The Missing Piece: On Namespace Management in NDN and how DNSSEC Might Help

Pouyan Fotouhi Tehrani,[1] Eric Osterweil,[2] Jochen Schiller,[3] Thomas C. Schmidt,[4] Matthias Waehlisch[3]

[1] Weizenbaum Institut / Fraunhofer FOKUS, [2] George Mason University, [3] Freie Universitä̈t Berlin, [4] Hamburg University of Applied Sciences

The dichotomy of Internet naming

- Internet naming: namespace → content
- w.r.t. how to bind names to content:
  ``… the network had better not care…''[1]
- Indeed, the mechanisms of NDN are well served by their focus on technical issues
- But, we argue that there is still a *demonstrated* (separate) need for namespace management

This isn't DNS, but as the Internet's 30+ year old de facto its phonebook, what can we learn from DNS' *success*?

[1] ``A Conversation with Van Jacobson,'' acmqueue Volume 7, Issue 1, February 23, 2009

Isn’t that what NDN DNS (NDNS) [Afanasyev, 2013] does?

Wait…

. . . or even CCN Key Resolution Service (CCN-KRS) [Mahadevan, 2014]?

i.e. has this already been addressed?

Yes

- Regarding many technical aspects
  - Self-certifying names
  - Trusted Third Parties (TTPs)
  - Etc.

No

- Regarding policy and non-technical aspects
  - Trademarks
  - Legal disputes
  - The operational and *industry* ecosystem that exists in the Internet today

There will be growing pains…

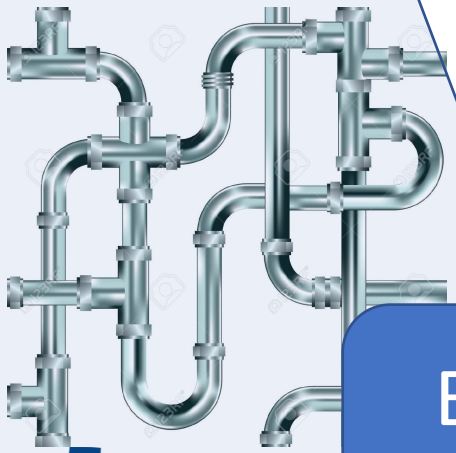
Technical aspects

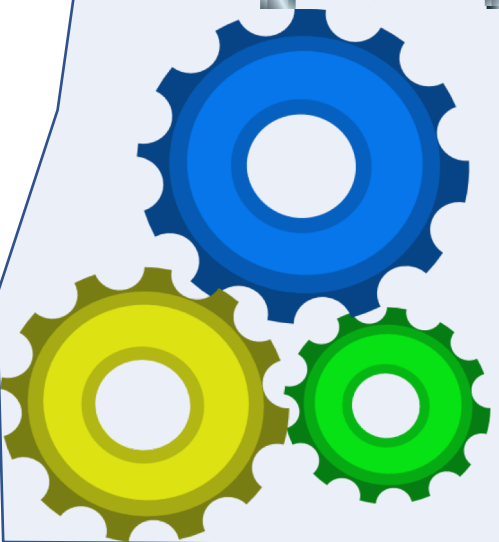
- Mapping names to content is critical
- Securing that mapping is a first-order design point
- Scaling all of the mechanisms is critical to producing deployable solutions
- …
- If industry needed for broad adoption, consider…
  - Has historically brought non-technical considerations

Non-technical

- Names developed commercial value (trademarks, intellectual property, etc.)
- Industry has long since coupled DNS domain names to this
- Technical security gets impacted (i.e. name collisions)

How entries are entered and read from phonebook (IETF for DNS)





How to decide what names *should* be entered in the phonebook (ICANN for DNS)

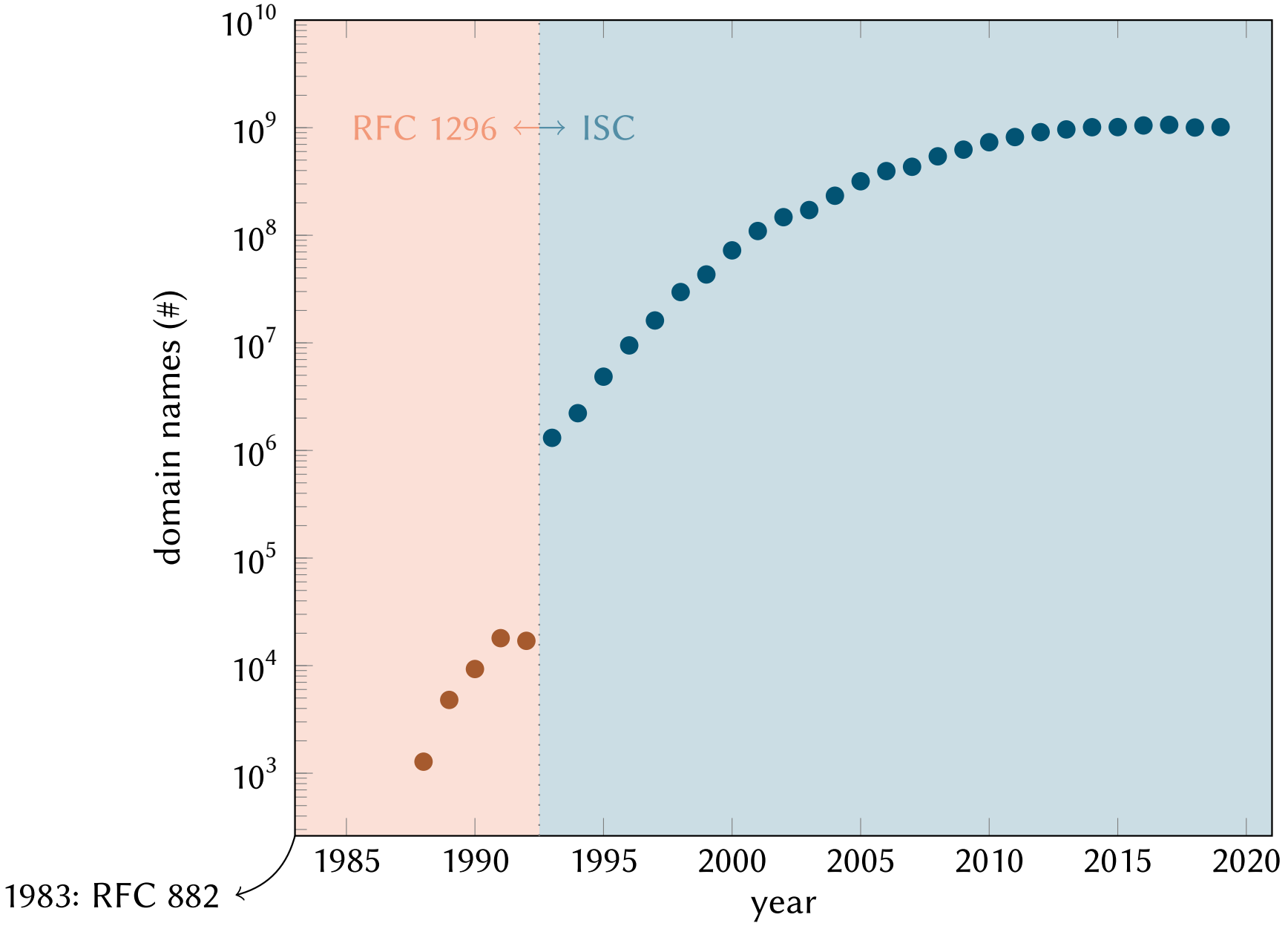
But, why did we wind up needing this (for DNS)???

