TELEFONBESKED

Til: Nutiden

Fra: 1982

Adresse / att. Alle sysadmins

Telefon nr. Lokal:

Ringes op ☐ Ringer igen ☒ Ønsker fax ☒ Besøges ☐

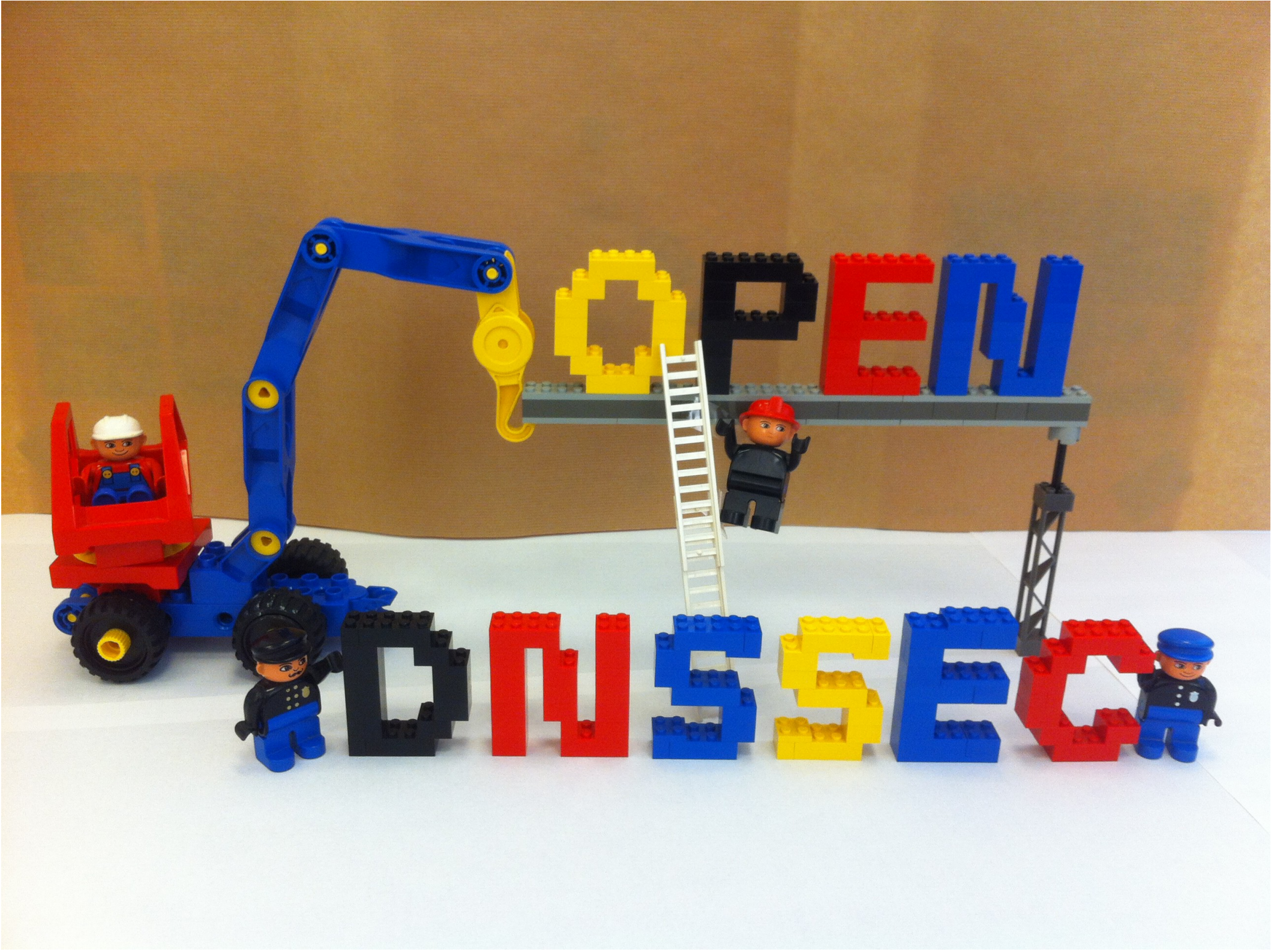
Angående: 1982 kalder:

De vil gerne have deres usikre DNS tilbage!

