DNSSEC
- Session 2

Sara Dickinson
Sinodun IT
sinodun.com

April 2014

DNSSEC- Session 1

- You've already seen…
  - History of DNSSEC
  - Validating a DNSSEC query (resolver perspective)
  - Signing a zone
    - DNSSEC RRs
    - Generating keys & signatures (BIND)

DNSSEC - Session 2

- DNSSEC recap
- Administering a signed zone
  - Signatures
  - Keys
- DNSSEC in practice
  - Queries
  - Deployment
- DNSSEC software overview
  - Validating / Serving / Signing / Others

Why DNSSEC?

You cannot trust the classic DNS response

DNSSEC:
An extension that is placed on top of classic DNS

DNSSEC in a nutshell

authoritative server	resolving/validating server

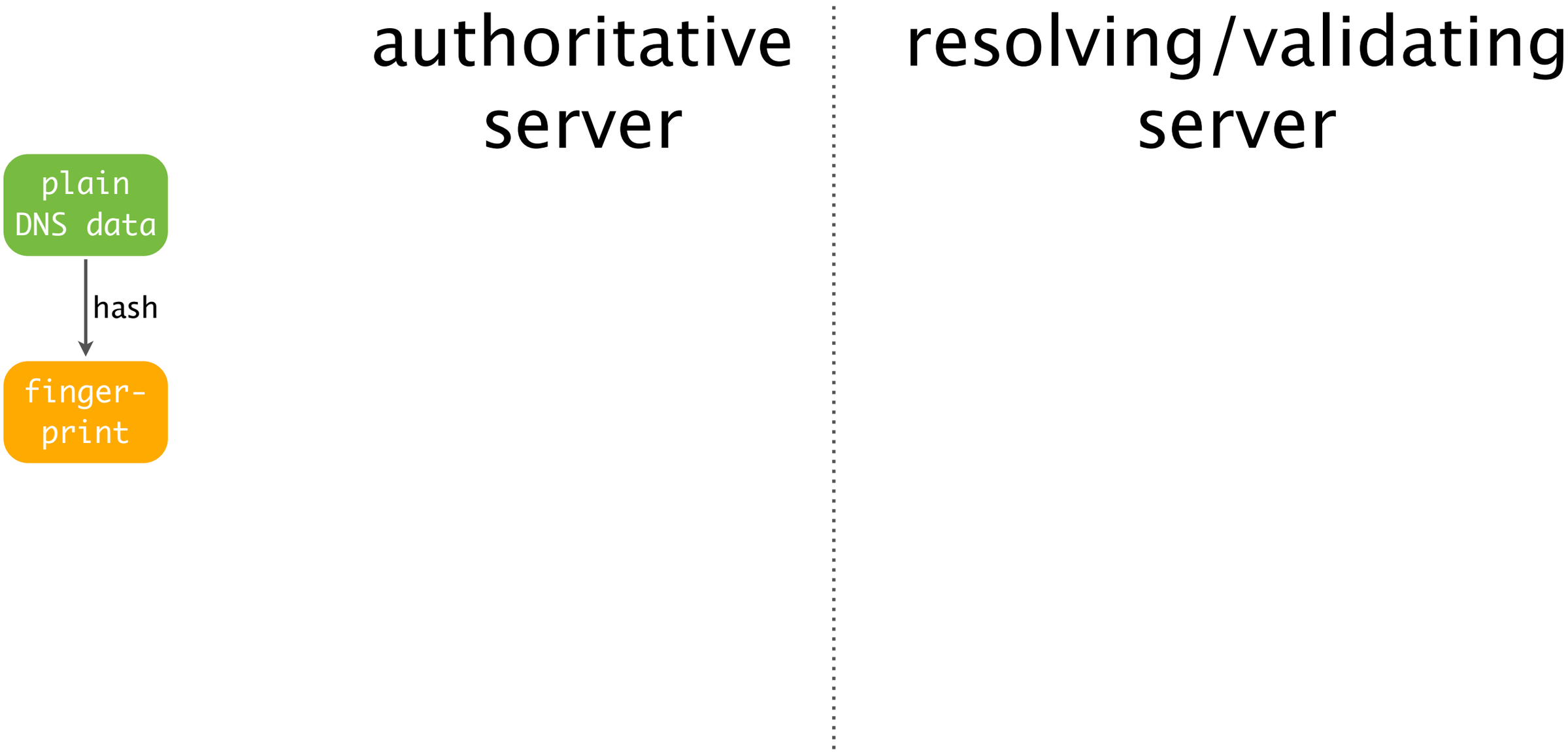
DNSSEC in a nutshell

authoritative server

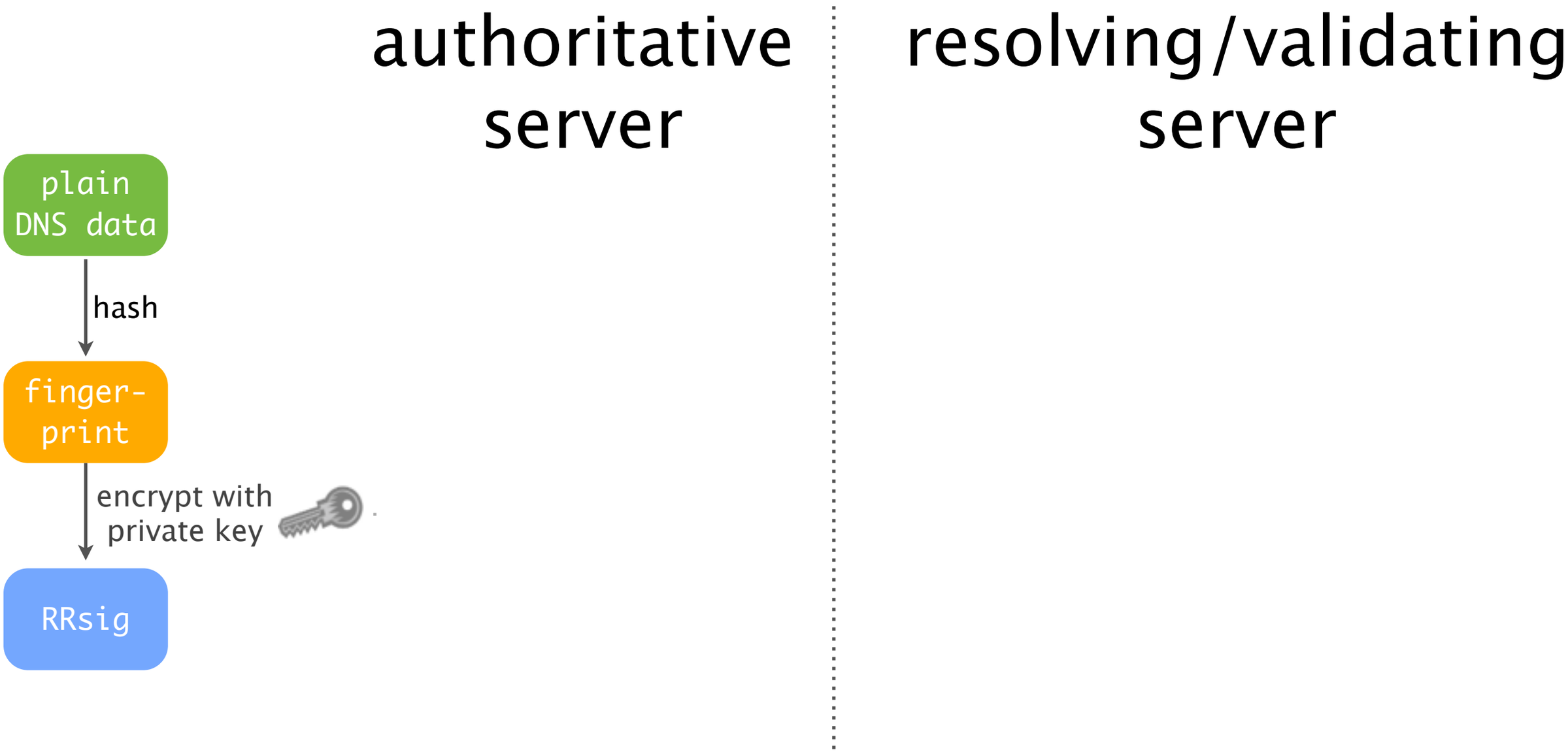
resolving/validating server

plain DNS data

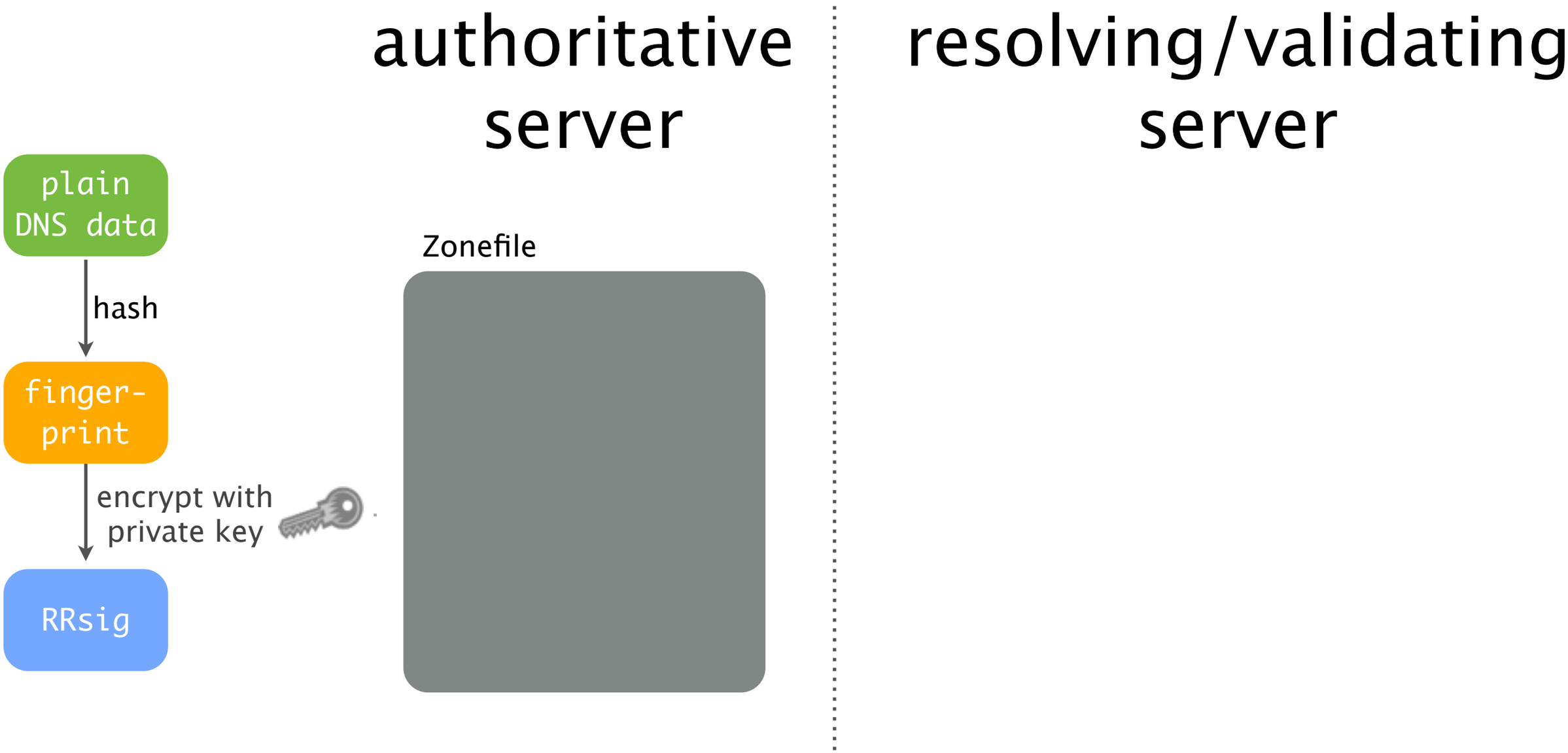
DNSSEC in a nutshell



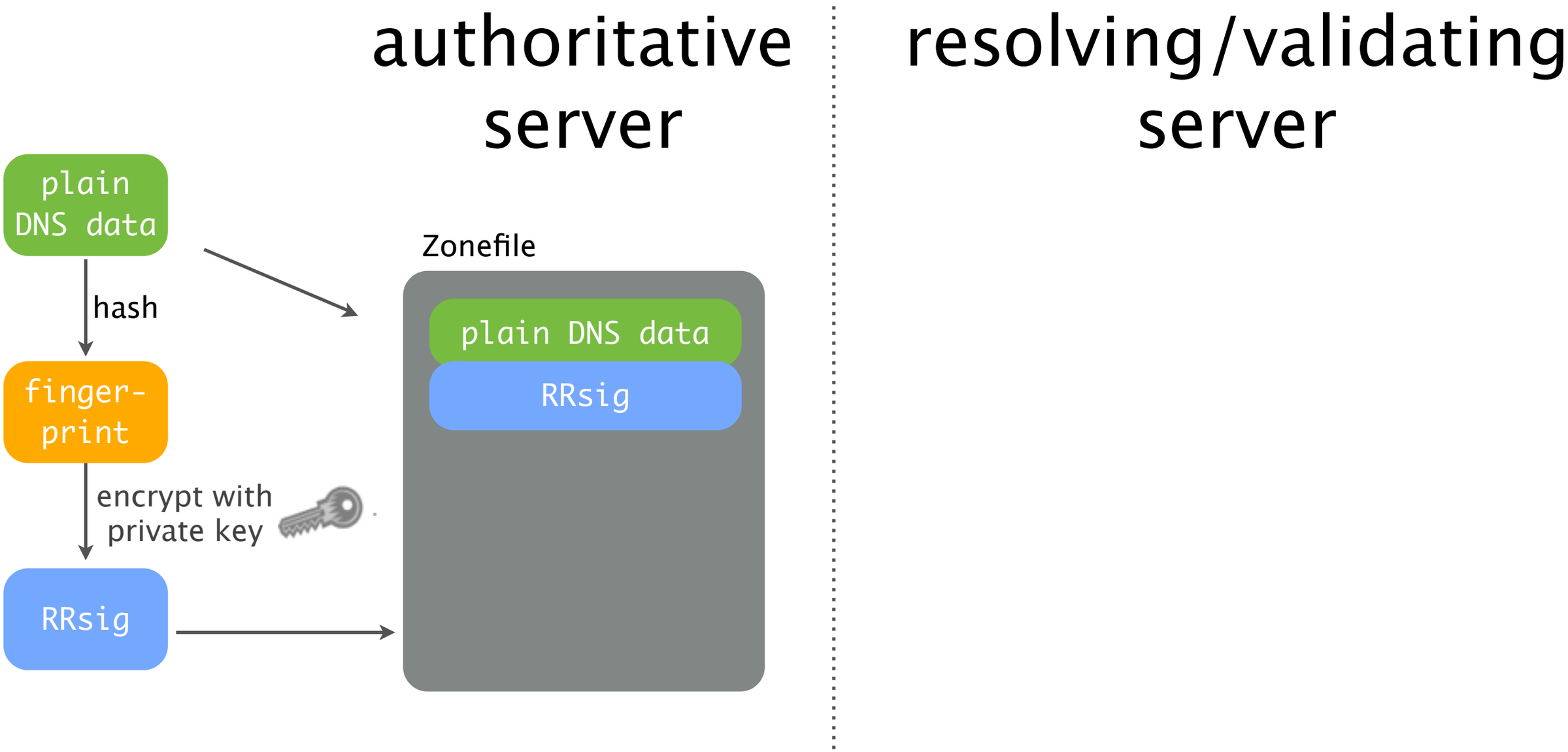
DNSSEC in a nutshell



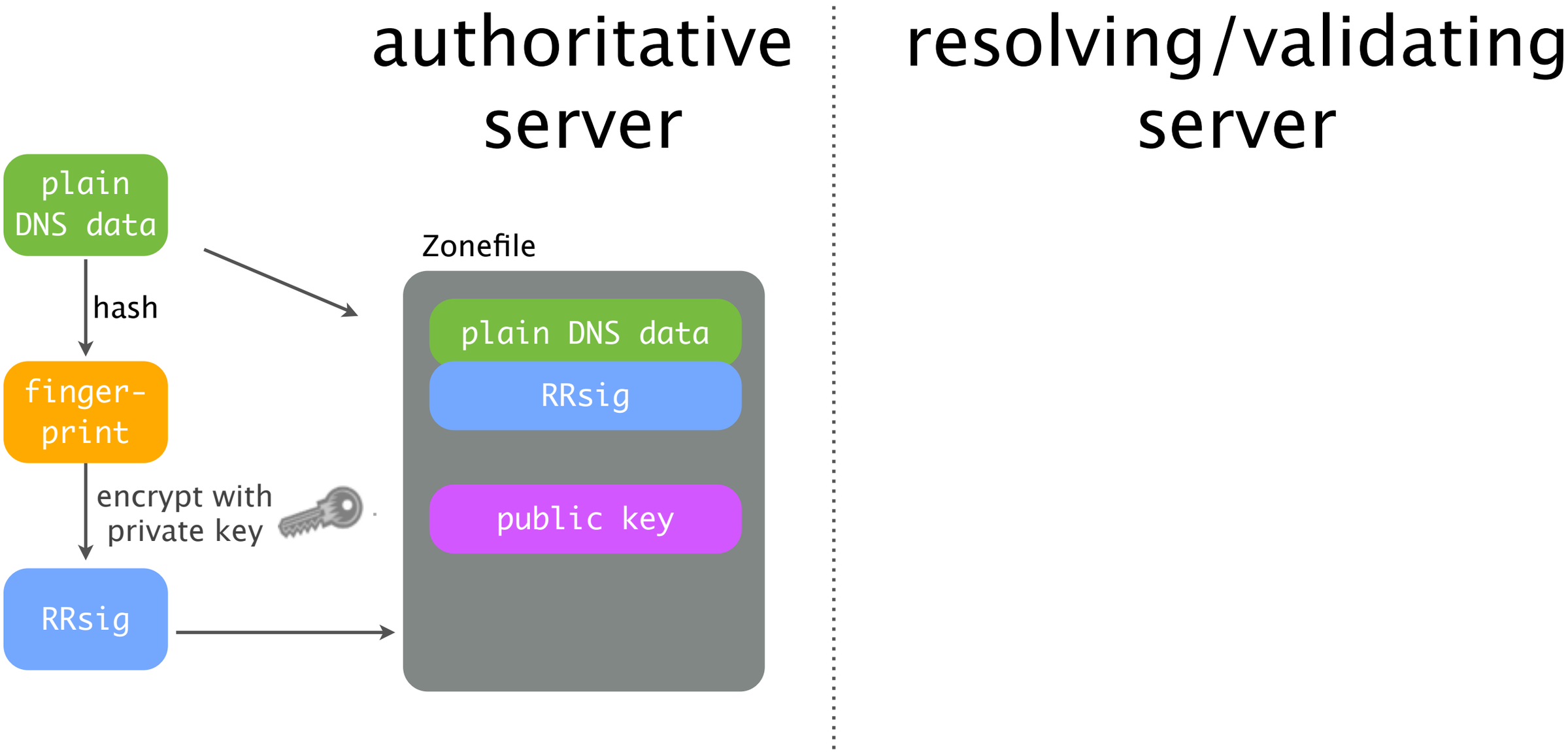
DNSSEC in a nutshell



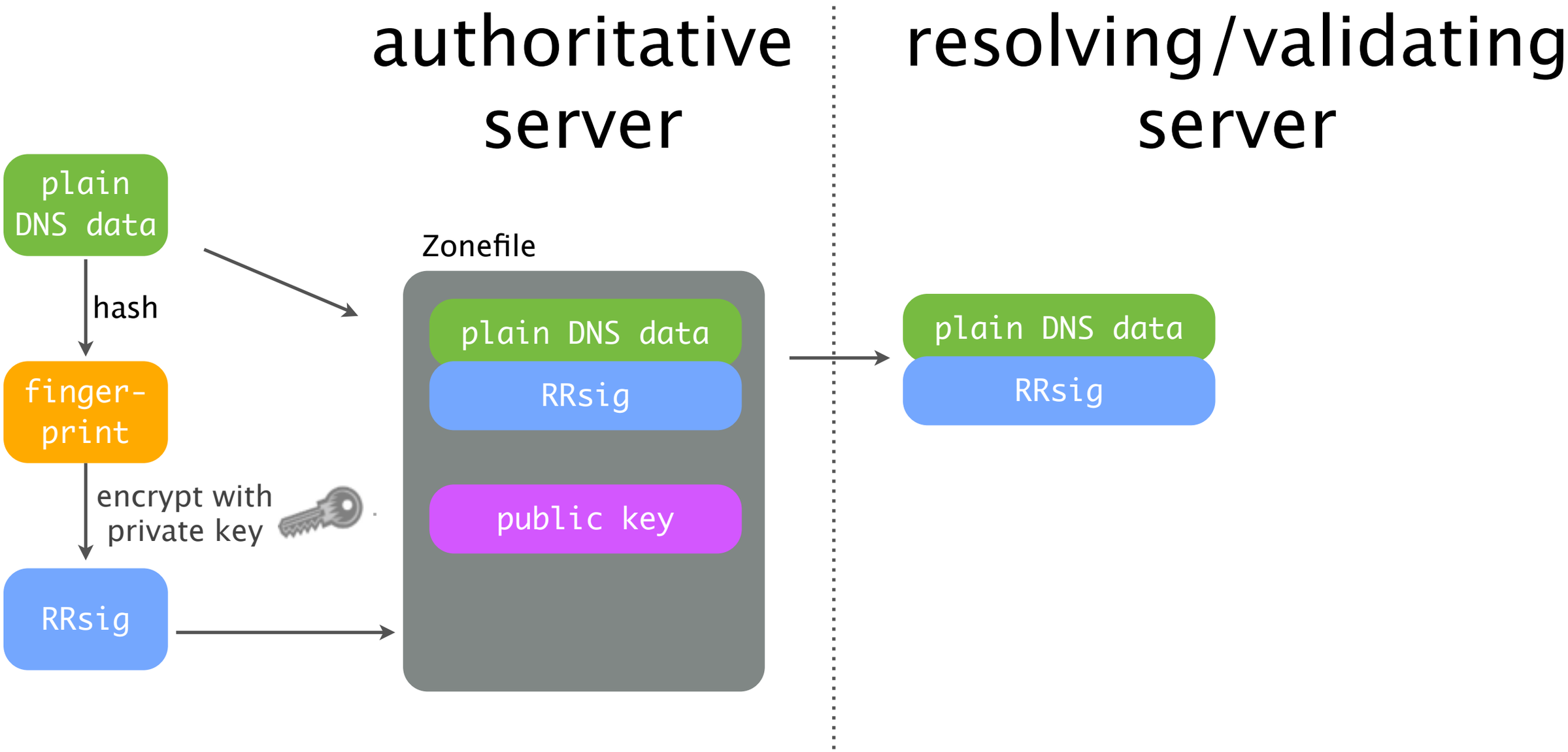
DNSSEC in a nutshell



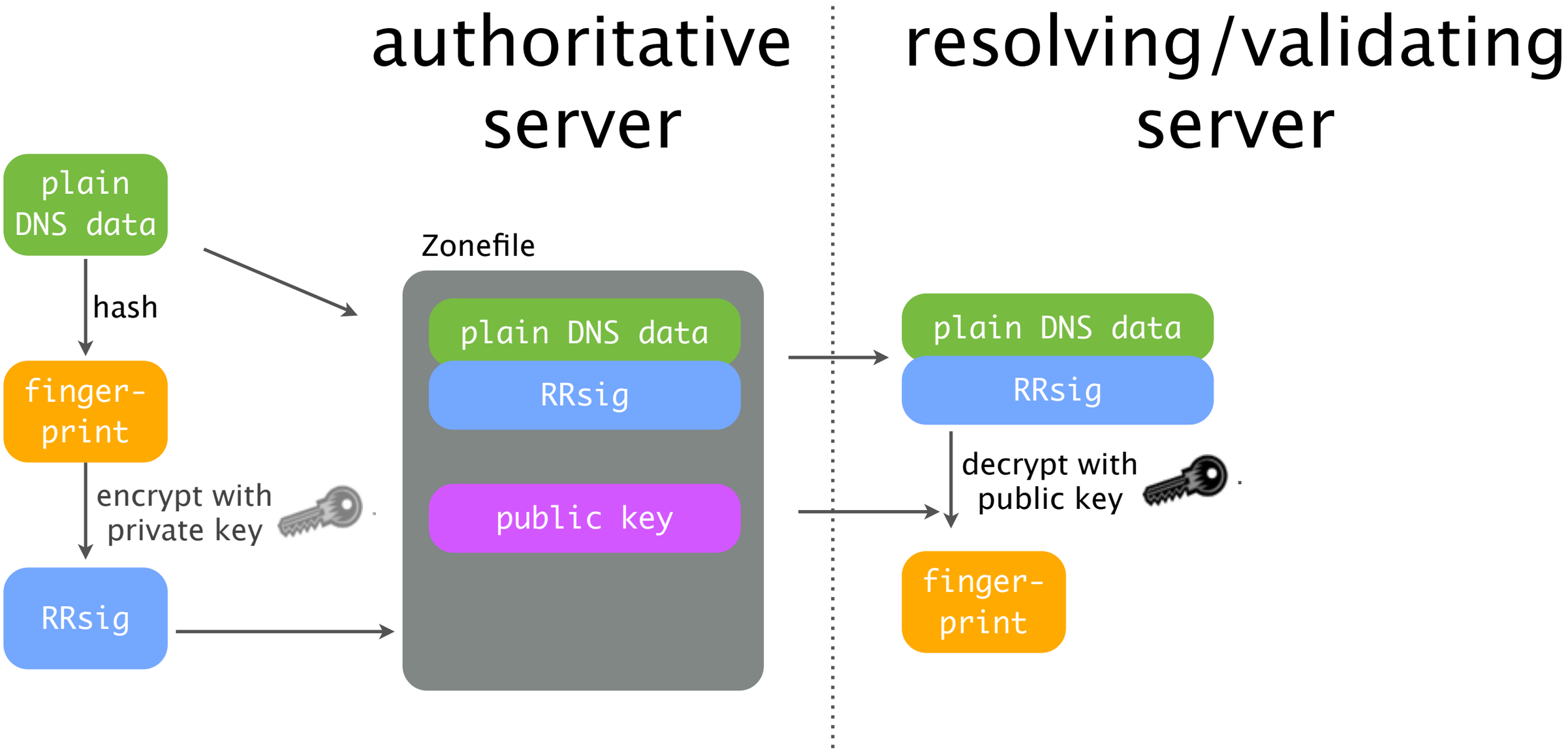
DNSSEC in a nutshell



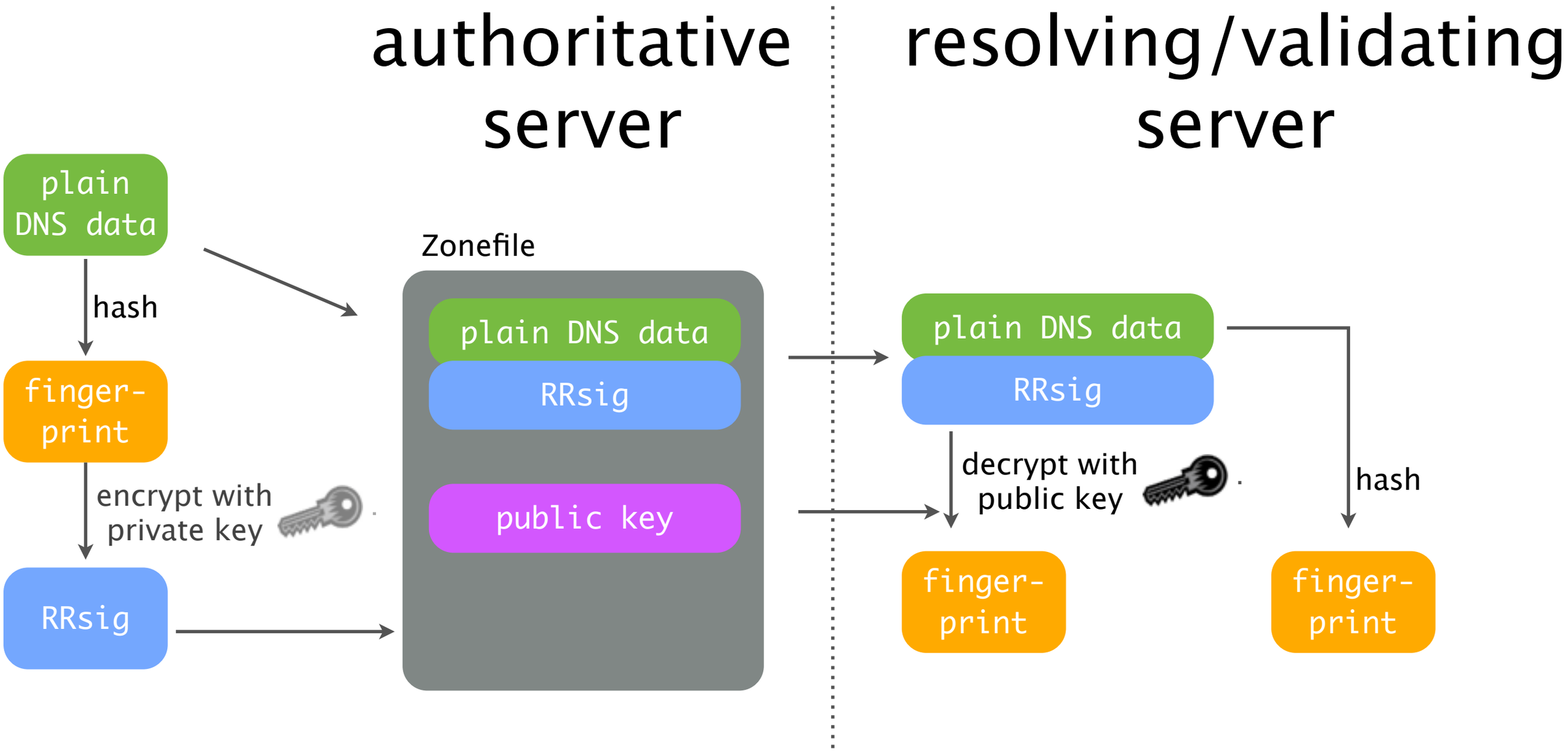
DNSSEC in a nutshell



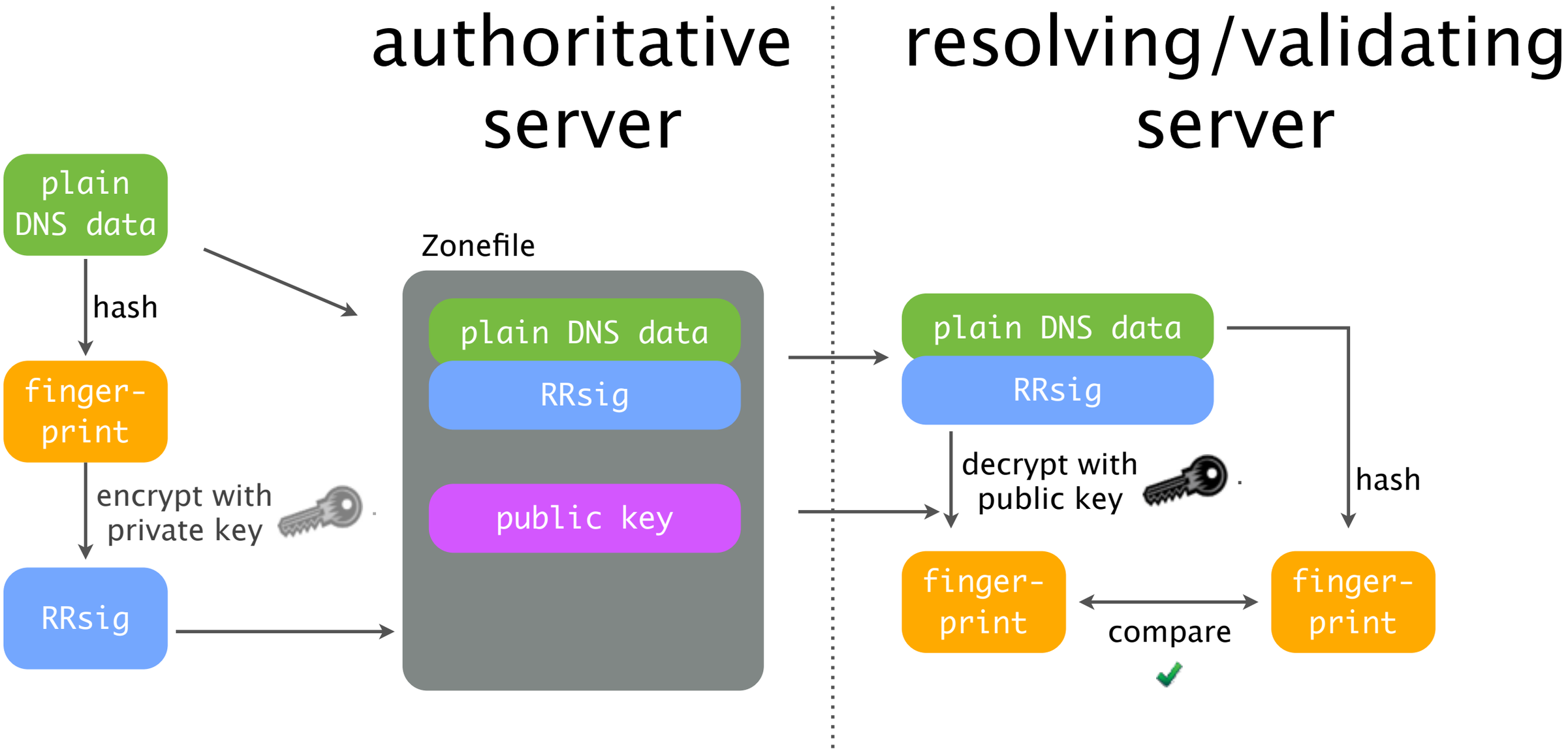
DNSSEC in a nutshell



DNSSEC in a nutshell



DNSSEC in a nutshell



Domain Name System Security Extension

- Chain of trust ensures validity of public keys.
- This allow DNS responses to be validated:
  - **Authentication of Data Origin**
  - **Authentication of Integrity**
  - **Authenticated Denial of Existence**

DNSSEC can be thought of as DNS error detection

Administering a Signed Zone

Zone without DNSSEC

```
$ORIGIN groupX.odslab.se.
$TTL 60
@        SOA nsX.odslab.se. test.odslab.se. (
                    2011062100 ; serial
                    360        ; refresh (6 minutes)
                    360        ; retry (6 minutes)
                    1800       ; expire (30 minutes)
                    60         ; minimum (1 minute)
                  )
@        NS    nsX.odslab.se.
www      CNAME nsX.odslab.se.
```

Zone with DNSSEC

```
groupX.odslab.se.       60 IN SOA nsx.odslab.se. test.odslab.se. (
                                2011062145 ; serial
                                360        ; refresh (6 minutes)
                                360        ; retry (6 minutes)
                                1800       ; expire (30 minutes)
                                60         ; minimum (1 minute)
                                )
groupX.odslab.se.       60 IN RRSIG SOA 8 3 60 20110628103724 (
                                20110628083552 44494 groupx.odslab.se.
                                NJ5lIdcdw3TJlSjTd5W/Gk1CtgZu2VfXAVIF49em/jdm
                                pA1JnejkwPAfb0TjdcXBUH6cQ2XIHobjgEJEpWRM9G/W
                                W7DYJZmdo6o09YrMexTLCZLcq6eyjTpS8TmwmconuNEN
                                FiCkBztqgHlyw0Teg9sw/1E0UVwGKKgd0SOv8Nw= )
groupX.odslab.se.       60 IN NS nsx.odslab.se.
groupX.odslab.se.       60 IN RRSIG NS 8 3 60 20110628103609 (
                                20110628083552 44494 groupx.odslab.se.
                                K3Yxcz25nv0m8SZDHkh0YXPBrZ0+78hVsT7FD4A9GZ9m
                                3sHpkpfzjZ/Bee+lgwZZGIJKmMfyRtQQon7oCa2Z9xe9
                                L/D9KQzPzZbZCMrOxG/usSZ+LhwYuN3b0Kl2BIhklji5
                                fBN6aEsyhw+hiV9ibobzqKe5bMnxaa9IfMscV1c= )
groupX.odslab.se.       120 IN DNSKEY 256 3 8 (
                                AwEAAasv0uyeTp5kIaw/fwPyQncY06YMn370lczC5SCx
                                veUNQXLhihm+tV/lTvkWd5GHg/ebjTPSR6mqB/jTu7CH
                                /iNhprxdnh3lVW7FjFpC5tDfFiHyDM97q8A+4lnBmiB4
                                SZJR1qOGmeoiU2BP2uyTlv31KJPDm08GwmPTTX8fi3LV
                                ) ; key id = 44494
groupX.odslab.se.       120 IN DNSKEY 257 3 8 (
                                AwEAAc6Wk/UqaEMaytXWL2y25I0Z8Uuubnkrufa JEEBw
                                niObHaNGMscp5I5207ScB6L70DJS46S9bA4k8mbcRNPA
                                Vi0OQVz1kFTTNt45XzYQ7yaQJyobQdFtVq8TXtaFPiFP
                                S7nz7ga8/HVW8VNRp4H5iajsgh4LCX+399tJX+rk613R
                                tbnHVvZPOUiuZNFqZLOkbzGtNRbl4UvoRQi5q+tjV/ow
                                cUkn8tljQGPpTe/HLImUT+MrftnY6m8jvgO+qhd2o/1Z
                                6XZcVBuDB+UGrhFcU72HmeKfQHMtCuGZhmWOcOymPcDJ
                                12ONkBqgj28Cu/4Kr44DMTu4q2ax07dDOfSyKqM=
                                ) ; key id = 62246
groupX.odslab.se.       120 IN RRSIG DNSKEY 8 3 120 20110628103715 (
                                20110628083552 62246 groupx.odslab.se.
                                Tw32FOW95e86g0FYxyXu3nDQNTdAELxVhg4BVoRA2RWx
                                iAgkZk/XQRUfozjd/qNNjrIA2+a9wwrvLWokRB6xzSTR
                                bwx199Mu8Xj9p9Q8CbzCvbvHPtRqPgf6Mto9jjlUaSK4
                                NlNQWg/qfsLvkvxRpdE4g9Xac3b71TPuylQSovvARR0v
                                4rJ4zmBdomdQHjtwOuQ4GeVfpgKqFCqa8HFK8D20Kmjk
                                56a7rbe6UWt5hHMjQfys3NfvulFAdCTW0Rbikss7YQMw
                                j6msmsRS8Zj+IlBbmku6RwxVxNF/ca09fuz4NhyOOSRP
                                2mBTBIwk+XcybA6vK5ofnrBTCSSoJOt4+g== )
```

```
groupX.odslab.se.       60 IN NSEC3PARAM 1 0 5 3A5BF749D1330DE3
groupX.odslab.se.       60 IN RRSIG NSEC3PARAM 8 3 60 20110628103502 (
                                20110628083552 44494 groupx.odslab.se.
                                Gvy1AOrm6dENvVUke1Ck3KmjB5W1mbvIsFdvm2p2MfZa
                                msgUJNJ0sT6R3jIyRIvc+6T3jADDHGpvr6ILLnWySFRb
                                9efAn/SDt060N3YsU6emv5iAh/TRbo7g8UNtokm1TAds
                                5rZ187cOo3yqQ05qBSTVo8wCcF1HS6+htEt+vQs= )
www.groupX.odslab.se.   60 IN CNAME nsx.odslab.se.
www.groupX.odslab.se.   60 IN RRSIG CNAME 8 4 60 20110628103414 (
                                20110628083552 44494 groupx.odslab.se.
                                BAs7KPVdwoPeC9isn/N00dV2OB62sSjbQS65r6h8EOGF
                                ToRqd6wRpd8OhNSNrJNn7ycH61m2j71WhE00fsMLA1T6
                                vxGKVcK6IeH+7Vpu4bgnH93jq8f3TftaiR22bYNl+Y9Q
                                Y7PHNFcmZ0PmoqVmilmtJdpn+YNjUJ5a+Riwojo= )
7oreb1sb9elhfqfp53bqqde6bcdm5eo3.groupx.odslab.se. 60 IN NSEC3 1 0 5
3A5BF749D1330DE3 OTANAROMKJB00QC2G6K2IT2GU2SB4DOA CNAME RRSIG
7oreb1sb9elhfqfp53bqqde6bcdm5eo3.groupx.odslab.se. 60 IN RRSIG NSEC3 8 4 60
20110628103552 (
                                20110628083552 44494 groupx.odslab.se.
                                azU2yBsLQNXANwyTxosI4hwf6JPfV5XKNdPtQzGprShE
                                w6N/sDG9QzMJjlQrPW82rY2SYl7xGJMBGdfsGVBZJJQ4
                                nXBmwnjT5Grm9k/a0hyCmYYAHzoq4ixV5fLDYrH8af/u
                                uvoFs90vJlN4OMbHNJUrNSsCsJRzps/k0/aH+0w= )
otanaromkjb00qc2g6k2it2gu2sb4doa.groupx.odslab.se. 60 IN NSEC3 1 0 5
3A5BF749D1330DE3 7OREB1SB9ELHFQFP53BQQDE6BCDM5EO3 NS SOA RRSIG DNSKEY NSEC3PARAM
otanaromkjb00qc2g6k2it2gu2sb4doa.groupx.odslab.se. 60 IN RRSIG NSEC3 8 4 60
20110628103526 (
                                20110628083552 44494 groupx.odslab.se.
                                QLlN/6CjlkU609P9/AntqRFHWAKJ8PUIS53HOZfN9D6P
                                PZEr/7dd+jlv2sgXmIYx/0VXySr4Bafgm8+k0fwEU+JY
                                TjmfkLUOD6O9DOQ/RqNtLp5HFH6TLMZxO7VdFr9vEZq1
                                5UIUQjIFT2+aQR3Dd/QMq26ysHGqOApSH/wkq6Y= )
```

Administering a signed zone:

Signatures

DNSSEC and time

- DNS - only changes are to your zone contents
- DNSSEC - introduces time as a factor due to the use of digital signatures and keys……..
- In DNSSEC time is absolute not relative

Signatures

- With DNSSEC, all authoritative resources records are signed.
- Signatures are valid for a limited (absolute) time
  - Inception = Not Valid Before
  - Expiration = Not Valid After
- **Signature refresh period.**
  - If a signature expires, validation fails!
- Signature validation depends on **correct time**. Use NTP.

