

NSEC5: Provably Preventing DNSSEC Zone Enumeration

NDSS Symposium 2015, San Diego, CA. February 10, 2015

Sharon Goldberg
Dimitrios Papadopoulos
Leonid Reyzin
Sachin Vasant



Moni Naor
Asaf Ziv



מכון ויצמן למדע
WEIZMANN INSTITUTE OF SCIENCE

DNSSEC model and denial-of-existence



Resolver



Zone File

a.com 155.41.24.250
c.com 155.41.24.251
z.com 155.41.24.252

DNSSEC model and denial-of-existence



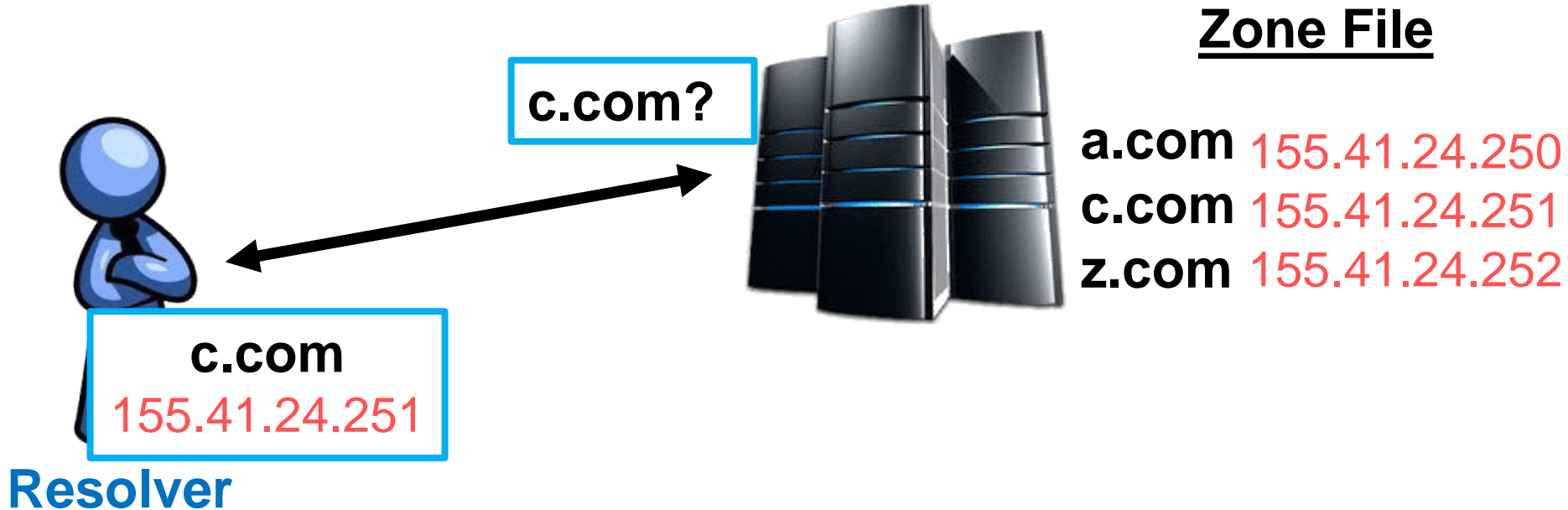
c.com?



Zone File

a.com	155.41.24.250
c.com	155.41.24.251
z.com	155.41.24.252

DNSSEC model and denial-of-existence



DNSSEC model and denial-of-existence



Resolver



Zone File

a.com 155.41.24.250
c.com 155.41.24.251
z.com 155.41.24.252

DNSSEC model and denial-of-existence



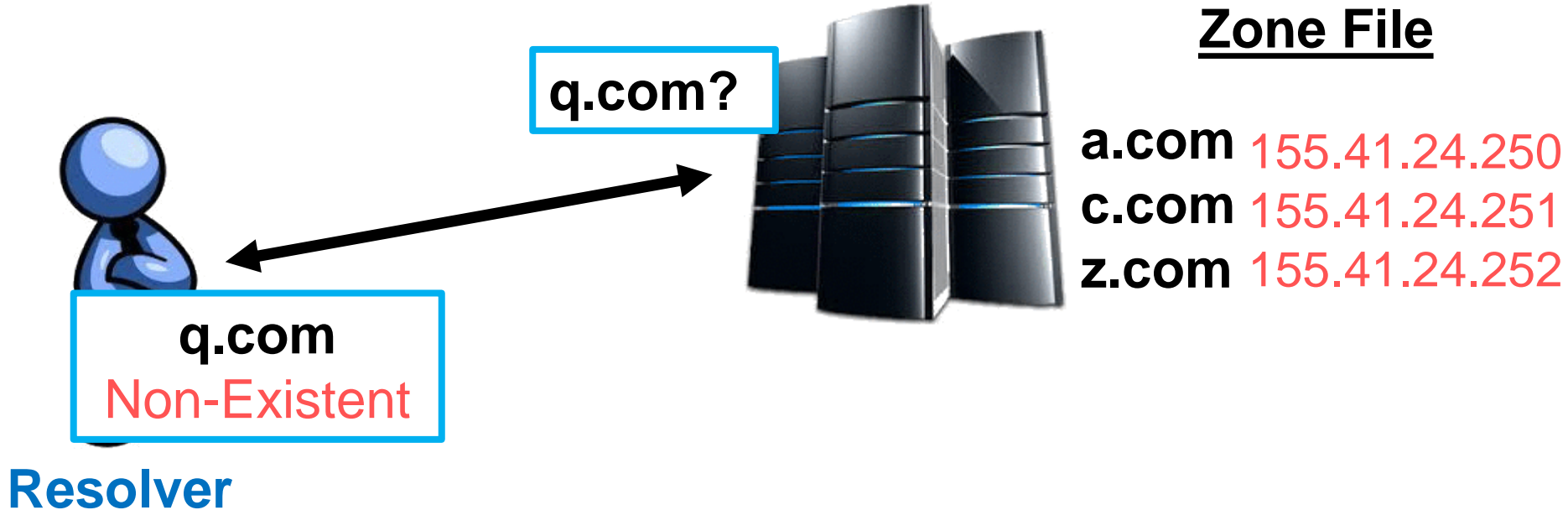
q.com?



Zone File

a.com 155.41.24.250
c.com 155.41.24.251
z.com 155.41.24.252

DNSSEC model and denial-of-existence



DNSSEC model and denial-of-existence



Resolver



Zone File

a.com 155.41.24.250
c.com 155.41.24.251
z.com 155.41.24.252

DNSSEC demands Integrity

DNSSEC model and denial-of-existence

Integrity



Resolver

DNSSEC demands Integrity



Zone File

a.com 155.41.24.250
c.com 155.41.24.251
z.com 155.41.24.252

DNSSEC model and denial-of-existence

Integrity



Zone File

a.com 155.41.24.250
c.com 155.41.24.251
z.com 155.41.24.252

Secondary nameserver

Resolver DNSSEC demands Integrity



Primary nameserver

DNSSEC model and denial-of-existence

Integrity



Zone File

a.com 155.41.24.250
c.com 155.41.24.251
z.com 155.41.24.252

Secondary nameserver

Resolver DNSSEC demands Integrity



 a.com
155.41.24.250

 c.com
155.41.24.251

 z.com
155.41.24.252

Primary nameserver

DNSSEC model and denial-of-existence

Integrity



Resolver

DNSSEC demands Integrity






Secondary nameserver

Zone File

a.com 155.41.24.250
c.com 155.41.24.251
z.com 155.41.24.252

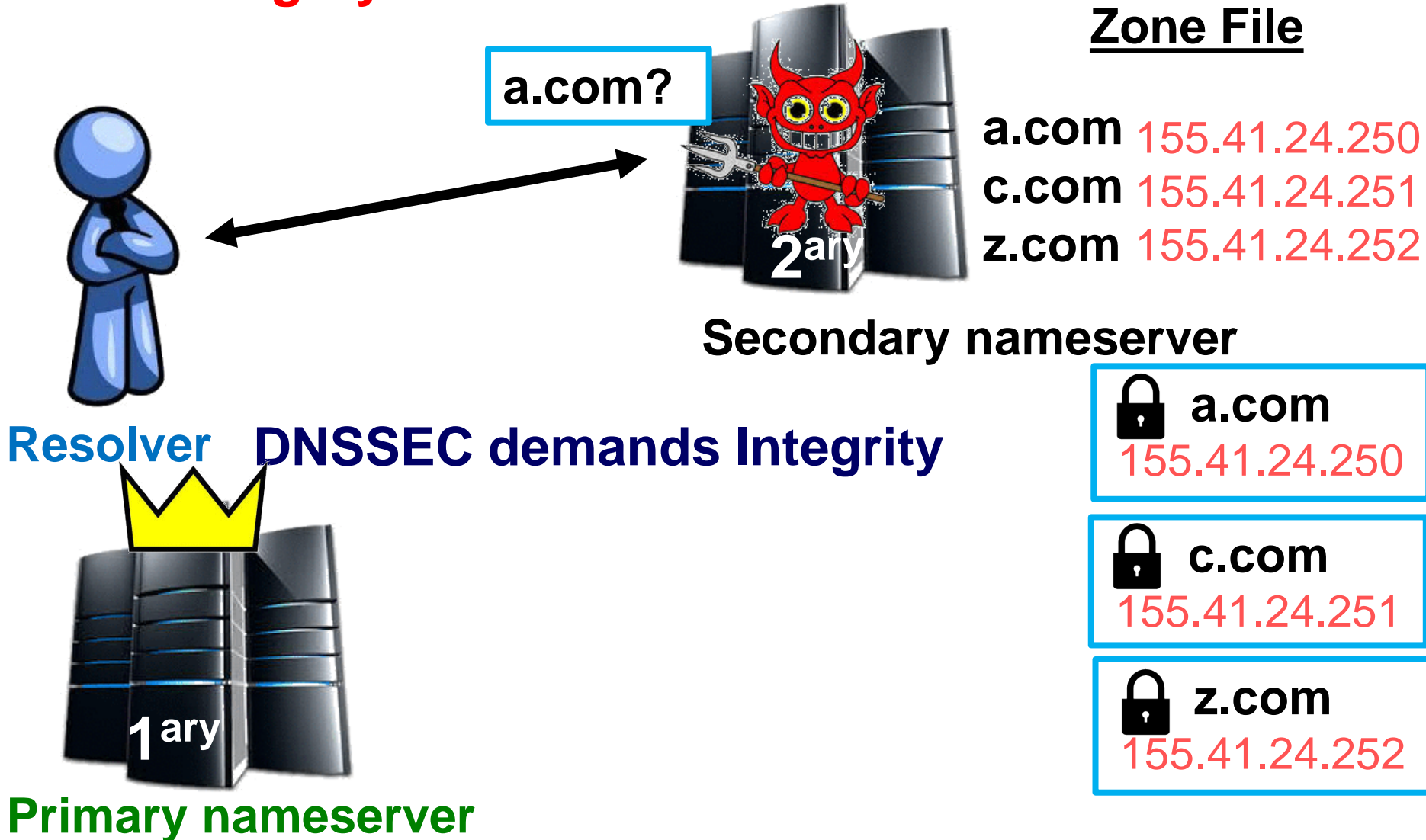


Primary nameserver

 a.com 155.41.24.250
 c.com 155.41.24.251
 z.com 155.41.24.252

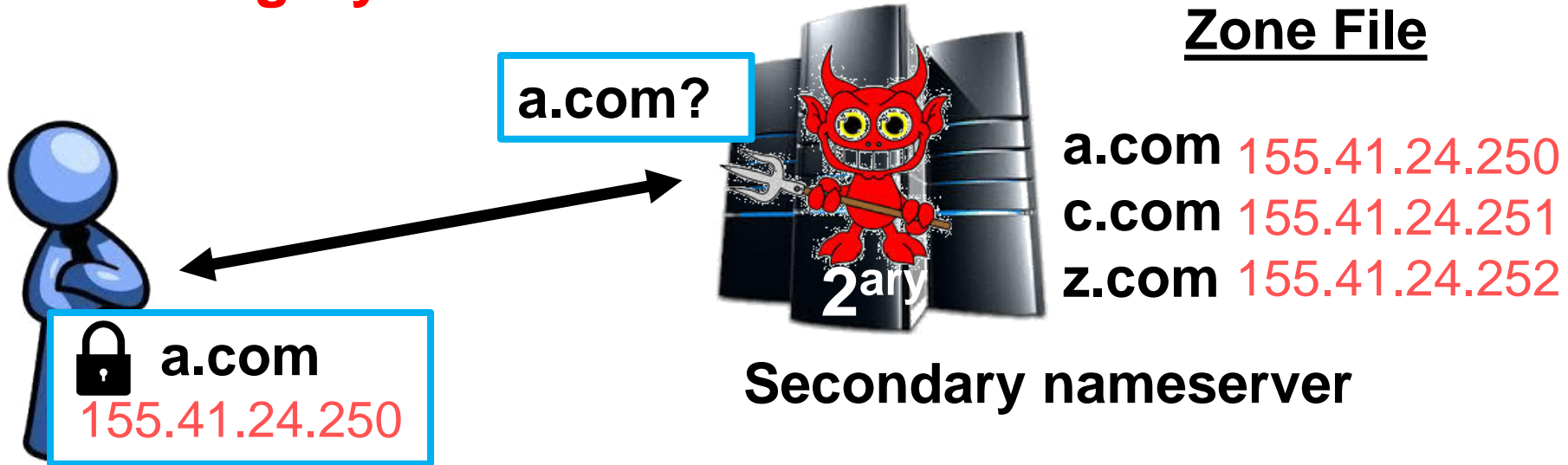
DNSSEC model and denial-of-existence

Integrity



DNSSEC model and denial-of-existence

Integrity



Resolver DNSSEC demands Integrity



Primary nameserver

c.com
155.41.24.251

z.com
155.41.24.252

DNSSEC model and denial-of-existence

Integrity



Zone File

a.com 155.41.24.250
c.com 155.41.24.251
z.com 155.41.24.252

Secondary nameserver

Resolver DNSSEC demands Integrity



?

