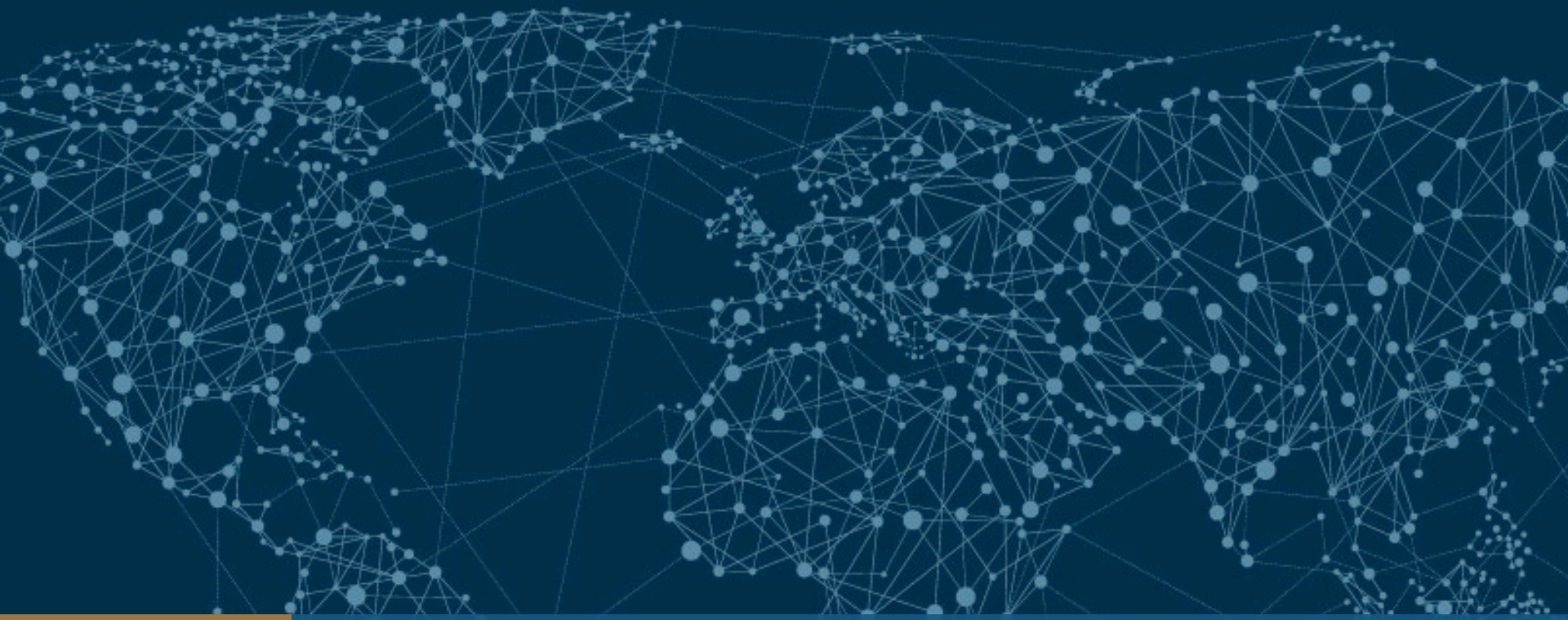

ICANN
ICANN | 53
Buenos Aires
21-25 JUNE 2015



How it Works: TLD Registry Protocols

Ed Lewis – Steve Conte | ICANN 53 | 21 June 2015

What is a Domain Name Registry?

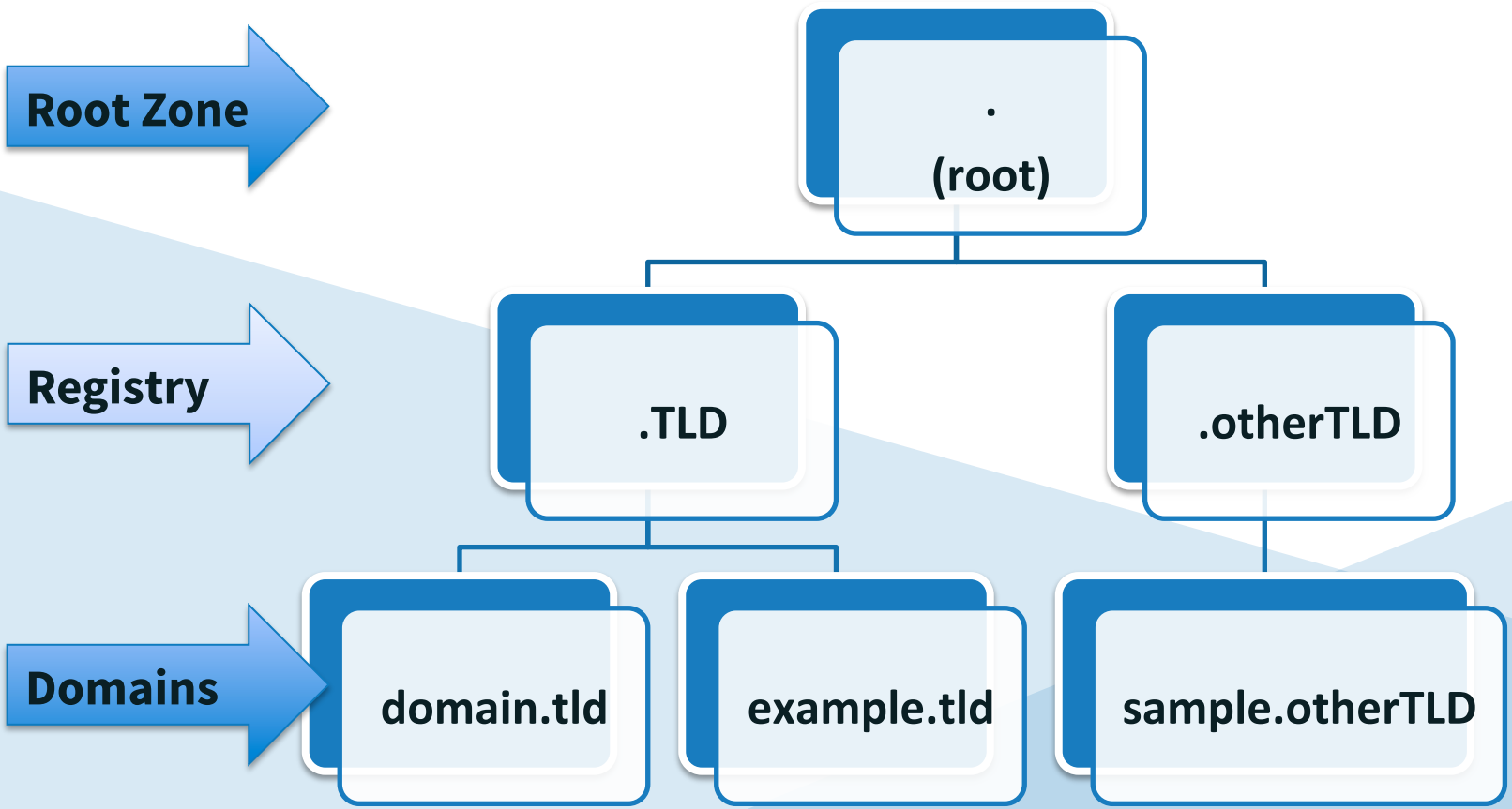
- Database of domain names and associated information in the top level domains of the Domain Name System (DNS) system

