: <https://tld-monitor.icann.org/nodes.txt>. Please whitelist these IP addresses for EPP and RDDS (Whois).

# SLA Monitoring, How to comply?

---

## Onboarding:

### What information is required:

- a. The username for the EPP client for the ICANN SLA Monitoring System.
- b. The password for the EPP client for the ICANN SLA Monitoring System.
- c. The EPP server hostname(s) and port that ICANN should use to connect.
- d. Special requirements: e.g., Registry uses their own internal CA, Registry uses SNI TLS extension, etc.

# SLA Monitoring, How to comply?

## Onboarding:

2. Provide the information to ICANN.

SLA Monitoring Information (EPP)

a → EPP Username :

b → EPP Password :

b → Confirm Password :

d → EPP Server :  :

d → Other Requirements :

# SLA Monitoring, How to comply?

## Continuous basis:

1. Respond promptly to SLA Incident Reports from ICANN.

### SLA Monitoring Information (EPP)

a	→	EPP Username :	<input type="text"/>
b	↔	EPP Password :	<input type="password"/>
	↔	Confirm Password :	<input type="password"/>
d	→	EPP Server :	<input type="text"/> : <input type="text" value="700"/>
d	→	Other Requirements :	<input type="text"/>



# Zone File Access

# ZFA – Overview

---

- Registry Operator must make available the zone file(s) of the TLD to ICANN on daily basis.
- Zone file(s) can be made available to ICANN via AXFR or SFTP.
  - Note: only key authentication is supported (e.g. no password authentication).
- ICANN's retrieval servers use the following networks (please whitelist them):
  - 192.0.32.224/27
  - 192.0.47.224/27
  - 192.0.35.91/32
  - 2620:0:2d0:211::60/64
  - 2620:0:2830:211::60/64.

# ZFA – SFTP

---

- If using SFTP, ICANN will connect to the specified SFTP server on a daily basis in order to download the zone file(s).
- Registry Operator must configure SFTP access for ICANN using the following public SSH key:  
<https://zfa.icann.org/icann-zfa-key.pub>
- Note: only key authentication is supported (e.g. no password authentication).

# ZFA – AXFR

---

- If using AXFR, ICANN will connect to the specified name server(s) on a daily basis in order to download the zone file(s).
- AXFR/IXFR with TSIG must be supported by the name server(s).

# I am a Registry, How to comply with ZFA?

# ZFA – How to comply?

---

- Choose between AXFR or SFTP.
- Note: If using AXFR, ICANN will provide the zone file(s) via CZDS to third-parties. If using SFTP, the registry operator is responsible for providing zone file(s) to third-parties.

# ZFA – How to comply? AXFR

---

## **Onboarding:**

1. Configure your name server(s) for zone transferring (AXFR/IXFR) using TSIG.

## **What information is required:**

- a. The CZDS user that will have the “Super Manager” role in CZDS for this TLD.
- b. The AXFR server(s) and port(s) (ask your IT guys).
- c. The TSIG key owner name (ask your IT guys).
- d. The TSIG key (ask your IT guys).
- e. The TSIG algorithm configured in your name server(s) (ask your IT guys).

# ZFA – How to comply? AXFR

## Onboarding:

### 2. Provide the information to ICANN.

Centralized Zone Data System/Zone File Access (CZDS / ZFA)

a →

CZDS Username :

Delivery Method :

b →

AXFR Server :

 : 

c →

TSIG Key Ownername :

d →

TSIG Key :

e →

TSIG Algorithm :



# ZFA – How to comply? SFTP

---

## **Onboarding:**

1. Configure your SFTP server using ICANN's SSH public key (<https://zfa.icann.org/icann-zfa-key.pub>).

## **What information is required:**

- a. The CZDS user that will have the “Super Manager” role for this TLD.
- b. The SFTP server hostname that third parties will use to transfer zones (CZDS).
- c. The SFTP URI that ICANN will use to download the zone file:
  - SFTP server name
  - SFTP user name
  - SFTP TCP/port
  - SFTP Path, note: if a path is not defined, ICANN will download the files from the home directory of the user.

