DID Resolution

A work item of the W3C CCG

14th November 2019
IPR rules apply!

Zoom Call:
https://zoom.us/j/7077077007

Text Chat:
http://irc.w3.org/?channels=ccg
(type q+ to get into the queue)

This call is being recorded!

Agenda Thursday 14 November 2019
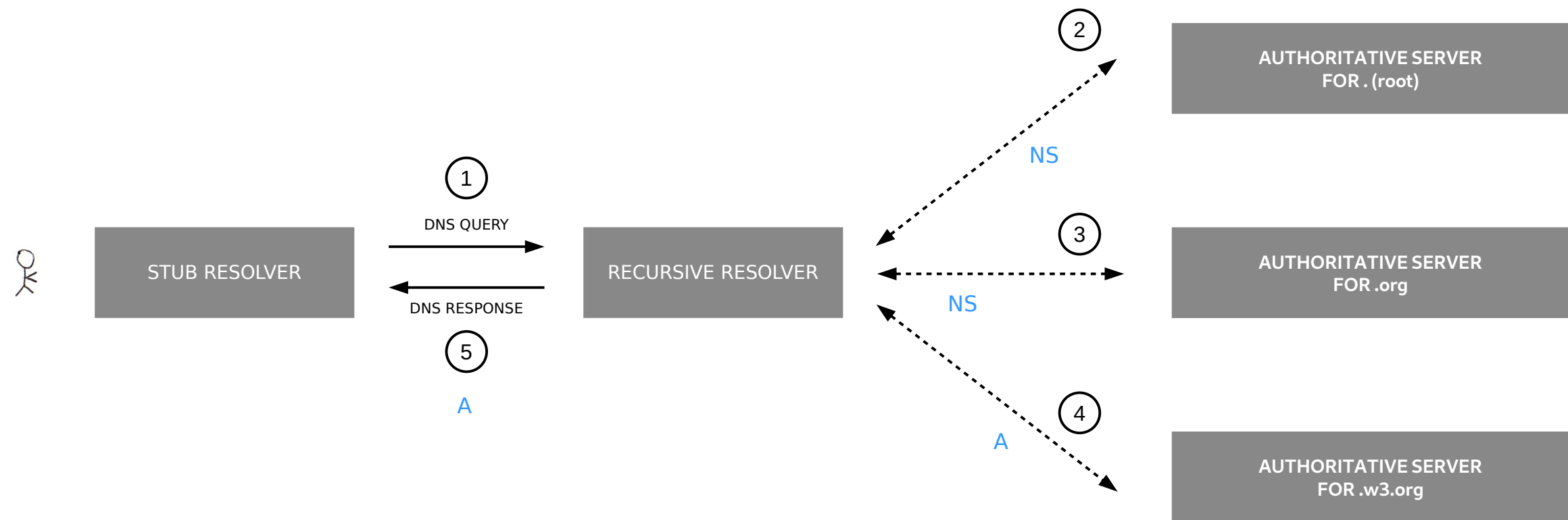
Welcome and CCG IPR reminder

Call info and scribe selection

Agenda creation/review/prioritization

Continue discussion about trusted resolution, proofs on DID documents and DID resolution results; comparison with DNSSEC.

AOB

Next meeting

1 → Lookup **"www.w3.org"**

2 → Lookup **"www.w3.org"**
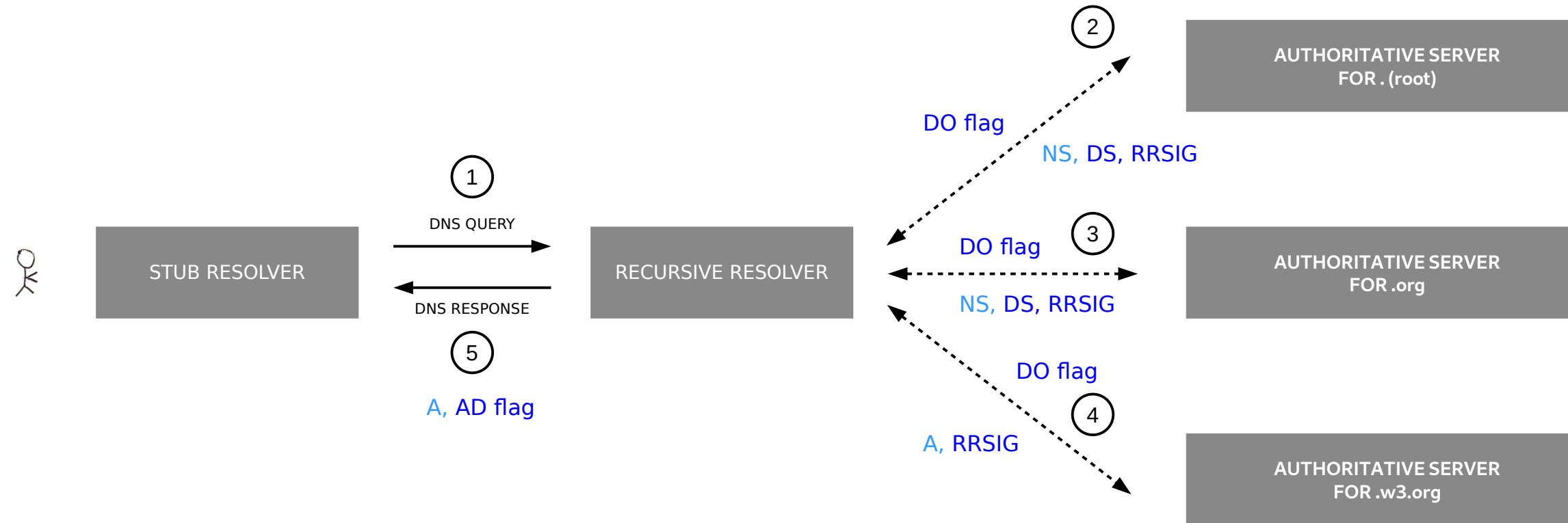
← NS – IP(s) of authoritative nameserver for **.org**