- Top-level domain (TLD) space often called a “zone” when discussing from a technical perspective

Other Kinds of Registries

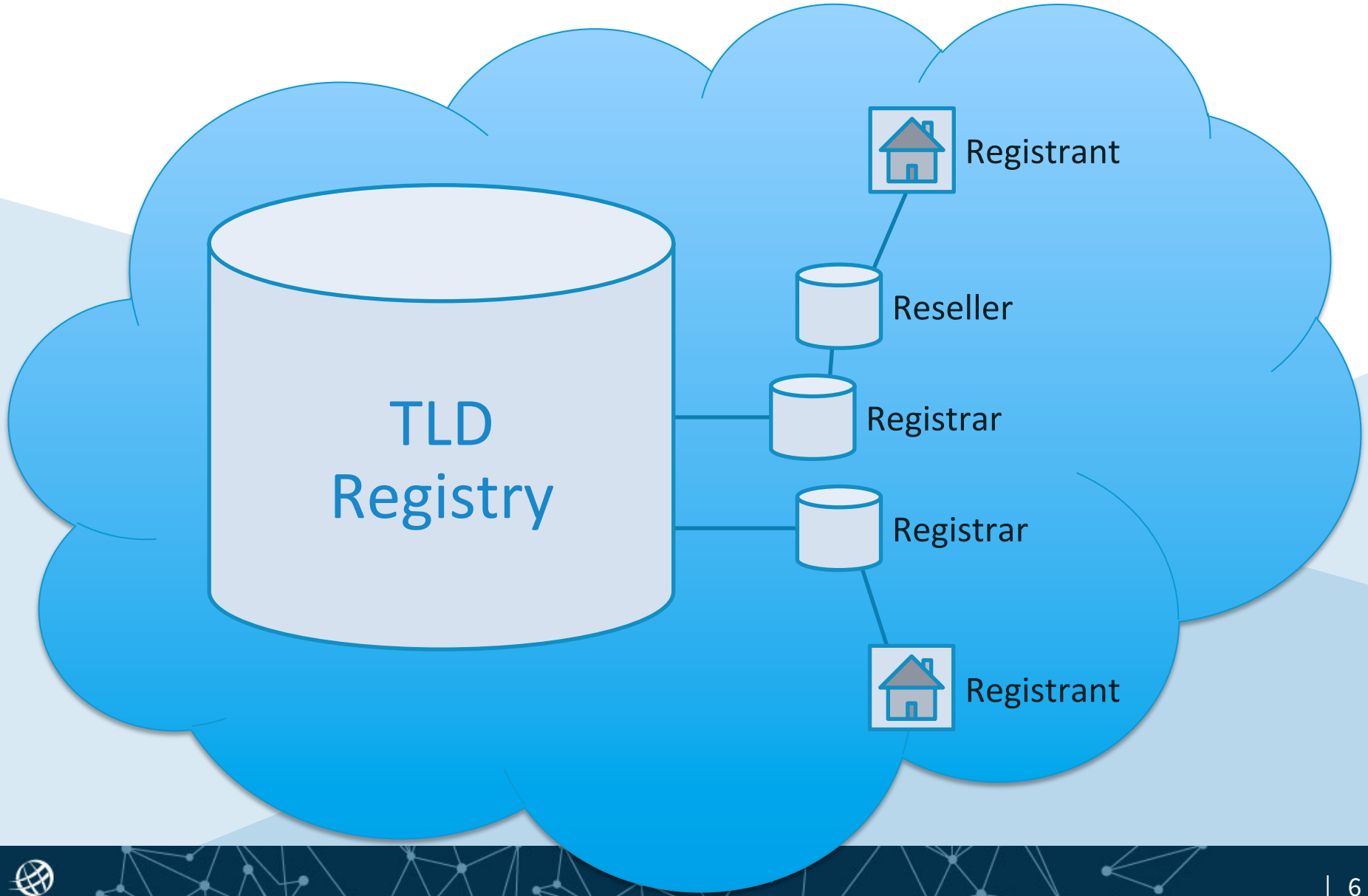
- Regional Internet Registries (RIRs)
  - Network addresses and routing information
- Protocol parameter registries
  - Internet Assigned Numbers Authority (IANA)
- Land ownership
- Motor vehicle ownership
- Gift registries (e.g., wedding, baby)