SOA Expire

- Always have valid signatures in your zone.
- The zone should expire by itself before the signatures expire (and the zone goes bogus).
- **Recommendation**
  - SOA Expire < Signature Refresh Period

Administering a signed zone:

Keys

Keys

- All signed zones have keys.
  - Key Signing Key (KSK) – Signs *only* other keys
  - Zone Signing Key (ZSK) – Signs all other records
- KSK vs ZSK is a pure administrative distinction
  - Can have a Combined Signing Key (CSK)
- One key set (ZSK/KSK) per signature algorithm

Signature Algorithms

Asymmetric algorithm

Hash algorithm

	RSA	DSA	ECC
MD5	RSAMD5		
SHA1	RSASHA1	DSA	
SHA256	RSASHA256		ECDASHA256
SHA384			ECDSASHA384
SHA512	RSASHA512		
GOST			ECC-GOST

Key Algorithm & Length

- RSA/SHA1 is mandatory but becoming weaker
- RSA/SHA256 used by the root
- ECC is not yet widely deployed
- **Recommendation:** RSA/SHA-256
  - 2048-bit KSK
  - 1024-bit ZSK

Best algorithm/length…
Discuss!

Key Lifetimes

This key is expired!
No, it is just pining for the fjords…

- Keys have no concept of a lifetime
  - However they can be replaced (key rollover)
  - Existing keys retired, new keys introduced
- The rollover process must follow a set of rules:
  - Keys have a lifecycle (PUBLISHED/READY/ACTIVE/RETIRED)
  - Light bedtime reading: Key timing draft
    - http://tools.ietf.org/html/draft-ietf-dnsop-dnssec-key-timing-03

Key Rollovers

- Why roll a key?
  - Algorithms changed
  - Compromised (Lost, hacked, cracked*)
  - Operational best practice

Bigger problems….

	KSK	ZSK
DS	Must interact with parent!	-
When	• Every 12 months • Hardware replacement • Only when you ‘need’ to	• Every month
Root	When needed or 5 years	Every 3 months

HSMs

- Hardware Security Module
  - Physical device for storing and managing keys
  - Will generate keys and signatures
  - (FIPS 140-2) Varying levels of security, performance and cost
  - PKCS#11 interface
  - Advice on HSMs: https://wiki.opendnssec.org/display/DOCREF/HSM

Administering a Signed Zone: General

Common Errors/Problems

- Signatures
  - Expired (or are not yet valid) or no signatures
- DS records. Interaction with parent.
  - Bogus DS record
  - The DS record refers to a non-existing key
- Transfers of domains between registrars
  - When the registrar does not support DNSSEC, or outgoing registrar uncooperative. Check your contract if they sign your zone!

DPS

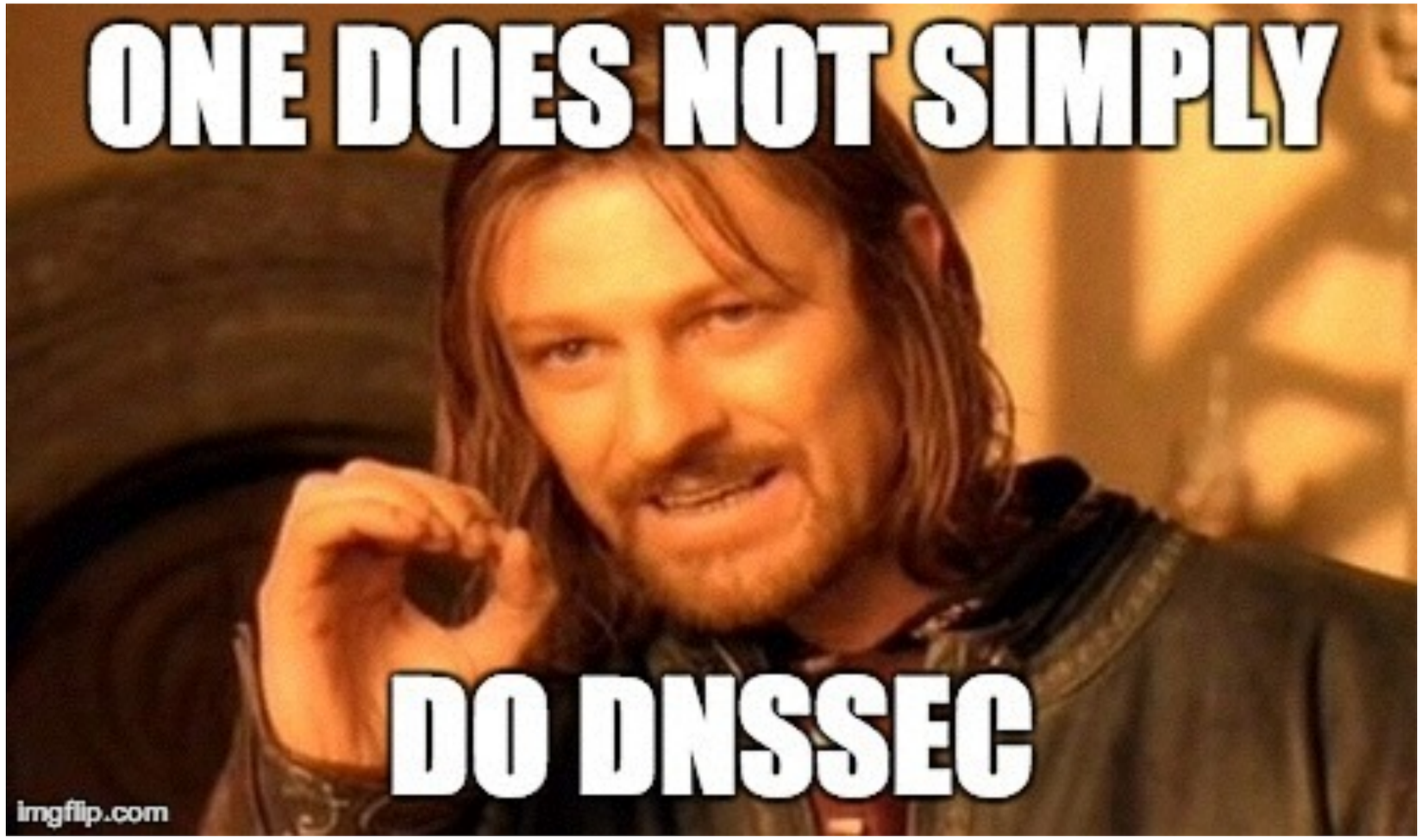
DNSSEC Policy & Practice Statement

- A framework for describing your DNSSEC Policy and operations
  - Useful for relying parties when trusting your zone
  - Also a good check list when deploying DNSSEC
- RFC 6841 – http://tools.ietf.org/html/rfc6841

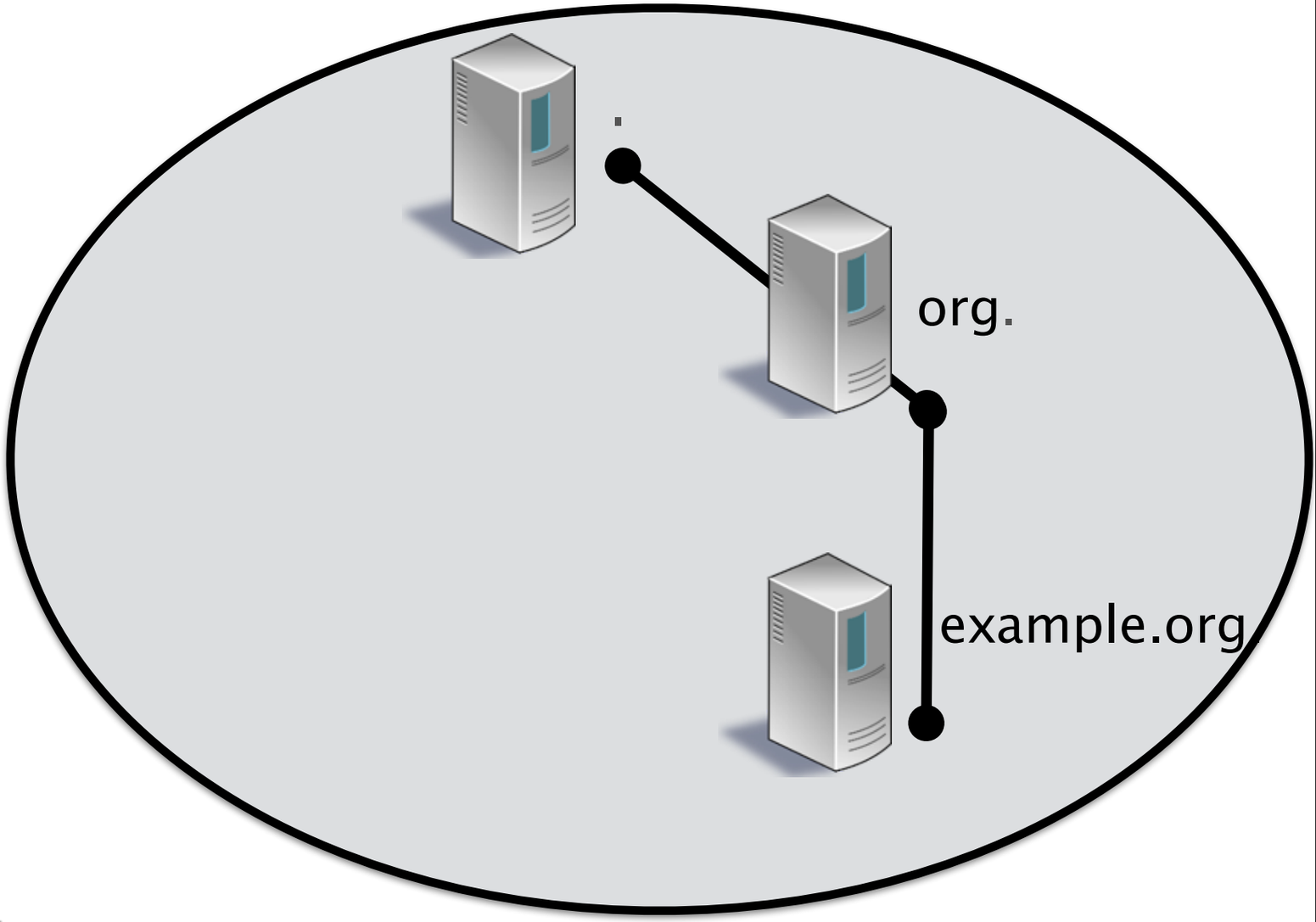
Disaster Recovery Plan

- Time in DNSSEC is absolute – not relative (act quickly).
  - Backup (key repositories and state info)
  - Sane policy (availability vs integrity)
    - Short lifetime on signatures are good but…Can you fix the problem before the signatures expires?
- Worst case is going bogus. Better is to go securely unsigned:
  - Remove DS before signatures expire. TTL + propagation delay.

DNSSEC in Practice

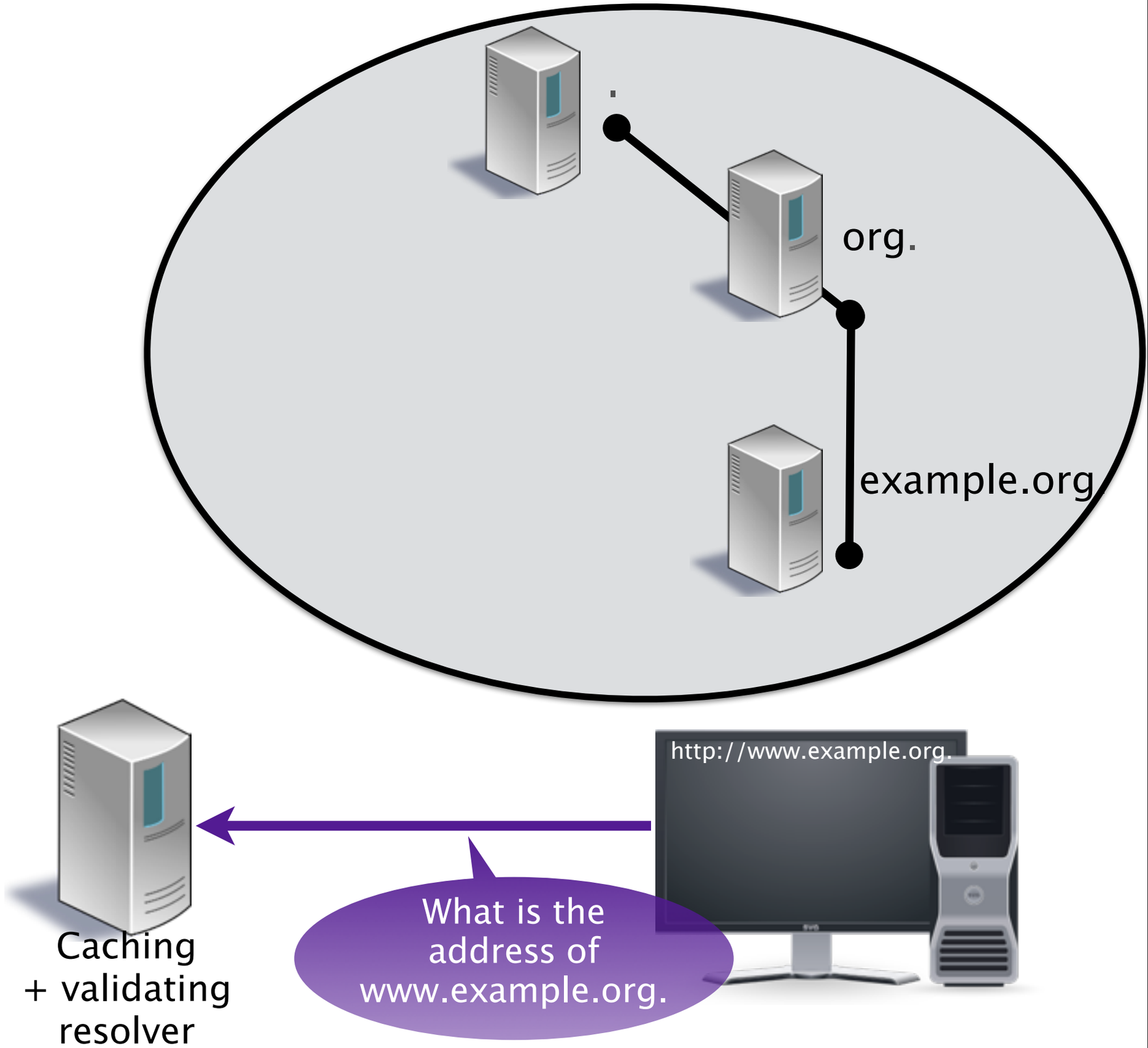


End-to-end DNSSEC

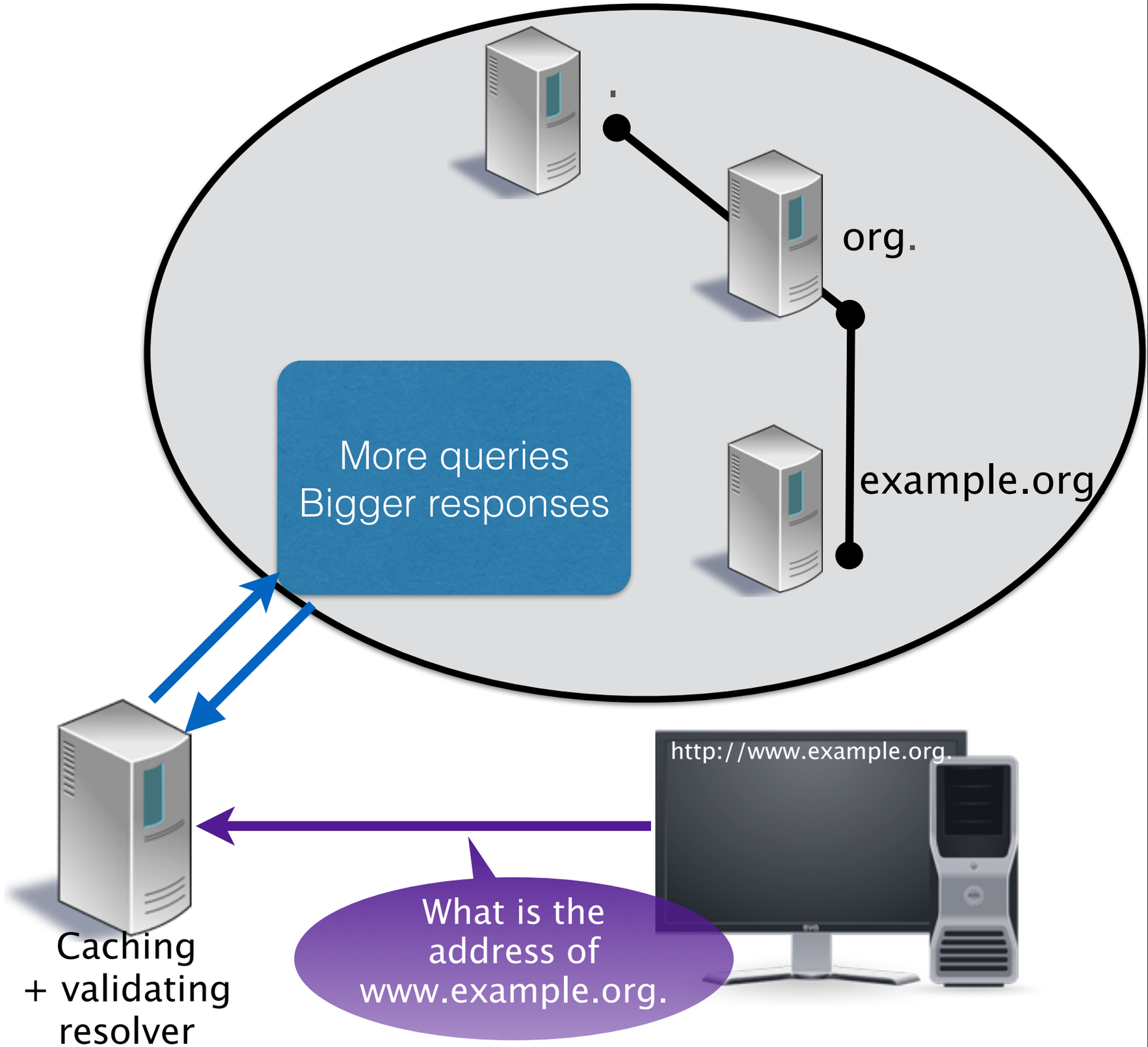


Caching
+ validating
resolver

End-to-end DNSSEC

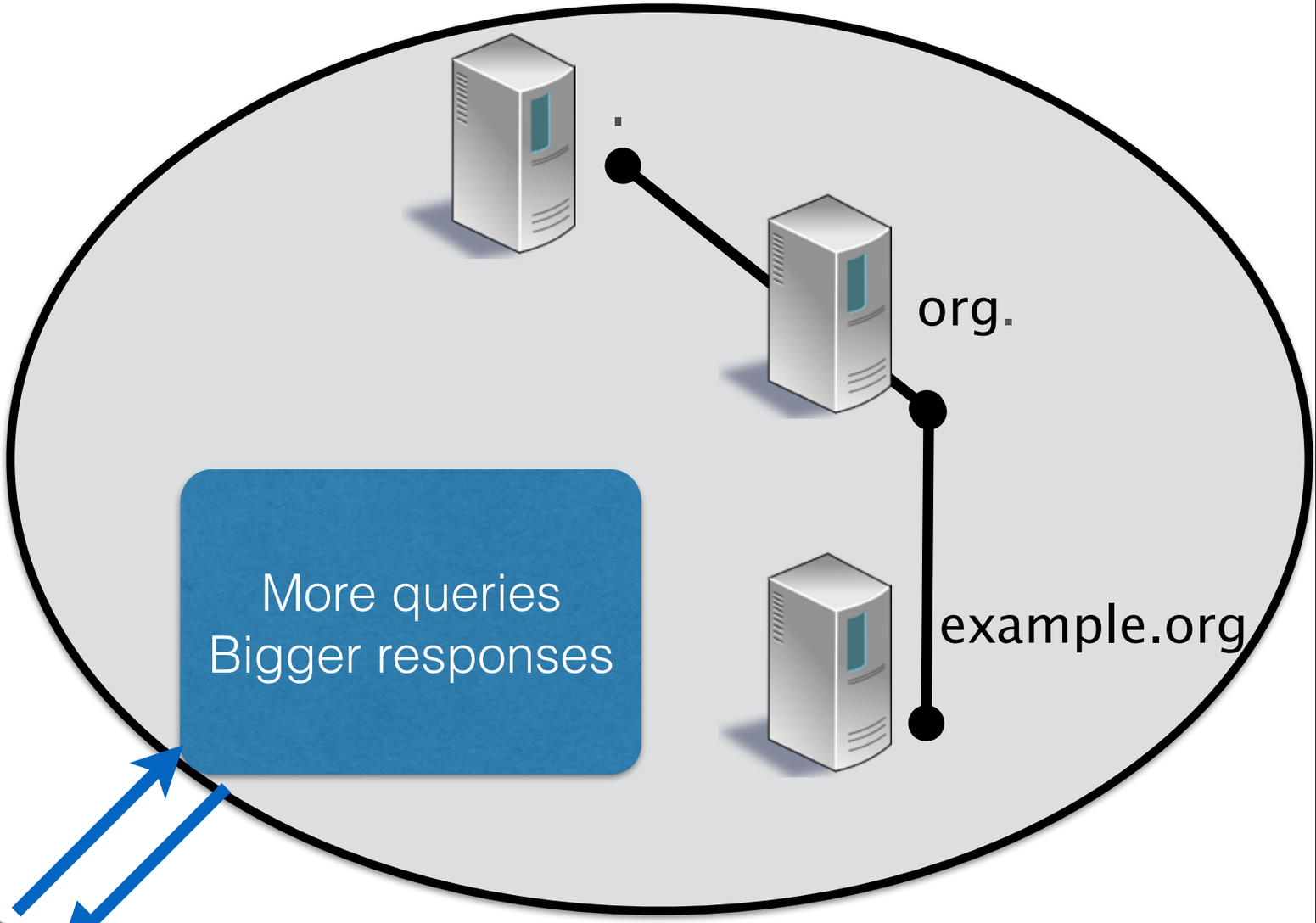


End-to-end DNSSEC



End-to-end DNSSEC

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑
. DNSKEY	public key
. RRSIG	signature ↑
Trust Anchor for "."	hash of public key



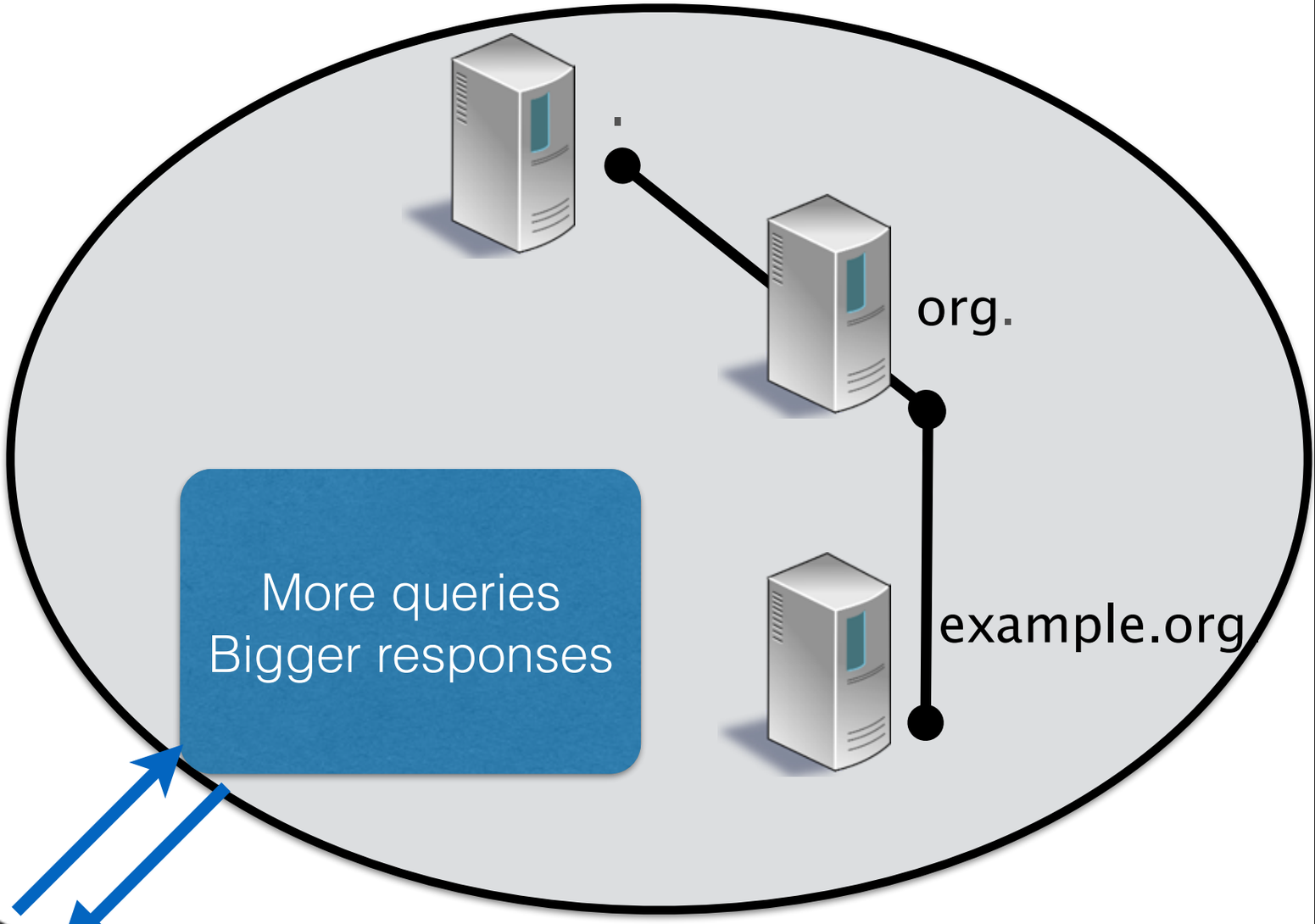
More queries
Bigger responses

Caching
+ validating
resolver

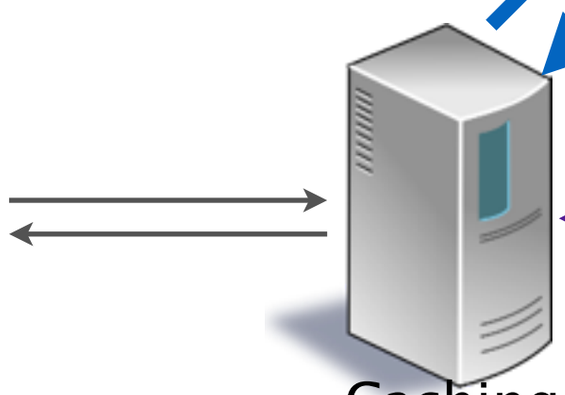
What is the
address of
www.example.org.

End-to-end DNSSEC

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑
. DNSKEY	public key
. RRSIG	signature ↑
Trust Anchor for "."	hash of public key



Trush Anchor for "." (root zone) from configuration file



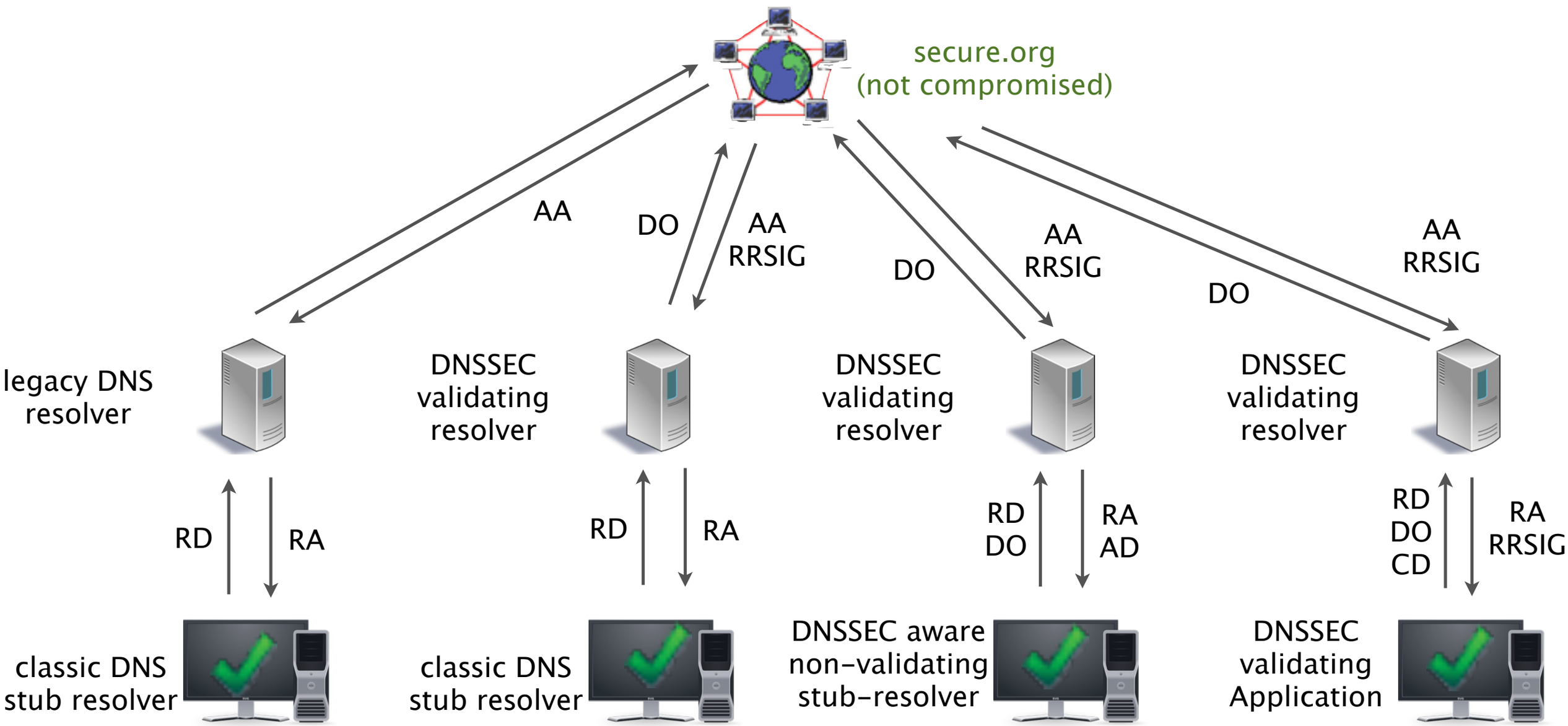
Caching + validating resolver

What is the address of www.example.org.

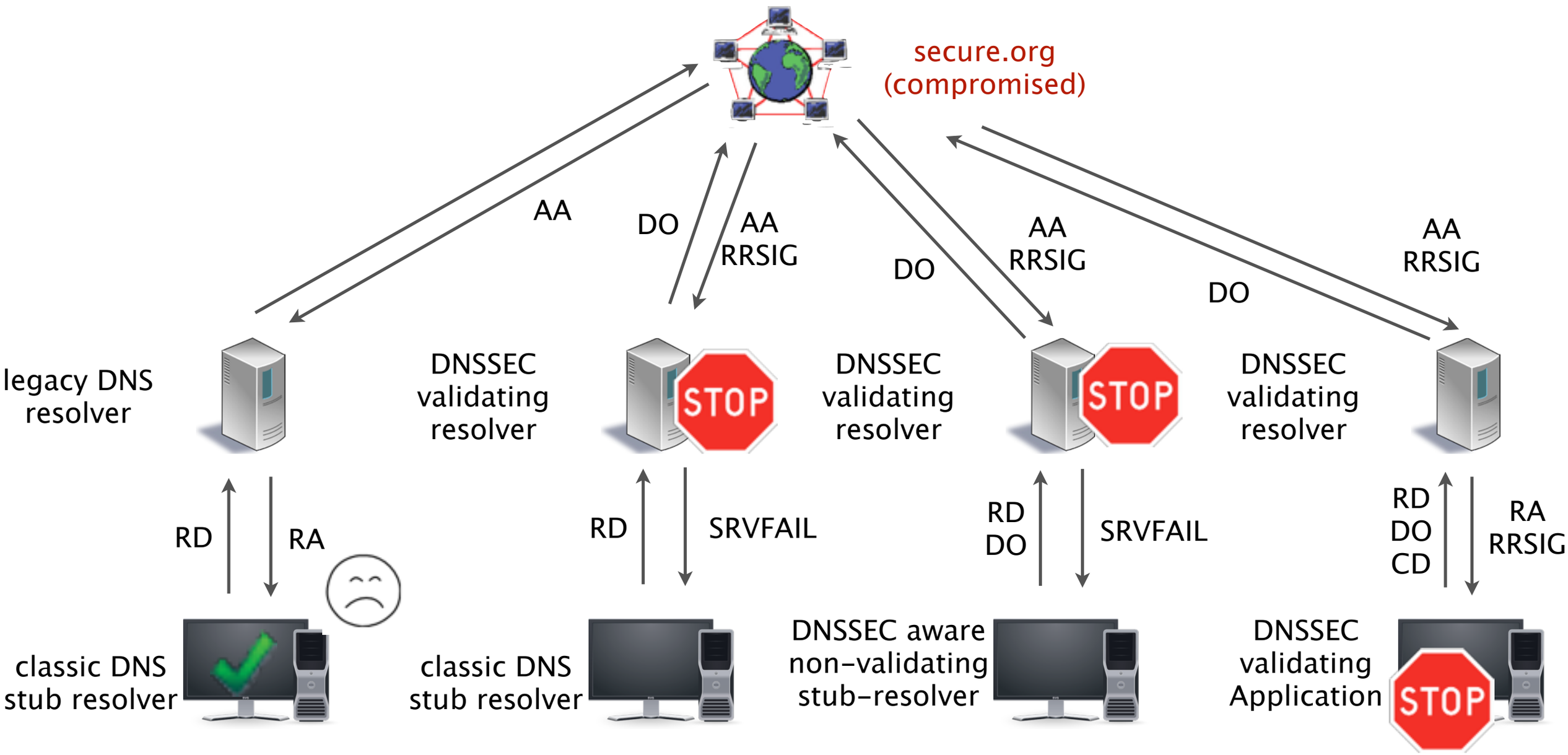
“Middleboxes”

- “Middleboxes” (Firewalls, Load-Balancer, NAT …).
  - Non-compliant boxes cause problems for DNSSEC. They need to:
    - Support EDNS0 (4K)
    - Support for DNS over TCP queries
    - <u>Not</u> make changes to DNS payload data passing through (see RFC 5625 - “DNS Proxy Implementation Guidelines”)
    - Work with higher query load due to DNSSEC validation

DNS clients and DNSSEC resolvers



DNS clients and DNSSEC resolvers



DNSSEC Deployment Today

- Root, ccTLDs, some gTLDs/SLD, banks
  - All new gTLDs, .gov have DNSSEC mandated
- *ISP haven't embraced DNSSEC (yet)*
  - *Additional overhead, complexity and support costs*
  - *Users aren't asking for it*
- Resolving/caching nameservers can validate DNS information

DNSSEC Deployment

- *Stub resolvers cannot validate (today).*
- *End user applications not using DNSSEC (Catch-22).*
- ***getDNS API*** *(https://github.com/getdnsapi/getdns)*
  - A modern asynchronous DNS API
  - Intended to make all types of DNS information easily available
  - Enable applications to take advantage of DNSSEC

DNSSEC

Software Overview

Validating Resolvers

- NLnet Labs **Unbound**
- ISC **BIND 9**
- Microsoft **Windows Server 2012**
- Nominum **Vantio Caching DNS**
- **Double check your root trust anchor!**
  - https://data.iana.org/root-anchors/root-anchors.xml

Authoritative Name Servers

- NLnet Labs **NSD**
- ISC **BIND 9**
- **PowerDNS** Authoritative Server
- Microsoft **Windows Server 2012**
- KNOT DNS/YADIFA

DNSSEC Signers

- **OpenDNSSEC**
- ISC **BIND 9**
- **PowerDNS** Authoritative Server
- Microsoft **Windows Server 2012**
- Nominum **Authoritative Name Server (ANS)**

DNSSEC Signers

	OpenDNSSEC	BIND 9	PowerDNS
Open source	BSD	BSD	GPL
Online signing	Yes	Yes	Yes
Offline signing	Yes	Yes	Yes
Platforms	Unix	Unix & Windows	Unix
Automatic rollovers	Policy driven	Basic	Basic
[HS]SM	Yes	Limited	None
Scales to 10,000+ zones	Not yet…	Yes	Yes

OpenDNSSEC

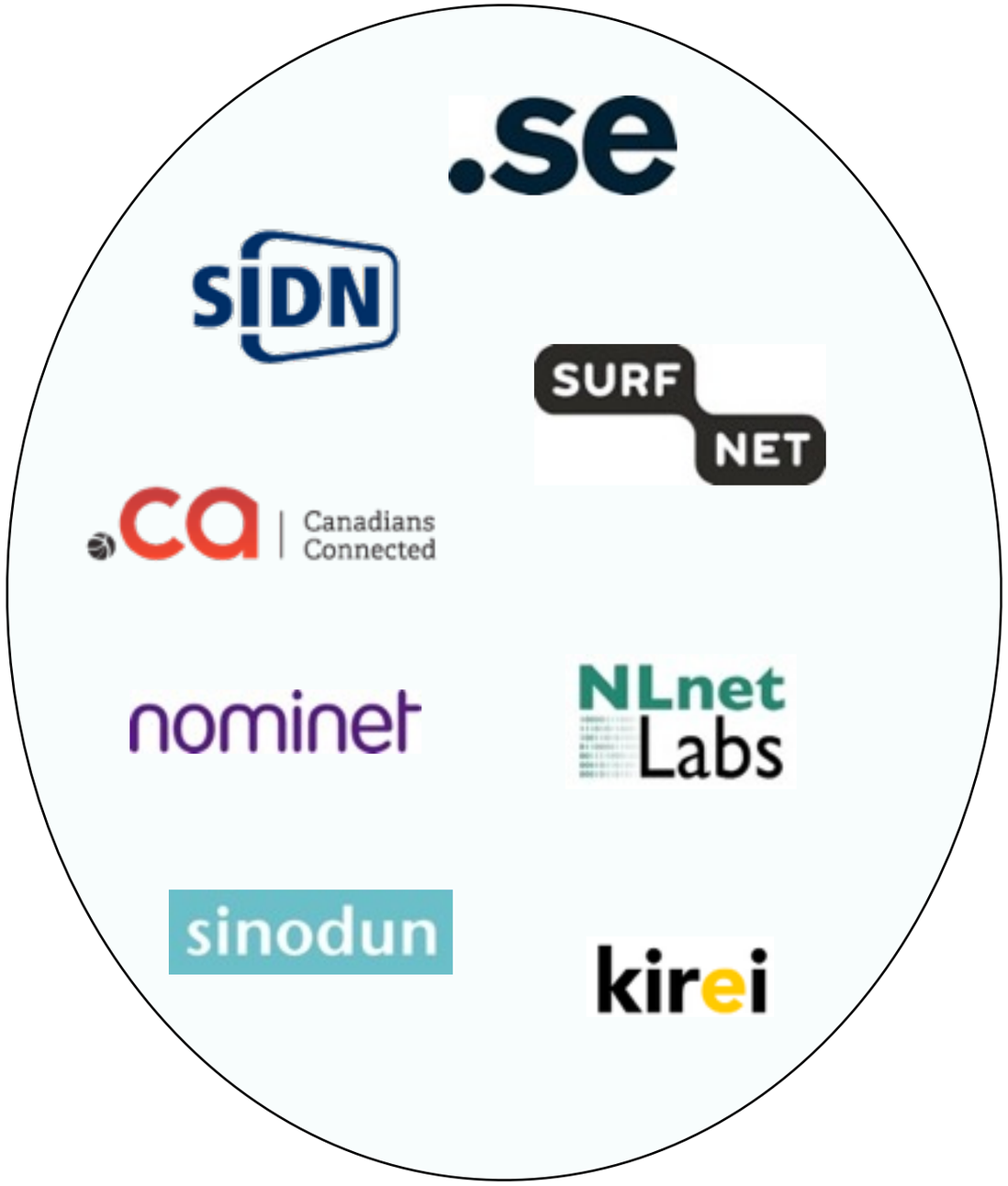
opendnssec.org

What is OpenDNSSEC?