q.com
Non-Existent

 c.com
155.41.24.251

 z.com
155.41.24.252

Primary nameserver

DNSSEC model and denial-of-existence



Privacy



Secondary nameserver

Zone File

a.com 155.41.24.250
c.com 155.41.24.251
z.com 155.41.24.252

Resolver DNSSEC demands Integrity and Privacy



Primary nameserver

 c.com
155.41.24.251

 z.com
155.41.24.252

RFC 4470 – Online signing

Resolver

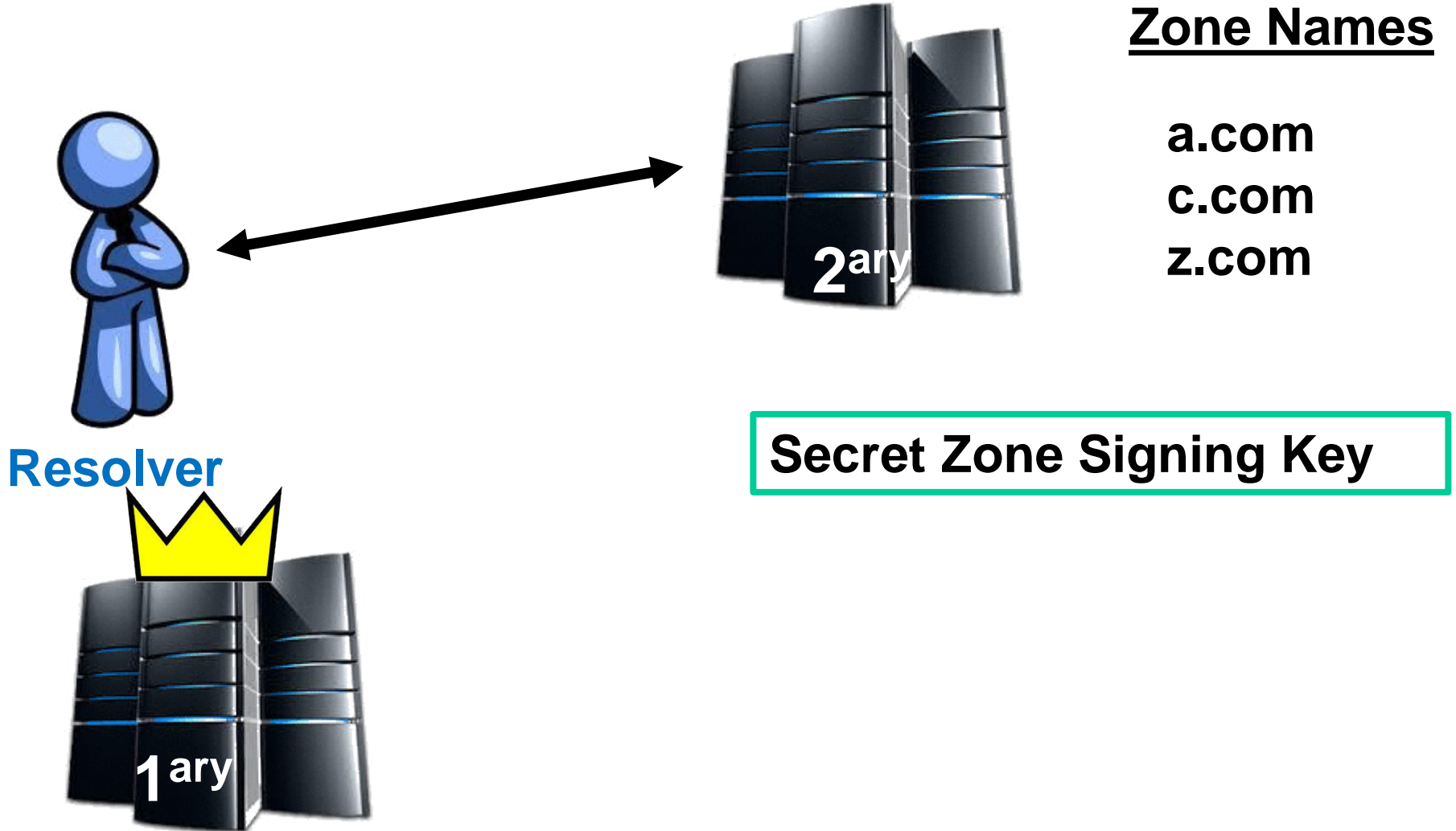


Zone Names

a.com
c.com
z.com



RFC 4470 – Online signing



RFC 4470 – Online signing

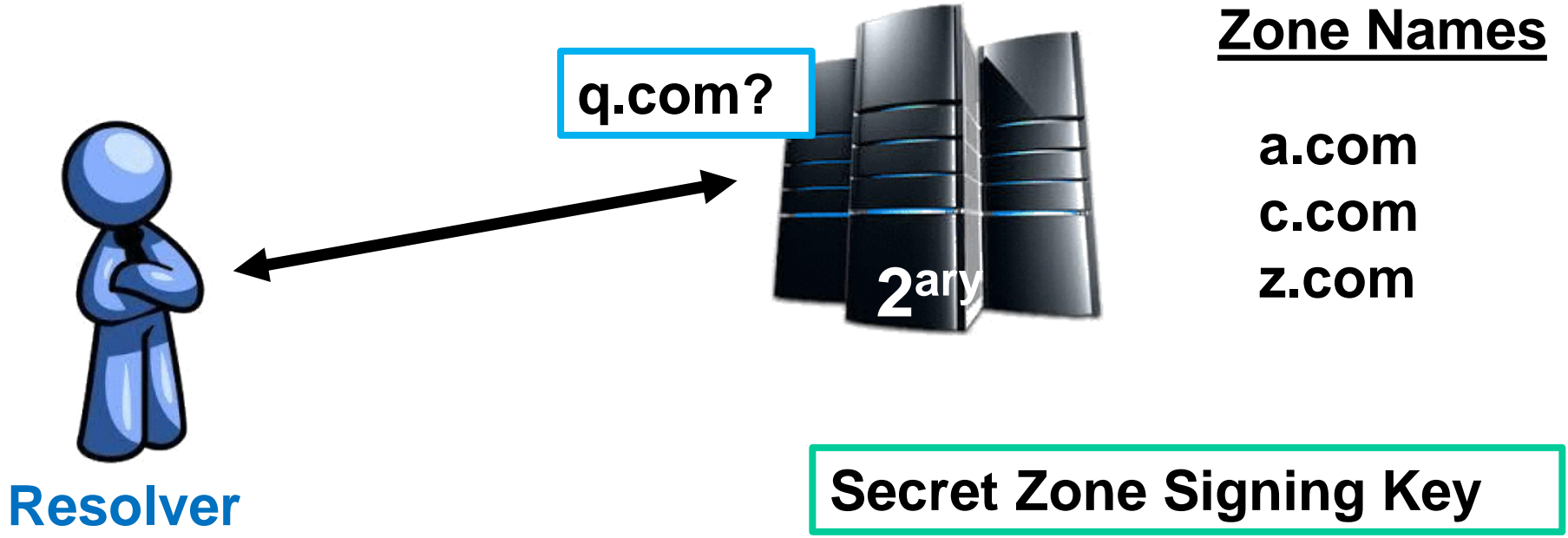


Zone Names

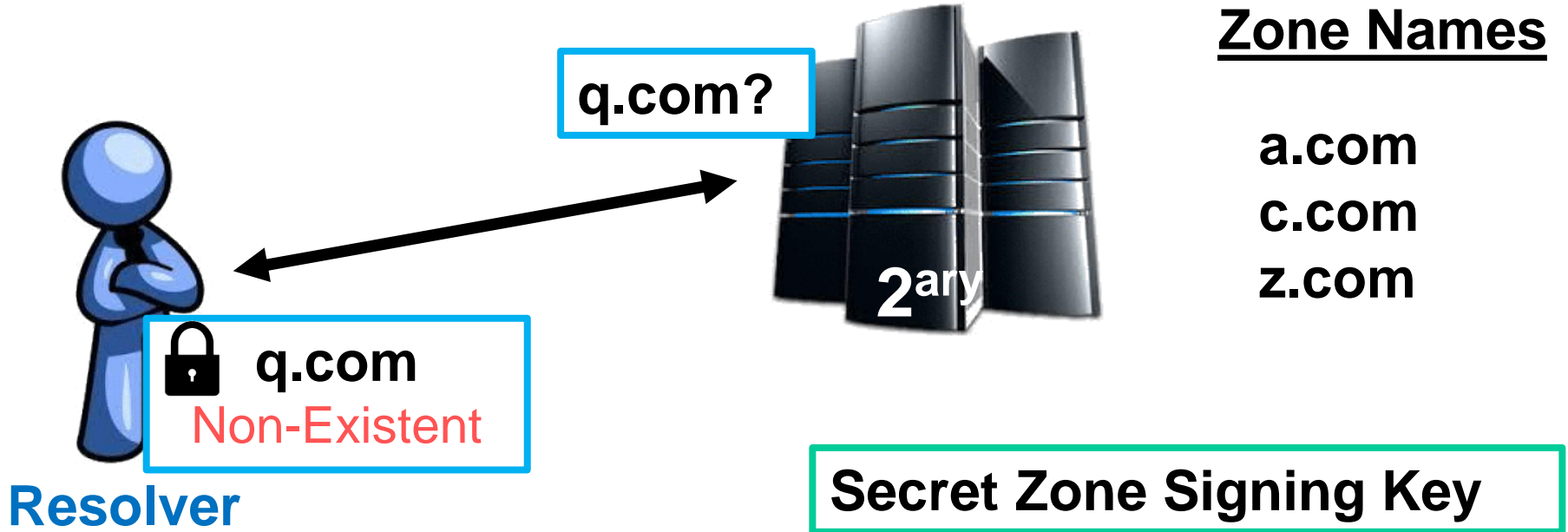
a.com
c.com
z.com

Secret Zone Signing Key

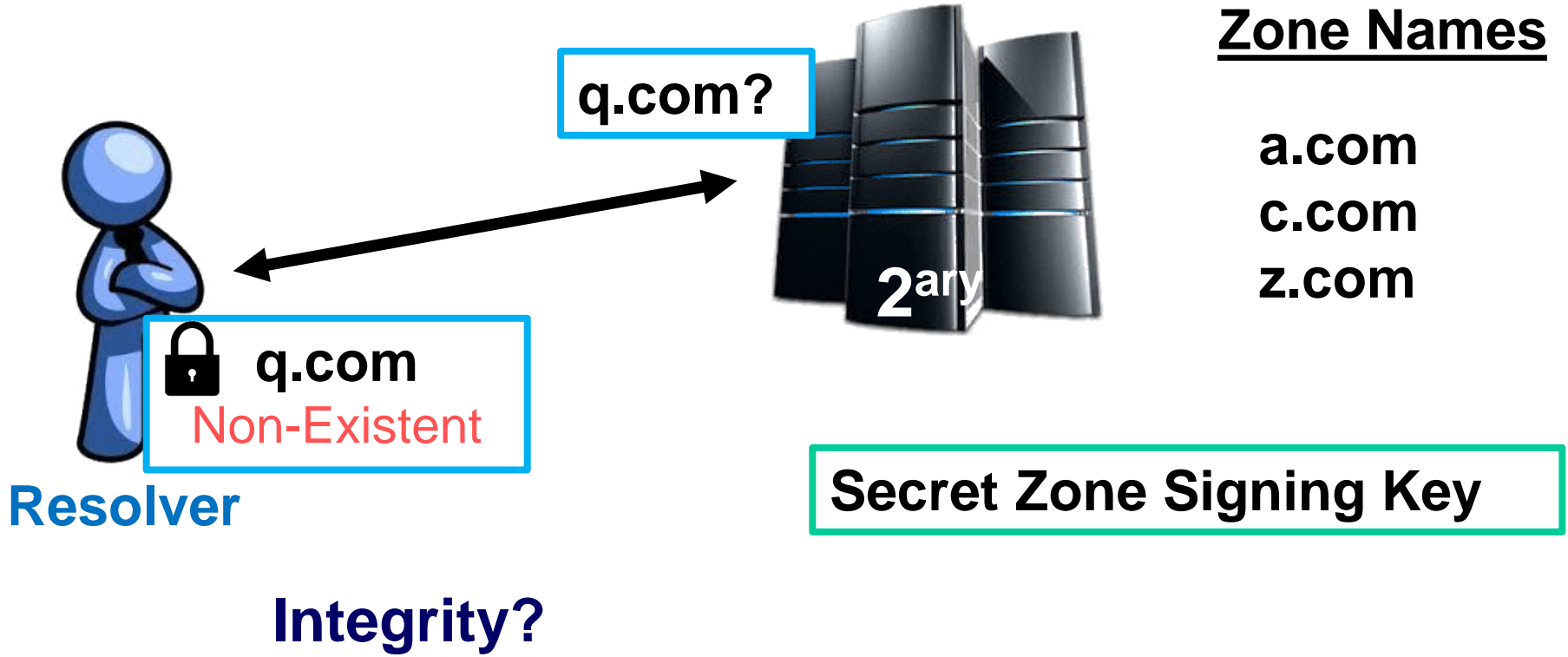
RFC 4470 – Online signing



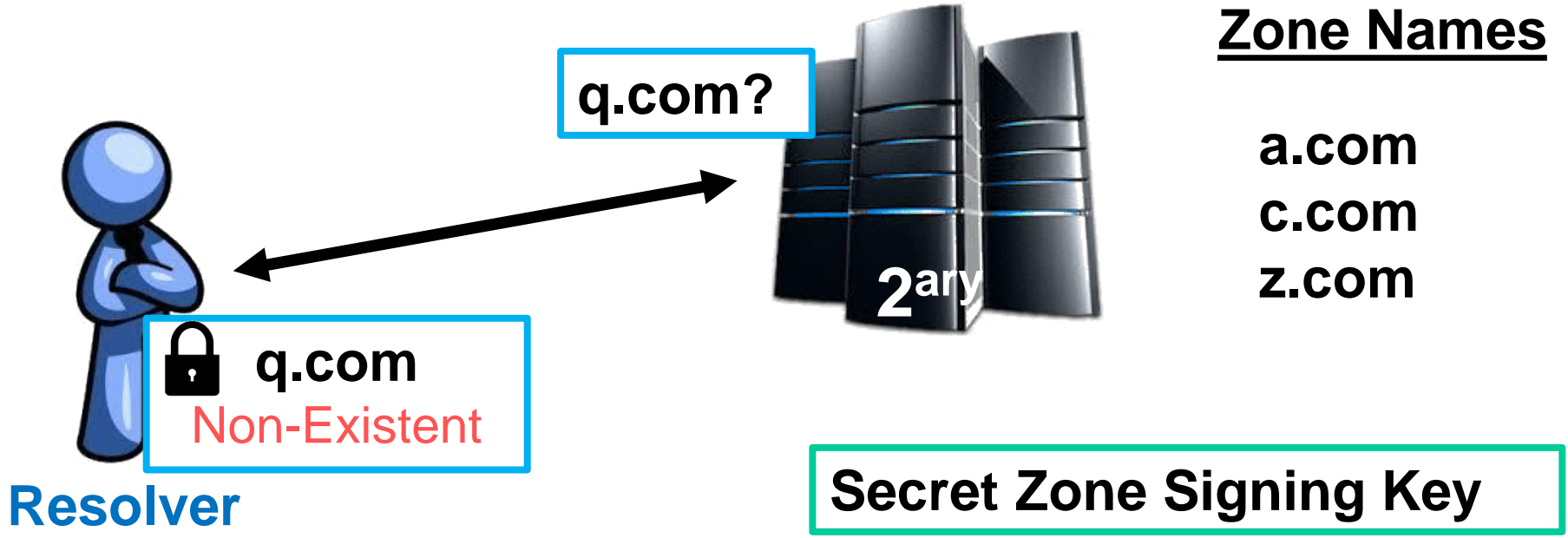
RFC 4470 – Online signing



RFC 4470 – Online signing



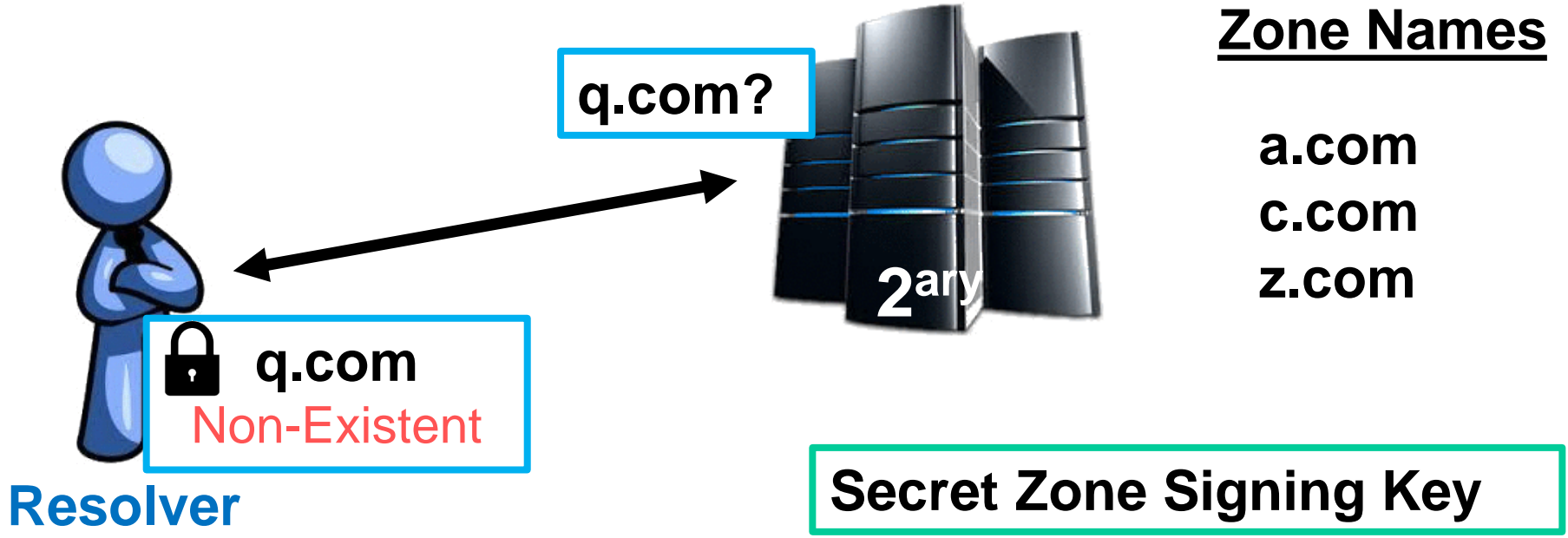
RFC 4470 – Online signing



Integrity?

Privacy?

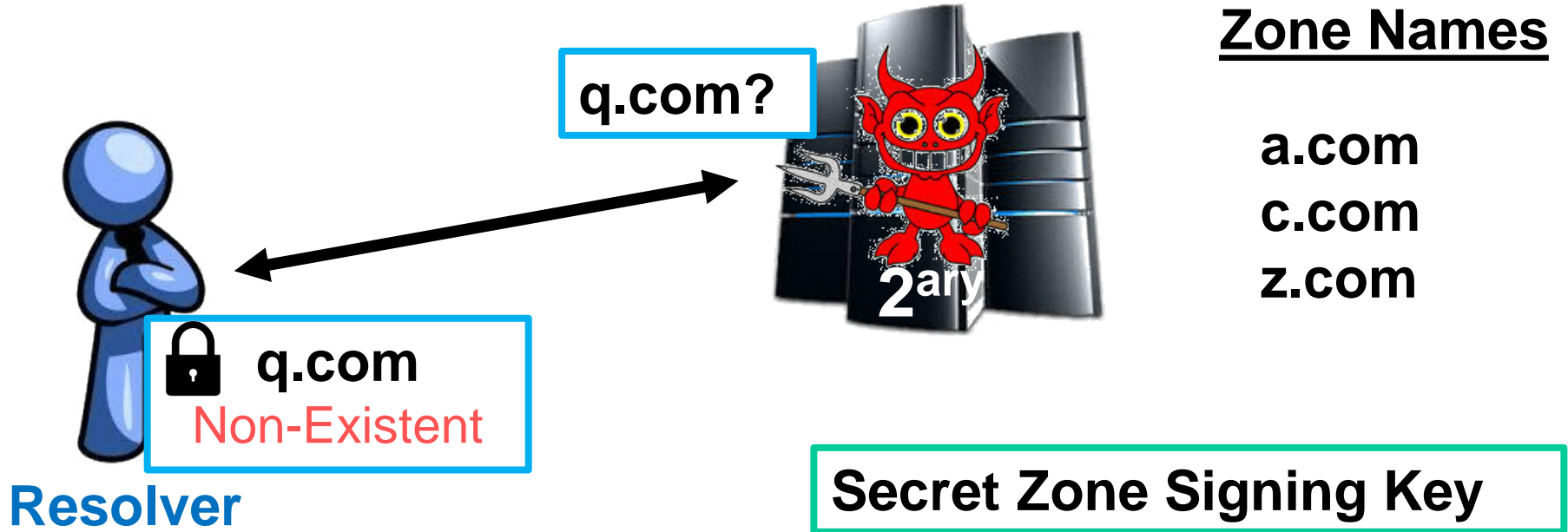
RFC 4470 – Online signing



Integrity?

Privacy? **Yes!**

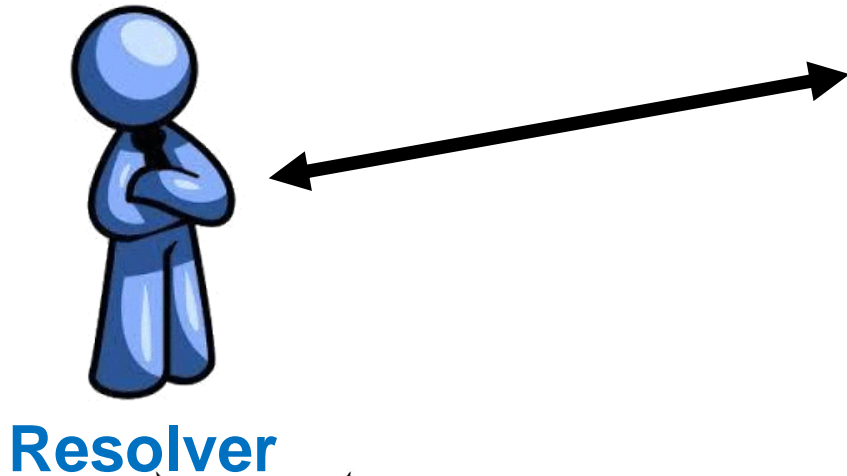
RFC 4470 – Online signing



Integrity? Only if we trust
Secondary nameserver!

Privacy? Yes!