Modtaget den / kl.

Af

JENSEN 2225


OPEN
DNSSEC

Agenda

- Who are we etc.
- DNS
- DNSSEC
- Bind and DNSSEC
- OpenDNSSEC
- Other fun stuff


Who are we?
Martin Toft
• Education: M.Sc. (Computer Science)
• Work: Netic
• Spare time: dotsrc.org, Grumpy BSD-fanatic
Georg Sluyterman
• Education: M.S.E. (Electronic & IT)
• Work: Netic
• Spare time:
dotsrc.org, HAL9k, Grumpy AFS & IPv6 fanatic


Franziskaner
Weissbier
NATURTRÜB
Staropramen
PREMIUM BEER
PRAGUE
#1 BEER
Kronenbourg
1664
Hoegaarden
ORIGINAL BELGIAN WHEAT BEER
WIT - BLANCHE
STELLA ARTOIS
Premium Lager Beer
Power
Error
Net
Disk
netic

Netic

- IT-konsulent og -hostingvirksomhed i Aalborg
  - Specialiserede hostingydelser i egne datacentre el. hos kunden
  - Udvikling af egne produkter el. opgaver for kunder
  - Fokus på kvalitet
  - Vi bruger i høj grad open source software, f.eks. Linux & FreeBSD
  - 16 ansatte, medarbejderejet
  - Godt socialt samværd og dygtige kollegaer
  - Kunder spænder over alt fra ISP'er og IT-virksomheder over private firmaer til offentlige institutioner

Netic

Eksempler

- Fælles Medicinkort
- Sundhedsdatanettet
- Debitor Registret
- National Sundheds Platform
- Splunk-partner

Eksempler på egne produkter

- Netic Hotspot Solution
- TidyDNS

DNS, DNSSEC, ...

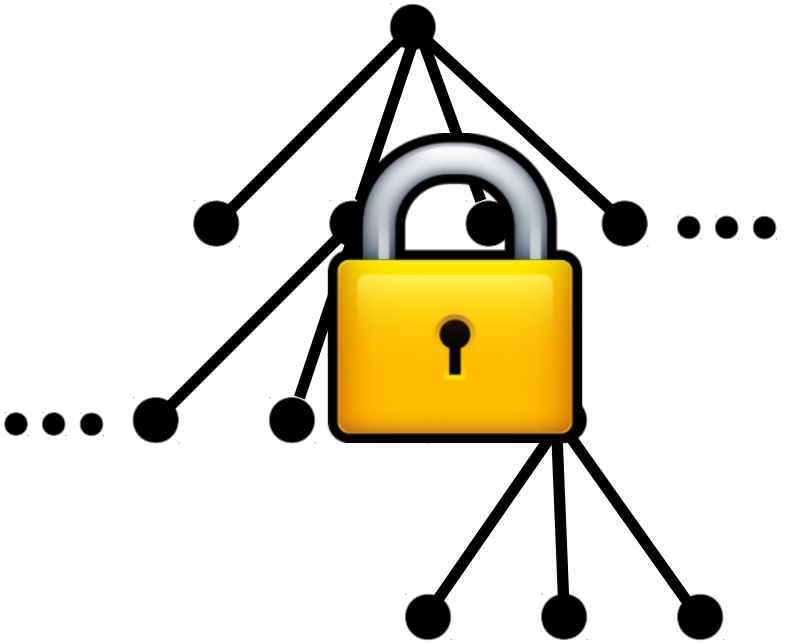
- Overblik over folks erfaringer
- DNS
- DNSSEC
- OpenDNSSEC

Motivation

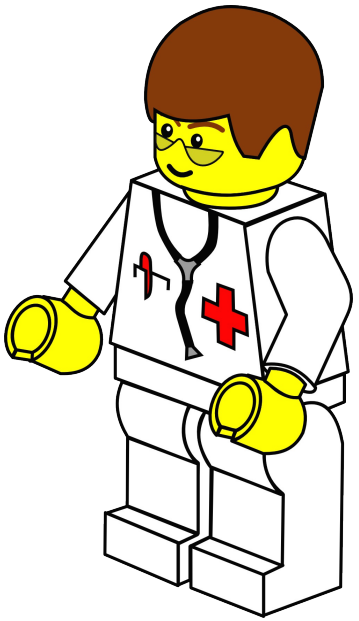
- Kaminsky
- Klip med Phil Regnaults ;-)
- Ny teknologi!
- Nye muligheder