4 → Lookup **"www.w3.org"**

← A – IP of **www.w3.org**

3 → Lookup **"www.w3.org"**

← NS – IP(s) of authoritative nameserver for **.w3.org**

5 ← A – IP of **www.w3.org**

STUB RESOLVER

RECURSIVE RESOLVER

① DNS QUERY

⑤ DNS RESPONSE

A, AD flag

② DO flag
NS, DS, RRSIG

AUTHORITATIVE SERVER
FOR . (root)

③ DO flag
NS, DS, RRSIG

AUTHORITATIVE SERVER
FOR .org

④ DO flag
A, RRSIG

AUTHORITATIVE SERVER
FOR .w3.org

① → Lookup **"www.w3.org"**

② → Lookup **"www.w3.org"**
→ Set DO flag ("DNSSEC OK")

← NS – IP(s) of authoritative nameserver for **.org**
← DS – Reference to public key for **.org**
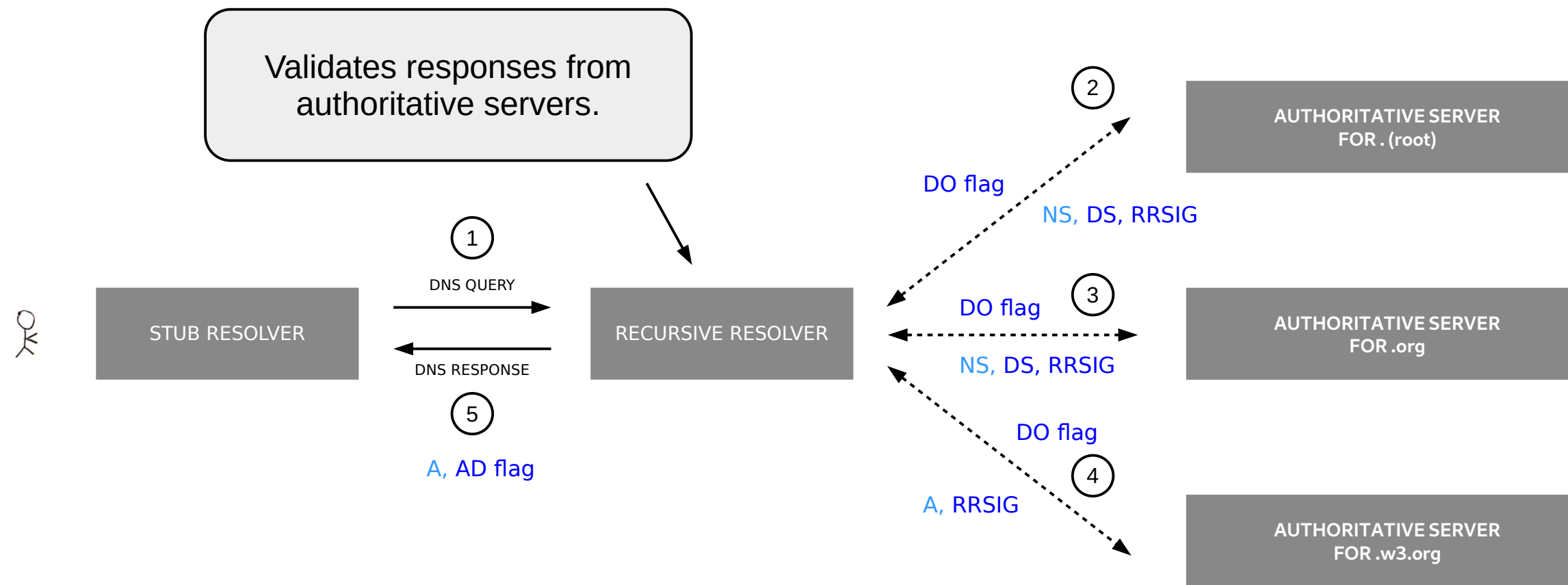← RRSIG – Proof, can be validated by public key for **. (root)**

③ → Lookup **"www.w3.org"**
→ Set DO flag ("DNSSEC OK")

← NS – IP(s) of authoritative nameserver for **.w3.org**
← DS – Reference to public key for **.w3.org**
← RRSIG – Proof, can be validated by public key for **.org**

④ → Lookup **"www.w3.org"**
→ Set DO flag ("DNSSEC OK")

← A – IP of **www.w3.org**
← RRSIG – Proof, can be validated by public key for **.w3.org**

⑤ ← A – IP of **www.w3.org**
← Set AD flag ("Authenticated Data")

Validates responses from authoritative servers.

STUB RESOLVER — **RECURSIVE RESOLVER**

① DNS QUERY
⑤ DNS RESPONSE
A, AD flag

② **AUTHORITATIVE SERVER FOR . (root)**
DO flag
NS, DS, RRSIG

③ **AUTHORITATIVE SERVER FOR .org**
DO flag
NS, DS, RRSIG

④ **AUTHORITATIVE SERVER FOR .w3.org**
DO flag
A, RRSIG

---

① → Lookup **"www.w3.org"**

② → Lookup **"www.w3.org"**
→ Set DO flag ("DNSSEC OK")