RFC 4034 – NSEC



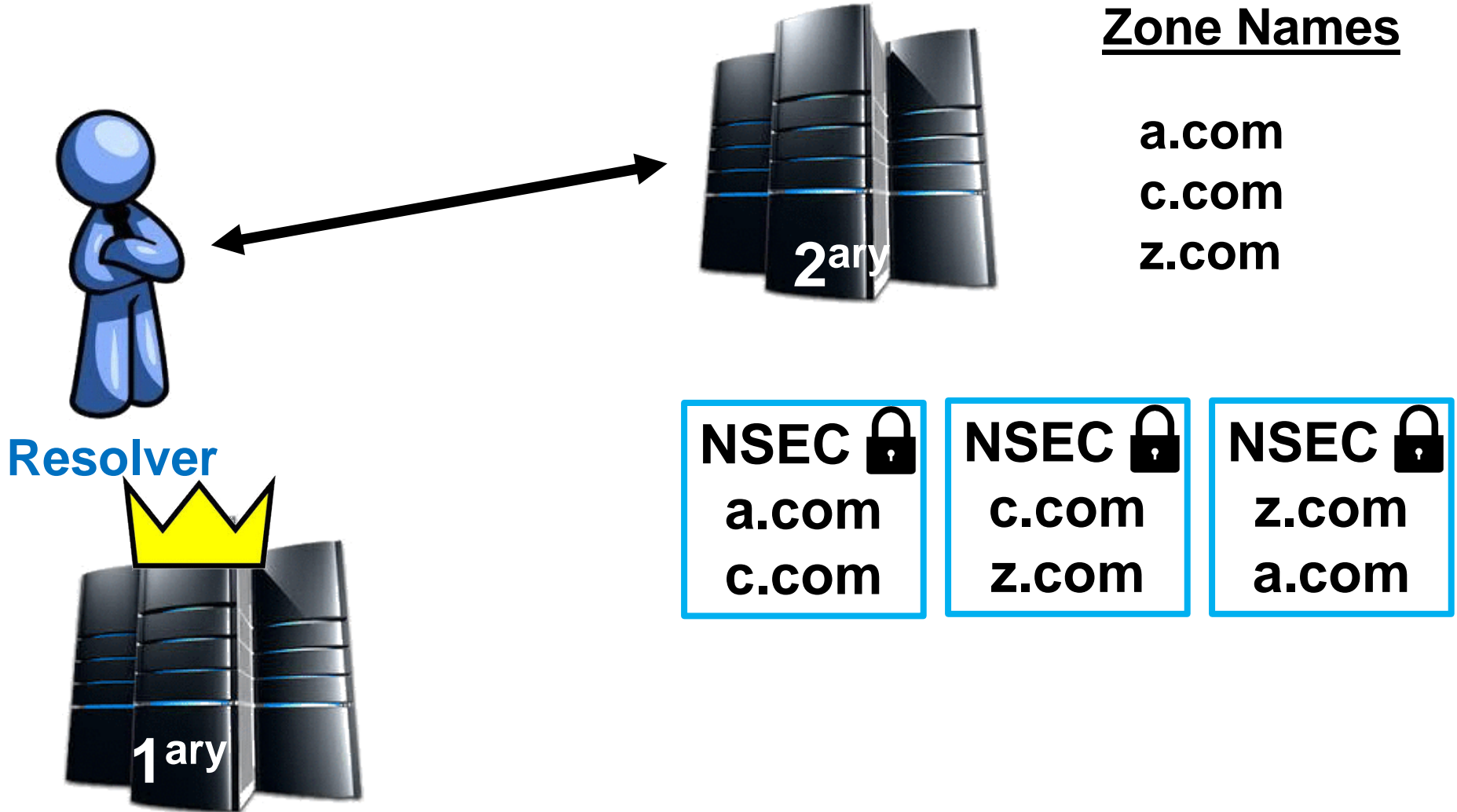
Resolver



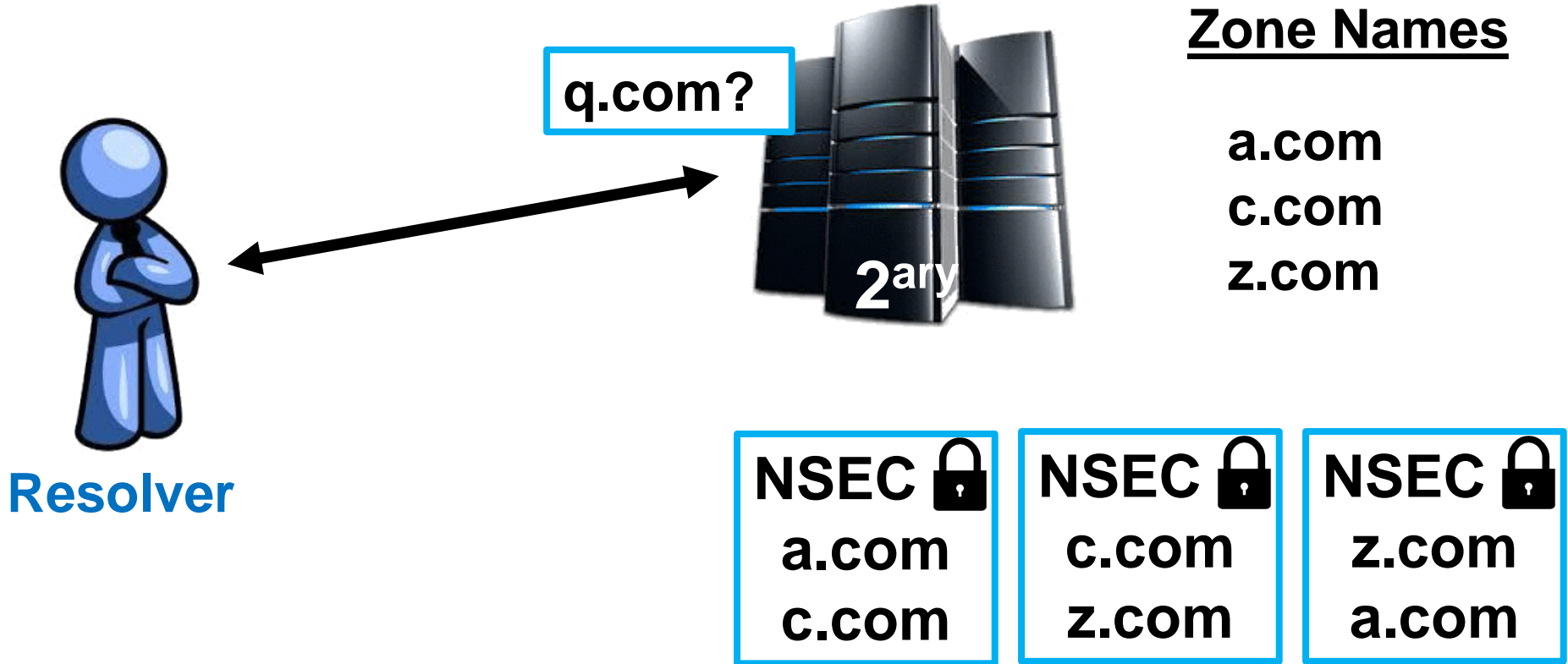
Zone Names

- a.com
- c.com
- z.com

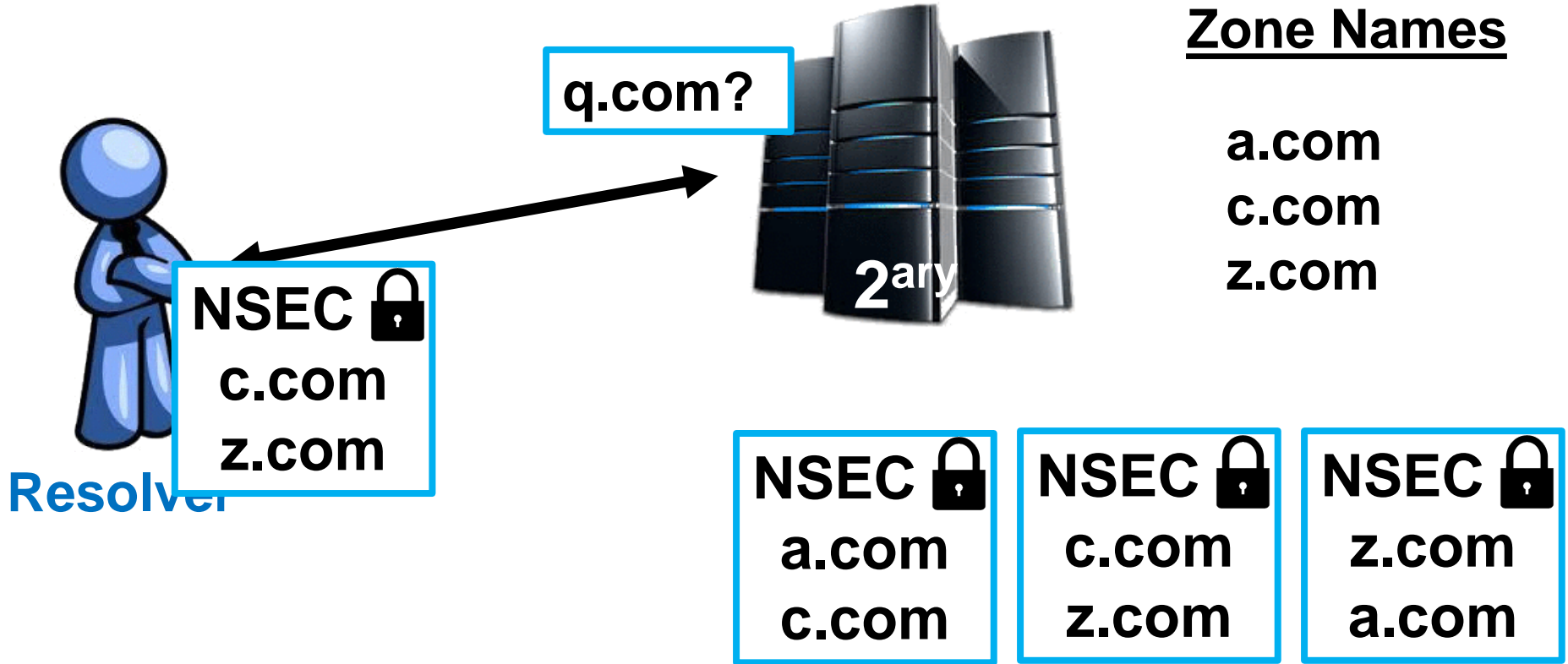
RFC 4034 – NSEC



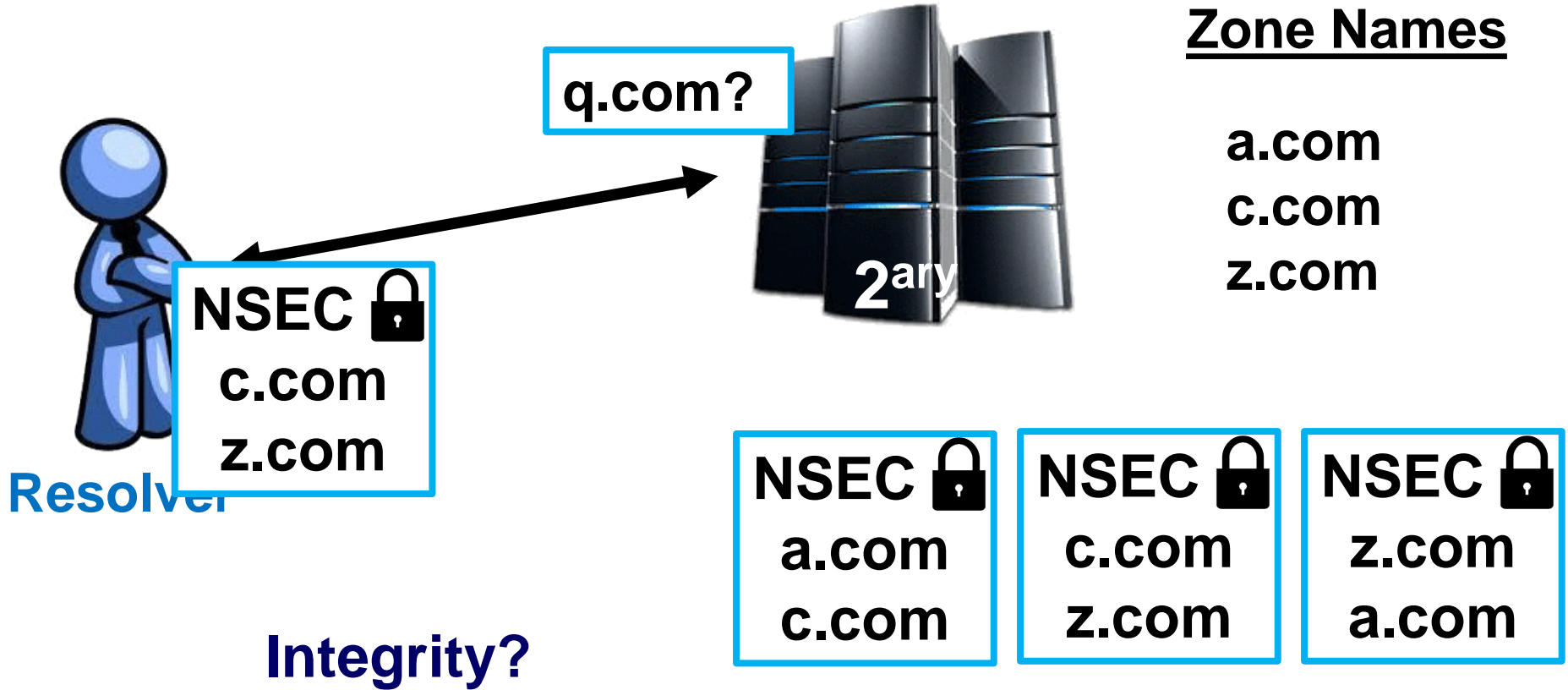
RFC 4034 – NSEC



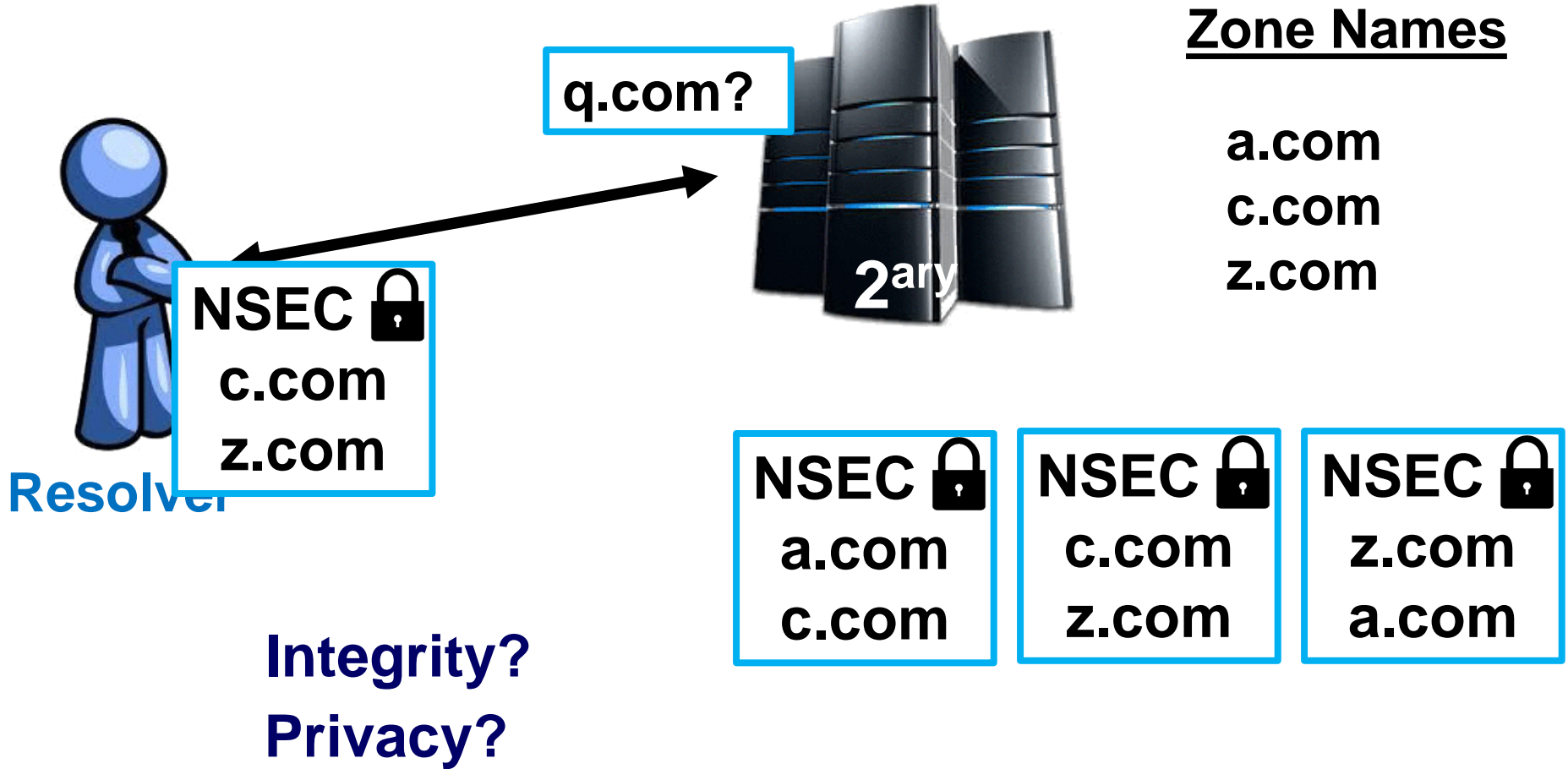
RFC 4034 – NSEC



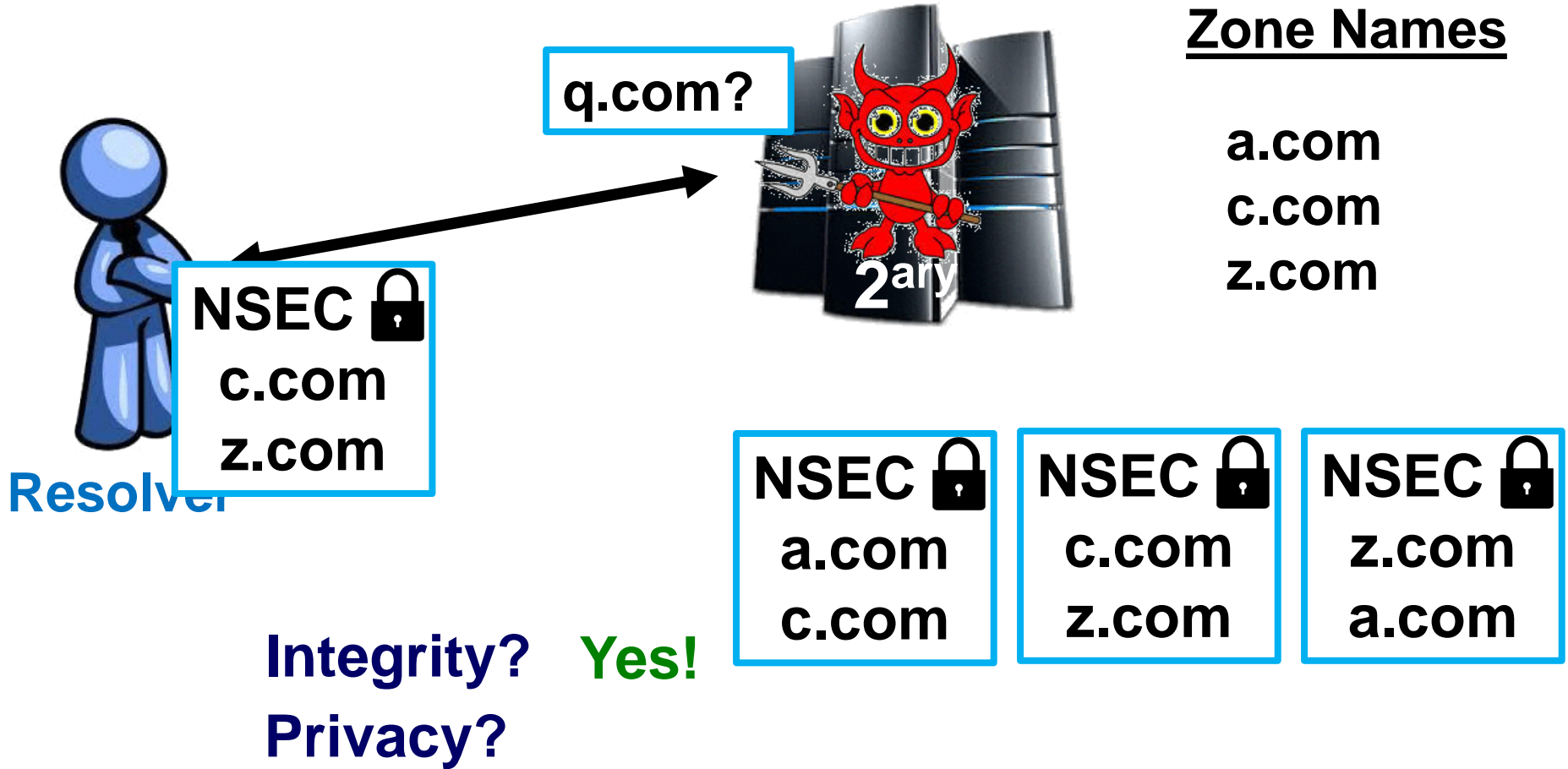
RFC 4034 – NSEC



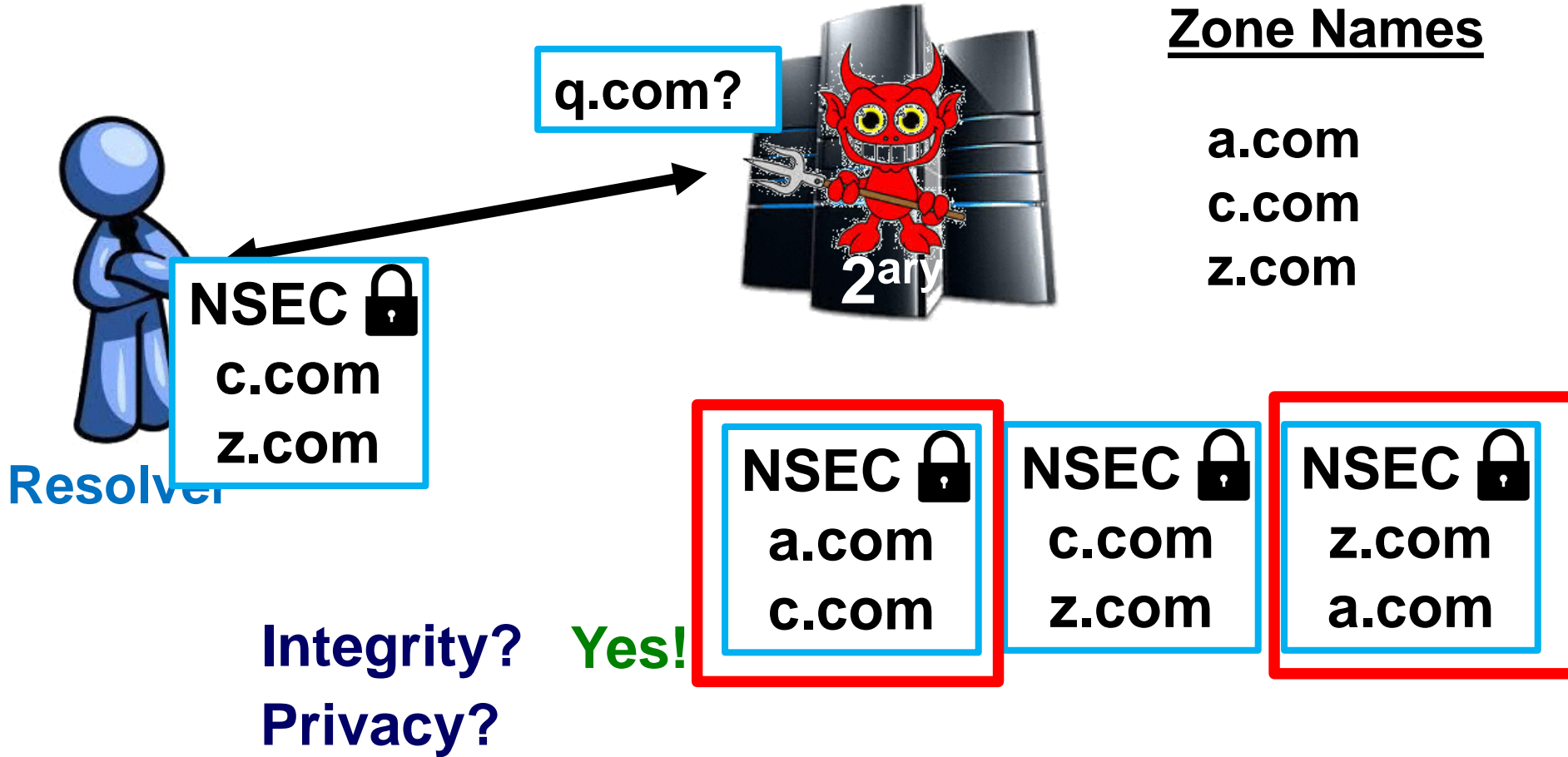
RFC 4034 – NSEC



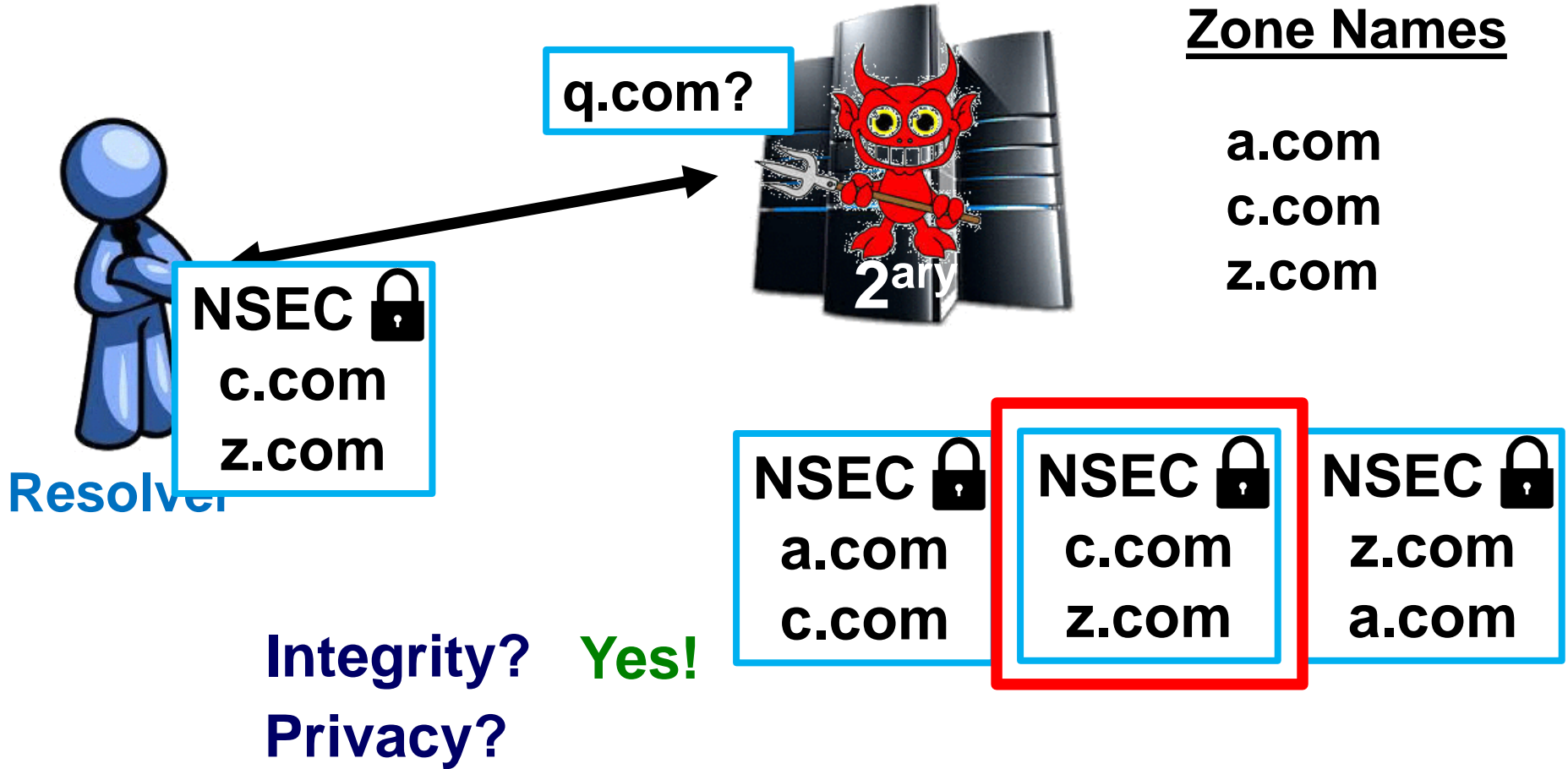
RFC 4034 – NSEC



RFC 4034 – NSEC



RFC 4034 – NSEC



RFC 4034 – NSEC



q.com?



Zone Names

a.com
c.com
z.com

NSEC 
c.com
z.com

NSEC 
a.com
c.com

NSEC 
c.com
z.com

NSEC 
z.com
a.com

Integrity?

Yes!

Privacy?