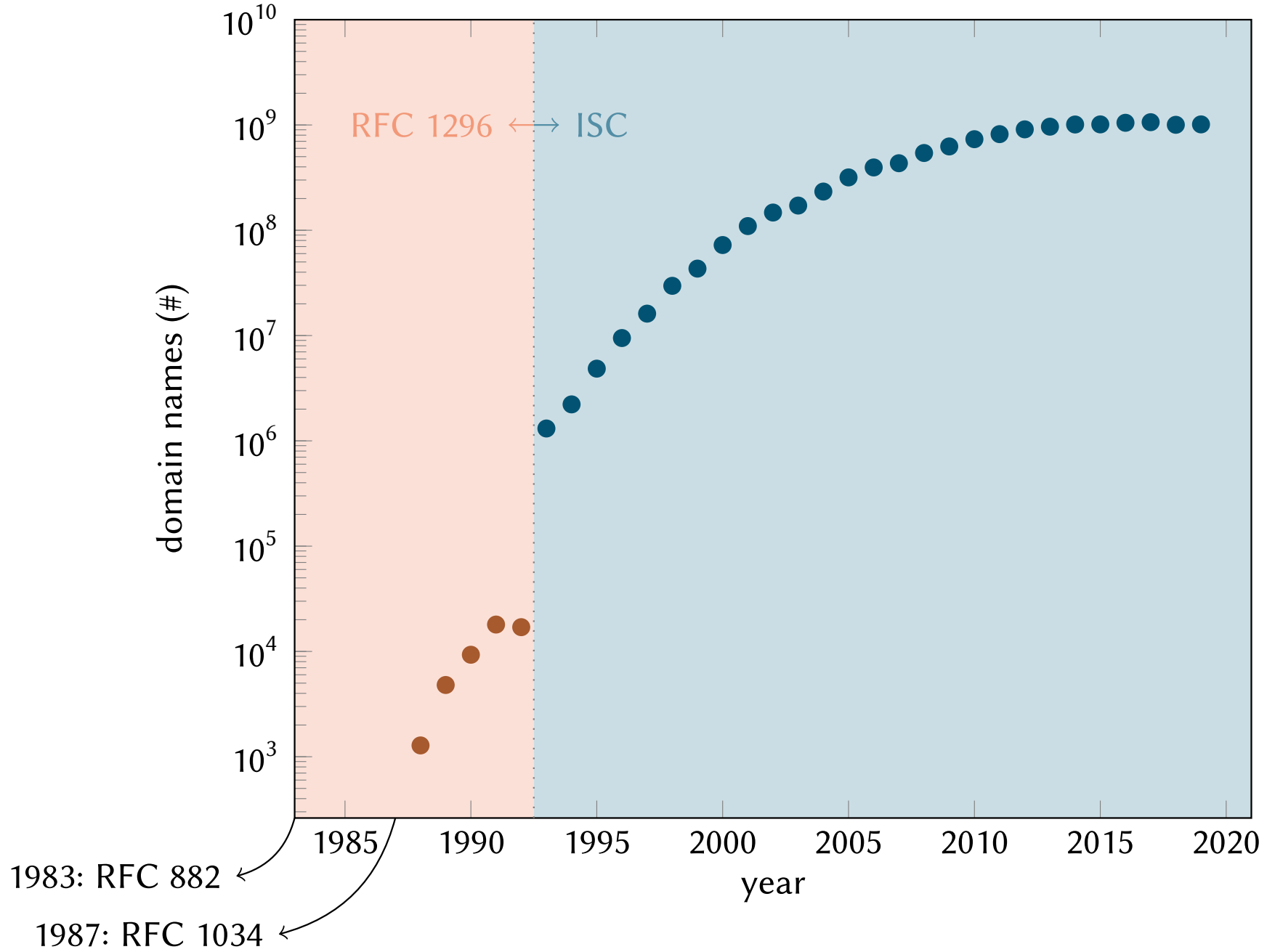
Often contentious

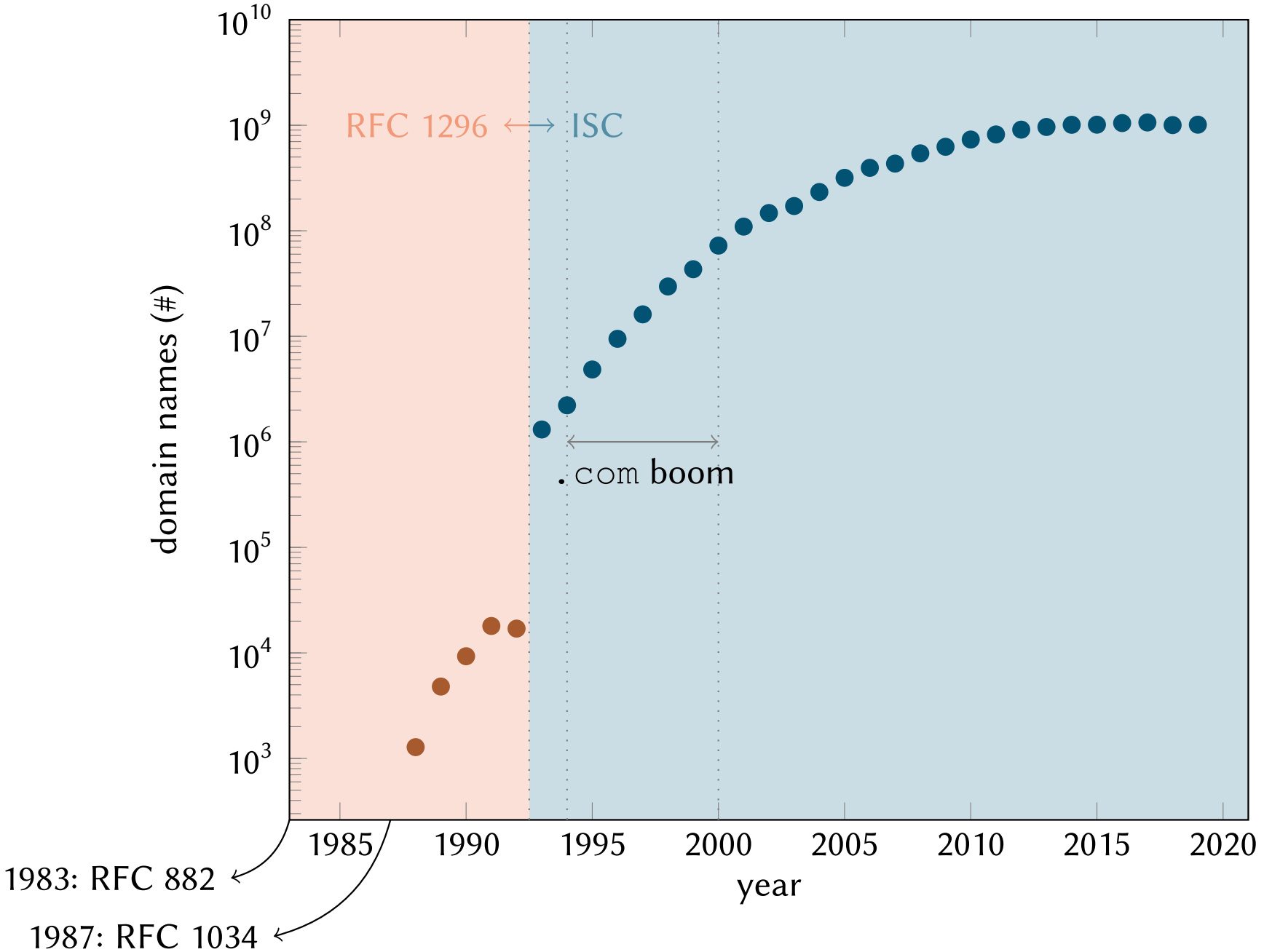
Did DNS really need a non-technical mechanism? Really?

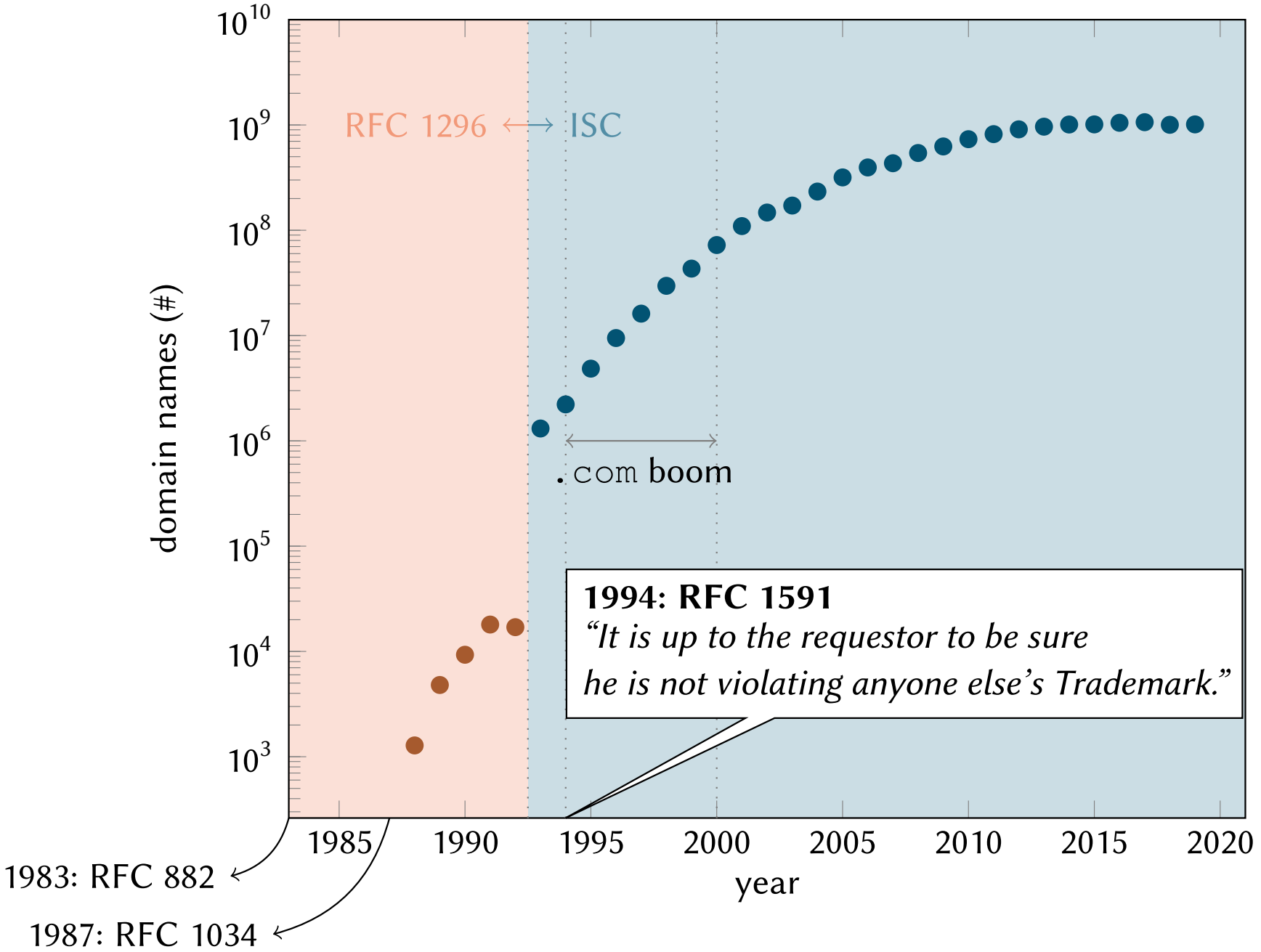
- Well, first it seemed not: technical protocols came from IETF
- Then *names* became business-critical, and it seemed to need something
- After enough *demonstrated* need, the DNS community evolved the Internet Corporation for Assigned Names and Numbers (ICANN)
- Is it perfect? No. But, perhaps,
  ``Those who cannot remember the past [may be] condemned to repeat it.''[1]

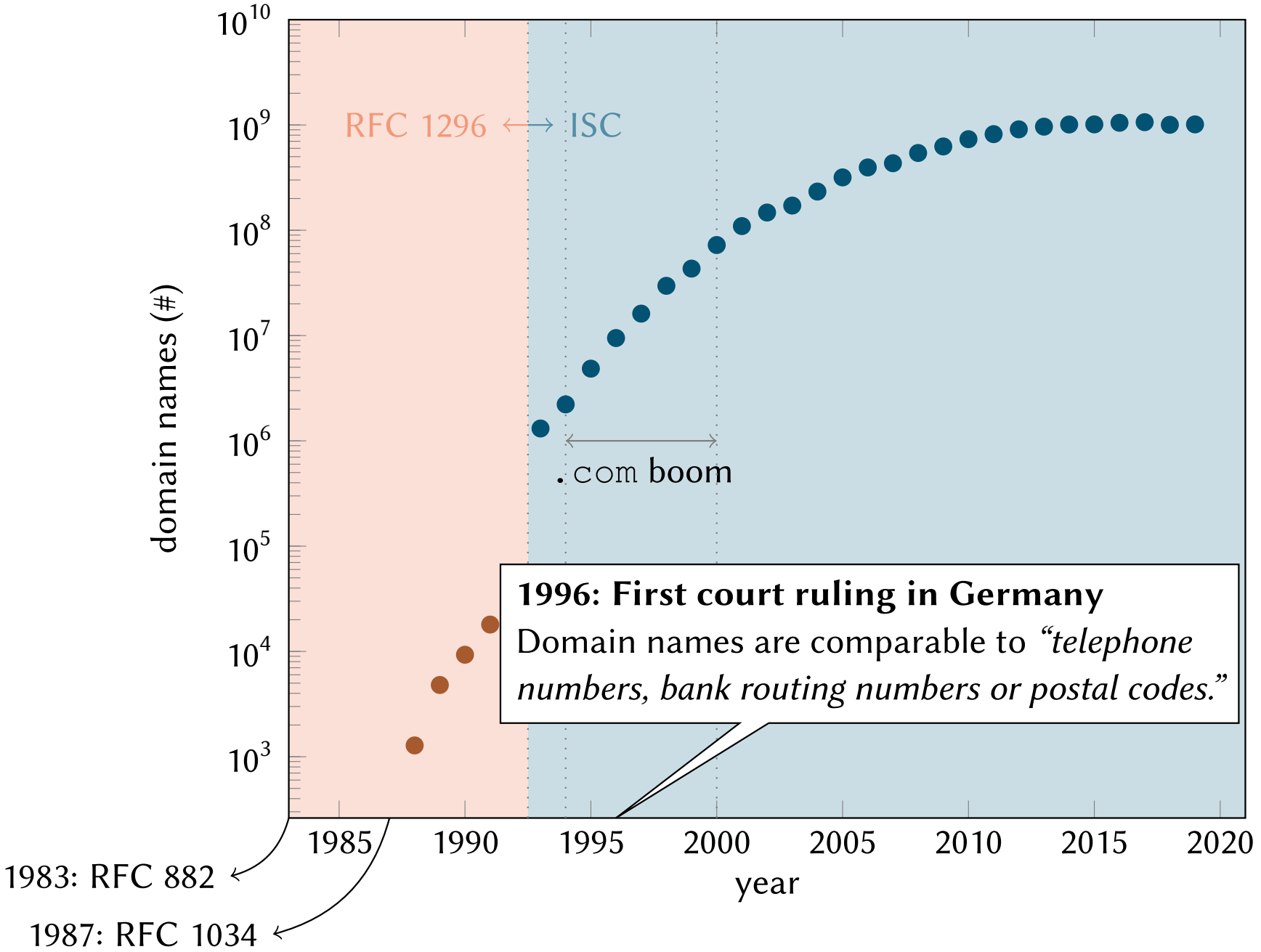
[1] George Santayana, ``The Life of Reason: The Phases of Human Progress'' Vol. 1, 1905

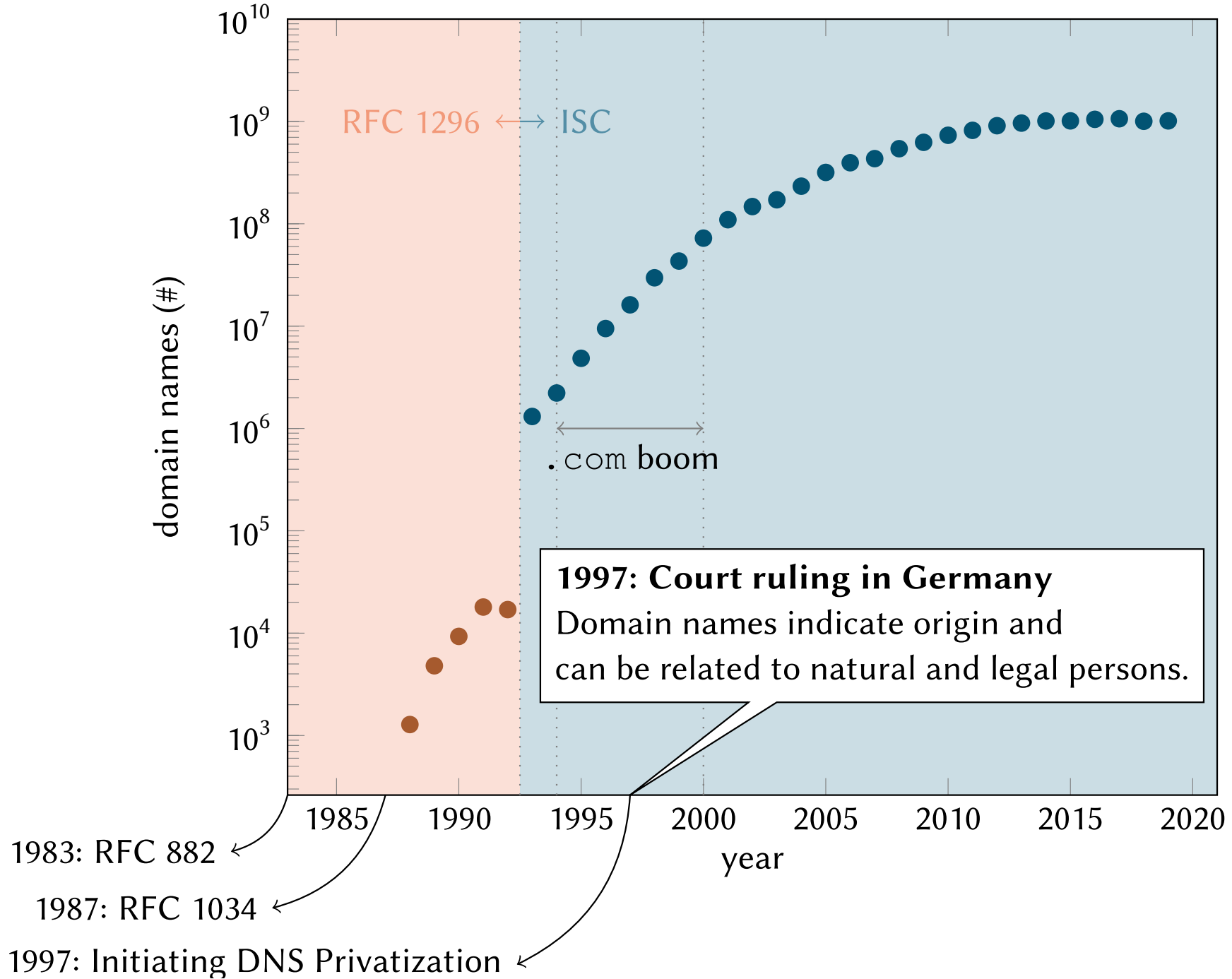

10^{10}
10^{9}
10^{8}
10^{7}
10^{6}
10^{5}
10^{4}
10^{3}
domain names (#)
RFC 1296 ⟷ ISC
1985
1990
1995
2000
2005
2010
2015
2020
year
1983: RFC 882