- Turn-key solution for DNSSEC

- Automates
  - Zone signing and management
  - Key & rollover management
- RFC compliant
- (Not a nameserver)

History of OpenDNSSEC



- Goals:
  - Address lack of tools
  - Make DNSSEC easy to deploy
  - HSM support
- Releases:
  - OpenDNSSEC v1.0 (Feb 2010)
  - Currently on 1.4
  - OpenDNSSEC 2.0 is on the way

Key Features

- Bump in the wire
- Policy-driven configuration. Specify:
  - Signature refresh period
  - Key algorithm/length, rollover.
- Files or IXFR/AXFR
- Support for Hardware Security Modules (HSM)
- Several high-profile reference deployments

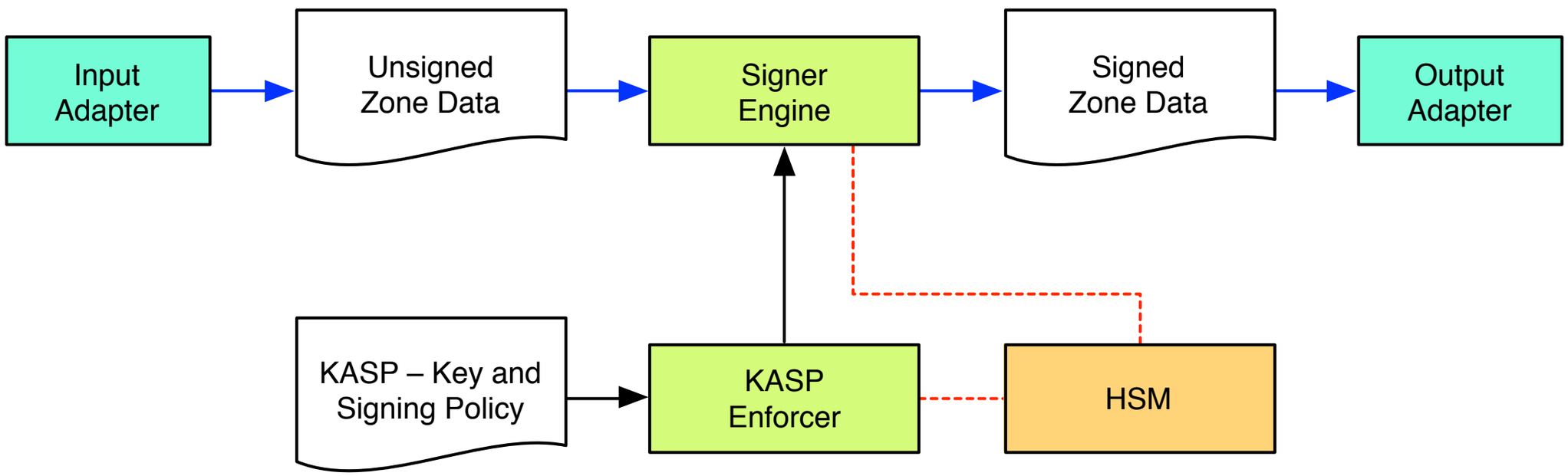
```
<Signatures>
    <Resign>PT2H</Resign>
    <Refresh>P3D</Refresh>
```

```
<!-- Parameters for KSK only -->
 <KSK>
   <Algorithm length="2048">8</Algorithm>
   <Lifetime>P1Y</Lifetime>
   <Repository>SoftHSM</Repository>
  </KSK>
```

Example of Users

- .UK – Nominet UK
- .SE – IIS
- .NL – SIDN
- .CA – CIRA
- .DK – DK Hostmaster
- .FR – AFNIC
- .FI – FICORA
- .LU – RESTENA
- .NU – IIS
- .SI – ARNES
- .PM, .RE, .TF, .WF, .YT – AFNIC

Architecture



https://wiki.opendnssec.org/display/DOCS

OpenDNSSEC in action

- 1 time configuration (Policy, HSM, logging)
- Start the 2 daemons. Watch the logs…

```
ods-enforcerd: opendnssec starting…
ods-signerd: [engine] running as pid 15420

ods-enforcerd: HSM opened successfully.
ods-enforcerd: Policy default found.
ods-enforcerd: 1 zone(s) found on policy "default"
ods-enforcerd: 1 new ZSK(s) (1024 bits) need to be created.
ods-enforcerd: SoftHSM: C_GenerateKeyPair: Key pair generated
ods-enforcerd: Created ZSK size: 1024, alg: 7 with id: 81013e1cc07282b91b1350d43c673b84 in
repository: SoftHSM and database.
ods-enforcerd: Zone ods found.
ods-enforcerd: Config will be output to /var/opendnssec/signconf/ods.xml.

ods-signerd: [signconf] zone ods signconf: RESIGN[PT180S] REFRESH[PT900S]
VALIDITY[PT3600S] DENIAL[PT3600S] JITTER[PT60S] OFFSET[PT60S] NSEC[50] DNSKEYTTL[PT600S]
SOATTL[PT600S] MINIMUM[PT300S] SERIAL[unixtime]

ods-signerd: [STATS] ods 1396253015 RR[count=264 time=0(sec)] NSEC3[count=24 time=0(sec)]
RRSIG[new=53 reused=0 time=0(sec) avg=0(sig/sec)] TOTAL[time=0(sec)]
```

OpenDNSSEC in action

```
$ ods-ksmutil zone list
Found Zone: ods; on policy Default
Found Zone: ods1; on policy Default
Found Zone: ods2; on policy Policy1
```

```
$ ods-ksmutil key list -v —zone odd
Keys:
Zone:            Keytype:      State:    Date of next transition (to):  Size:   Algorithm:
ods1             KSK           active    2011-01-01 13:15:00 (retire)   2048    5
ods1             KSK           retire    2010-01-01 13:07:40 (dead)     2048    5
ods1             ZSK           active    2010-01-01 13:03:40 (retire)   2048    5
ods1             ZSK           publish   2010-01-01 13:02:40 (ready)    2048    5
```

```
$ ods-ksmutil key rollover --zone ods1 --all

Manual key rollover for key type all on zone ods1 initiated
```

OpenDNSSEC training

- 1 day courses to 3 day ‘Master class’
- Free training courses run regularly in Stockholm
  - Advertised on the users list
- Other training courses can be arranged based on demand

SoftHSM

- SoftHSM is a software-only implementation of a security module using the PKCS#11 API.
  - Can be used to test the PKCS#11 interface without buying a real HSM.
- Uses Botan for crypto and SQLite for storage.
- SoftHSM makes it possible to use OpenDNSSEC in a software-only environment.
- V2 will support OpenSSL for crypto.

DNSSEC Appliances

- Secure64 (based on NSD)
- Infoblox (based on BIND)
- BlueCat (based on BIND)

Other Tools

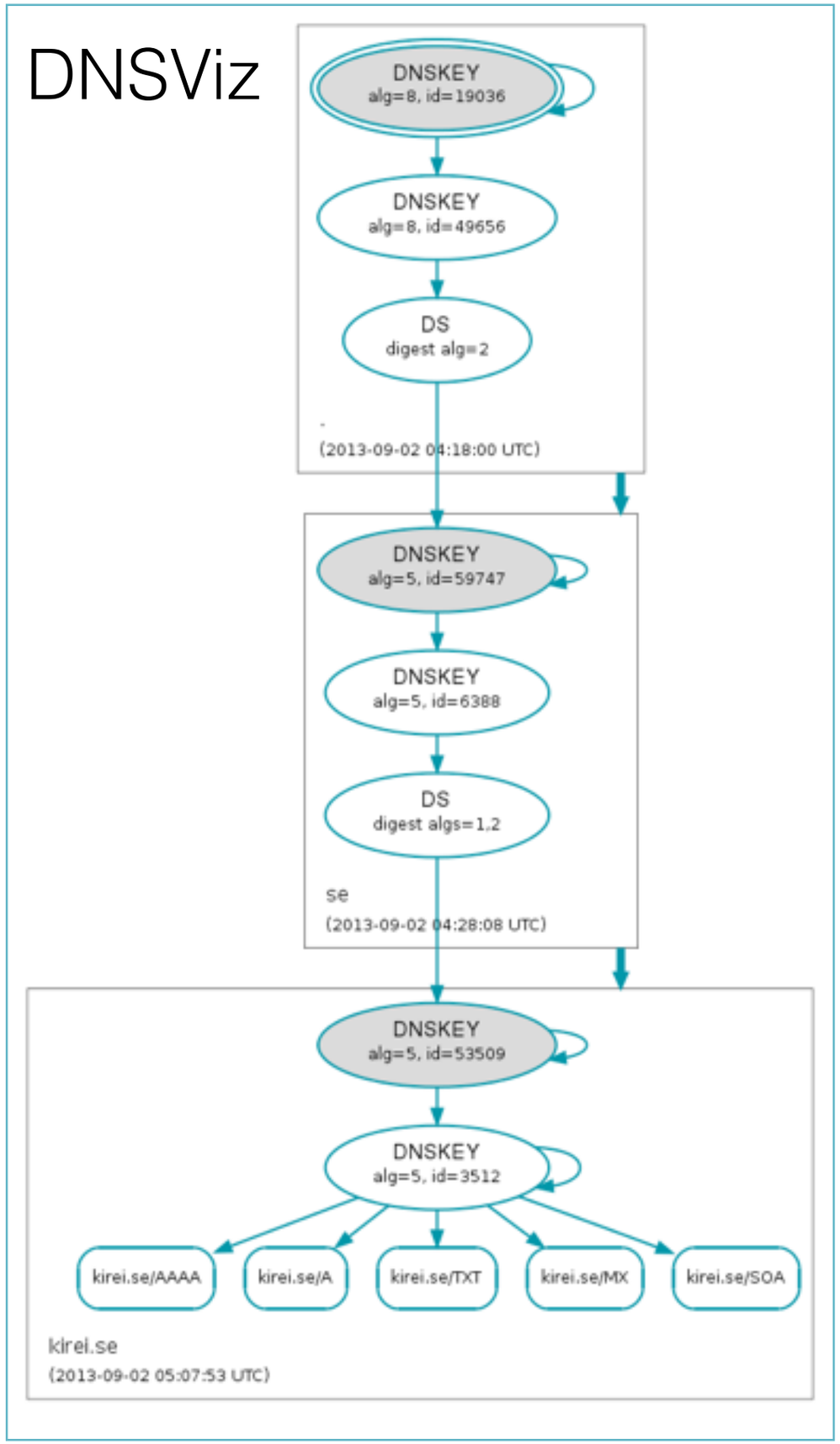
Zone File Validators

- **validns**
  - http://www.validns.net/
- **dnssec-verify**
  - Part of ISC BIND 9.9.x
- **Credns**
  - AXFR/IXFR frontend for standalone zone file validators (e.g., validns or dnssec-verify)
  - https://www.nlnetlabs.nl/projects/credns/

DNS(SEC) Status Validators

- **DNSCheck** (http://dnscheck.iis.se): Designed to check, measure and help understand the workings of DNS.
  - Open source software written in Perl. Web-based front end and CLI.
- **DNSViz** is a very useful tool for visualizing the status, including detailed DNSSEC information, of a DNS zone.
  - http://dnsviz.net/
- **DNS Debugger**: Online tool to verify the trust chain.
  - http://dnssec-debugger.verisignlabs.com/

DNSViz

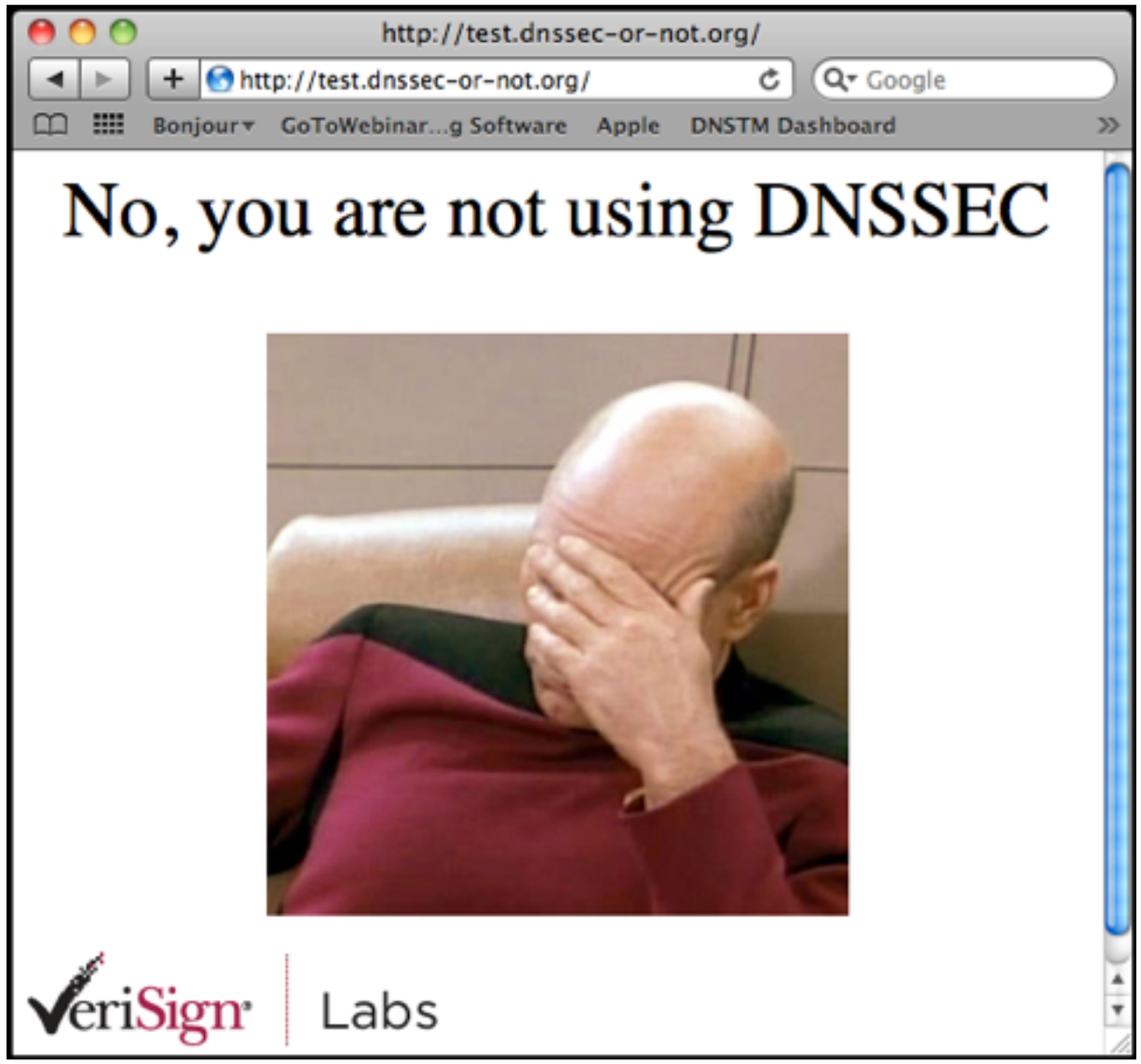


DNSDebugger

Analyzing DNSSEC problems for kirei.se

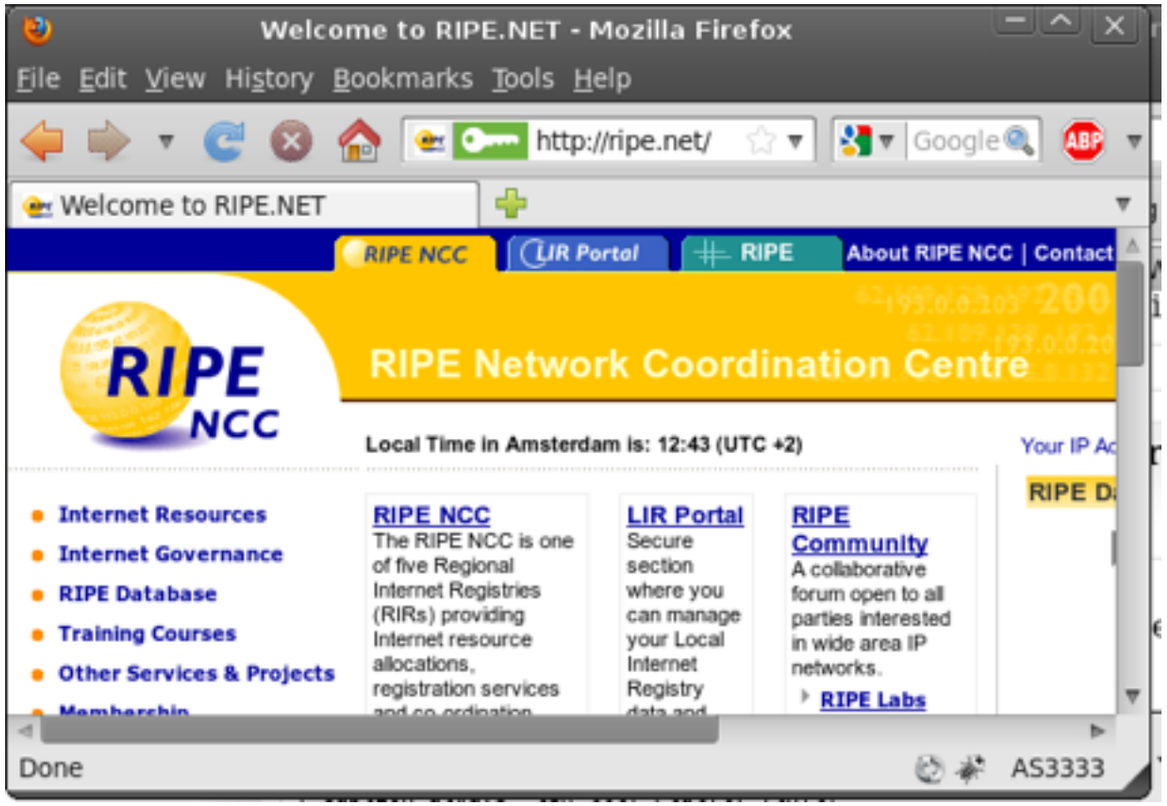
.	Found 2 DNSKEY records for . DS=19036/SHA1 verifies DNSKEY=19036/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
se	Found 1 DS records for se in the . zone Found 1 RRSIGs over DS RRset RRSIG=49656 and DNSKEY=49656 verifies the DS RRset Found 2 DNSKEY records for se DS=59747/SHA256 verifies DNSKEY=59747/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=59747 and DNSKEY=59747/SEP verifies the DNSKEY RRset
kirei.se	Found 2 DS records for kirei.se in the se zone Found 1 RRSIGs over DS RRset RRSIG=6388 and DNSKEY=6388 verifies the DS RRset Found 2 DNSKEY records for kirei.se DS=53509/SHA1 verifies DNSKEY=53509/SEP Found 2 RRSIGs over DNSKEY RRset RRSIG=3512 and DNSKEY=3512 verifies the DNSKEY RRset kirei.se A RR has value 91.206.174.18 Found 1 RRSIGs over A RRset RRSIG=3512 and DNSKEY=3512 verifies the A RRset

http://dnssec-or-not.org



http://www.verisigninc.com/en_US/innovation/verisign-labs/internet-security-tools/index.xhtml

DNSSEC Validation in Browsers



- Install the Firefox DNSSEC Add-On (`http://www.dnssec-validator.cz/`)

- and then go to

  `http://www.root-dnssec.org`

  or `http://www.ripe.net`

  and you should see a nice green key icon in the URL bar telling you that this DNS information was DNSSEC validated.

- Also available for IE

DNS Trigger

- http://www.nlnetlabs.nl/projects/dnssec-trigger/
- **Dnssec-trigger** (re)configures the local Unbound DNS server which is running on localhost (127.0.0.1) as a validating (caching) local resolver.
  - It probes for DNSSEC capable servers, indicates result via status icon.
  - There is the option to go with insecure DNS only.
- This software is experimental, open source (BSD).

Acknowledgements

- OpenDNSSEC training material:
  - https://wiki.opendnssec.org/display/DOCREF/Training+Videos+and+Study+Material
- Additional material based on slides from Men & Mice:
  - http://www.menandmice.com/training

Contact

sara@sinodun.com

sara@opendnssec.org

Should you do DNSSEC…? Yes - or you might regret it!

Appendix

Administering a signed zone:

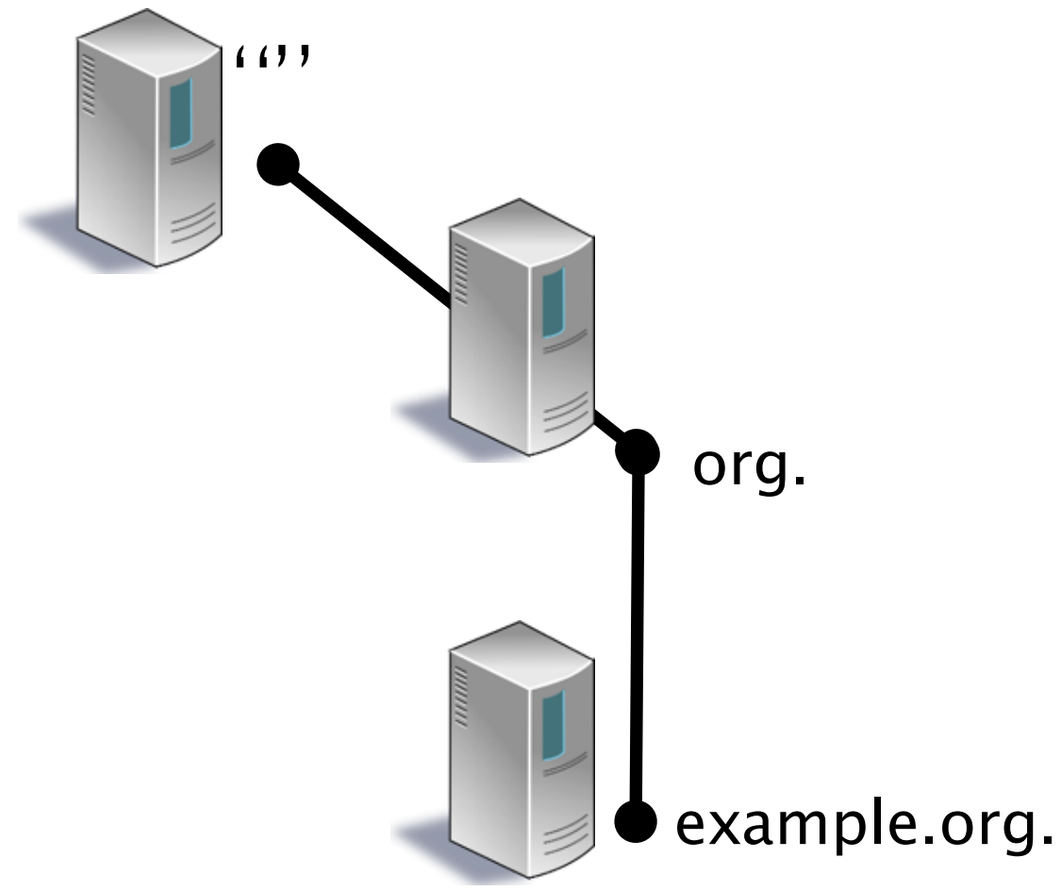
NSEC/NSEC3

NSEC or NSEC3?

- **NSEC (Simple option)**
  - When zone content is not highly structured or trivially guessable
  - Ease the work required by signers and validators
- **NSEC3 (More complex)**
  - Make zone enumeration harder (as hard as trying to enumerate an unsigned zone)
  - ‘Opt-out’ might be an option when the number of secure delegations is low
- **Recommendation:** Use NSEC unless the benefits of NSEC3 are important to you

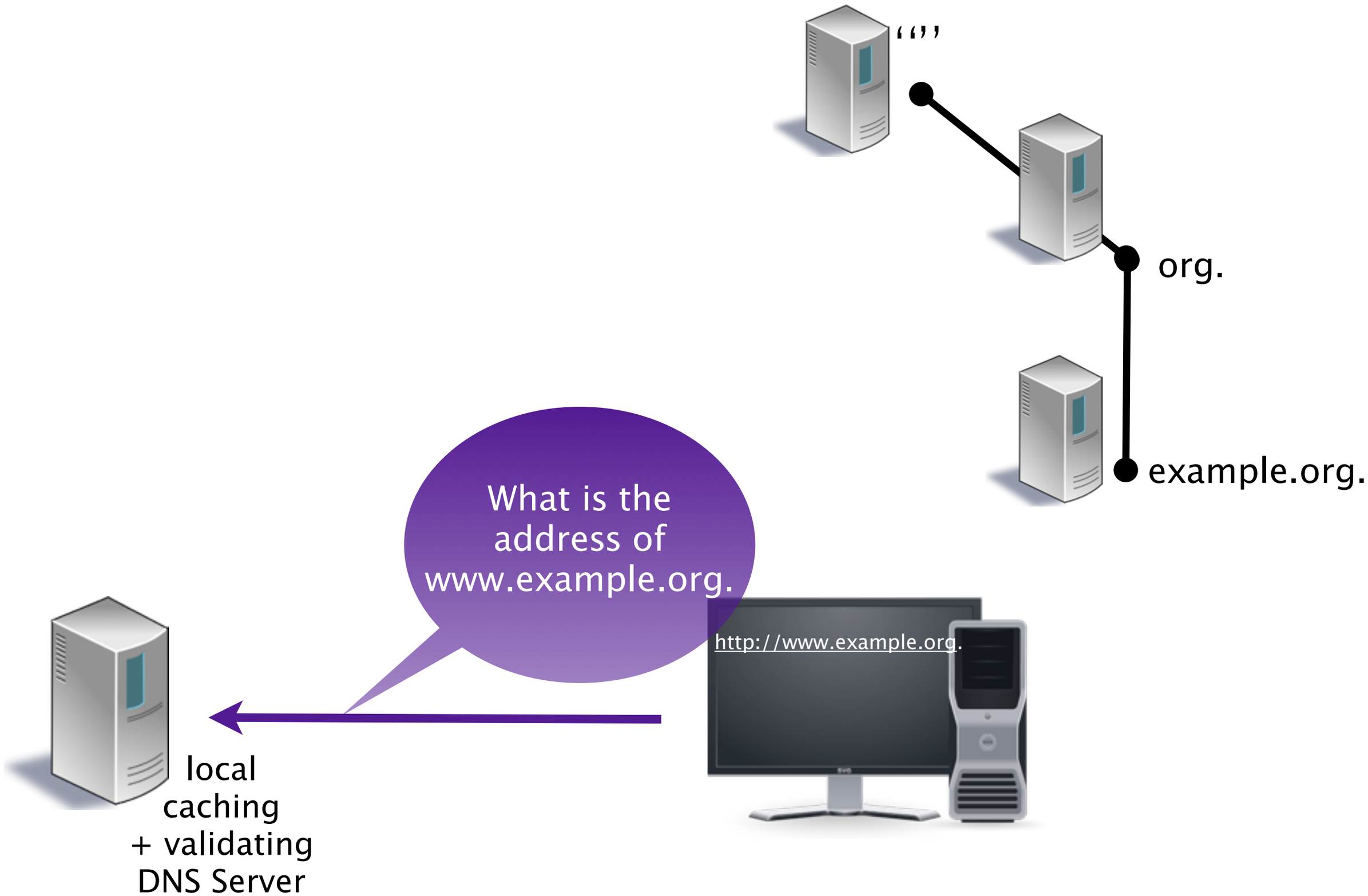
DNSSEC Name Resolution (simplified)

