SoK: Namespace and Public Key Management in NDN

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

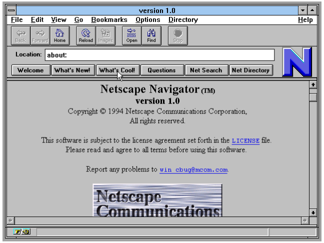
[1]Weizenbaum Institut / Fraunhofer FOKUS [2]George Mason University [3]Hamburg University of Applied Sciences [4]Freie Universität Berlin

ACM ICN 2022, September 19-21, 2022 – Osaka, Japan

Information Centric Networking the next generation Internet.

A brief and inaccurate history.

Commercialization of the Internet



Location: about:

Netscape Navigator (TM)
version 1.0
Copyright © 1994 Netscape Communications Corporation,
All rights reserved.

This software is subject to the license agreement set forth in the LICENSE file.
Please read and agree to all terms before using this software.

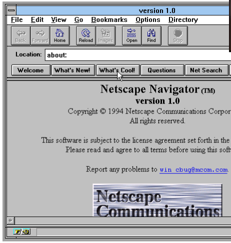
Report any problems to win_cbug@mcom.com.

1994

Information Centric Networking the next generation Internet.

A brief and inaccurate history.

Commercialization of the Internet


version 1.0
File Edit View Go Bookmarks Options Directory
Back Forward Home Reload Images Open Find Stop
Welcome What's New! What's Cool! Questions Net Search Net Directory

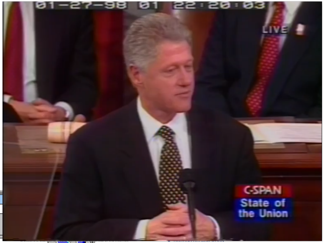
Location: about:

Netscape Navigator (TM)
version 1.0
Copyright © 1994 Netscape Communications Corporation,
All rights reserved.

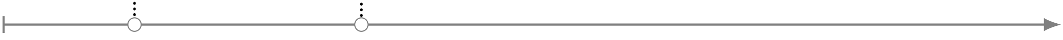
This software is subject to the license agreement set forth in the LICENSE file.
Please read and agree to all terms before using this software.

Report any problems to win_cbug@mcom.com.

Netscape Communications

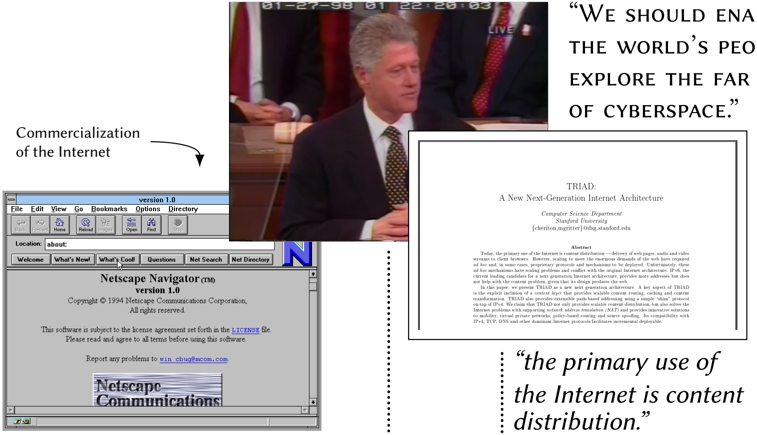


> “We should enable all the world’s people to explore the far reaches of cyberspace.”



Information Centric Networking the next generation Internet.

A brief and inaccurate history.


01-27-98 01 22:20:03
LIVE
version 1.0
File Edit View Go Bookmarks Options Directory
Back Forward Home Reload Images Open Find Stop
Location: about:
Welcome What's New! What's Cool! Questions Net Search Net Directory

Netscape Navigator (TM)
version 1.0
Copyright © 1994 Netscape Communications Corporation,
All rights reserved.

This software is subject to the license agreement set forth in the LICENSE file.
Please read and agree to all terms before using this software.

Report any problems to win_cbug@mcom.com

Netscape Communications

TRIAD:
A New Next-Generation Internet Architecture

Computer Science Department
Stanford University
{cheriton,mgritter}@dsg.stanford.edu

Abstract

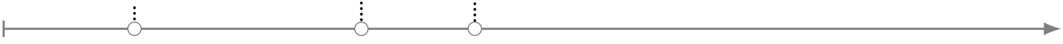
Today, the primary use of the Internet is content distribution — delivery of web pages, audio and video streams to client browsers. However, scaling to meet the enormous demands of the web have required *ad hoc* and, in some cases, proprietary protocols and mechanisms to be deployed. Unfortunately, these *ad hoc* mechanisms have scaling problems and conflict with the original Internet architecture. IPv6, the current leading candidate for a next generation Internet architecture, provides more addresses but does not help with the content problem, given that its design predates the web.

In this paper, we present TRIAD as a new next generation architecture. A key aspect of TRIAD is the explicit inclusion of a *content layer* that provides scalable content routing, caching and content transformation. TRIAD also provides extensible path-based addressing using a simple "shim" protocol on top of IPv4. We claim that TRIAD not only provides scalable content distribution, but also solves the Internet problems with supporting *network address translation (NAT)* and provides innovative solutions to mobility, virtual private networks, policy-based routing and source spoofing. Its compatibility with IPv4, TCP, DNS and other dominant Internet protocols facilitates incremental deployable.

Commercialization of the Internet

"We should enable all the world's people to explore the far reaches of cyberspace."

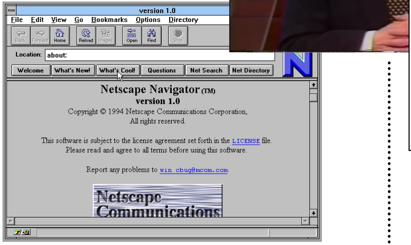
"the primary use of the Internet is content distribution."



Information Centric Networking the next generation Internet.

A brief and inaccurate history.

Commercialization of the Internet



version 1.0
File Edit View Go Bookmarks Options Directory
Back Forward Home Reload Images Open Find Stop
Welcome What's New! What's Cool! Questions Net Search Net Directory
Netscape Communications

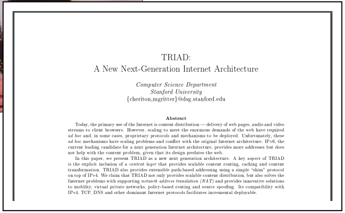
Location: about:

Netscape Navigator (TM)
version 1.0
Copyright © 1994 Netscape Communications Corporation,
All rights reserved.

This software is subject to the license agreement set forth in the LICENSE file.
Please read and agree to all terms before using this software.

Report any problems to win cbug@mcom.com.

"WE SHOULD ENABLE ALL THE WORLD'S PEOPLE TO EXPLORE THE FAR REACHES OF CYBERSPACE."



TRIAD:
A New Next-Generation Internet Architecture

Computer Science Department
Stanford University
{cheriton,mgritter}@dsg.stanford.edu

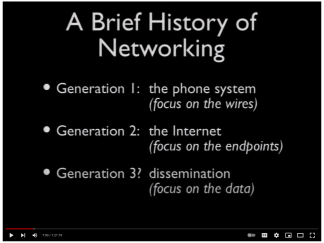
Abstract

Today, the primary use of the Internet is content distribution — delivery of web pages, audio and video streams to client browsers. However, scaling to meet the enormous demands of the web have required *ad hoc* and, in some cases, proprietary protocols and mechanisms to be deployed. Unfortunately, these *ad hoc* mechanisms have scaling problems and conflict with the original Internet architecture. IPv6, the current leading candidate for a next generation Internet architecture, provides more addresses but does not help with the content problem, given that its design predates the web.

In this paper, we present TRIAD as a new next generation architecture. A key aspect of TRIAD is the explicit inclusion of a *content layer* that provides scalable content routing, caching and content transformation. TRIAD also provides extensible path-based addressing using a simple "shim" protocol on top of IPv4. We claim that TRIAD not only provides scalable content distribution, but also solves the Internet problems with supporting *network address translation (NAT)* and provides innovative solutions to mobility, virtual private networks, policy-based routing and source spoofing. Its compatibility with IPv4, TCP, DNS and other dominant Internet protocols facilitates incremental deployable.