No! Can enumerate over the names



Zone enumeration is an issue



Zone enumeration is an issue

- Can expose private device names in the network



Zone enumeration is an issue

- Can expose private device names in the network
- Can be a source for probable email addresses for spam



Zone enumeration is an issue

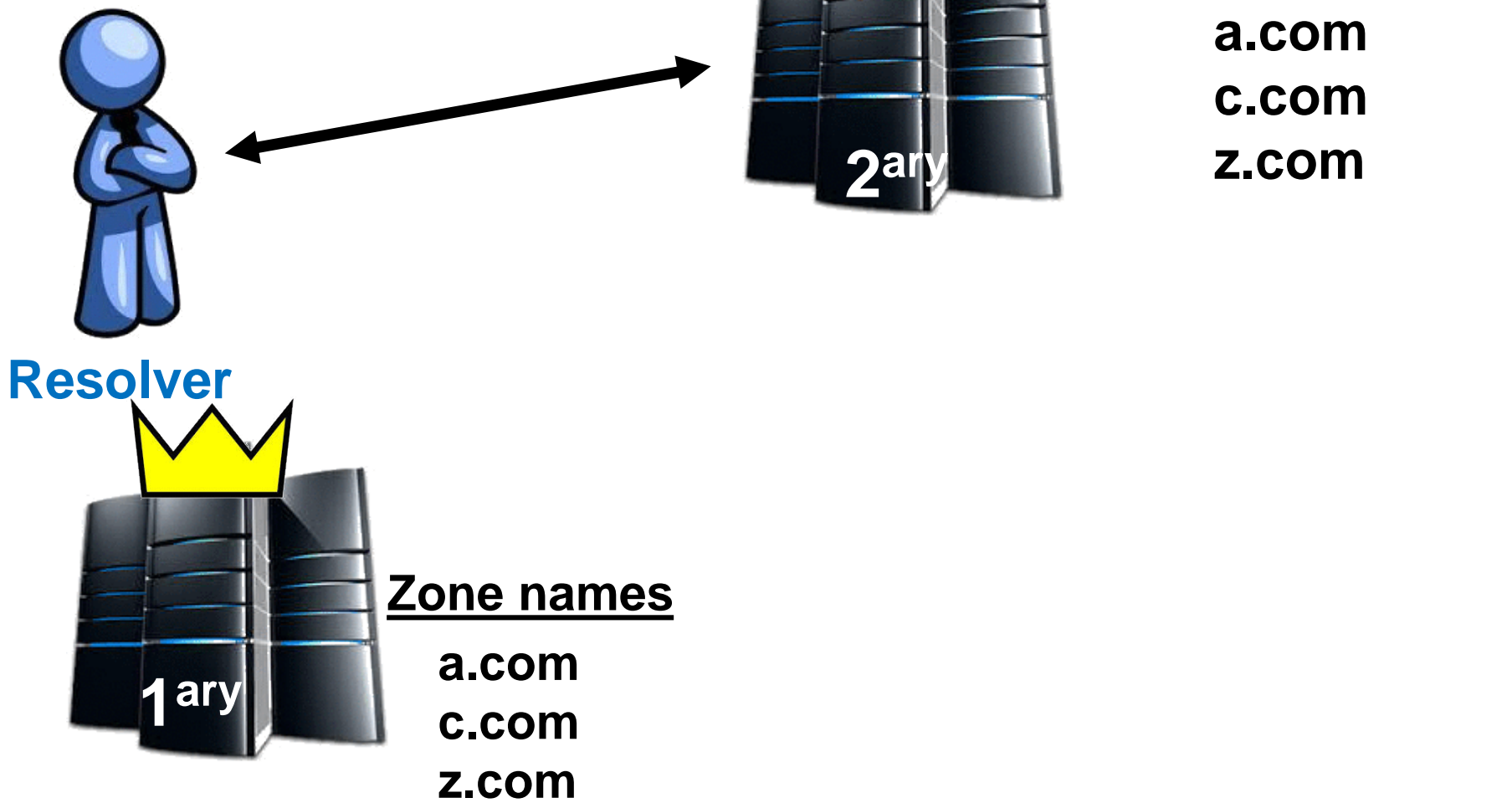
- Can expose private device names in the network
- Can be a source for probable email addresses for spam
- Can be used to reveal information that domain registries are **legally obliged to protect**
(e.g., EU-registries due to European Data Privacy Directive)



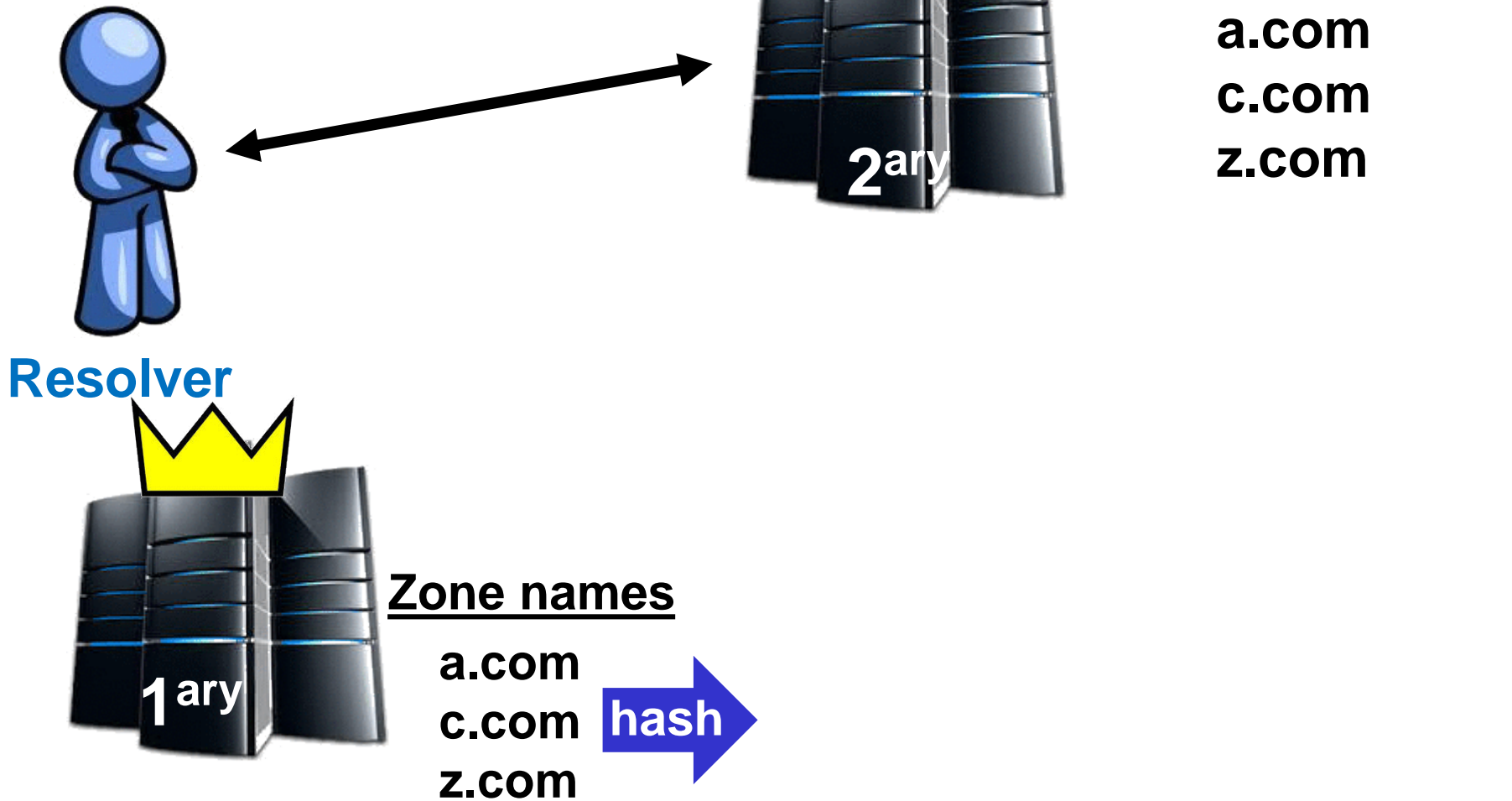
Zone enumeration is an issue

- Can expose private device names in the network
- Can be a source for probable email addresses for spam
- Can be used to reveal information that domain registries are **legally obliged to protect** (e.g., EU-registries due to European Data Privacy Directive)
- Formalized in **RFC 5155**, as a requirement for DNSSEC, which introduces **NSEC3**

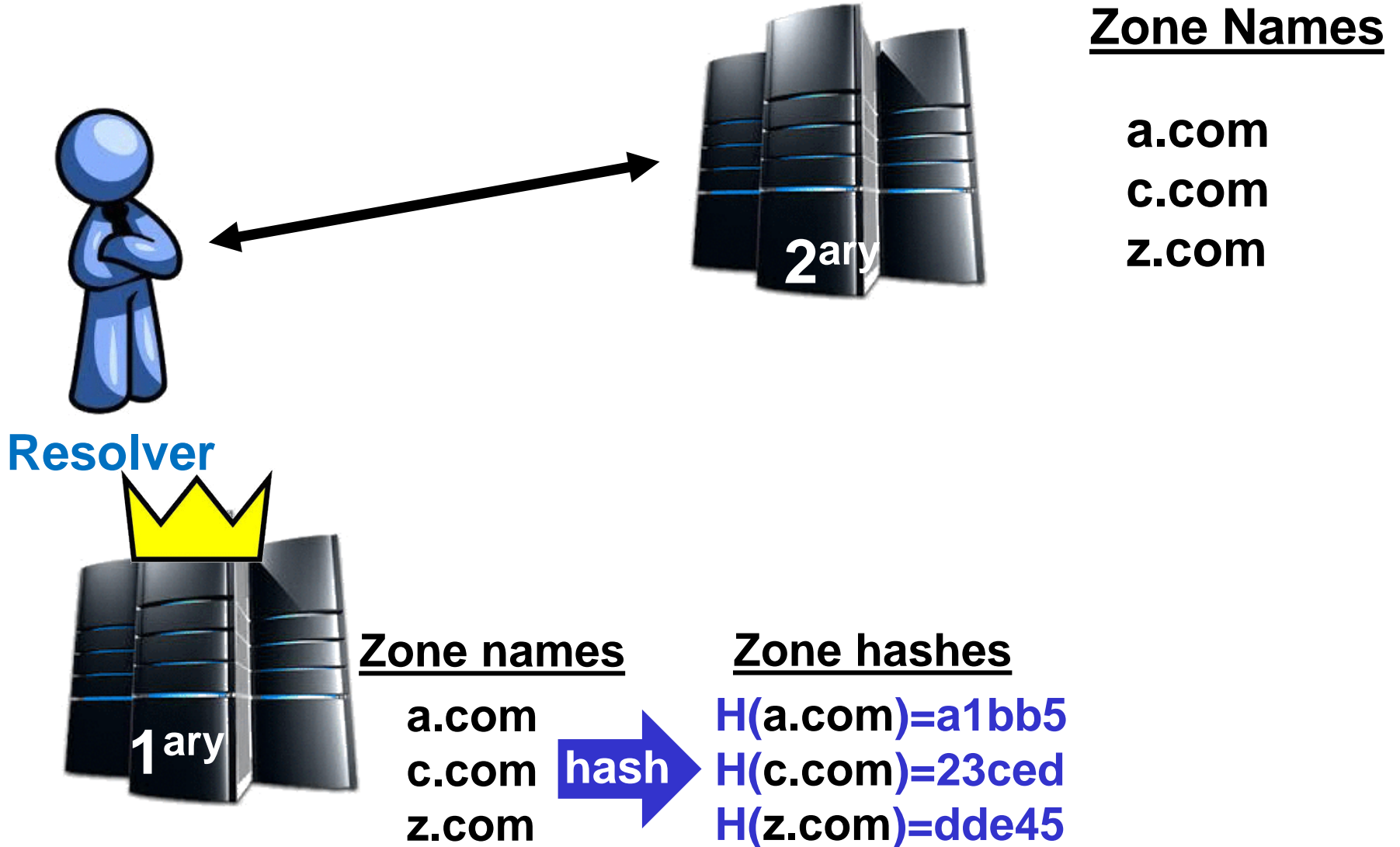
RFC 5155 – NSEC3



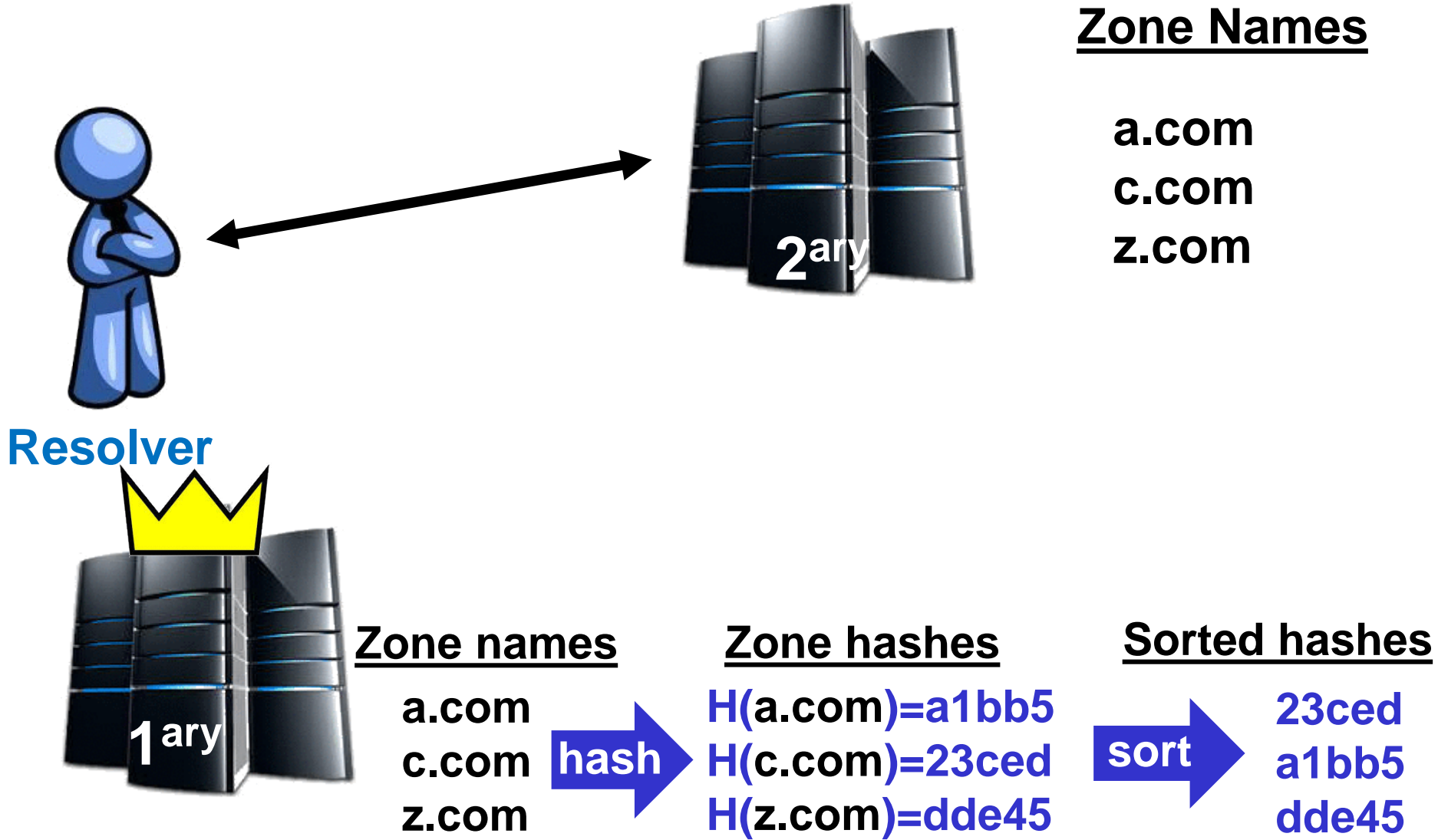
RFC 5155 – NSEC3



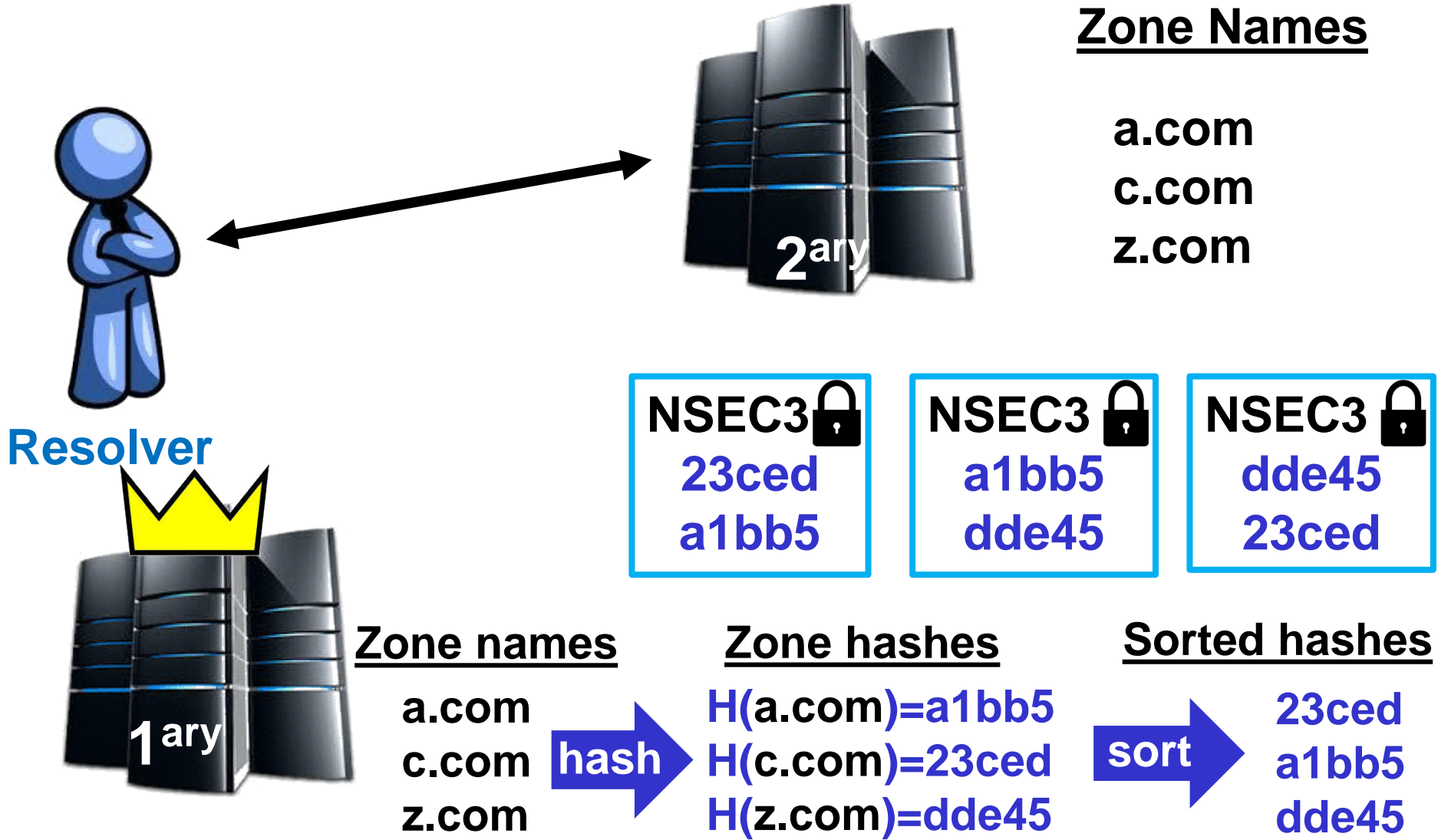
RFC 5155 – NSEC3



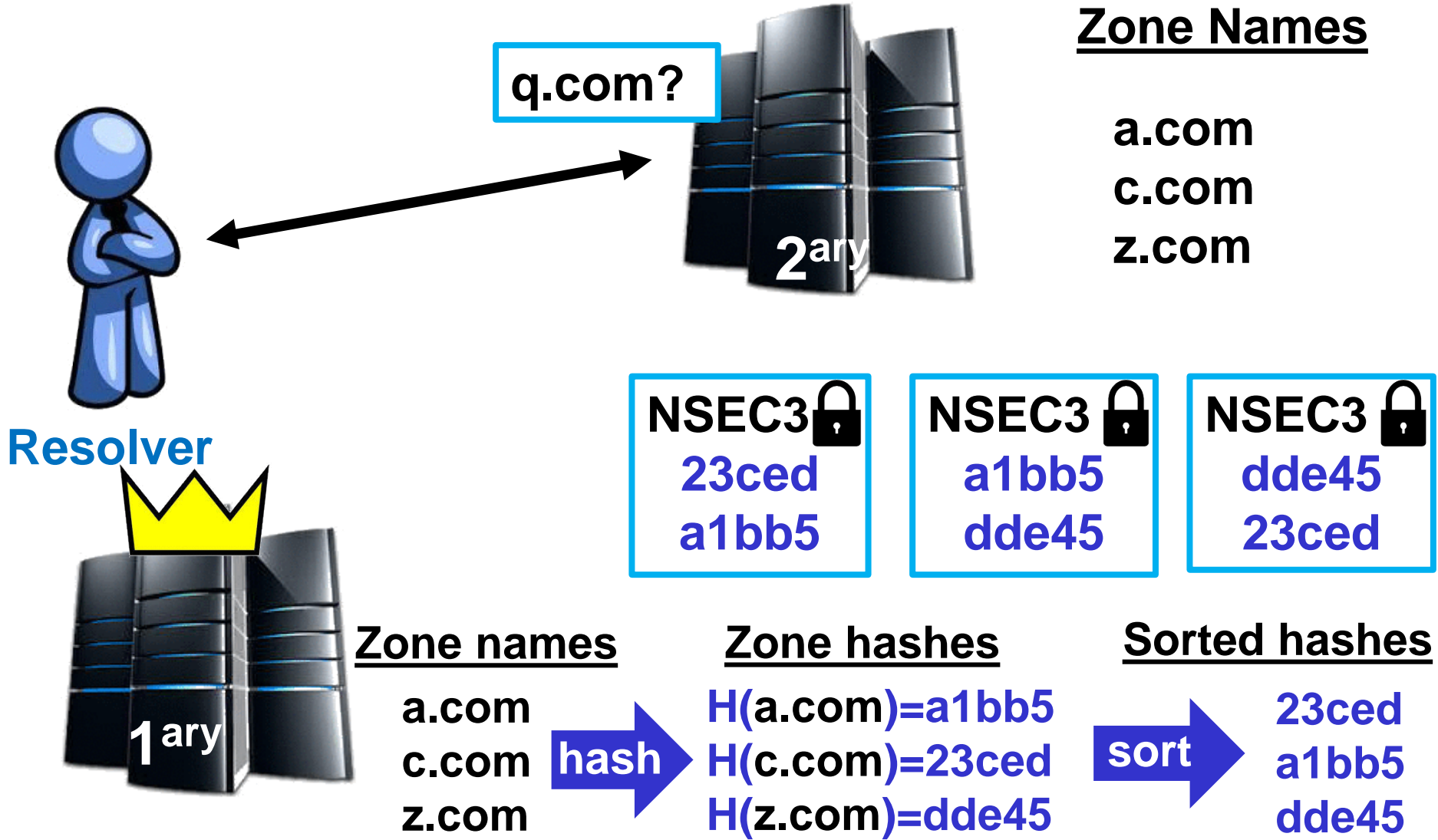
RFC 5155 – NSEC3



RFC 5155 – NSEC3



RFC 5155 – NSEC3



RFC 5155 – NSEC3

$H(q.com)=b35e7$

Zone Names

a.com
c.com
z.com

q.com?