← NS – IP(s) of authoritative nameserver for **.org**
← DS – Reference to public key for **.org**
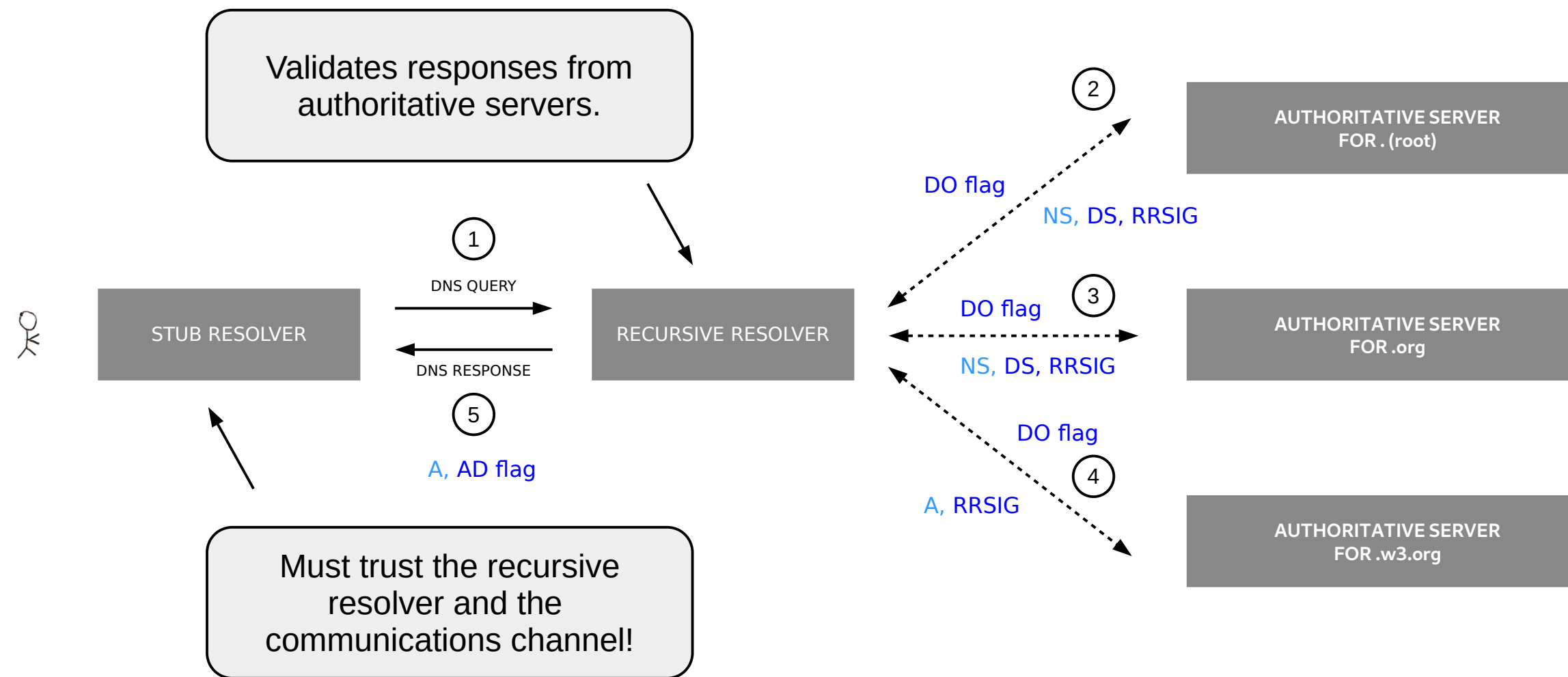← RRSIG – Proof, can be validated by public key for **. (root)**

③ → Lookup **"www.w3.org"**
→ Set DO flag ("DNSSEC OK")

← NS – IP(s) of authoritative nameserver for **.w3.org**
← DS – Reference to public key for **.w3.org**
← RRSIG – Proof, can be validated by public key for **.org**

④ → Lookup **"www.w3.org"**
→ Set DO flag ("DNSSEC OK")

← A – IP of **www.w3.org**
← RRSIG – Proof, can be validated by public key for **.w3.org**

⑤ ← A – IP of **www.w3.org**
← Set AD flag ("Authenticated Data")

Validates responses from authoritative servers.

Must trust the recursive resolver and the communications channel!

STUB RESOLVER

RECURSIVE RESOLVER

AUTHORITATIVE SERVER FOR . (root)

AUTHORITATIVE SERVER FOR .org

AUTHORITATIVE SERVER FOR .w3.org

① DNS QUERY

DNS RESPONSE

⑤ A, AD flag

② DO flag / NS, DS, RRSIG

③ DO flag / NS, DS, RRSIG

④ DO flag / A, RRSIG

① → Lookup **"www.w3.org"**

② → Lookup **"www.w3.org"**
→ Set DO flag ("DNSSEC OK")

← NS – IP(s) of authoritative nameserver for **.org**
← DS – Reference to public key for **.org**
← RRSIG – Proof, can be validated by public key for **. (root)**

③ → Lookup **"www.w3.org"**
→ Set DO flag ("DNSSEC OK")

← NS – IP(s) of authoritative nameserver for **.w3.org**
← DS – Reference to public key for **.w3.org**
← RRSIG – Proof, can be validated by public key for **.org**

④ → Lookup **"www.w3.org"**
→ Set DO flag ("DNSSEC OK")

← A – IP of **www.w3.org**
← RRSIG – Proof, can be validated by public key for **.w3.org**

⑤ ← A – IP of **www.w3.org**
← Set AD flag ("Authenticated Data")

① → Lookup **"www.w3.org"**
→ Set CD flag ("Checking Disabled")
→ Set DO flag ("DNSSEC OK")

② → Lookup **"www.w3.org"**
→ Set DO flag ("DNSSEC OK")