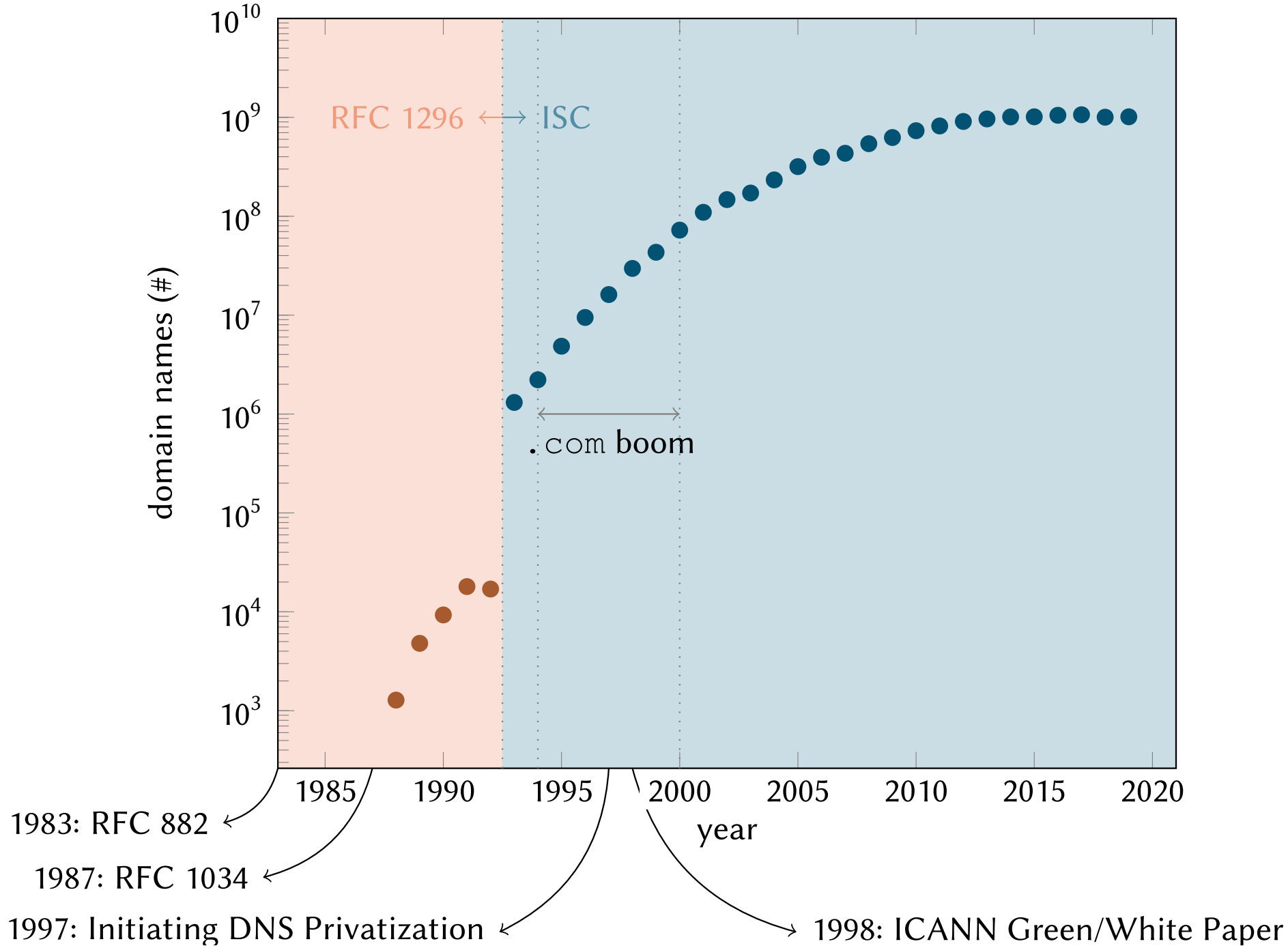

10^{10}
10^{9}
10^{8}
10^{7}
10^{6}
10^{5}
10^{4}
10^{3}
domain names (#)
RFC 1296 ⟷ ISC
1985
1990
1995
2000
2005
2010
2015
2020
year
1983: RFC 882
1987: RFC 1034

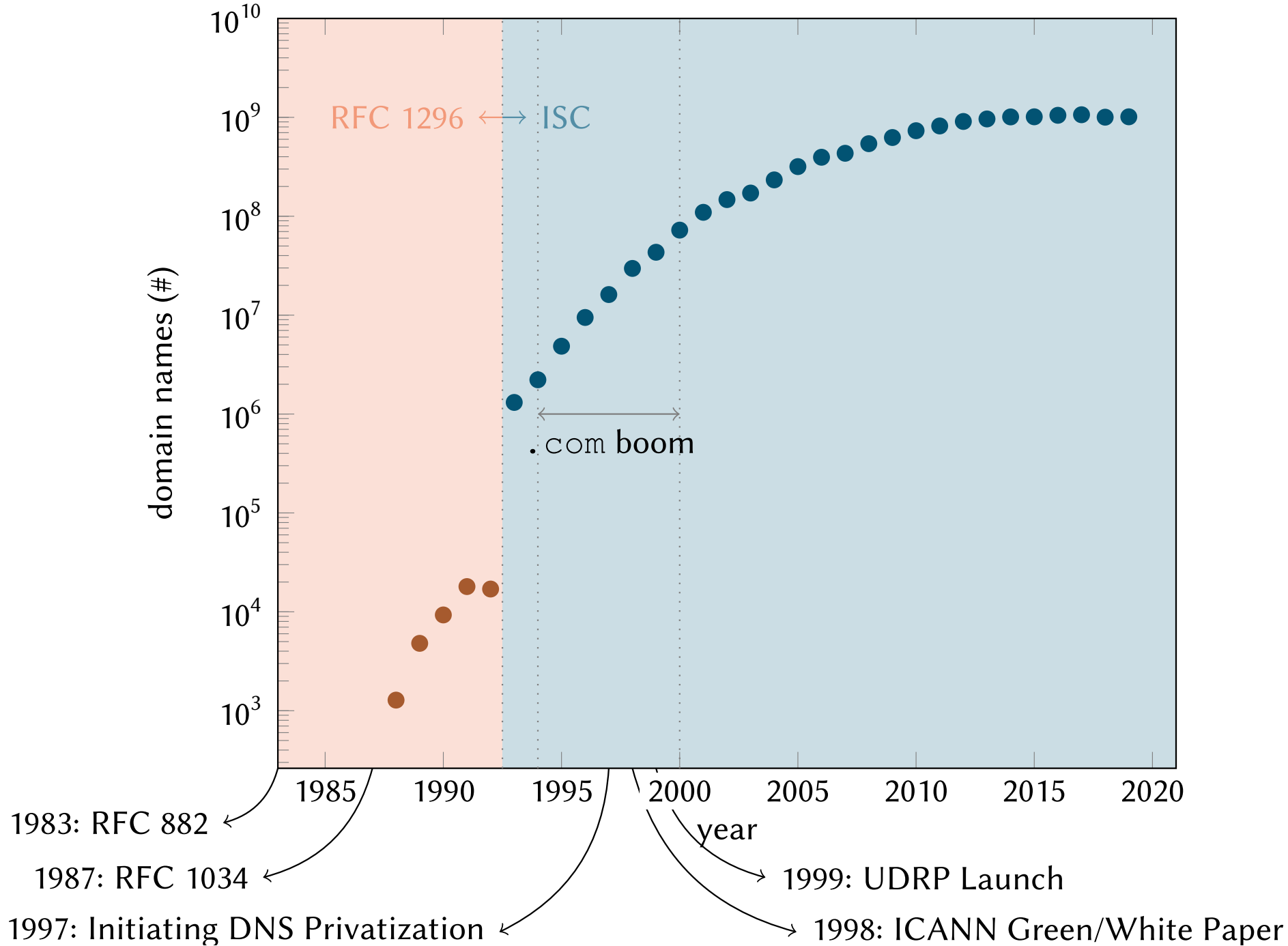

10^{10}
10^{9}
10^{8}
10^{7}
10^{6}
10^{5}
10^{4}
10^{3}
domain names (#)
RFC 1296
ISC
.com boom
1985
1990
1995
2000
2005
2010
2015
2020
year
1983: RFC 882
1987: RFC 1034

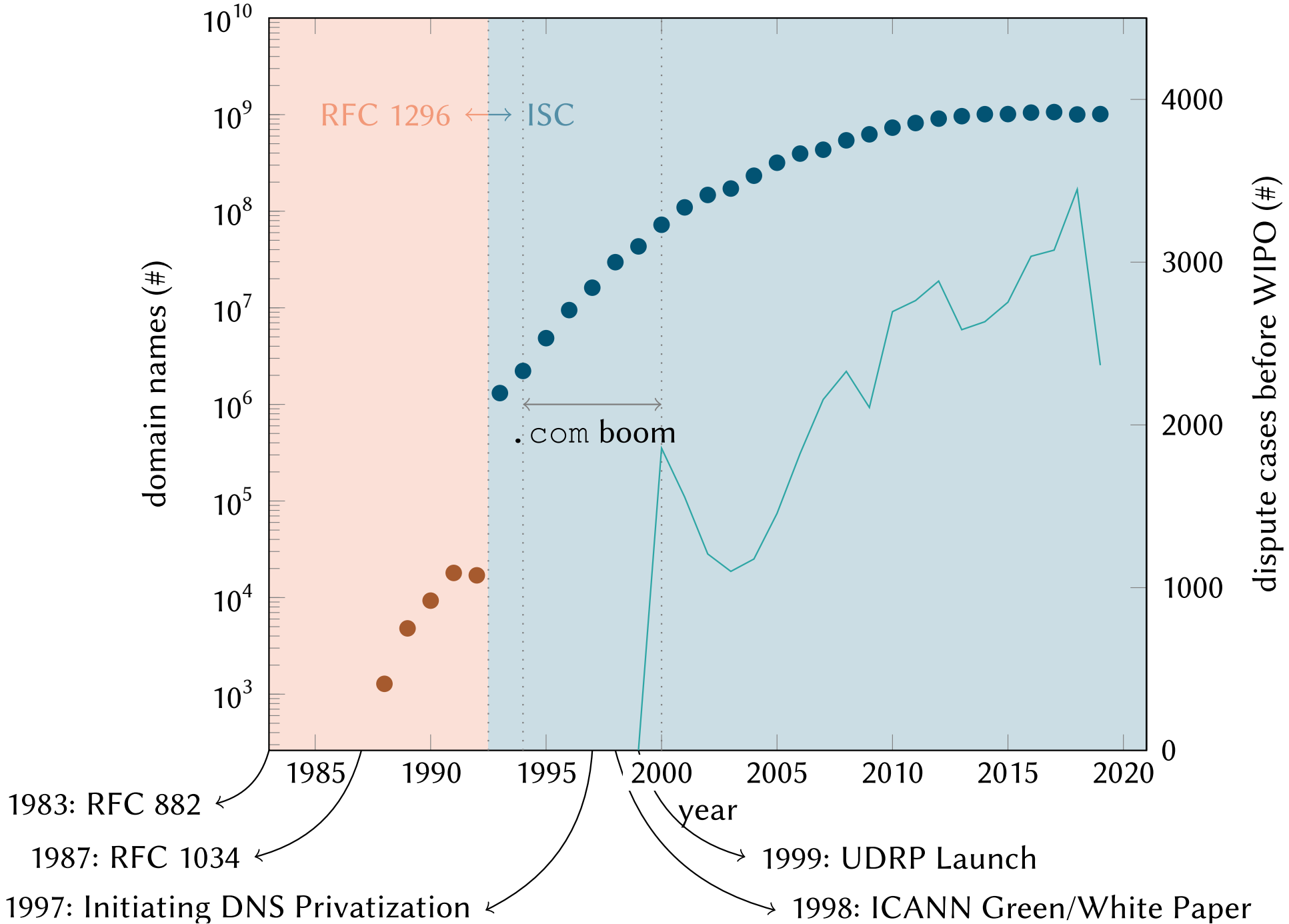

10^{10}
10^{9}
10^{8}
10^{7}
10^{6}
10^{5}
10^{4}
10^{3}
domain names (#)
RFC 1296 ⟷ ISC
.com boom
1994: RFC 1591
"It is up to the requestor to be sure
he is not violating anyone else's Trademark."
1985
1990
1995
2000
2005
2010
2015
2020
year
1983: RFC 882
1987: RFC 1034