"the primary use of the Internet is content distribution."

CCN was born



A Brief History of Networking

- Generation 1: the phone system *(focus on the wires)*
- Generation 2: the Internet *(focus on the endpoints)*
- Generation 3? dissemination *(focus on the data)*

1994 1998 2000 2006

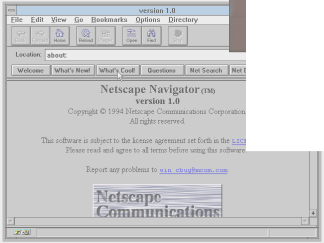
Information Centric Networking the next generation Internet.

A brief and inaccurate history.

"We should enable all the world's people to

Are we there yet? Why not?

Commercialization of the Internet

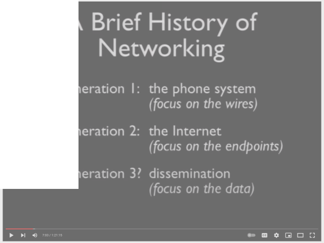

version 1.0
File Edit View Go Bookmarks Options Directory
Back Forward Home Reload Images Open Find Stop
Location: about:
Welcome What's New! What's Cool! Questions Net Search Net D

Netscape Navigator (TM)
version 1.0
Copyright © 1994 Netscape Communications Corporation
All rights reserved.

This software is subject to the license agreement set forth in the LICE
Please read and agree to all terms before using this software.

Report any problems to win_cbug@mcom.com

CCN was born



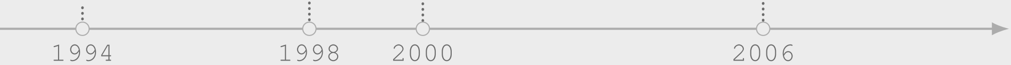
Brief History of Networking

eration 1: the phone system (focus on the wires)

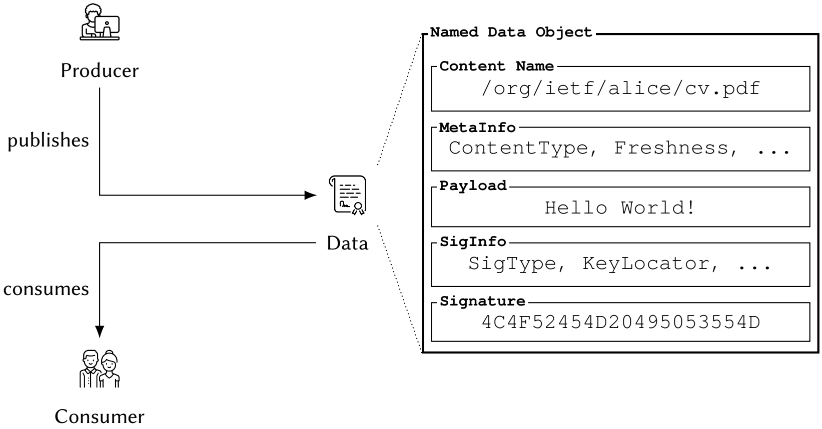
eration 2: the Internet (focus on the endpoints)

eration 3? dissemination (focus on the data)

"the primary use of the Internet is content distribution."



Named Data Networking NDN



Named Data Object

Content Name
/org/ietf/alice/cv.pdf

MetaInfo
ContentType, Freshness, ...

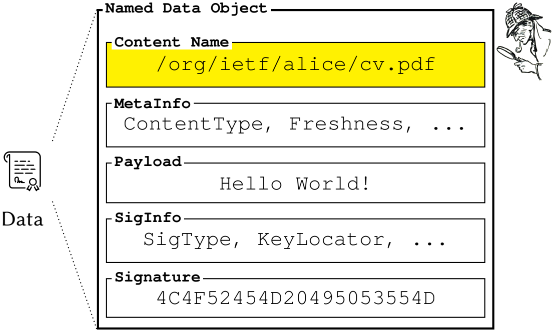
Payload
Hello World!

SigInfo
SigType, KeyLocator, ...

Signature
4C4F52454D20495053554D

Named Data Networking NDN

$\underbrace{\texttt{/org/ietf}}_{\text{Global}}\underbrace{\texttt{/alice/cv.pdf}}_{\text{Local / Application name}}$



Data

Named Data Object

Content Name
/org/ietf/alice/cv.pdf

MetaInfo
ContentType, Freshness, ...

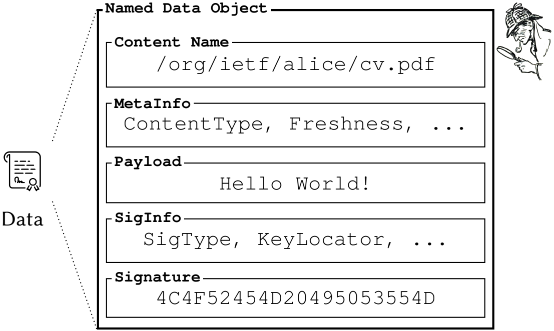
Payload
Hello World!

SigInfo
SigType, KeyLocator, ...

Signature
4C4F52454D20495053554D

Named Data Networking NDN

$$\underbrace{\texttt{/org/ietf}}_{\text{Global}}\underbrace{\texttt{/alice/cv.pdf}}_{\text{Local / Application name}}$$



Data

Named Data Object

Content Name
/org/ietf/alice/cv.pdf

MetaInfo
ContentType, Freshness, ...

Payload
Hello World!

SigInfo
SigType, KeyLocator, ...

Signature
4C4F52454D20495053554D

```
http://ietf.org/alice/cv.pdf
alice@ietf.org
```

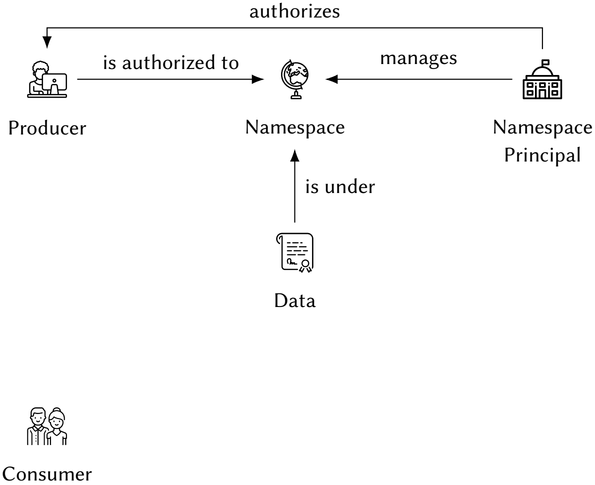
Named Data Networking NDN

Producer

Challenge: how can data be securely bound to its name?