← NS – IP(s) of authoritative nameserver for **.org**
← DS – Reference to public key for **.org**
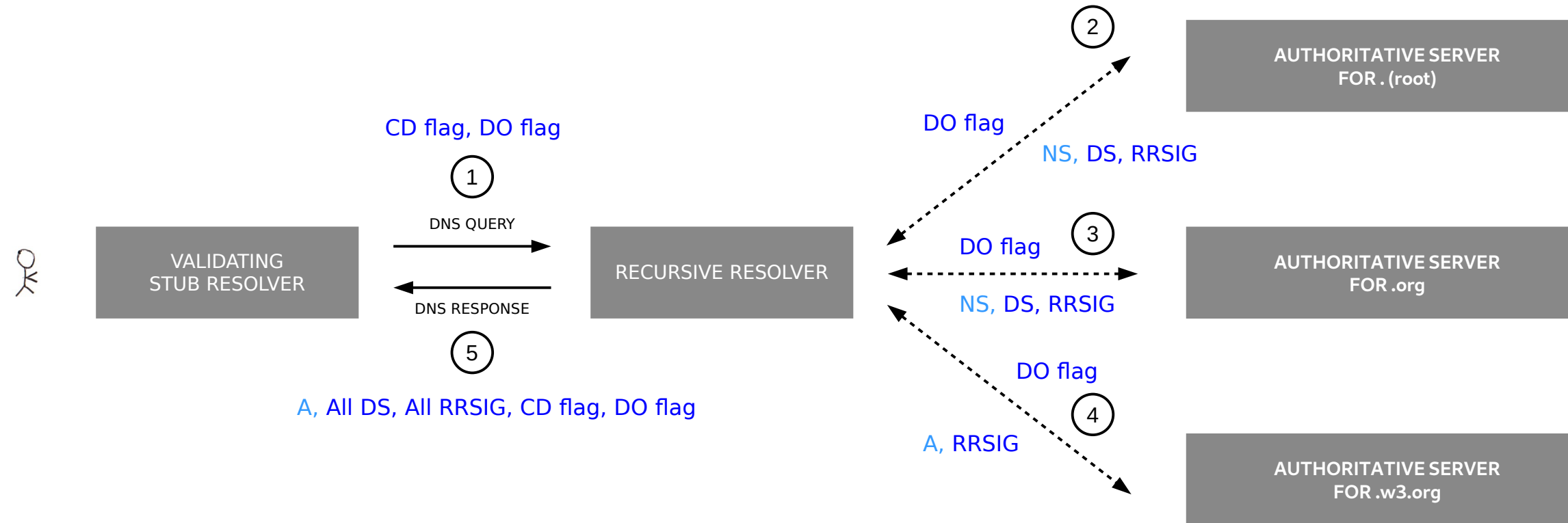← RRSIG – Proof, can be validated by public key for **. (root)**

③ → Lookup **"www.w3.org"**
→ Set DO flag ("DNSSEC OK")

← NS – IP(s) of authoritative nameserver for **.w3.org**
← DS – Reference to public key for **.w3.org**
← RRSIG – Proof, can be validated by public key for **.org**

④ → Lookup **"www.w3.org"**
→ Set DO flag ("DNSSEC OK")

← A – IP of **www.w3.org**
← RRSIG – Proof, can be validated by public key for **.w3.org**

⑤ ← A – IP of **www.w3.org**
← All DS – References to public keys
← All RRSIG – Proofs
← Set CD flag ("Checking Disabled")
← Set DO flag ("DNSSEC OK")

Simply passed through responses without validating them.

CD flag, DO flag
① DNS QUERY

VALIDATING STUB RESOLVER → RECURSIVE RESOLVER

DNS RESPONSE
⑤
A, All DS, All RRSIG, CD flag, DO flag

②
DO flag
NS, DS, RRSIG
AUTHORITATIVE SERVER FOR . (root)

③
DO flag
NS, DS, RRSIG
AUTHORITATIVE SERVER FOR .org

④
DO flag
A, RRSIG
AUTHORITATIVE SERVER FOR .w3.org

---

① → Lookup **"www.w3.org"**
→ Set CD flag ("Checking Disabled")
→ Set DO flag ("DNSSEC OK")

② → Lookup **"www.w3.org"**
→ Set DO flag ("DNSSEC OK")

← NS – IP(s) of authoritative nameserver for **.org**
← DS – Reference to public key for **.org**
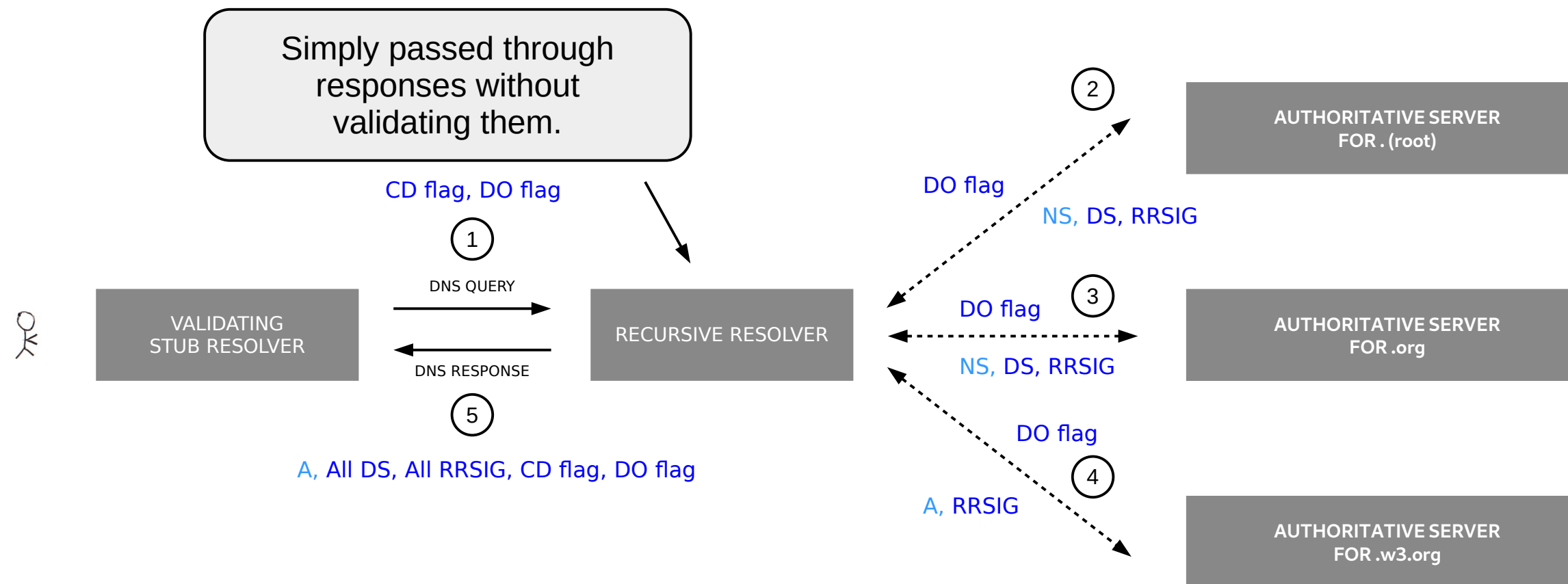← RRSIG – Proof, can be validated by public key for **. (root)**

