

## DID Resolution

A work item of the W3C CCG

7<sup>th</sup> 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 07 November 2019

Welcome and CCG IPR reminder

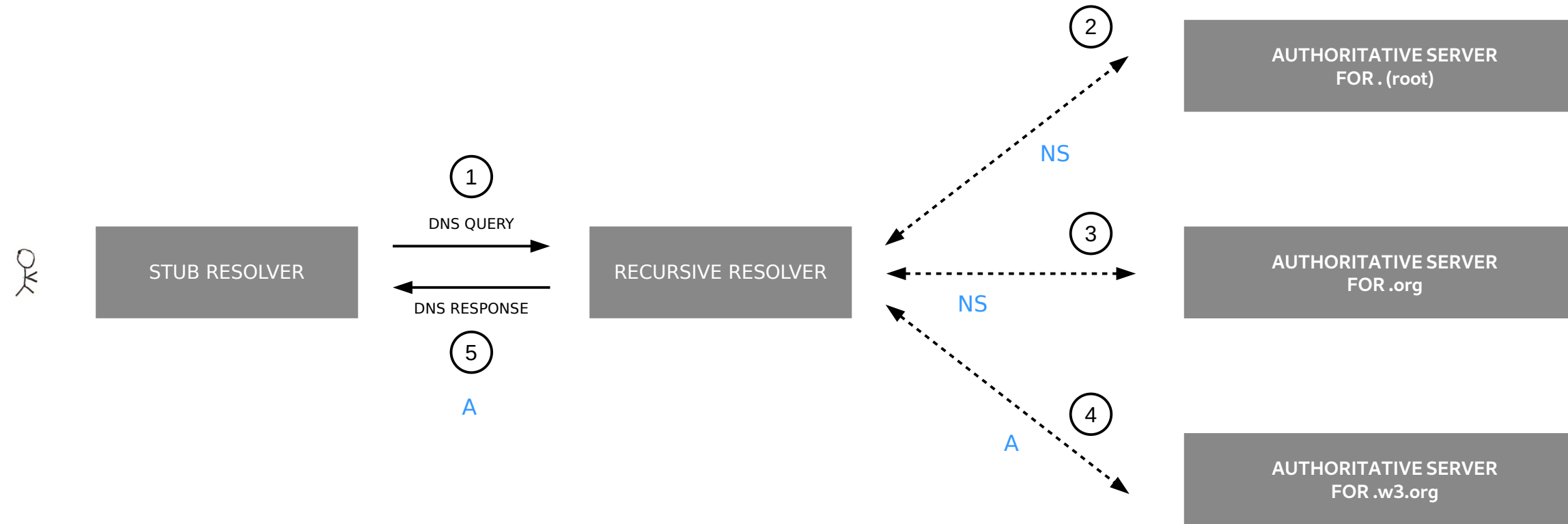
Call info and scribe selection

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**

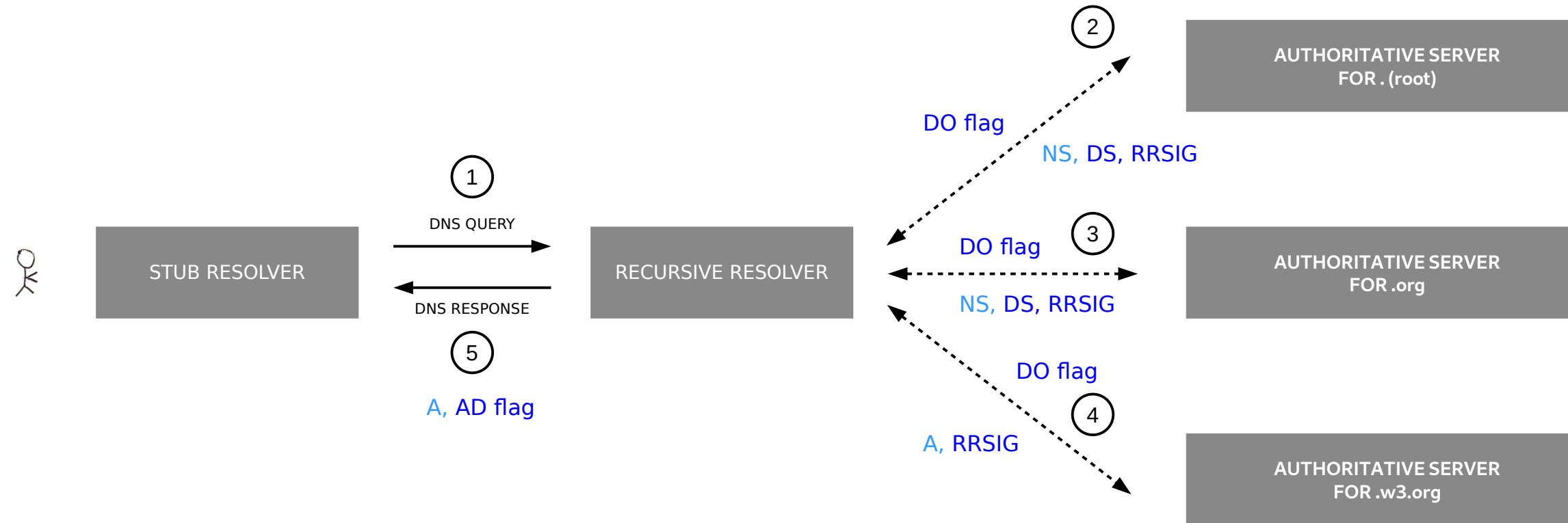
④ → Lookup “**www.w3.org**”