DNSSEC Name Resolution

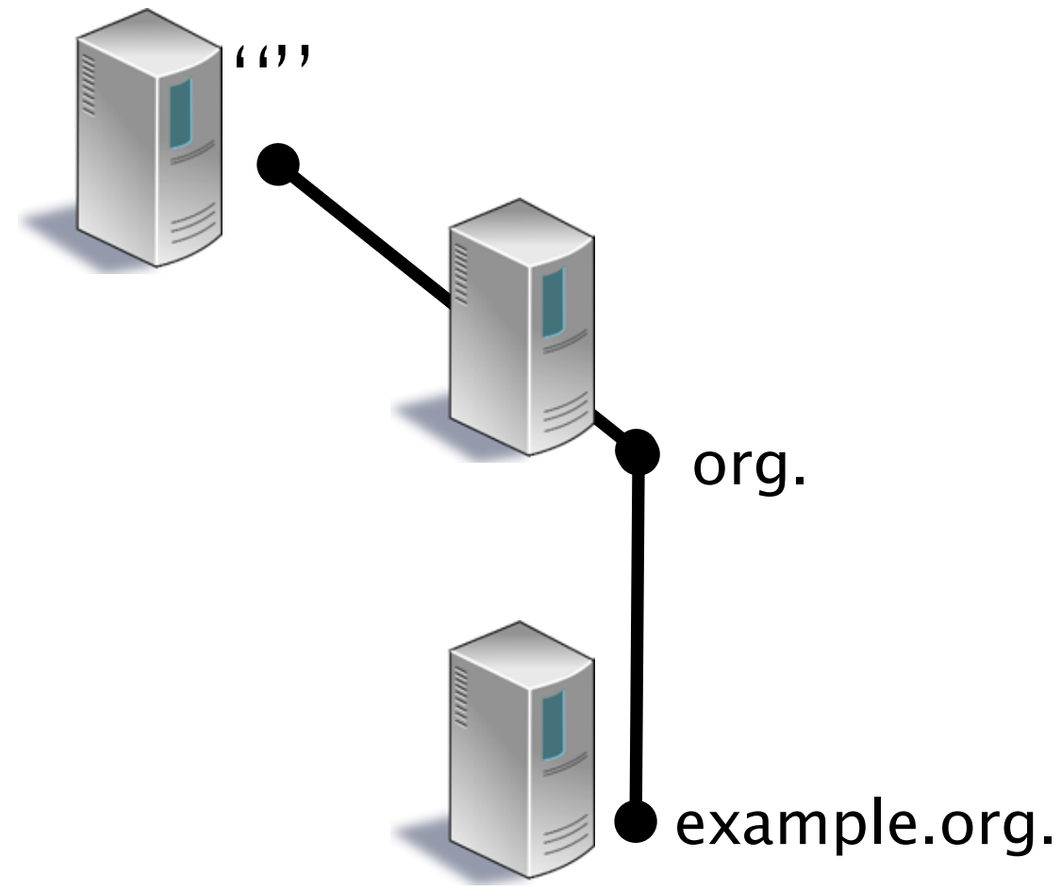


local
caching
+ validating
DNS Server

DNSSEC Name Resolution

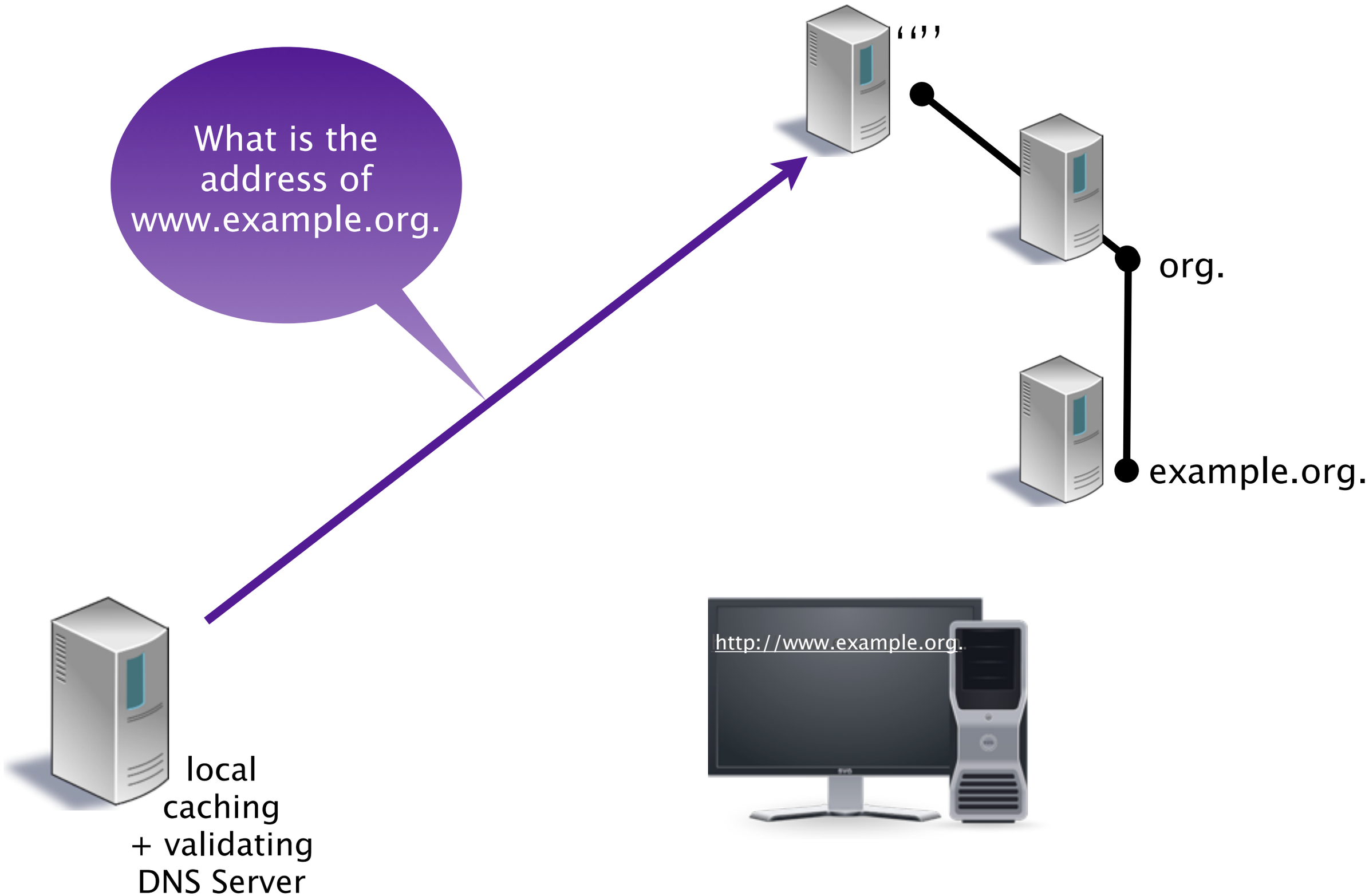


DNSSEC Name Resolution

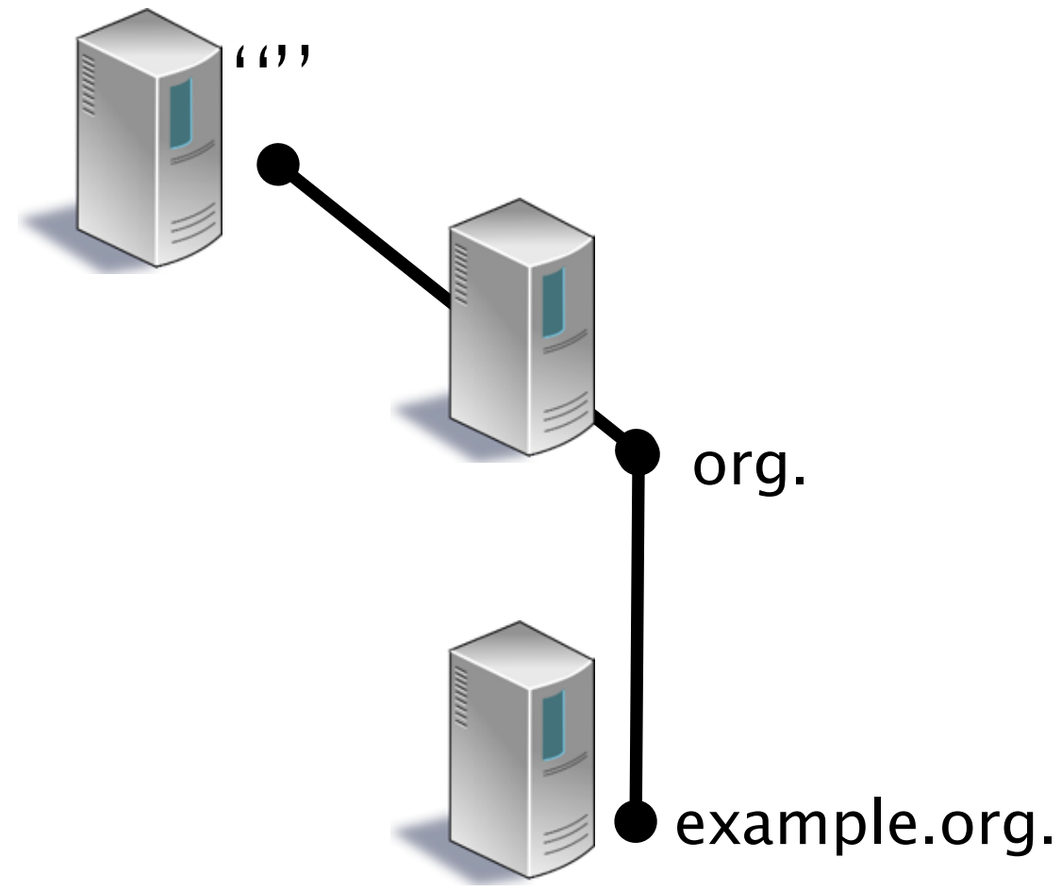


local
caching
+ validating
DNS Server

DNSSEC Name Resolution

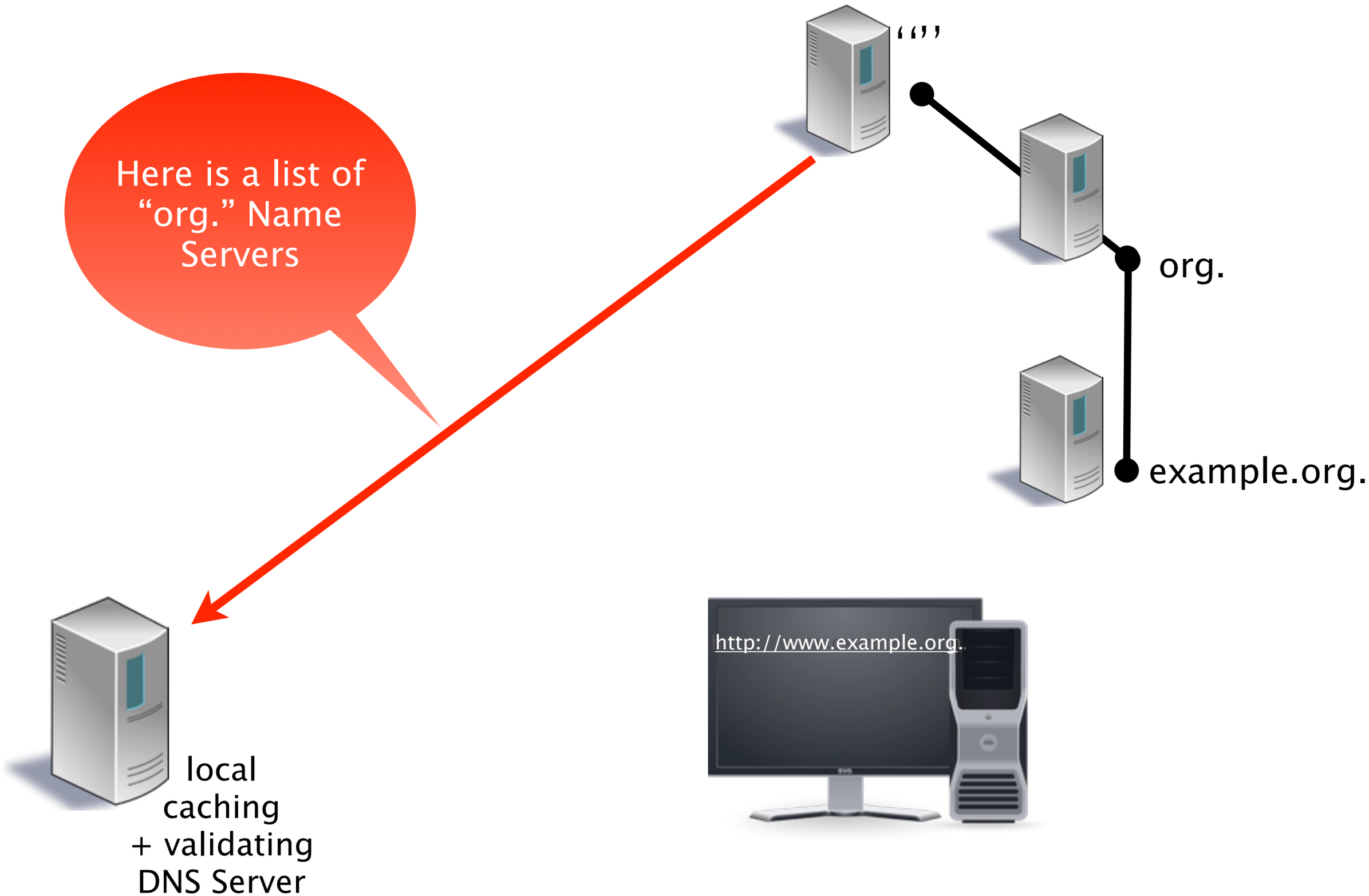


DNSSEC Name Resolution

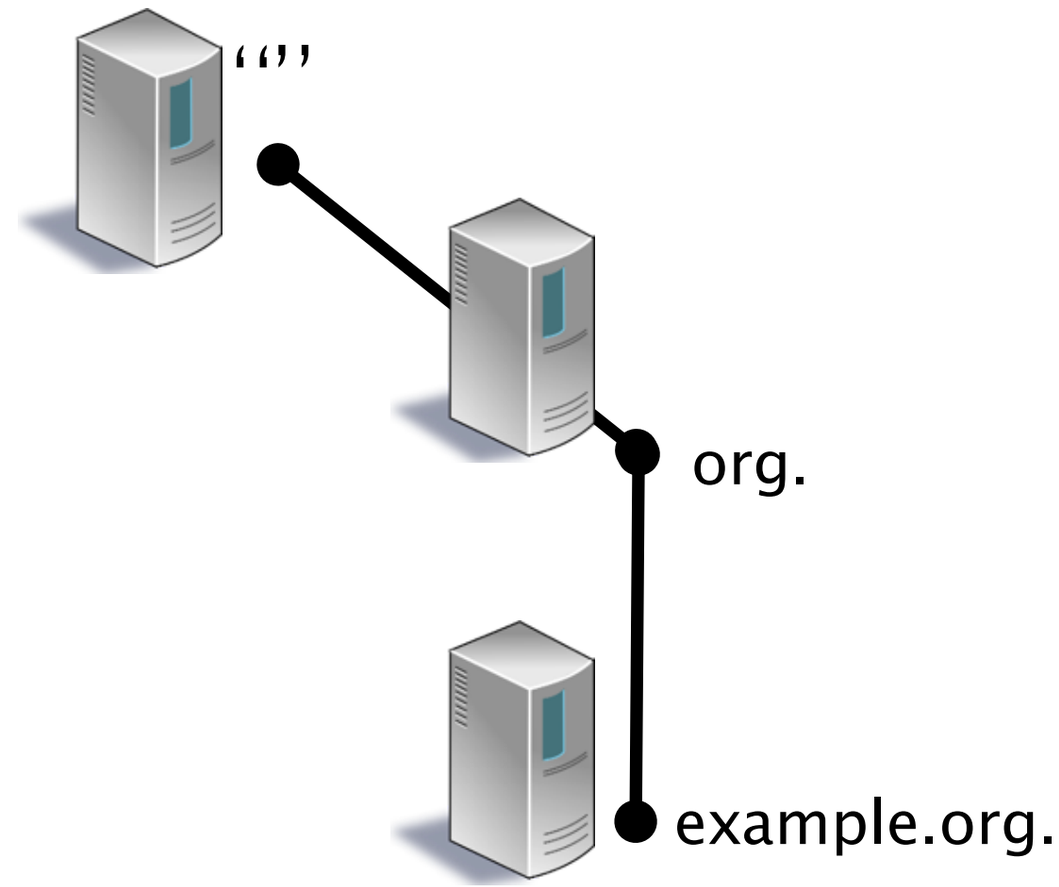


local
caching
+ validating
DNS Server

DNSSEC Name Resolution

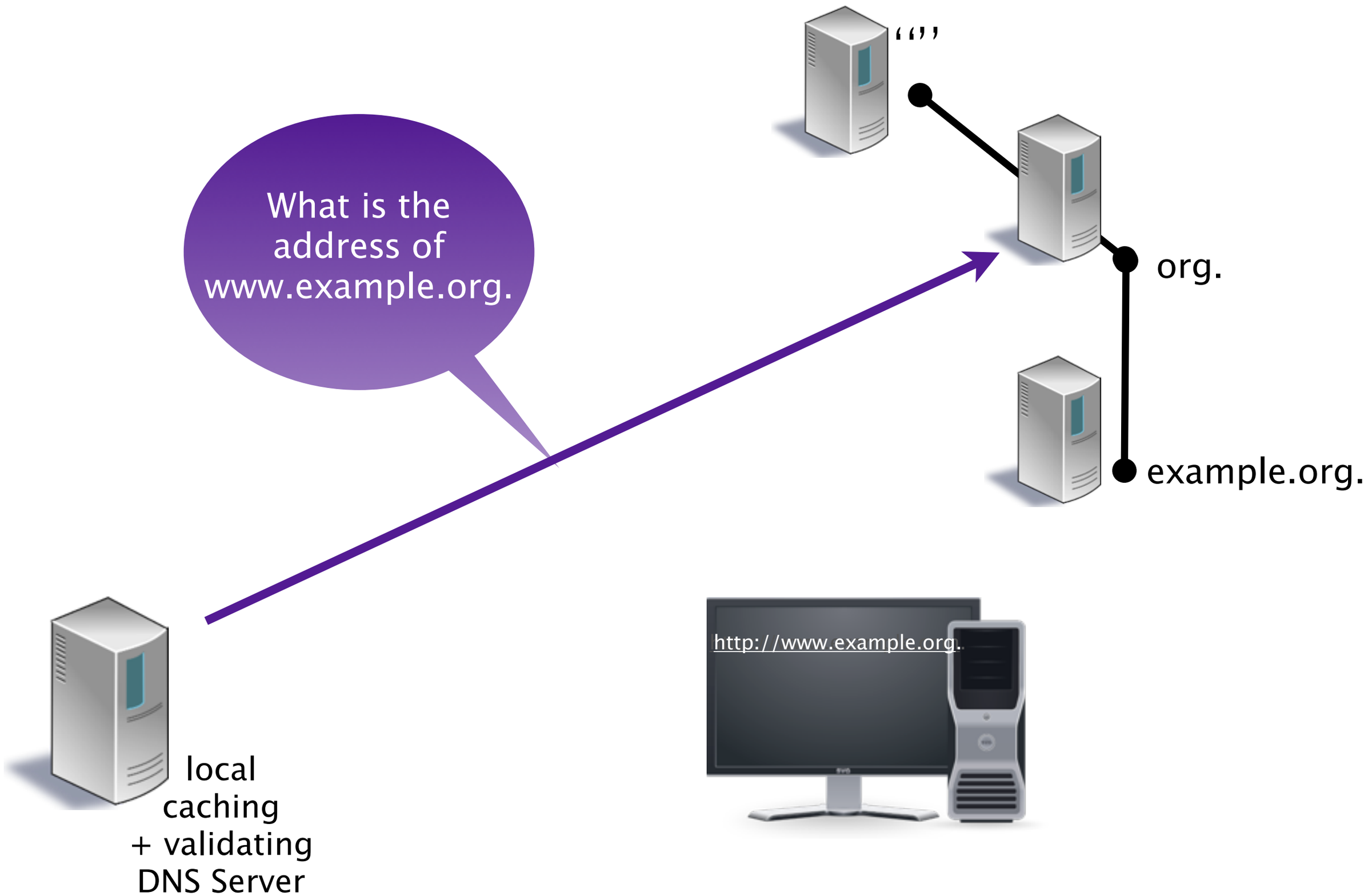


DNSSEC Name Resolution

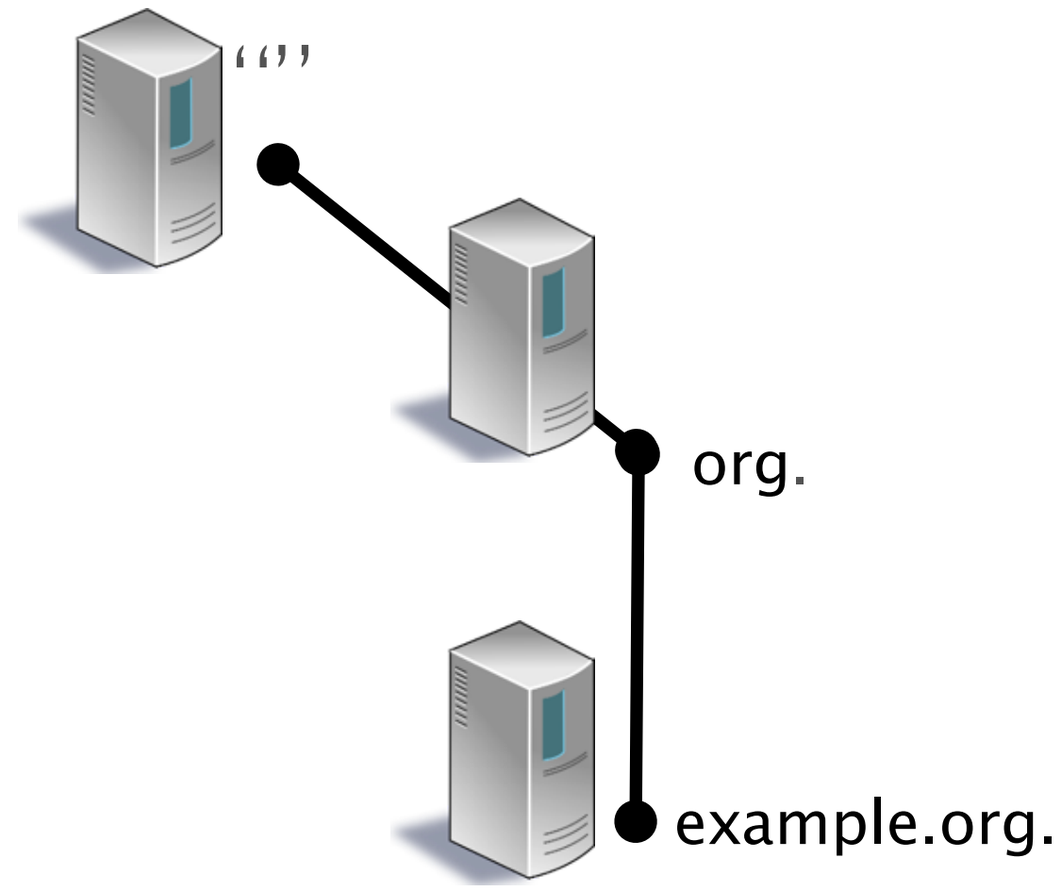


local
caching
+ validating
DNS Server

DNSSEC Name Resolution

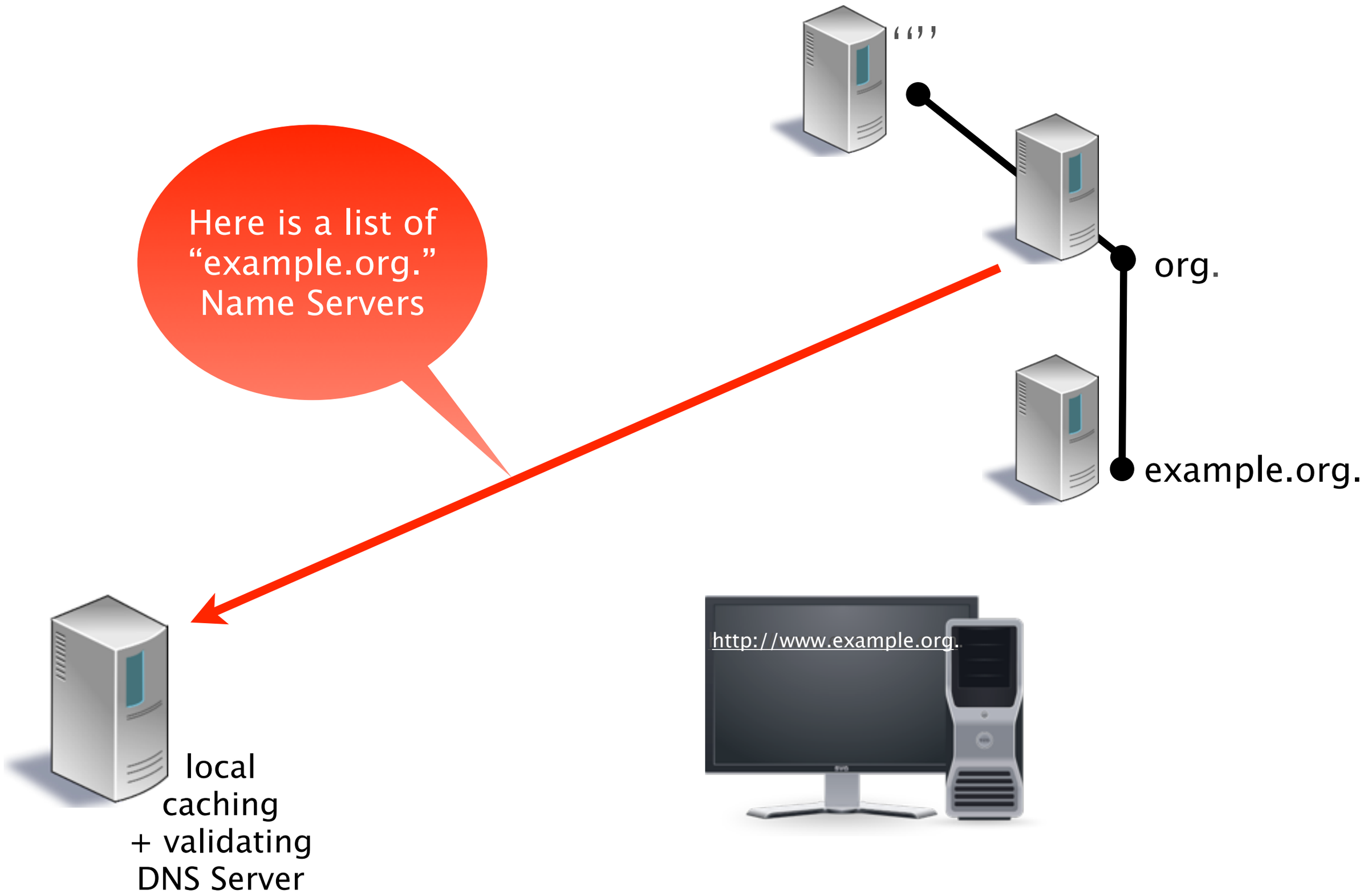


DNSSEC Name Resolution

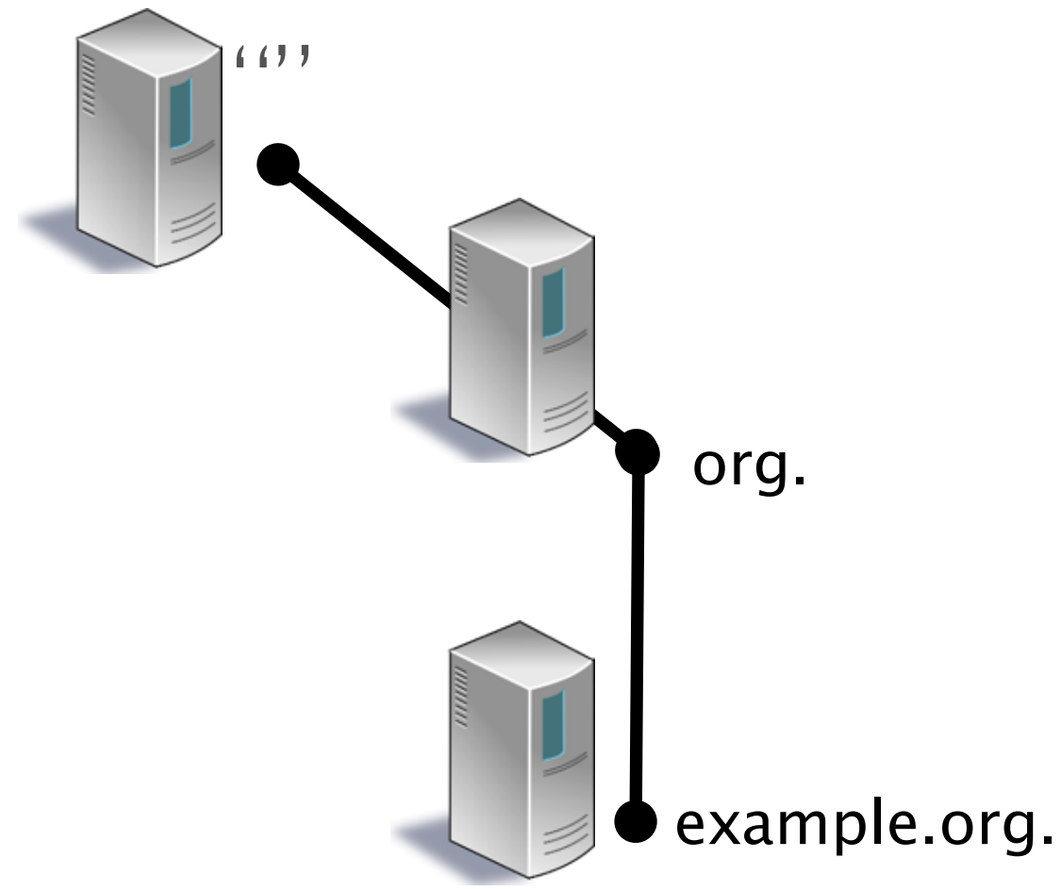


local
caching
+ validating
DNS Server

DNSSEC Name Resolution

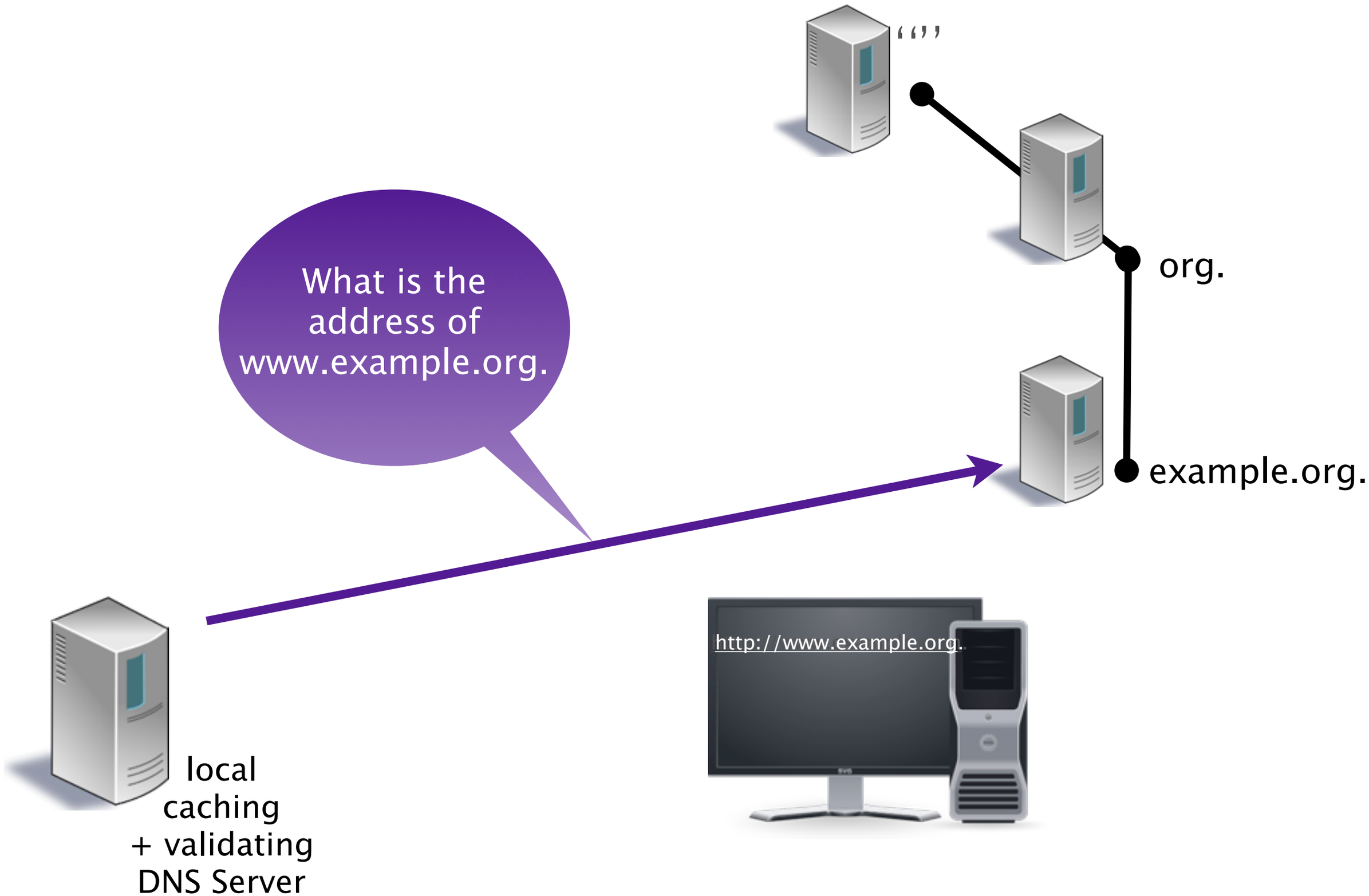


DNSSEC Name Resolution

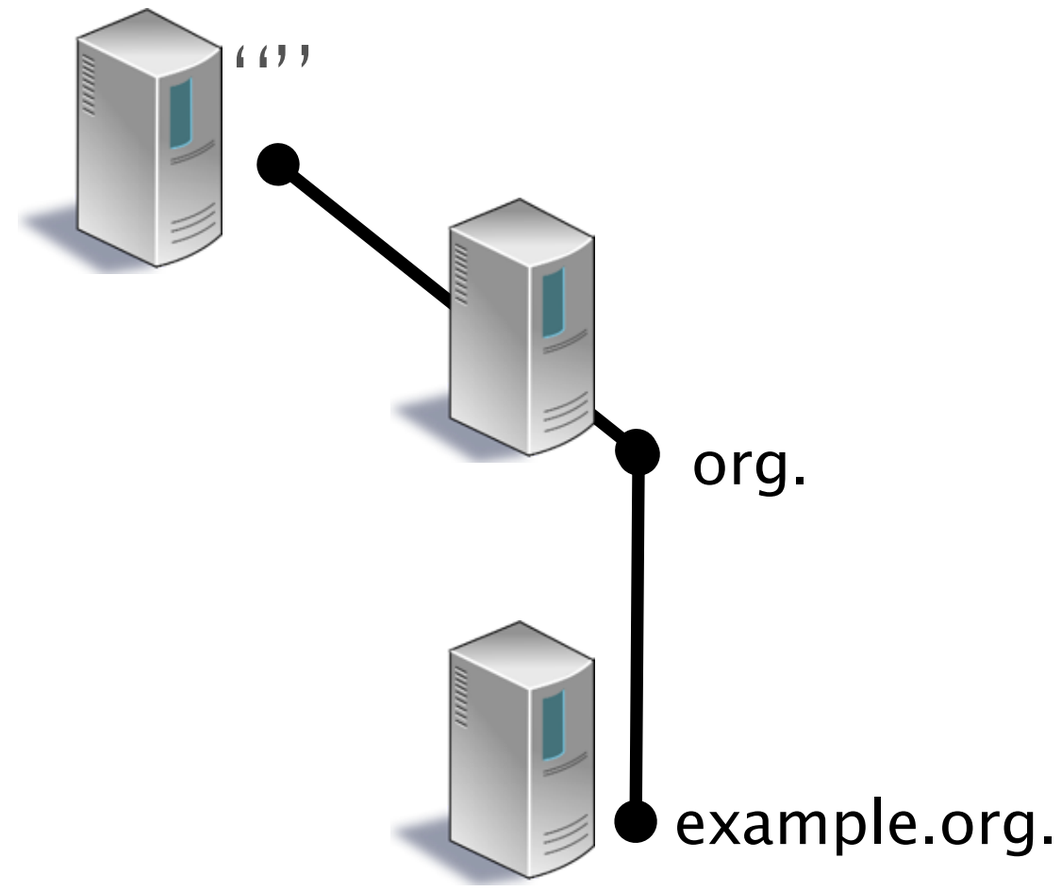


local
caching
+ validating
DNS Server

DNSSEC Name Resolution

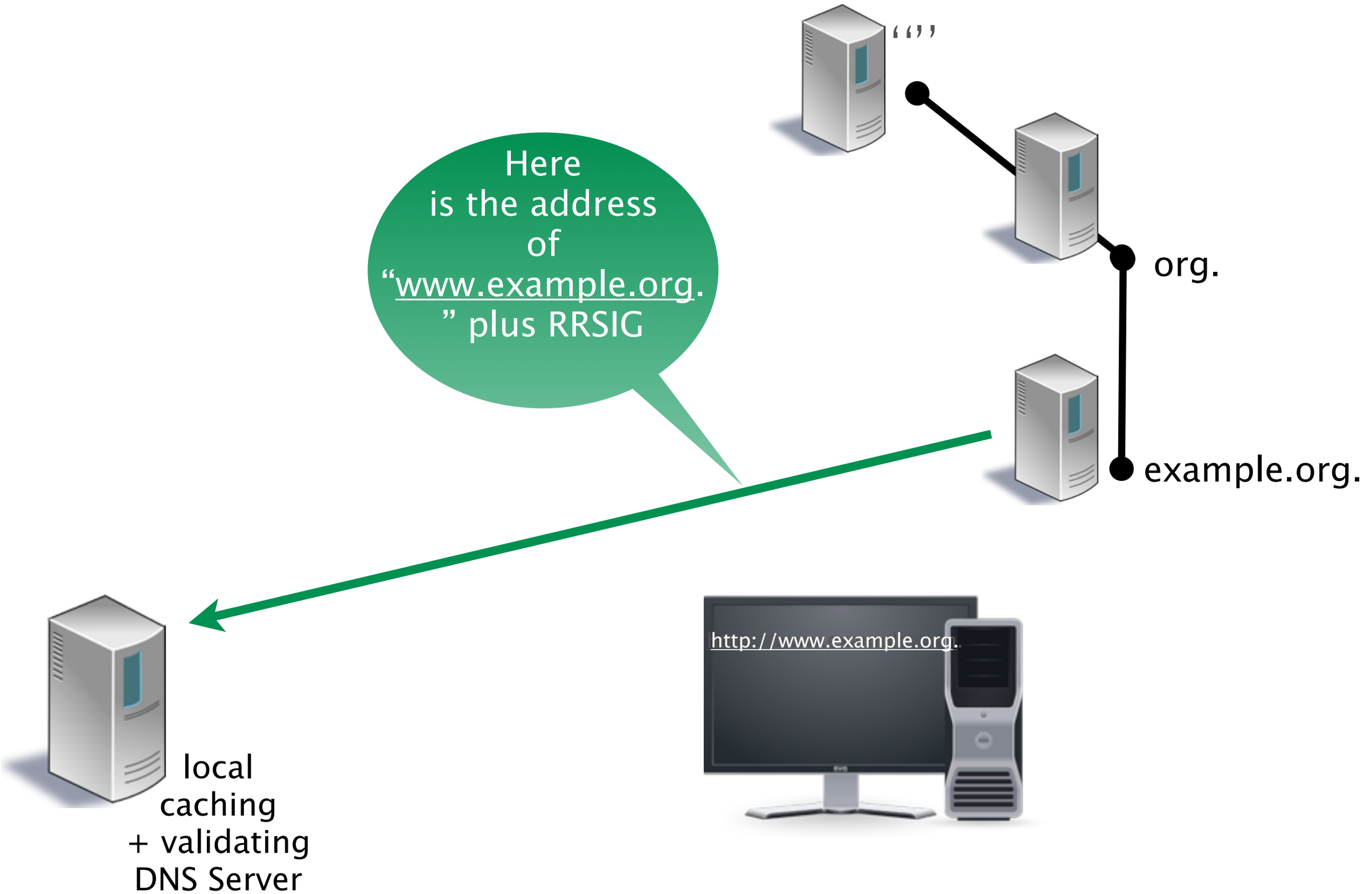


DNSSEC Name Resolution

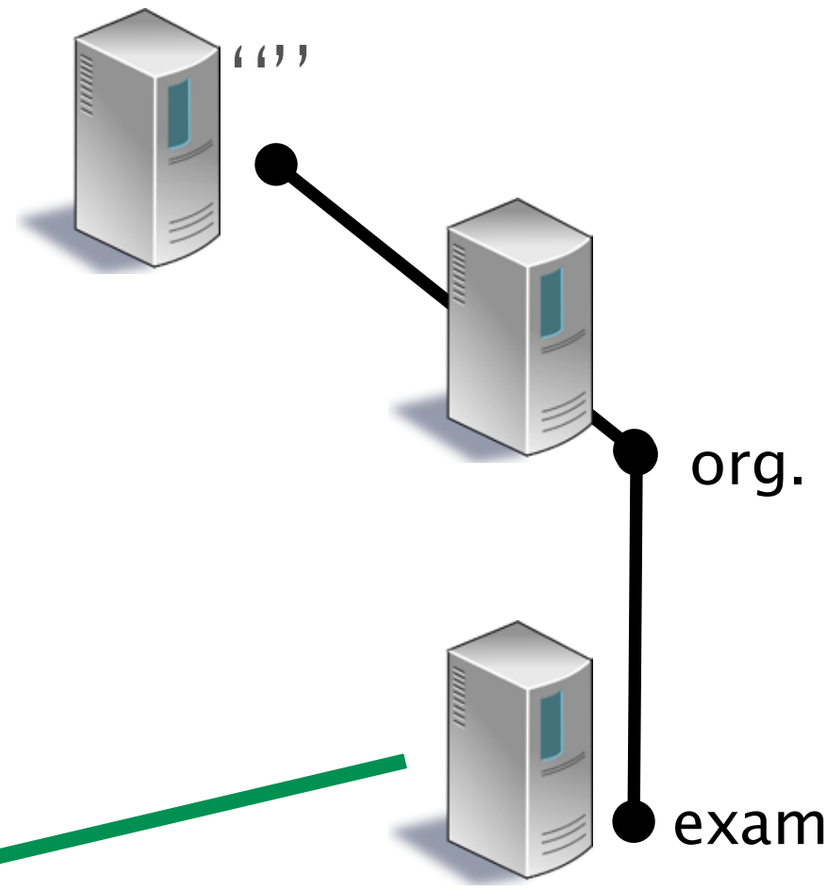


local
caching
+ validating
DNS Server

DNSSEC Name Resolution



DNSSEC Name Resolution

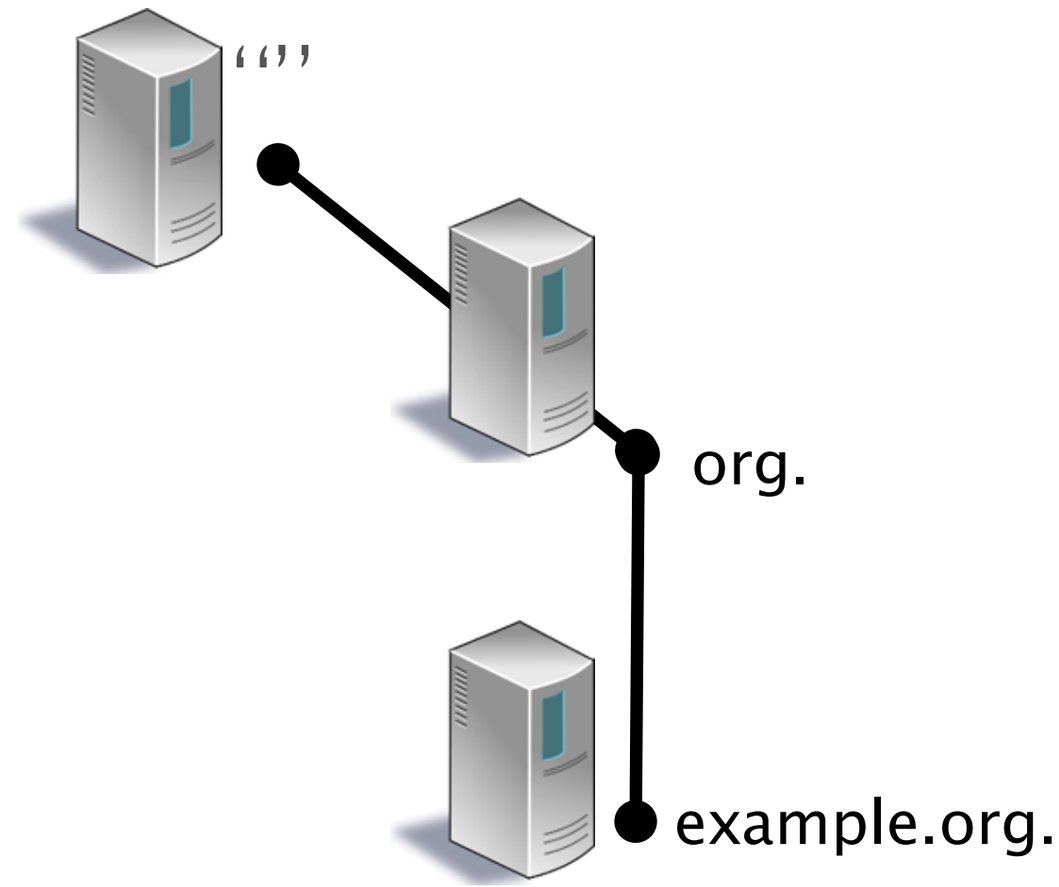


Here
is the address
of
“www.example.org.
” plus RRSIG

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑

local
caching
+ validating
DNS Server

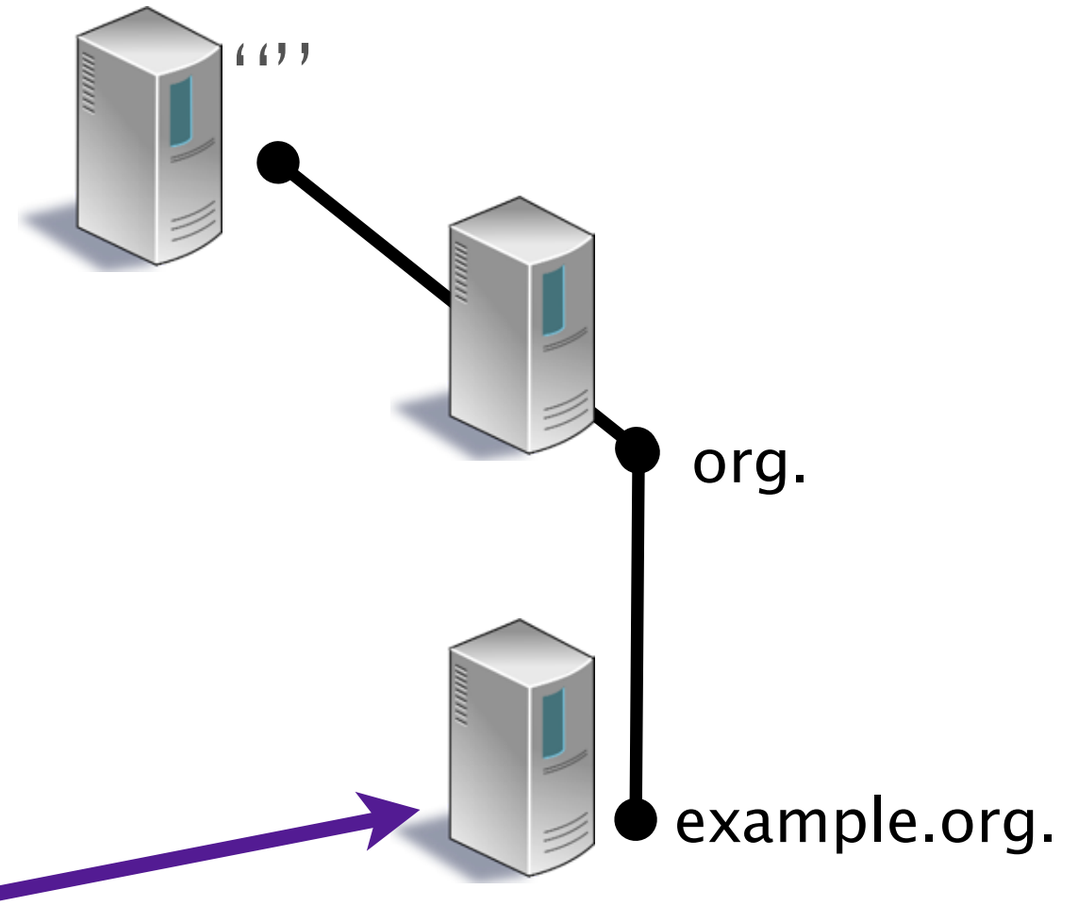
DNSSEC Name Resolution



Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑

local
caching
+ validating
DNS Server

DNSSEC Name Resolution

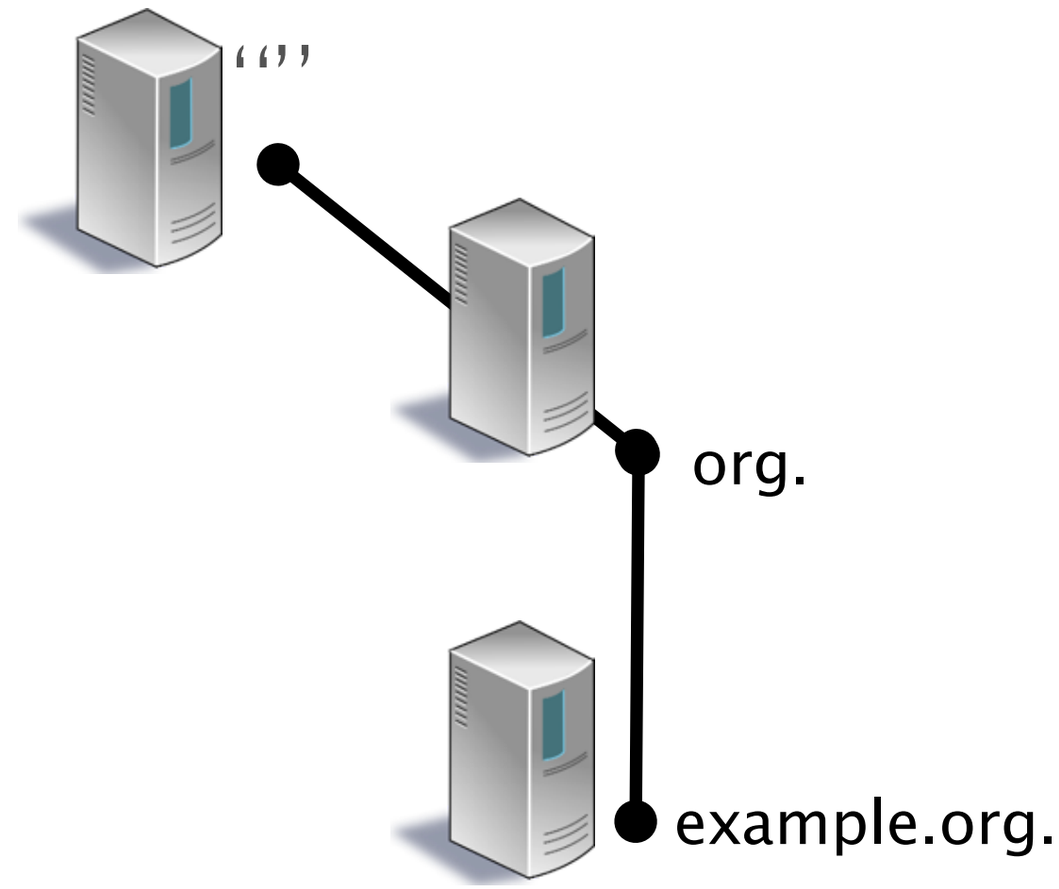


What is the public key of example.org.