Consumer

Named Data Networking NDN



authorizes

is authorized to

manages

Producer

Namespace

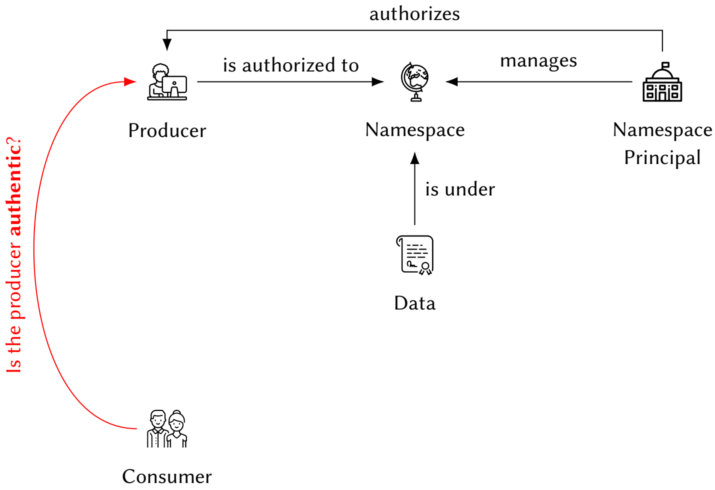
Namespace Principal

is under

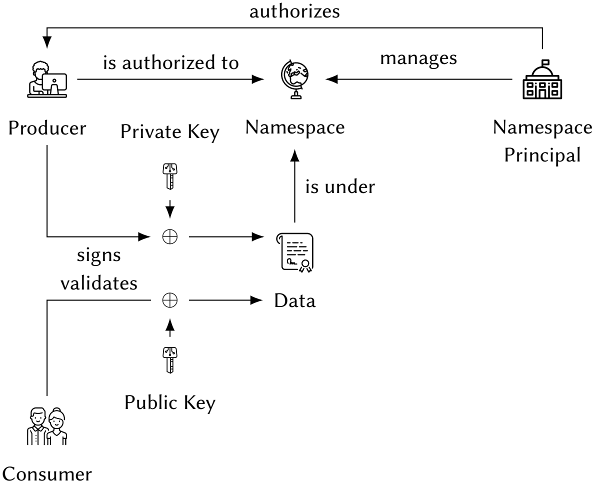
Data

Consumer

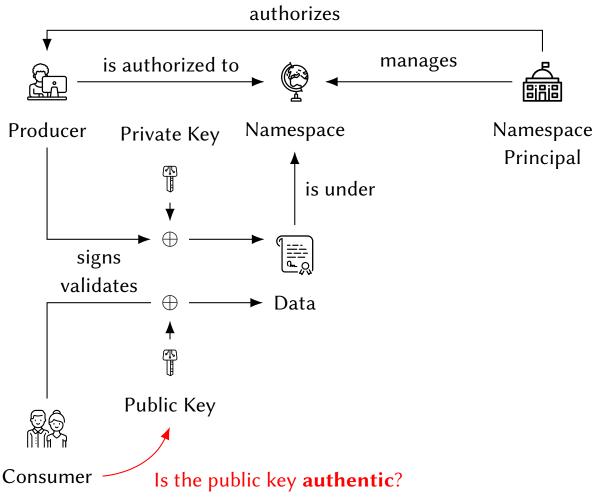
Named Data Networking NDN



Named Data Networking NDN

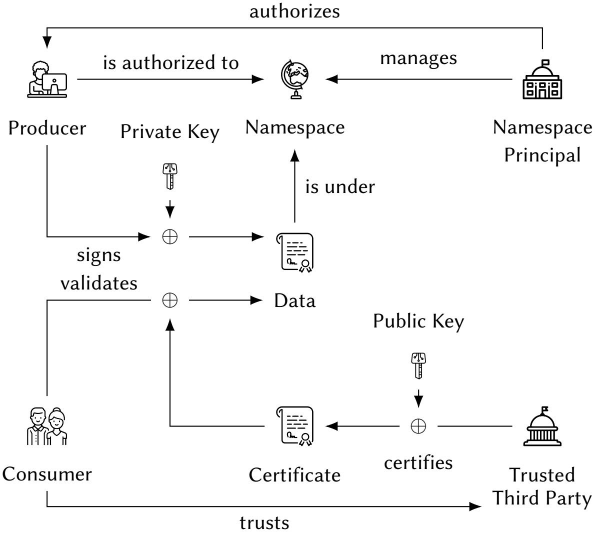


Named Data Networking NDN

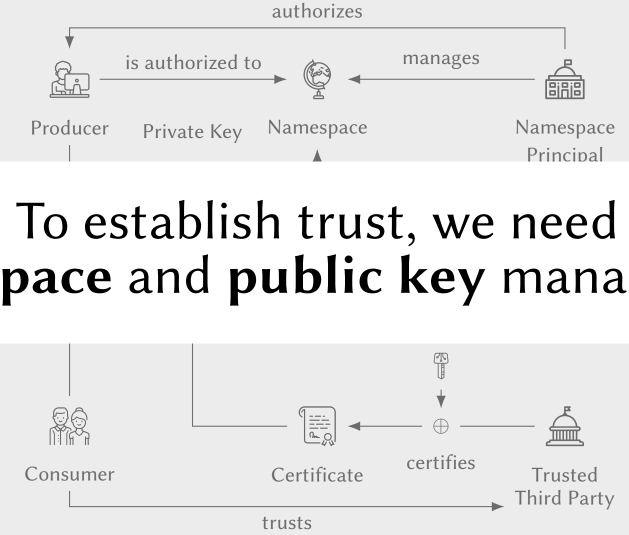


Is the public key **authentic**?

Named Data Networking NDN



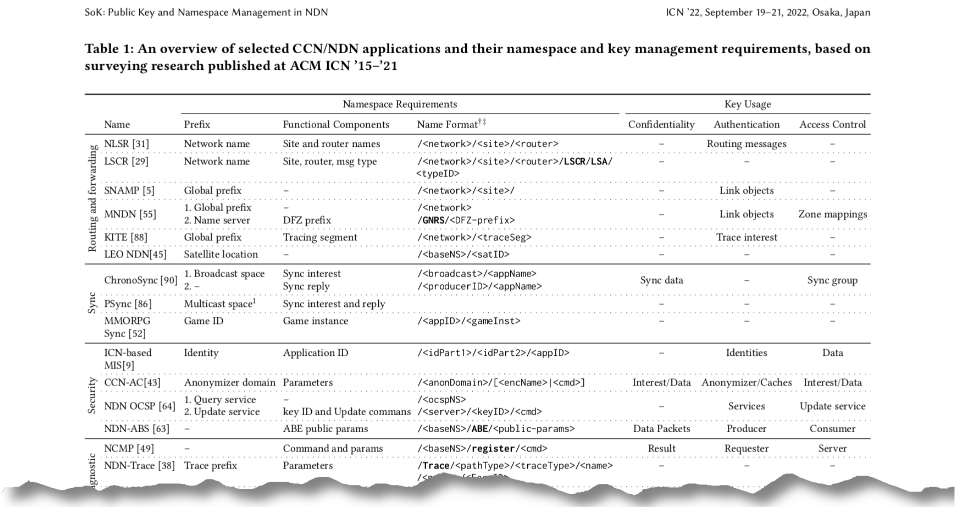
Named Data Networking NDN



To establish trust, we need **namespace** and **public key** management

Status Quo ACM ICN ’15 – ’21

Survey of over 30 NDN applications



SoK: Public Key and Namespace Management in NDN — ICN ’22, September 19–21, 2022, Osaka, Japan

Table 1: An overview of selected CCN/NDN applications and their namespace and key management requirements, based on surveying research published at ACM ICN ’15–’21

		Namespace Requirements			Key Usage		
	Name	Prefix	Functional Components	Name Format†‡	Confidentiality	Authentication	Access Control
Routing and forwarding	NLSR [31]	Network name	Site and router names	`/<network>/<site>/<router>`	–	Routing messages	–
	LSCR [29]	Network name	Site, router, msg type	`/<network>/<site>/<router>/`**`LSCR/LSA`**`/<typeID>`	–	–	–
	SNAMP [5]	Global prefix	–	`/<network>/<site>/`	–	Link objects	–

	MNDN [55]	1. Global prefix
		2. Name server
			–
			DFZ prefix
				`/<network>`
				`/`**`GNRS`**`/<DFZ-prefix>`
					–	Link objects	Zone mappings

	KITE [88]	Global prefix	Tracing segment	`/<network>/<traceSeg>`	–	Trace interest	–
	LEO NDN[45]	Satellite location	–	`/<baseNS>/<satID>`	–	–	–

Sync	ChronoSync [90]	1. Broadcast space
		2. –
			Sync interest
			Sync reply
				`/<broadcast>/<appName>`
				`/<producerID>/<appName>`
					Sync data	–	Sync group

	PSync [86]	Multicast space[1]	Sync interest and reply		–	–	–
	MMORPG Sync [52]	Game ID	Game instance	`/<appID>/<gameInst>`	–	–	–
Security	ICN-based MIS[9]	Identity	Application ID	`/<idPart1>/<idPart2>/<appID>`	–	Identities	Data
	CCN-AC[43]	Anonymizer domain	Parameters	`/<anonDomain>/[<encName>|<cmd>]`	Interest/Data	Anonymizer/Caches	Interest/Data