← **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**



- 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)**

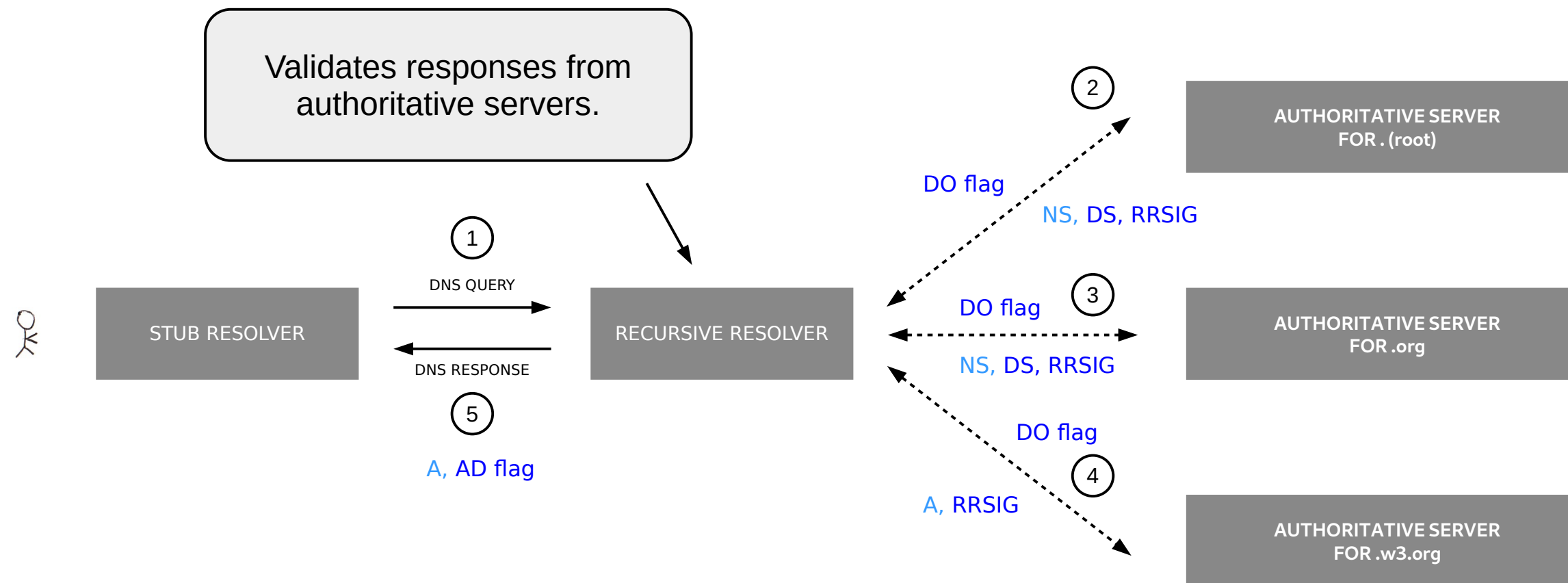
- ③ → Lookup “**www.w3.org**”  
→ Set **DO flag** (“DNSSEC OK”)