Registries in the DNS Tree

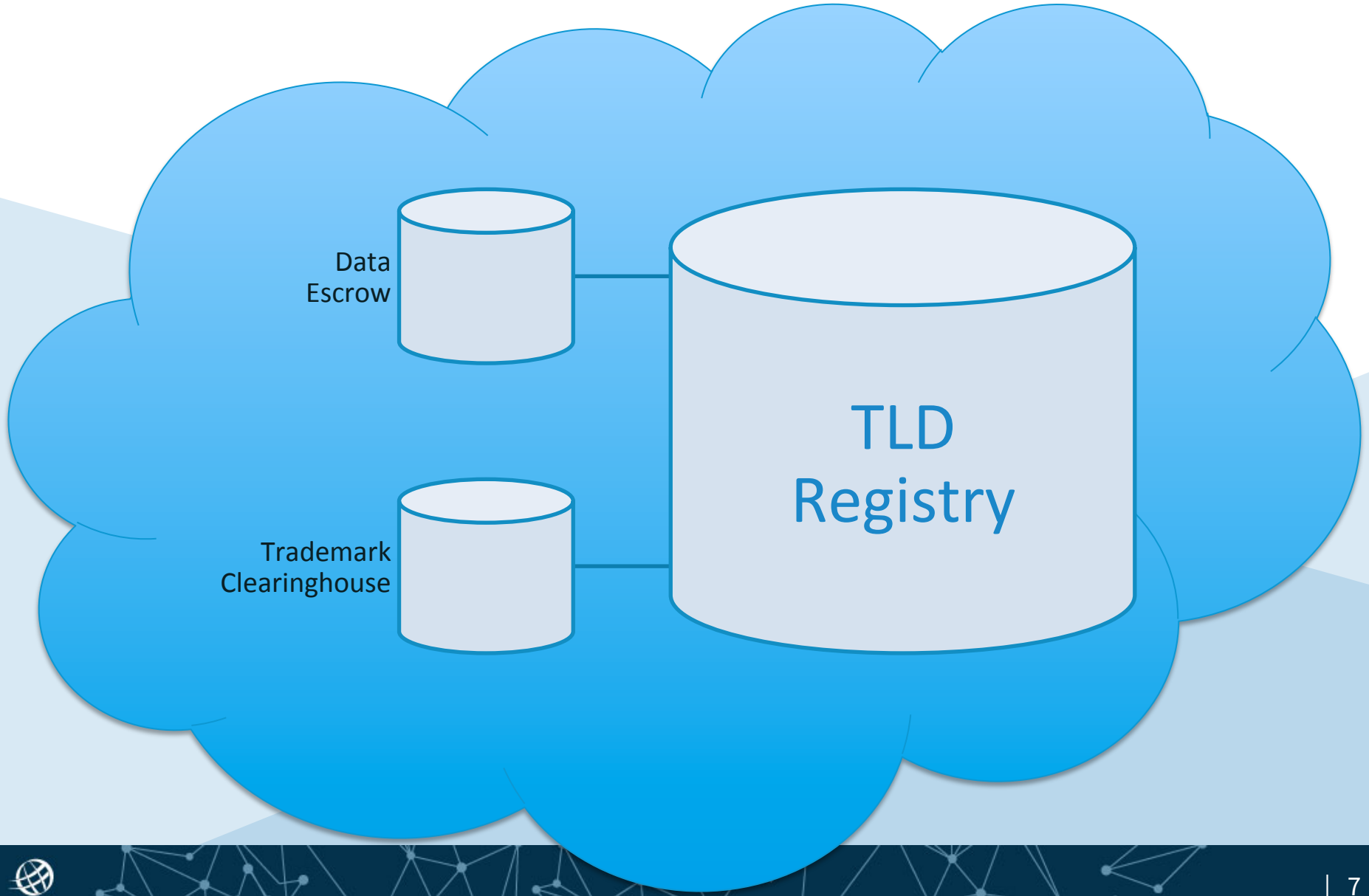


host.domain.TLD

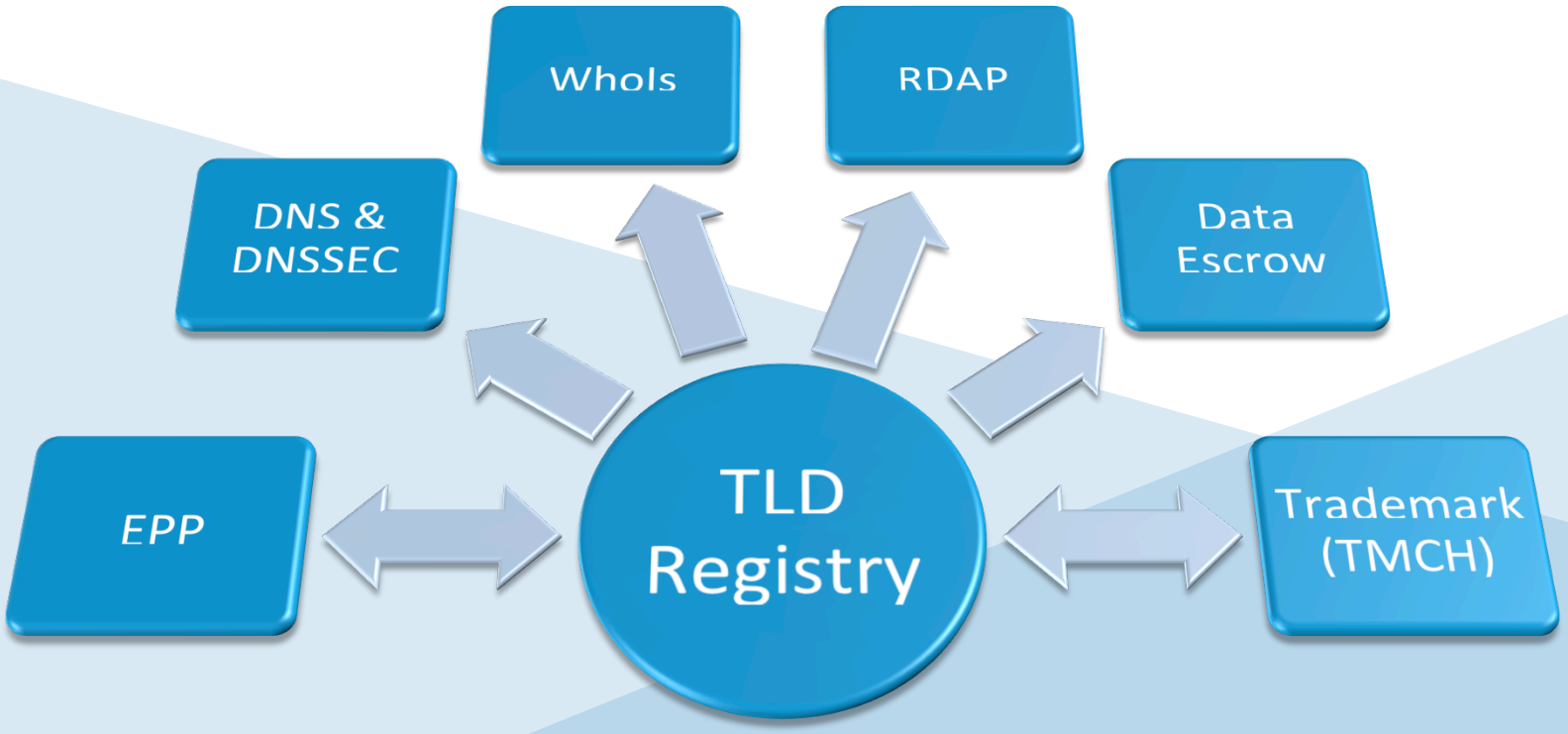
TLD Registry Relationship



From the Other Side…



Protocols of a TLD Registry




DNS
Domain Name System

What is the DNS Protocol?