③ → Lookup **"www.w3.org"**
→ Set DO flag ("DNSSEC OK")

← NS – IP(s) of authoritative nameserver for **.w3.org**
← DS – Reference to public key for **.w3.org**
← RRSIG – Proof, can be validated by public key for **.org**

④ → Lookup **"www.w3.org"**
→ Set DO flag ("DNSSEC OK")

← A – IP of **www.w3.org**
← RRSIG – Proof, can be validated by public key for **.w3.org**

⑤ ← A – IP of **www.w3.org**
← All DS – References to public keys
← All RRSIG – Proofs
← Set CD flag ("Checking Disabled")
← Set DO flag ("DNSSEC OK")

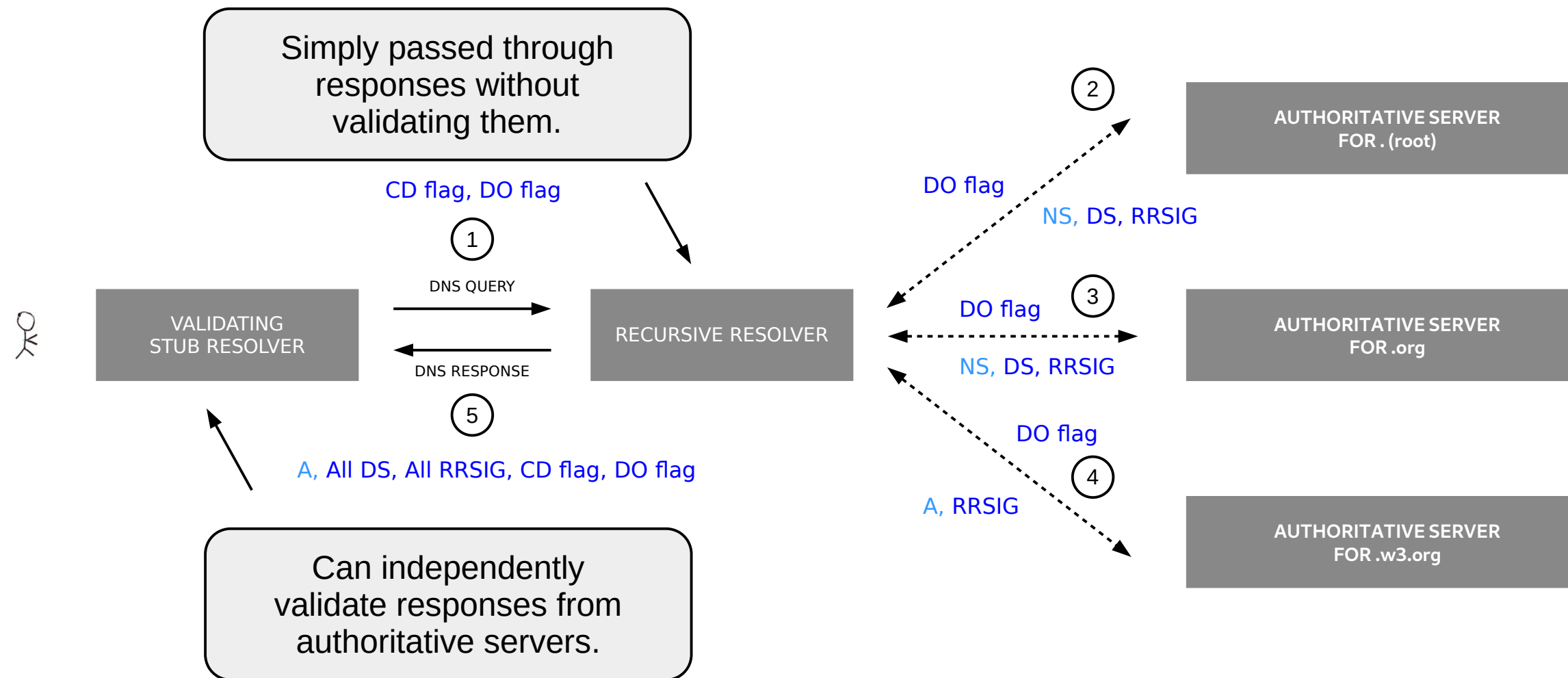Simply passed through responses without validating them.

Can independently validate responses from authoritative servers.