- ← **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**”

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)**

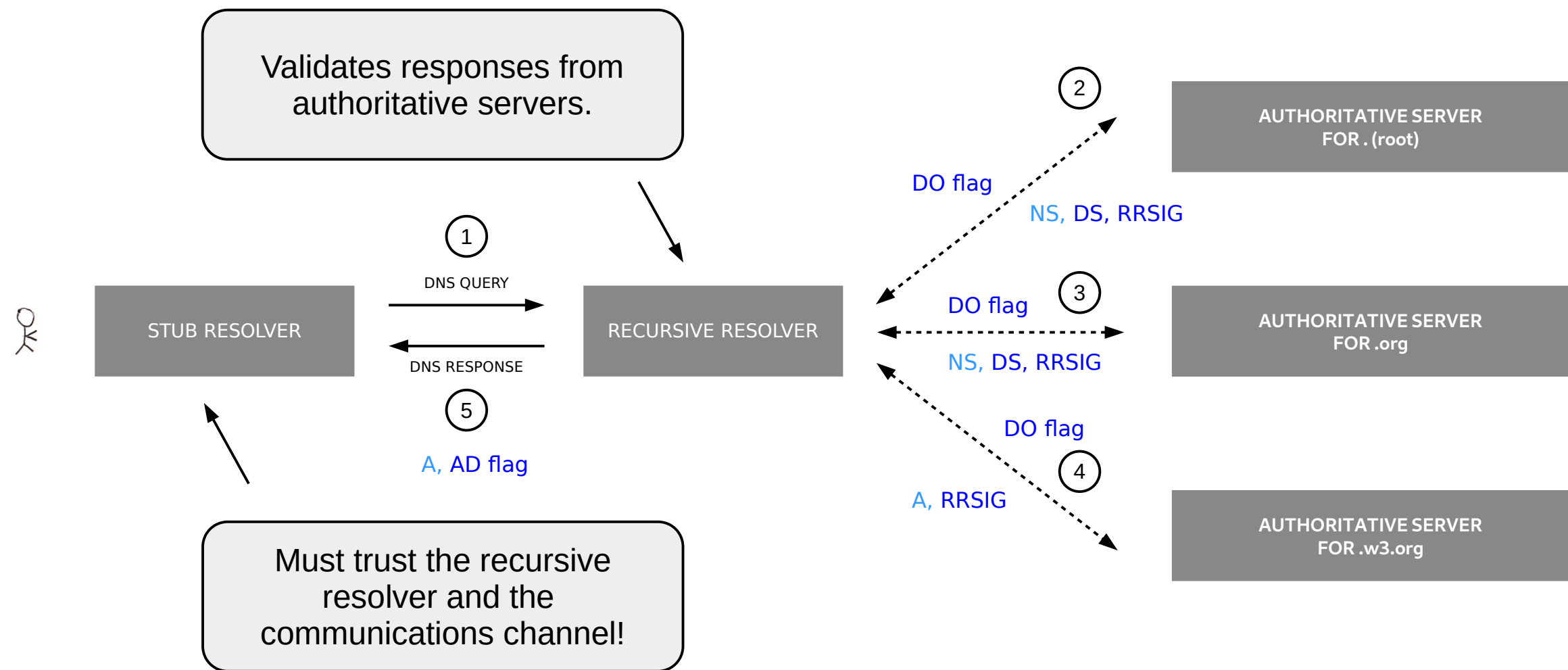
③ → Lookup “**www.w3.org**”  
→ Set **DO flag** (“DNSSEC OK”)

- ← **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**”