DNSSEC

- Agenda:
  - DNS primer
  - Cryptography primer
  - DNSSEC
    - Overview
    - Ressource records
    - Chain of trust
    - Header flags and bits
    - Maintenance



DNS primer



- Domain Name System
- Invented in 1982 to replace hosts files
- Two namespaces:
  - Domain name hierarchy
  - IP address space
- No need to remember 195.215.30.182 – just use ”thecamp.dk”
- Reverse:

```
$ dig 182.30.215.195.in-addr.arpa ptr +short
cat5.thecamp.dk.
```

DNS primer

- Ressource records
  (Name, Type, Class, TTL, RDLength, RData)
- Name is the domain name, e.g. thecamp.dk
- Types: A, AAAA, CNAME, MX, SOA, NS, TXT, SPF, PTR, etc.
- Classes: Only IN (for Internet) is relevant :-)
- Time To Live (TTL): How long to cache it
- RDLength is the length of RData
- RData is the actual ”value” of the record

DNS primer

```
$ORIGIN pinkponies.net.
$TTL 3600
@          IN SOA   a.authns.evul-isp.br hostmaster.evul-isp.br. (
                    2012061801 ; serial
                    86400      ; refresh (1 day)
                    7200       ; retry   (2 hours)
                    3600000    ; expire  (1000 hours)
                    172800 )   ; minimum (2 days)
           IN NS    a.authns.evul-isp.br.
           IN NS    b.authns.evul-isp.br.
           IN A     46.163.113.176
           IN MX    10 a.mail.evul-isp.br.
           IN MX    20 b.mail.evul-isp.br.
www        IN A     46.163.113.176
forum      IN CNAME www
localhost  IN A     127.0.0.1
```

DNS primer

```
$ dig pinkponies.net ns +short
a.authns.evul-isp.br.
b.authns.evul-isp.br.
```

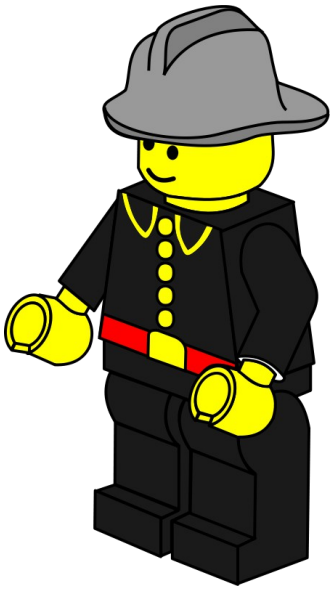
```
$ORIGIN pinkponies.net.
$TTL 3600
@           IN NS    a.authns.evul-isp.br.
            IN NS    b.authns.evul-isp.br.
            IN A     46.163.113.176
            IN MX    10 a.mail.evul-isp.br.
            IN MX    20 b.mail.evul-isp.br.
www         IN A     46.163.113.176
forum       IN CNAME www
localhost   IN A     127.0.0.1
```

DNS primer

```
$ORIGIN pinkponies.net.
$TTL 3600
@         IN SOA   a.authns.evul-isp.br hostmaster.evul-isp.br. (
                   2012061801 ; serial
                   86400      ; refresh (1 day)
                   7200       ; retry   (2 hours)
```

```
$ dig forum.pinkponies.net cname +short
www.pinkponies.net.
$ dig www.pinkponies.net a +short
46.163.113.176
```

```
www       IN A     46.163.113.176
forum     IN CNAME www
localhost IN A     127.0.0.1
```



DNS primer

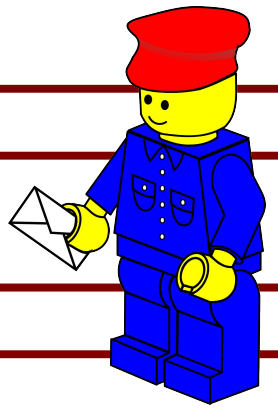
```
$ORIGIN pinkponies.net.
$TTL 3600
@         IN SOA   a.authns.evul-isp.br hostmaster.evul-isp.br. (
                   2012061801 ; serial
                   86400      ; refresh (1 day)
                   7200       ; retry   (2 hours)
                   3600000    ; expire  (1000 hours)
                   172800 )   ; minimum (2 days)

www
forum     IN CNAME www
localhost IN A     127.0.0.1
```

```
$ dig pinkponies.net soa +short
a.authns.evul-isp.br.  hostmaster.evul-isp.br.
2012061801 86400 7200 3600000 172800
```