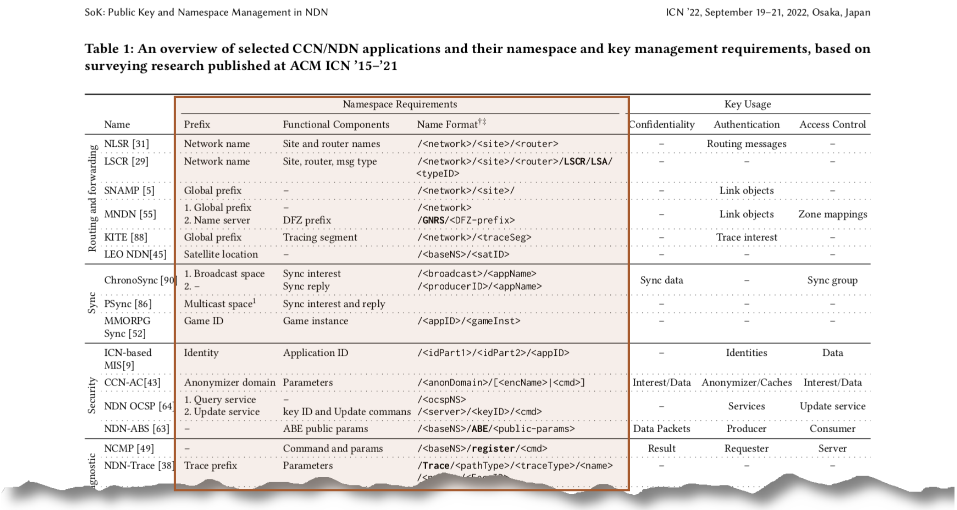
	NDN OCSP [64]	1. Query service
		2. Update service
			–
			key ID and Update commans
				`/<ocspNS>`
				`/<server>/<keyID>/<cmd>`
					–	Services	Update service

	NDN-ABS [63]	–	ABE public params	`/<baseNS>/`**`ABE`**`/<public-params>`	Data Packets	Producer	Consumer
gnostic	NCMP [49]	–	Command and params	`/<baseNS>/`**`register`**`/<cmd>`	Result	Requester	Server

	NDN-Trace [38]	Trace prefix	Parameters	`/`**`Trace`**`/<pathType>/<traceType>/<name>`
				`/<p[illegible]/<Fac[illegible]>`
					–	–	–

Status Quo ACM ICN ’15 – ’21

Survey of over 30 NDN applications



SoK: Public Key and Namespace Management in NDN

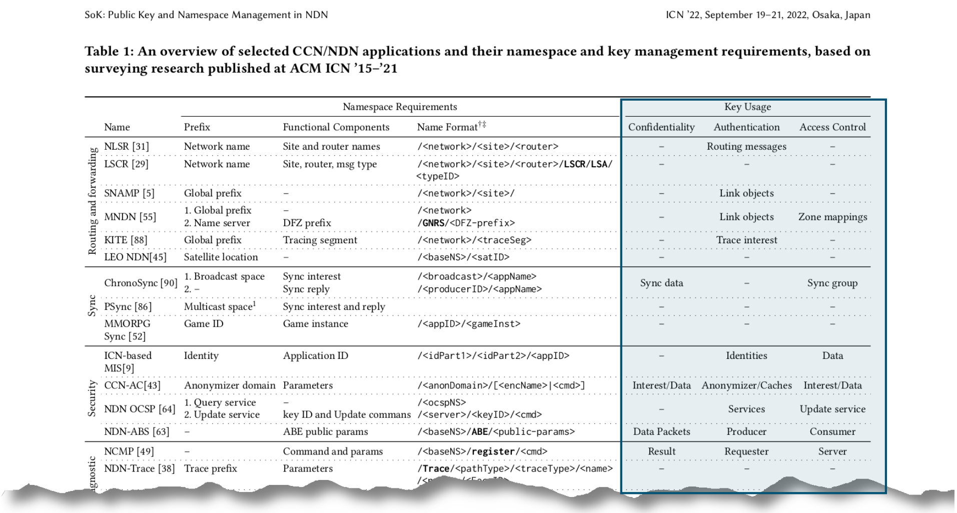
ICN ’22, September 19–21, 2022, Osaka, Japan

Table 1: An overview of selected CCN/NDN applications and their namespace and key management requirements, based on surveying research published at ACM ICN ’15–’21

		Namespace Requirements			Key Usage		
	Name	Prefix	Functional Components	Name Format†‡	Confidentiality	Authentication	Access Control
Routing and forwarding	NLSR [31]	Network name	Site and router names	/<network>/<site>/<router>	–	Routing messages	–
	LSCR [29]	Network name	Site, router, msg type	/<network>/<site>/<router>/**LSCR**/**LSA**/<typeID>	–	–	–
	SNAMP [5]	Global prefix	–	/<network>/<site>/	–	Link objects	–
	MNDN [55]	1. Global prefix 2. Name server	– DFZ prefix	/<network> /**GNRS**/<DFZ-prefix>	–	Link objects	Zone mappings
	KITE [88]	Global prefix	Tracing segment	/<network>/<traceSeg>	–	Trace interest	–
	LEO NDN[45]	Satellite location	–	/<baseNS>/<satID>	–	–	–
Sync	ChronoSync [90]	1. Broadcast space 2. –	Sync interest Sync reply	/<broadcast>/<appName> /<producerID>/<appName>	Sync data	–	Sync group
	PSync [86]	Multicast space[1]	Sync interest and reply		–	–	–
	MMORPG Sync [52]	Game ID	Game instance	/<appID>/<gameInst>	–	–	–
Security	ICN-based MIS[9]	Identity	Application ID	/<idPart1>/<idPart2>/<appID>	–	Identities	Data
	CCN-AC[43]	Anonymizer domain	Parameters	/<anonDomain>/[<encName>|<cmd>]	Interest/Data	Anonymizer/Caches	Interest/Data
	NDN OCSP [64]	1. Query service 2. Update service	– key ID and Update commans	/<ocspNS> /<server>/<keyID>/<cmd>	–	Services	Update service
	NDN-ABS [63]	–	ABE public params	/<baseNS>/**ABE**/<public-params>	Data Packets	Producer	Consumer
gnostic	NCMP [49]	–	Command and params	/<baseNS>/**register**/<cmd>	Result	Requester	Server
	NDN-Trace [38]	Trace prefix	Parameters	/**Trace**/<pathType>/<traceType>/<name>	–	–	–

Status Quo ACM ICN ’15 – ’21

Survey of over 30 NDN applications



SoK: Public Key and Namespace Management in NDN — ICN ’22, September 19–21, 2022, Osaka, Japan

Table 1: An overview of selected CCN/NDN applications and their namespace and key management requirements, based on surveying research published at ACM ICN ’15–’21

		Namespace Requirements			Key Usage		
	Name	Prefix	Functional Components	Name Format[†‡]	Confidentiality	Authentication	Access Control
Routing and forwarding	NLSR [31]	Network name	Site and router names	`/<network>/<site>/<router>`	–	Routing messages	–
	LSCR [29]	Network name	Site, router, msg type	`/<network>/<site>/<router>/`**`LSCR`**`/`**`LSA`**`/<typeID>`	–	–	–
	SNAMP [5]	Global prefix	–	`/<network>/<site>/`	–	Link objects	–

	MNDN [55]	1. Global prefix
		2. Name server
			–
			DFZ prefix
				`/<network>`
				`/`**`GNRS`**`/<DFZ-prefix>`
					–	Link objects	Zone mappings

	KITE [88]	Global prefix	Tracing segment	`/<network>/<traceSeg>`	–	Trace interest	–
	LEO NDN[45]	Satellite location	–	`/<baseNS>/<satID>`	–	–	–

Sync	ChronoSync [90]	1. Broadcast space
		2. –
			Sync interest
			Sync reply
				`/<broadcast>/<appName>`
				`/<producerID>/<appName>`
					Sync data	–	Sync group

