Hosting Community

A Leading Russian Domain Name Registrar

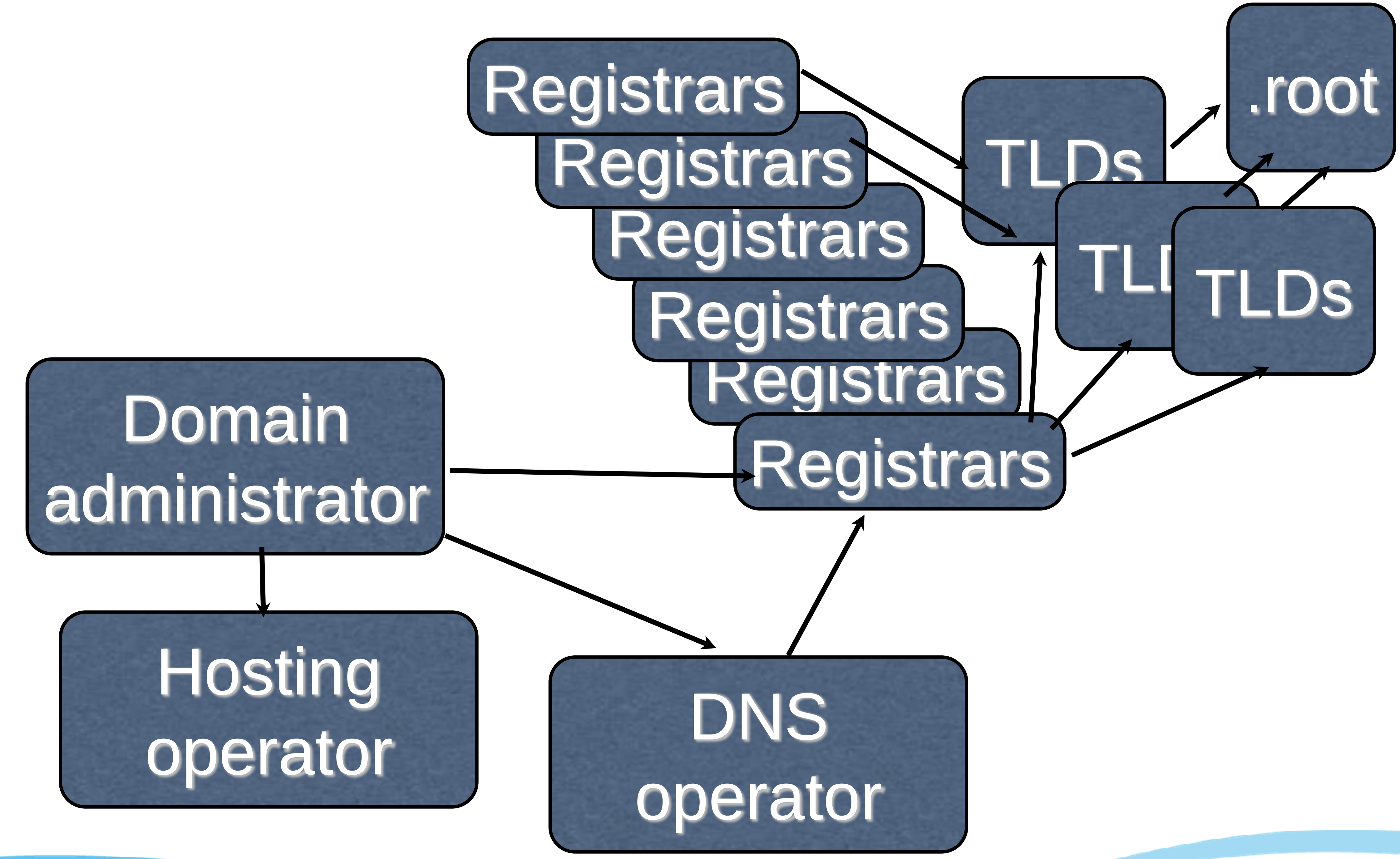
RU-Center DNSSEC experience and expectations

(registrar point of view)