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑

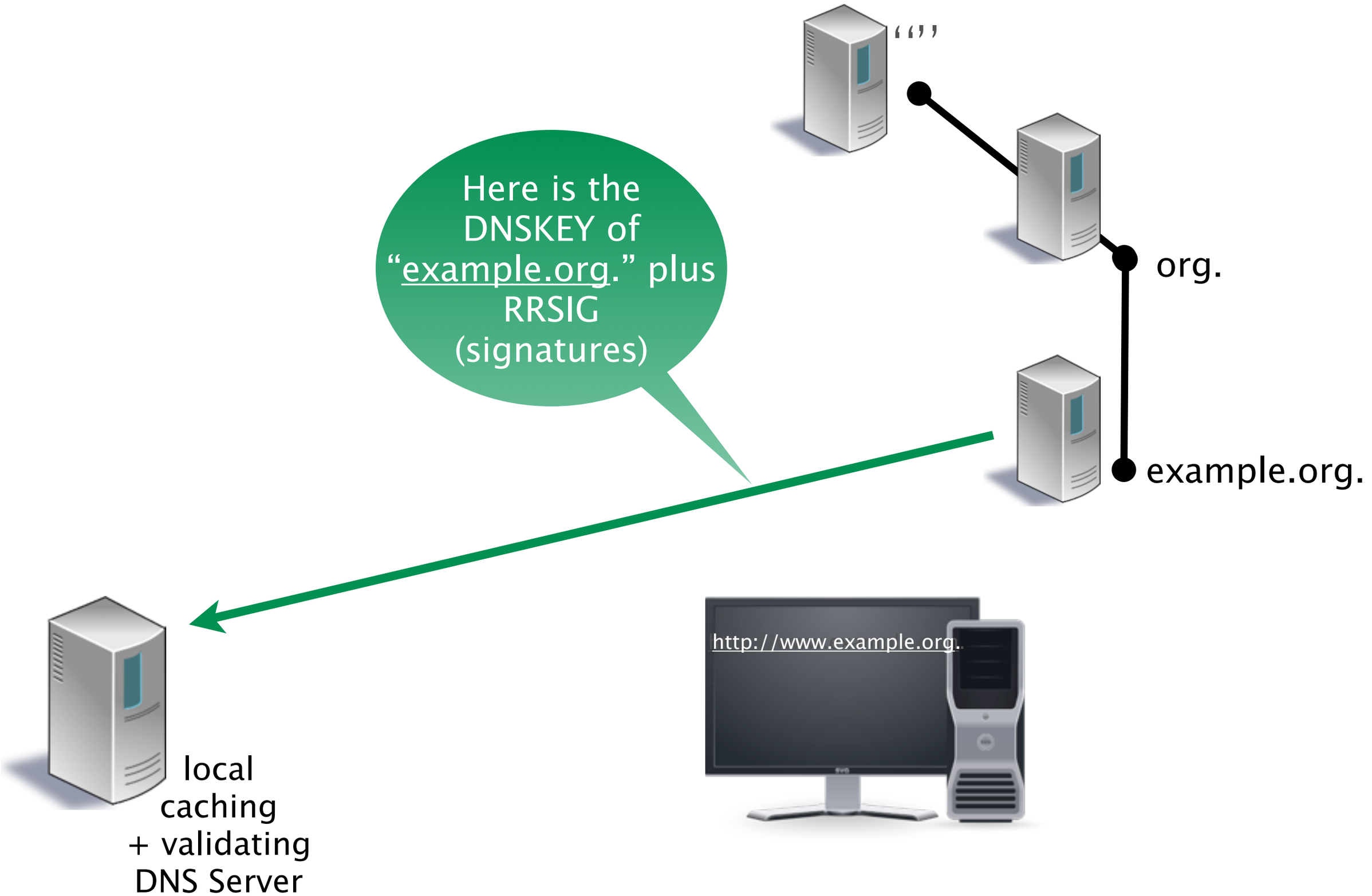
local caching + validating DNS Server

DNSSEC Name Resolution

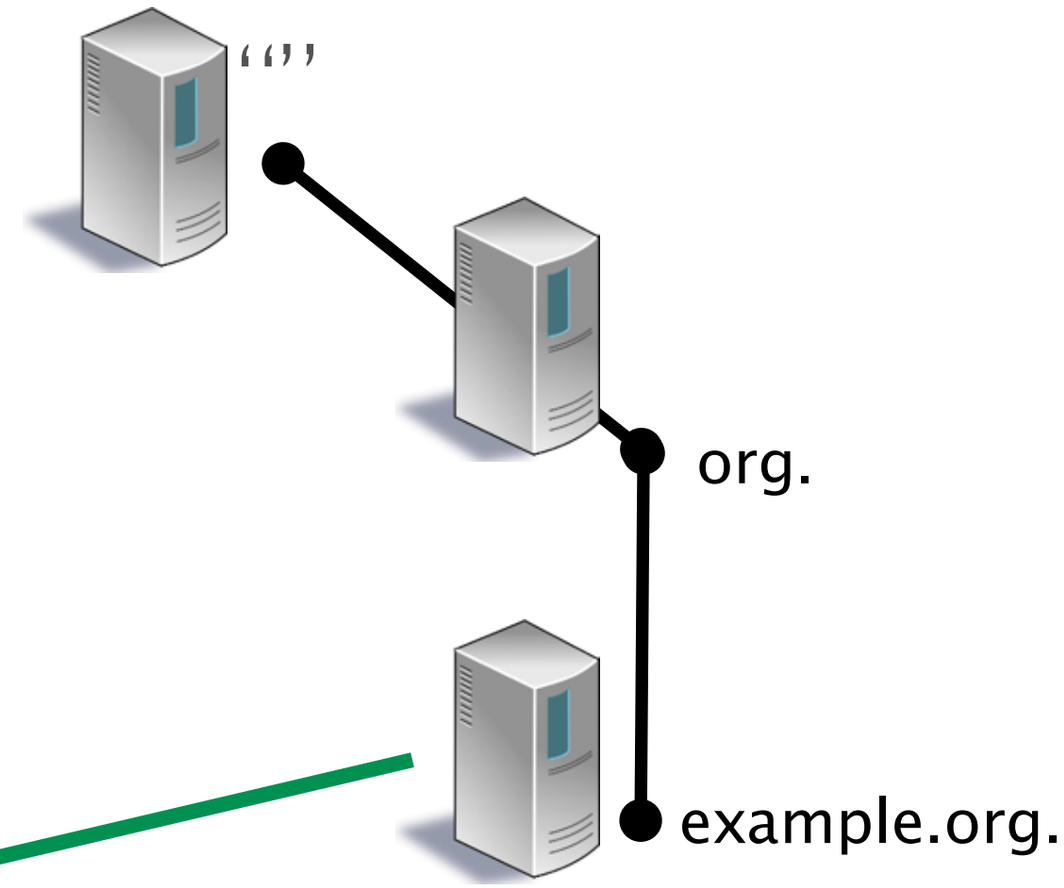


local
caching
+ validating
DNS Server

DNSSEC Name Resolution



DNSSEC Name Resolution

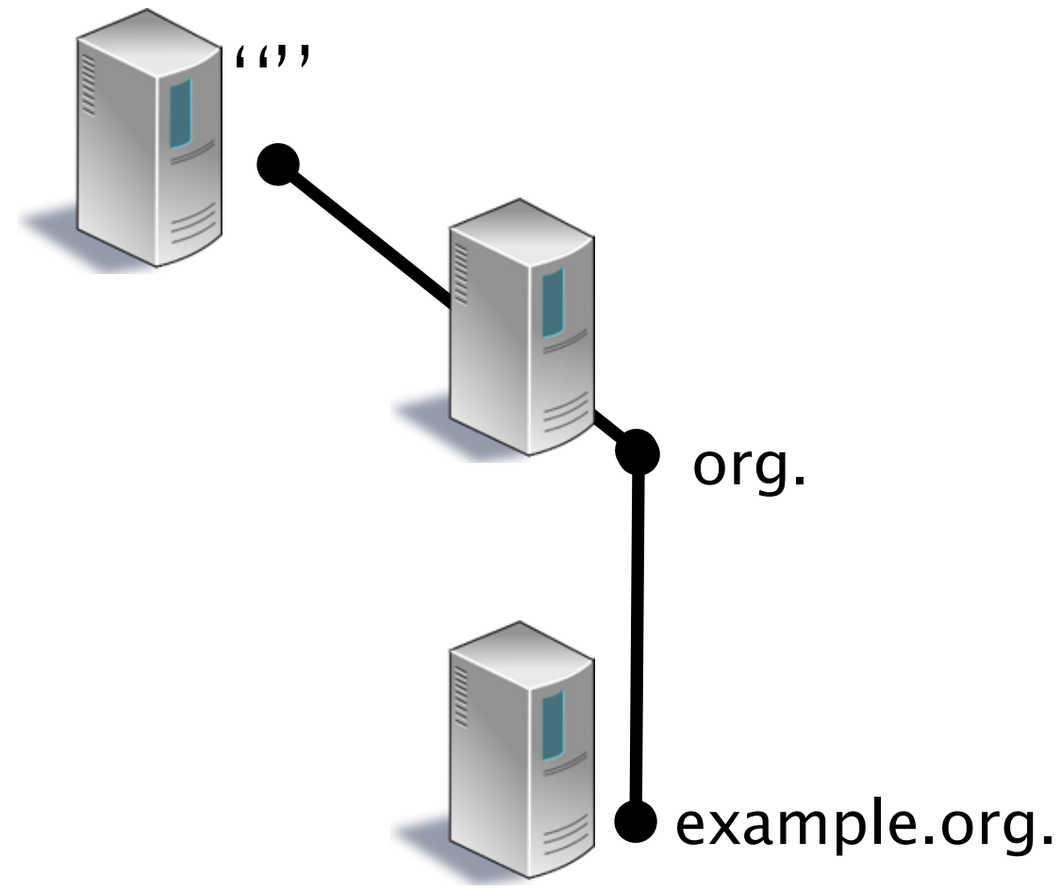


Here is the DNSKEY of “example.org.” plus RRSIG (signatures)

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑

local caching + validating DNS Server

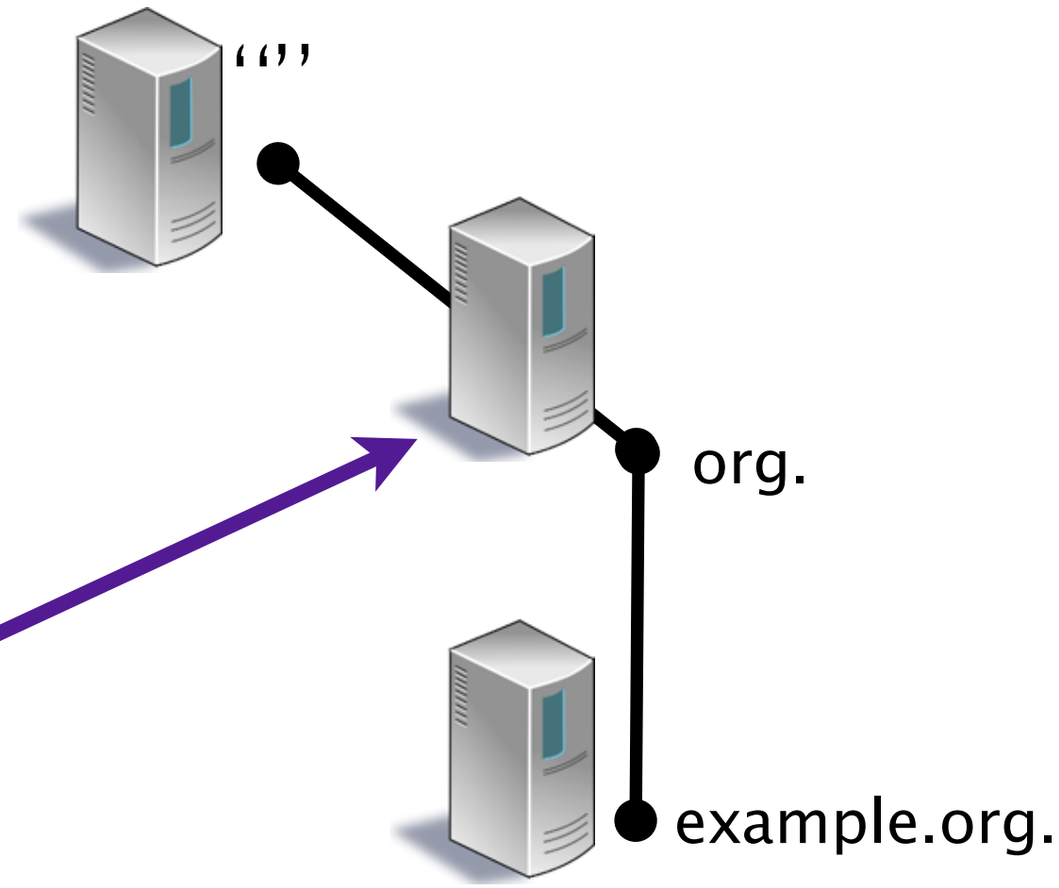
DNSSEC Name Resolution



Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑

local
caching
+ validating
DNS Server

DNSSEC Name Resolution

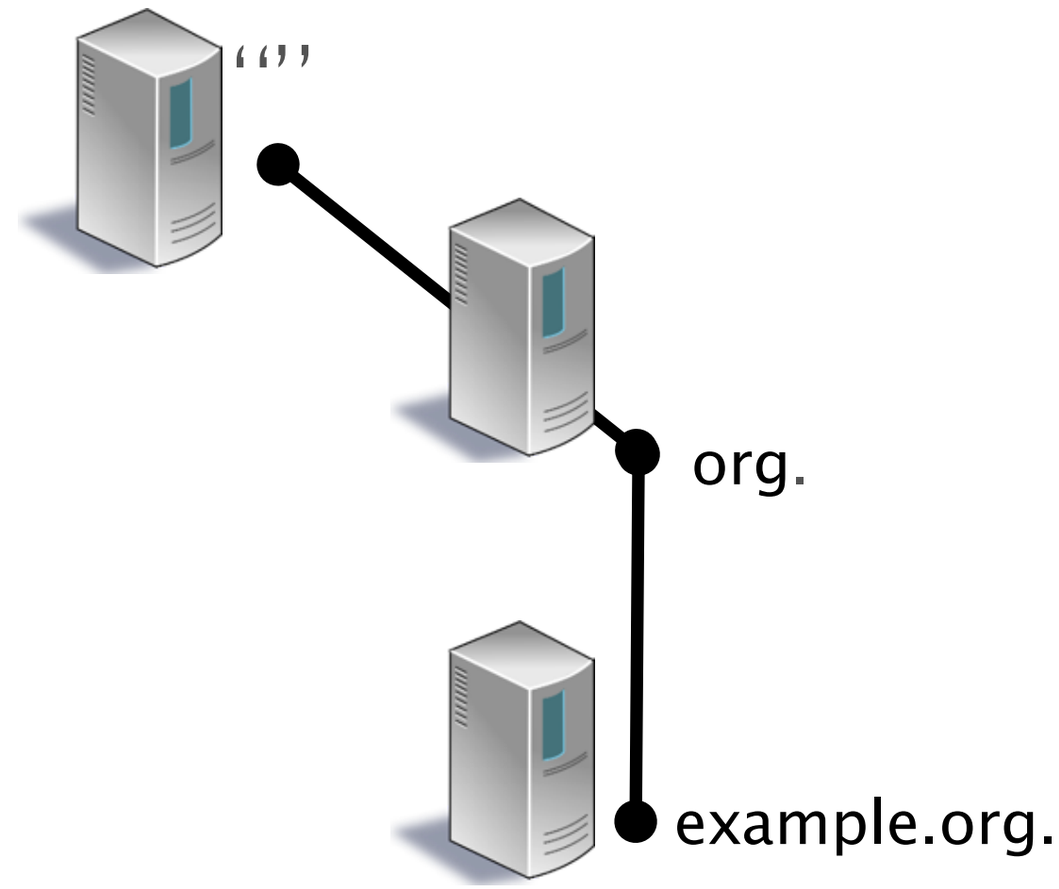


What is the DS of example.org.

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑

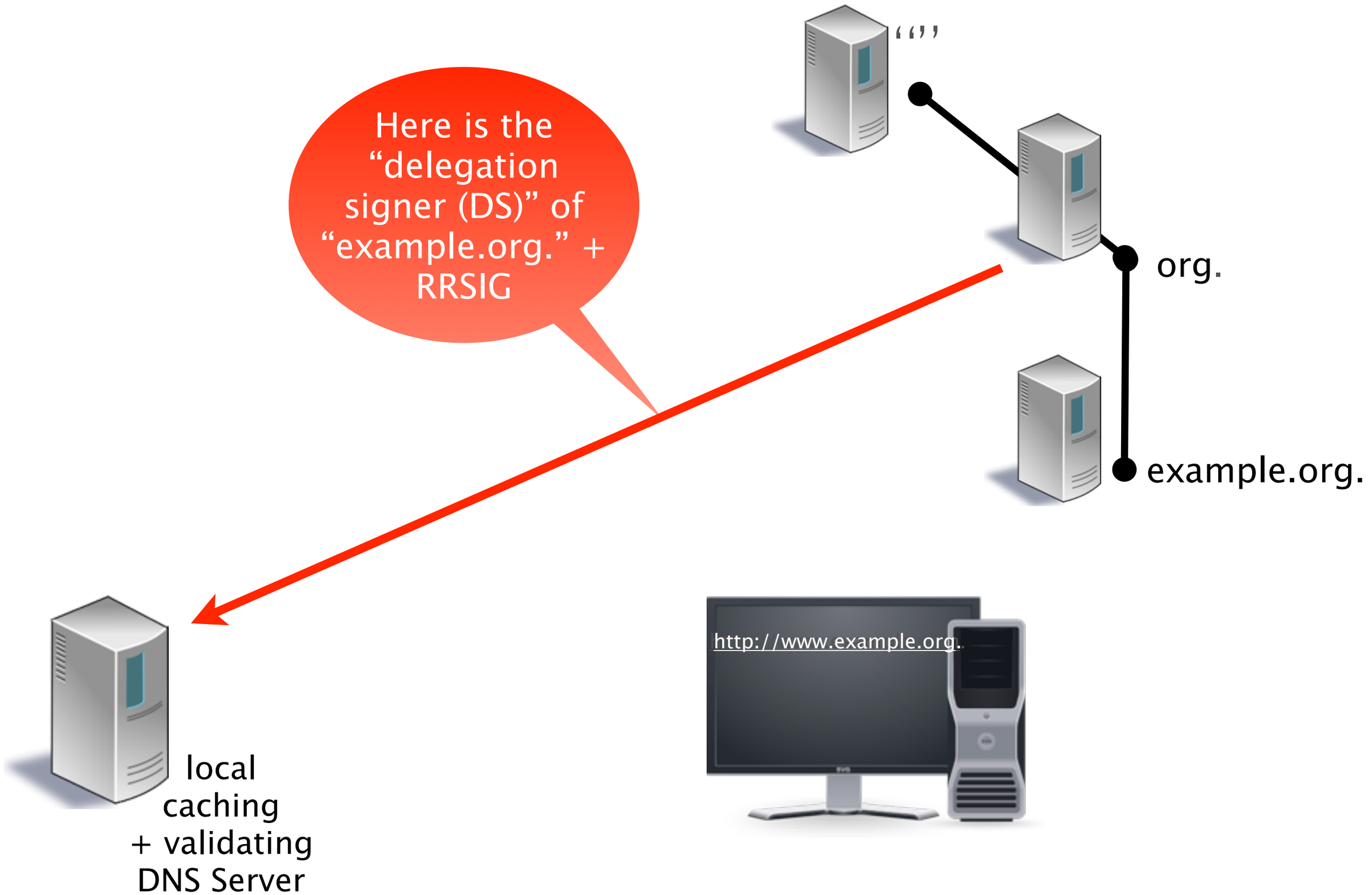
local caching + validating DNS Server

DNSSEC Name Resolution

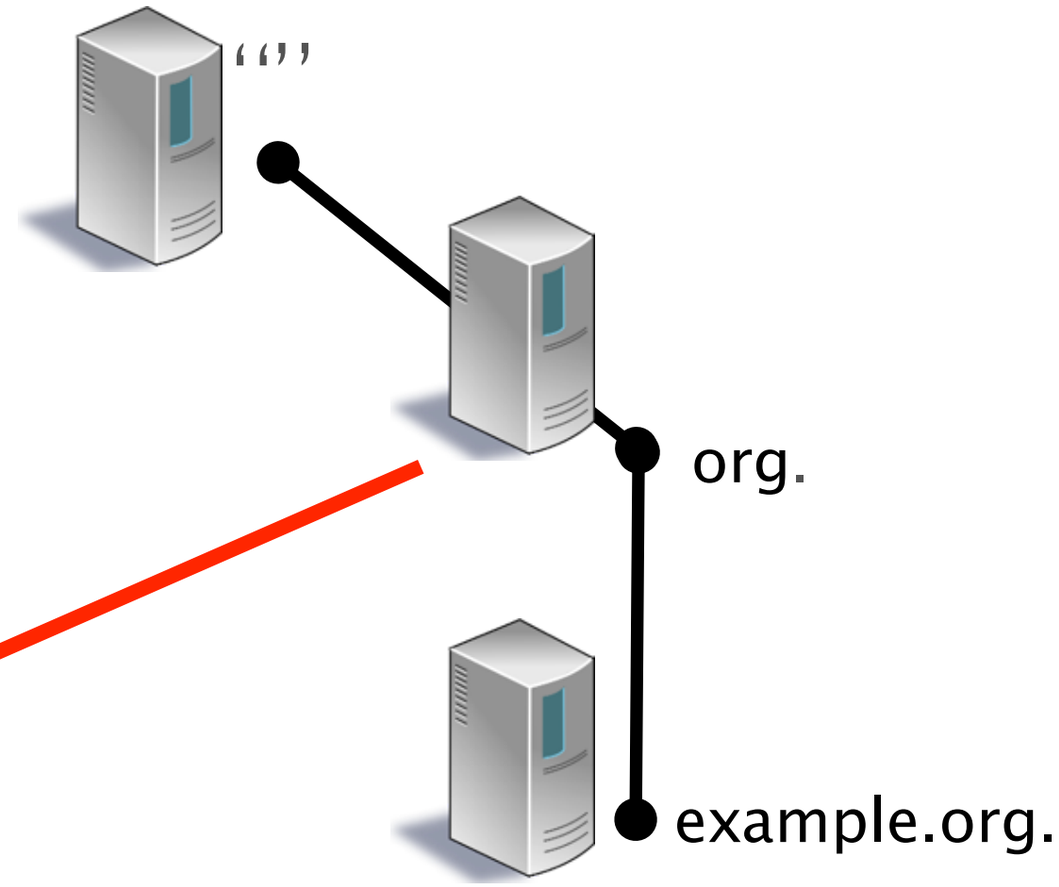


local
caching
+ validating
DNS Server

DNSSEC Name Resolution



DNSSEC Name Resolution

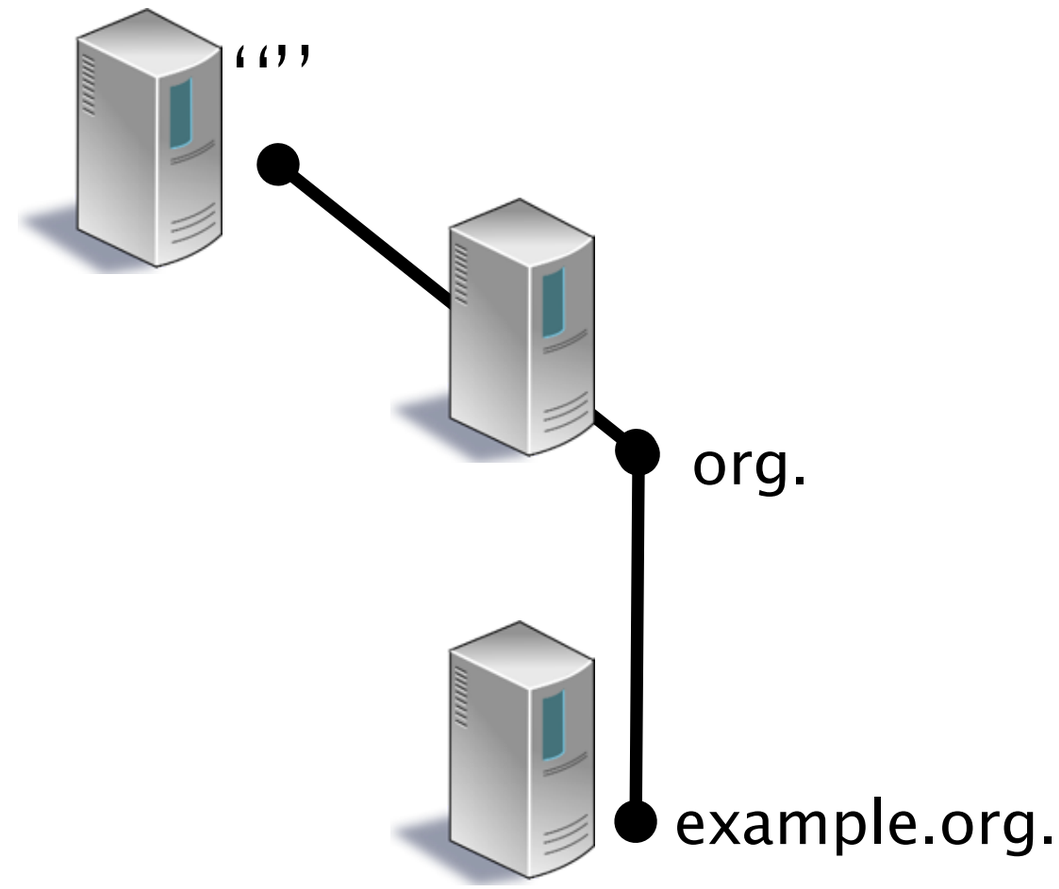


Here is the “delegation signer (DS)” of “example.org.” + RRSIG

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑

local caching + validating DNS Server

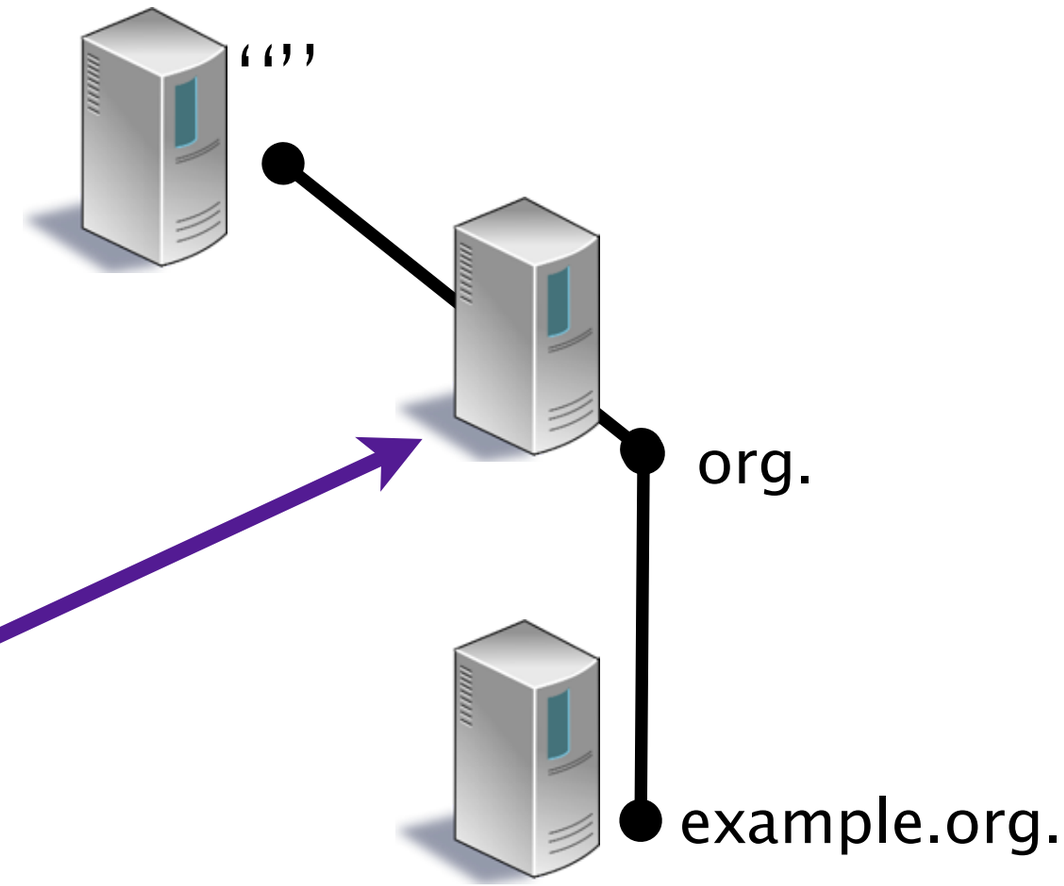
DNSSEC Name Resolution



Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑

local
caching
+ validating
DNS Server

DNSSEC Name Resolution

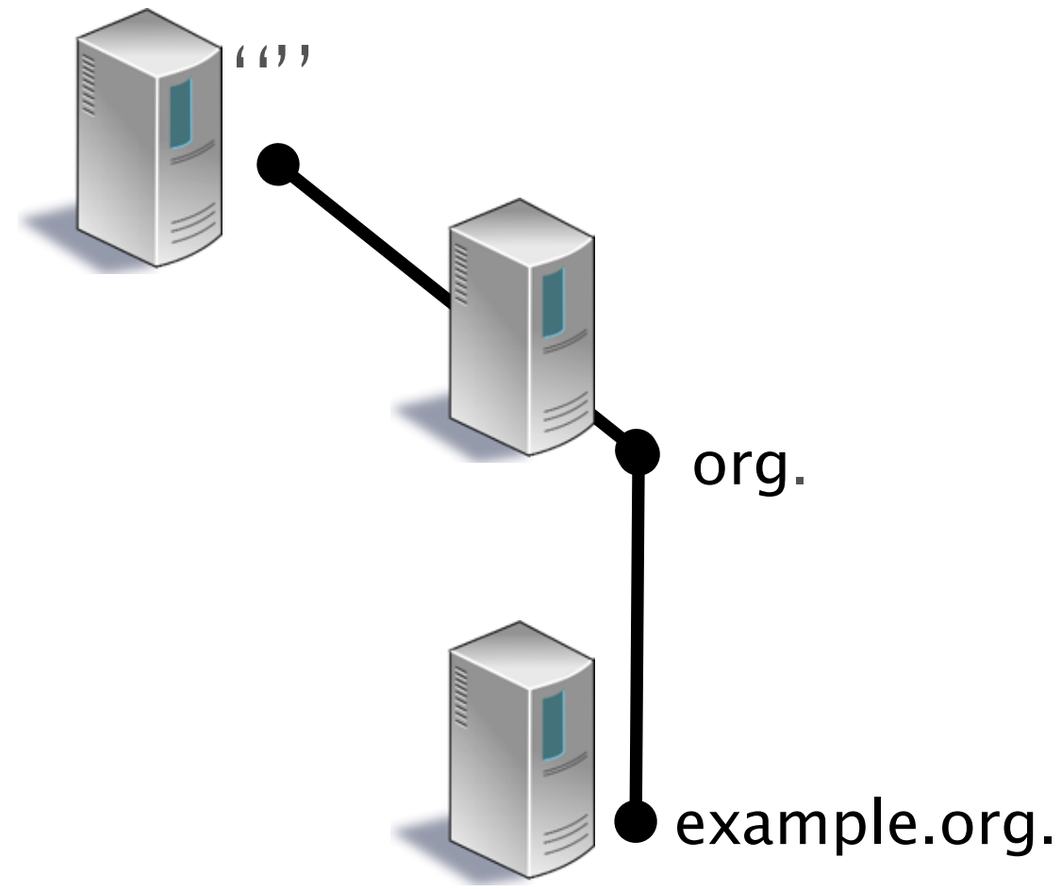


What is the public key (DNSKEY) of “org.”