# ZFA – How to comply? SFTP

## Onboarding:

2. Provide the information to ICANN.

Centralized Zone Data System/Zone File Access (CZDS / ZFA)

a → CZDS Username :

Delivery Method :

b → CZDS SFTP Server : sftp://

c → ZFA SFTP URI : sftp://  @  : 22 /

# BRDA



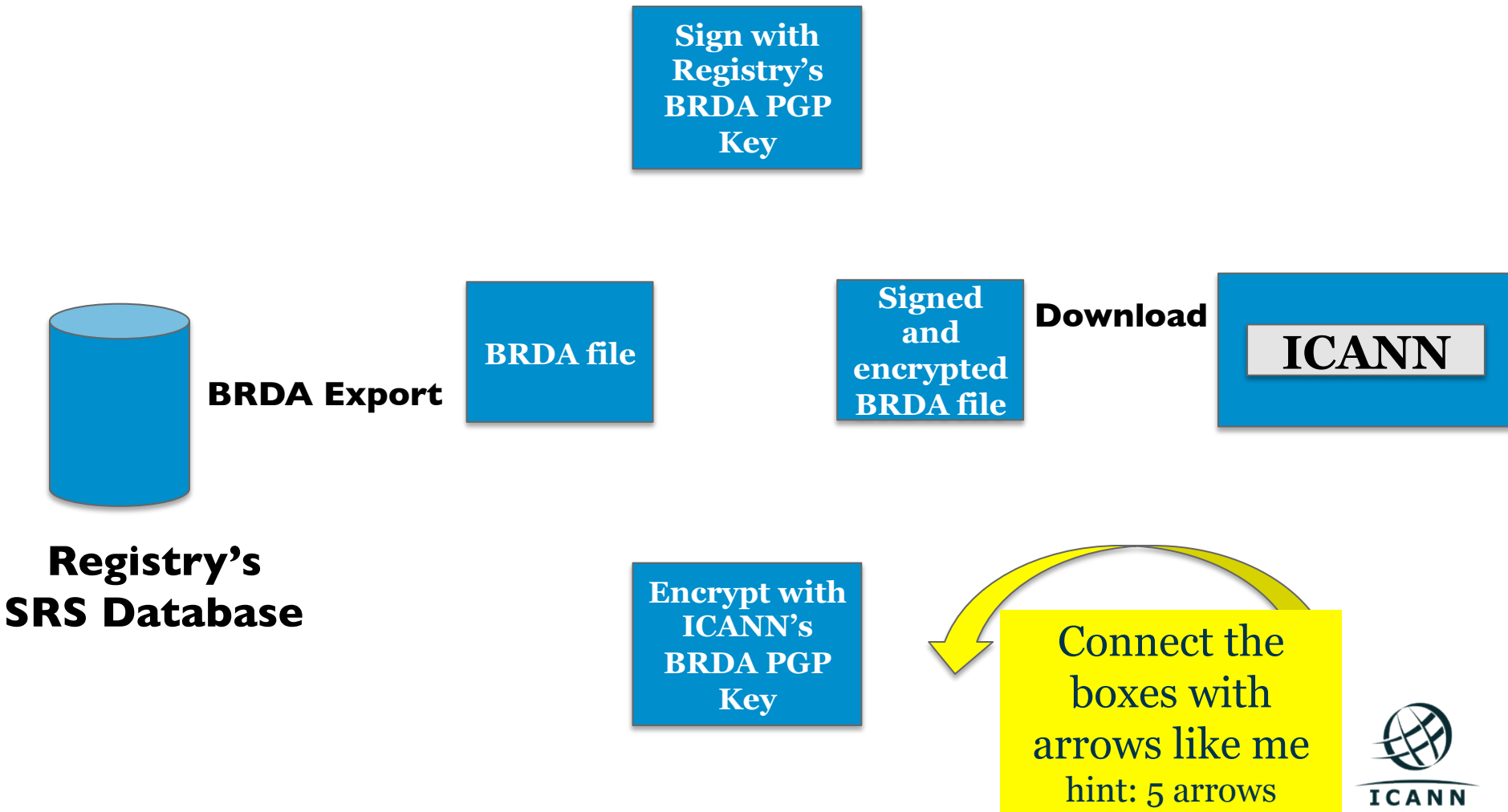
# BRDA – Overview

---

- A BRDA file contains at least Thin Registration Data for the TLD. The data escrow format is used for generating the BRDA file.
- Registry Operator must make available the BRDA file(s) of the TLD to ICANN on weekly basis.
- The file must be made available to ICANN via SFTP.
  - Note: only key authentication is supported (e.g. no password authentication).
- ICANN's retrieval servers use the following networks (please whitelist them):
  - 192.0.32.224/27
  - 192.0.47.224/27
  - 192.0.35.91/32
  - 2620:0:2do:211::60/64
  - 2620:0:2830:211::60/64