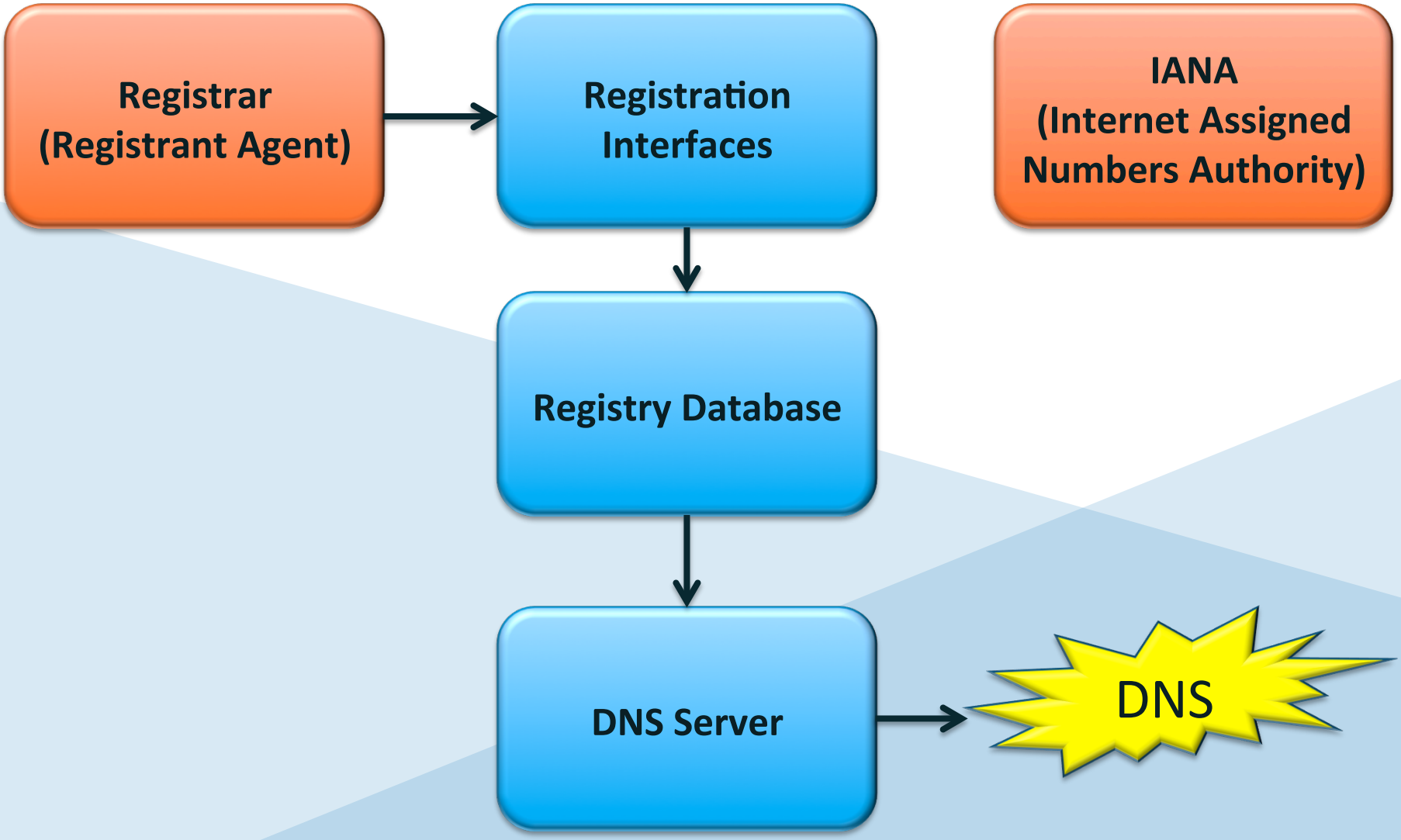
- A lookup, much akin to looking up someone's phone number in an old style phone book
- Query asks for information (e.g., domain name, type)
- Response contains the information or "no"

Significance of the DNS

- One of the earliest protocols
  - Impacts design, attempts to improve
  - Has proven to be resistant to replacement
- Domain Name Registries exist because of it
  - Means to enter and manage data transferred

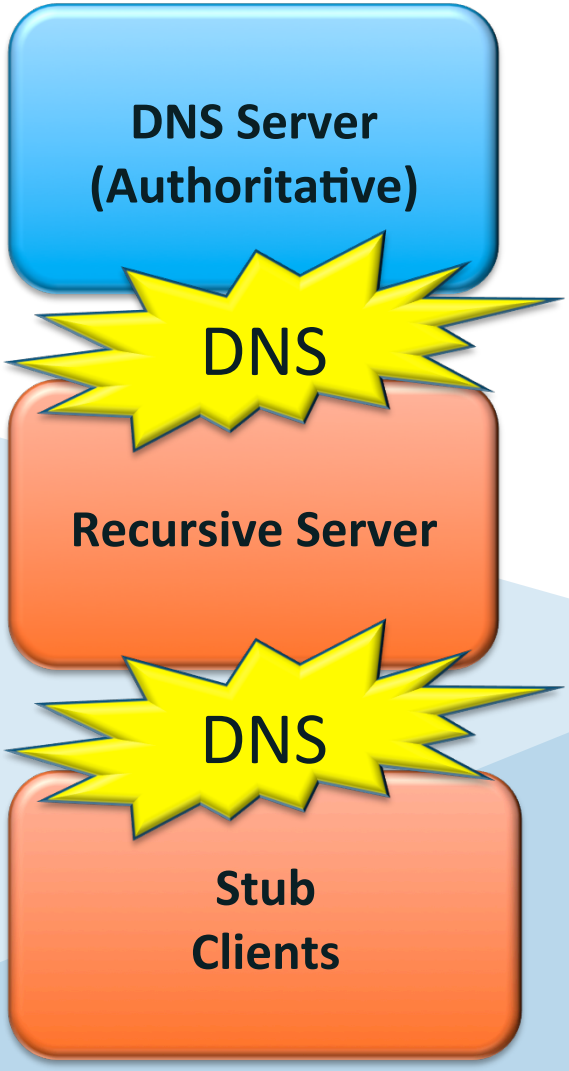
What DNS Means to a Registry

- Most important component in terms of resiliency
  - Unlike other components, approaches critical status
- Most used component, untold relying parties
  - High capacity for volume of use
  - Senders of queries are anonymous


Registrar
(Registrant Agent)
Registration
Interfaces
IANA
(Internet Assigned
Numbers Authority)
Registry Database
DNS Server
DNS

Components of the DNS

- Authoritative server
  - What the registry operates
- Recursive server
  - What issues queries to registry servers
- Stub/clients
  - Individual users (people or automated systems)


DNS Server
(Authoritative)
DNS
Recursive Server
DNS
Stub
Clients

DNSSEC

DNS Security Extensions

What does DNSSEC do?

- The end user rarely contacts the true source of DNS information directly
  - DNS data is stored in intermediate servers
  - DNS data is transferred in the open
- End-to-end encryption, like HTTPS, isn't a solution
  - Provide authenticity, completeness
  - Within constraints of DNS