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑

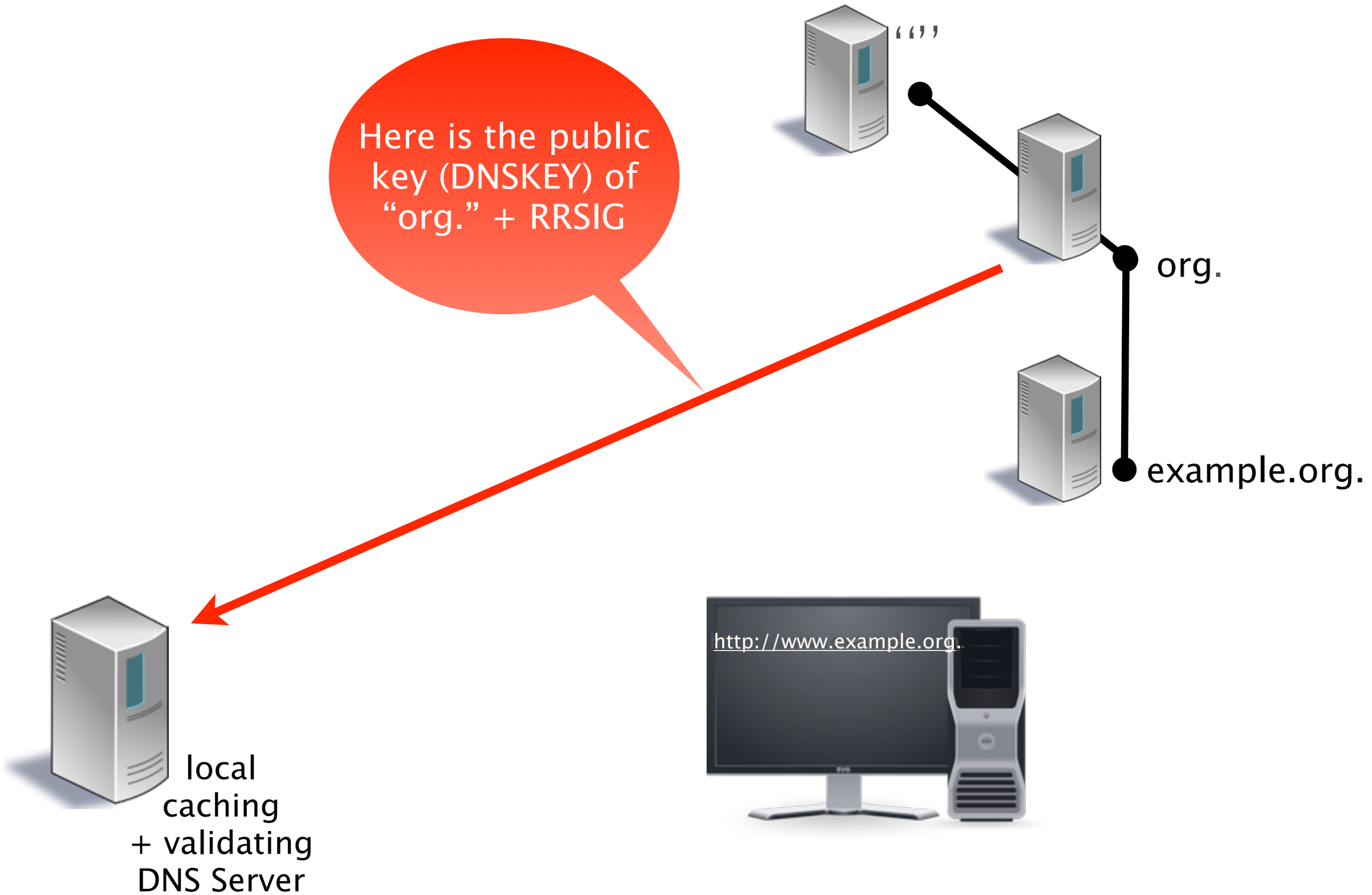
local caching + validating DNS Server

DNSSEC Name Resolution

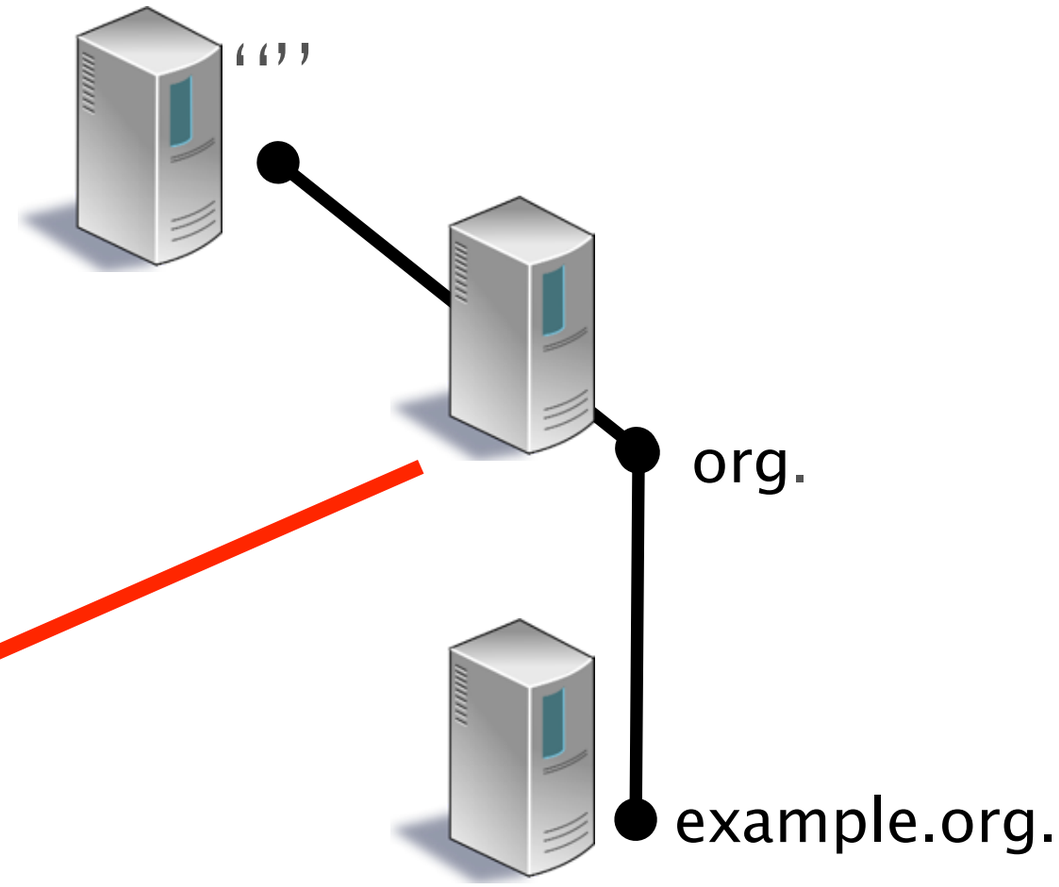


local
caching
+ validating
DNS Server

DNSSEC Name Resolution



DNSSEC Name Resolution

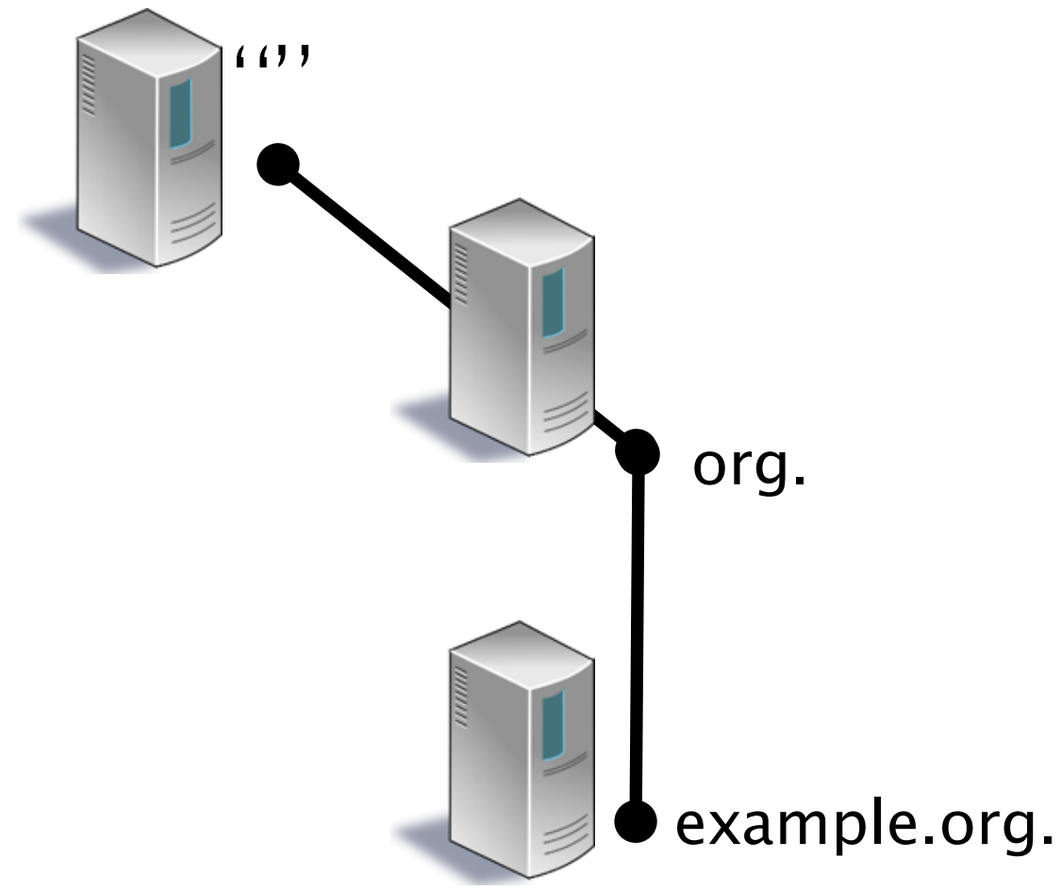


Here is the public key (DNSKEY) of “org.” + RRSIG

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑

local caching + validating DNS Server

DNSSEC Name Resolution



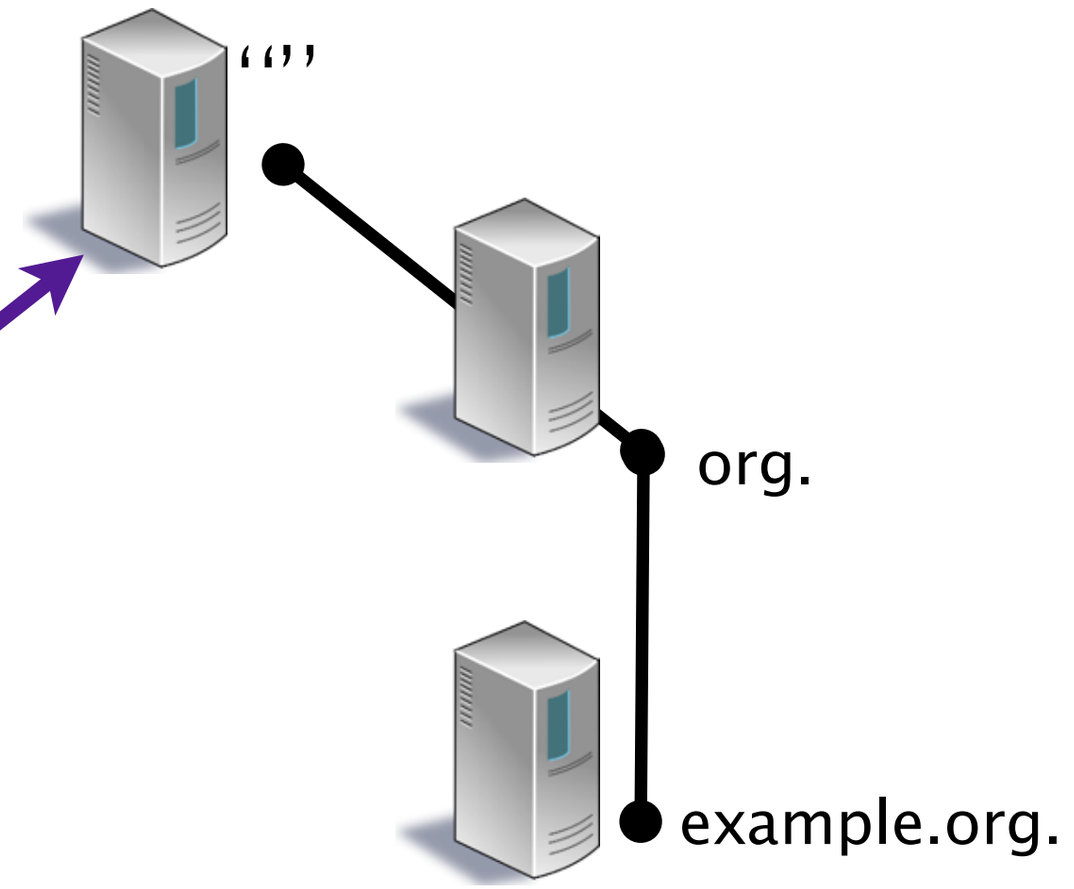
Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑

local
caching
+ validating
DNS Server

DNSSEC Name Resolution

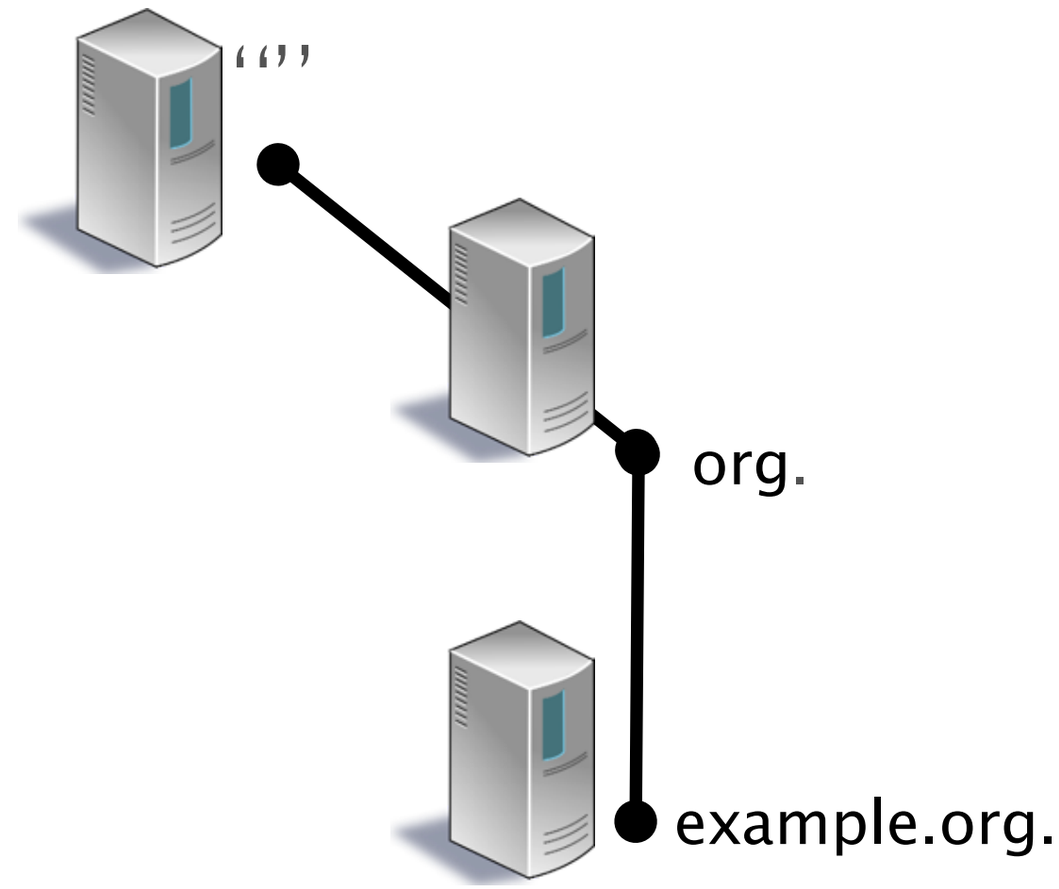
What is the DS of "org."

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑



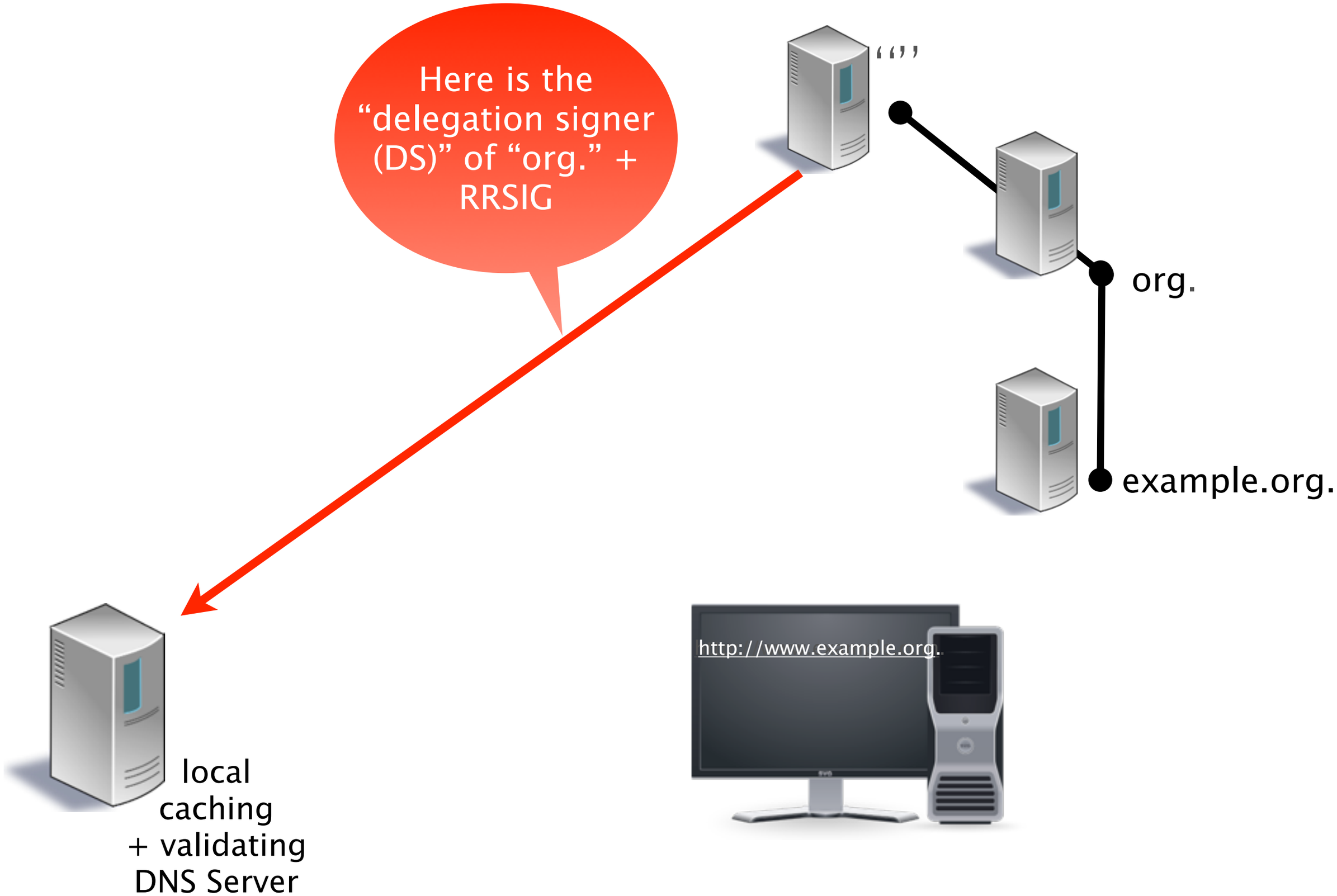
local
caching
+ validating
DNS Server

DNSSEC Name Resolution



local
caching
+ validating
DNS Server

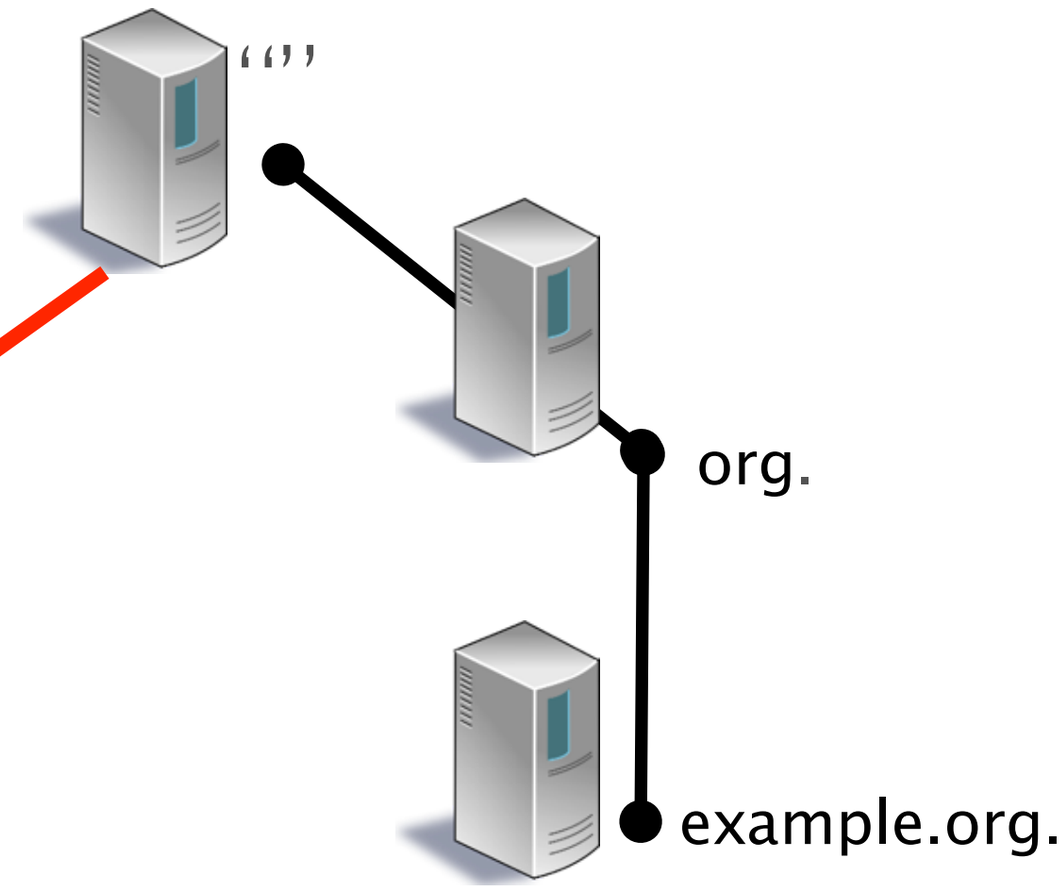
DNSSEC Name Resolution



DNSSEC Name Resolution

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑

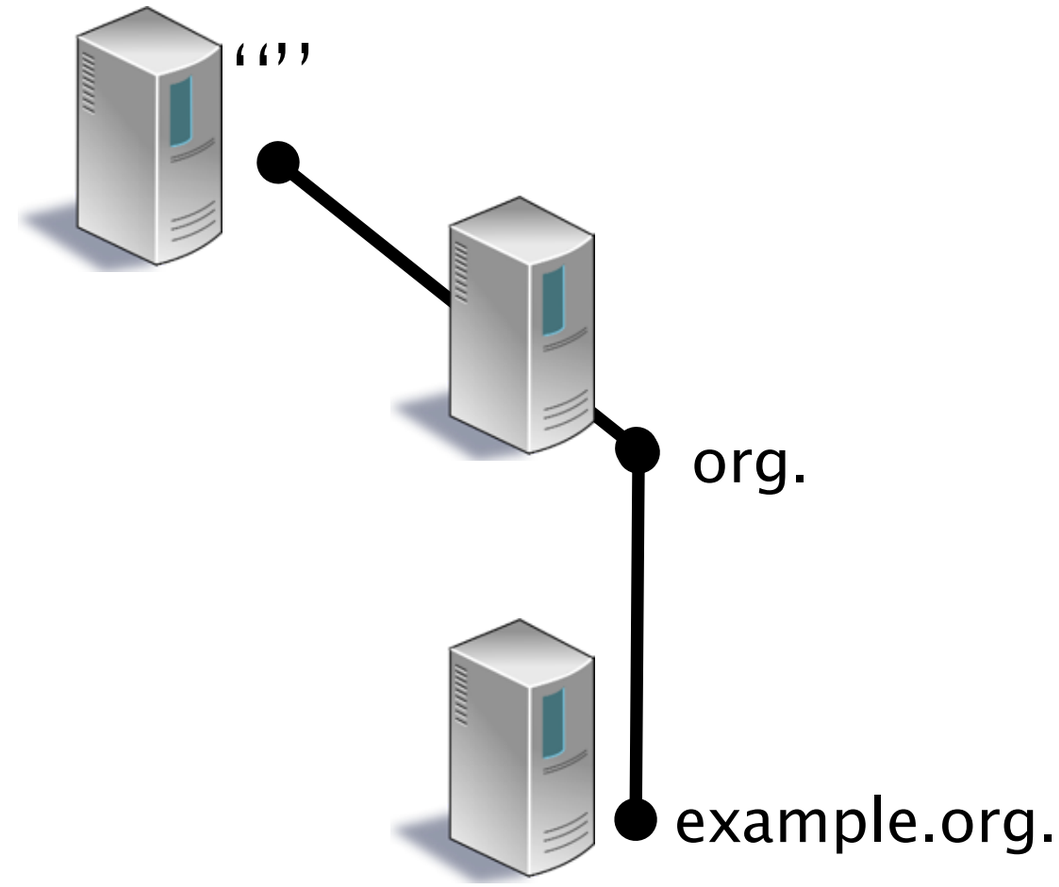
Here is the "delegation signer (DS)" of "org." + RRSIG



local caching + validating DNS Server

DNSSEC Name Resolution

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑

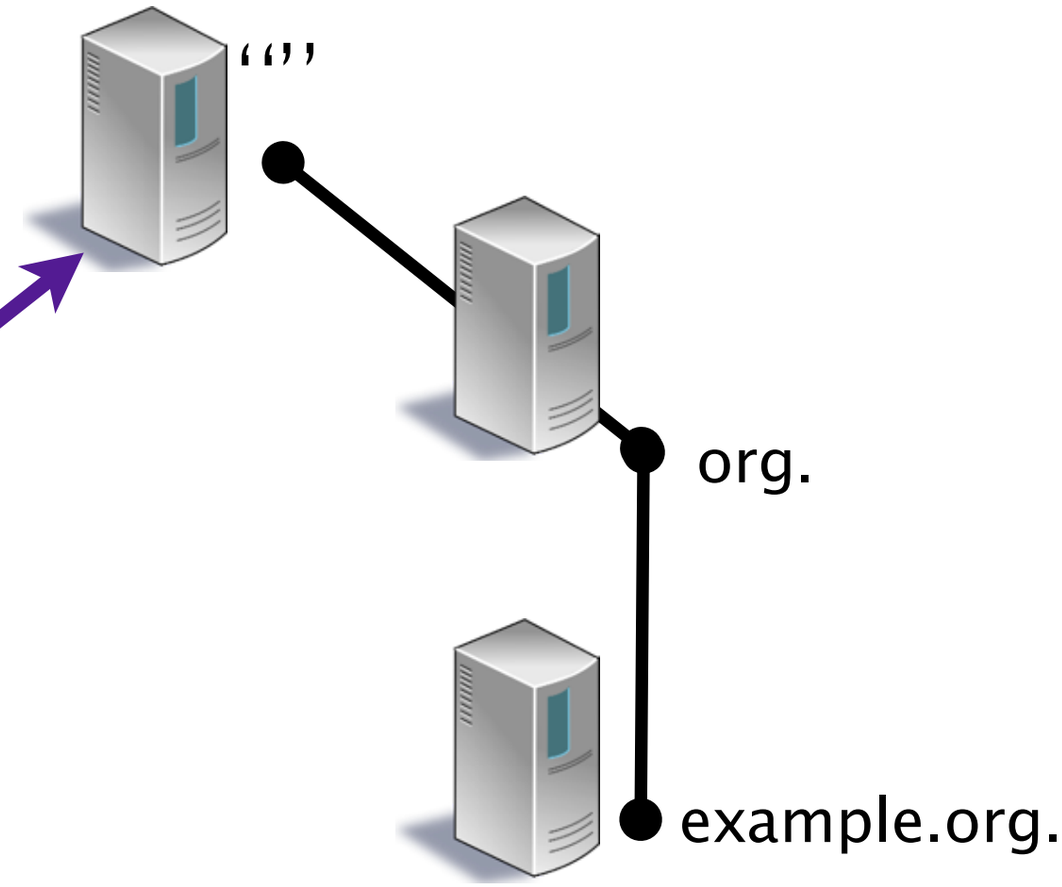


local
caching
+ validating
DNS Server

DNSSEC Name Resolution

What is the public key (DNSKEY) of “ ”

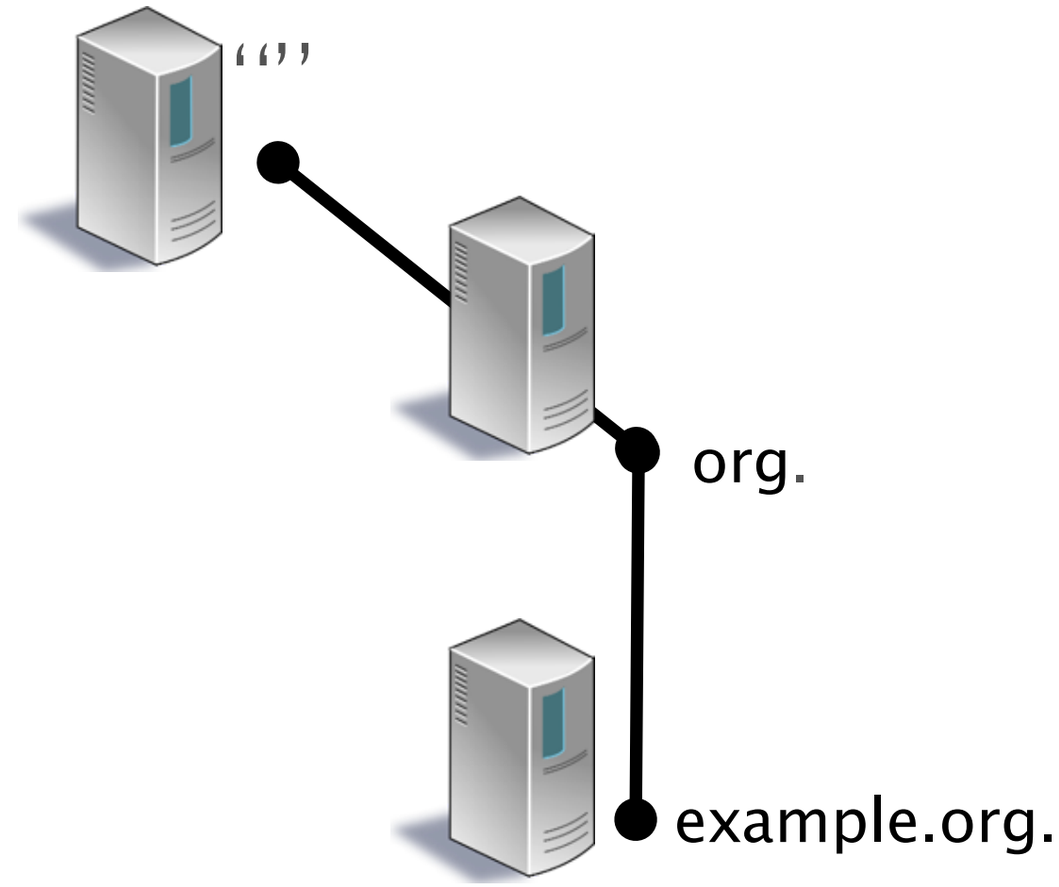
Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑



local
caching
+ validating
DNS Server

DNSSEC Name Resolution

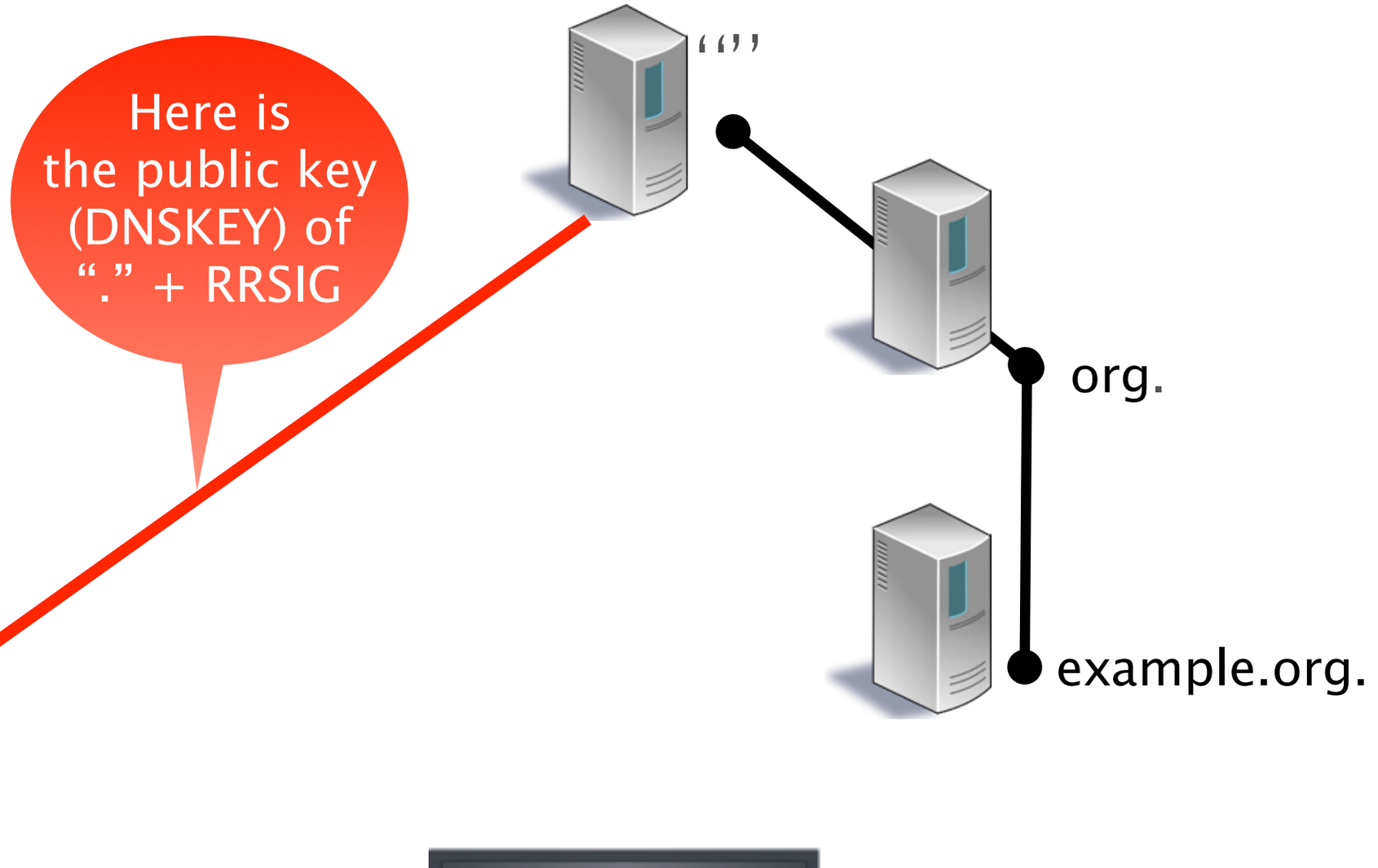
Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑
. DNSKEY	public key
. RRSIG	signature ↑



local
caching
+ validating
DNS Server

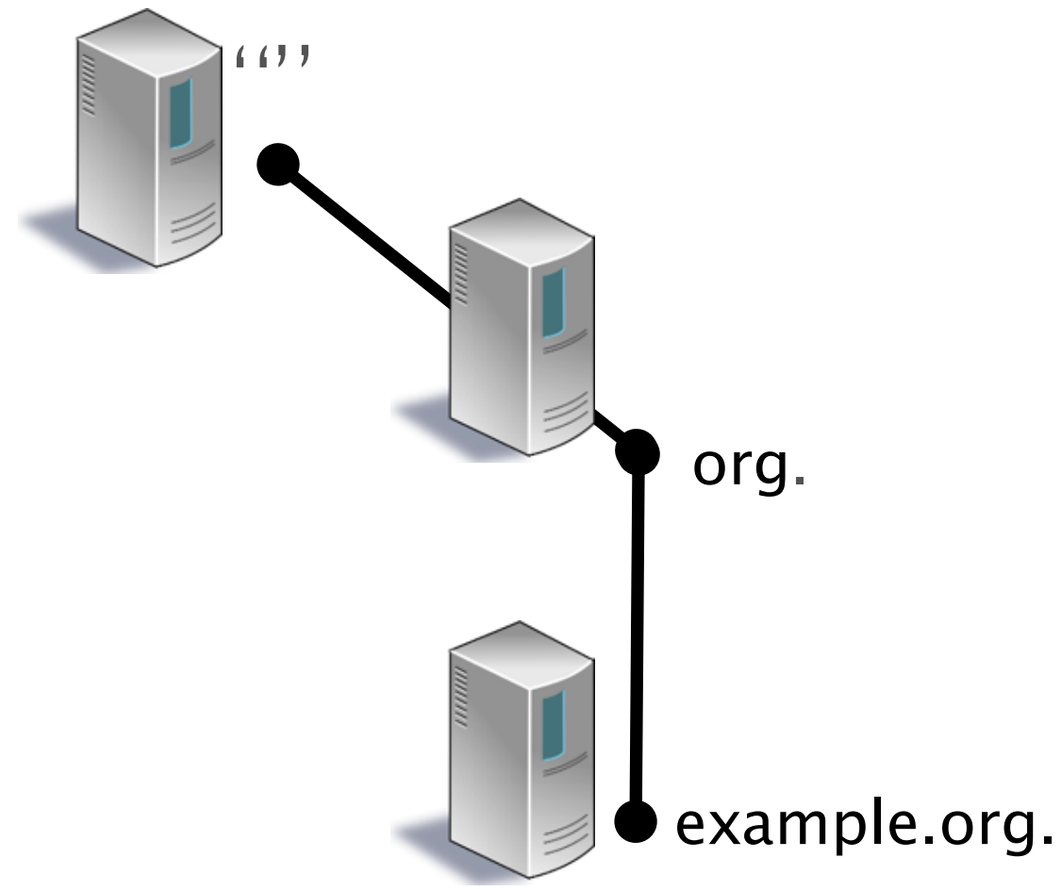
DNSSEC Name Resolution

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑
. DNSKEY	public key
. RRSIG	signature ↑



local caching + validating DNS Server

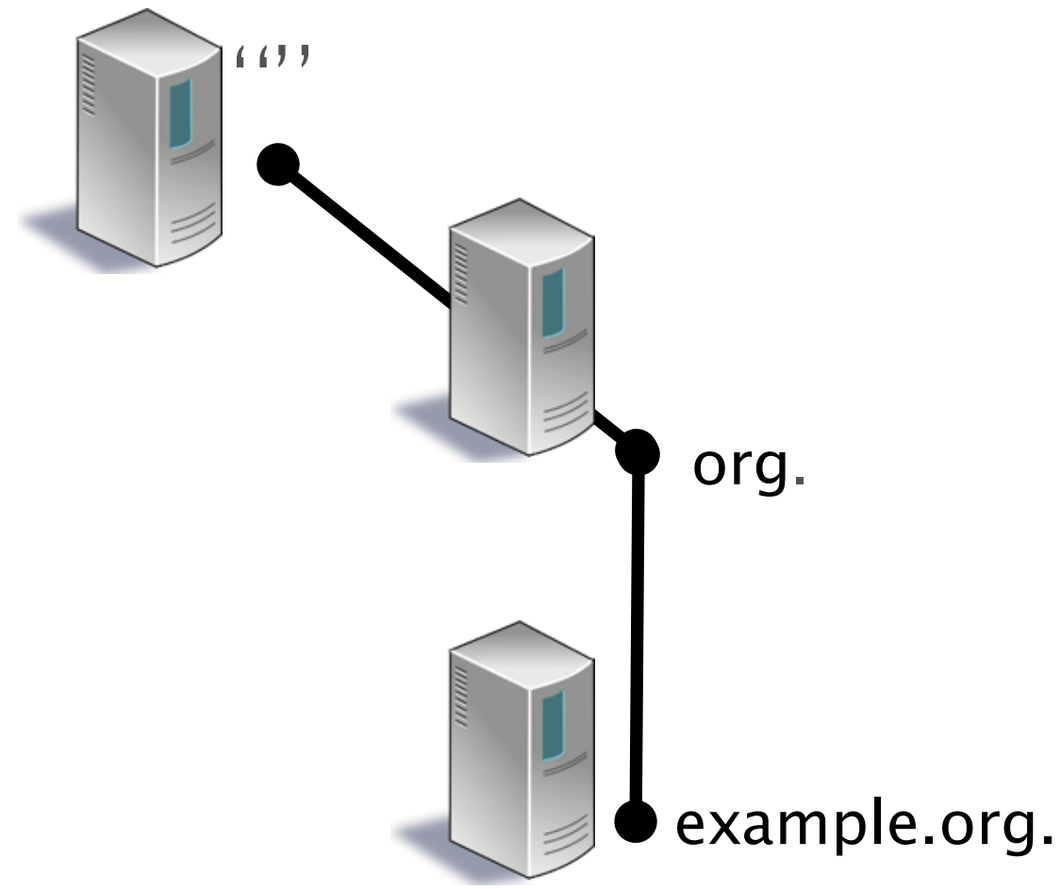
DNSSEC Name Resolution

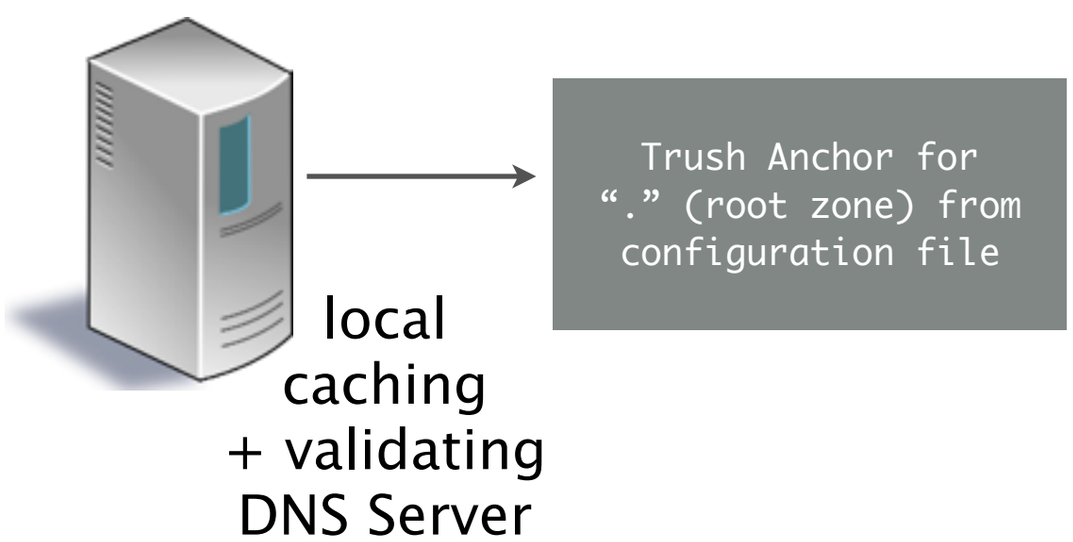


local
caching
+ validating
DNS Server

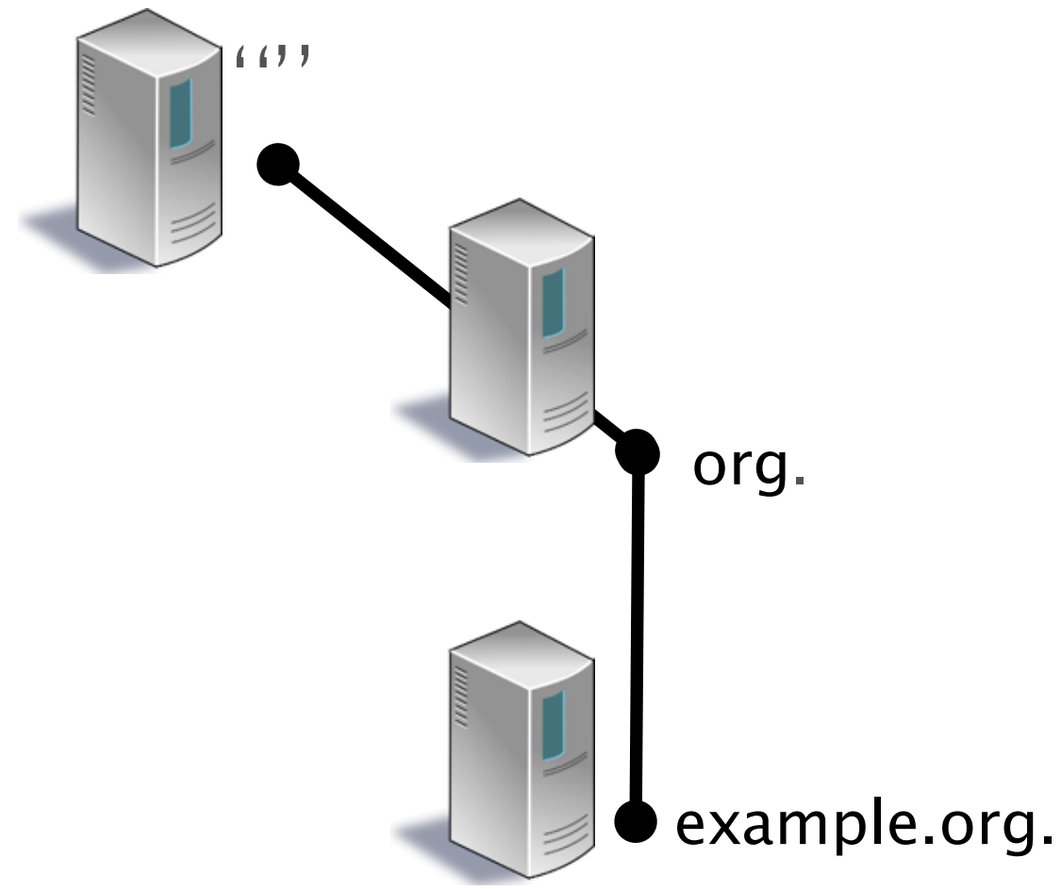
Trush Anchor for
“.” (root zone) from
configuration file