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)**

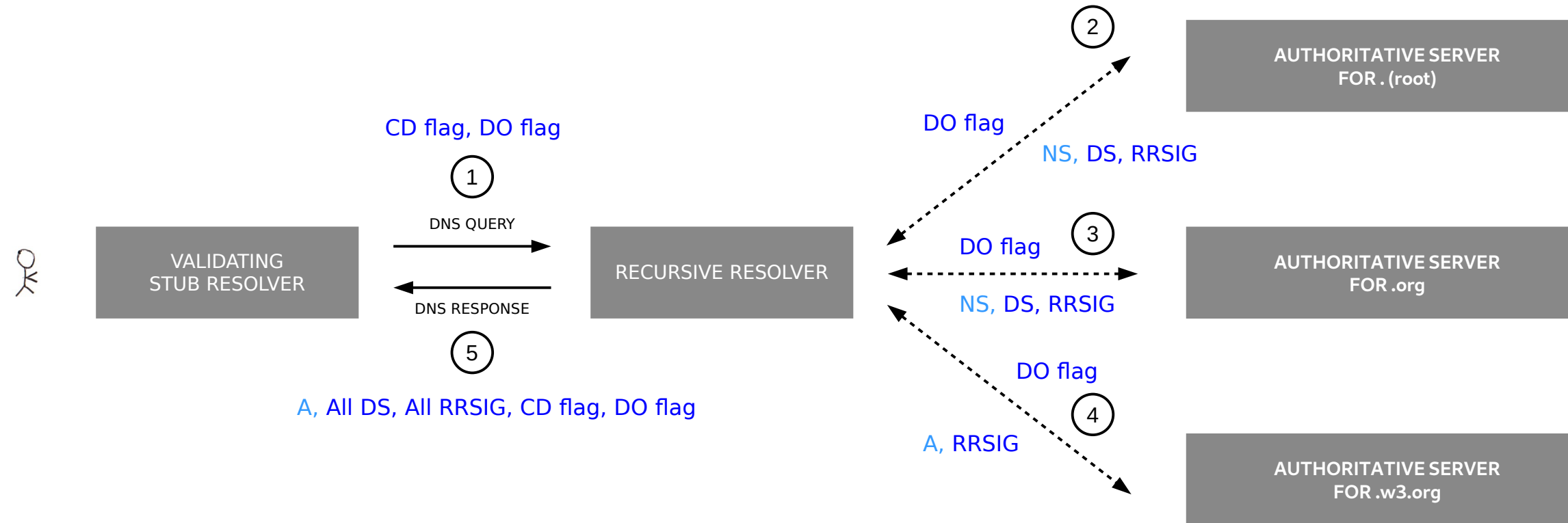
③ → Lookup “**www.w3.org**”  
→ Set **DO flag** (“DNSSEC OK”)

- ← **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)**

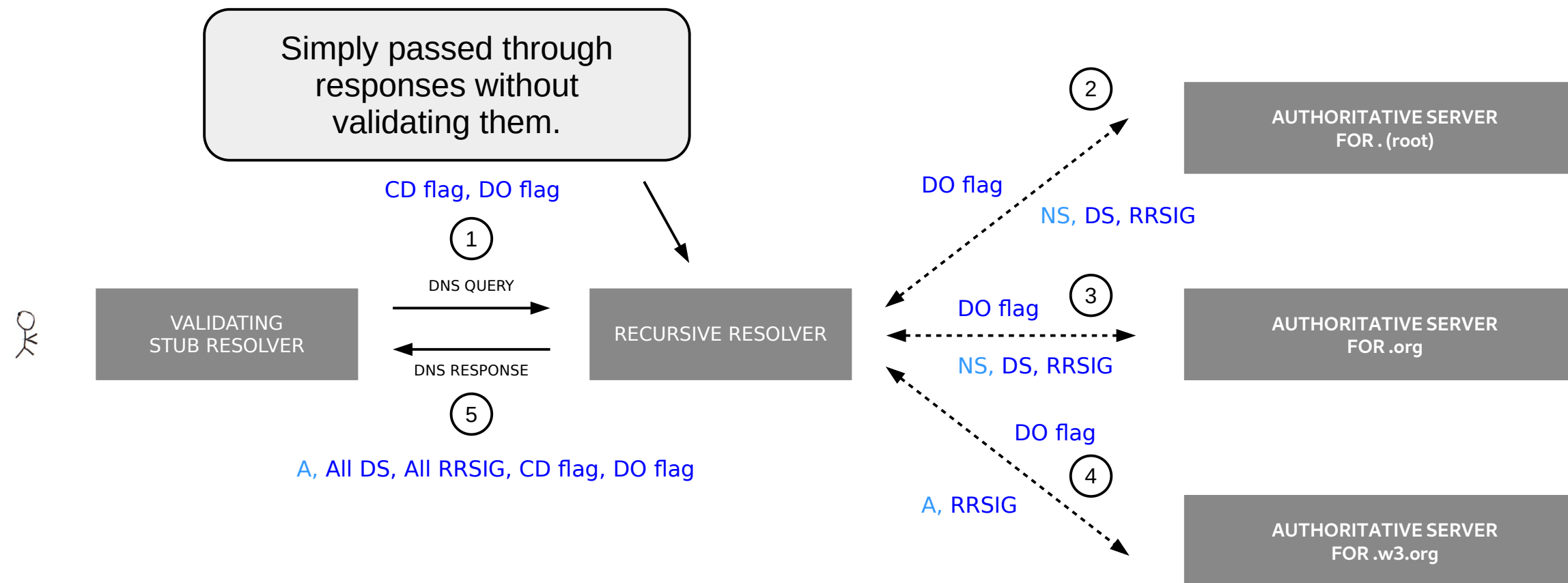
- ③ → Lookup “**www.w3.org**”  
 → Set **DO flag** (“DNSSEC OK”)