History of DNSSEC

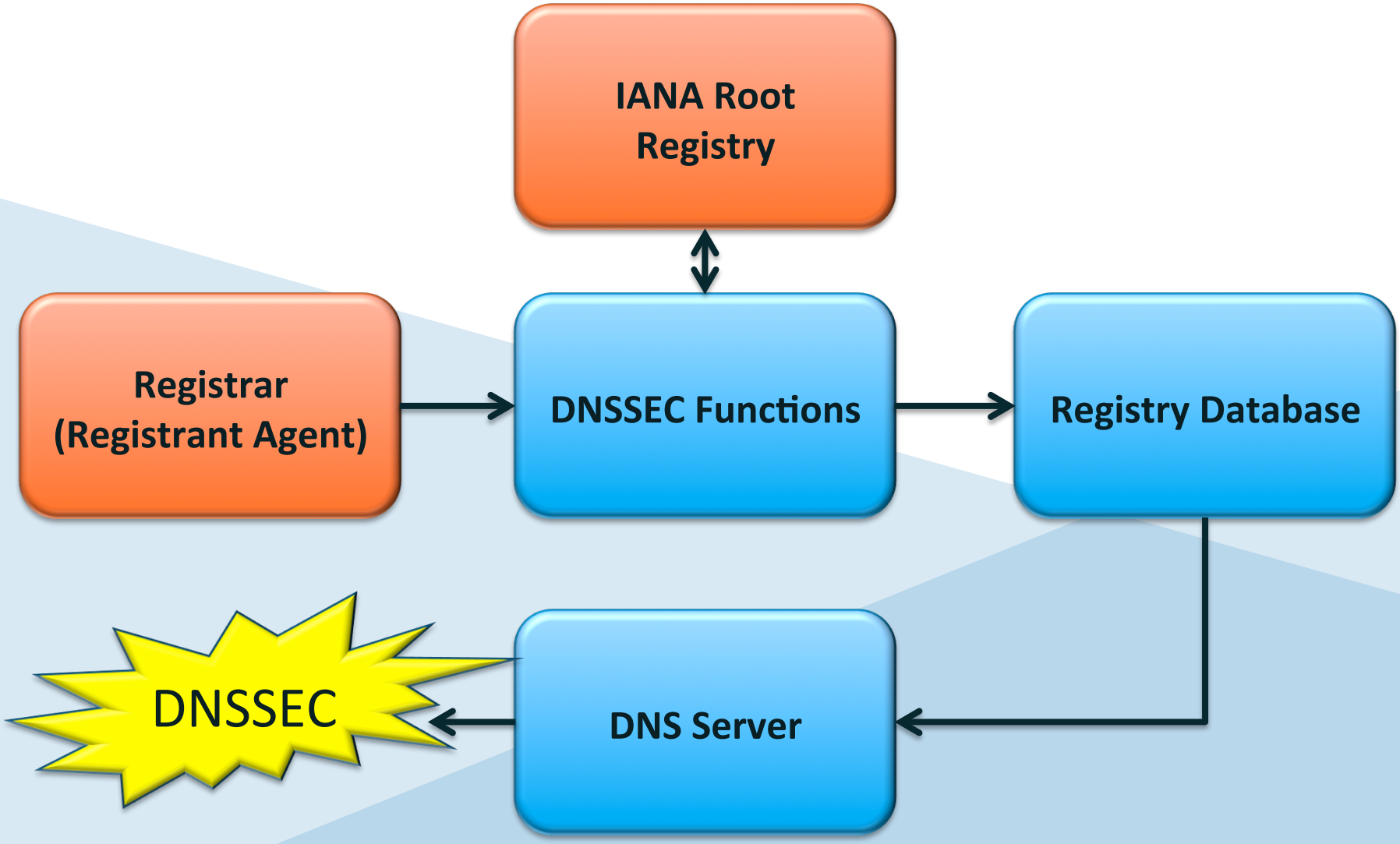
- Developed in 1990's, workshops with operators through 2004
- Internet Engineering Task Force (IETF) base documents published 2004
- Dan Kaminsky's 2008 talk elevated priority
  - *The End Of The Cache As We Know It*
  - Black Hat Conference 2008
- Since 2009 has been in operations in TLDs and the root zone (2010)

Approach to DNSSEC

- Data is accompanied with a digital signature which can be validated with a public key
- Public key cryptography enables a scalable trust building framework
- A hierarchy matching the DNS tree enables a verifiable trust building framework

The Registry's Portion of DNSSEC

- Managing keys for the TLD
- Registering delegation signer (DS) records from registrants
- Signing DS records and publishing
- Signing negative answers ("no")
- Interacting with IANA to register TLD key material


IANA Root Registry
Registrar (Registrant Agent)
DNSSEC Functions
Registry Database
DNSSEC
DNS Server

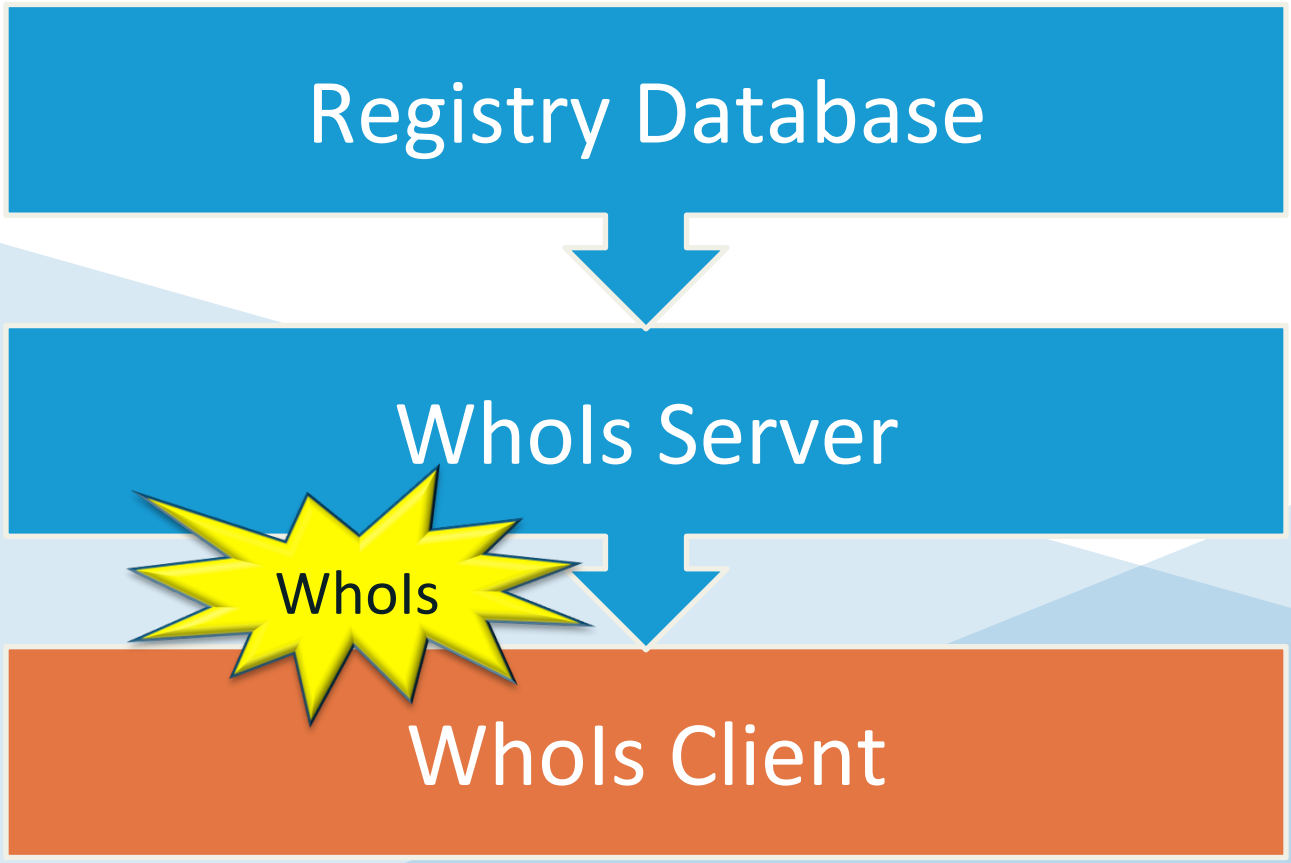
WhoIs

History of WhoIs

- Predating even DNS
- Means to identify the other end(s) of the network
- Simplistic question and answer
- At the time, no concerns about privacy, security, accuracy

WhoIs Protocol Definition

- Open a TCP connection to port 43
- Send a question
- Wait
- Receive an answer
- Close the connection


Registry Database
WhoIs Server
WhoIs
WhoIs Client

Why is that a Problem? (WhoIs Challenges?)