VALIDATING STUB RESOLVER

RECURSIVE RESOLVER

AUTHORITATIVE SERVER FOR . (root)

AUTHORITATIVE SERVER FOR .org

AUTHORITATIVE SERVER FOR .w3.org

CD flag, DO flag

① DNS QUERY

⑤ DNS RESPONSE

A, All DS, All RRSIG, CD flag, DO flag

② DO flag / NS, DS, RRSIG

③ DO flag / NS, DS, RRSIG

④ DO flag / A, RRSIG

① → Lookup **"www.w3.org"**
→ Set CD flag ("Checking Disabled")
→ Set DO flag ("DNSSEC OK")

② → Lookup **"www.w3.org"**
→ Set DO flag ("DNSSEC OK")

← NS – IP(s) of authoritative nameserver for **.org**
← DS – Reference to public key for **.org**
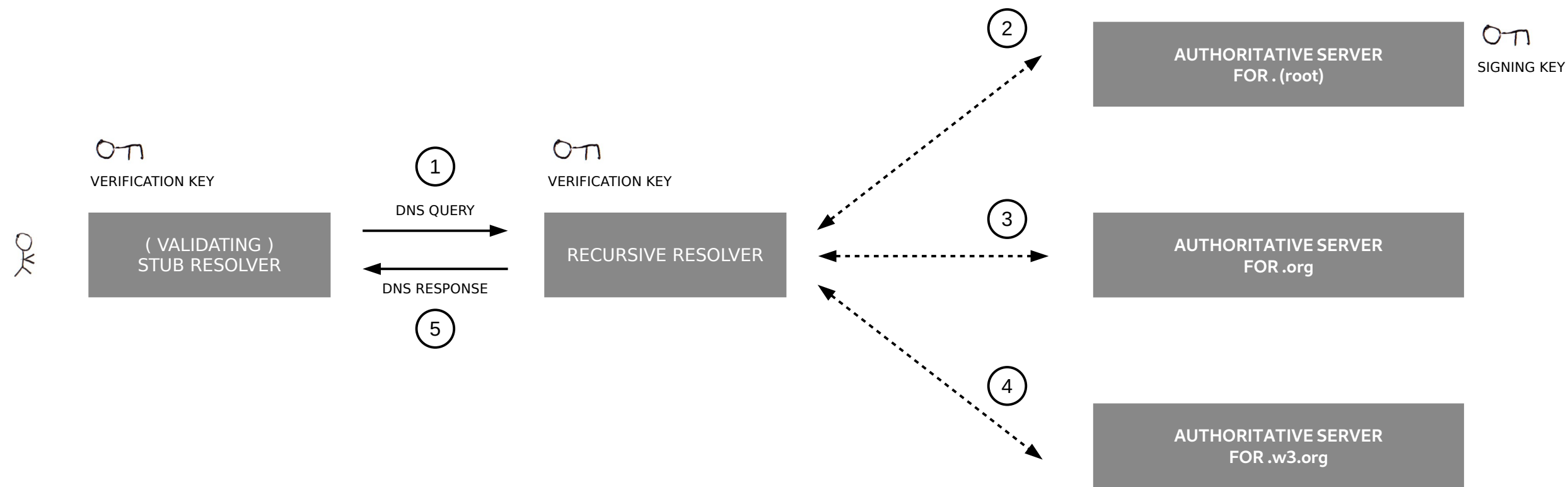← RRSIG – Proof, can be validated by public key for **. (root)**

③ → Lookup **"www.w3.org"**
→ Set DO flag ("DNSSEC OK")

← NS – IP(s) of authoritative nameserver for **.w3.org**
← DS – Reference to public key for **.w3.org**
← RRSIG – Proof, can be validated by public key for **.org**

④ → Lookup **"www.w3.org"**
→ Set DO flag ("DNSSEC OK")

← A – IP of **www.w3.org**
← RRSIG – Proof, can be validated by public key for **.w3.org**

⑤ ← A – IP of **www.w3.org**
← All DS – References to public keys
← All RRSIG – Proofs
← Set CD flag ("Checking Disabled")
← Set DO flag ("DNSSEC OK")

VERIFICATION KEY

**(VALIDATING)
STUB RESOLVER**

① DNS QUERY

⑤ DNS RESPONSE

VERIFICATION KEY

RECURSIVE RESOLVER

② **AUTHORITATIVE SERVER
FOR . (root)**   **SIGNING KEY**

③ **AUTHORITATIVE SERVER
FOR .org**

④ **AUTHORITATIVE SERVER
FOR .w3.org**

Can the recursive resolver verify the DNS records? ← Achieved by DNSSEC

Can the stub resolver verify the DNS records? ← Achieved by DNSSEC

DID RESOLVER

REMOTE BINDING

HTTPS GET

DID RESOLVER

REMOTE READ

DECENTRALIZED IDENTIFIER REGISTRY

Can the resolver verify the DID document? ← Should always be possible,
specific to DID method,
and depends on implementation

Can the client verify the DID document? ← May or may not be possible,
specific to DID method,
and depends on implementation

VERIFICATION KEY

(VALIDATING)
STUB RESOLVER

VERIFICATION KEY

RECURSIVE RESOLVER

① DNS QUERY

⑤ DNS RESPONSE

② AUTHORITATIVE SERVER
FOR . (root)