- ← **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”)



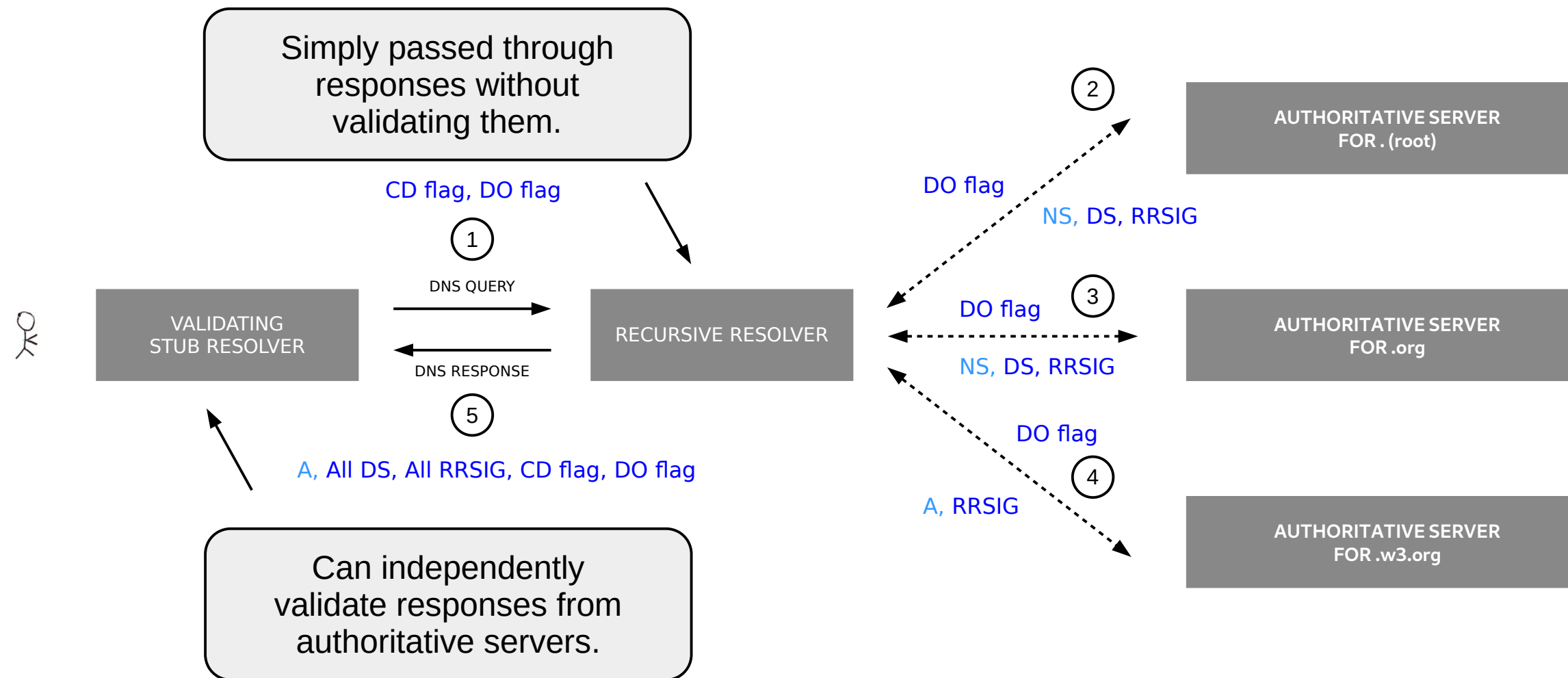
- (1) → Lookup **“www.w3.org”**  
 → Set **CD flag** (“Checking Disabled”)  
 → Set **DO flag** (“DNSSEC OK”)