2ary

Resolver

NSEC3 

23ced
a1bb5

NSEC3 

a1bb5
dde45

NSEC3 

dde45
23ced

Zone names

a.com
c.com
z.com

hash

Zone hashes

$H(a.com)=a1bb5$
 $H(c.com)=23ced$
 $H(z.com)=dde45$

Sorted hashes

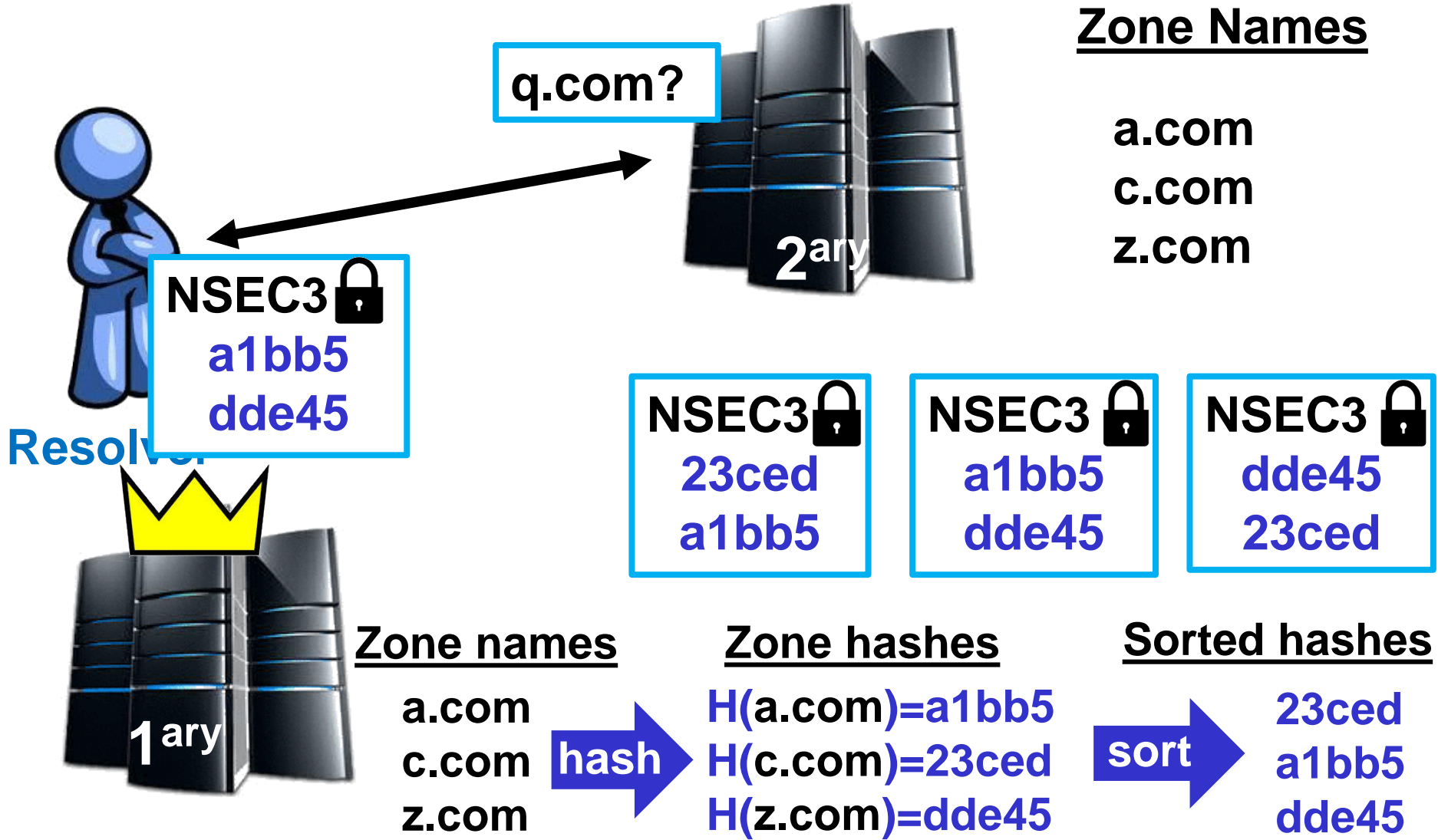
sort

23ced
a1bb5
dde45



RFC 5155 – NSEC3

$H(q.com)=b35e7$



RFC 5155 – NSEC3


$H(q.com)=b35e7$

Zone Names


a.com
c.com
z.com


q.com?




NSEC3 
a1bb5
dde45

Resolver

NSEC3 
23ced
a1bb5

NSEC3 
a1bb5
dde45

NSEC3 
dde45
23ced

Integrity?

RFC 5155 – NSEC3


$H(q.com)=b35e7$

Zone Names

a.com
c.com
z.com


q.com?




NSEC3 
a1bb5
dde45

Resolver

NSEC3 
23ced
a1bb5

NSEC3 
a1bb5
dde45

NSEC3 
dde45
23ced

Integrity?
Privacy?

RFC 5155 – NSEC3



Zone Names

a.com
c.com
z.com

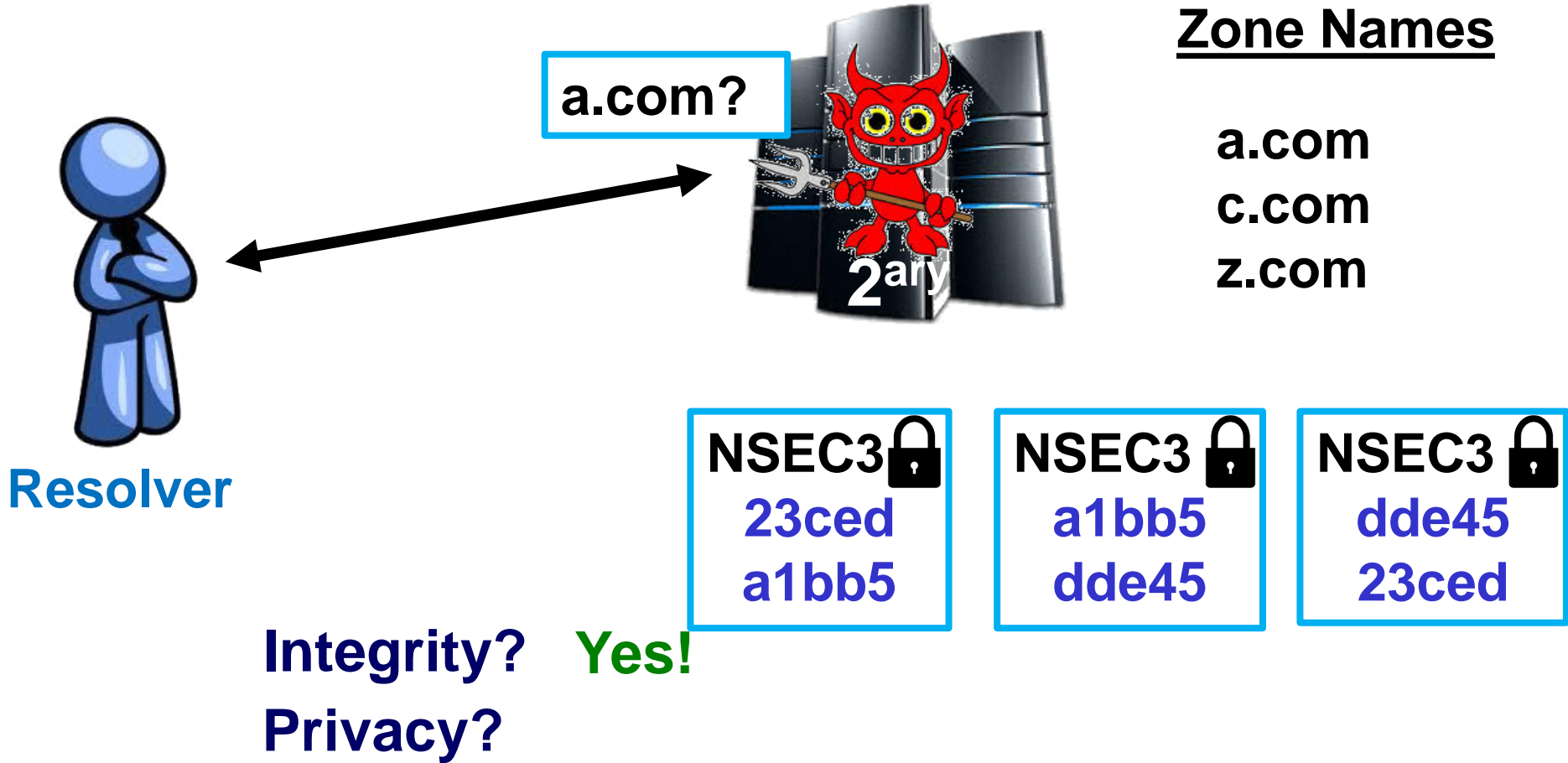
NSEC3 
23ced
a1bb5

NSEC3 
a1bb5
dde45

NSEC3 
dde45
23ced

Integrity? **Yes!**
Privacy?

RFC 5155 – NSEC3



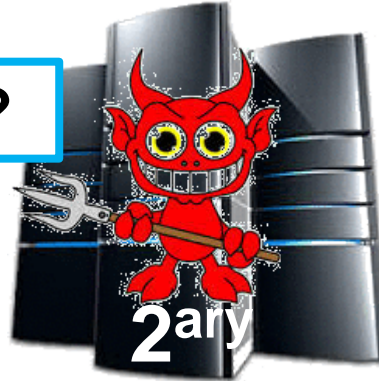
RFC 5155 – NSEC3

$H(a.com)=a1bb5$

Zone Names

a.com
c.com
z.com


a.com?




Resolver



NSEC3 
23ced
a1bb5

NSEC3 
a1bb5
dde45

NSEC3 
dde45
23ced

Integrity? **Yes!**

Privacy?

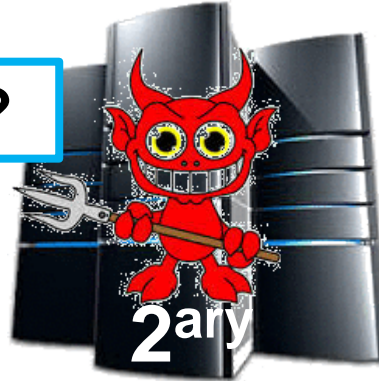
RFC 5155 – NSEC3

$H(a.com)=a1bb5$

Zone Names

a.com
c.com
z.com

a.com?



Resolver

NSEC3  23ced a1bb5	NSEC3  a1bb5 dde45	NSEC3  dde45 23ced
--	--	--

Integrity? **Yes!**

Privacy?

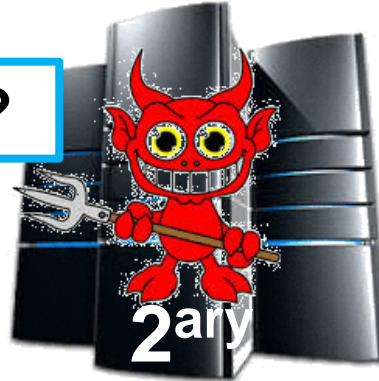
RFC 5155 – NSEC3

$H(a.com)=a1bb5$

Zone Names

a.com
c.com
z.com


a.com?



Resolver



NSEC3 
23ced
a1bb5

NSEC3 
a1bb5
dde45

NSEC3 
dde45
23ced

Integrity? **Yes!**
Privacy?

RFC 5155 – NSEC3



Zone Names

a.com
c.com
z.com

NSEC3 
23ced
a1bb5

NSEC3 
a1bb5
dde45

NSEC3 
dde45
23ced

Integrity? **Yes!**
Privacy? **Still no**

Zone enumeration in NSEC3



Resolver



Zone Names

a.com
c.com
z.com

NSEC3 
23ced
a1bb5

NSEC3 
a1bb5
dde45

NSEC3 
dde45
23ced

Zone enumeration in NSEC3



Random queries




Resolver



Zone Names

a.com
c.com
z.com

NSEC3 
23ced
a1bb5

NSEC3 
a1bb5
dde45

NSEC3 
dde45
23ced

Zone enumeration in NSEC3



Random queries




Zone Names

a.com
c.com
z.com



Resolver

NSEC3 
23ced
a1bb5

NSEC3 
a1bb5
dde45

NSEC3 
dde45
23ced

Zone enumeration in NSEC3



Random queries



Zone Names

a.com
c.com
z.com

Resolver

Learned hashes

23ced
a1bb5
dde45

Zone enumeration in NSEC3



Random queries



Zone Names

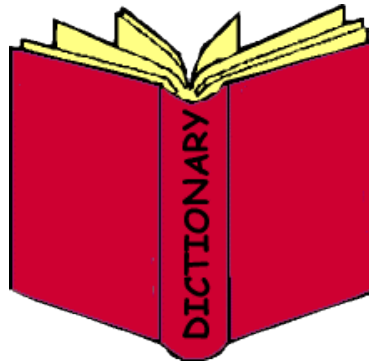
a.com
c.com
z.com

Resolver

Learned hashes

23ced
a1bb5
dde45

Make a dictionary of plausible names



a.com
b.com
c.com
...
z.com

Zone enumeration in NSEC3



Random queries



Zone Names

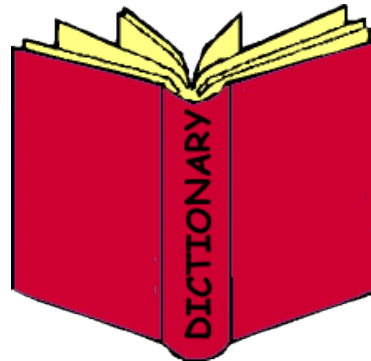
a.com
c.com
z.com

Resolver

Learned hashes

23ced
a1bb5
dde45

Make a dictionary of plausible names



a.com
b.com
c.com
...
z.com

Hash dictionary to find matches

$H(a.com)=a1bb5$
 $H(b.com)=a1bb5$
 $H(c.com)=23ced$
 $H(z.com)=dde45$

Zone enumeration in NSEC3



Random queries



Zone Names

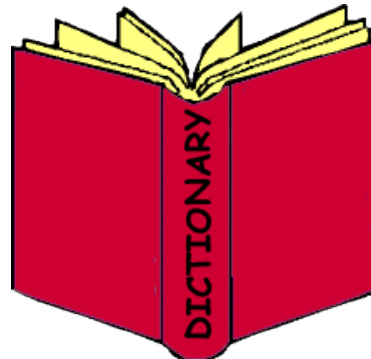
a.com
c.com
z.com

Resolver

Learned hashes

23ced
a1bb5
dde45

Make a dictionary of plausible names

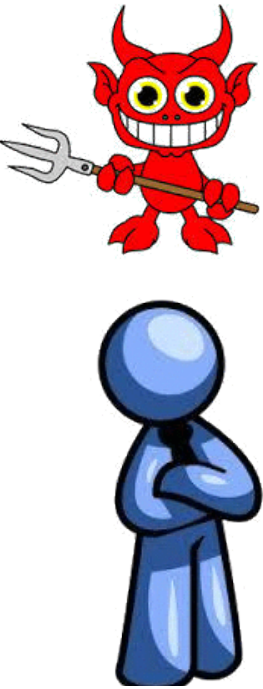


a.com
b.com
c.com
...
z.com

Hash dictionary to find matches

H(a.com)=a1bb5
H(b.com)=a1bb5
H(c.com)=23ced
H(z.com)=dde45

Zone enumeration in NSEC3



Random
queries



Zone Names

a.com
c.com
z.com

Resolver

NSEC3 zone enumeration has been demonstrated:

- [Wander, Schwittmann, Boelmann, Weis 2014] enumerated **64% of the .com TLD in under 5 days using one GPU.**
- In 2011, [Bernstein]'s `nsec3walker` guessed 2^{34} hashes/per day on a laptop.

Existing solutions summary

	Integrity against outsiders	Integrity against compromised 2 ^{dry} nameserver	No zone enumeration
DNS	X	X	✓

Existing solutions summary

	Integrity against outsiders	Integrity against compromised 2 ^{dry} nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓

Existing solutions summary

	Integrity against outsiders	Integrity against compromised 2 ^{dry} nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓
NSEC	✓	✓	✗

Existing solutions summary

	Integrity against outsiders	Integrity against compromised 2 ^{dry} nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓
NSEC	✓	✓	✗
NSEC3	✓	✓	✗

Existing solutions summary

	Integrity against outsiders	Integrity against compromised 2 ^{dry} nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓
NSEC	✓	✓	✗
NSEC3	✓	✓	✗

NSEC5 Desiderata

Existing solutions summary

	Integrity against outsiders	Integrity against compromised 2 ^{dry} nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓
NSEC	✓	✓	✗
NSEC3	✓	✓	✗

NSEC5 Desiderata

1. **Integrity** (even when the nameserver was compromised)

Existing solutions summary

	Integrity against outsiders	Integrity against compromised 2 ^{dry} nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓
NSEC	✓	✓	✗
NSEC3	✓	✓	✗

NSEC5 Desiderata

1. **Integrity** (even when the nameserver was compromised)
2. Preventing **Zone enumeration**

Existing solutions summary

	Integrity against outsiders	Integrity against compromised 2 ^{dry} nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓
NSEC	✓	✓	✗
NSEC3	✓	✓	✗

NSEC5 Desiderata

1. **Integrity** (even when the nameserver was compromised)
2. Preventing **Zone enumeration**
3. **Efficiency and simplicity** (e.g. no “exotic” crypto)

The idea for constructing NSEC5

The idea for constructing NSEC5

Reason NSEC3 failed to prevent zone enumeration:
Resolvers can compute hashes offline

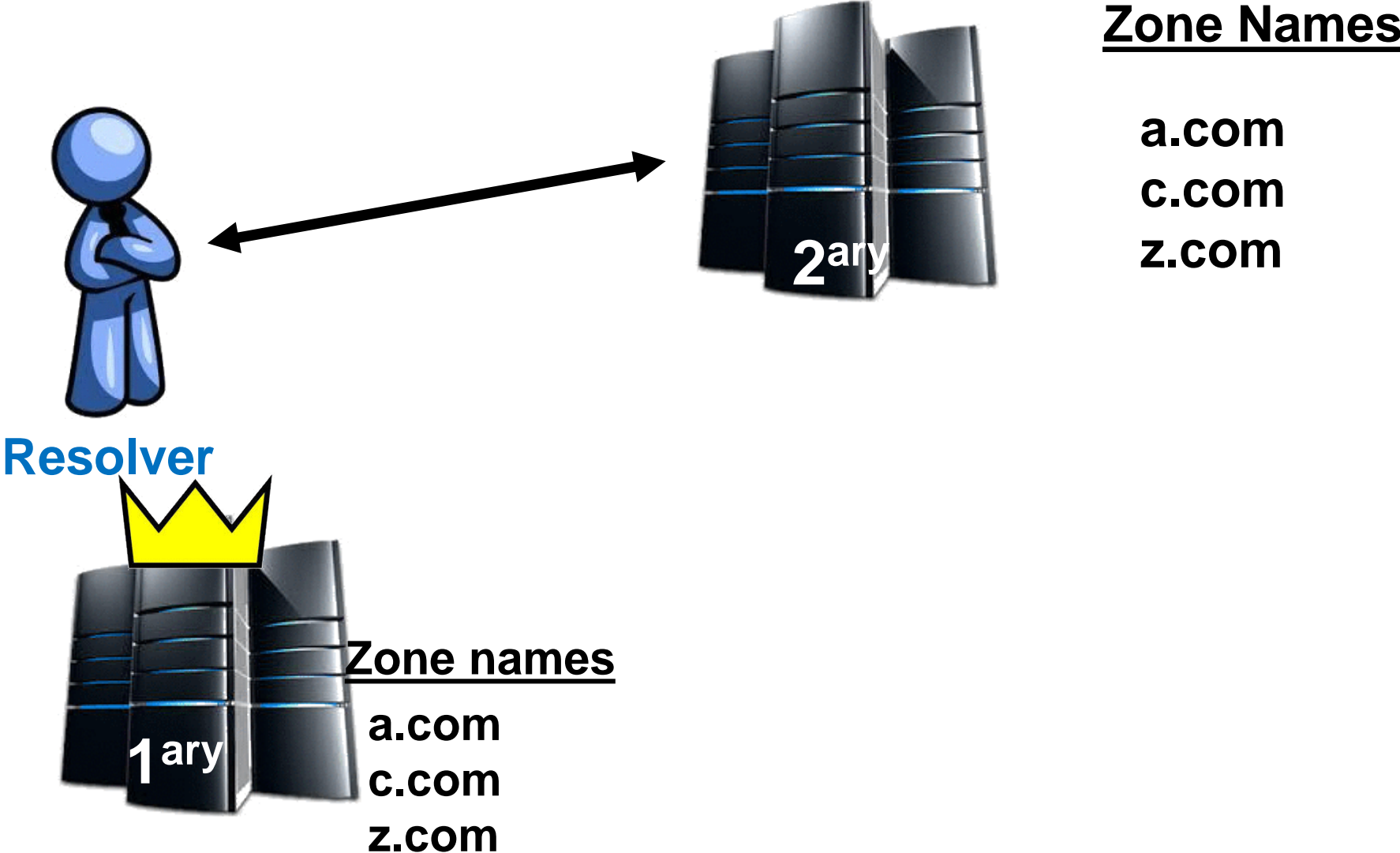
The idea for constructing NSEC5

Reason NSEC3 failed to prevent zone enumeration:
Resolvers can compute hashes offline