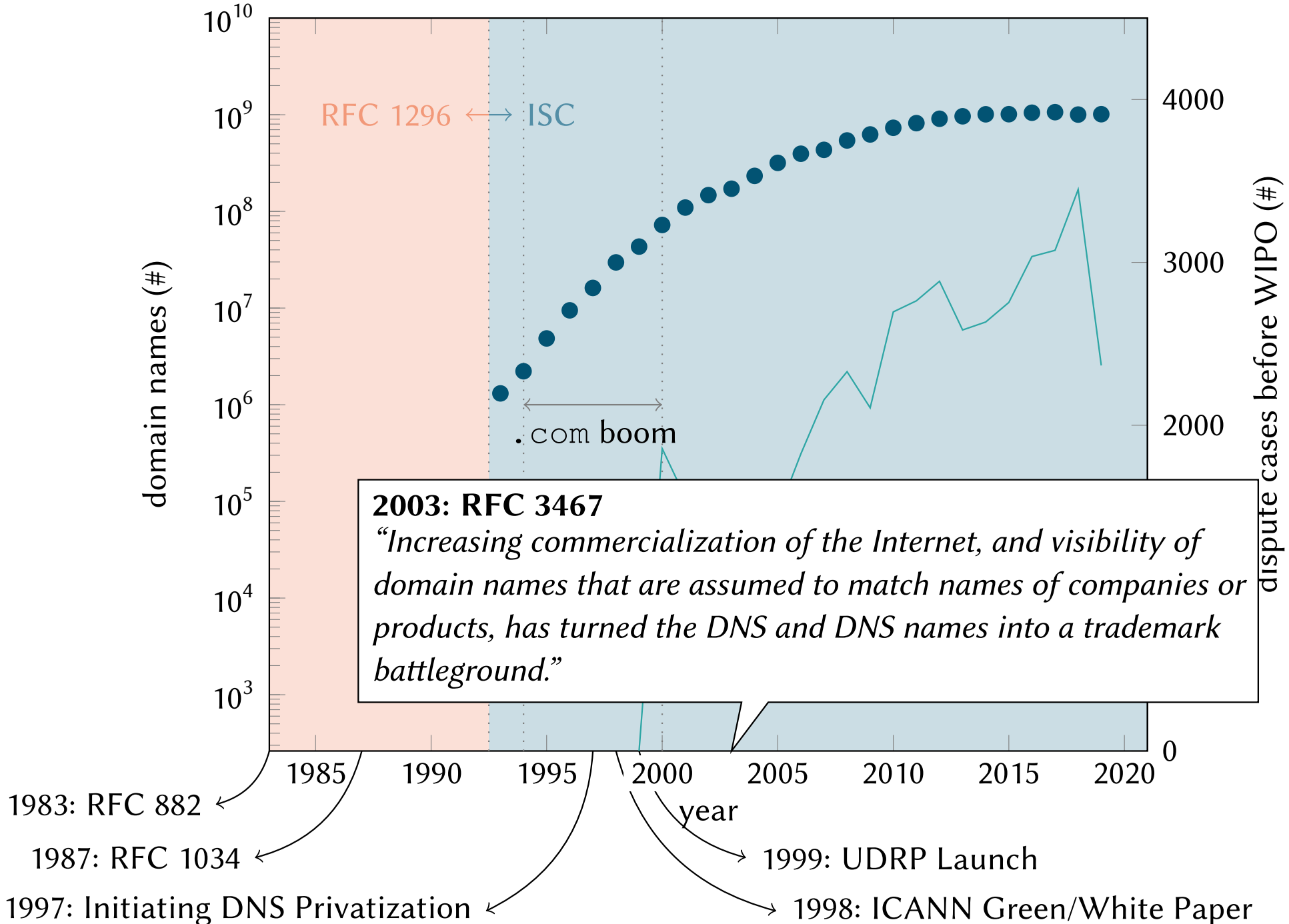

10^{10}
10^{9}
10^{8}
10^{7}
10^{6}
10^{5}
10^{4}
10^{3}
domain names (#)
RFC 1296
ISC
.com boom
1996: First court ruling in Germany
Domain names are comparable to "telephone numbers, bank routing numbers or postal codes."
1985
1990
1995
2000
2005
2010
2015
2020
year
1983: RFC 882
1987: RFC 1034

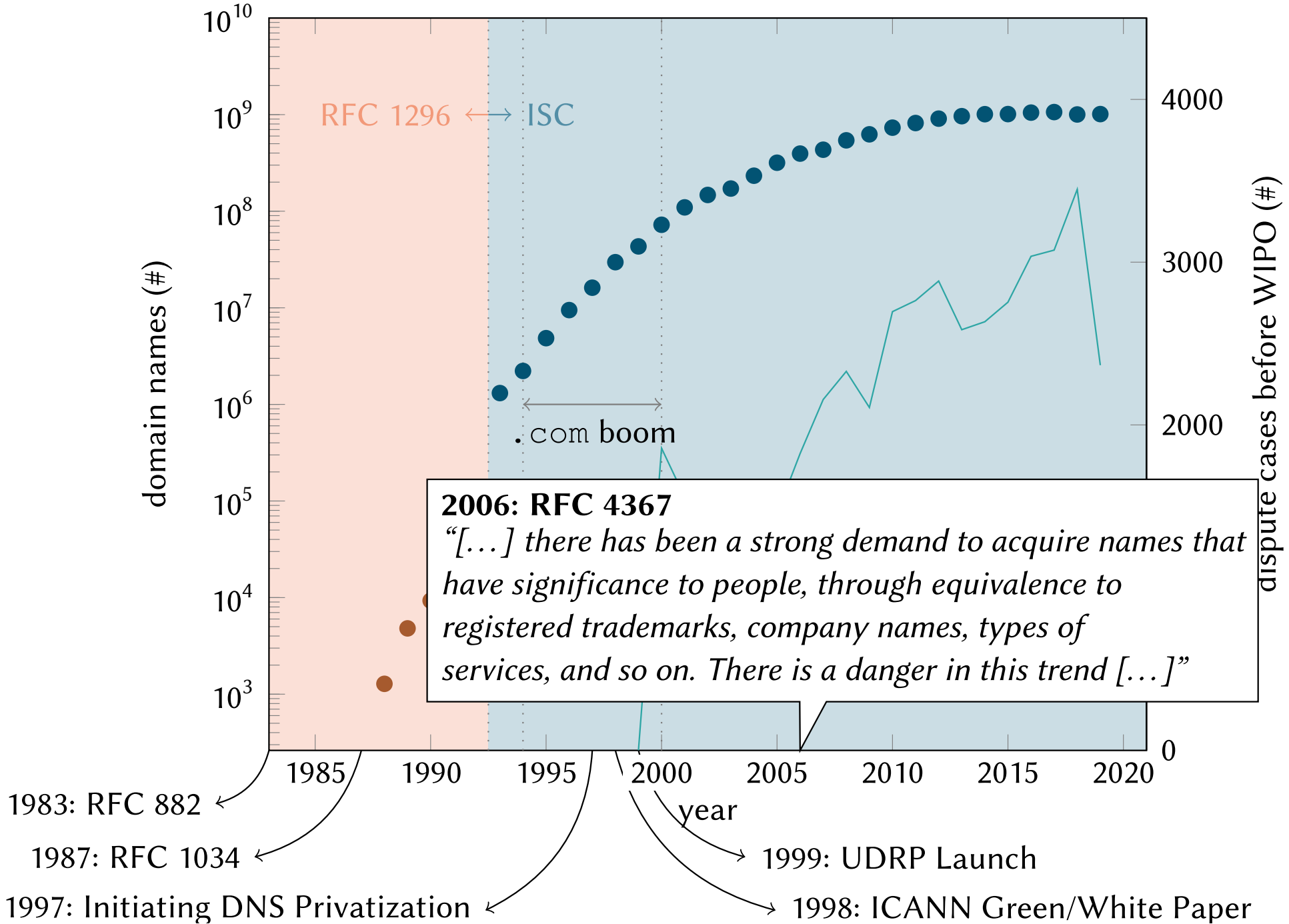

10^{10}
10^{9}
10^{8}
10^{7}
10^{6}
10^{5}
10^{4}
10^{3}
domain names (#)
RFC 1296
ISC
.com boom
1997: Court ruling in Germany
Domain names indicate origin and
can be related to natural and legal persons.
1985
1990
1995
2000
2005
2010
2015
2020
year
1983: RFC 882
1987: RFC 1034
1997: Initiating DNS Privatization


10^{10}
10^{9}
10^{8}
10^{7}
10^{6}
10^{5}
10^{4}
10^{3}
domain names (#)
RFC 1296
ISC
.com boom
1985
1990
1995
2000
2005
2010
2015
2020
year
1983: RFC 882
1987: RFC 1034
1997: Initiating DNS Privatization
1998: ICANN Green/White Paper


10^{10}
10^{9}
10^{8}
10^{7}
10^{6}
10^{5}
10^{4}
10^{3}
domain names (#)
RFC 1296
ISC
.com boom
1985
1990
1995
2000
2005
2010
2015
2020
year
1983: RFC 882
1987: RFC 1034
1997: Initiating DNS Privatization
1998: ICANN Green/White Paper
1999: UDRP Launch

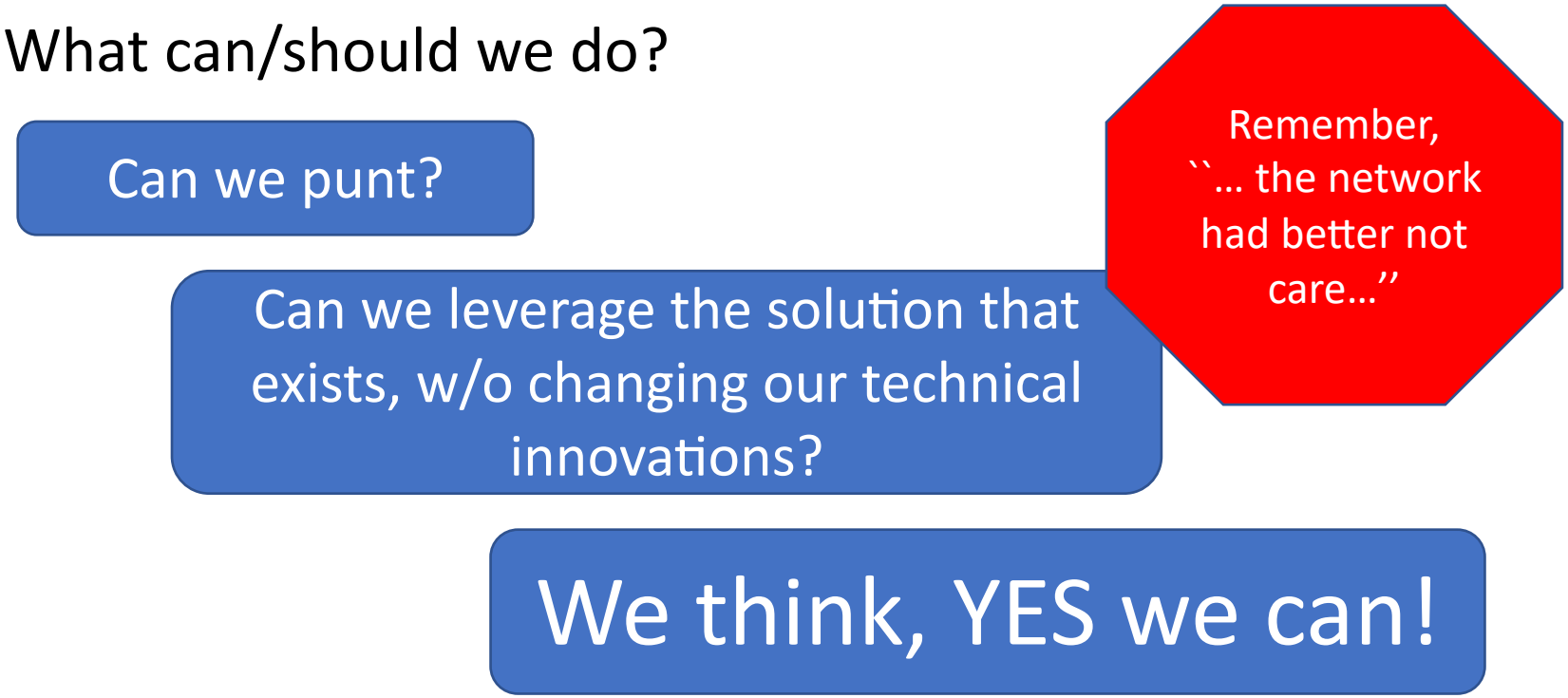

RFC 1296
ISC
.com boom
domain names (#)
dispute cases before WIPO (#)
year
1985
1990
1995
2000
2005
2010
2015
2020
0
1000
2000
3000
4000
1983: RFC 882
1987: RFC 1034
1997: Initiating DNS Privatization
1998: ICANN Green/White Paper
1999: UDRP Launch


RFC 1296
ISC
.com boom
domain names (#)
dispute cases before WIPO (#)
year
2003: RFC 3467
"Increasing commercialization of the Internet, and visibility of domain names that are assumed to match names of companies or products, has turned the DNS and DNS names into a trademark battleground."
1983: RFC 882
1987: RFC 1034
1997: Initiating DNS Privatization
1998: ICANN Green/White Paper
1999: UDRP Launch


RFC 1296 ⟷ ISC
.com boom
2006: RFC 4367
"[…] there has been a strong demand to acquire names that have significance to people, through equivalence to registered trademarks, company names, types of services, and so on. There is a danger in this trend […]"
domain names (#)
dispute cases before WIPO (#)
year
1983: RFC 882
1987: RFC 1034
1997: Initiating DNS Privatization
1998: ICANN Green/White Paper
1999: UDRP Launch

ICN will be successful!