SIGNING KEY

③ AUTHORITATIVE SERVER
FOR .org

④ AUTHORITATIVE SERVER
FOR .w3.org

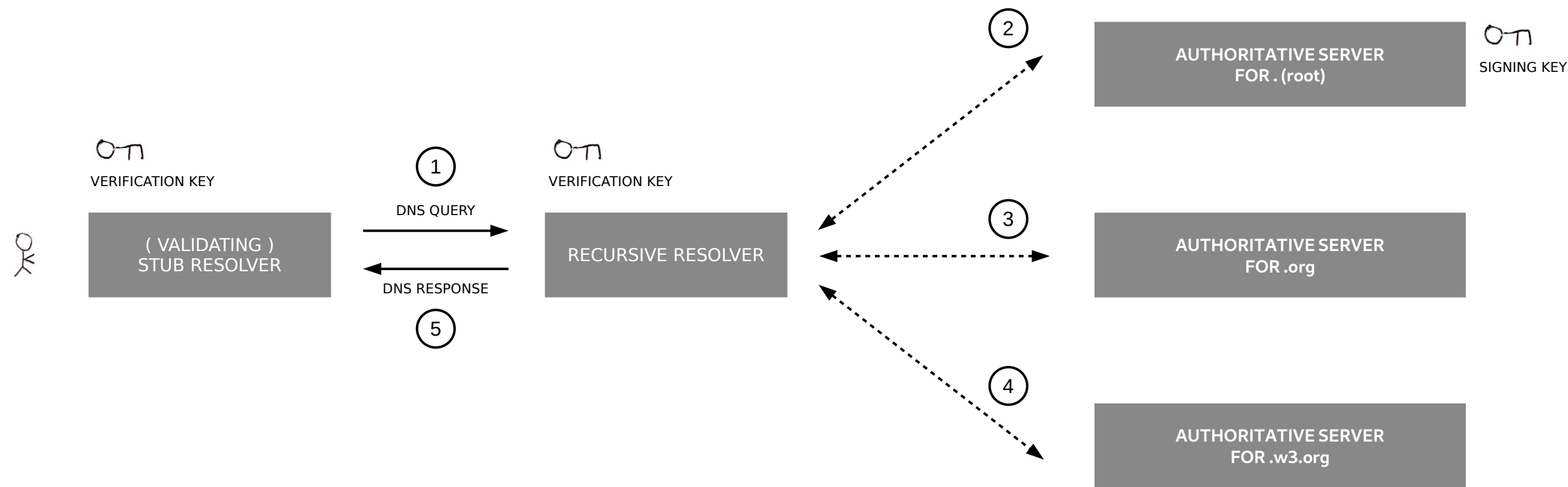Can the stub resolver verify the recursive resolver response?

Can the recursive resolver verify the DNS records? ← Achieved by DNSSEC

Can the stub resolver verify the DNS records? ← Achieved by DNSSEC

DID RESOLVER

REMOTE BINDING

HTTPS GET

DID RESOLVER

REMOTE READ

DECENTRALIZED IDENTIFIER REGISTRY
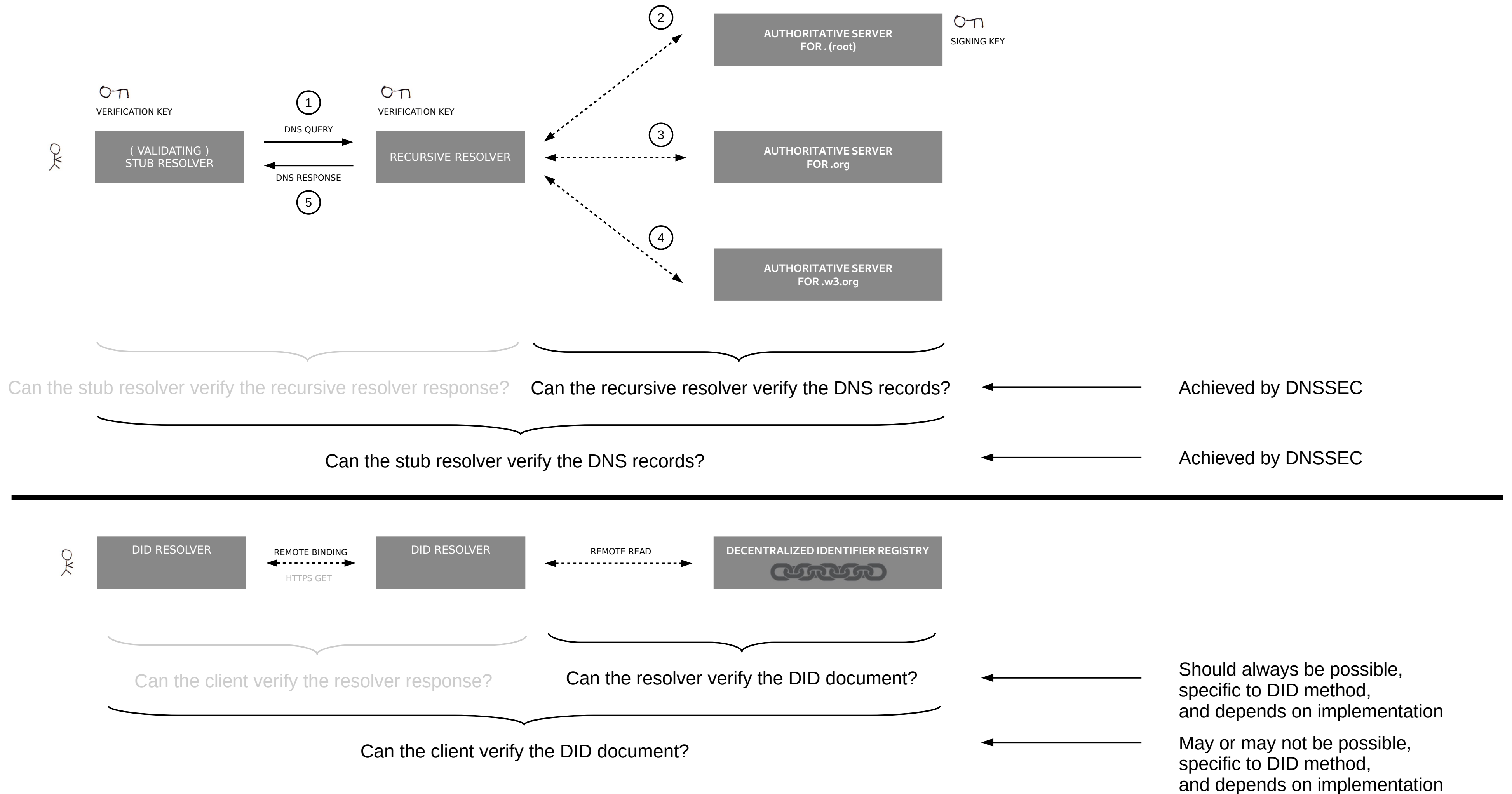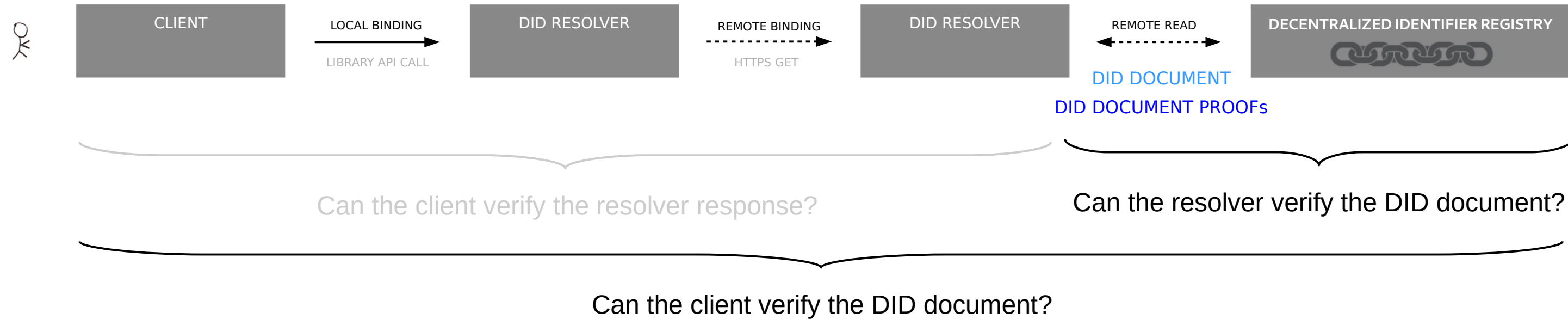
Can the client verify the resolver response?