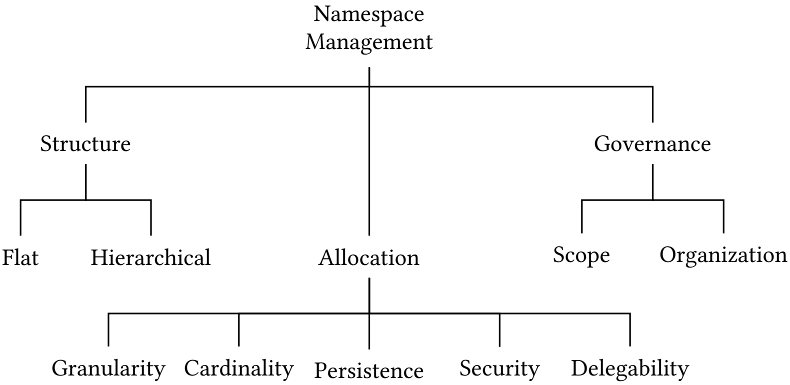
	PSync [86]	Multicast space[1]	Sync interest and reply		–	–	–
	MMORPG Sync [52]	Game ID	Game instance	`/<appID>/<gameInst>`	–	–	–
Security	ICN-based MIS[9]	Identity	Application ID	`/<idPart1>/<idPart2>/<appID>`	–	Identities	Data
	CCN-AC[43]	Anonymizer domain	Parameters	`/<anonDomain>/[<encName>|<cmd>]`	Interest/Data	Anonymizer/Caches	Interest/Data

	NDN OCSP [64]	1. Query service
		2. Update service
			–
			key ID and Update commans
				`/<ocspNS>`
				`/<server>/<keyID>/<cmd>`
					–	Services	Update service

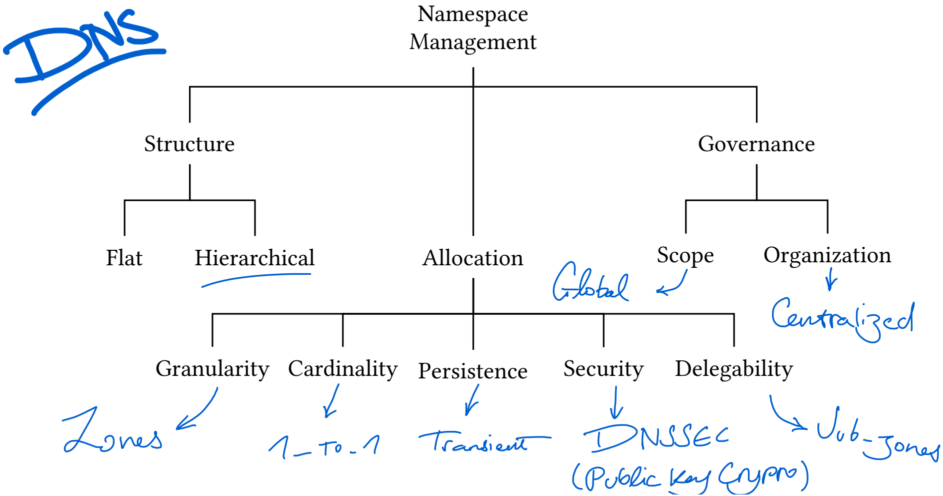
	NDN-ABS [63]	–	ABE public params	`/<baseNS>/`**`ABE`**`/<public-params>`	Data Packets	Producer	Consumer
gnostic	NCMP [49]	–	Command and params	`/<baseNS>/`**`register`**`/<cmd>`	Result	Requester	Server

	NDN-Trace [38]	Trace prefix	Parameters	`/`**`Trace`**`/<pathType>/<traceType>/<name>`
				`/<[illegible]>/<FaceID>`
					–	–	–

Namespace Management



Namespace Management

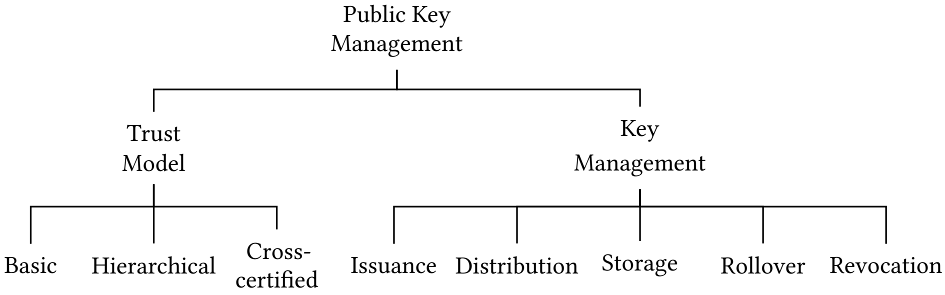


DNS

Namespace Management

- Structure
  - Flat
  - Hierarchical
- Allocation
  - Granularity → Zones
  - Cardinality → 1-To-1
  - Persistence → Transient
  - Security → DNSSEC (Public Key Crypto)
  - Delegability → Sub-Zones
- Governance
  - Scope → Global
  - Organization → Centralized

Public Key Management



Public Key Management

Trust Model

Key Management

Basic

Hierarchical

Cross-certified

Issuance

Distribution

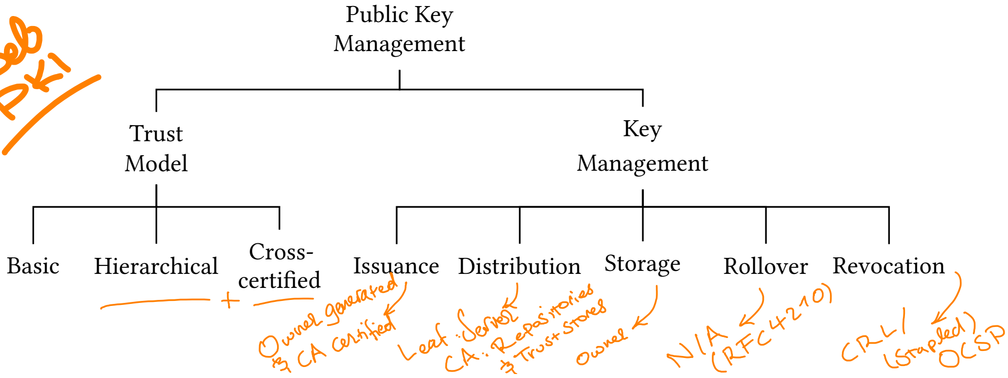
Storage

Rollover

Revocation

Public Key Management

Web PKI



Public Key Management

Trust Model

Basic

Hierarchical

Cross-certified

+

Key Management

Issuance

Owner generated & CA certified

Distribution

Leaf : Server

CA : Repositories & Trust Stores

Storage

Owner

Rollover

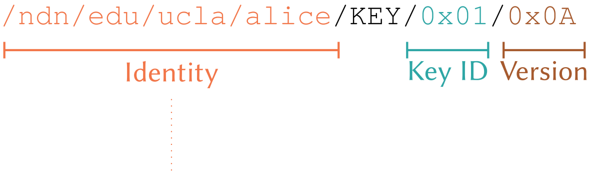
N/A (RFC4210)

Revocation

CRL / (Stapled) OCSP

NDN Public Key Management NDN PKM

NDN Technical Report – 2015



/ndn/edu/ucla/alice/KEY/0x01/0x0A

Denotes **both** Certificate owner and the namespace it controls

Namespace Management

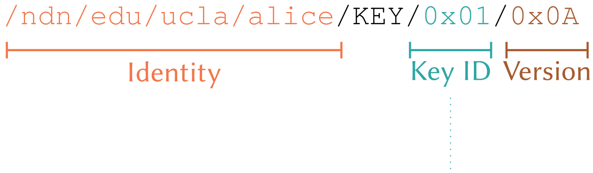
Structure:		Hierarchical
Allocation:		
↪	Granularity:	Subspace
↪	Cardinality:	$1 - n$
↪	Persistence:	Transient
↪	Security:	TA Signature
↪	Delegability:	✓
Governance:		
↪	Scope:	Local
↪	Organization:	Centralized