- (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”)



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

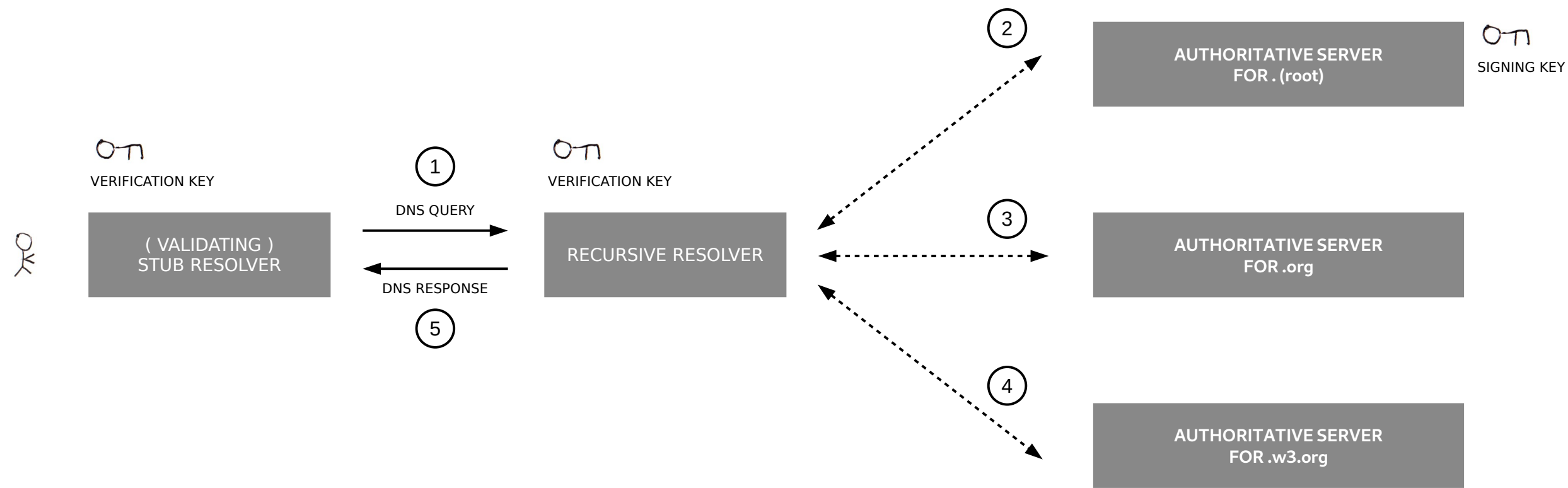
- ② → Lookup **“www.w3.org”**  
 → Set **DO flag** (“DNSSEC OK”)
- ← **NS** – IP(s) of authoritative nameserver for **.org**
  - ← **DS** – Reference to public key for **.org**
  - ← **RRSIG** – Proof, can be validated by public key for **.(root)**

- 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”)