- Questions and answers undefined
  - Free form is not good for interoperability
  - Early software assumed ASCII only
- No meta-answers, no "use some other server"
- Differentiated access impossible
- No means to validate data in answers

WhoIs Sessions @ICANN53

Next Steps for WhoIs Accuracy Reporting

- Wednesday, 24 June
- 17:00 – 18:30
- Auditorio

Thick WhoIs Policy Implementation – Meeting with the IRT

- Wednesday, 24 June
- 17:00 – 18:30
- Retiro B

EPP

Extensible Provisioning Protocol

What it EPP?

- A business-to-business protocol between a registrar and registry

- Purpose is to edit the registration data base
  - Add, delete registered names
  - Add, delete, modify contacts
  - Transfers
  - Plus some other "maintenance"

History of EPP

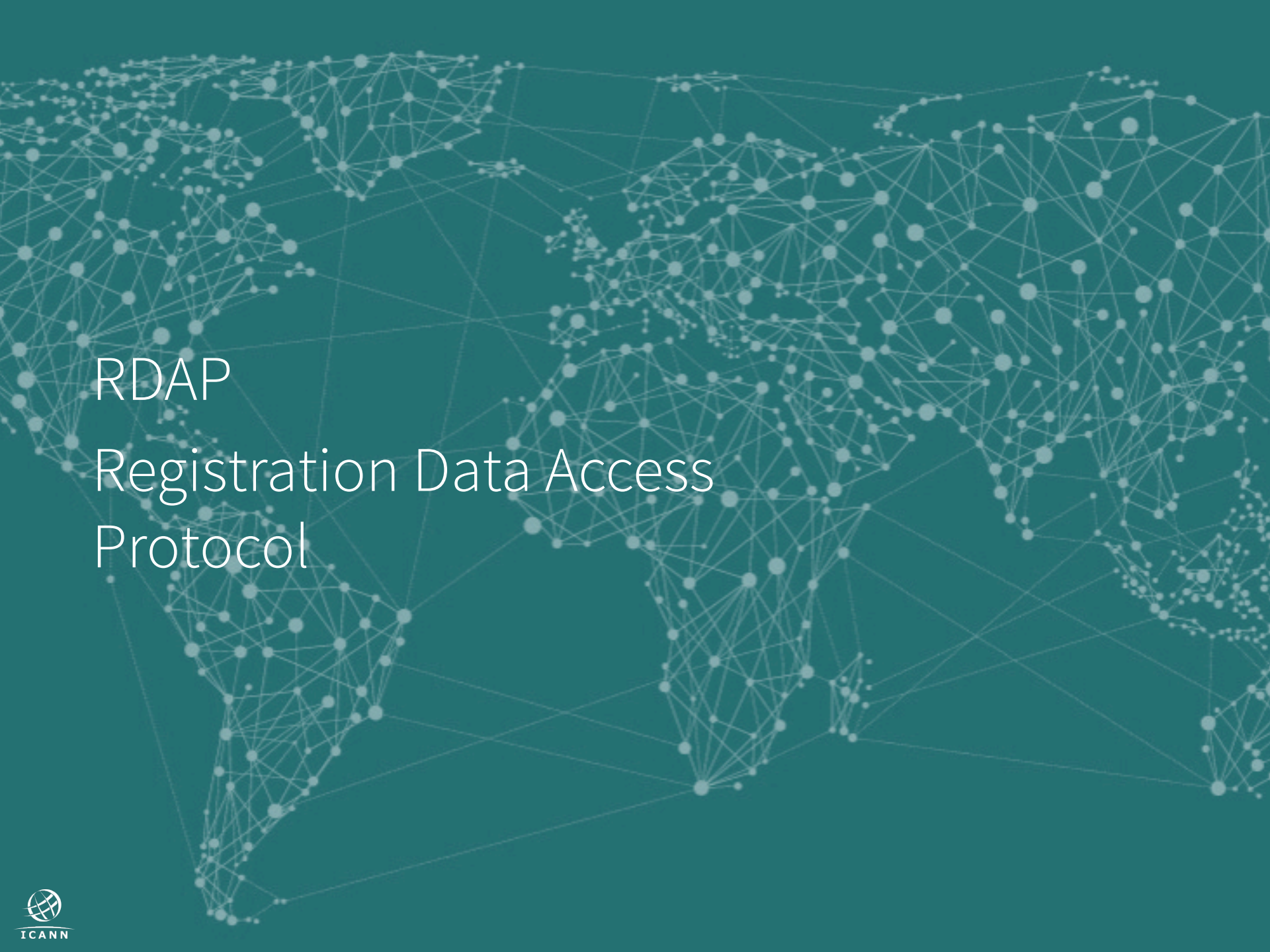
- 2000-2003 developed in IETF
  - Based on earlier protocols with the COM/NET registry
- 2003-2009 progressed to full standard
- Mandated for gTLDs and sTLDs
- Gained acceptance among ccTLDs
- Current IETF WG to manage extension designated as standard

EPP Exclusivity

- EPP need not be exclusive
  - A registry is technically able to use multiple protocols for this
  - Policy might restrict (such as strict First Come First Served via registrars)

EPP Protocol Architecture

- Uses TLS or strongly secured transport layer
- Exchange is encoded in XML
- Server inside registry, clients at registrars



RDAP

Registration Data Access Protocol

What is RDAP?

- Registration Data Access Protocol (RDAP)
- A query/response means to inspect a registration database
  - Regardless of where it is hosted
  - Biased towards registration not only domain names
- A layer on top of HTTPS
  - Reuses much of web-developed technology

Components of RDAP

- Server
  - Software to parse queries
  - Software to access the database
  - Software to prepare response
- Client
  - Web browser API with specific abilities
  - Can perform authentication steps

History of RDAP

- Dissatisfaction with WhoIs led two RIRs to experiment with a Web-based approach
  - Very successful
- From this, the story of RDAP is very much tied to
  - Replacement of the WhoIs protocol
  - Commonality of names and numbers
  - The HTTPS protocol

Basic Description of RDAP

- Query over HTTPS, looks like a URL
  - Like WhoIs, but formalized
- Response over HTTPS
  - Formatted data answering query, using "JSON"
    - Like WhoIs, but formalized
  - Formatted redirection message
    - Not in WhoIs
- To do: operational profile

Features of RDAP

- Defined data model
  - Expansion-friendly query and response formats
- Expansion beyond ASCII characters (I18N)
- Distribution of data sources
- Differentiated access (authorization model)
  - Presumes an authentication model too
- Compatibility with 2010-era software engineering


RDAP
RDAP Client
RDAP Message Handler
Registry Database

RDAP Sessions @ICANN53

Registration Data Access Protocol: What's Next?