DNS primer

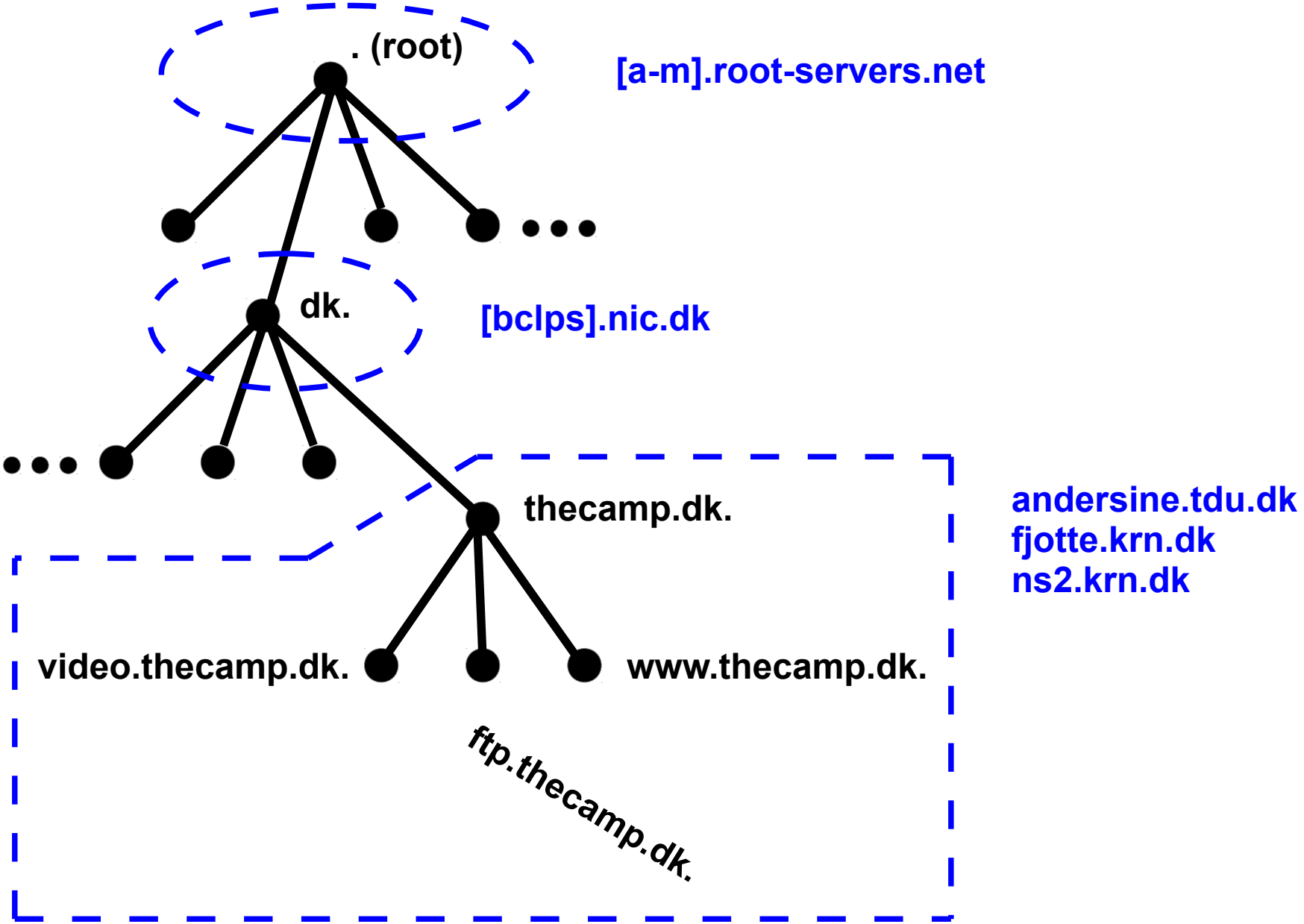
```
$ORIGIN pinkponies.net.
$TTL 3600
```