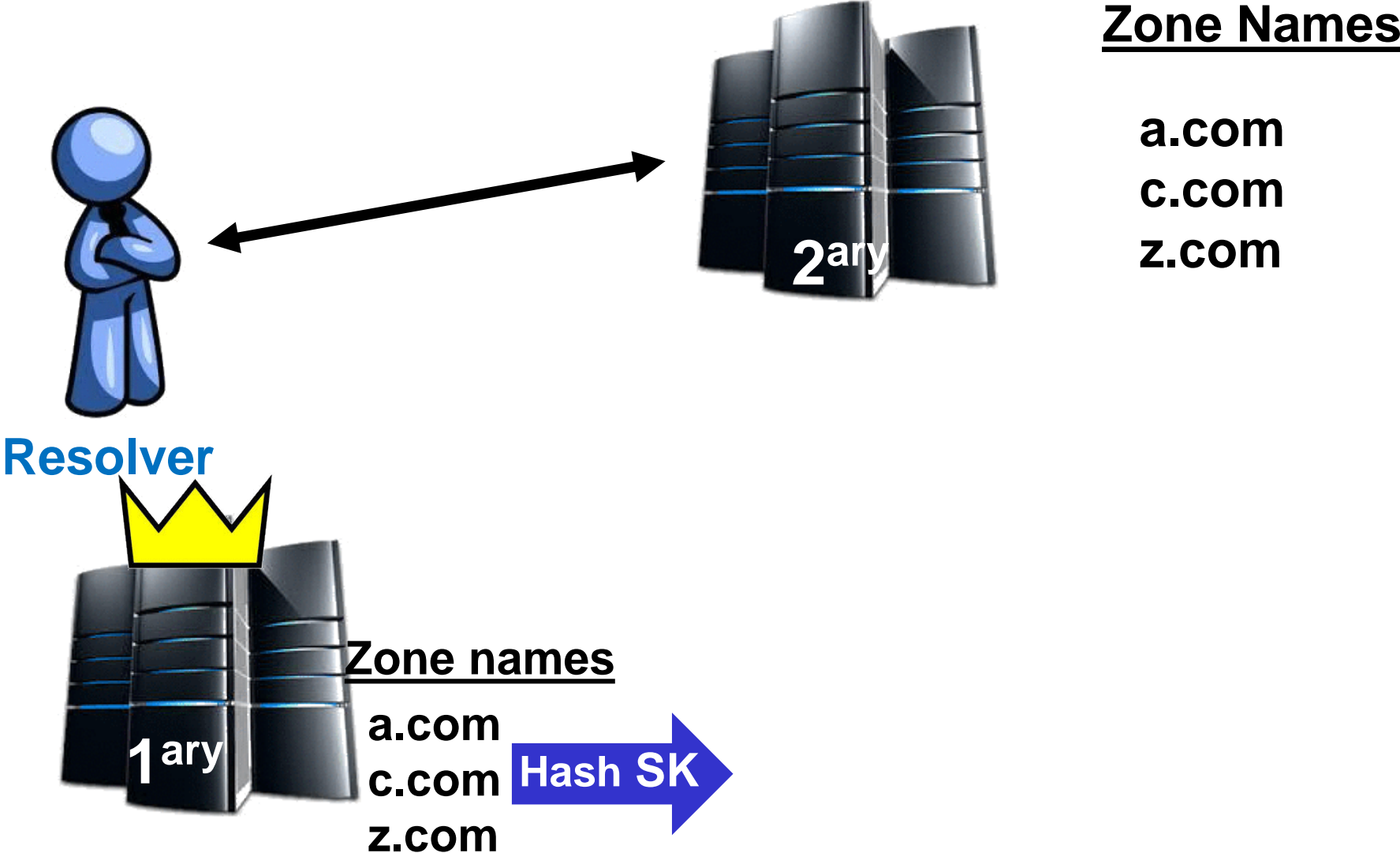
Solution:

add a **Secret NSEC5 Key** and a **Public NSEC5 Key**
required to compute and verify the hashes respectively