Public Key Management

Trust Model:		Hierarchical
Key Management:		
↪	Issuance:	Namespace Principal
↪	Distribution:	Owner / cert hosts
↪	Storage:	Owner
↪	Rollover:	✘
↪	Revocation:	Owner

NDN Public Key Management NDN PKM

NDN Technical Report – 2015



/ndn/edu/ucla/alice/KEY/0x01/0x0A

Allows binding multiple keys to the same identity

Namespace Management

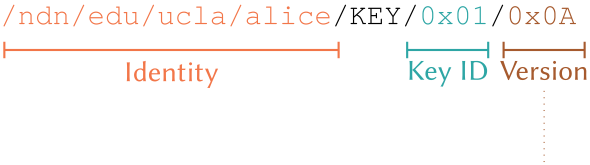
Structure:		Hierarchical
Allocation:		
↪	Granularity:	Subspace
↪	Cardinality:	$1 - n$
↪	Persistence:	Transient
↪	Security:	TA Signature
↪	Delegability:	✓
Governance:		
↪	Scope:	Local
↪	Organization:	Centralized

Public Key Management

Trust Model:		Hierarchical
Key Management:		
↪	Issuance:	Namespace Principal
↪	Distribution:	Owner / cert hosts
↪	Storage:	Owner
↪	Rollover:	✘
↪	Revocation:	Owner

NDN Public Key Management NDN PKM

NDN Technical Report – 2015



/ndn/edu/ucla/alice/KEY/0x01/0x0A

Identity

Key ID

Version

Allows certificate renewals
and multi-signatures

Namespace Management

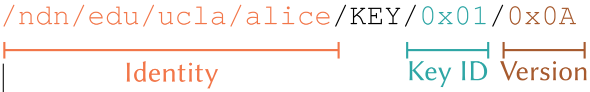
Structure:		Hierarchical
Allocation:		
↪	Granularity:	Subspace
↪	Cardinality:	1 — n
↪	Persistence:	Transient
↪	Security:	TA Signature
↪	Delegability:	✓
Governance:		
↪	Scope:	Local
↪	Organization:	Centralized

Public Key Management

Trust Model:		Hierarchical
Key Management:		
↪	Issuance:	Namespace Principal
↪	Distribution:	Owner / cert hosts
↪	Storage:	Owner
↪	Rollover:	✘
↪	Revocation:	Owner

NDN Public Key Management NDN PKM

NDN Technical Report – 2015



Delegation: Alice signs the key of delegatee, *e.g.*, /ndn/edu/ucla/alice/**c64**

/KEY/<KeyID>/<Version>

Namespace Management

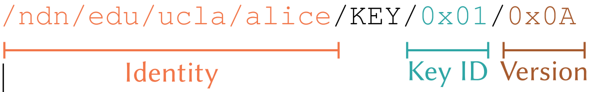
Structure:		Hierarchical
Allocation:		
↪	Granularity:	Subspace
↪	Cardinality:	$1 - n$
↪	Persistence:	Transient
↪	Security:	TA Signature
↪	Delegability:	✓
Governance:		
↪	Scope:	Local
↪	Organization:	Centralized

Public Key Management

Trust Model:		Hierarchical
Key Management:		
↪	Issuance:	Namespace Principal
↪	Distribution:	Owner / cert hosts
↪	Storage:	Owner
↪	Rollover:	✗
↪	Revocation:	Owner

NDN Public Key Management NDN PKM

NDN Technical Report – 2015



/ndn/edu/ucla/alice/KEY/0x01/0x0A

- **Delegation**: Alice signs the key of delegatee, *e.g.*, /ndn/edu/ucla/alice/**c64** /KEY/<KeyID>/<Version>
- **Certificate revocation**: Alice publishes a new packet signed with revoked key, *e.g.*, /ndn/edu/ucla/alice/ /KEY/0x01/0x0A/**REVOKED**

Namespace Management

Structure:		Hierarchical
Allocation:		
↪	Granularity:	Subspace
↪	Cardinality:	1 — *n*
↪	Persistence:	Transient
↪	Security:	TA Signature
↪	Delegability:	✓
Governance:		
↪	Scope:	Local
↪	Organization:	Centralized

Public Key Management

Trust Model:		Hierarchical
Key Management:		
↪	Issuance:	Namespace Principal
↪	Distribution:	Owner / cert hosts
↪	Storage:	Owner
↪	Rollover:	✗
↪	Revocation:	Owner

NDN Public Key Management NDN PKM

NDN Technical Report – 2015

/ndn/edu/ucla/alice/KEY/0x01/0x0A

Identity Key ID Version

- **Delegation**: Alice signs the key of delegatee, *e.g.*, /ndn/edu/ucla/alice/**c64** /KEY/<KeyID>/<Version>
- **Certificate revocation**: Alice publishes a new packet signed with revoked key, *e.g.*, /ndn/edu/ucla/alice/ /KEY/0x01/0x0A/**REVOKED**
- **Signature revocation**: regular signature status, *e.g.*, /ndn/edu/ucla/alice/ /**SigStatus**/<HASH>/<TS>

Namespace Management

Structure:		Hierarchical
Allocation:		
↪	Granularity:	Subspace
↪	Cardinality:	1 — *n*
↪	Persistence:	Transient
↪	Security:	TA Signature
↪	Delegability:	✓
Governance:		
↪	Scope:	Local
↪	Organization:	Centralized

Public Key Management

Trust Model:		Hierarchical
Key Management:		
↪	Issuance:	Namespace Principal
↪	Distribution:	Owner / cert hosts
↪	Storage:	Owner
↪	Rollover:	✘
↪	Revocation:	Owner

NDN Public Key Management NDN PKM

NDN Technical Report – 2015

Challenges:

- Burden of key management is on key owner
- Compromised keys can be used to suppress certificate or signature revocations
- Cumbersome verification (minimum of 3 Additional packages to validate a single NDO)

Namespace Management

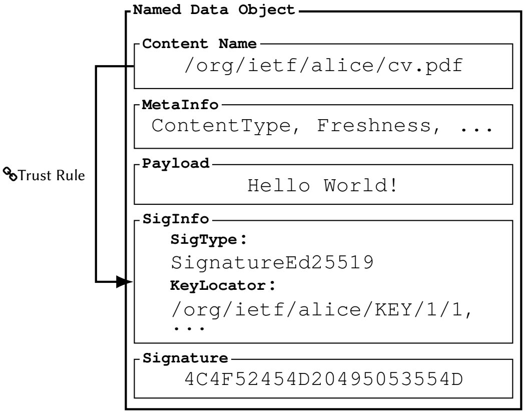
Structure:		Hierarchical
Allocation:		
↪	Granularity:	Subspace
↪	Cardinality:	$1 — n$
↪	Persistence:	Transient
↪	Security:	TA Signature
↪	Delegability:	✓
Governance:		
↪	Scope:	Local
↪	Organization:	Centralized

Public Key Management

Trust Model:		Hierarchical
Key Management:		
↪	Issuance:	Namespace Principal
↪	Distribution:	Owner / cert hosts
↪	Storage:	Owner
↪	Rollover:	✘
↪	Revocation:	Owner

Trust Schema

ACM ICN '15



Named Data Object

Content Name

/org/ietf/alice/cv.pdf

MetaInfo

ContentType, Freshness, ...

Payload

Hello World!

SigInfo

SigType:

SignatureEd25519

KeyLocator:

/org/ietf/alice/KEY/1/1,
...