- If the past is prolog, we will encounter similar (the same?) problems
- What can/should we do?



- We think we *can* synergize the technical design with a separate policy function

Our proposed solution

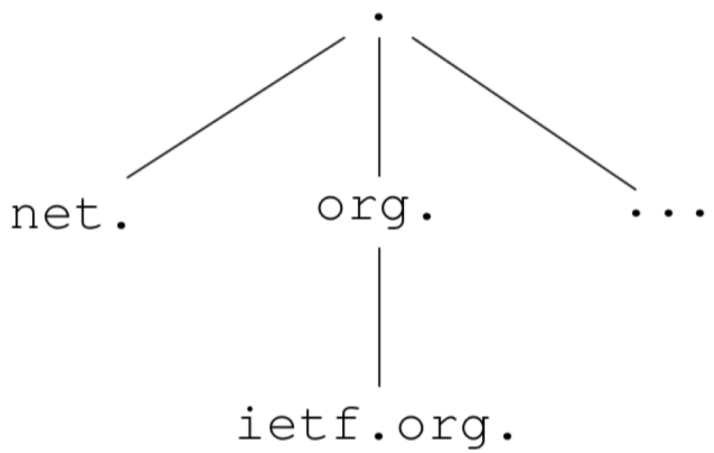
- Namespace

  "set of names from which all names for a given collection of objects are taken" [3, §8]

- Namespace Management

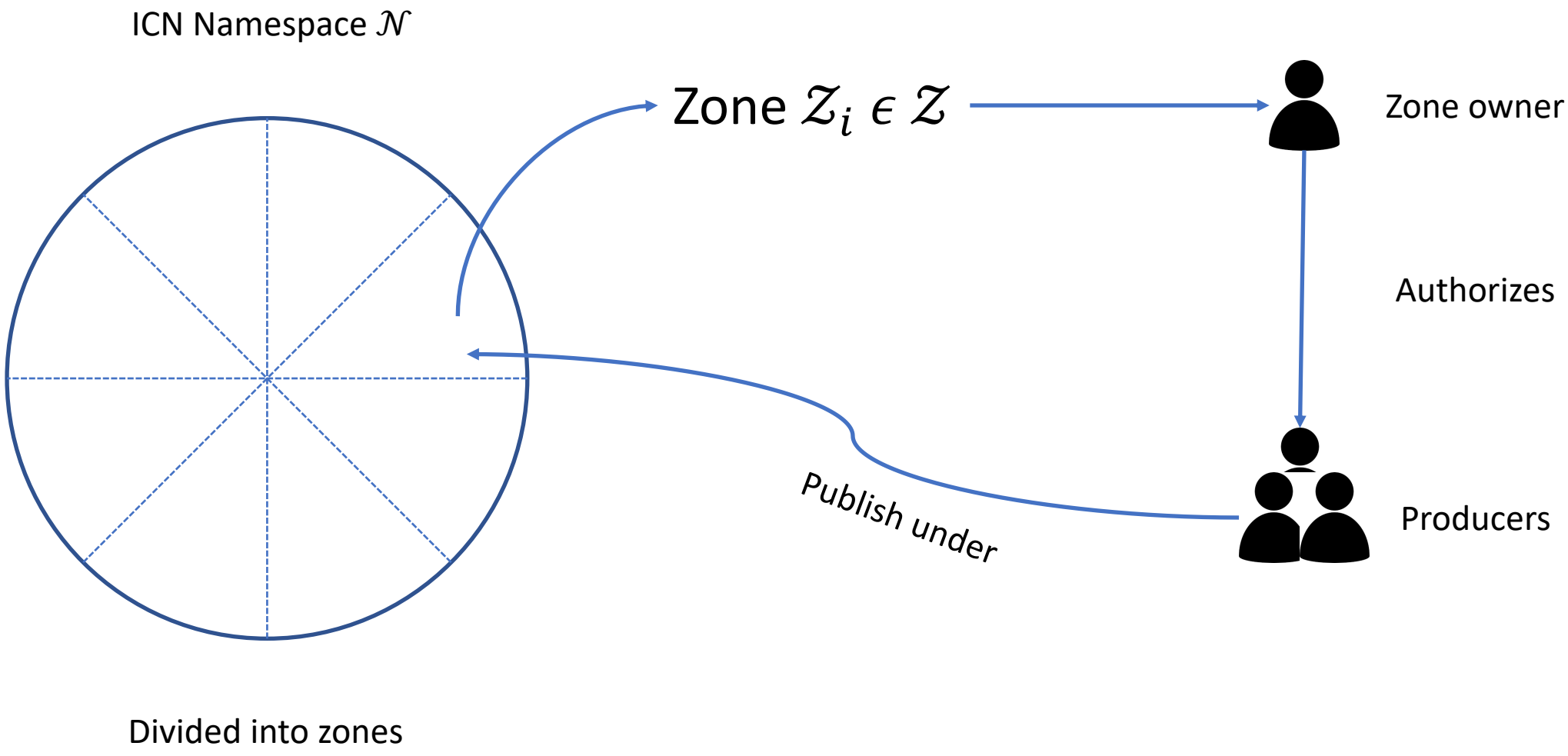
  a (decentralized) namespace management scheme partitions a namespace into management units, zones [6, §6], which are owned and maintained by an authoritative entity.

Example



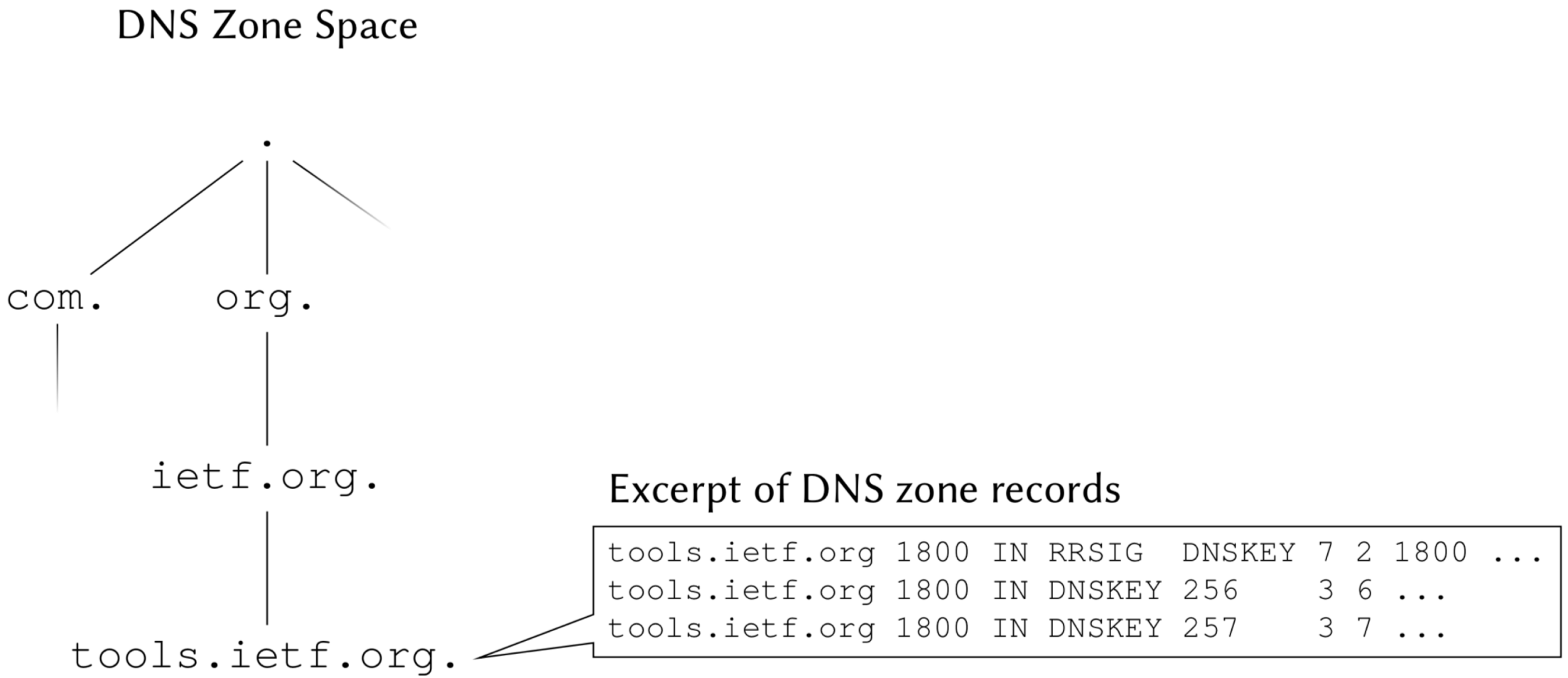

```
ietf.org.   300    IN MX 0 mail.ietf.org.
ietf.org.   300    IN A 4.31.198.44
```

Namespace management concept



Namespace Management Concept

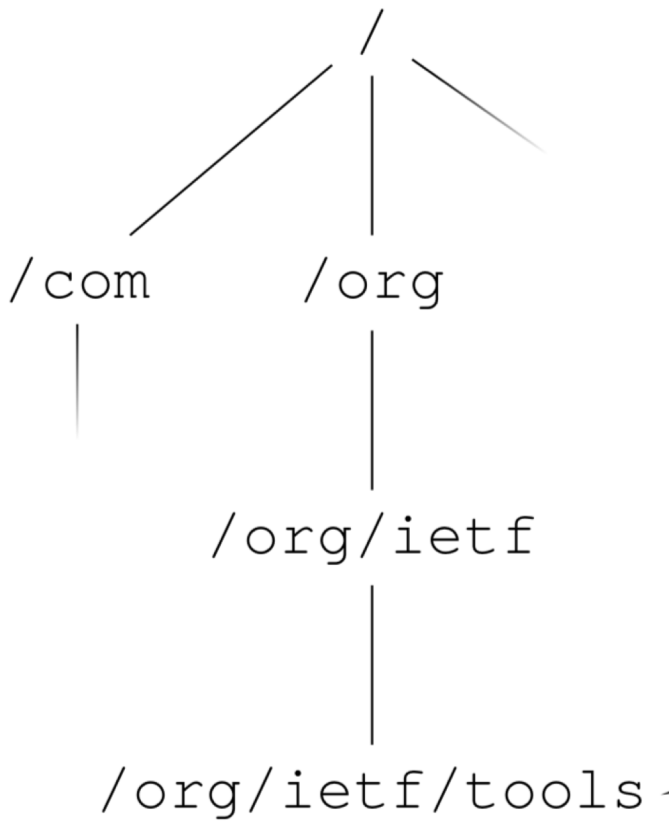
NDNSSEC



Namespace Management Concept

NDNSSEC: DNS Zone Appropriation for NDN

ndnified DNS Zone Space



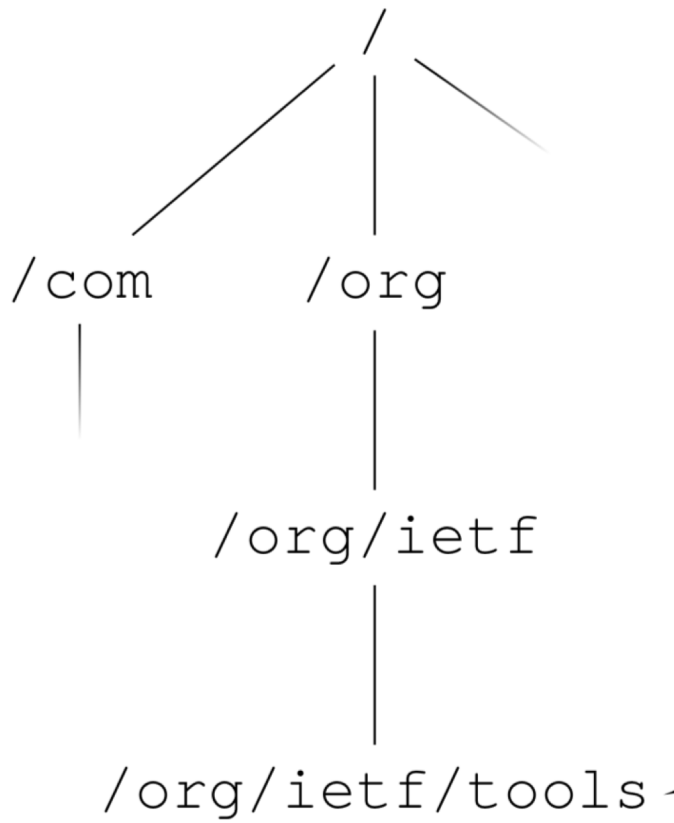
Excerpt of DNS zone records

```
tools.ietf.org 1800 IN RRSIG  DNSKEY 7 2 1800 ...
tools.ietf.org 1800 IN DNSKEY 256    3 6 ...
tools.ietf.org 1800 IN DNSKEY 257    3 7 ...
```