- Wednesday, 24 June
- 14:15 – 15:30
- Retiro A

Data Escrow

Purpose of Data Escrow

- Store the registration database contents with a third party for safe keeping

- Why?
  - Operator "business" failure
  - Allows for restart of registry by another operator

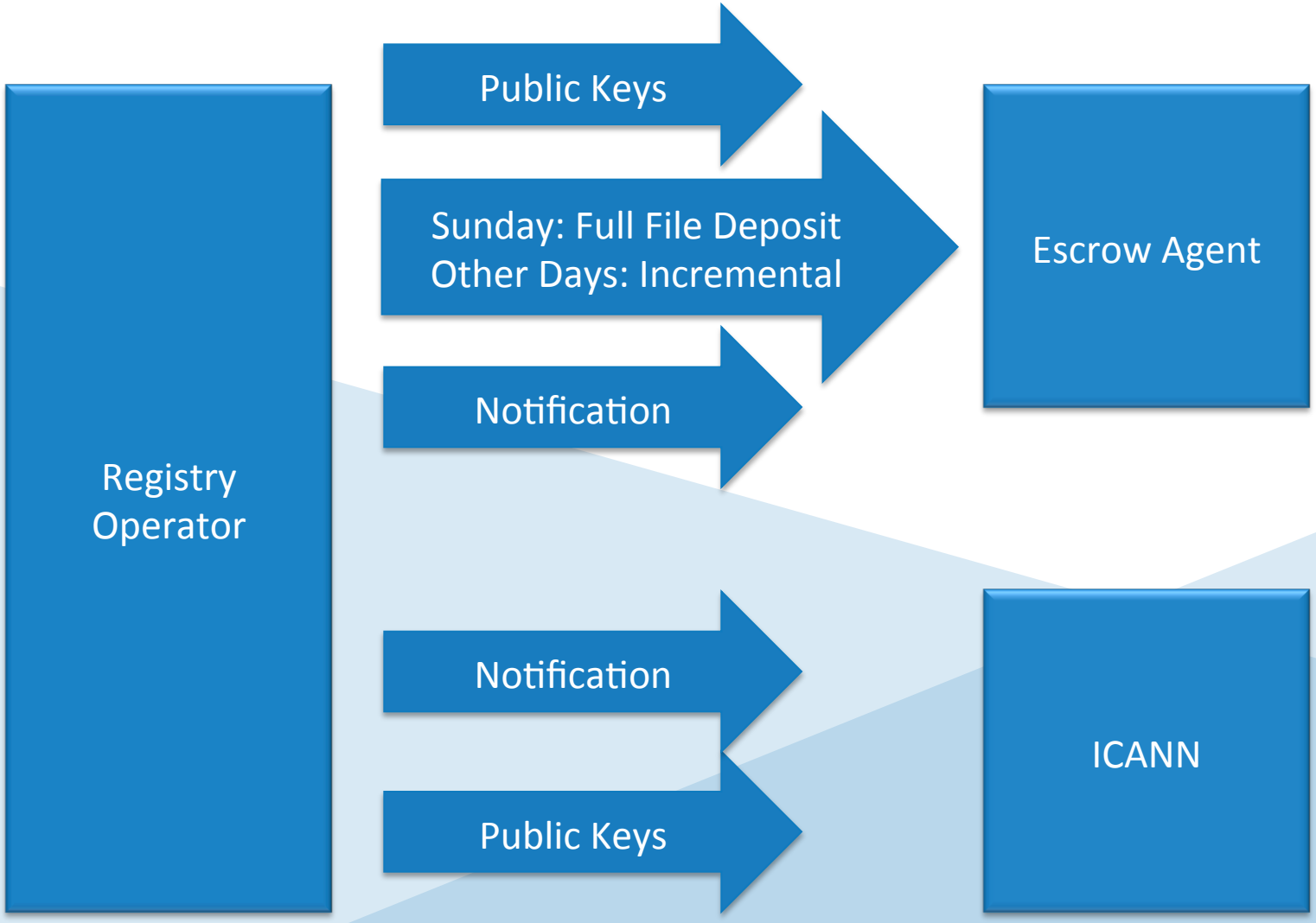
- Stored by a third party with strict rules for access by anyone else
  - E.g., ICANN can request the deposits under a slim set of circumstances

History of Data Escrow

- IETF Birds of Feather session
  - Deemed uninteresting to the IETF
- This doesn't mean data escrow is unimportant
- The reason is that data escrow is technically very simple, but very specific and related to governing policy

Data Escrow Deposits

- Defined in two places
  - Data "framework" in an Internet Draft
  - Timing of actions in Specification 2 of registry agreements
- A "dump" of the registry database
  - XML version in one or more files
  - Compressed/Encrypted
  - Deposit made every day
    - Full on Sunday; Incremental all other days of the week


Public Keys
Sunday: Full File Deposit
Other Days: Incremental
Notification
Escrow Agent
Registry
Operator
Notification
Public Keys
ICANN

TMCH

Trademark Clearinghouse

What is TMCH?

- Trademark Clearing House (TMCH) is an open but mostly ICANN-specific mechanism to address trademarks in domain names

- Limiting the discussion to registry-touching protocols
  - Two phases, Sunrise and Trademark Claims
  - Protocol built over HTTPS (secured Web)