Signature

4C4F52454D20495053554D

Namespace Management

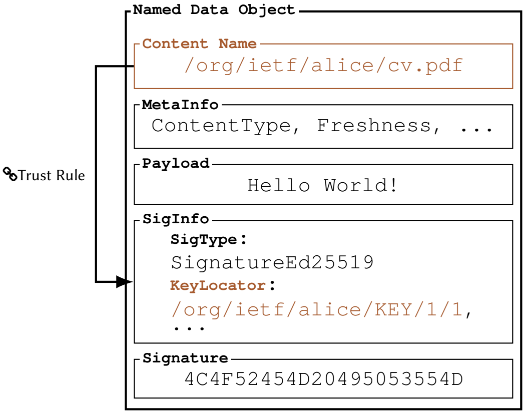
Structure:		Hierarchical
Allocation:		
↪	Granularity:	Arbitrary
↪	Cardinality:	1 — *n*
↪	Persistence:	Permanent
↪	Security:	TA Signature
↪	Delegability:	✘
Governance:		
↪	Scope:	Local
↪	Organization:	Centralized

Public Key Management

Trust Model:		Hierarchical
Key Management:		
↪	Issuance:	Designated CA
↪	Distribution:	Owner
↪	Storage:	Owner
↪	Rollover:	✘
↪	Revocation:	✘

Trust Schema

ACM ICN '15



Namespace Management

Structure:		Hierarchical
Allocation:		
↪	Granularity:	Arbitrary
↪	Cardinality:	1 — n
↪	Persistence:	Permanent
↪	Security:	TA Signature
↪	Delegability:	✘
Governance:		
↪	Scope:	Local
↪	Organization:	Centralized

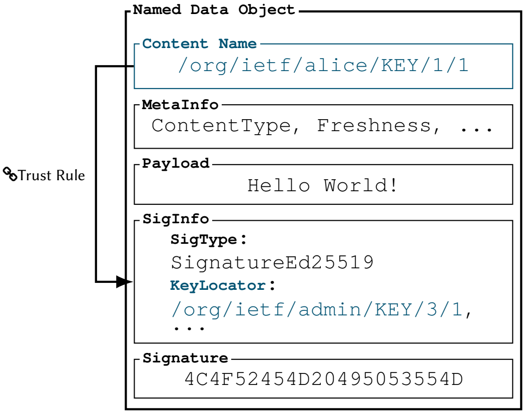
Public Key Management

Trust Model:		Hierarchical
Key Management:		
↪	Issuance:	Designated CA
↪	Distribution:	Owner
↪	Storage:	Owner
↪	Rollover:	✘
↪	Revocation:	✘

`<org><ietf>[user]<>` → `<org><ietf>[user]<KEY>`

Trust Schema

ACM ICN '15



Named Data Object

Content Name
/org/ietf/alice/KEY/1/1

MetaInfo
ContentType, Freshness, ...

Payload
Hello World!

SigInfo
SigType:
SignatureEd25519
KeyLocator:
/org/ietf/admin/KEY/3/1,
...

Signature
4C4F52454D20495053554D

Namespace Management

Structure:		Hierarchical
Allocation:		
↪	Granularity:	Arbitrary
↪	Cardinality:	1 — *n*
↪	Persistence:	Permanent
↪	Security:	TA Signature
↪	Delegability:	✗
Governance:		
↪	Scope:	Local
↪	Organization:	Centralized

Public Key Management

Trust Model:		Hierarchical
Key Management:		
↪	Issuance:	Designated CA
↪	Distribution:	Owner
↪	Storage:	Owner
↪	Rollover:	✗
↪	Revocation:	✗

```
<org><ietf>[user]<KEY> → <org><ietf><admin><KEY>
<org><ietf>[user]<KEY> → <org><ietf><ndnmaster><KEY>
```

Trust Schema

ACM ICN '15

Challenges:

- Key Revocation is not explicitly defined
- No a priori known authentication paths can be used for availability attacks
- No possibility of delegation
- No synchronization between data and corresponding trust schema

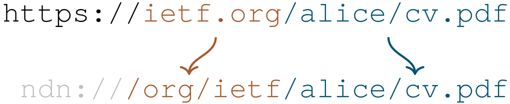
Namespace Management

Structure:		Hierarchical
Allocation:		
↪	Granularity:	Arbitrary
↪	Cardinality:	1 — n
↪	Persistence:	Permanent
↪	Security:	TA Signature
↪	Delegability:	✘
Governance:		
↪	Scope:	Local
↪	Organization:	Centralized

Public Key Management

Trust Model:		Hierarchical
Key Management:		
↪	Issuance:	Designated CA
↪	Distribution:	Owner
↪	Storage:	Owner
↪	Rollover:	✘
↪	Revocation:	✘

NDNSSEC



Namespace Management

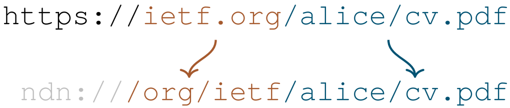
Structure:		Hierarchical
Allocation:		
↪	Granularity:	Subspace
↪	Cardinality:	1 — n
↪	Persistence:	Transient
↪	Security:	DNSSEC PKI
↪	Delegability:	✓
Governance:		
↪	Scope:	Global
↪	Organization:	Centralized

Public Key Management

Trust Model:		Hierarchical
Key Management:		
↪	Issuance:	DNS Zone owner
↪	Distribution:	Owner / DNS
↪	Storage:	Owner
↪	Rollover:	✓
↪	Revocation:	Issuer

NDNSSEC

ACM ICN ’19



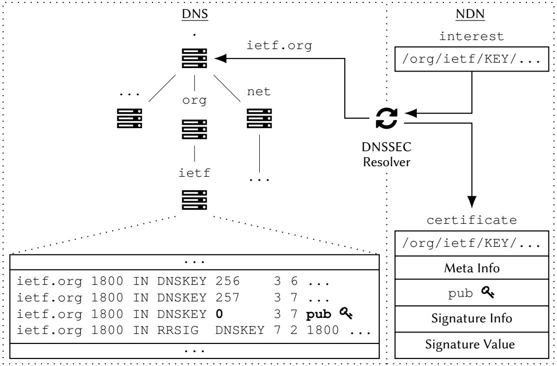
Use DNS(SEC) for both namespace and public key management

Namespace Management		
Structure:		Hierarchical
Allocation:		
↪	Granularity:	Subspace
↪	Cardinality:	1 — *n*
↪	Persistence:	Transient
↪	Security:	DNSSEC PKI
↪	Delegability:	✓
Governance:		
↪	Scope:	Global
↪	Organization:	Centralized

Public Key Management		
Trust Model:		Hierarchical
Key Management:		
↪	Issuance:	DNS Zone owner
↪	Distribution:	Owner / DNS
↪	Storage:	Owner
↪	Rollover:	✓
↪	Revocation:	Issuer

NDNSSEC

ACM ICN '19



```
                          ...
ietf.org 1800 IN DNSKEY 256    3 6 ...
ietf.org 1800 IN DNSKEY 257    3 7 ...
ietf.org 1800 IN DNSKEY 0      3 7 pub
ietf.org 1800 IN RRSIG  DNSKEY 7 2 1800 ...
                          ...
```

Namespace Management

Structure:		Hierarchical
Allocation:		
↪	Granularity:	Subspace
↪	Cardinality:	1 — *n*
↪	Persistence:	Transient
↪	Security:	DNSSEC PKI
↪	Delegability:	✓
Governance:		
↪	Scope:	Global
↪	Organization:	Centralized

Public Key Management

Trust Model:		Hierarchical
Key Management:		
↪	Issuance:	DNS Zone owner
↪	Distribution:	Owner / DNS
↪	Storage:	Owner
↪	Rollover:	✓
↪	Revocation:	Issuer

NDNSSEC

Challenges:

- Complex maintenance of trust chains
- Poor scalability performance (all keys are fetched and validated at once)
- Reliance on DNS transport

Namespace Management

Structure:		Hierarchical
Allocation:		
↪	Granularity:	Subspace
↪	Cardinality:	1 — *n*
↪	Persistence:	Transient
↪	Security:	DNSSEC PKI
↪	Delegability:	✓
Governance:		
↪	Scope:	Global
↪	Organization:	Centralized

Public Key Management

Trust Model:		Hierarchical
Key Management:		
↪	Issuance:	DNS Zone owner
↪	Distribution:	Owner / DNS
↪	Storage:	Owner
↪	Rollover:	✓
↪	Revocation:	Issuer