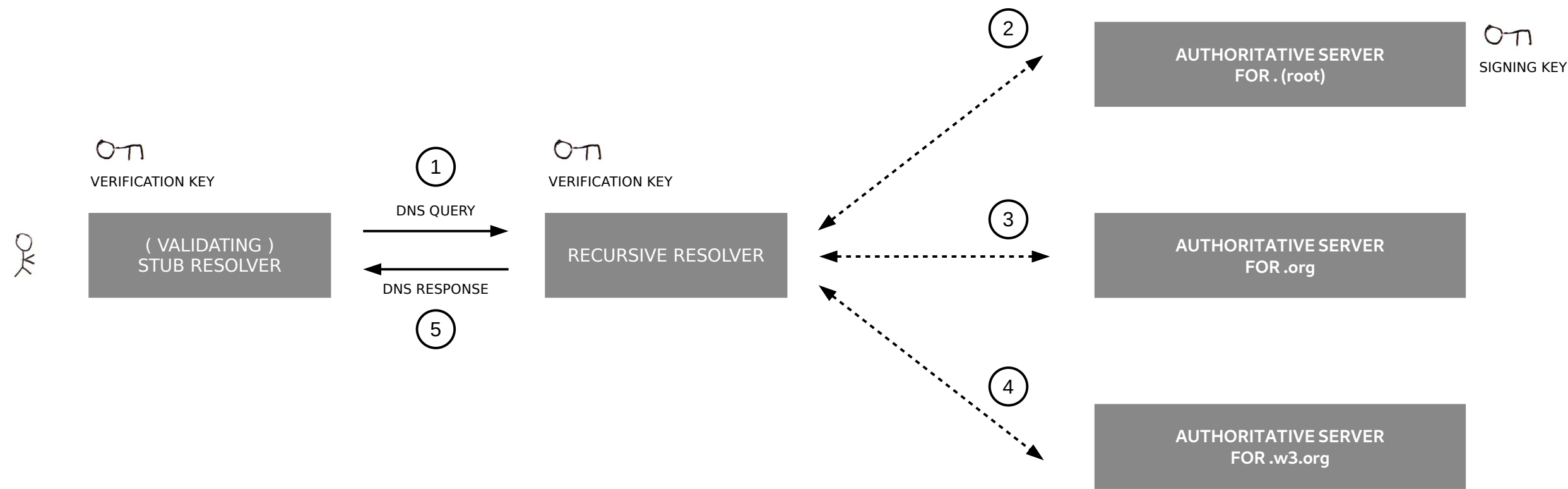


Can the recursive resolver verify the DNS records?

Achieved by DNSSEC

Can the stub resolver verify the DNS records?

Achieved by DNSSEC



Can the recursive resolver verify the DNS records?

Achieved by DNSSEC

Can the stub resolver verify the DNS records?