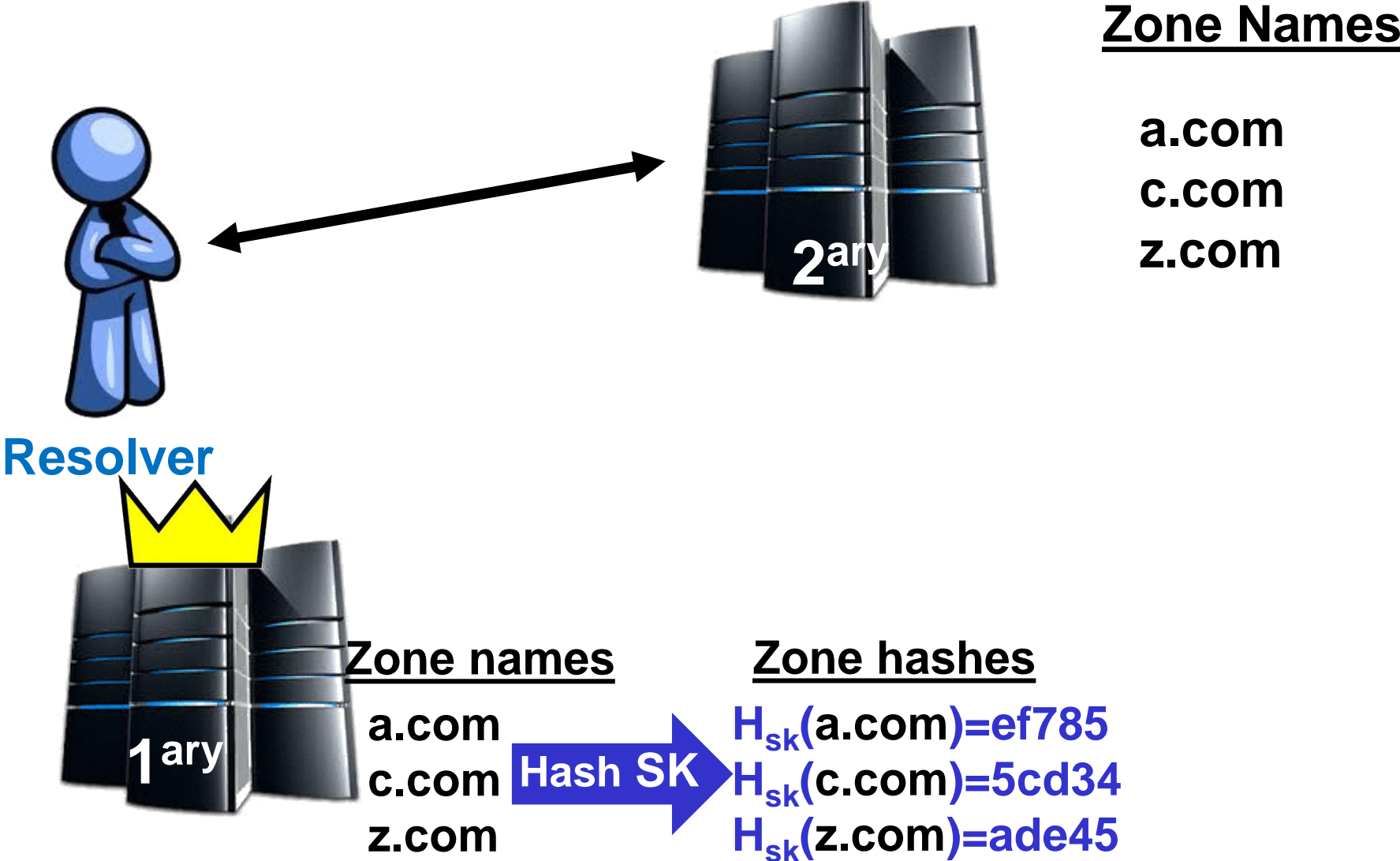
NSEC5 – Primary setup



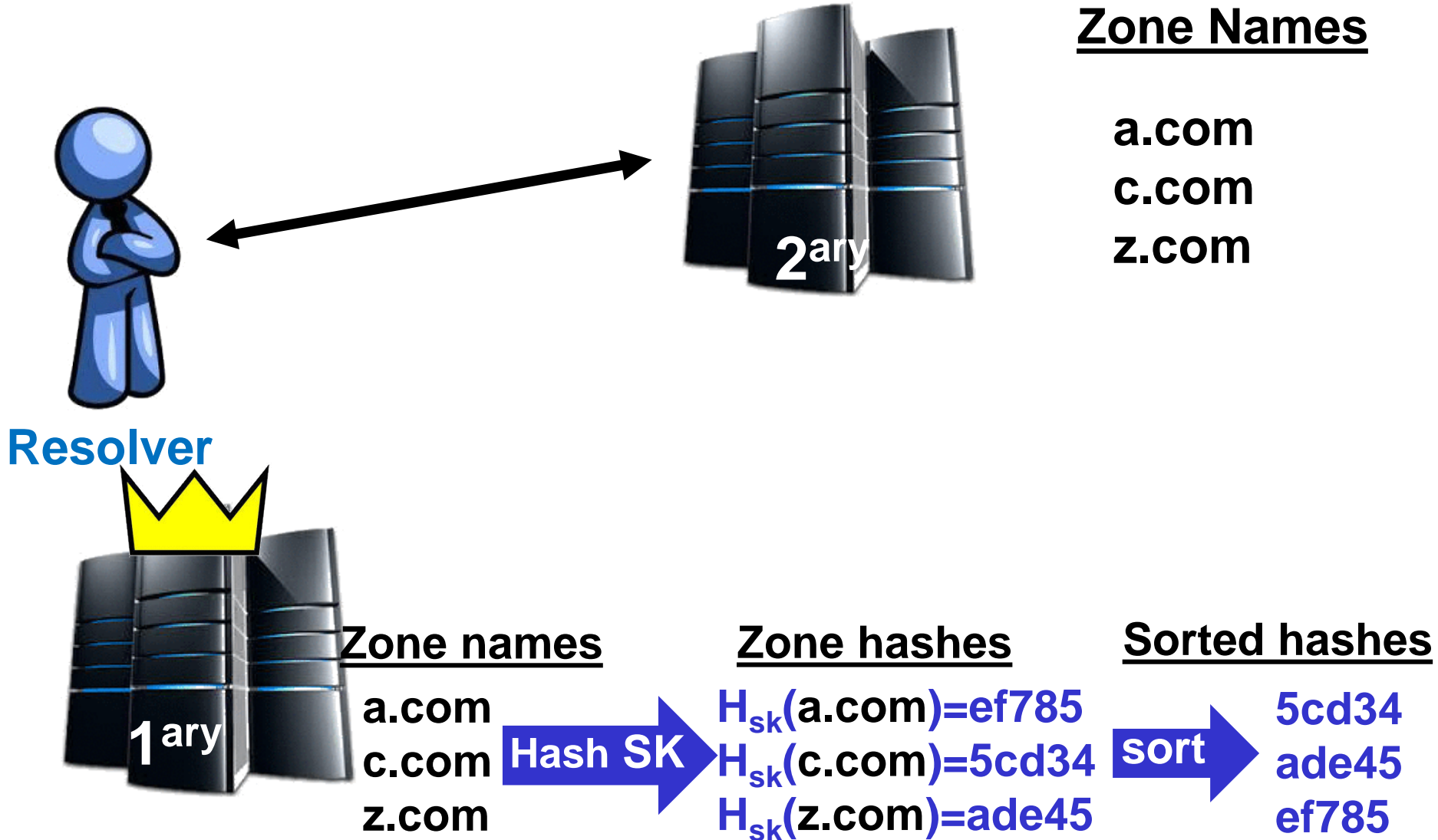
NSEC5 – Primary setup



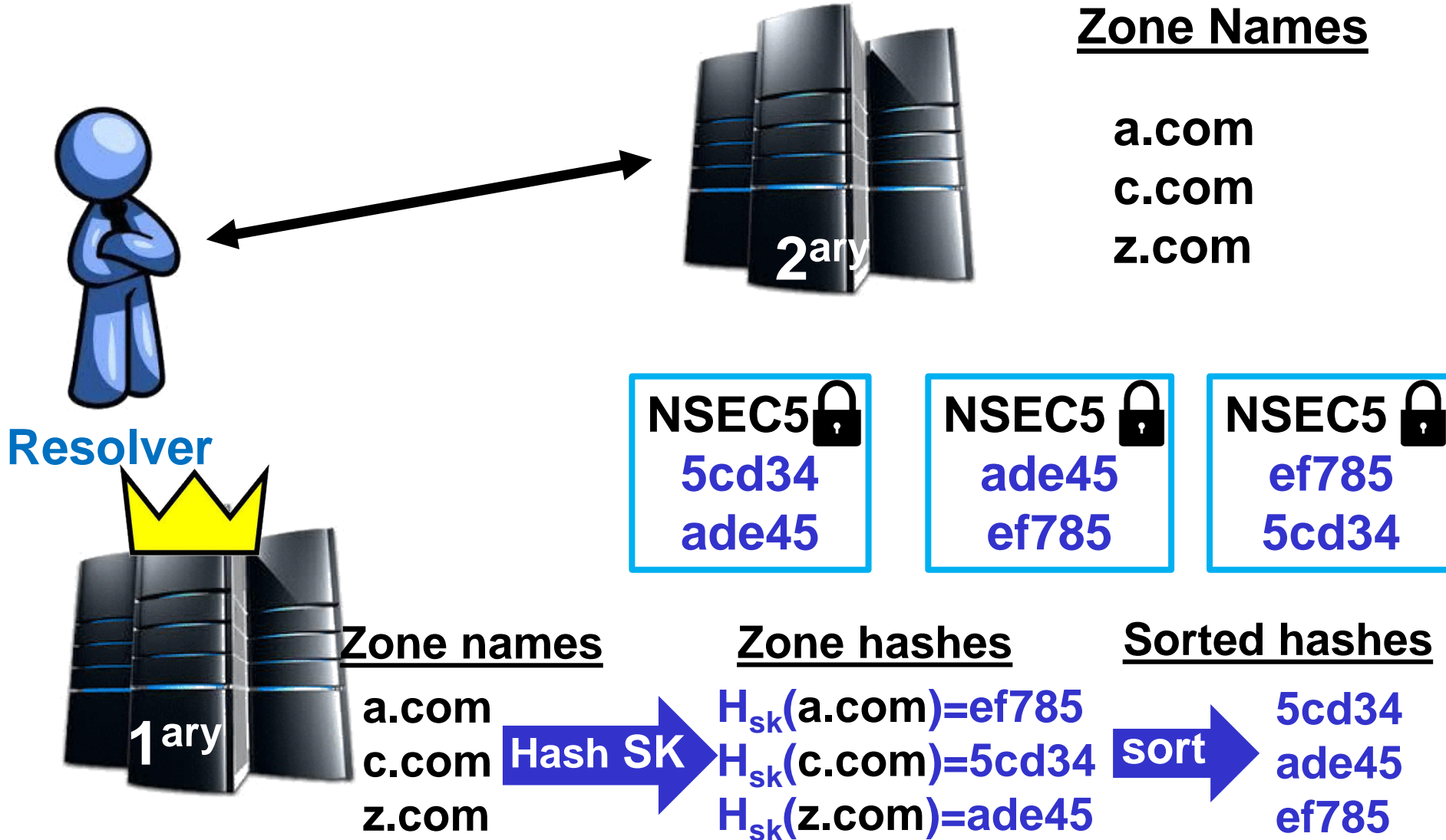
NSEC5 – Primary setup



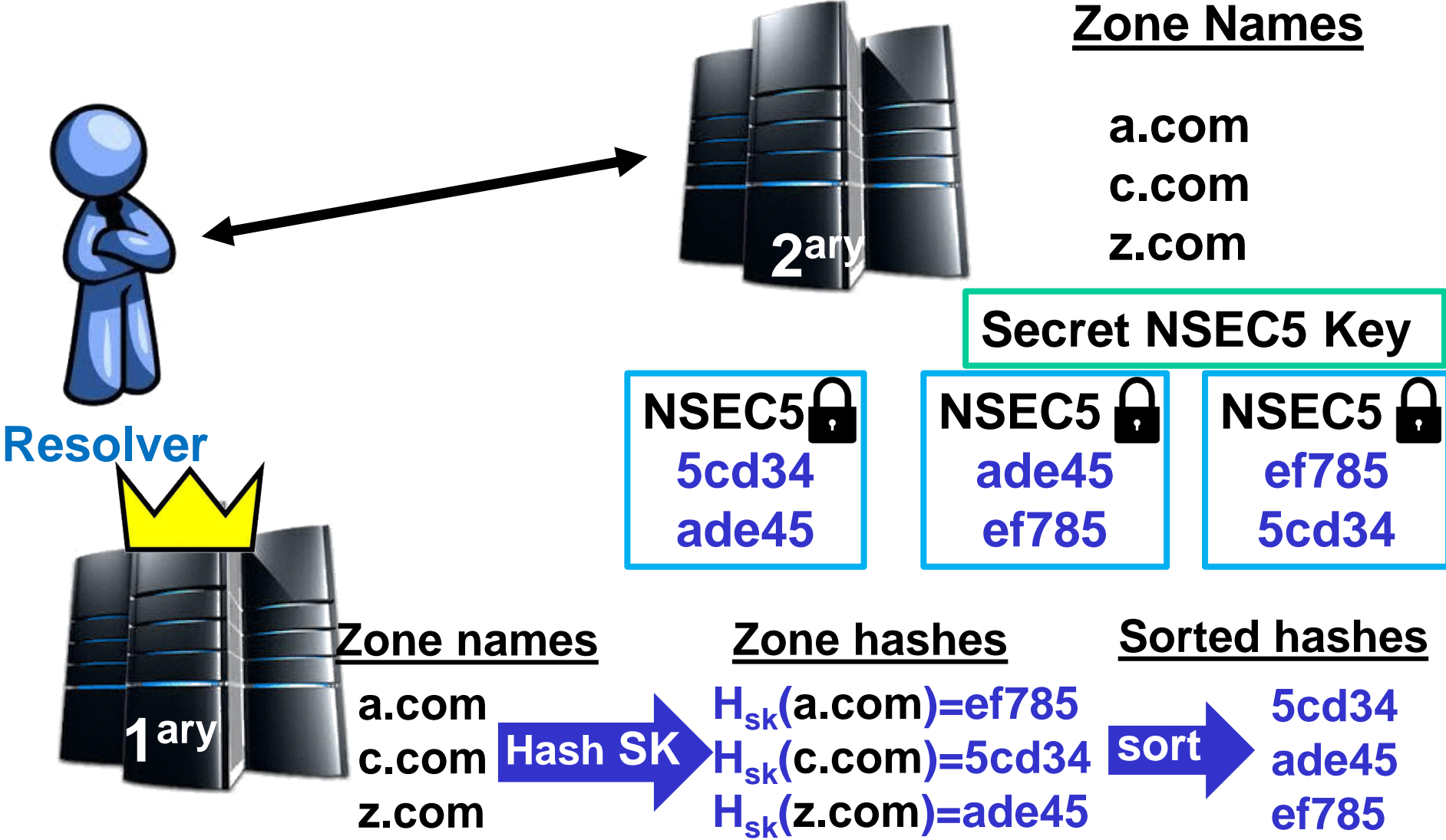
NSEC5 – Primary setup



NSEC5 – Primary setup



NSEC5 – Primary setup



NSEC5 – Primary setup

Public NSEC5 Key



Resolver



2ary

Zone Names

a.com
c.com
z.com

Secret NSEC5 Key

NSEC5
5cd34
ade45

NSEC5
ade45
ef785

NSEC5
ef785
5cd34



1ary

Zone names

a.com
c.com
z.com

Zone hashes

$H_{sk}(a.com)=ef785$
 $H_{sk}(c.com)=5cd34$
 $H_{sk}(z.com)=ade45$

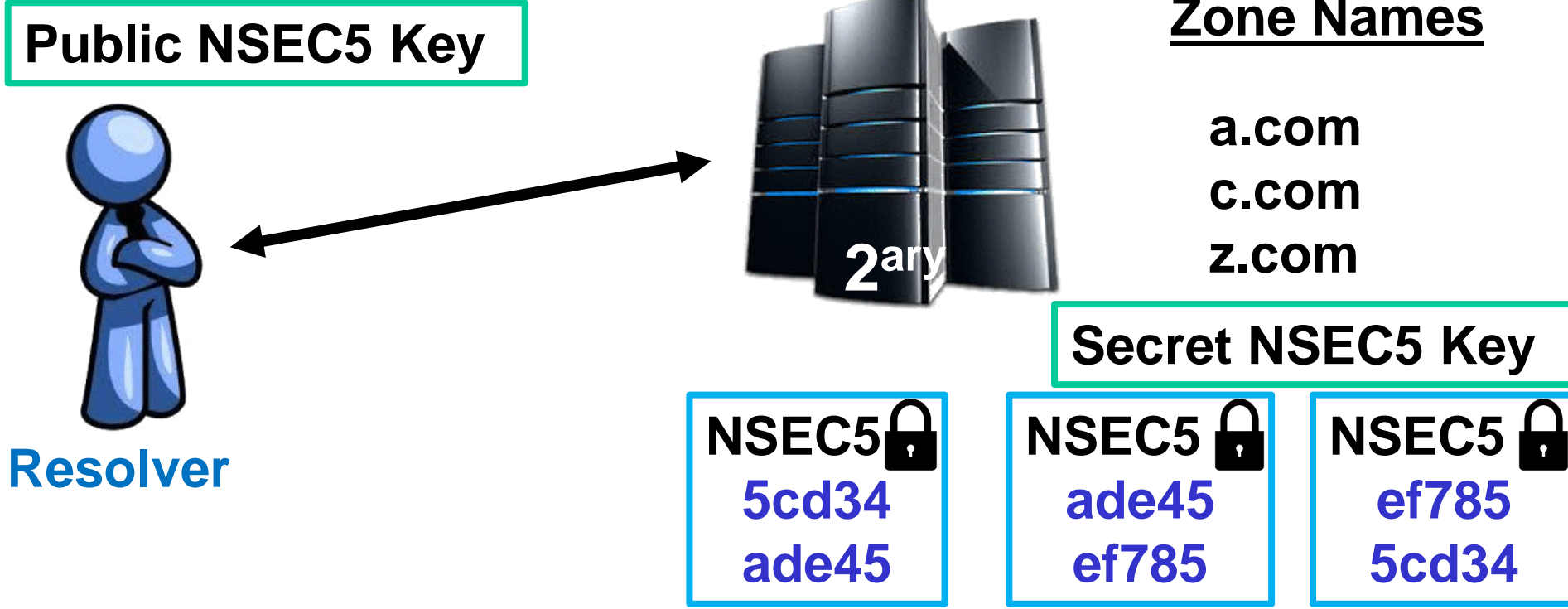
Sorted hashes

5cd34
ade45
ef785

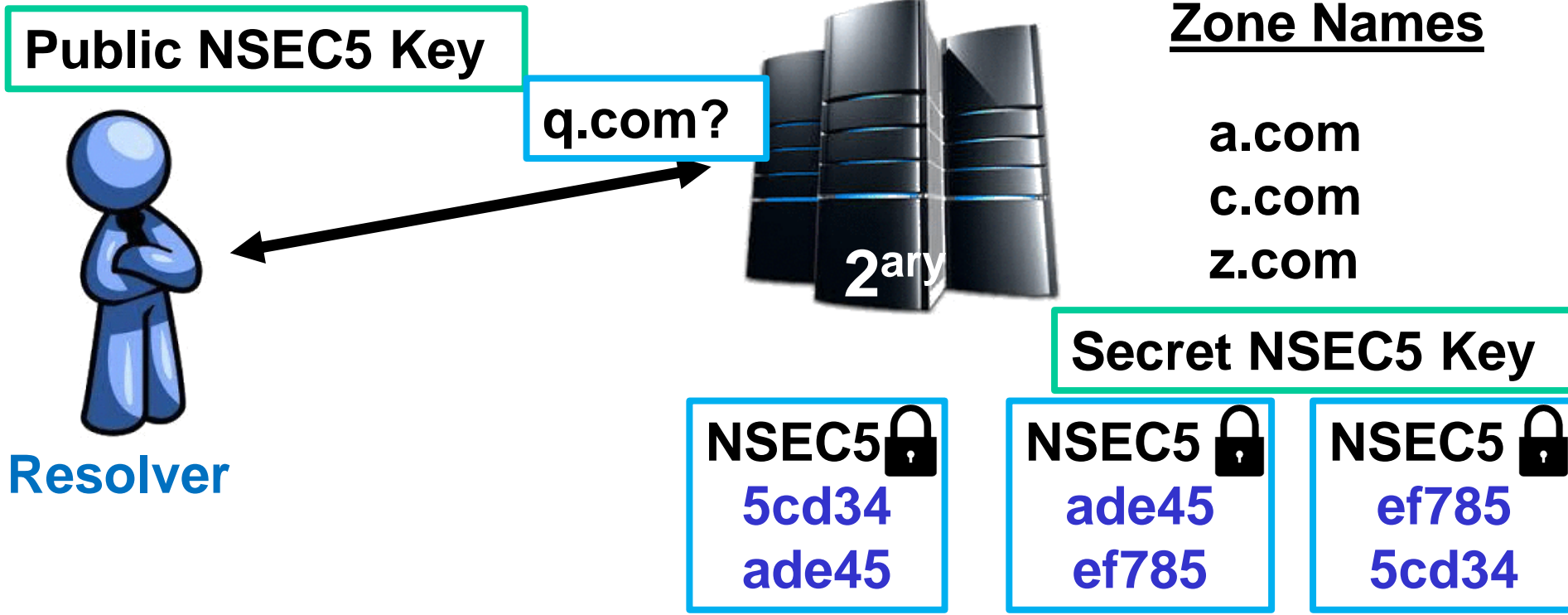
Hash SK

sort

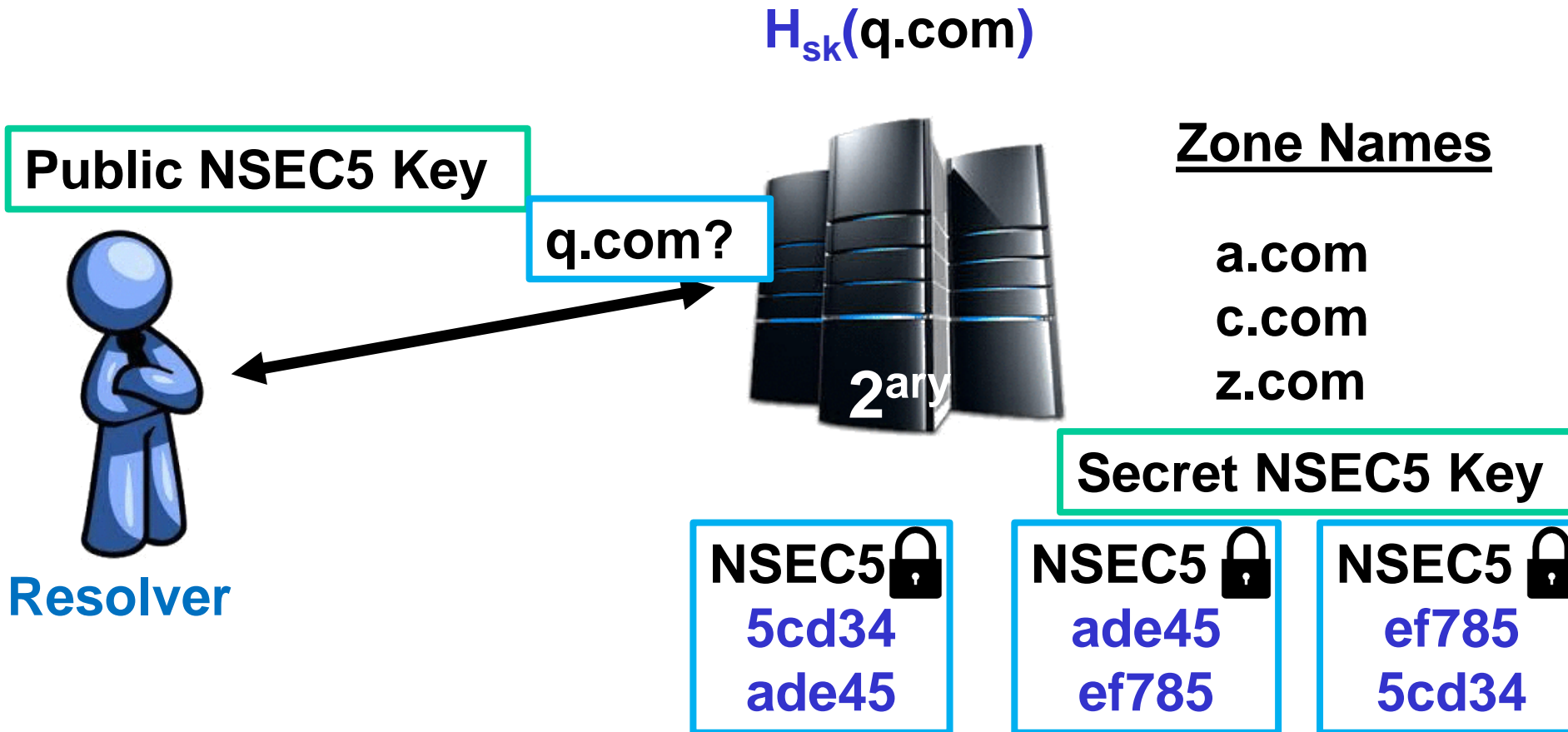
NSEC5 in action



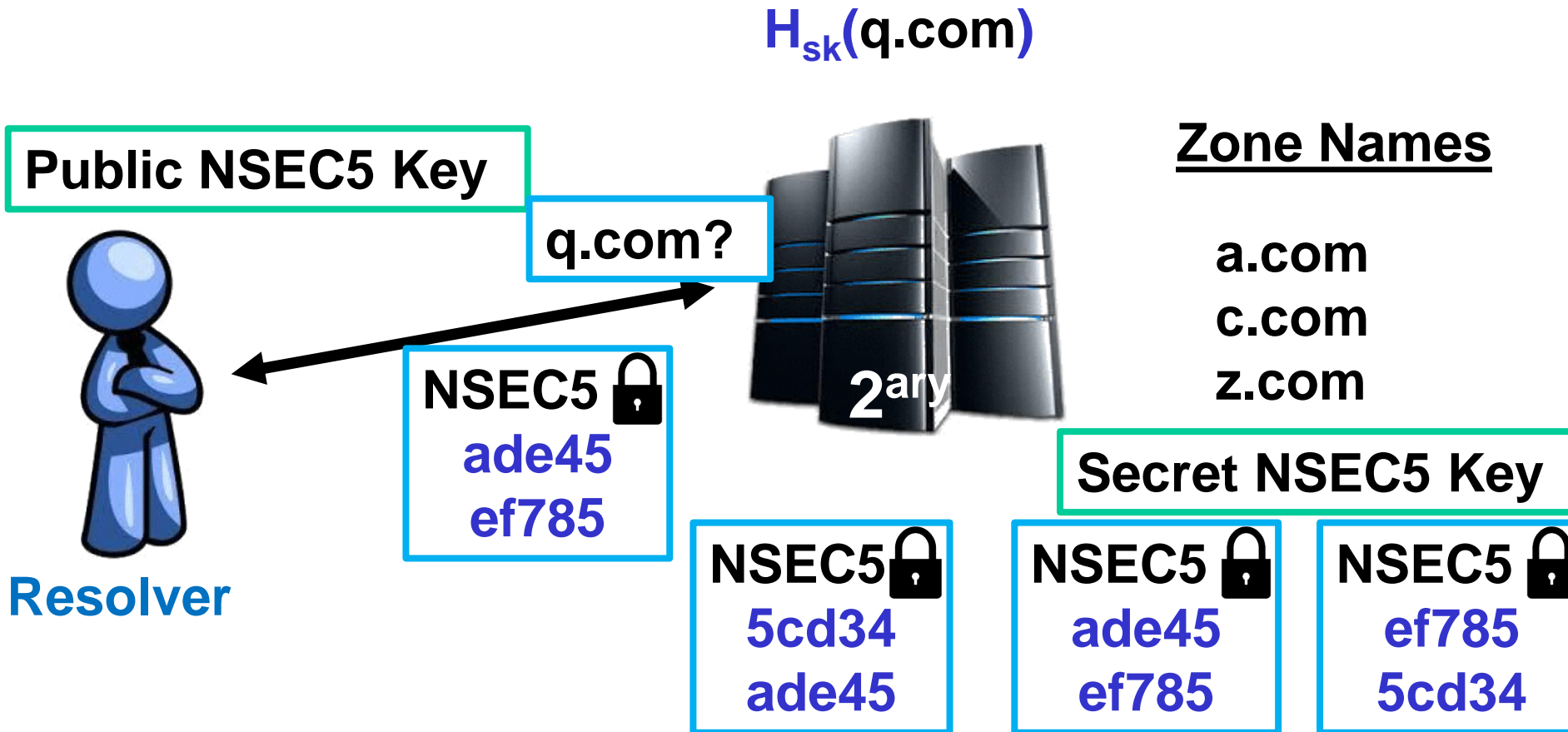
NSEC5 in action



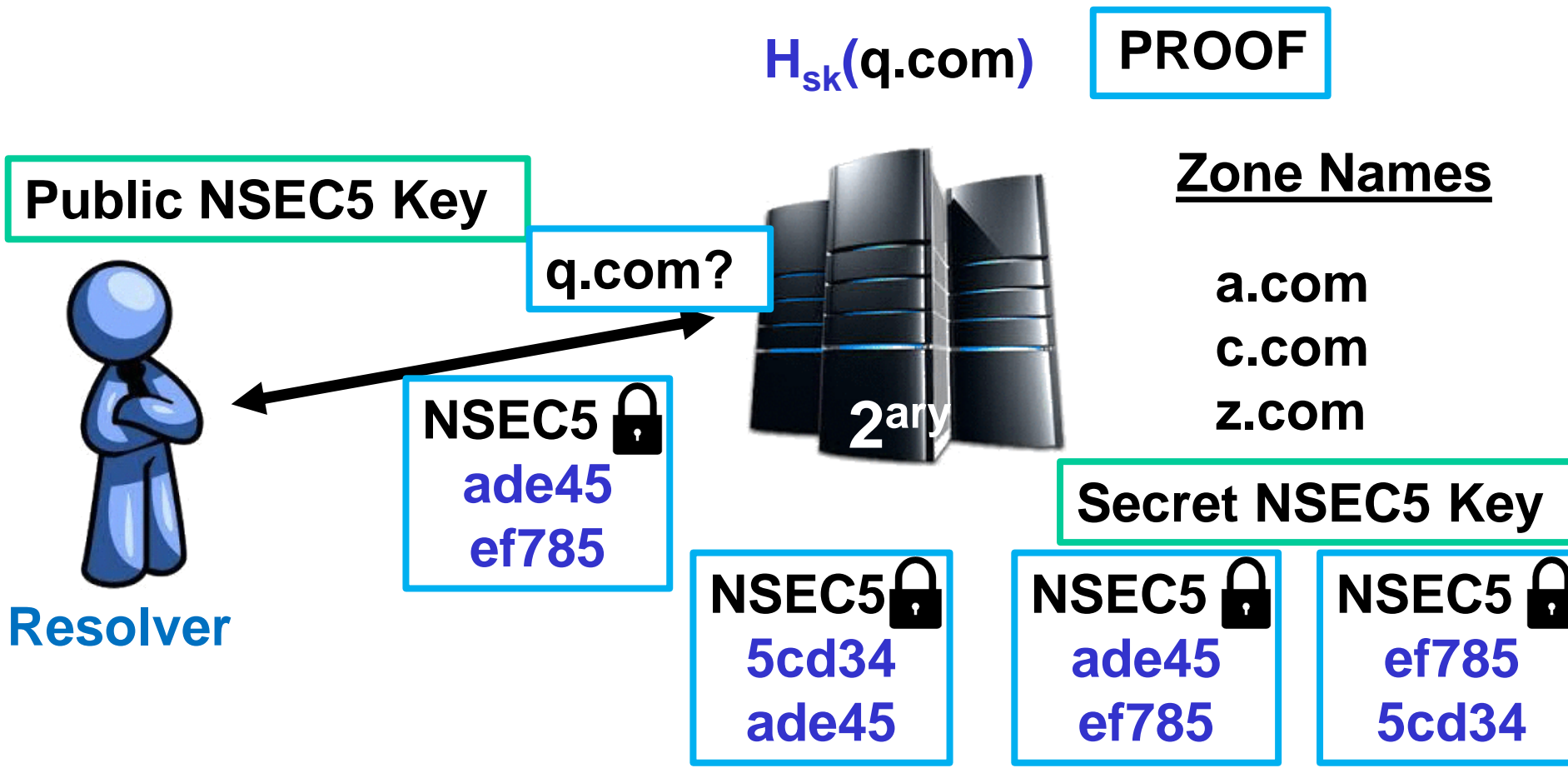
NSEC5 in action



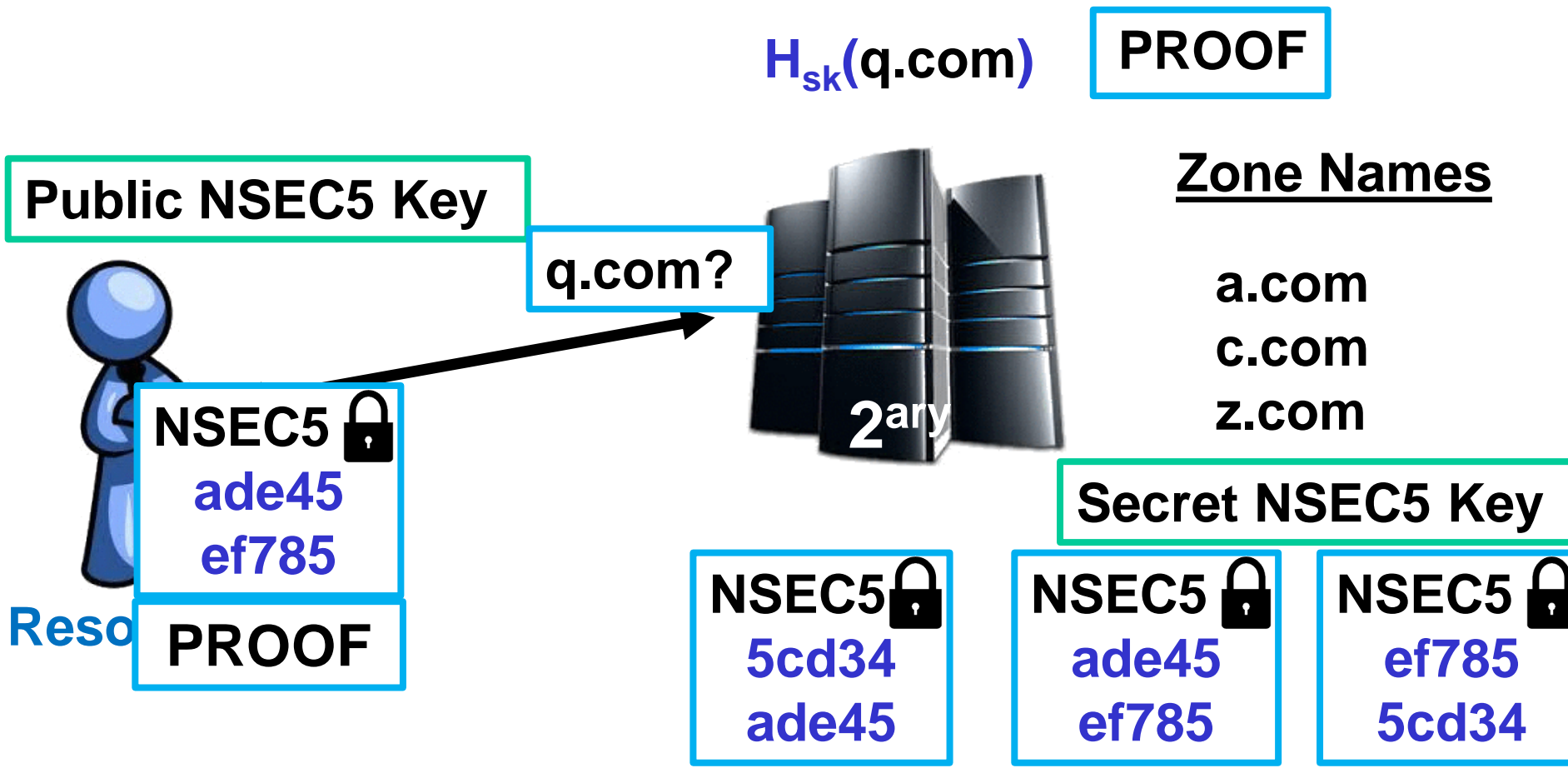
NSEC5 in action



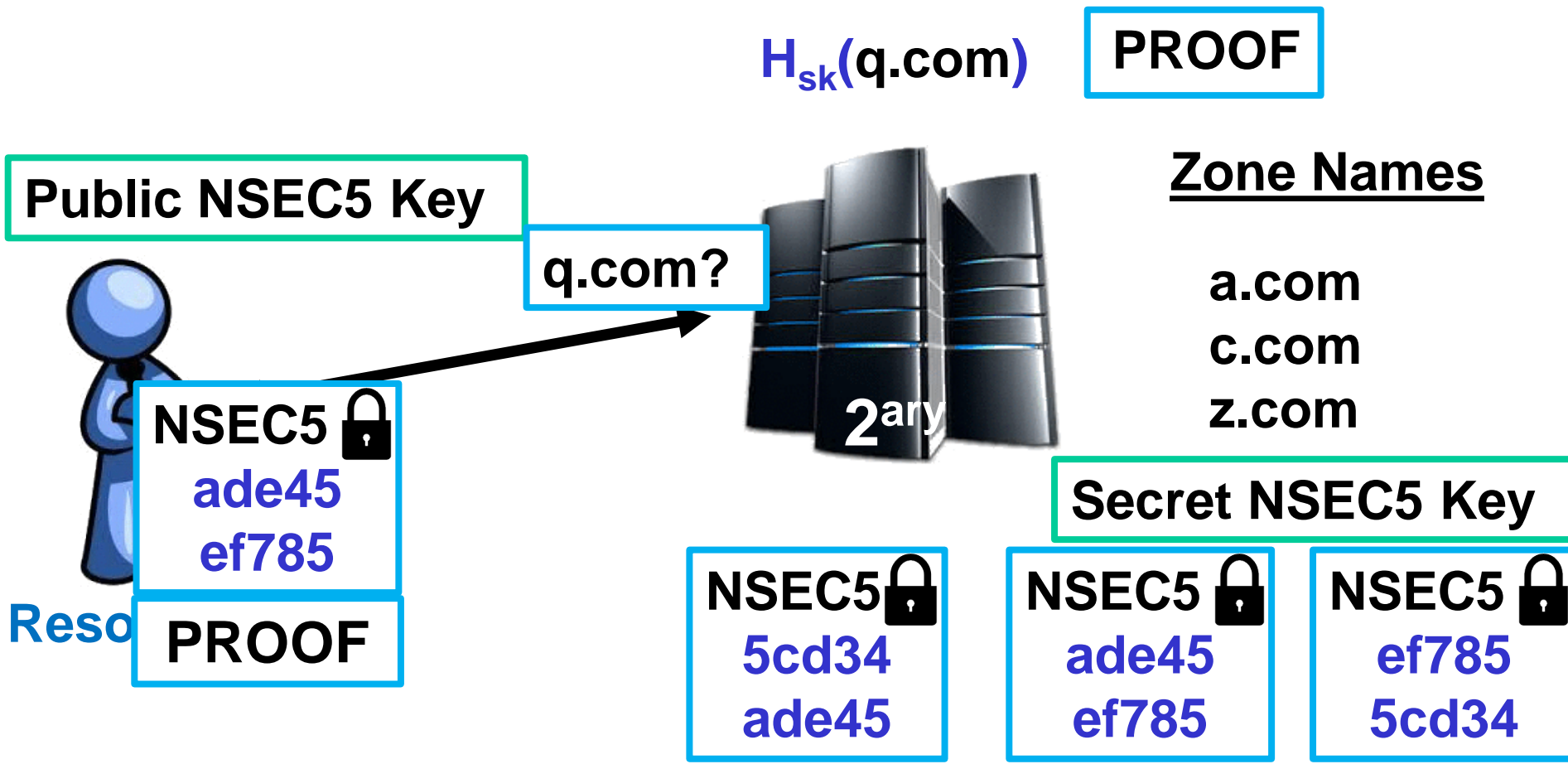
NSEC5 in action



NSEC5 in action

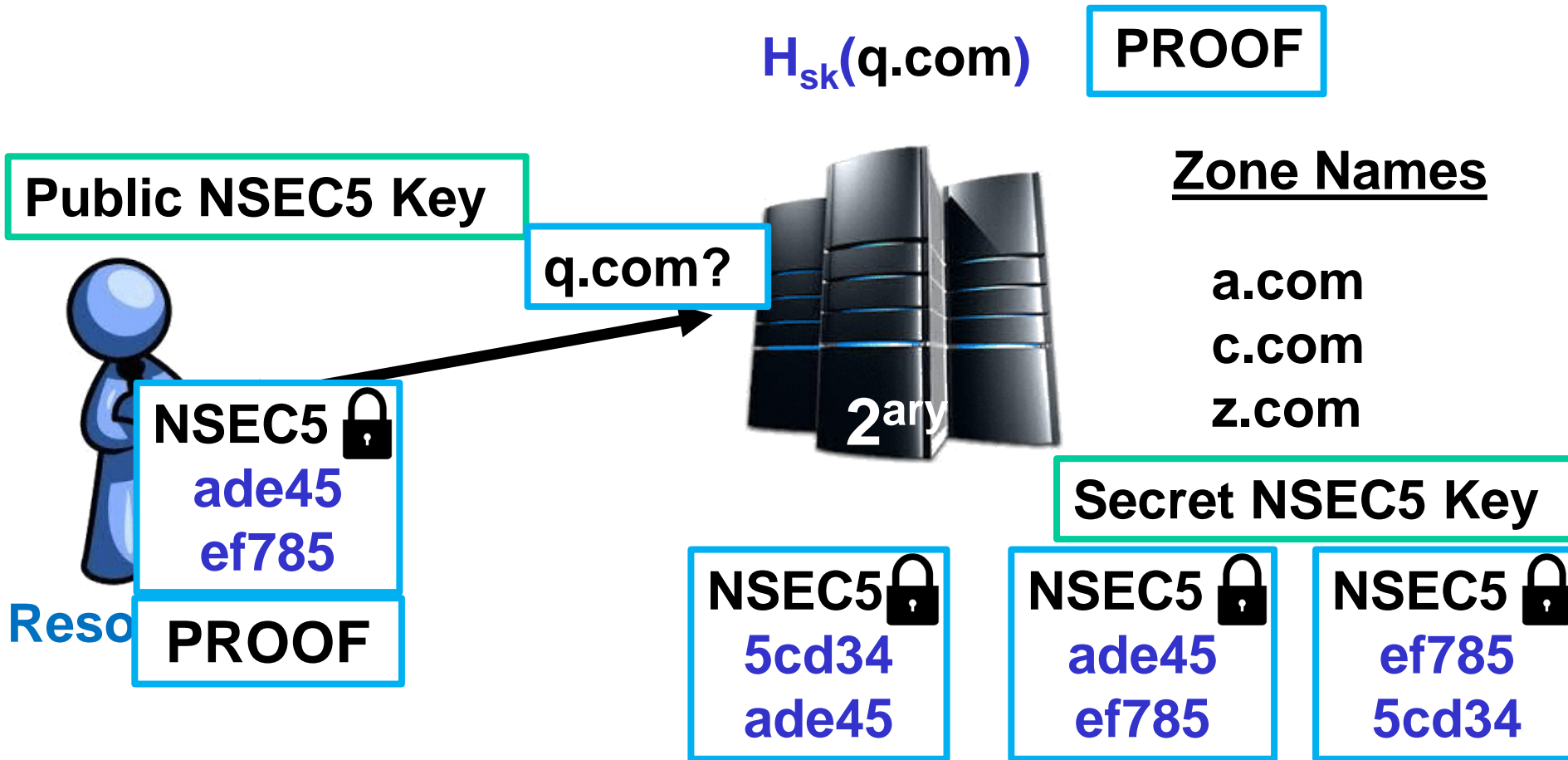


NSEC5 in action



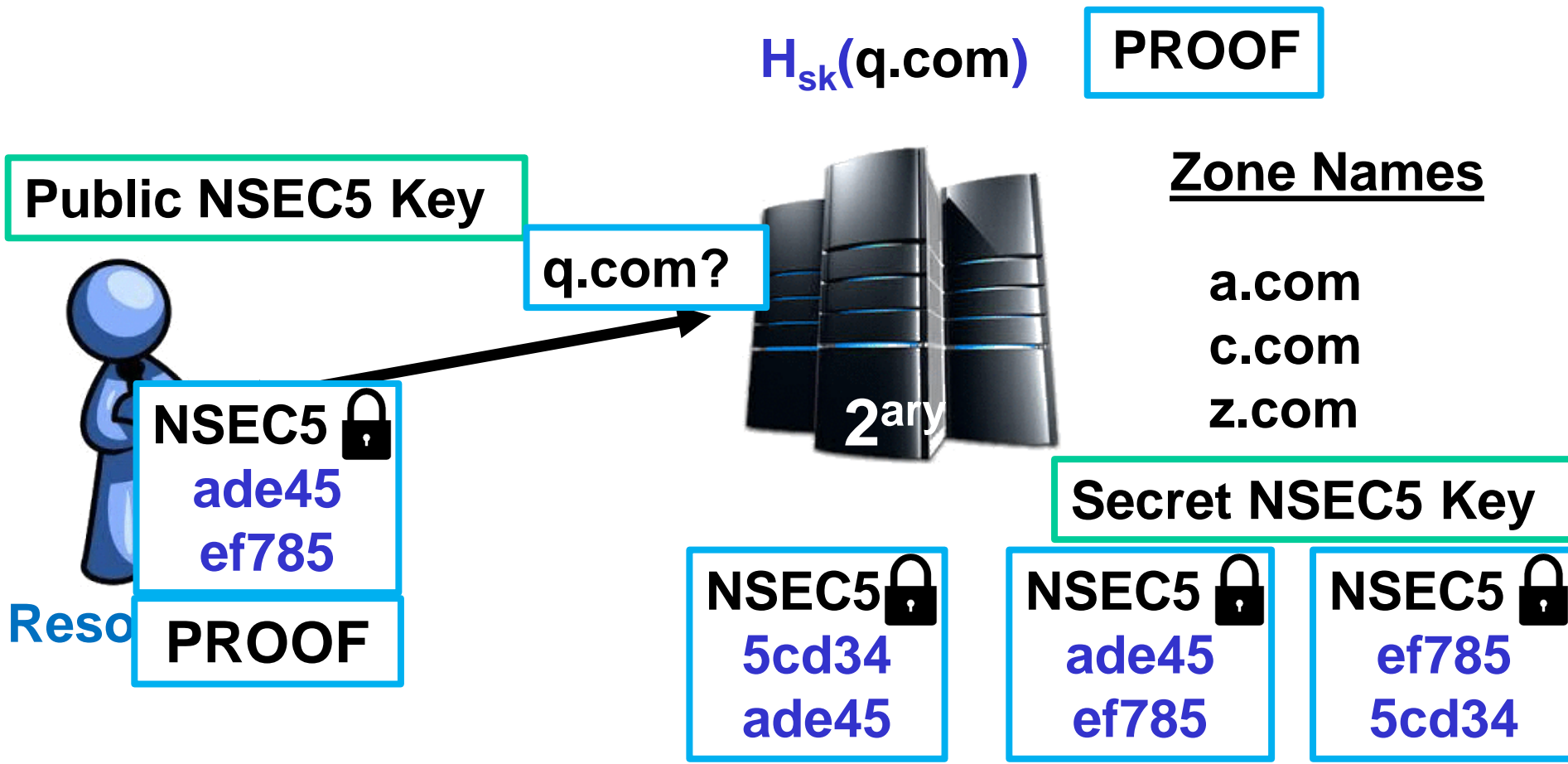
1. Verify $H_{sk}(q.com)$ was computed correctly using public NSEC5 key

NSEC5 in action



1. Verify $H_{sk}(q.com)$ was computed correctly using public NSEC5 key
2. $ade45 < H_{sk}(q.com) < ef785$

NSEC5 in action

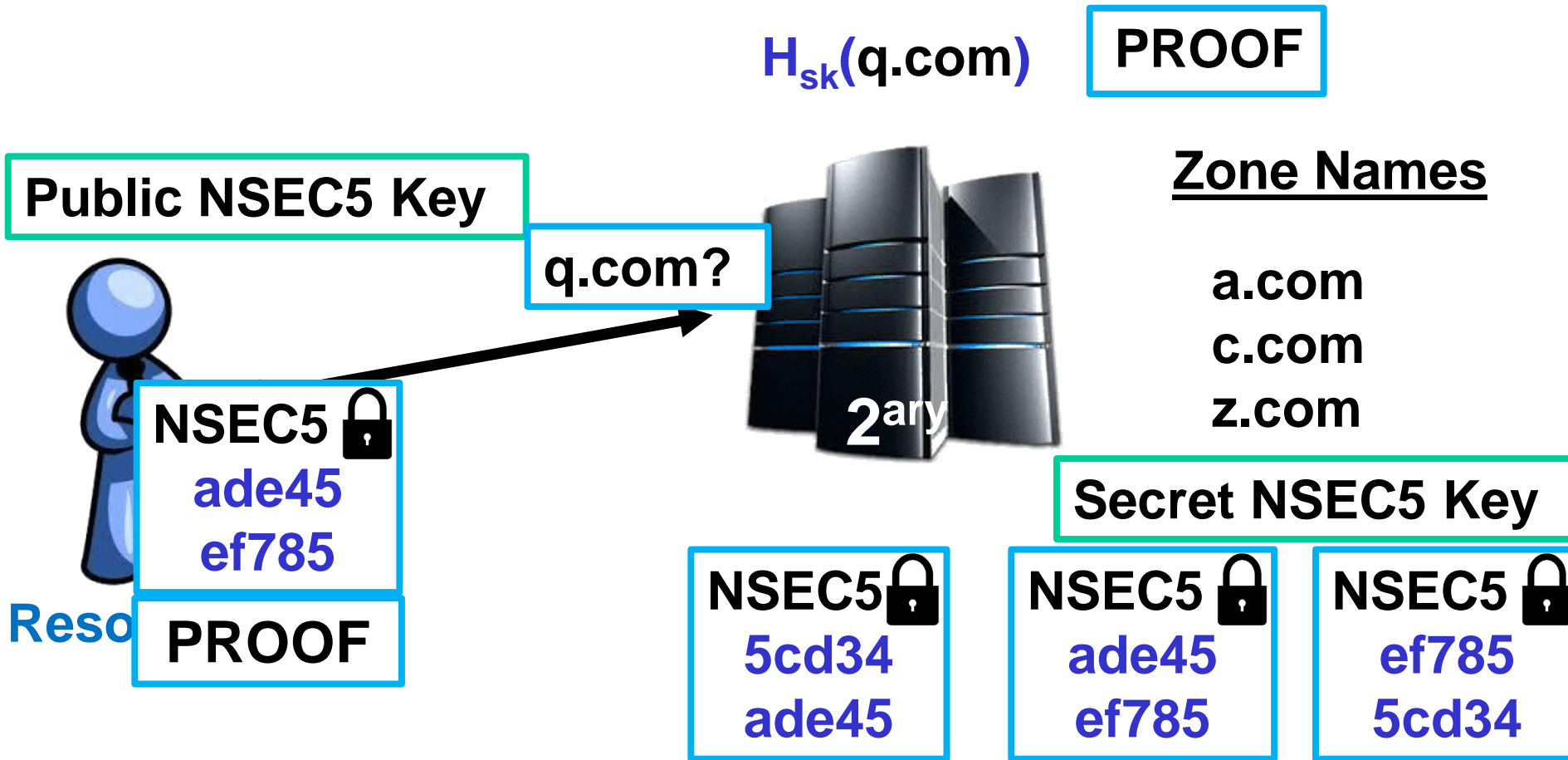


1. Verify $H_{sk}(q.com)$ was computed correctly using public NSEC5 key

Integrity?

2. $ade45 < H_{sk}(q.com) < ef785$

NSEC5 in action

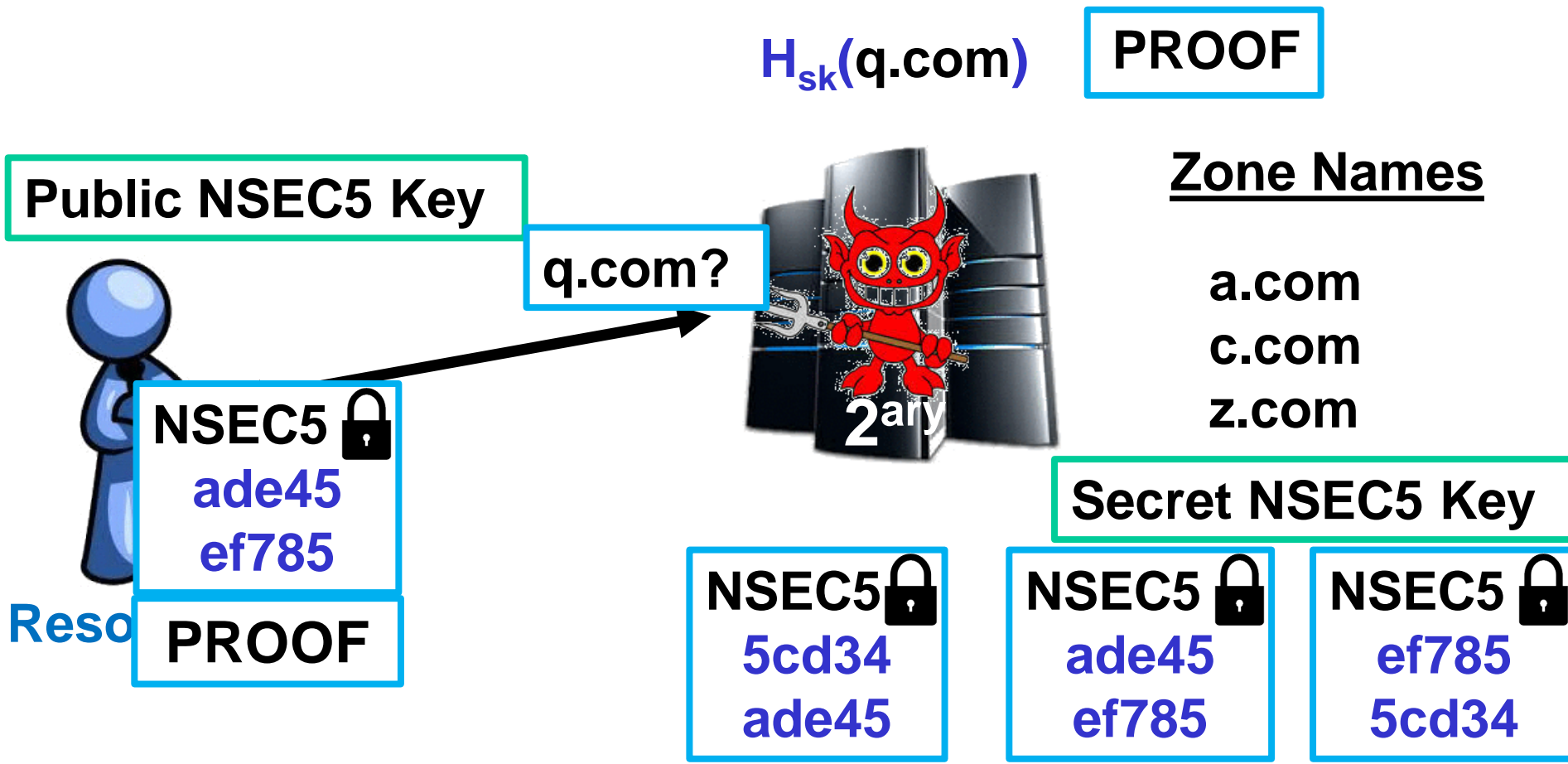


1. Verify $H_{sk}(q.com)$ was computed correctly using public NSEC5 key

2. $ade45 < H_{sk}(q.com) < ef785$

Integrity?
Privacy?

NSEC5 in action



1. Verify $H_{sk}(q.com)$ was computed correctly using public NSEC5 key
2. $ade45 < H_{sk}(q.com) < ef785$

Integrity? **Yes!**
Privacy?

NSEC5 in action



Public NSEC5 Key

$H_{sk}(q.com)$

PROOF

Zone Names

a.com
c.com
z.com



q.com?



NSEC5
ade45
ef785

Secret NSEC5 Key

Resource

PROOF

NSEC5
5cd34
ade45

NSEC5
ade45
ef785

NSEC5
ef785
5cd34

1. Verify $H_{sk}(q.com)$ was computed correctly using public NSEC5 key

Integrity? **Yes!**

Privacy? **Yes!**

2. $ade45 < H_{sk}(q.com) < ef785$



NSEC5 – Implementing the keyed hash function



NSEC5 – Implementing the keyed hash function

NSEC5 -

a.com



NSEC5 – Implementing the keyed hash function

NSEC5 -

$h_1(\text{a.com})$

NSEC5 – Implementing the keyed hash function

NSEC5 -

$RSA_{SK}(h_1(a.com))$

NSEC5 – Implementing the keyed hash function

NSEC5 -

$RSA_{SK}(h_1(\text{a.com}))$

$$RSA_{SK}(x) = x^d \pmod{N}$$

NSEC5 – Implementing the keyed hash function

NSEC5 -

$RSA_{SK}(h_1(\text{a.com}))$

$$RSA_{SK}(x) = x^d \bmod N$$

NSEC5 – Implementing the keyed hash function

NSEC5 -

$h_2(\text{RSA}_{\text{SK}}(h_1(\text{a.com})))$

$$\text{RSA}_{\text{SK}}(x) = x^d \bmod N$$

NSEC5 – Implementing the keyed hash function

NSEC5 -

$$h_2(\text{RSA}_{\text{SK}}(h_1(\text{a.com})))$$

$$\text{RSA}_{\text{SK}}(x) = x^d \text{ mod } N$$

NSEC3 - $h_2(\text{a.com})$

(SHA256)

NSEC5 – Implementing the keyed hash function

$$\text{NSEC5} - H_{sk}(a.com) = h_2(\text{RSA}_{sk}(h_1(a.com)))$$

$$\text{RSA}_{sk}(x) = x^d \bmod N$$

$$\text{NSEC3} - h_2(a.com)$$

(SHA256)

NSEC5 – Implementing the keyed hash function

$$\text{NSEC5} - H_{sk}(a.com) = h_2(\underbrace{RSA_{sk}(h_1(a.com))}_{\text{Full Domain Hash}})$$

(“Full Domain Hash” [BR93])

$$RSA_{sk}(x) = x^d \bmod N$$

$$\text{NSEC3} - h_2(a.com)$$

(SHA256)

NSEC5 – Implementing the keyed hash function

H_{sk} is a Verifiable Random Function (VRF) [MRV99]

$$\text{NSEC5} - H_{sk}(a.com) = h_2(\underbrace{RSA_{sk}(h_1(a.com))}_{\text{VRF}})$$

(“Full Domain Hash” [BR93])

$$RSA_{sk}(x) = x^d \bmod N$$

NSEC3 - $h_2(a.com)$

(SHA256)

NSEC5 – Implementing the keyed hash function

H_{sk} is a Verifiable Random Function (VRF) [MRV99]