Can the resolver verify the DID document? ← Should always be possible, specific to DID method, and depends on implementation

Can the client verify the DID document? ← May or may not be possible, specific to DID method, and depends on implementation
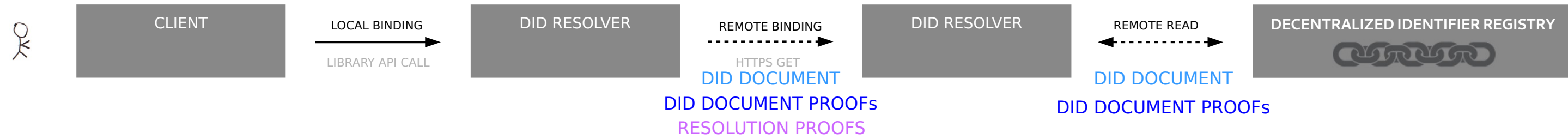
CLIENT — LOCAL BINDING / LIBRARY API CALL → DID RESOLVER — REMOTE BINDING / HTTPS GET → DID RESOLVER ← REMOTE READ → DECENTRALIZED IDENTIFIER REGISTRY

DID DOCUMENT
DID DOCUMENT PROOFs

Can the client verify the resolver response?

Can the resolver verify the DID document?

Can the client verify the DID document?

Examples of DID DOCUMENT PROOFS:
• Satoshi audit trail (btcr)
• BLS state proofs (sov)
• Signature by DID subject (web)

Partially analogous to DS, RRSIG in DNSSEC !

Is this part of the DID document, or DID resolution metadata?
(see https://github.com/w3c/did-core/issues/65)

```
{
    "@id": "did:example:12345",
    "service": [ ... ],
    "publicKey": [ ... ],
    "proof": [{
        "type": "SatoshiAuditTrail",
        ...
    }, {
        "type": "SovrinStateProof",
        ...
    }, {
        "type": "RsaSignature2018",
        ...
    }]
}
```

CLIENT	LOCAL BINDING	DID RESOLVER	REMOTE BINDING	DID RESOLVER	REMOTE READ	DECENTRALIZED IDENTIFIER REGISTRY
	LIBRARY API CALL		HTTPS GET			

DID DOCUMENT
DID DOCUMENT PROOFs
RESOLUTION PROOFS

DID DOCUMENT
DID DOCUMENT PROOFs

Can the client verify the resolver response?

Example of RESOLUTION PROOF:
- Signature added by DID resolver
- Method-independent

```
{
    "didDocument": {
        "@id": "did:example:12345",
        "service": [ ... ],
        "publicKey": [ ... ],
        "proof": [{
            "type": "SatoshiAuditTrail",
            ...
        }, {
            "type": "SovrinStateProof",
            ...
        }, {
            "type": "RsaSignature2018",
            ...
        }]
    },
    "resolverMetadata": {
    },
    "methodMetadata": {
    },
    "proof": {
        "type": "RsaSignature2018",
        "proofPurpose": "assertionMethod",
        "created": "2019-11-23T10:14:22Z",
        "verificationMethod": "https://uniresolver.io/keys.json",
        "jws": "eyJ0eXAiOiJK...gFWFOEjXk"
    }
}
```