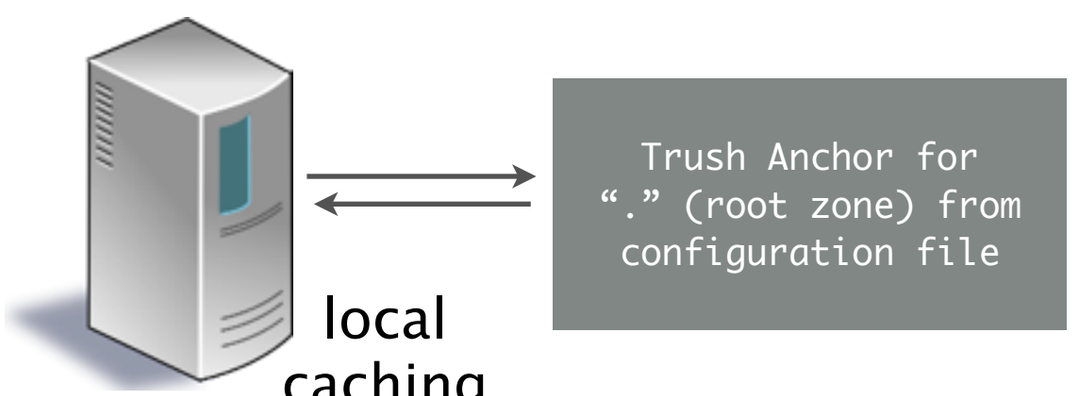
DNSSEC Name Resolution





DNSSEC Name Resolution

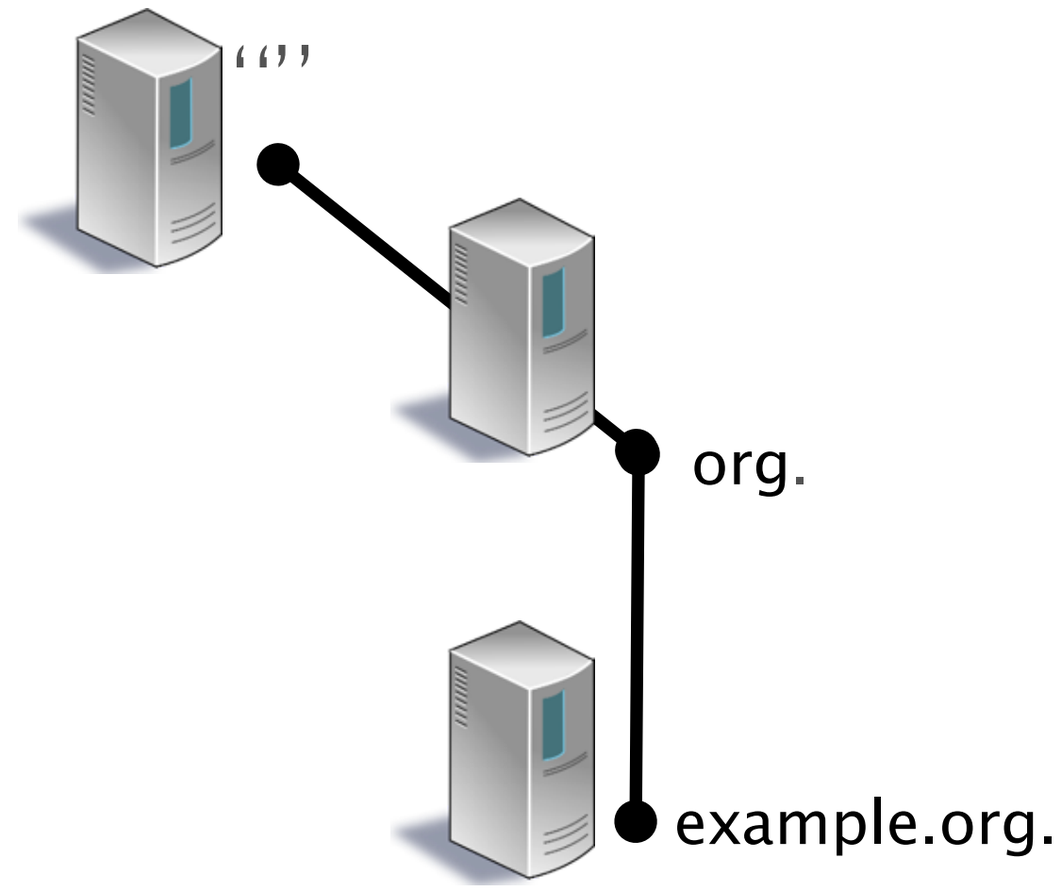


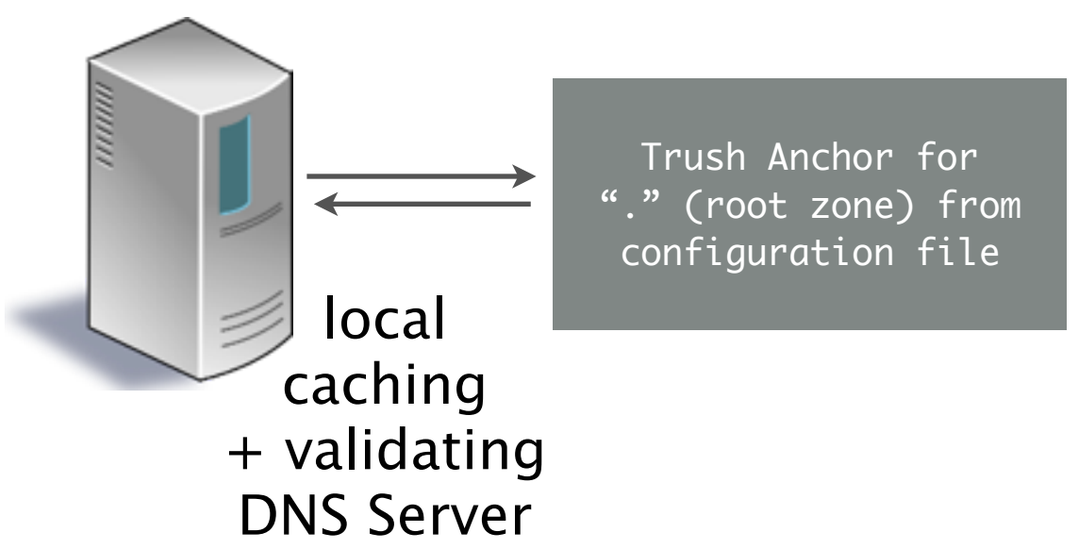


local
caching
+ validating
DNS Server

DNSSEC Name Resolution

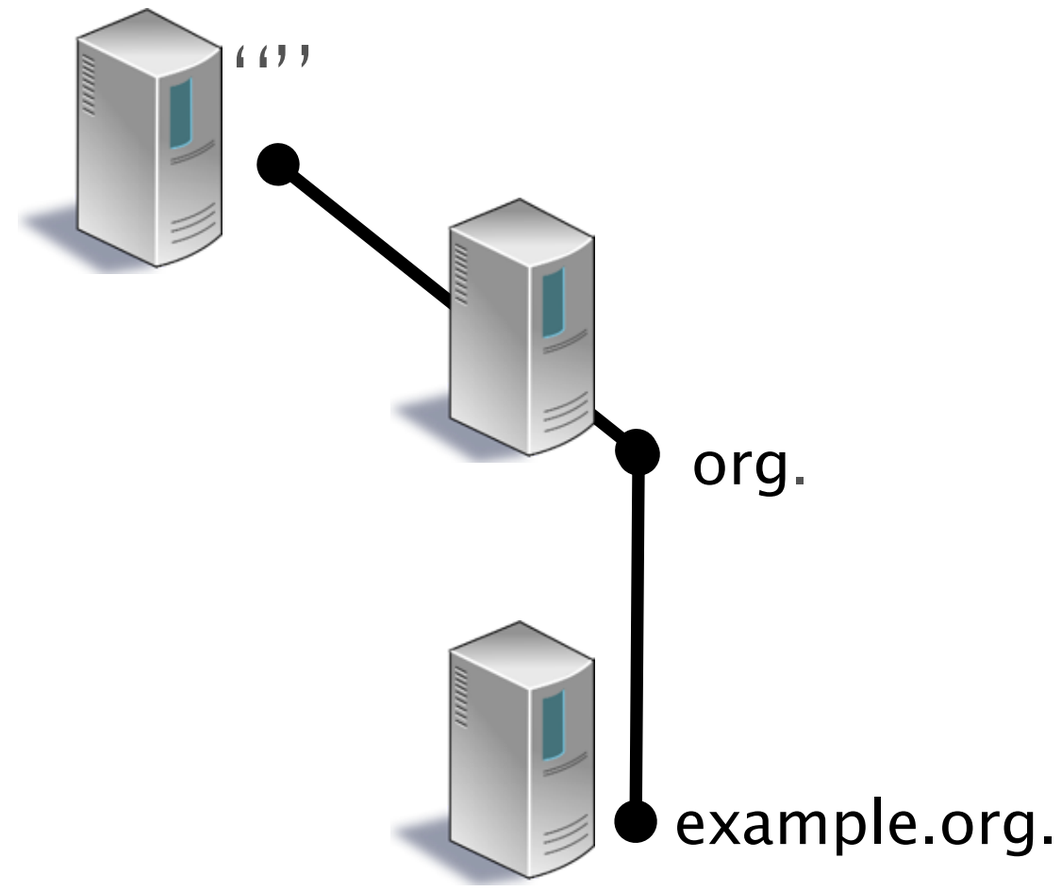
Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑
. DNSKEY	public key
. RRSIG	signature ↑
Trust Anchor for “.”	hash of public key

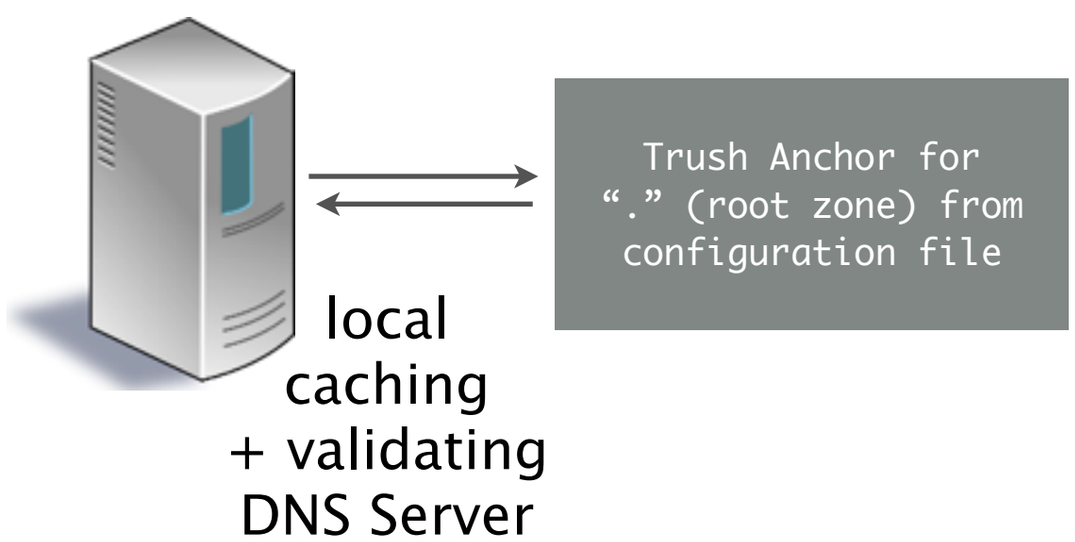




DNSSEC Name Resolution

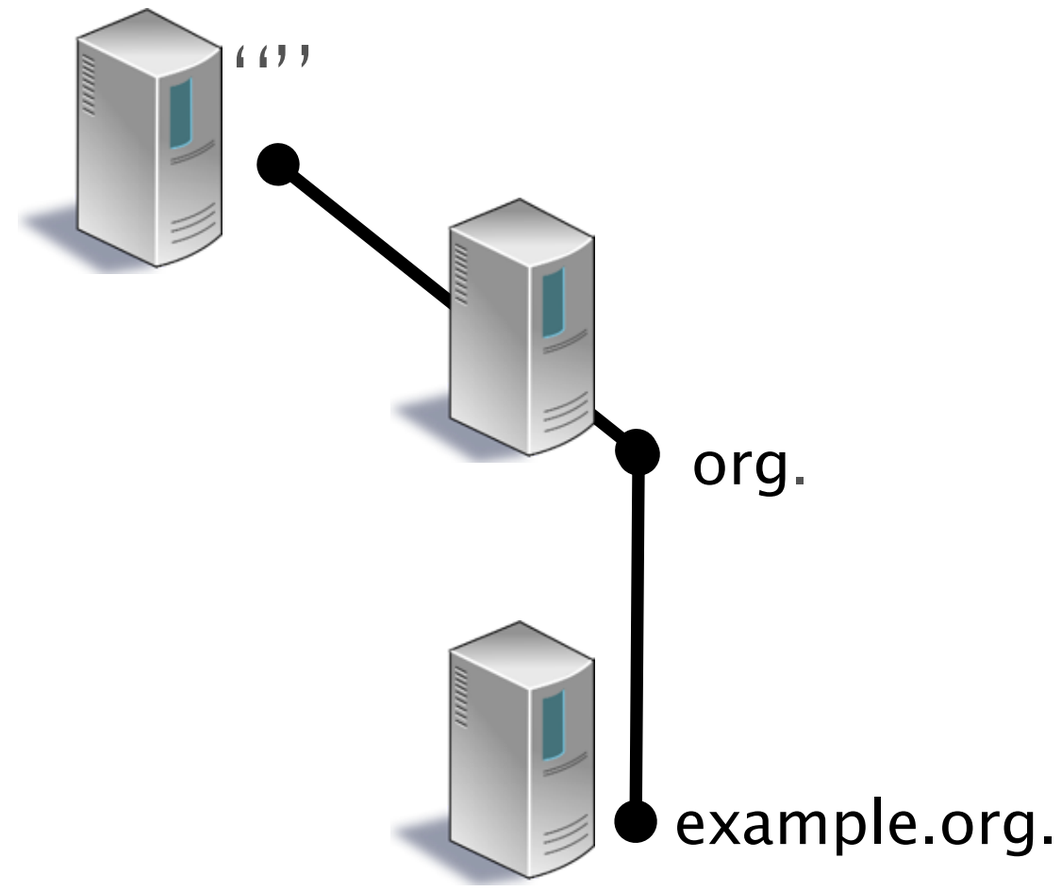
Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑
. DNSKEY	public key
. RRSIG	signature ↑
Trust Anchor for “.”	hash of public key

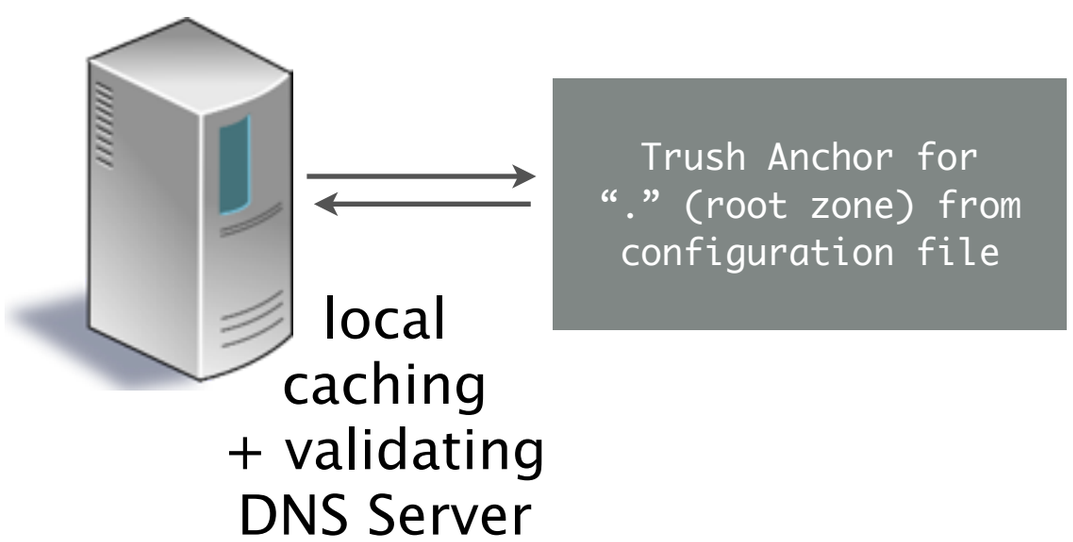




DNSSEC Name Resolution

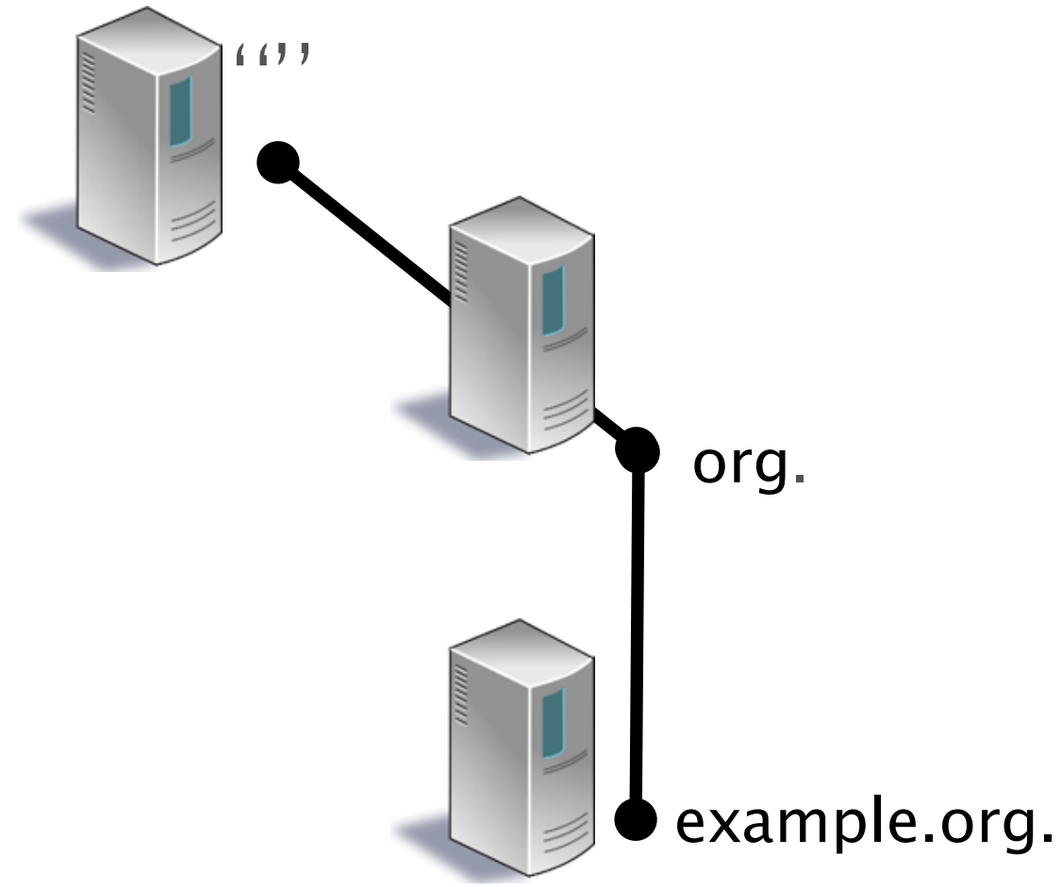
Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑
. DNSKEY	public key ✔
. RRSIG	signature ↑ ✔
Trust Anchor for "."	hash of public key

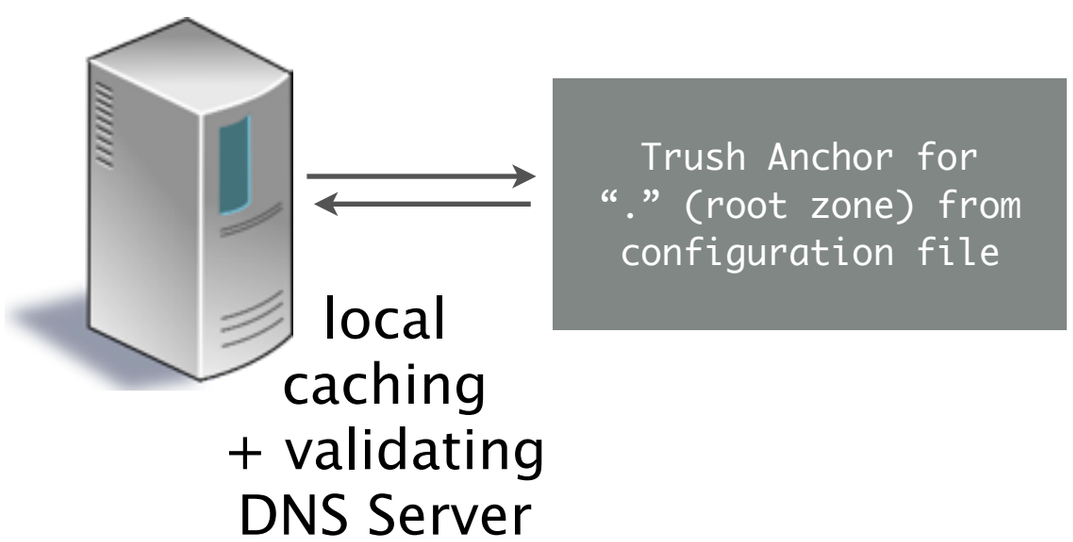




DNSSEC Name Resolution

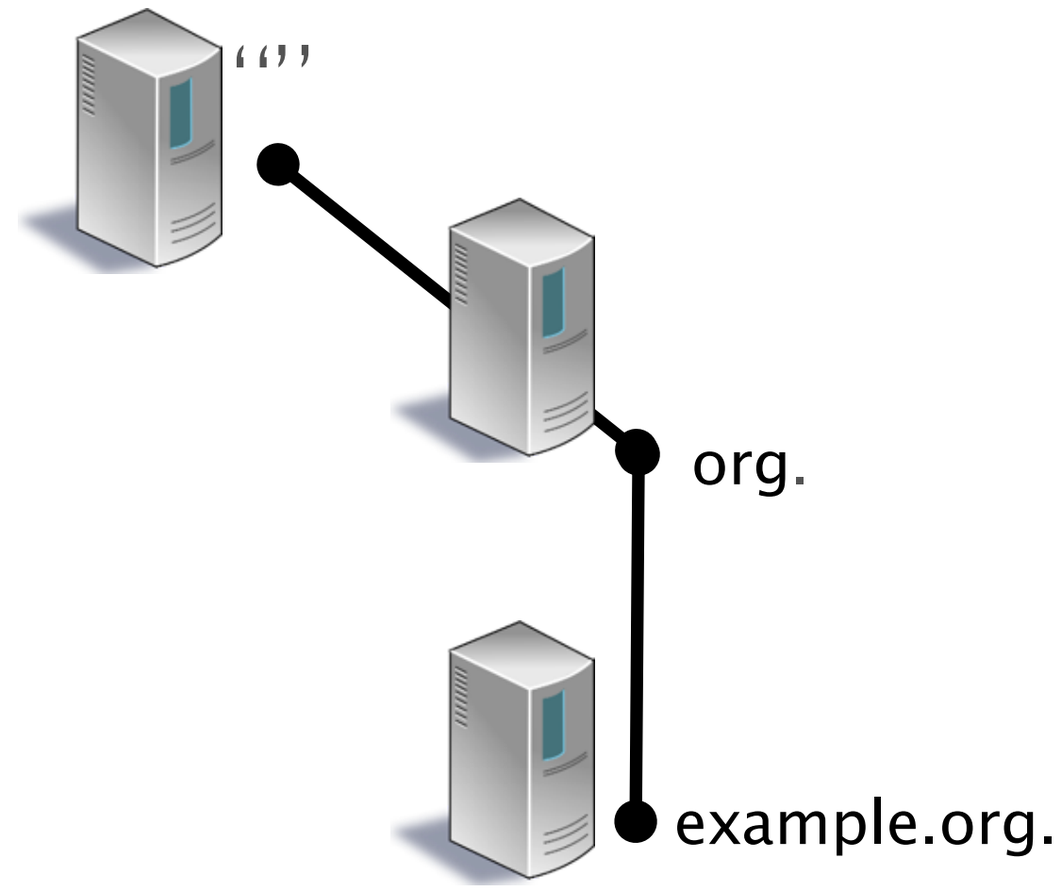
Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑ ✔
. DNSKEY	public key ✔
. RRSIG	signature ↑ ✔
Trust Anchor for “.”	hash of public key

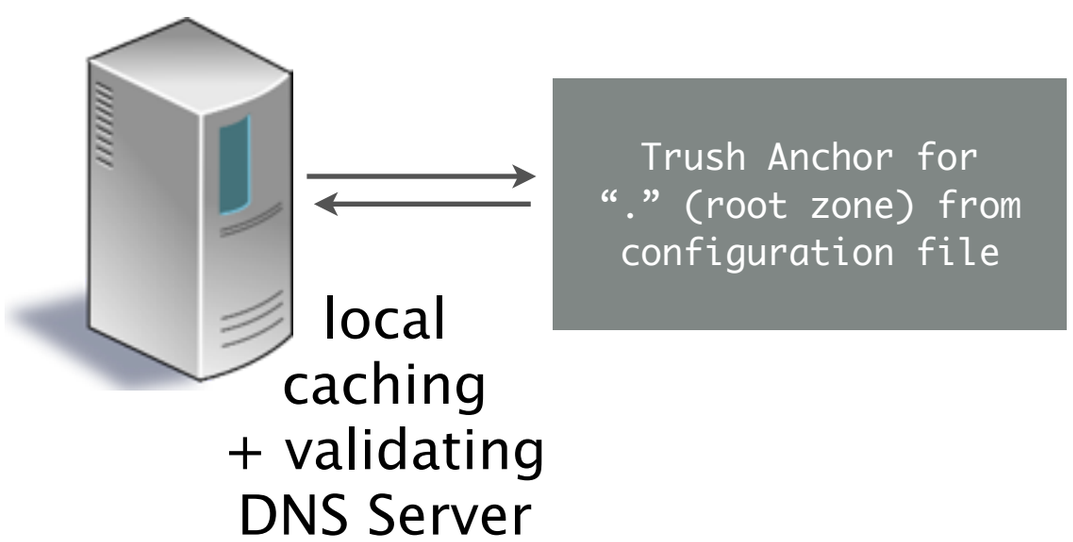




DNSSEC Name Resolution

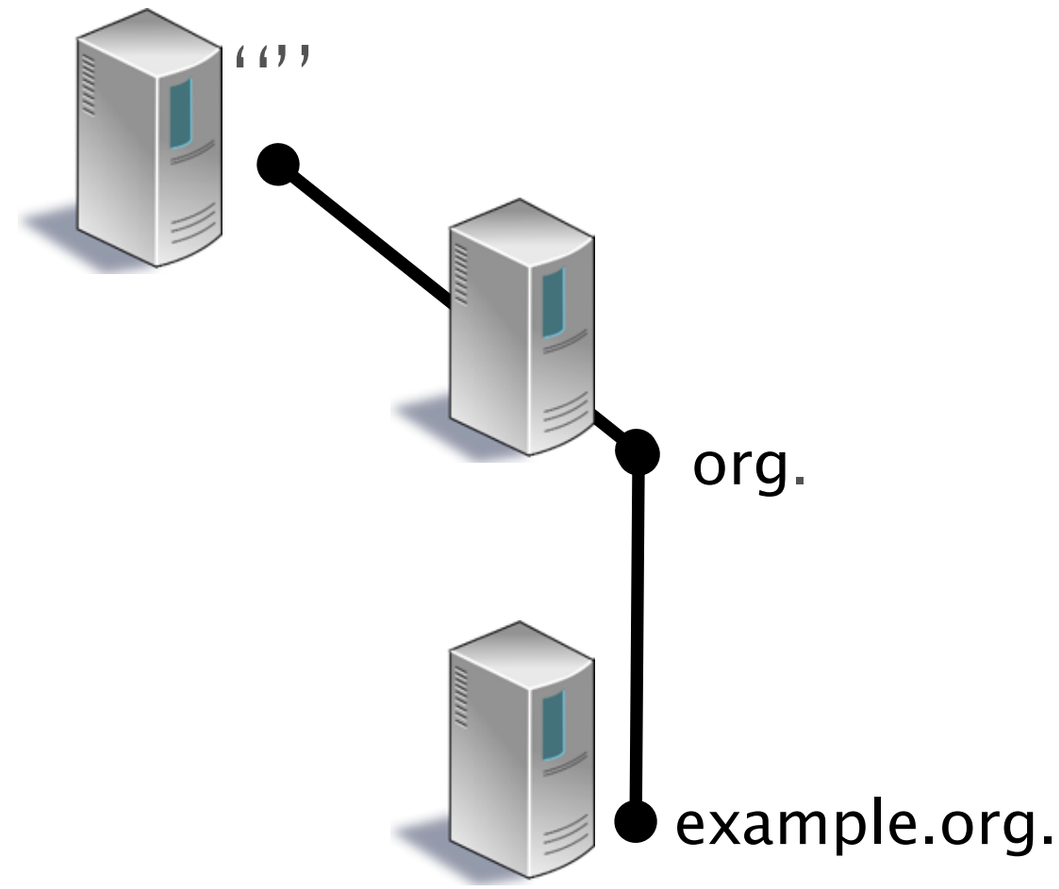
Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key ✔
. RRSIG	signature ↑ ✔
. DNSKEY	public key ✔
. RRSIG	signature ↑ ✔
Trust Anchor for "."	hash of public key

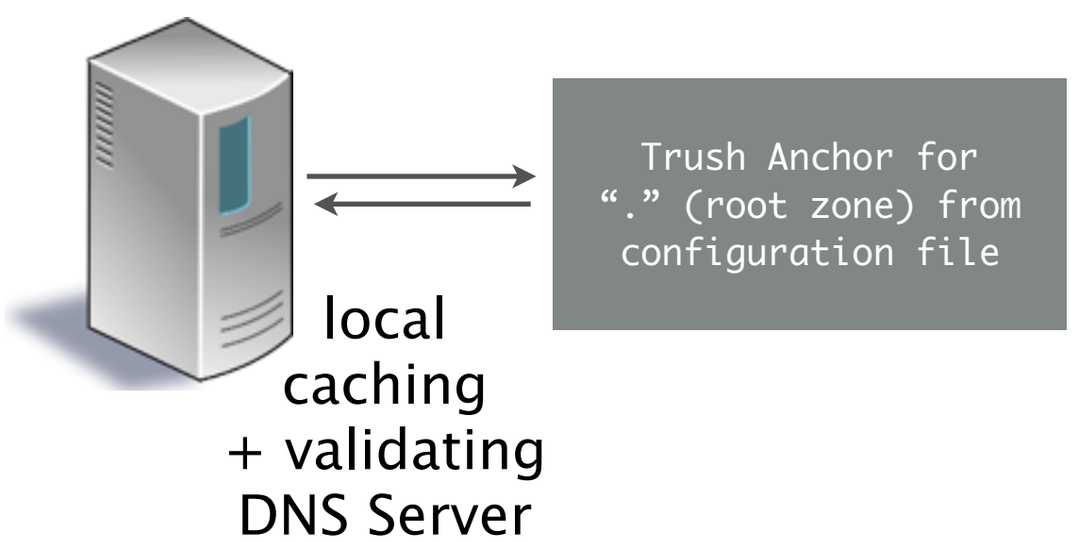




DNSSEC Name Resolution

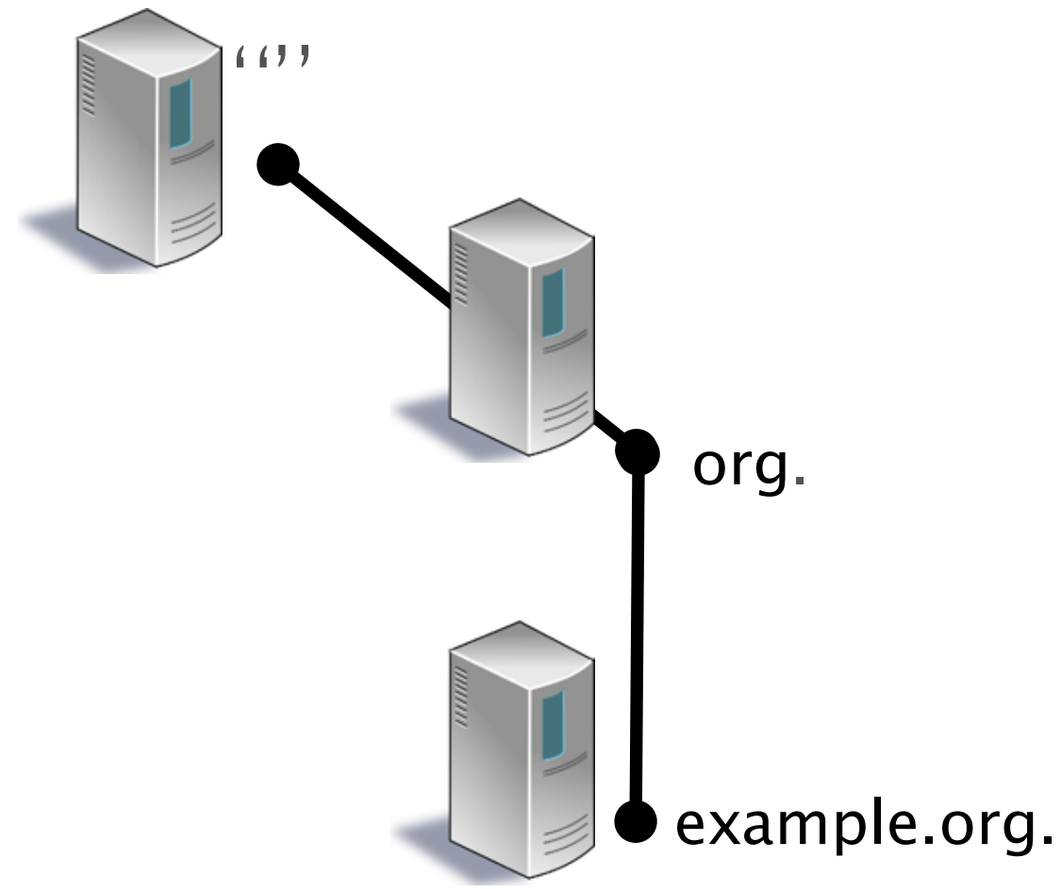
Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑
. DNSKEY	public key
. RRSIG	signature ↑
Trust Anchor for “.”	hash of public key

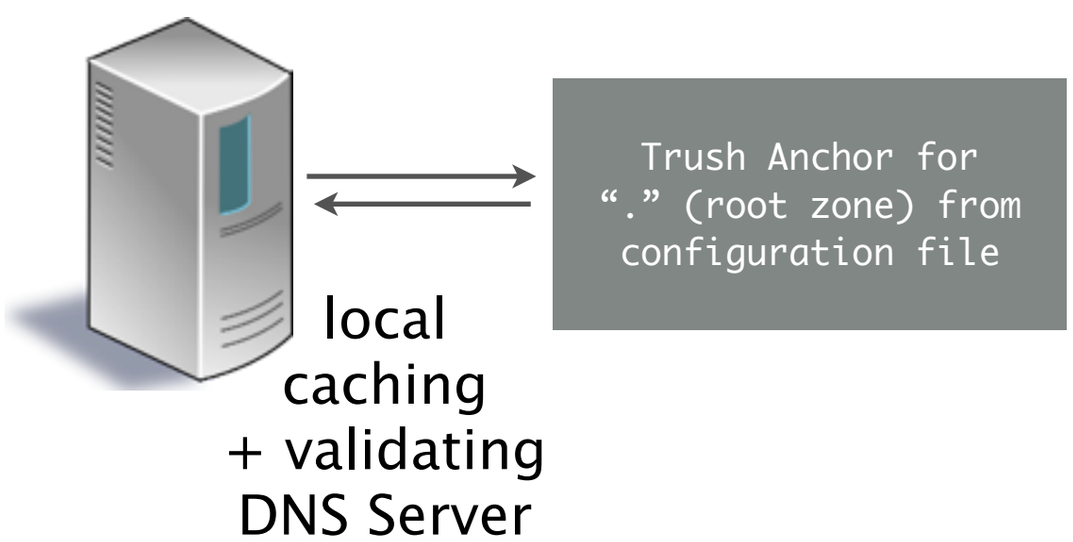




DNSSEC Name Resolution

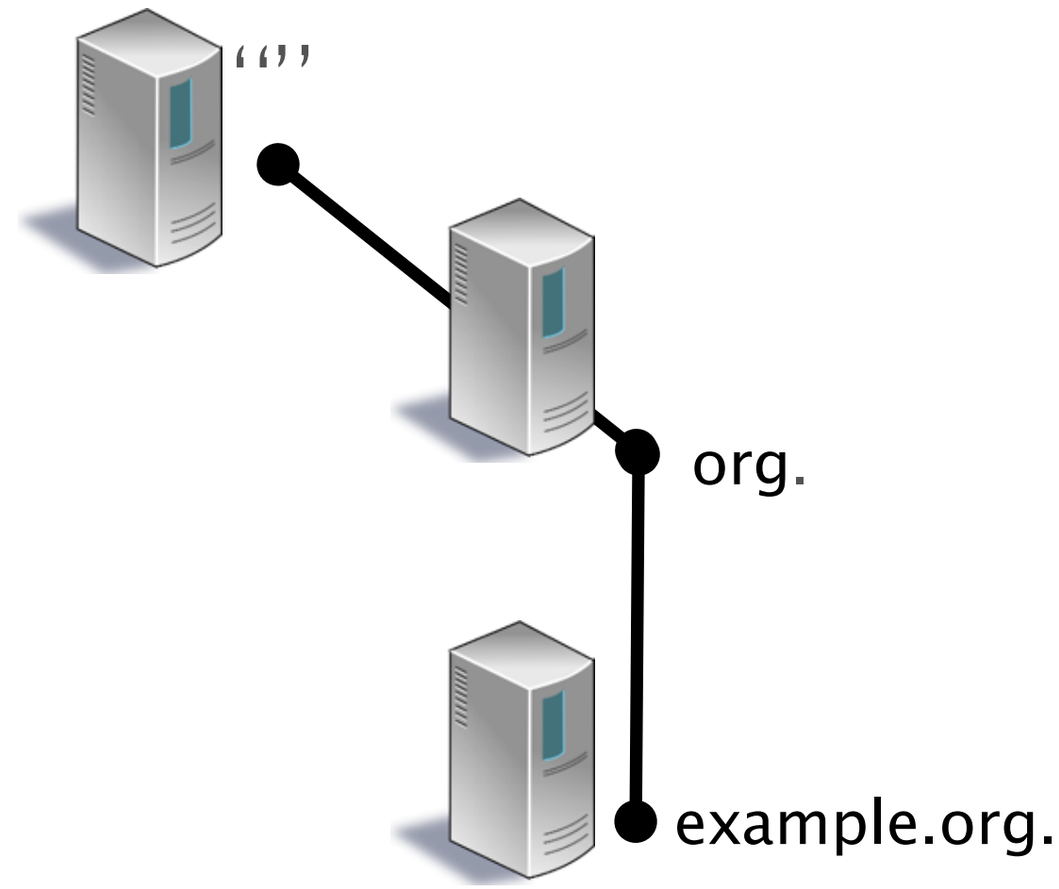
Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑
. DNSKEY	public key
. RRSIG	signature ↑
Trust Anchor for “.”	hash of public key