Namespace Management Concept

NDNSSEC: Producer Authorization

ndnified DNS Zone Space



Producer

Zone Owner

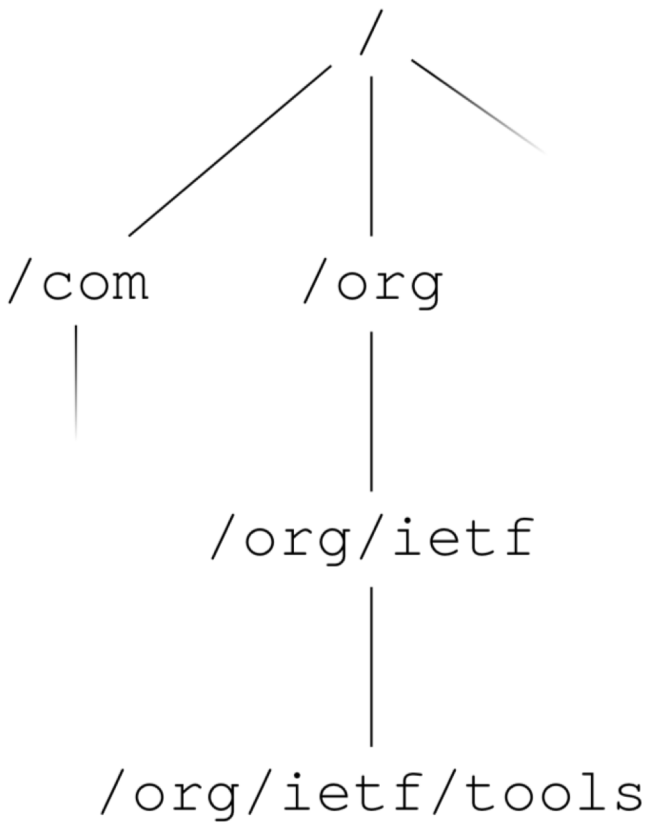
Excerpt of DNS zone records

```
tools.ietf.org 1800 IN RRSIG  DNSKEY 7 2 1800 ...
tools.ietf.org 1800 IN DNSKEY 256    3 6 ...
tools.ietf.org 1800 IN DNSKEY 257    3 7 ...
tools.ietf.org 1800 IN DNSKEY XXX    X X ...
```

Namespace Management Concept

NDNSSEC: Producer Authorization

ndnified DNS Zone Space

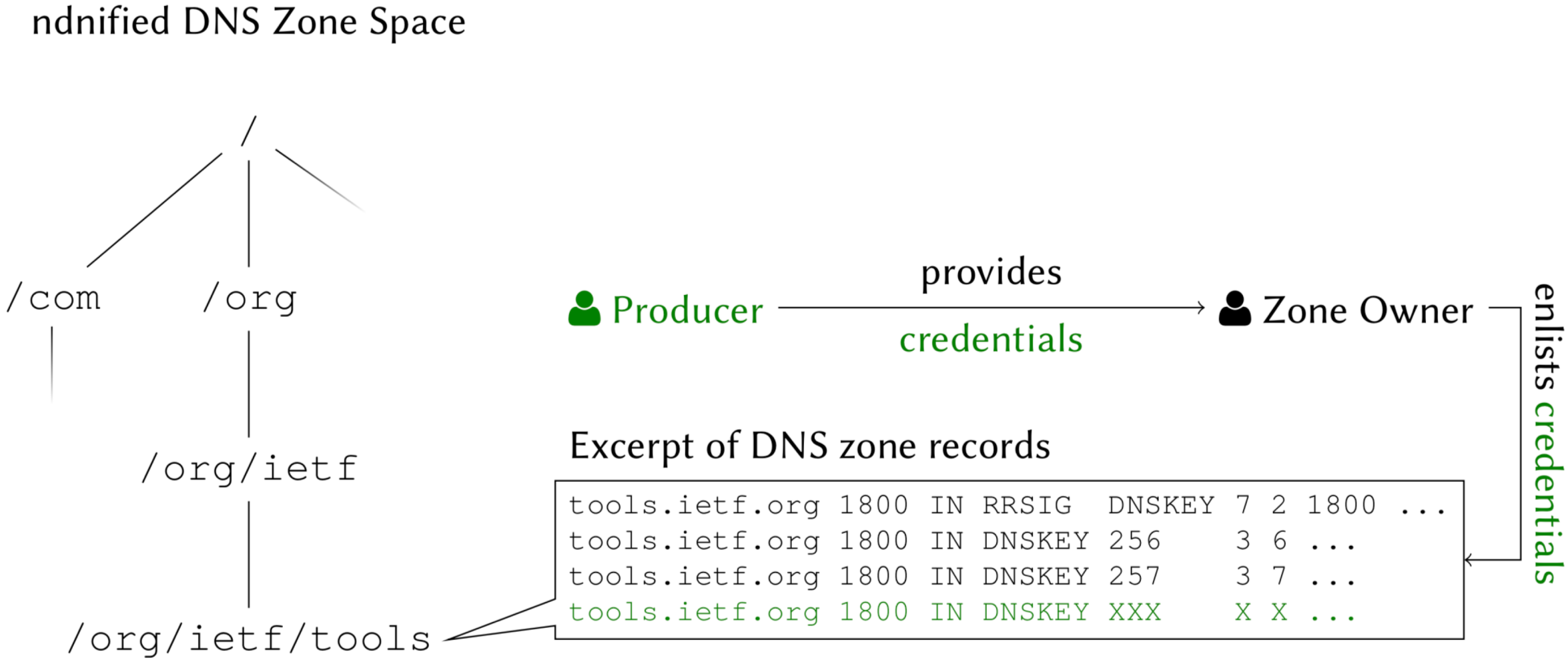


Excerpt of DNS zone records

```
tools.ietf.org 1800 IN RRSIG  DNSKEY 7 2 1800 ...
tools.ietf.org 1800 IN DNSKEY 256    3 6 ...
tools.ietf.org 1800 IN DNSKEY 257    3 7 ...
tools.ietf.org 1800 IN DNSKEY XXX    X X ...
```

Namespace Management Concept

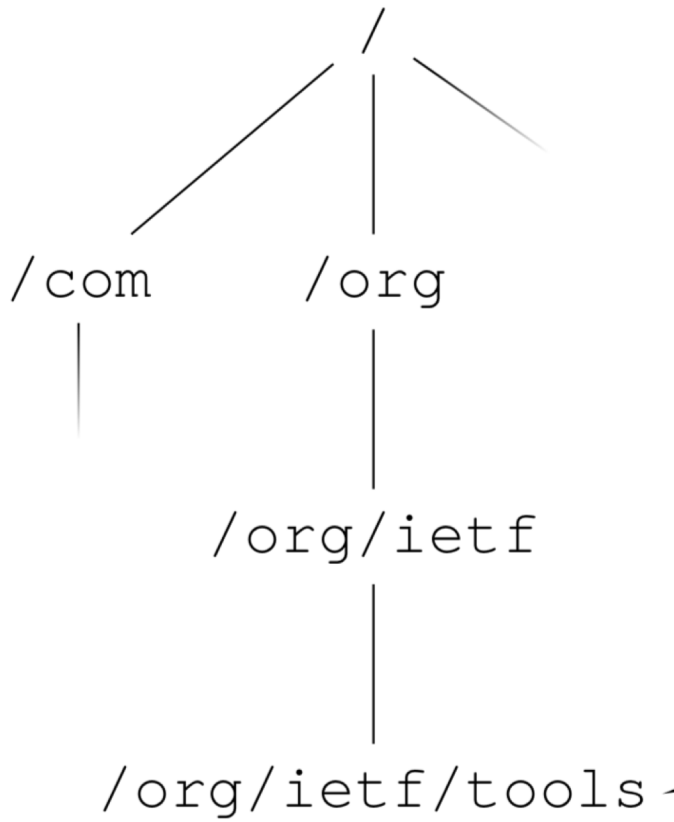
NDNSSEC: Producer Authorization



Namespace Management Concept

NDNSEC: Data Publishing

ndnified DNS Zone Space



Data Packet

/html/rfc882
Meta Info
Content

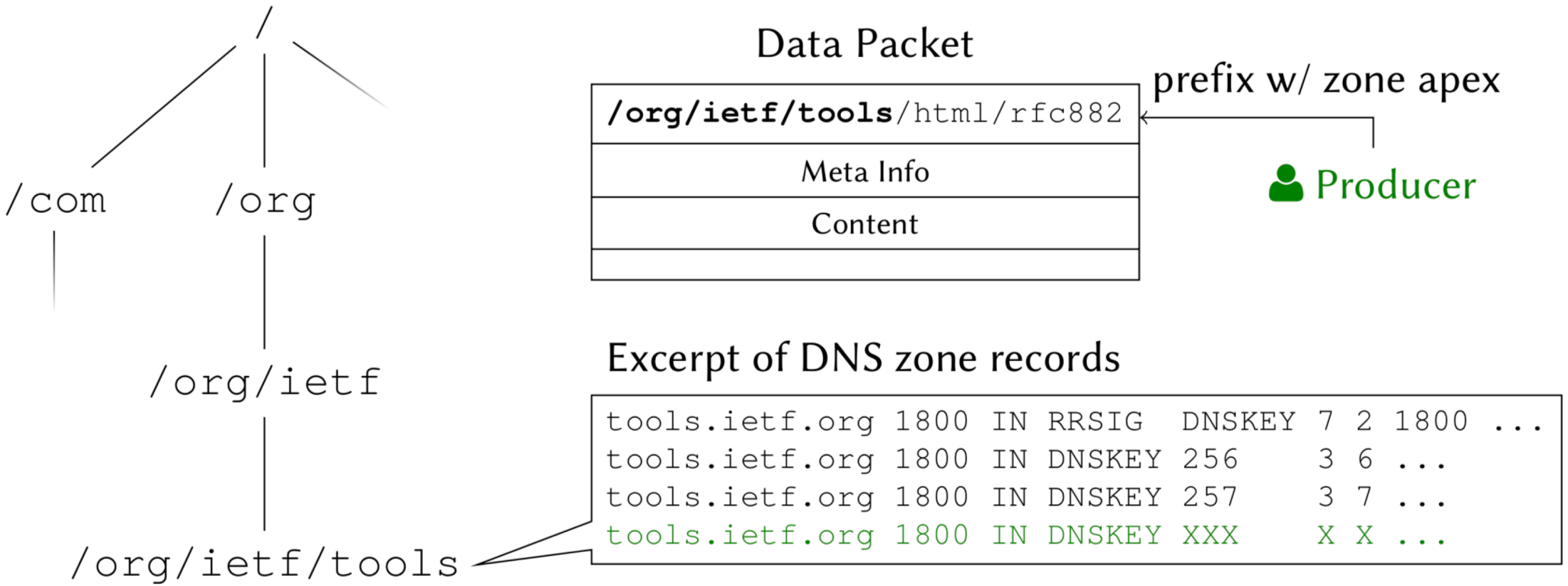
Producer

Excerpt of DNS zone records

```
tools.ietf.org 1800 IN RRSIG  DNSKEY 7 2 1800 ...
tools.ietf.org 1800 IN DNSKEY 256    3 6 ...
tools.ietf.org 1800 IN DNSKEY 257    3 7 ...
tools.ietf.org 1800 IN DNSKEY XXX    X X ...
```