TMCH in Sunrise

- Sunrise refers to opening of TLD to trademark holders first

- Registry supplies to a TMCH
  - List of domain name registered

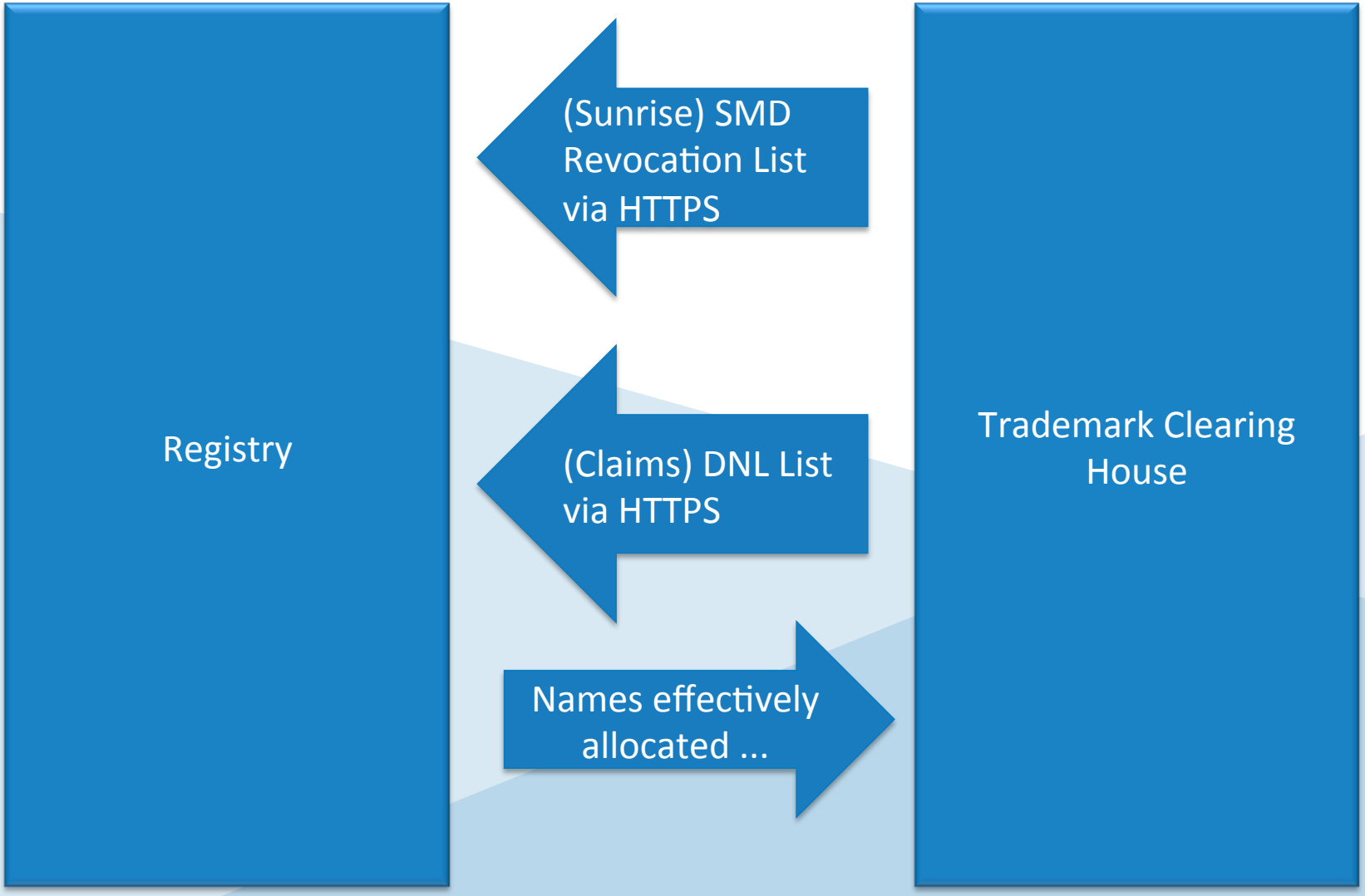
- Registry receives from a TMCH
  - A list of marks no longer listed (revoked from a previously published list)

TMCH in Trademark Claims

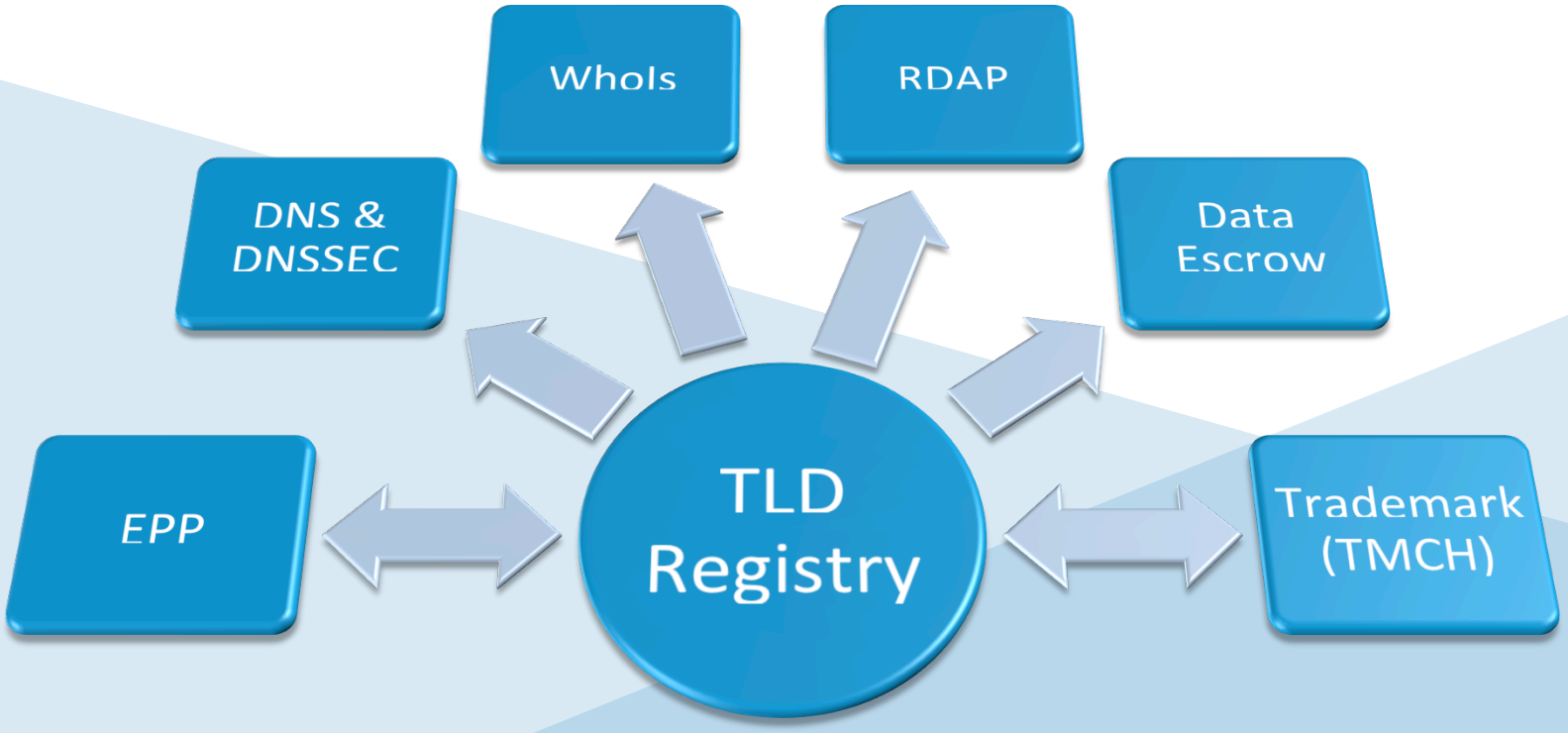
- Claims refers to early days of a TLD when registrations of trademark "look alikes" result in notices

- Registry supplies to a Trademark Clearing House
  - List of domain names registered matching the pre-registered trademarks

- Registry receives from a Trademark Clearing House
  - A list of labels corresponding to pre-registered trademarks


Registry
(Sunrise) SMD Revocation List via HTTPS
(Claims) DNL List via HTTPS
Names effectively allocated ...
Trademark Clearing House

Protocols of a TLD Registry



Engage with ICANN – http://www.icann.org

Thank You and Questions

Reach us at:
Email:
edward.lewis@icann.org
steve.conte@icann.org

twitter.com/icann

gplus.to/icann

facebook.com/icannorg

weibo.com/ICANNorg

linkedin.com/company/icann

flickr.com/photos/icann

youtube.com/user/icannnews

slideshare.net/icannpresentations