@	IN	SOA	a.authns.evul-isp.br hostmaster.evul-isp.br. (
			2012061801 ; serial
			86400 ; refresh (1 day)
			7200 ; retry (2 hours)
			3600000 ; expire (1000 hours)
			172800) ; minimum (2 days)
	IN	NS	a.authns.evul-isp.br.
	IN	NS	b.authns.evul-isp.br.
	IN	A	46.163.113.176
	IN	MX	10 a.mail.evul-isp.br.
	IN	MX	20 b.mail.evul-isp.br.
www	IN	A	46.163.113.176
forum	IN	CNAME	www
localhost	IN	A	127.0.0.1



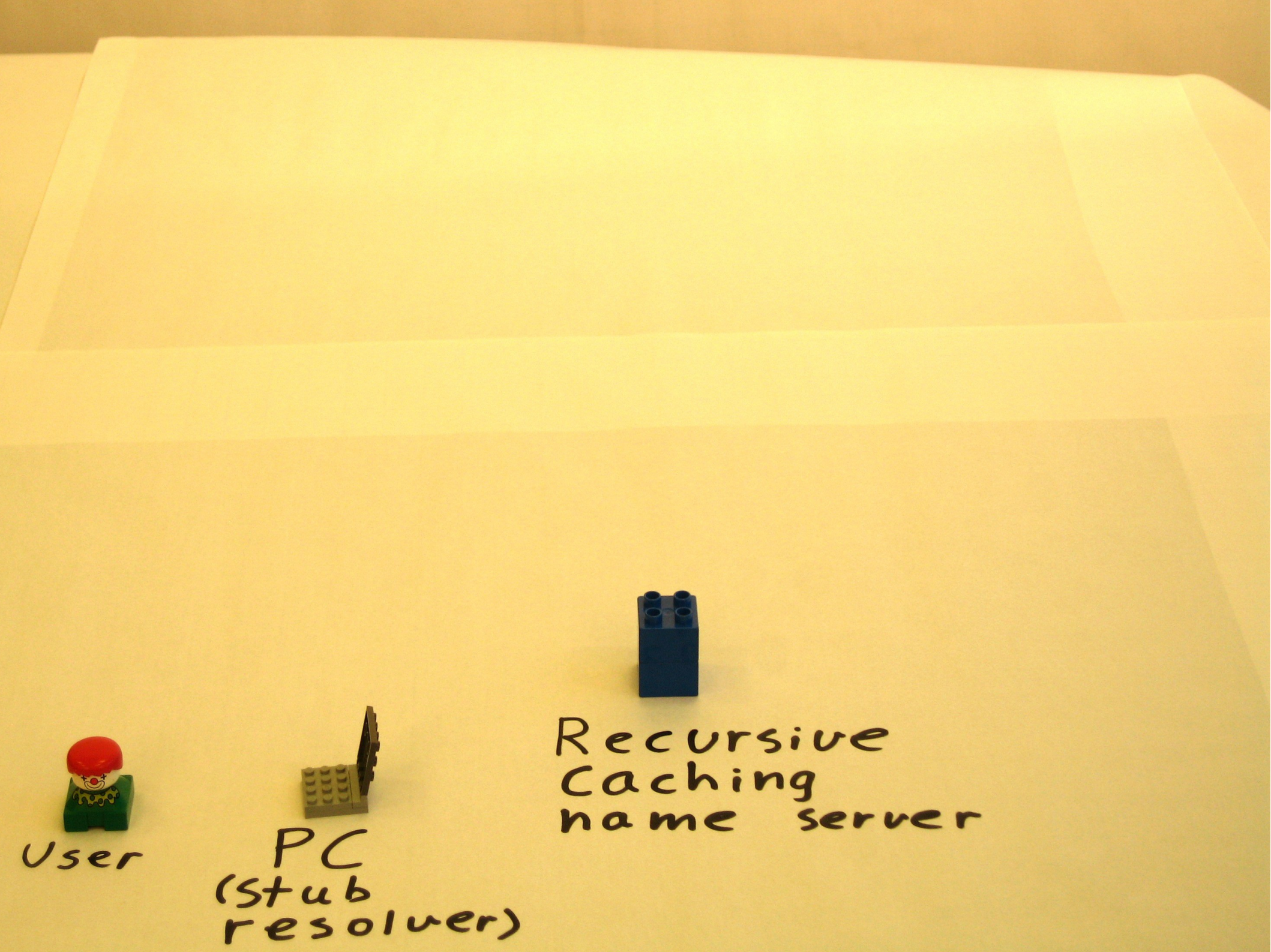
Ressource record sets