Vasily Dolmatov - Head of R&D

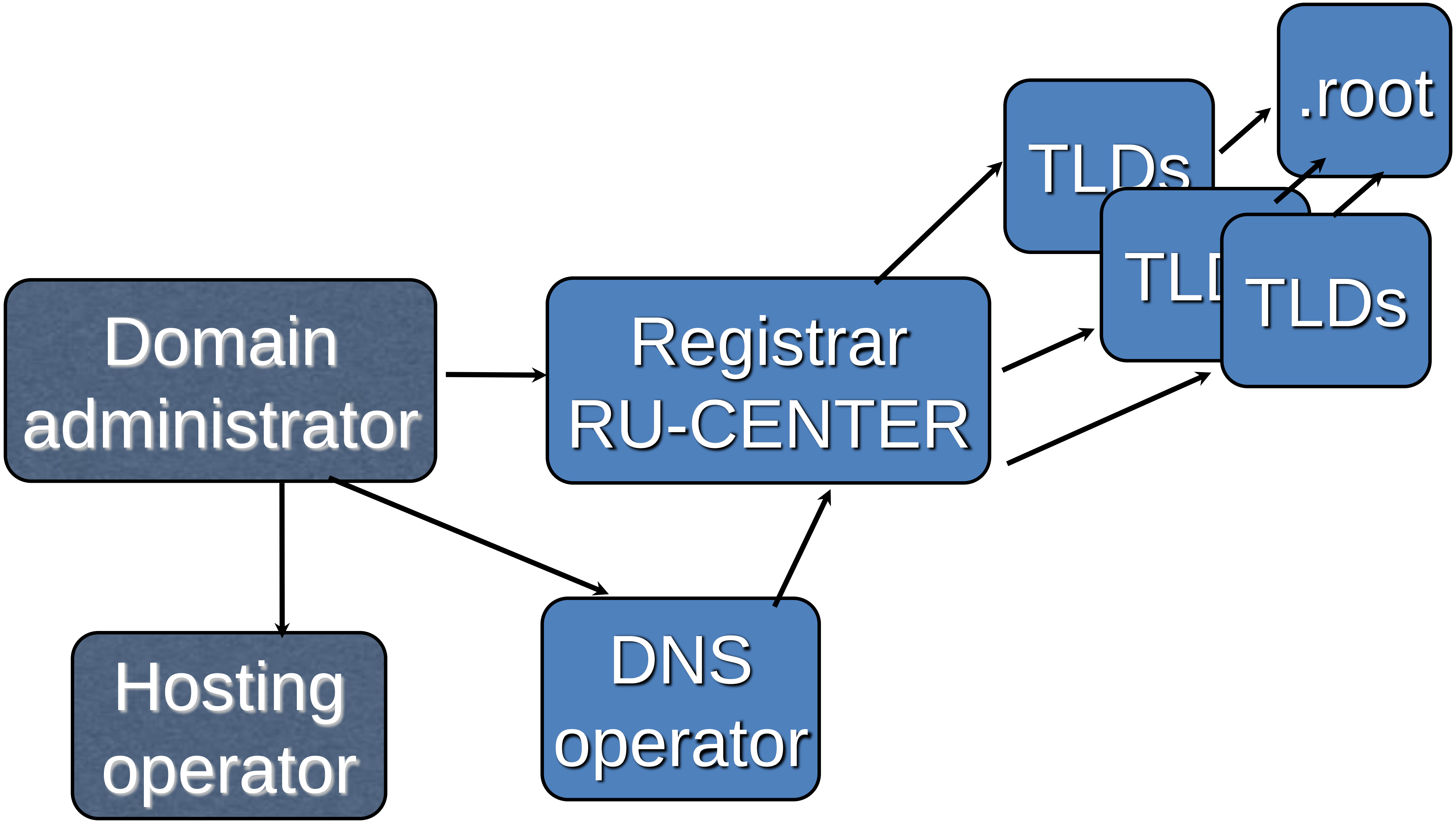
12.09.2013

Current DNS system

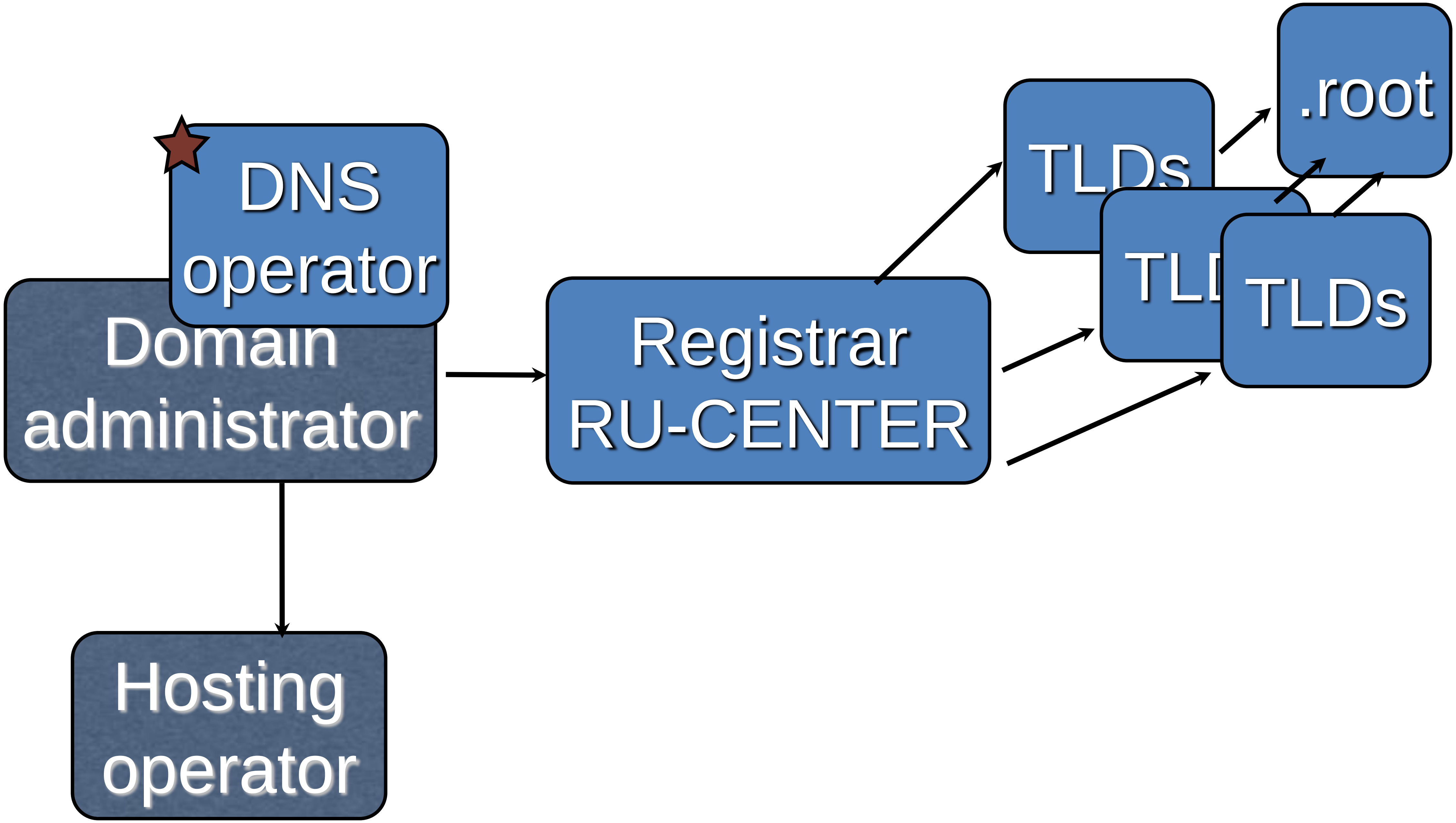


Hosting Community

DNSSEC participants

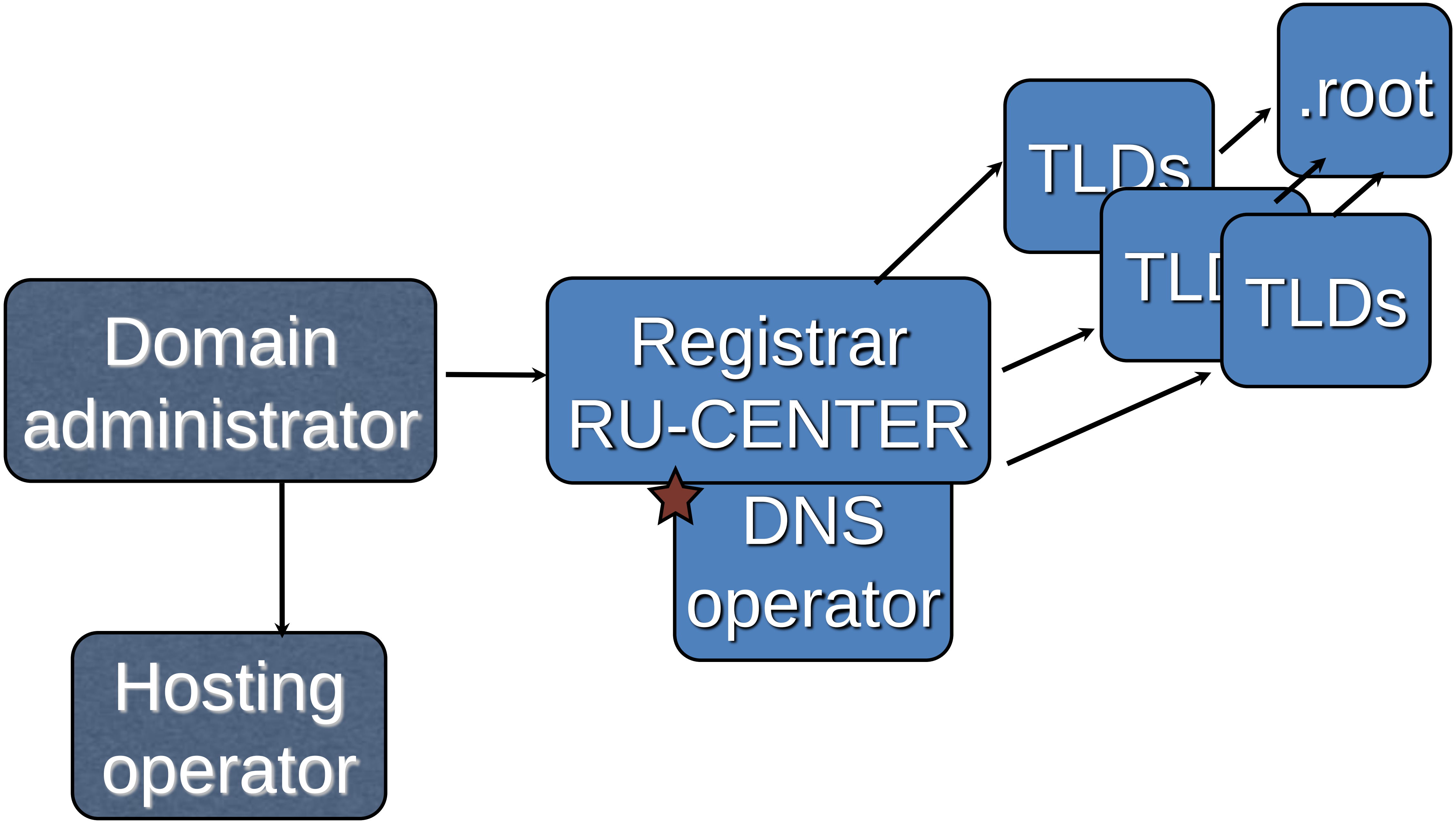


DNSSEC participants



Hosting Community

DNSSEC participants



Domain administrator

Registrar RU-CENTER

DNS operator

Hosting operator

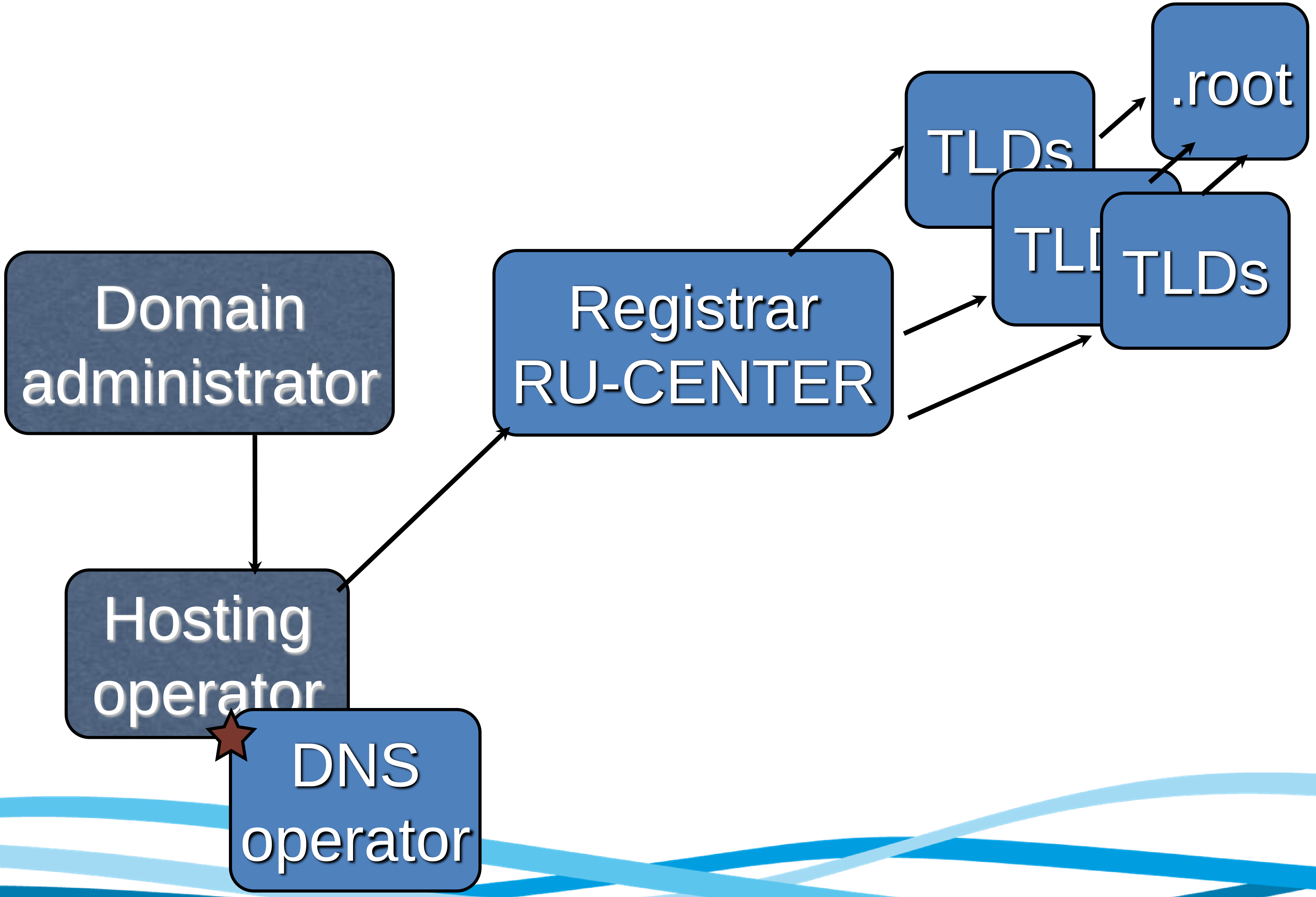
TLDs

TLDs

TLDs

.root

DNSSEC participants



What we see?
Part 1 - DNS operators

Hosting Community

- Different set of used algorithms (not a problem)
- Different number of keys (not a problem)
- Different key rollover procedures (not a problem)