Identity-based Trust

IBC: IEEE ICNP ’11 / HIBC: IEEE WETICE ’17

Private Key Generator

Namespace Management

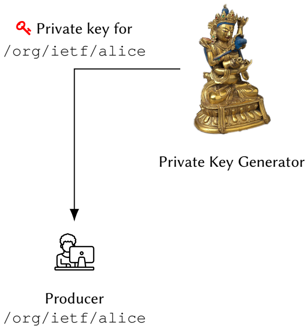
Structure:		Hierarchical
Allocation:		
↪	Granularity:	Subspace
↪	Cardinality:	1 — 1
↪	Persistence:	Permanent
↪	Security:	PKG Signature
↪	Delegability:	✗
Governance:		
↪	Scope:	Local
↪	Organization:	Centralized

Public Key Management

Trust Model:		Basic / Hierarchical
Key Management:		
↪	Issuance:	PKG
↪	Distribution:	NA
↪	Storage:	Owner / PKG
↪	Rollover:	✗
↪	Revocation:	✗

Identity-based Trust

IBC: IEEE ICNP ’11 / HIBC: IEEE WETICE ’17



Namespace Management

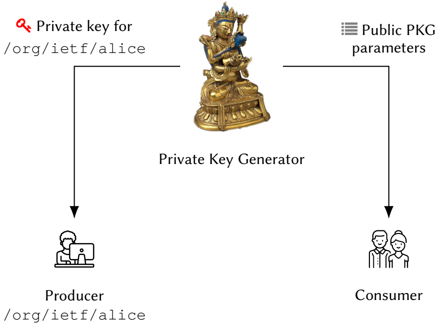
Structure:		Hierarchical
Allocation:		
↪	Granularity:	Subspace
↪	Cardinality:	1 — 1
↪	Persistence:	Permanent
↪	Security:	PKG Signature
↪	Delegability:	✘
Governance:		
↪	Scope:	Local
↪	Organization:	Centralized

Public Key Management

Trust Model:		Basic / Hierarchical
Key Management:		
↪	Issuance:	PKG
↪	Distribution:	NA
↪	Storage:	Owner / PKG
↪	Rollover:	✘
↪	Revocation:	✘

Identity-based Trust

IBC: IEEE ICNP ’11 / HIBC: IEEE WETICE ’17



🔑 Private key for /org/ietf/alice

Private Key Generator

☰ Public PKG parameters

Producer /org/ietf/alice

Consumer

Namespace Management

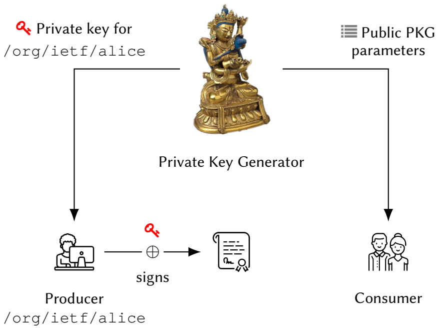
Structure:		Hierarchical
Allocation:		
↪	Granularity:	Subspace
↪	Cardinality:	1 — 1
↪	Persistence:	Permanent
↪	Security:	PKG Signature
↪	Delegability:	✗
Governance:		
↪	Scope:	Local
↪	Organization:	Centralized

Public Key Management

Trust Model:		Basic / Hierarchical
Key Management:		
↪	Issuance:	PKG
↪	Distribution:	NA
↪	Storage:	Owner / PKG
↪	Rollover:	✗
↪	Revocation:	✗

Identity-based Trust

IBC: IEEE ICNP ’11 / HIBC: IEEE WETICE ’17



Private key for /org/ietf/alice

Public PKG parameters

Private Key Generator

signs

Producer /org/ietf/alice

Consumer

Namespace Management

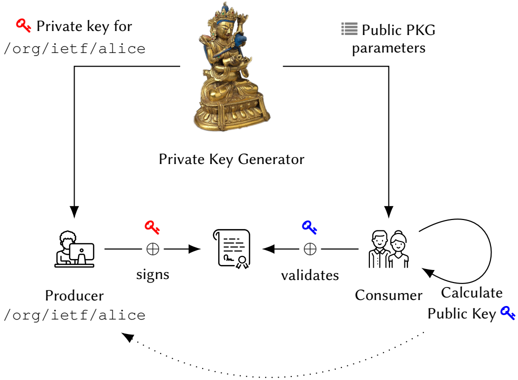
Structure:		Hierarchical
Allocation:		
↪	Granularity:	Subspace
↪	Cardinality:	1 — 1
↪	Persistence:	Permanent
↪	Security:	PKG Signature
↪	Delegability:	✘
Governance:		
↪	Scope:	Local
↪	Organization:	Centralized

Public Key Management

Trust Model:		Basic / Hierarchical
Key Management:		
↪	Issuance:	PKG
↪	Distribution:	NA
↪	Storage:	Owner / PKG
↪	Rollover:	✘
↪	Revocation:	✘

Identity-based Trust

IBC: IEEE ICNP ’11 / HIBC: IEEE WETICE ’17



Namespace Management

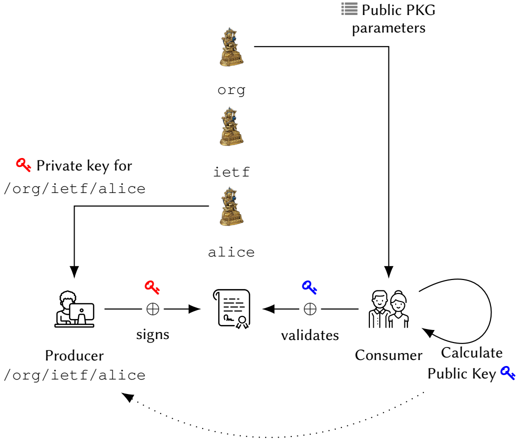
Structure:		Hierarchical
Allocation:		
↪	Granularity:	Subspace
↪	Cardinality:	1 — 1
↪	Persistence:	Permanent
↪	Security:	PKG Signature
↪	Delegability:	✘
Governance:		
↪	Scope:	Local
↪	Organization:	Centralized

Public Key Management

Trust Model:		Basic / Hierarchical
Key Management:		
↪	Issuance:	PKG
↪	Distribution:	NA
↪	Storage:	Owner / PKG
↪	Rollover:	✘
↪	Revocation:	✘

Identity-based Trust

IBC: IEEE ICNP ’11 / HIBC: IEEE WETICE ’17



Namespace Management

Structure:		Hierarchical
Allocation:		
↪	Granularity:	Subspace
↪	Cardinality:	1 — 1
↪	Persistence:	Permanent
↪	Security:	PKG Signature
↪	Delegability:	✘
Governance:		
↪	Scope:	Local
↪	Organization:	Centralized

Public Key Management

Trust Model:		Basic / Hierarchical
Key Management:		
↪	Issuance:	PKG
↪	Distribution:	NA
↪	Storage:	Owner / PKG
↪	Rollover:	✘
↪	Revocation:	✘

Identity-based Trust

IBC: IEEE ICNP '11 / HIBC: IEEE WETICE '17

Challenges:

- Private keys are known to PKG (key escrow)
- Lack of namespace delegability
- Poor scalability performance
- Revoking a key equals to revoking an identity and respective data

Namespace Management

Structure:		Hierarchical
Allocation:		
↪	Granularity:	Subspace
↪	Cardinality:	1 — 1
↪	Persistence:	Permanent
↪	Security:	PKG Signature
↪	Delegability:	✘
Governance:		
↪	Scope:	Local
↪	Organization:	Centralized

Public Key Management

Trust Model:		Basic / Hierarchical
Key Management:		
↪	Issuance:	PKG
↪	Distribution:	NA
↪	Storage:	Owner / PKG
↪	Rollover:	✘
↪	Revocation:	✘

Conclusion

Namespace Management

- Application-level names are used at the network layer
- Current proposals focus on locally unique names
- Internet-wide names will consists of two parts, one that requires global and one that requires application-level management
- Security is based on custom PKIs

Public Key Management

- Bootstrapping procedures and renewal and revocation schema are open problems

Conclusion

Namespace Management

- Application-level names are used at the network layer
- Current proposals focus on locally unique names
- Internet-wide names will consists of two parts, one that requires global and one that requires application-level management
- Security is based on custom PKIs

Public Key Management

- Bootstrapping procedures and renewal and revocation schema are open problems

Question, critique, cooperation? `pft@acm.org`