Namespace Management Concept

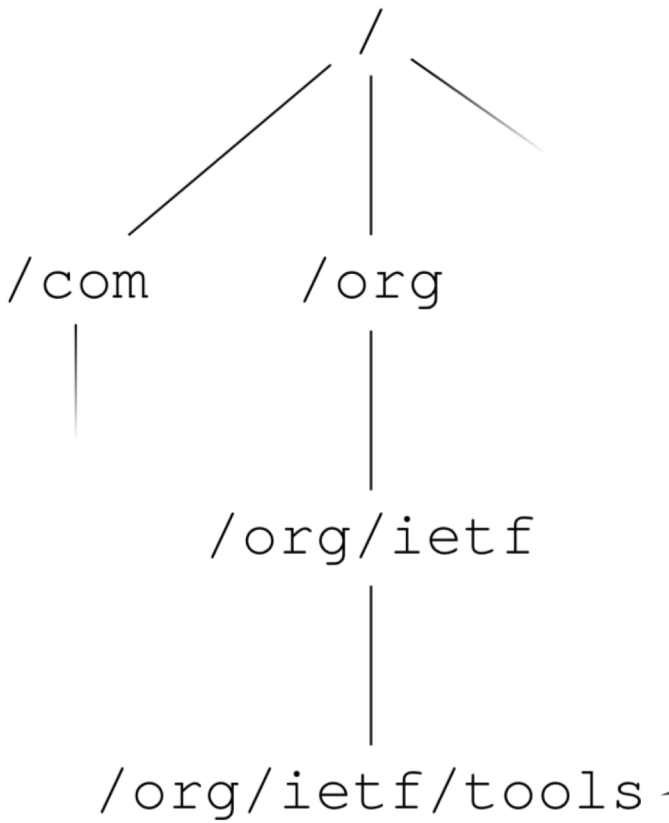
NDNSSEC: Data Publishing



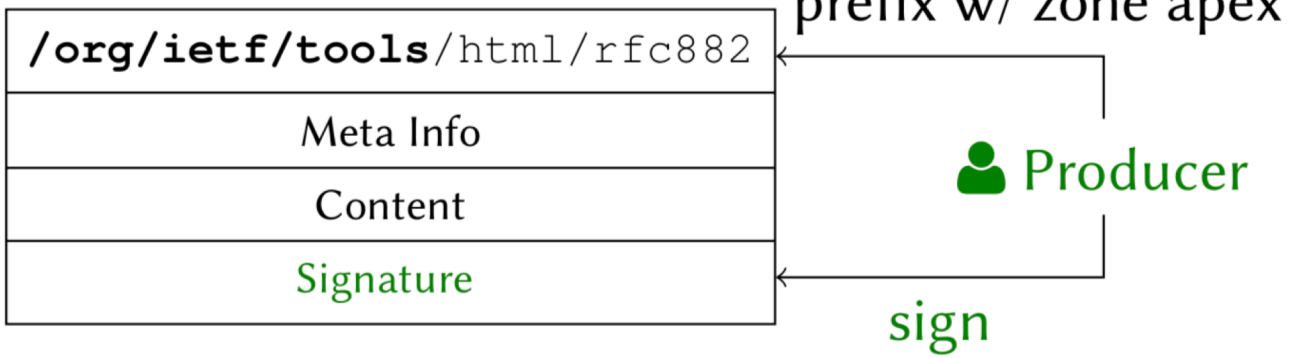
Namespace Management Concept

NDNSSEC: Data Publishing

ndnified DNS Zone Space



Data Packet

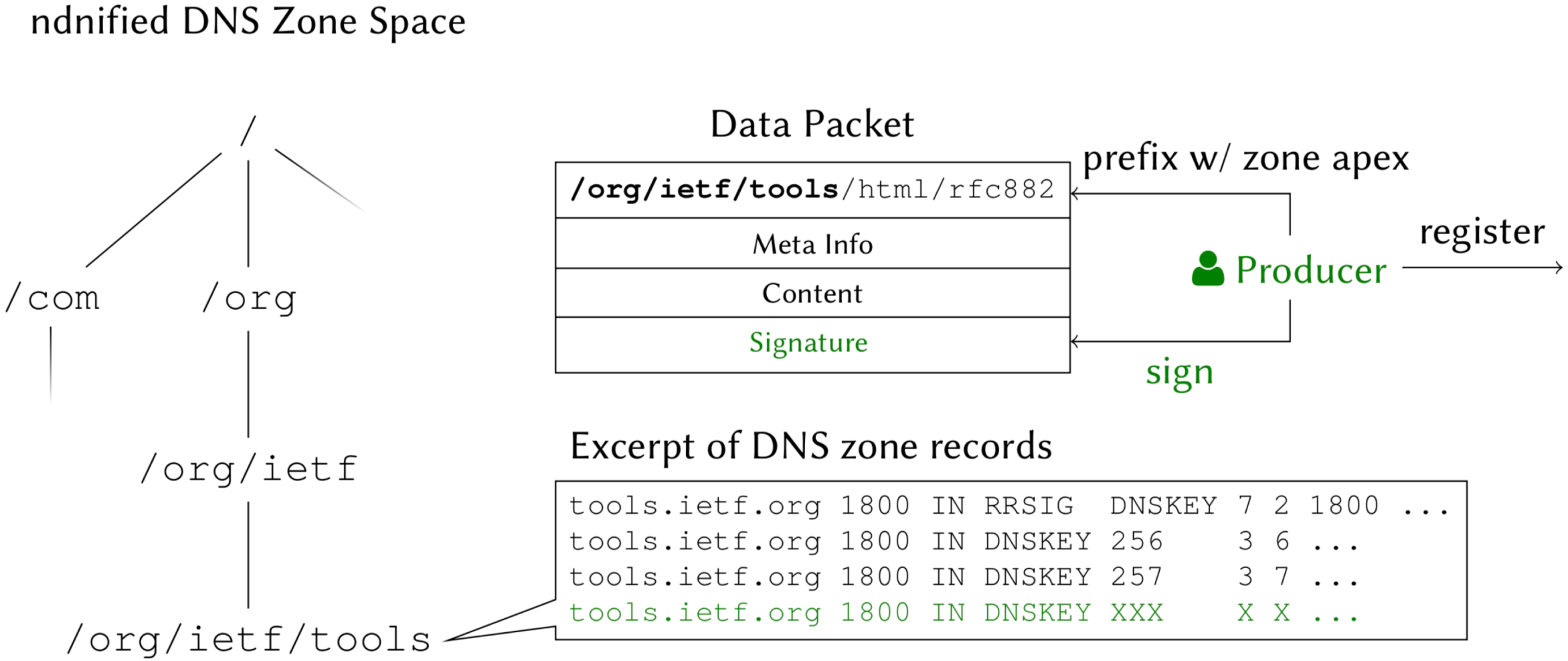


Excerpt of DNS zone records

```
tools.ietf.org 1800 IN RRSIG  DNSKEY 7 2 1800 ...
tools.ietf.org 1800 IN DNSKEY 256    3 6 ...
tools.ietf.org 1800 IN DNSKEY 257    3 7 ...
tools.ietf.org 1800 IN DNSKEY XXX    X X ...
```

Namespace Management Concept

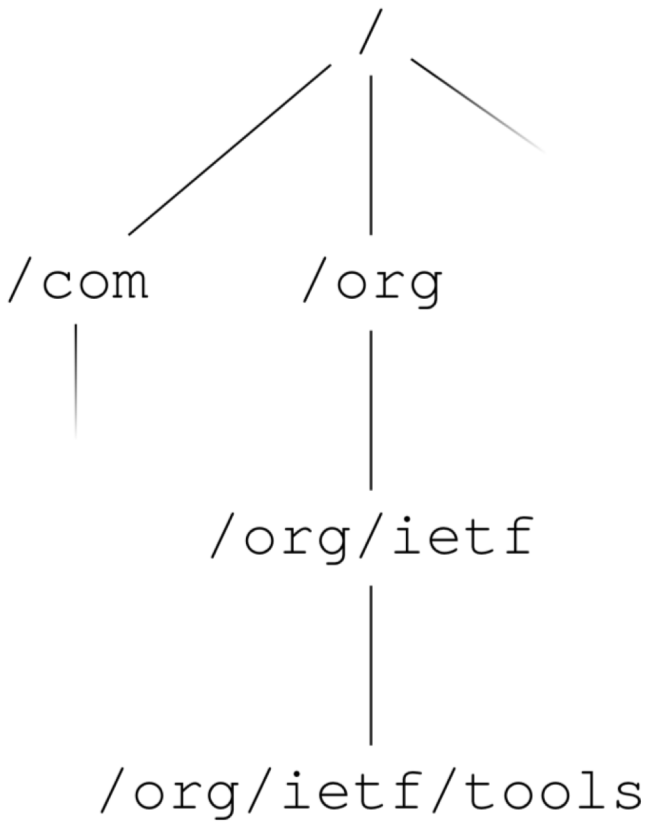
NDNSEC: Data Publishing



Namespace Management Concept

NDNSSEC: Producer Authentication

ndnified DNS Zone Space



Data Packet

/org/ietf/tools/html/rfc882
Meta Info
Content
Signature

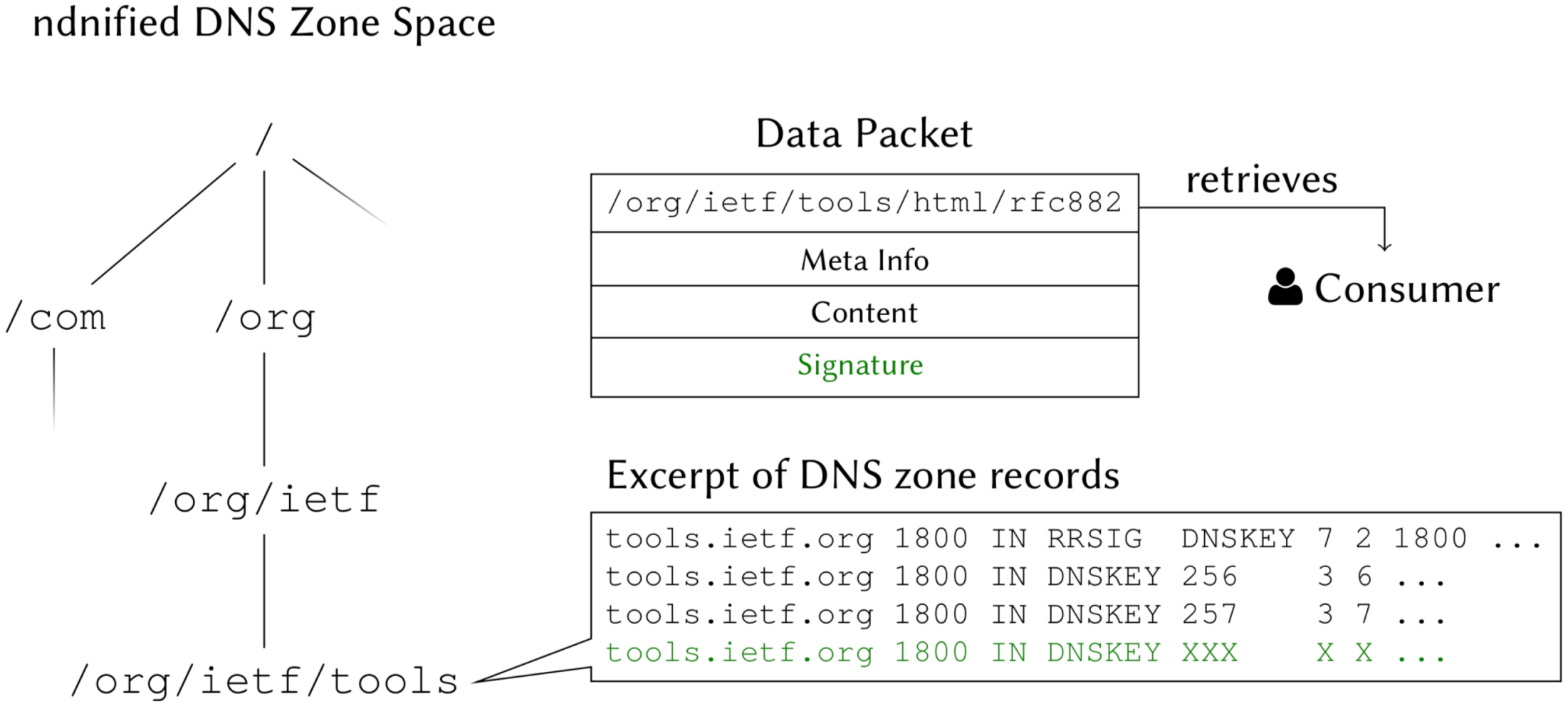
Consumer

Excerpt of DNS zone records

```
tools.ietf.org 1800 IN RRSIG  DNSKEY 7 2 1800 ...
tools.ietf.org 1800 IN DNSKEY 256    3 6 ...
tools.ietf.org 1800 IN DNSKEY 257    3 7 ...
tools.ietf.org 1800 IN DNSKEY XXX    X X ...
```