Achieved by DNSSEC

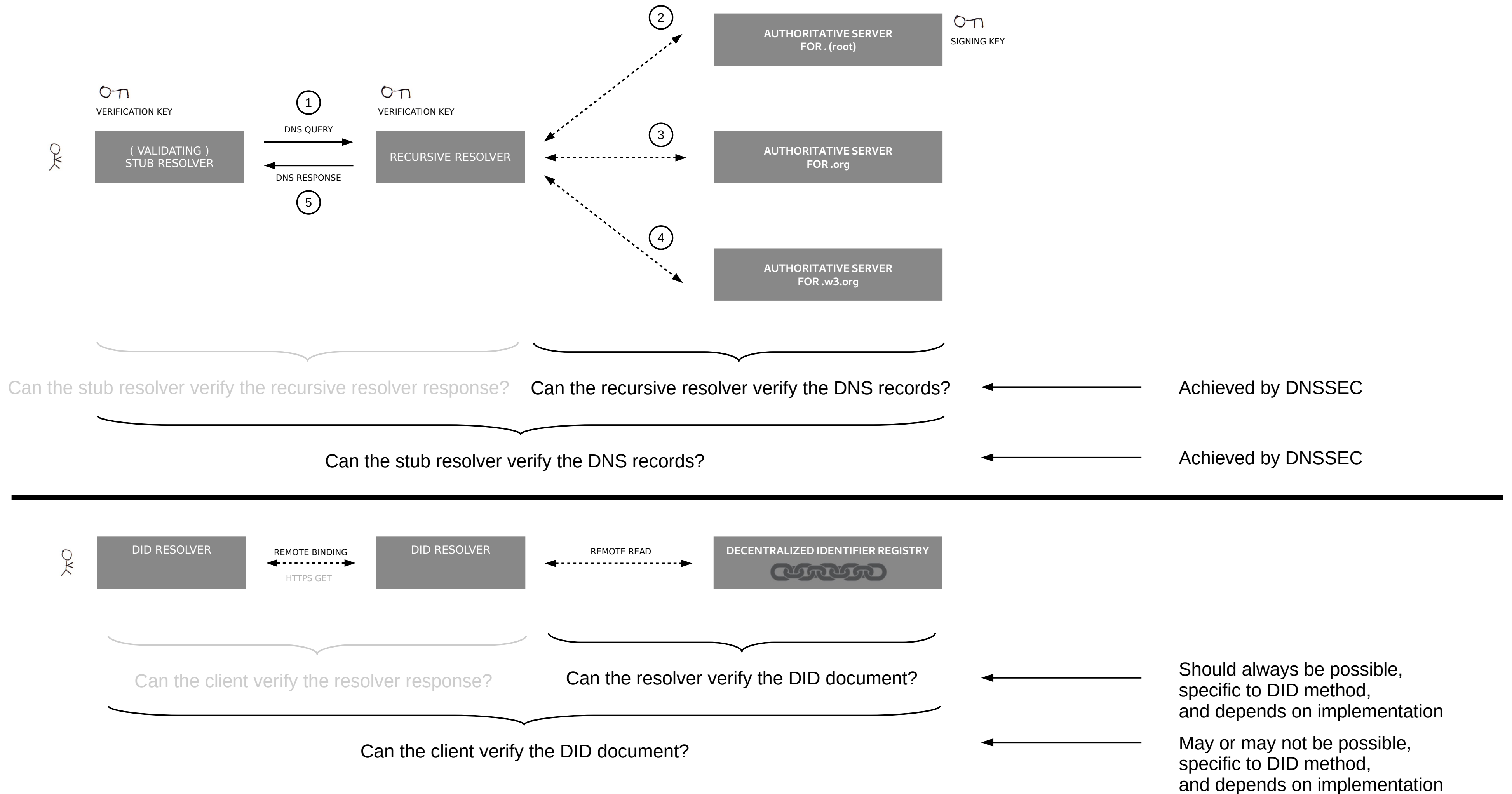


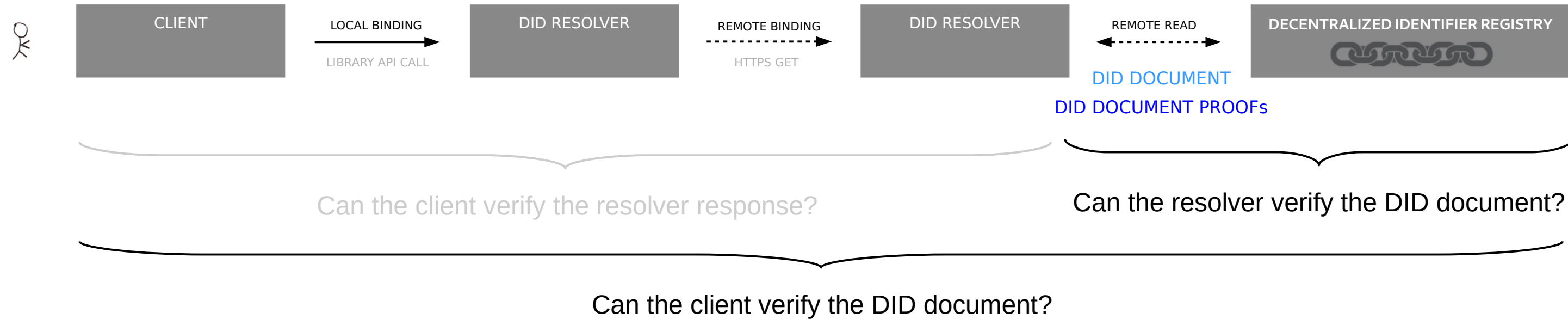
Can the resolver verify the DID document?

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





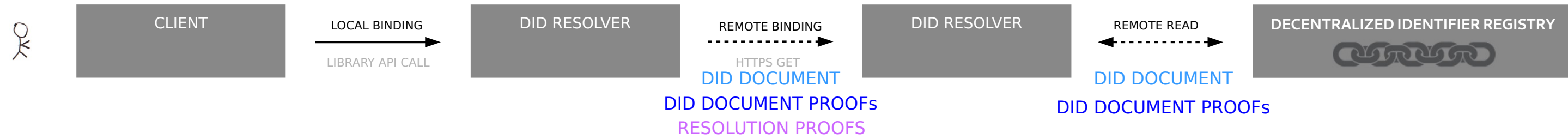
Examples of **DID DOCUMENT PROOFS**:

- 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",
    ...
  }]
}
```



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...gFWF0EjXk"
  }
}
```