# BRDA – High level view of the process


## Connect the Boxes Arringo Game



# BRDA – High level view of the process

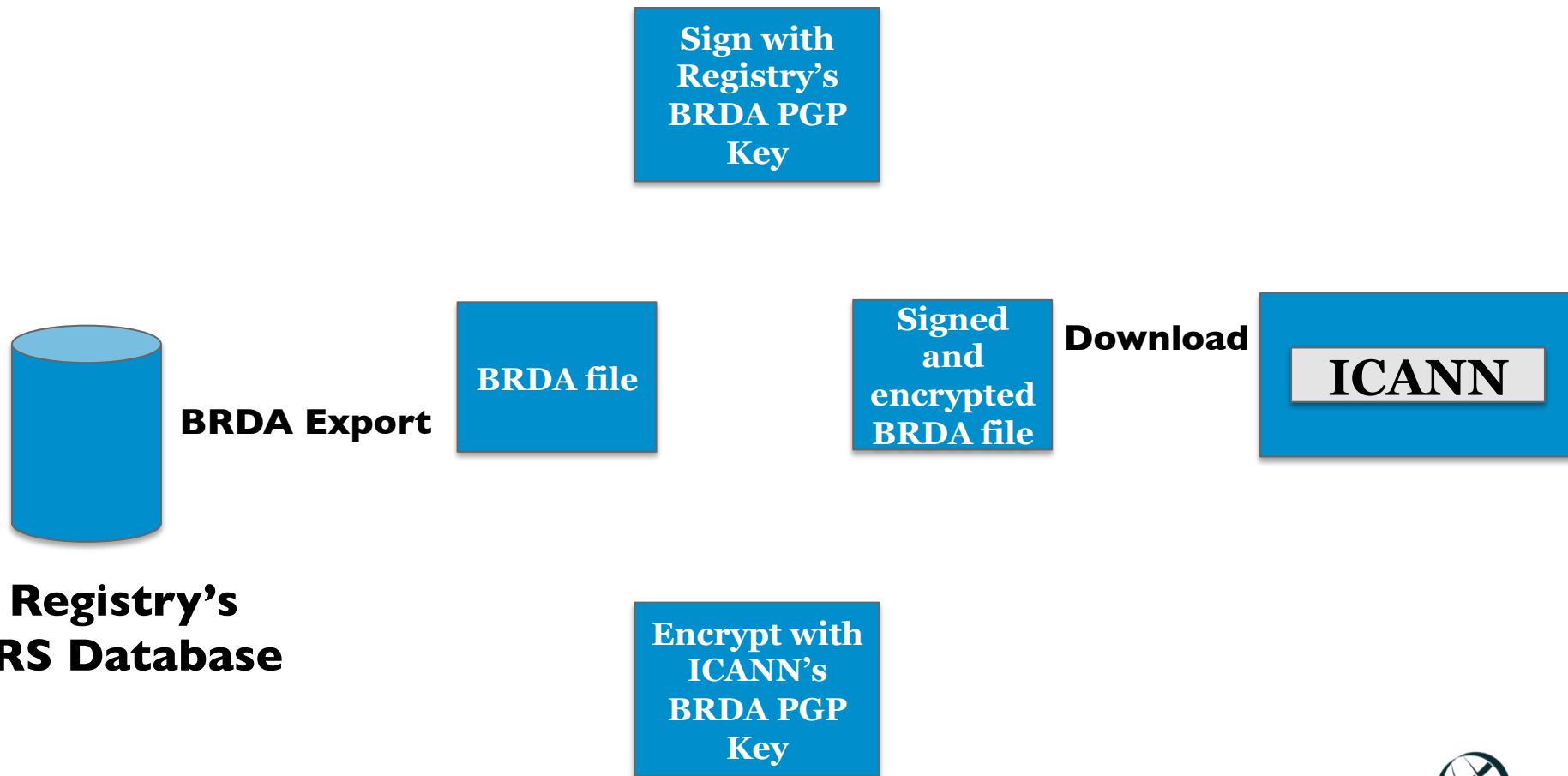
## Connect the Boxes Arringo Game

**Yell Out **Arringo!****  
**When you are done**  
**Bring your up your completed**  
**sheet for verification and Win**