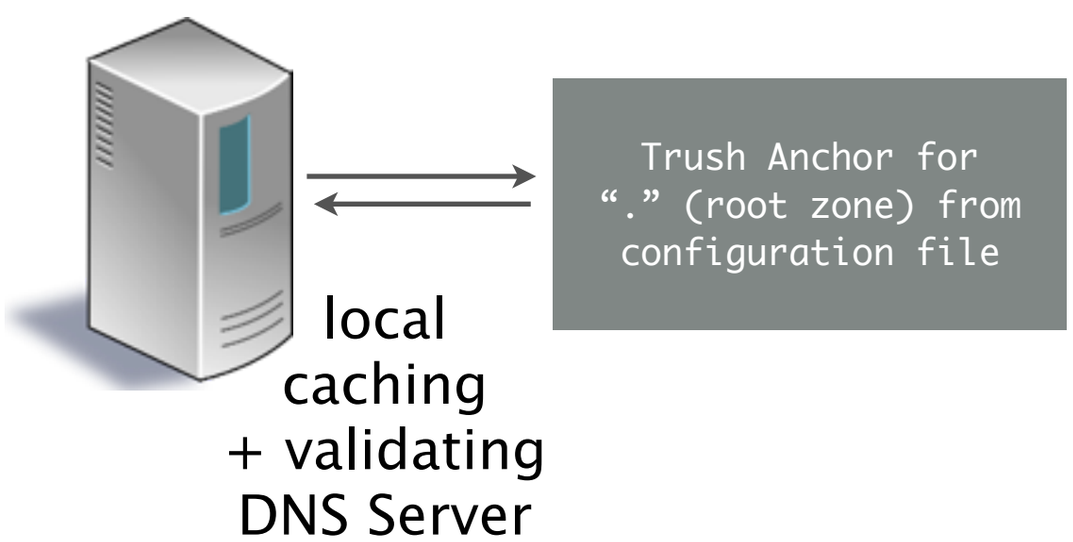




DNSSEC Name Resolution

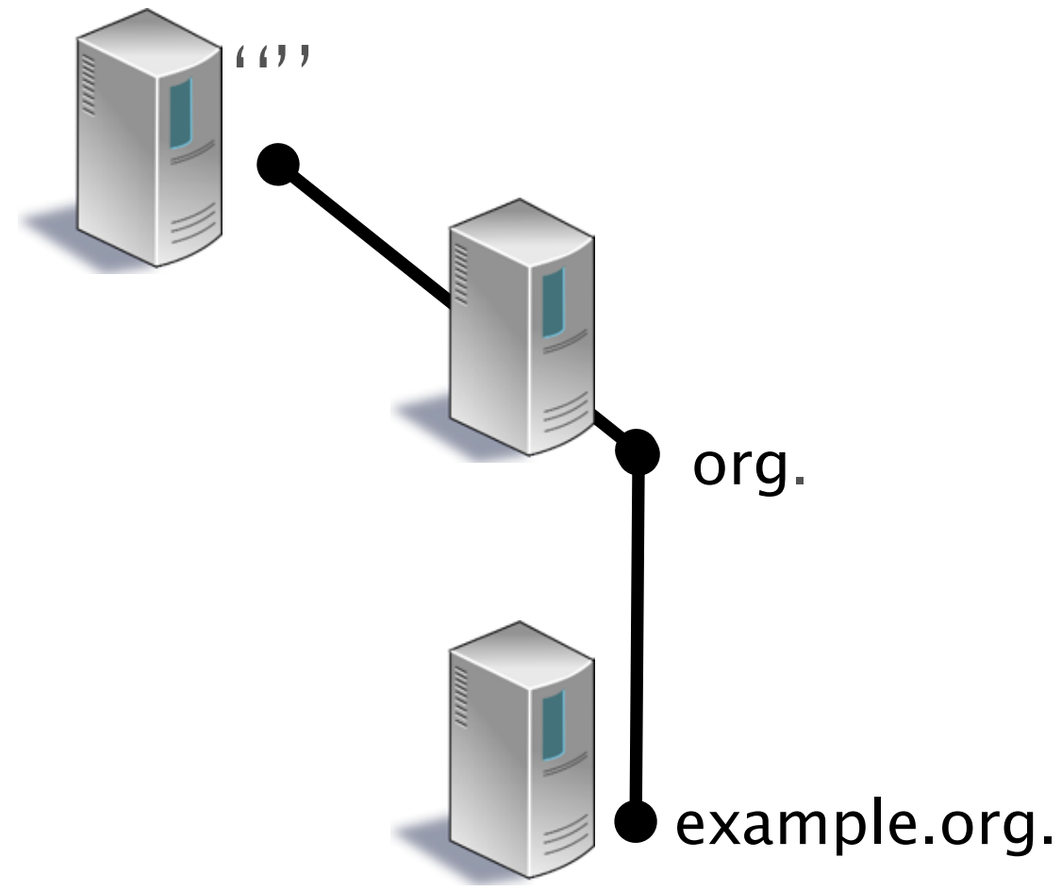
Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑
. DNSKEY	public key
. RRSIG	signature ↑
Trust Anchor for “.”	hash of public key

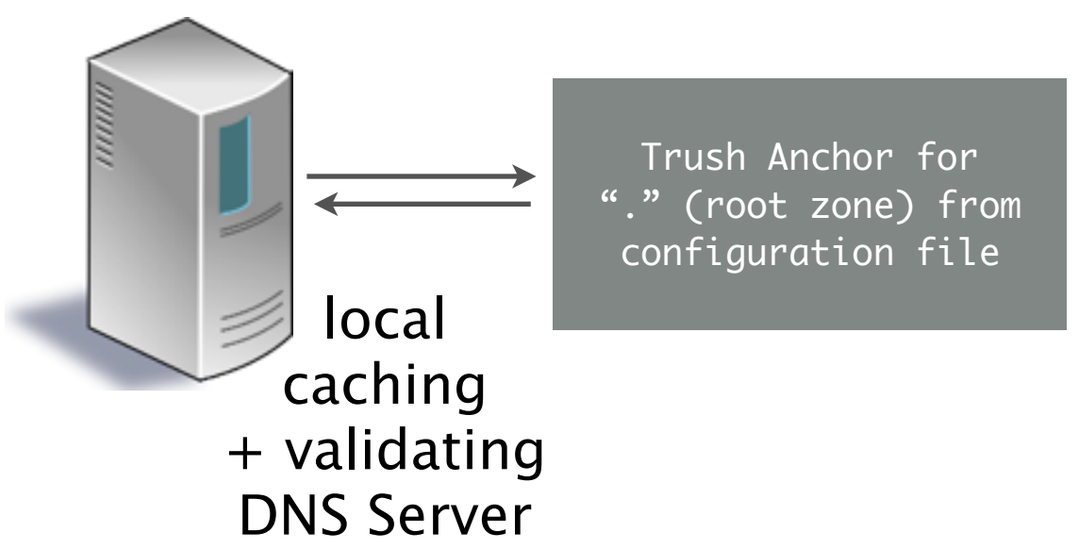




DNSSEC Name Resolution

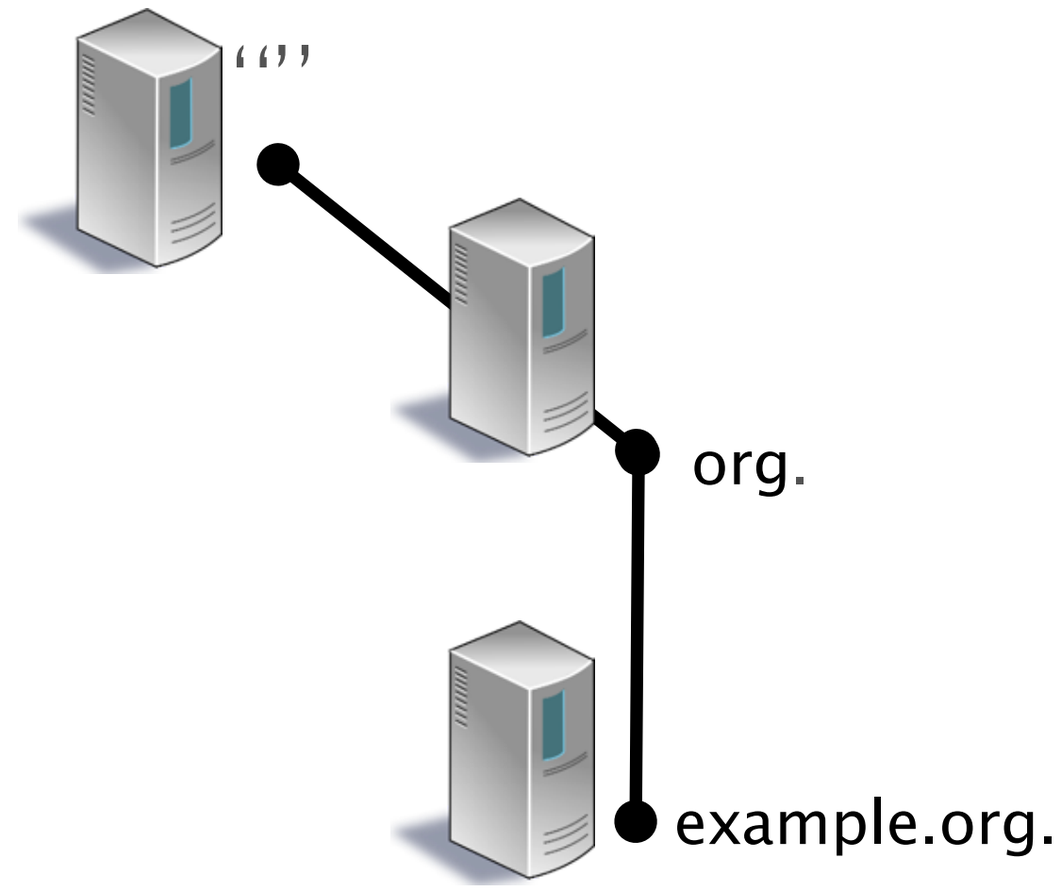
Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑
. DNSKEY	public key
. RRSIG	signature ↑
Trust Anchor for “.”	hash of public key

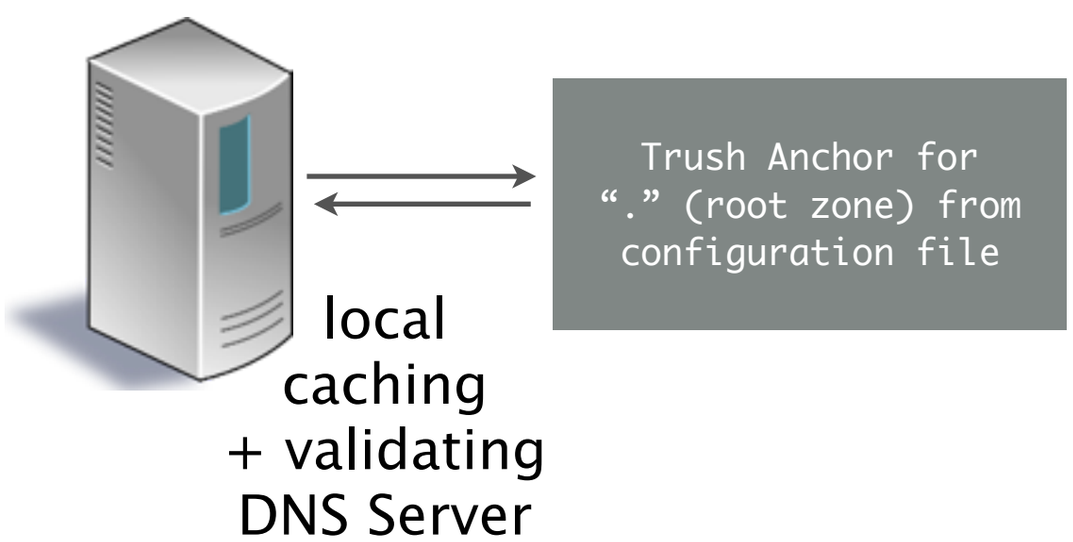




DNSSEC Name Resolution

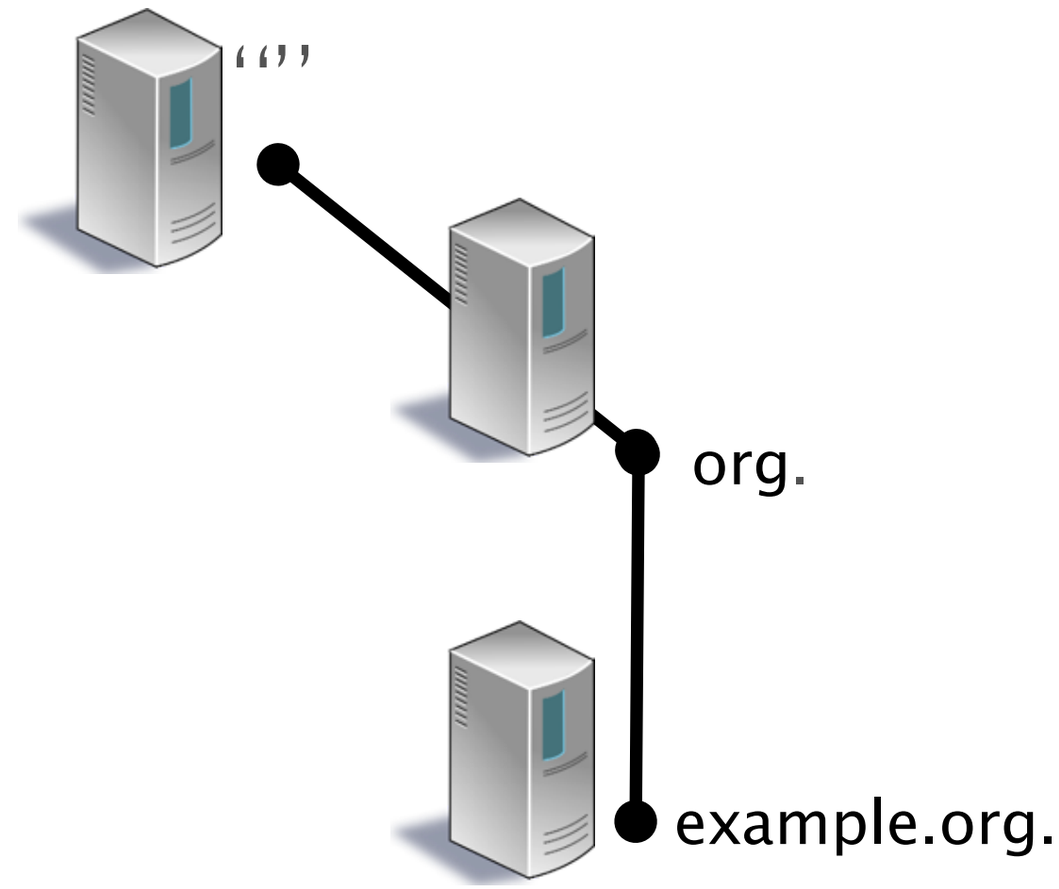
Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑
. DNSKEY	public key
. RRSIG	signature ↑
Trust Anchor for "."	hash of public key

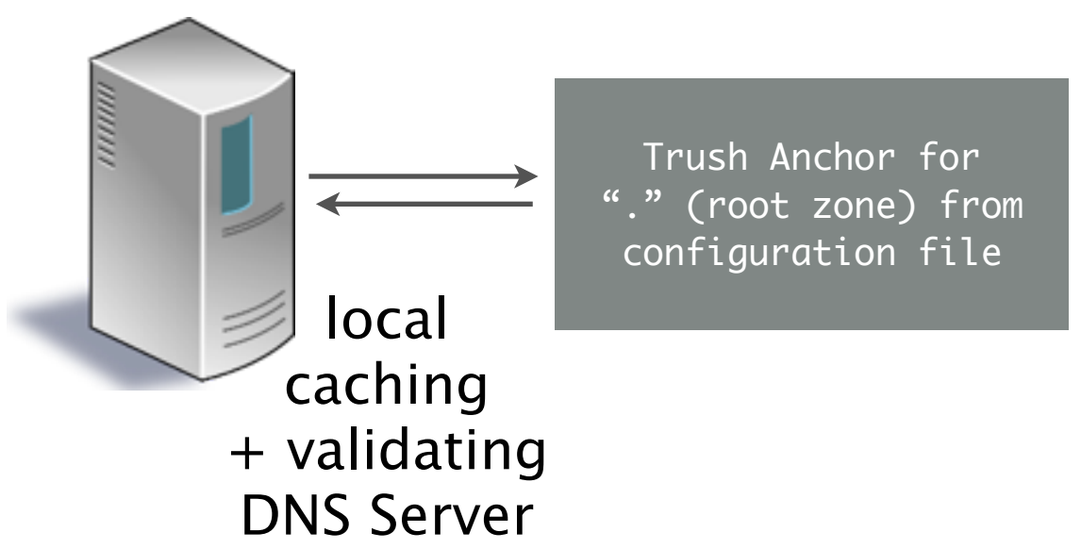




DNSSEC Name Resolution

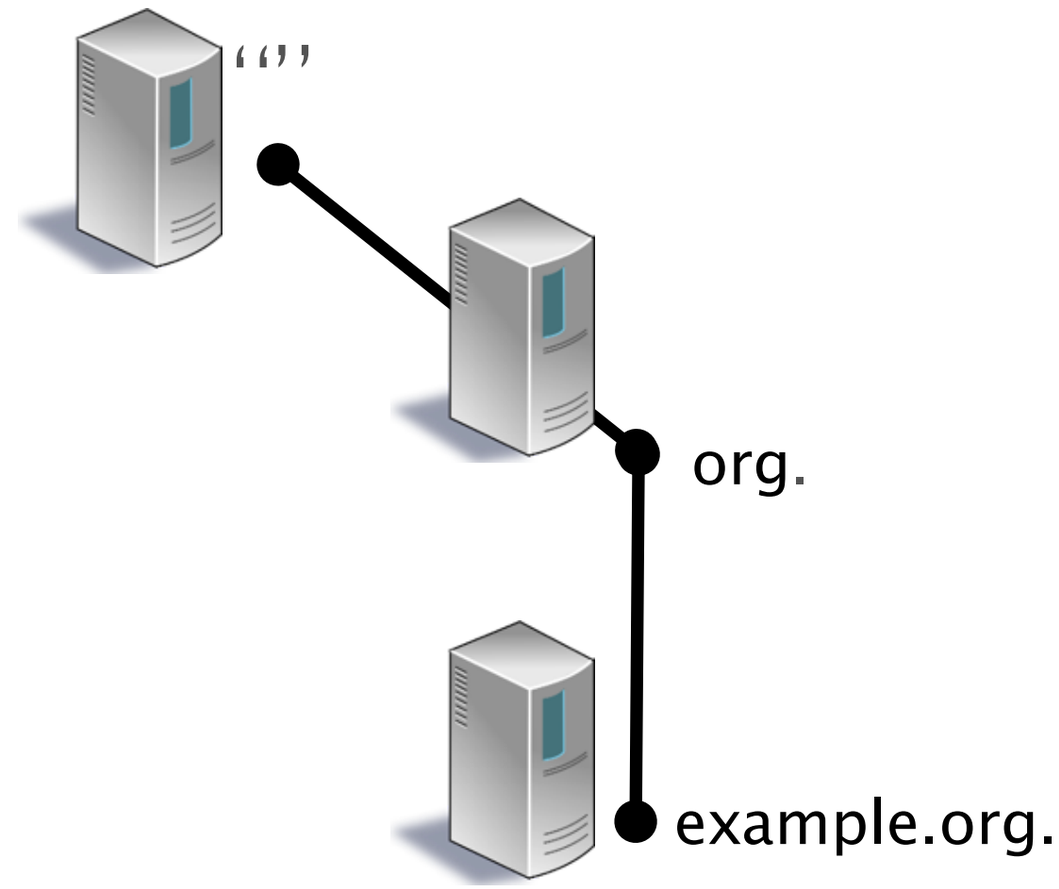
Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑
. DNSKEY	public key
. RRSIG	signature ↑
Trust Anchor for "."	hash of public key

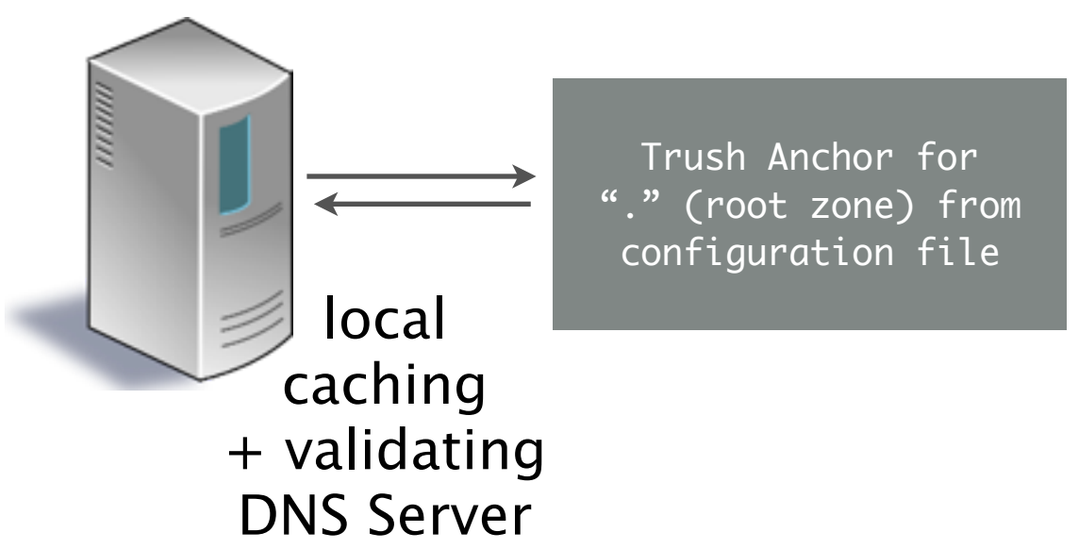




DNSSEC Name Resolution

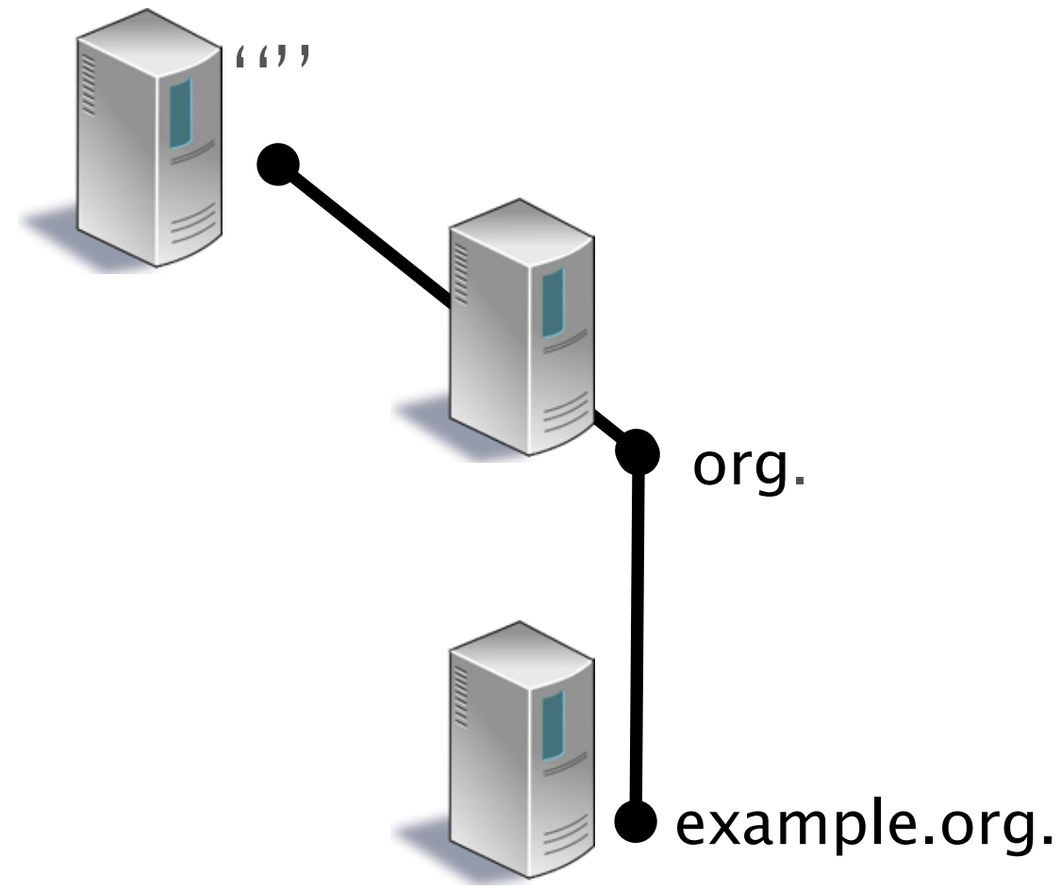
Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑
. DNSKEY	public key
. RRSIG	signature ↑
Trust Anchor for "."	hash of public key

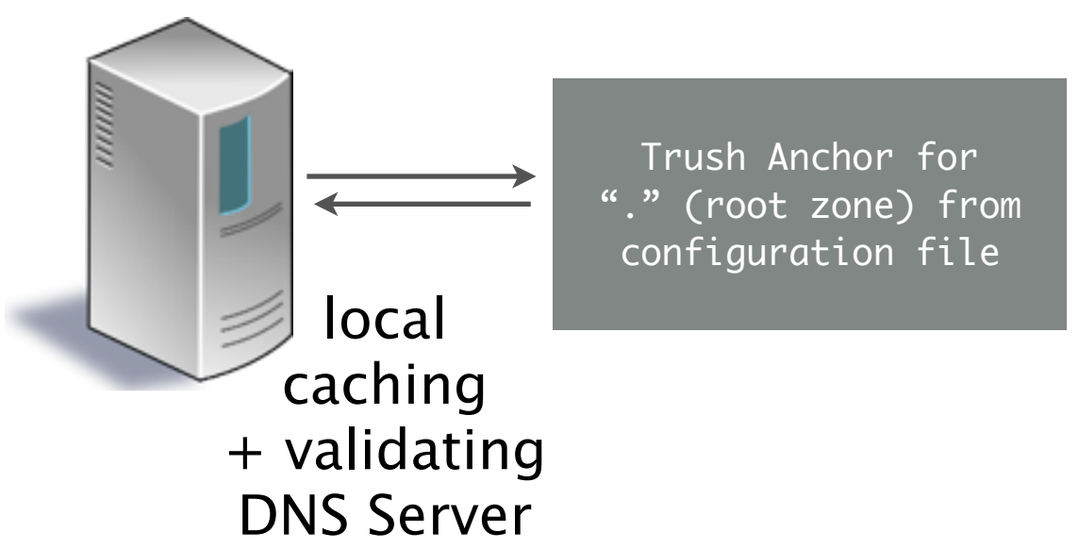




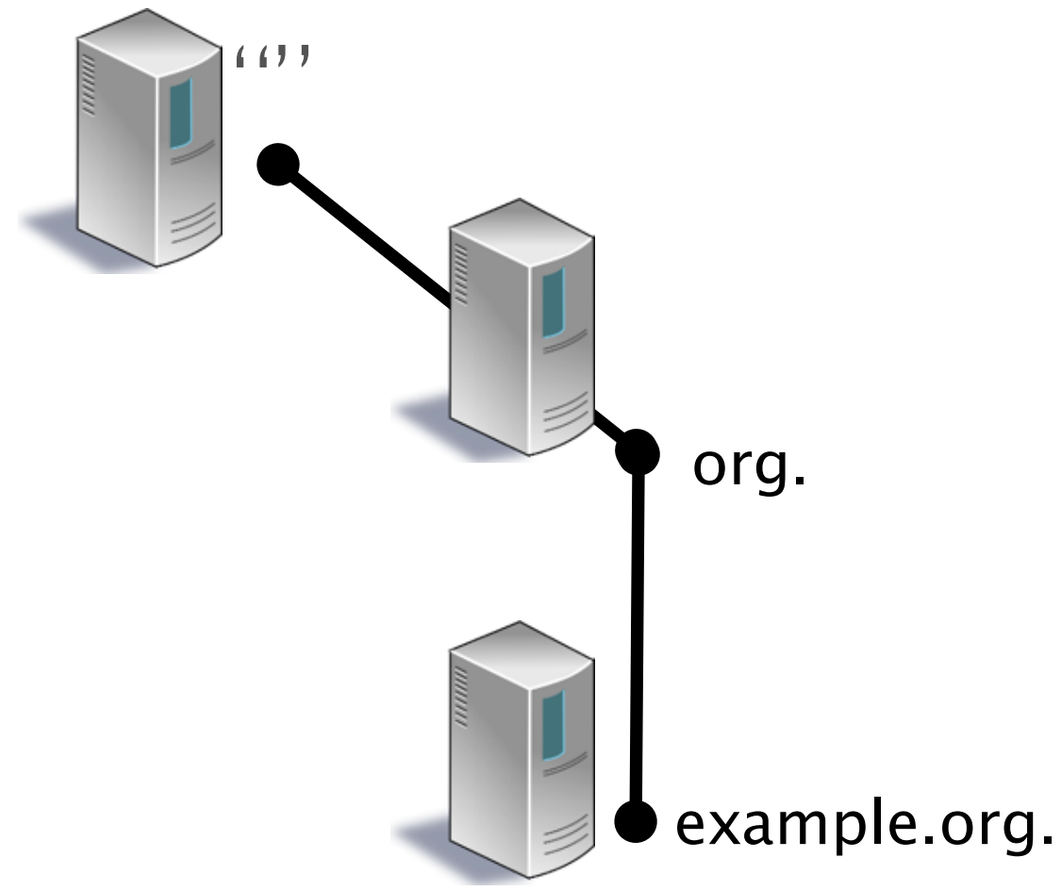
DNSSEC Name Resolution

Record	Function
www.example.org.A	IPv4 Address
www.example.org. RRSIG	signature ↑
example.org. DNSKEY	public key
example.org. RRSIG	signature ↑
example.org. DS	hash of public key
org. RRSIG	signature ↑
org DNSKEY	public key
org RRSIG	signature ↑
org DS	hash of public key
. RRSIG	signature ↑
. DNSKEY	public key
. RRSIG	signature ↑
Trust Anchor for “.”	hash of public key



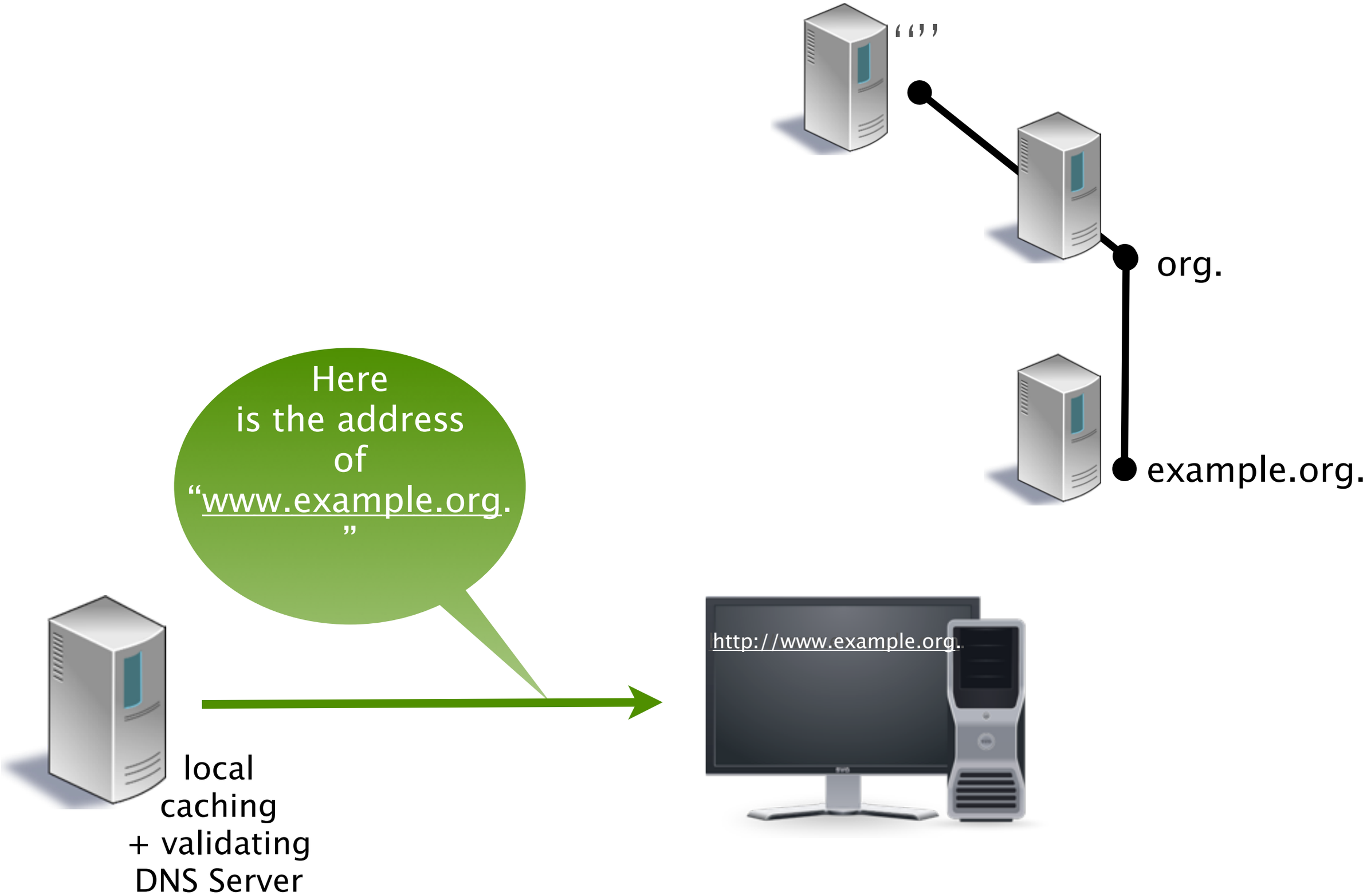


DNSSEC Name Resolution

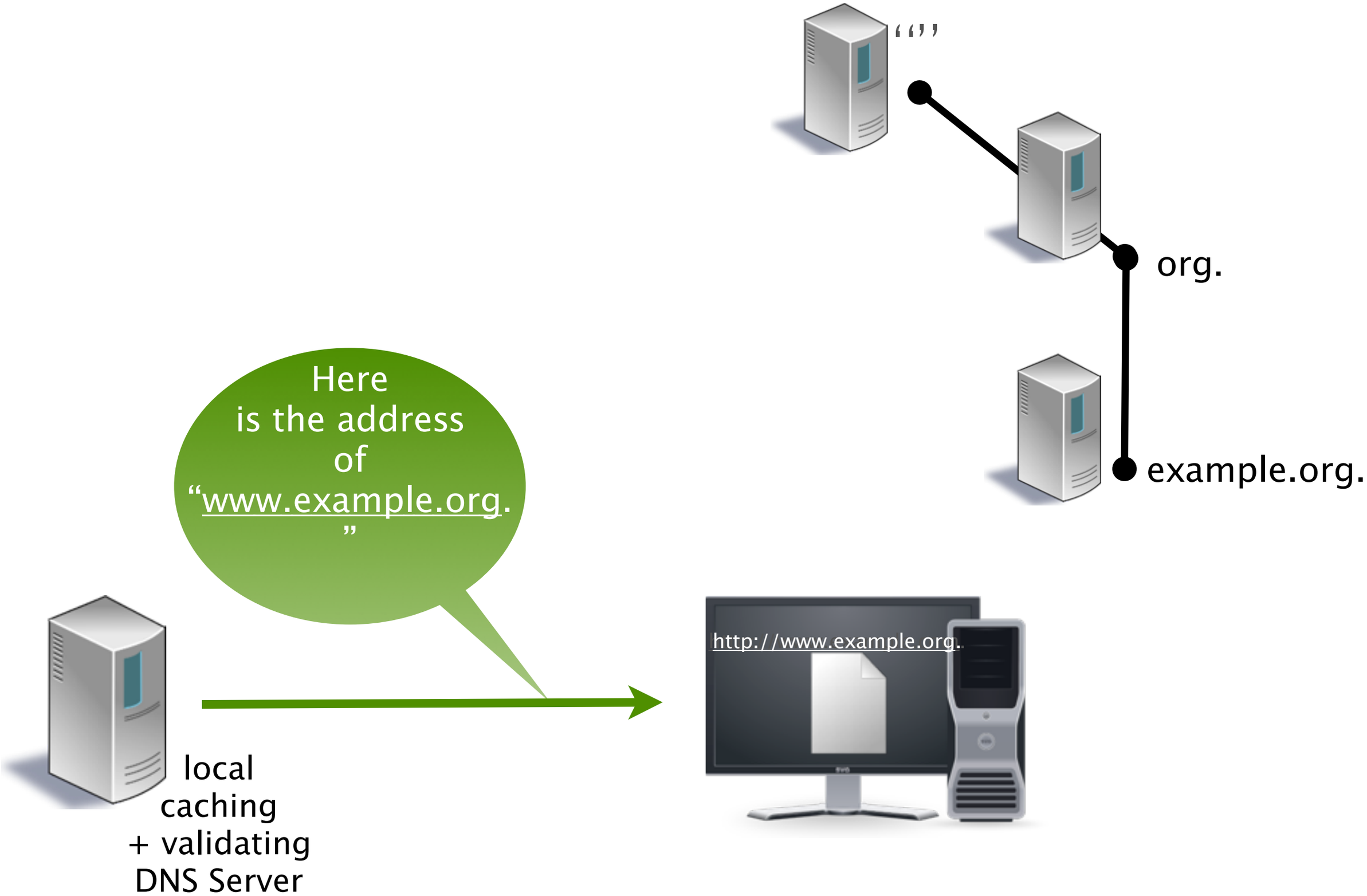


local
caching
+ validating
DNS Server

DNSSEC Name Resolution



DNSSEC Name Resolution



Validation

- The steps on the previous slides are simplified
  - They only show validation on the last DNS query
    - But DNSSEC validation will be done for every query down to the requested domain
  - It only shows validation of one key per zone
    - In reality, we have ZSK and KSK, so twice the amount of checking