# Resource Directory

draft-ietf-core-resource-directory

*Christian Amsüss*, Zach Shelby, Michael Koster, Carsten Bormann,
Peter van der Stok

2020-11-17

Picking highlights here; full changelog is detailed.

- "First Come First Remembered": example policy; implementatons may choose as default
- Host discovery *is not* secured, path discovery *is* if needed
- Move simple registration from `/.well-known/core` to `/.well-known/rd`
- More care for `rt` registered values

# But treating them raised questions

"When DTLS is used like TLS, replay protection should be considered"

| Event | Reqeust | Response |
|---|---|---|
| Power on | `POST /rd?ep=node1` | `/reg/reg1` |
| Power off | `DELETE /reg/1`[1] | Deleted |
| Power on | `POST /rd?ep=node1` | `/reg/reg1` |
| Replayed message | `DELETE /reg/1` | on but gone |

Works with and without replay protection, even in OSCORE

[1] sniff sniff

# Step to be taken

Server ensures freshness using Echo.

Mechanism already referenced for Simple Registration and amplification mitigation.

WIP text is in #291[2].

[2] See there for explored alternatives.

# Server authorization

Q: “How much can you trust links from the RD?”

A: “As far as this is allowed by security policies.”

## Server authorization

Q: “How much can you trust links from the RD?”

A: “As far as this is allowed by security policies.”

---

Intention $\rightarrow$ Request $\rightarrow$ Effect / Response

# Server authorization

Q: "How much can you trust links from the RD?"

A: "As far as this is allowed by security policies."

---

Create a topic $\xrightarrow{\texttt{rt=topics}}$ $\underbrace{\texttt{POST /tpcs} \rightarrow \text{Topic gets created}}_{\text{security layers}}$

Trust an authorized RD that checks, or verify before use.

And this can be way more powerful with forms, or when the RS sets the ACE scope.

# Possibilities to be explored

## on the long term – outside RD

- Single-use servers: "If it's on this host, it's the PubSub server." Security contexts multiply.
- Deposited verifiable statments in the RD. Granularity? Audience?
- Finer grained authorization: "...is authorized to provide the PubSub service at its `/tpcs` resource." Linking to requests without multiplying contexts?

## And by the way, your examples are needlessly large

Yes. RFC6690, ambiguity, different readings...

## And by the way, your examples are needlessly large

Yes. RFC6690, ambiguity, different readings...

...but turned out mine was the worst.

- In many resource lookup results, `anchor` is superfluous.
- TBD: Give precise rules when anchor must still be set, rewrite examples.
- Existing RD servers stay compliant (just verbose).
- Pending recheck of the RFC6690 implementations.

# Outlook

-27 around start of December:

Freshness on registration updates.

Relaxed anchor setting.

Continued exploration of protecting intention?