- Lack of understanding of DNSSEC operation (IS a PROBLEM!)

What we see?
Part 2 - Registries

- Different protocols (EPP parameters, web-interfaces, etc.) (IS a PROBLEM!)
- Different set of accepted algorithms (IS a PROBLEM!)
- Different number of keys (not a problem)
- Different rules (DS or DS+DNSKEY) (IS a PROBLEM!)
- Different key rollover procedures (not a problem)

What we feel?
Part 3 - Registrar to Registry

- Developing and testing own subset of protocol for every registry (soon will be the hundreds of them!)
- Implementing different lifecycles and rollover procedures for every registry (hundreds!!)
- Different sets of algorithms and different rules (DS or DS+DNSKEY)

What we feel?
Part 4 - Registrar to Clients

- Clients do not understand DNSSEC functionality and processes (tons of questions to support, lots of configuring errors)
- Problems if DNS operator is not in the business chain
- Registrar is considered responsible by the clients for all unclear DNSSEC procedures.

What we NEED?
Part 1 - Registrar to Registry

- IDENTICAL set of protocols, algorithms and DNSSEC lifecycles for all registries (new RA seems to address this), possibility to connect to new registries quickly without creating unique interface modules for every new registry
- Communication mechanisms between registry and registrars better than “periodically consult registry web-site”

Hosting Community

What we NEED?
Part 2 - Registrar to Clients

- Educational materials for clients, describing DNSSEC and its usage in simple words (not an-RFC style!)
- Recommended practices for end-user DNS operators for implementing DNSSEC, performing key rollovers, etc.
- Recommendation to put DNS operator in business chain

NSA and DNSSEC

- (+) No CAs, no certificates
- (+) Different algorithms (including GOST)
- (=) Private keys security
- (=) RNG quality
- (-) (none seen so far)
- (++) DANE – alternative way of trust

Questions?

Thank you!

v.dolmatov@hostcomm.ru