$$\text{NSEC5} - H_{sk}(\text{a.com}) = h_2(\underbrace{\text{RSA}_{sk}(h_1(\text{a.com}))}_{\text{PROOF } \pi})$$

VRF

$$\text{RSA}_{sk}(x) = x^d \bmod N$$

NSEC3 - $h_2(\text{a.com})$

(SHA256)

NSEC5 – Implementing the keyed hash function

H_{sk} is a Verifiable Random Function (VRF) [MRV99]

$$\text{NSEC5} - H_{sk}(a.com) = h_2(\underbrace{RSA_{sk}(h_1(a.com))}_{\text{PROOF } \pi})$$

VRF

$$RSA_{SK}(x) = x^d \bmod N$$
$$RSA_{PK}(\pi) = \pi^e \bmod N \equiv x$$

NSEC3 - $h_2(a.com)$

(SHA256)

NSEC5 – Implementing the keyed hash function

H_{sk} is a Verifiable Random Function (VRF) [MRV99]

$$\text{NSEC5} - H_{sk}(a.com) = \underbrace{h_2(\underbrace{RSA_{sk}(h_1(a.com))}_{\text{PROOF } \pi})}_{\text{VRF}}$$

$$\begin{aligned} RSA_{SK}(x) &= x^d \bmod N \\ RSA_{PK}(\pi) &= \pi^e \bmod N \equiv x \end{aligned}$$

NSEC3 - $h_2(a.com)$

(SHA256)

Summary

	Integrity against outsiders	Integrity against compromised 2 ^{dry} nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓
NSEC	✓	✓	✗
NSEC3	✓	✓	✗

Summary

	Integrity against outsiders	Integrity against compromised 2 ^{dry} nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓
NSEC	✓	✓	✗
NSEC3	✓	✓	✗
NSEC5	✓	✓	✓

Summary

	Integrity against outsiders	Integrity against compromised 2 ^{dry} nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓
NSEC	✓	✓	✗
NSEC3	✓	✓	✗
NSEC5	✓	✓	✓
NSEC5; lost secret N5K	✓	✓	✗

Summary

	Integrity against outsiders	Integrity against compromised 2 ^{dry} nameserver	No zone enumeration
DNS	✗	✗	✓
Sign Online	✓	✗	✓
NSEC	✓	✓	✗
NSEC3	✓	✓	✗
NSEC5	✓	✓	✓
NSEC5; lost secret N5K	✓	✓	✗

Just like
NSEC3!



Lower bound

NSEC5 uses RSA computations online!



Lower bound

NSEC5 uses RSA computations online!

- Is this really necessary?



Lower bound

NSEC5 uses RSA computations online!

- Is this really necessary?
- Unfortunately yes! 😞

Lower bound

NSEC5 uses RSA computations online!

- Is this really necessary?

- Unfortunately yes! 😞

Theorem [Informal]: ANY denial of existence scheme that

1. prevents **zone enumeration**, and

2. provides **integrity** against network attackers

requires nameservers to perform **public-key operations** for every negative response.

Lower bound

NSEC5 uses RSA computations online!

- Is this really necessary?

- Unfortunately yes! 😞

Theorem [Informal]: ANY denial of existence scheme that

1. prevents **zone enumeration**, and
2. provides **integrity** against network attackers

requires nameservers to perform **public-key operations** for every negative response.

→ Explains why NSEC3 is still vulnerable to zone enumeration.

Lower bound

NSEC5 uses RSA computations online!

- Is this really necessary?

- Unfortunately yes! 😞

Theorem [Informal]: ANY denial of existence scheme that

1. prevents **zone enumeration**, and

2. provides **integrity** against network attackers

requires nameservers to perform **public-key operations** for every negative response.

→ Explains why NSEC3 is still vulnerable to zone enumeration.

(NSEC5 is **optimal** - requires only **one** RSA computation)



Conclusion

This work

- proposes NSEC5
first DNSSEC scheme that prevents zone enumeration while maintaining integrity for a compromised nameserver
- proves that zone-enumeration cannot be avoided without online public-key operations
- we would like to implement NSEC5
we are writing an Internet draft
give us your feedback and suggestions!

Project webpage:

<http://www.cs.bu.edu/~goldbe/papers/nsec5.html>



Conclusion

This work

- proposes NSEC5
first DNSSEC scheme that prevents zone enumeration while maintaining integrity for a compromised nameserver
- proves that zone-enumeration cannot be avoided without online public-key operations
- we would like to implement NSEC5
we are writing an Internet draft
give us your feedback and suggestions!

Project webpage:

<http://www.cs.bu.edu/~goldbe/papers/nsec5.html>

THANK YOU!