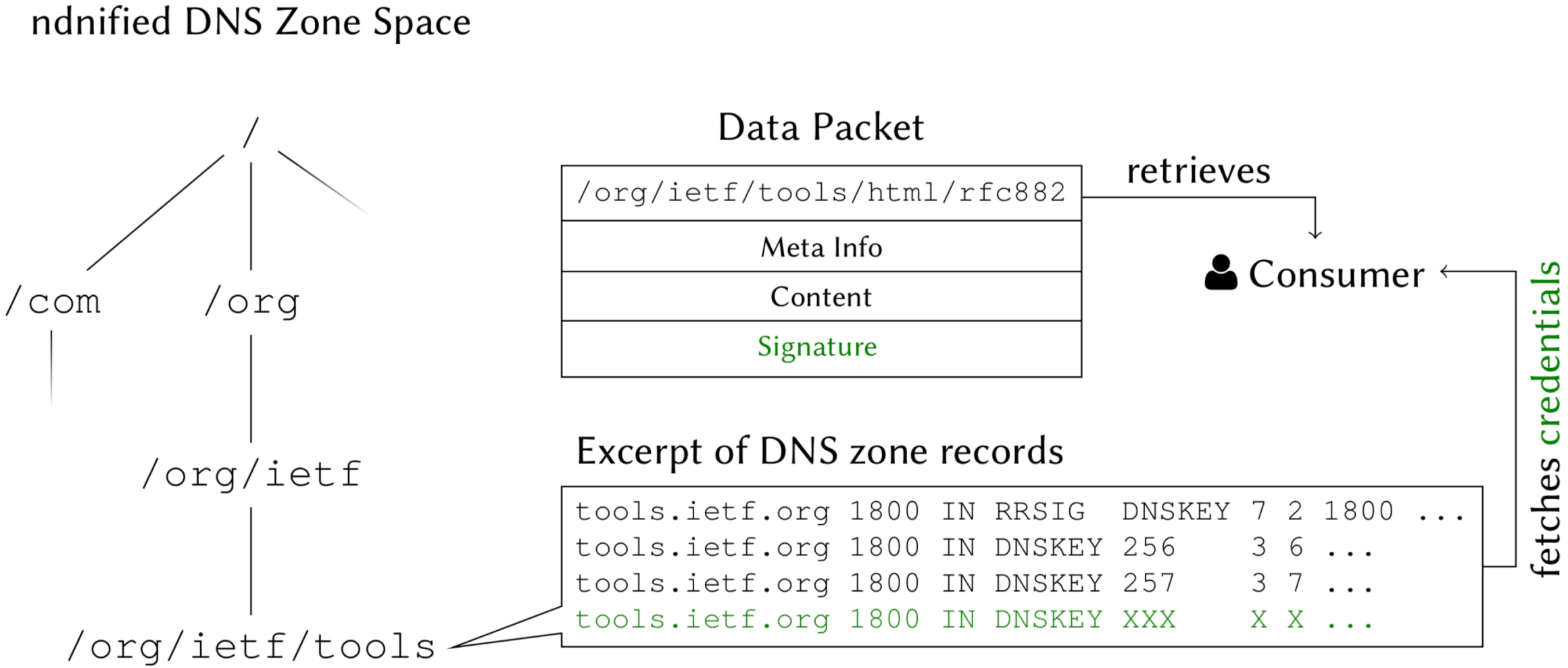
Namespace Management Concept

NDNSSEC: Producer Authentication



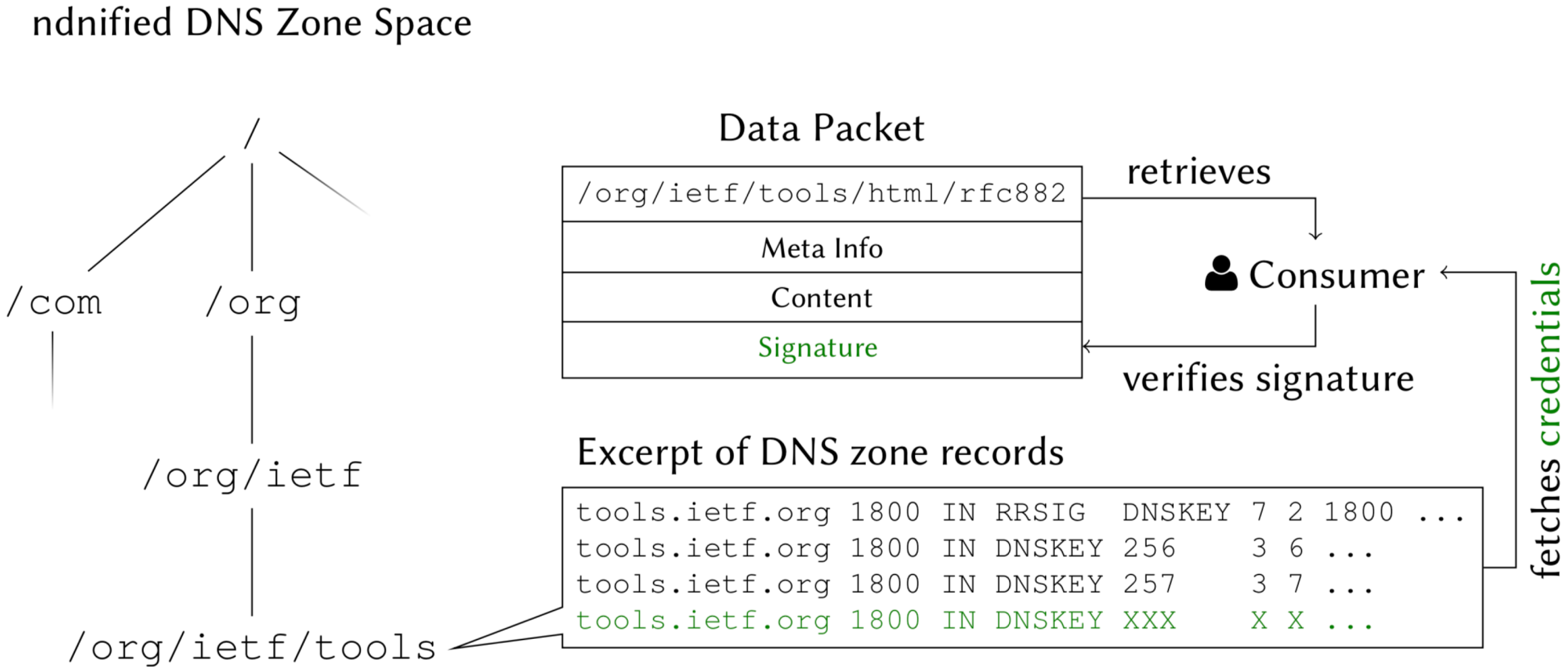
Namespace Management Concept

NDNSSEC: Producer Authentication



Namespace Management Concept

NDNSSEC: Producer Authentication



Conclusions and research roadmap

Where we are:

- Non-technical policy enforcement
- Synergized with ICN
- Deterministic authentication
- No additional infrastructure for certificate revocation

Where we're headed

- DNS data w/o DNS transport
- Evaluate performance (synchronization disparities, etc.)
- Evaluate with user studies
- Explore feasibility in use cases

Thank you

Questions?

Bib

- Afanasyev, A. Addressing Operational Challenges in Named Data Networking Through NDNS Distributed Database. PhD thesis, University of California Los Angeles, 2013.
- Afanasyev, A., Jiang, X., Yu, Y., Tan, J., Xia, Y., Mankin, A., and Zhang, L. NDNS: A DNS-Like Name Service for NDN. In 2017 26th International Conference on Computer Communication and Networks (ICCCN) (07 2017), IEEE, pp. 1–9.
- Day, J. Patterns in Network Architecture: A Return to Fundamentals. Pearson Education, 2007.
- Detti, A., Blefari Melazzi, N., Salsano, S., and Pomposini, M. CONET. In Proceedings of the ACM SIGCOMM workshop on Information-centric networking - ICN ’11 (New York, New York, USA, 2011), ACM Press, pp. 50–55.

Bib (2)

- DiBenedetto, S., and Papadopoulos, C. Mitigating poisoned content with forwarding strategy. In 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (04 2016), no. 970, IEEE, pp. 164–169.
- Elz, R., and Bush, R. Clarifications to the DNS Specification. RFC 2181, 07 1997.
- Farrell, S., Kutscher, D., Dannewitz, C., Ohlman, B., Kera¨nen, A., and Hallam-Baker, P. Naming Things with Hashes. RFC 6920, 04 2013.
- Hamdane, B., Boussada, R., Elhdhili, M. E., and Fatmi, S. G. E. Hierarchical Identity Based Cryptography for Security and Trust in Named Data Networking. In 2017 IEEE 26th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE) (06 2017), IEEE, pp. 226–231.
- Mahadevan, P., Uzun, E., Sevilla, S., and Garcia-Luna-Aceves, J. CCN-KRS. In Proceedings of the 1st international conference on Information-centric networking - INC ’14 (New York, New York, USA, 2014), vol. 94304, ACM Press, pp. 97–106.

Bib (3)

- Rose, S., Larson, M., Massey, D., Austein, R., and Arends, R. DNS Security Introduction and Requirements. RFC 4033, 03 2005.
- Venkataramani,A.,Kurose,J.F.,Raychaudhuri,D.,Nagaraja,K.,Mao,M.,andBanerjee,S. Mobilityfirst: A mobility-centric and trustworthy internet architecture. SIGCOMM Comput. Commun. Rev. 44, 3 (07 2014), 74–80.
- Wong, W., and Nikander, P. Secure naming in information-centric networks. In Proceedings of the Re-Architecting the Internet Workshop on - ReARCH ’10 (New York, New York, USA, 2010), ACM Press, pp. 12:1–12:6.
- Zhang, X., Chang, K., Xiong, H., Wen, Y., Shi, G., and Wang, G. Towards name-based trust and security for content-centric network. In 2011 19th IEEE International Conference on Network Protocols (10 2011), IEEE, pp. 1–6.

Backup

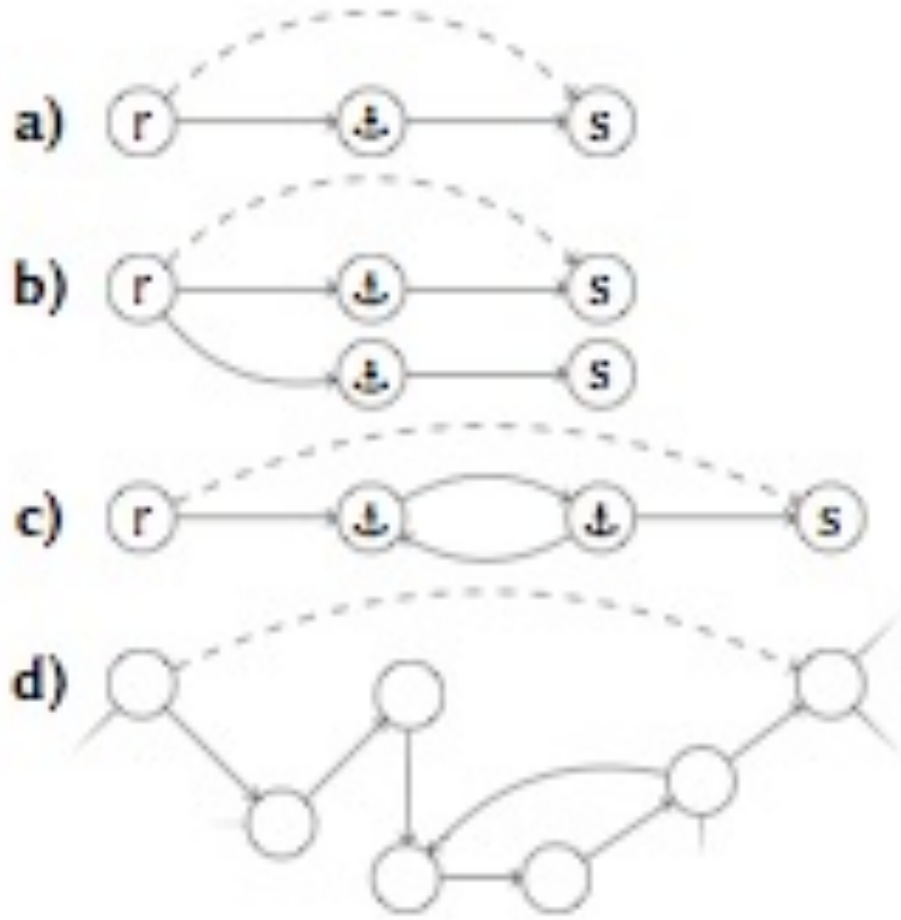
Industry's role in the Internet's history

- Commercial incentives have driven considerations in naming
- Successful companies rely on (among other things) name-recognition,
  - Trademarks and naming are important security elements

- DNS is a historical example of successful Internet name management
- Has had a very large component of non-technical innovations and protections

Trust Models

Transitive Trust



Trust Models

Certificate Chain Verification Complexity

	Level 1 (root)	Level i (interim)	Level n (leaf)	⚓
Trust Schema	⚓ C_0 ⟵ ⋯ ⟵ C_i ⟵ ⋯ ⟵ C_n			≥ 1
NDNS	⚓ $\texttt{KSK}_0$ → $\texttt{DSK}_0$ ⋰	$\texttt{DKEY}_i$ → $\texttt{KSK}_i$ → $\texttt{DSK}_i$ ⋰	$\texttt{DKEY}_n$ → $\texttt{KSK}_n$ → $\texttt{DSK}_n$ → $\texttt{APPCERT}_n$	≥ 1
NDNSSEC	⚓ $\texttt{DNSKEY}_0$ → $\texttt{NS}_0$ ⋮ $\texttt{DS}_0$	$\texttt{DNSKEY}_i$ → $\texttt{NS}_i$ ⋱ $\texttt{DS}_i$	→ $\texttt{DNSKEY}_n$	$= 1$

Related Work

	Authentication				
	$\mathcal{N} \rightarrow \mathcal{T}$	$\mathcal{N} \rightarrow \mathcal{Z}$	Self-auth	Zone Scope	Trust Relation
DNSSEC [10]	✓	✓	✘	$\mathcal{N}$	Decentralized
Detti et al. [4]	✓	✓	✓*	$\mathcal{I}$	Decentralized
Venkataramani et al. [11]	✓	✘	✓*	$\emptyset$	N/A
Farrell et al. [7]	✓	✘	✓	$\emptyset$	N/A
Wong and Nikander [12]	✓	✓	✘	$\mathcal{I}$	Centralized
Afanasyev [2, 1]	✓	✓	✘	$\mathcal{N}$	Decentralized
Mahadevan et al. [9]	✓	✓	✘	$\mathcal{N}$	Decentralized
DiBenedetto and Papadopoulos [5]	✓	✓	✘	$\mathcal{N}$	Decentralized
Zhang et al. [13]	✓	✓	✓*	$\mathcal{I}/\mathcal{N}$	Decentralized
Hamdane et al. [8]	✓	✓	✓*	$\mathcal{I}$	Decentralized

* Denotes *self-certification*