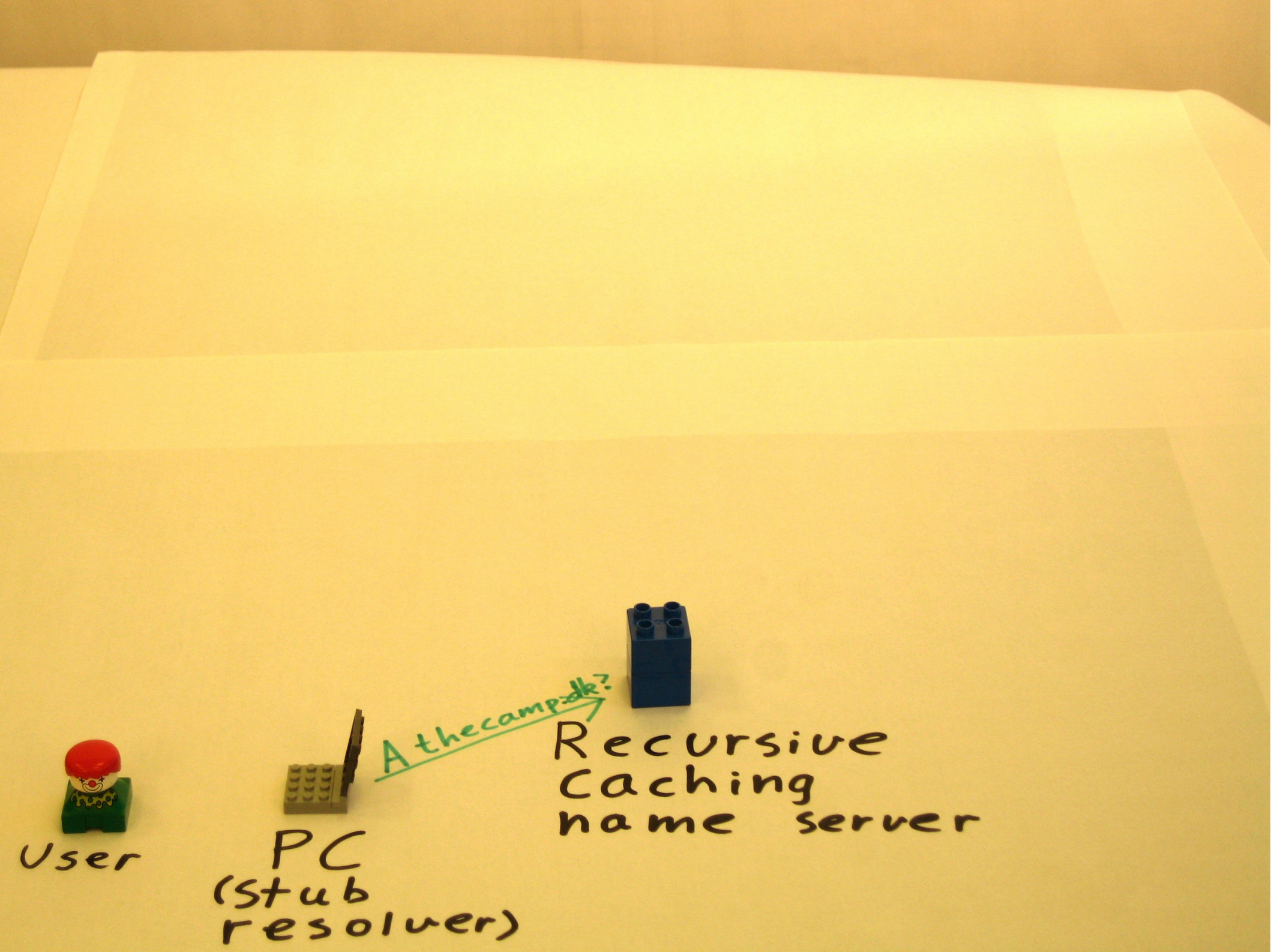
DNS primer

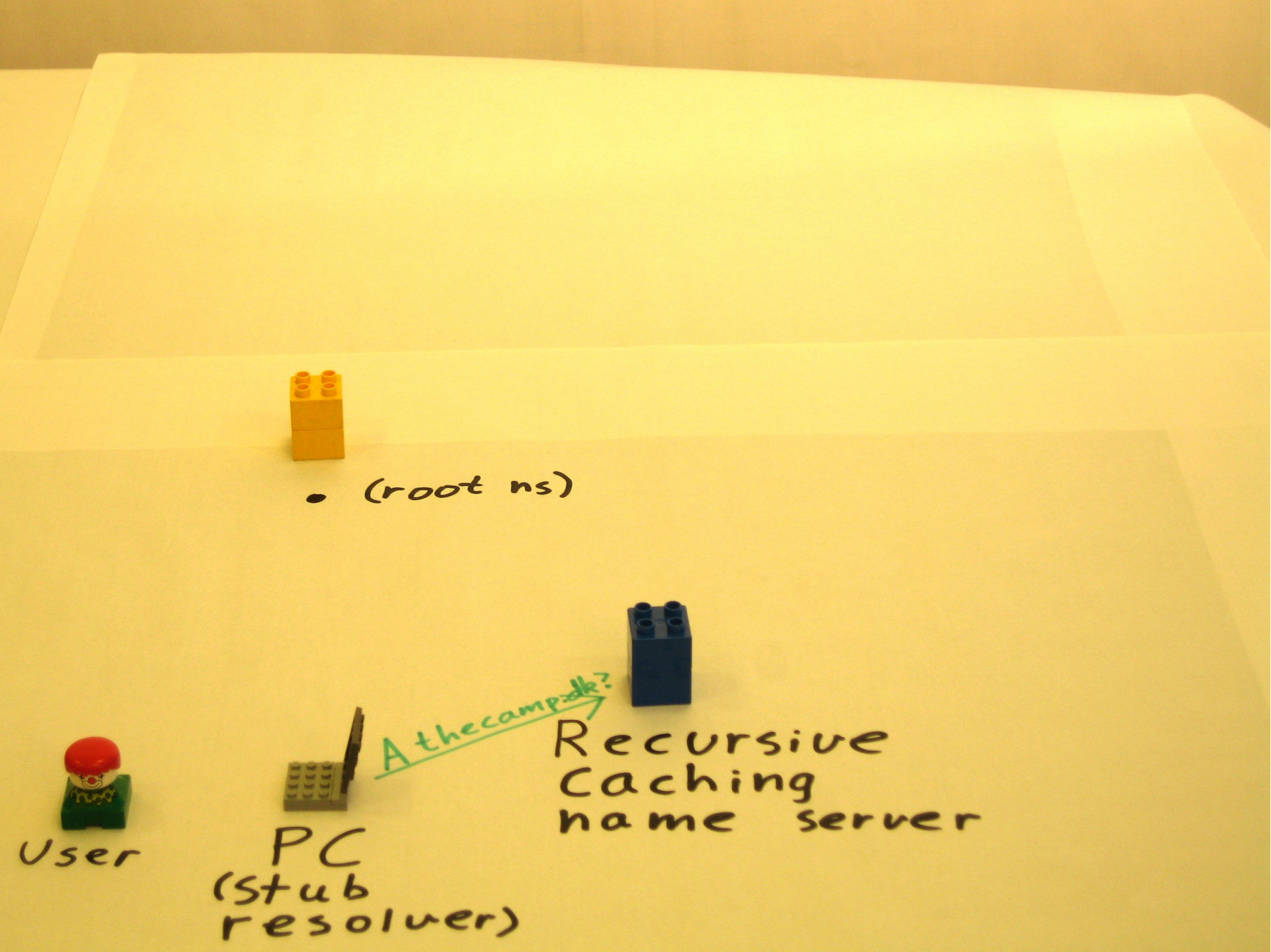

. (root)
[a-m].root-servers.net
dk.
[bclps].nic.dk
thecamp.dk.
andersine.tdu.dk
fjotte.krn.dk
ns2.krn.dk
video.thecamp.dk.
www.thecamp.dk.
ftp.thecamp.dk.