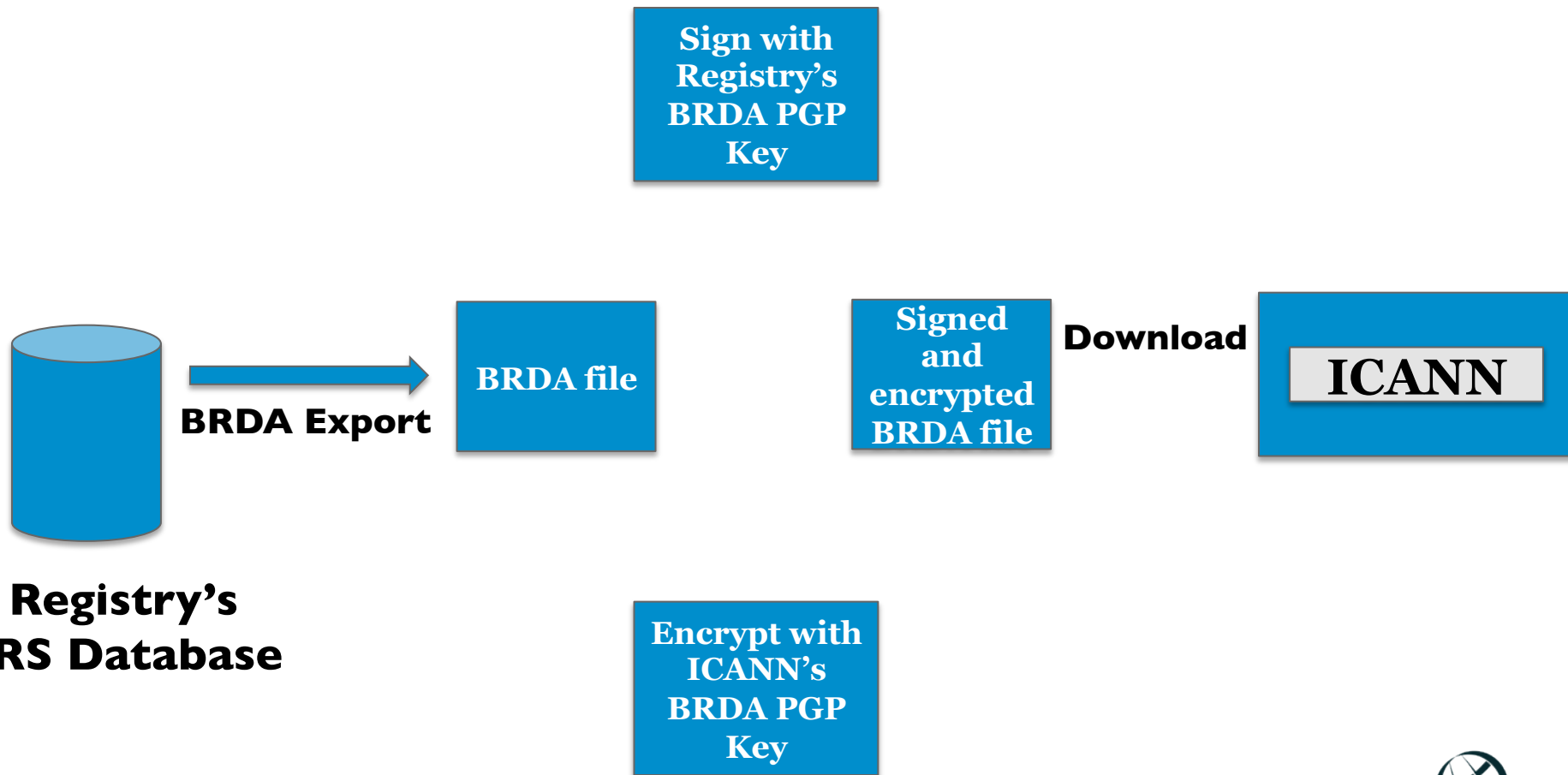


Connect the boxes  
with arrows like me  
hint: 5 arrows

# BRDA – High level view of the process

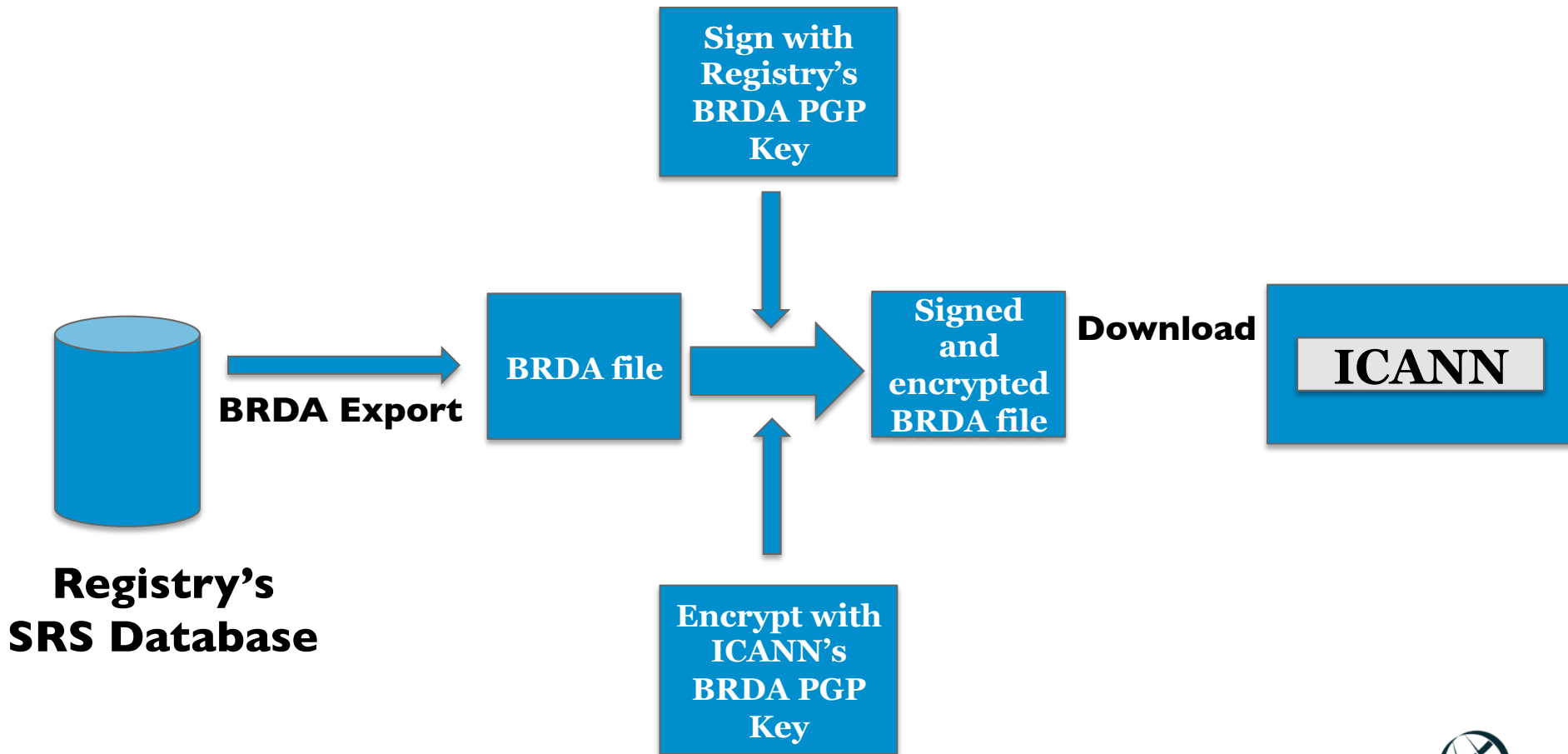


# BRDA – High level view of the process

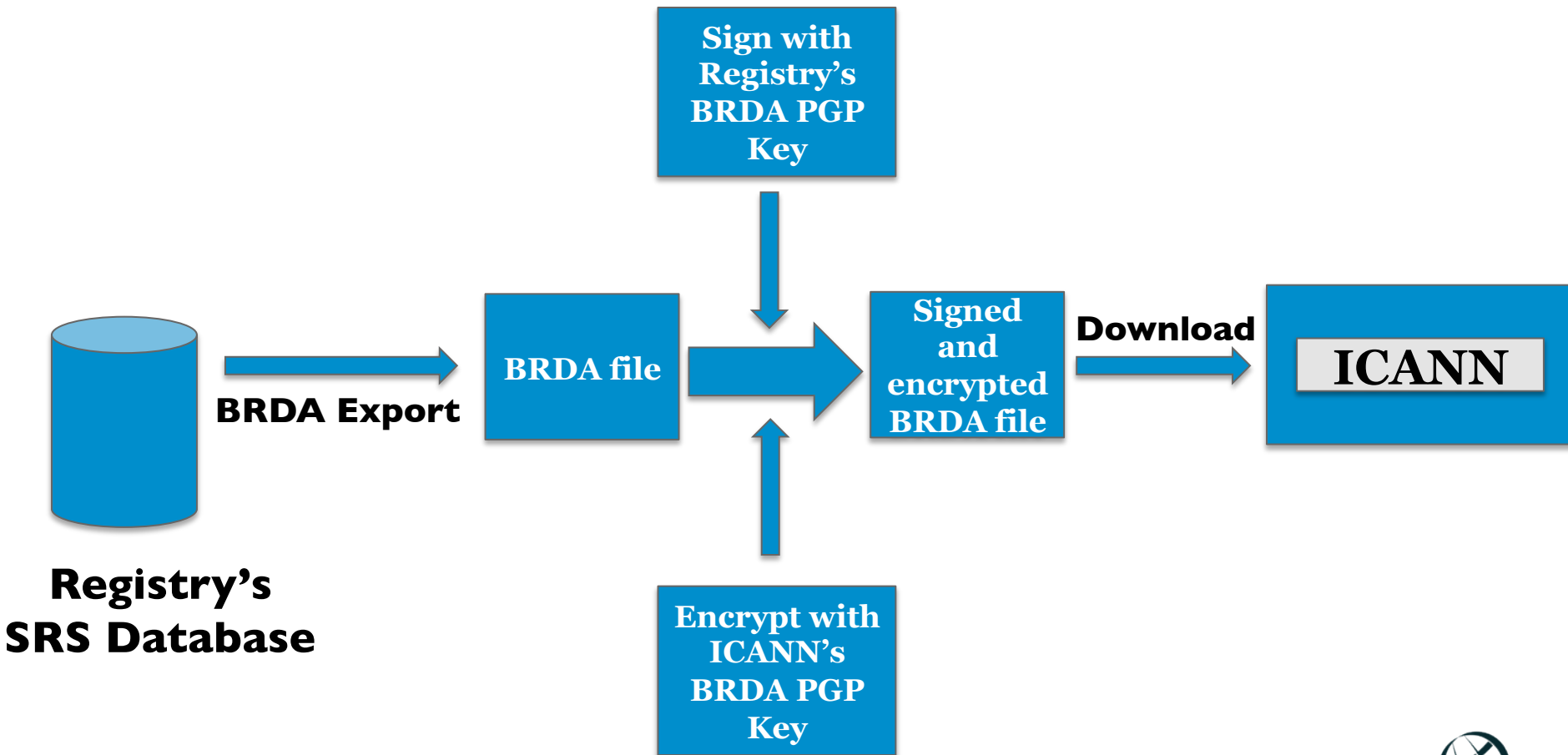




# BRDA – High level view of the process



# BRDA – High level view of the process



# I am a Registry, How to comply with BRDA?

# BRDA – How to comply?

---

- Registry Operator needs to generate a PGP key in order to sign the BRDA file and provide the public portion of the PGP key to ICANN.
- Registry Operator needs to encrypt the BRDA file using ICANN's BRDA PGP key: <https://brda.icann.org/icann-brda-gpg.pub>

# BRDA – How to comply?

---

## Onboarding:

1. Configure your SFTP server using ICANN's SSH public key (<https://brda.icann.org/icann-brda-key.pub>).

## What do you need to provide:

- a. The SFTP URI that ICANN will use to download the BRDA file:
  - SFTP server name
  - SFTP user name
  - SFTP TCP/port
  - SFTP Path, note: if a path is not defined, ICANN will download the files from the home directory of the user.
- b. The day of the week that ICANN will download the BRDA file.
- c. The BRDA PGP public key used to sign the BRDA file.

# BRDA – How to comply?

---

## Onboarding:

2. Provide the information to ICANN.

Thin Bulk Registration Data Access (BRDA)

a → BRDA SFTP URI : sftp://  @  : 22 /

b → BRDA Day of the Week :

c → BRDA Public Key :

Thank you  
for attending  
the Roadshow