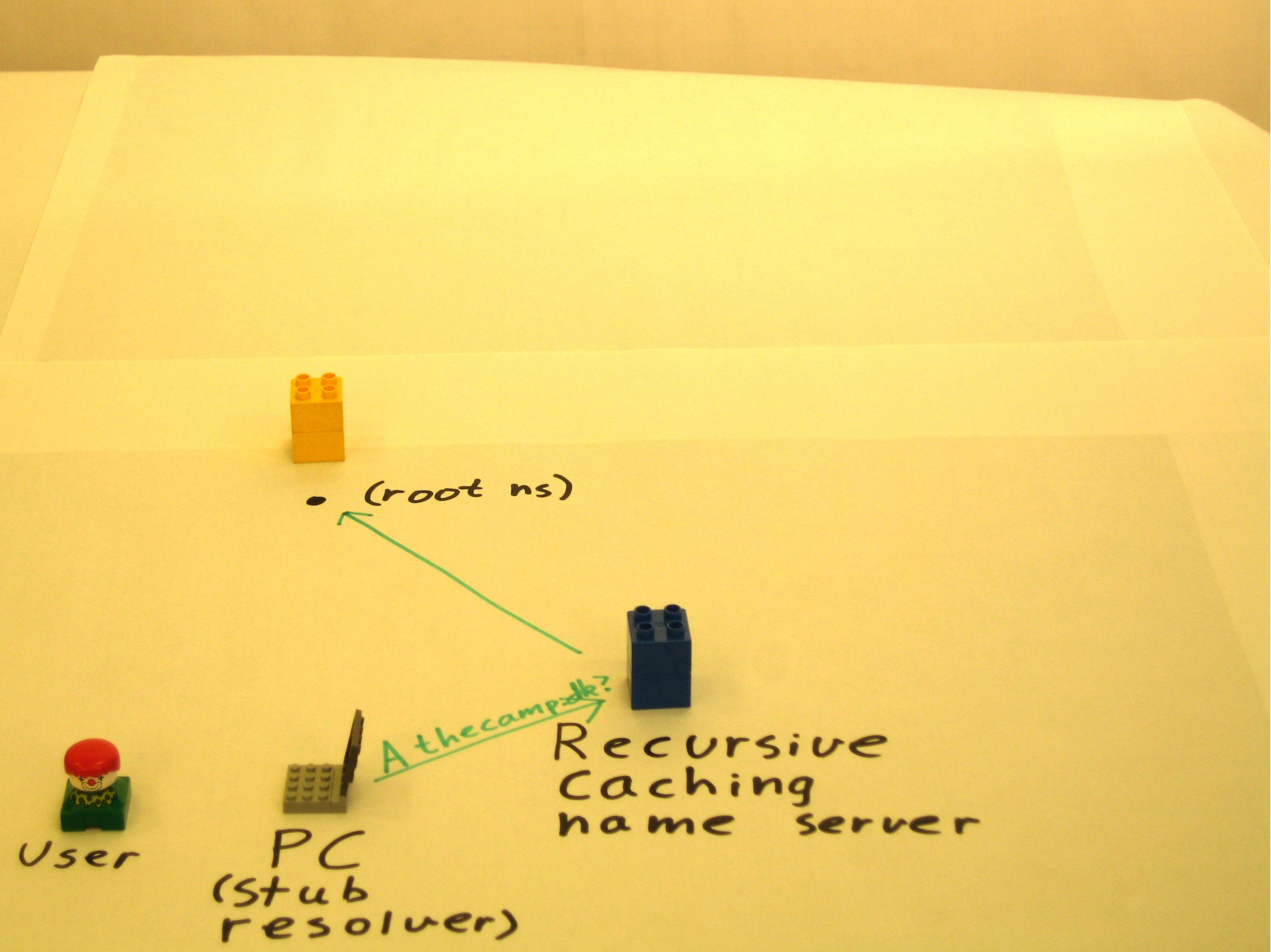

User

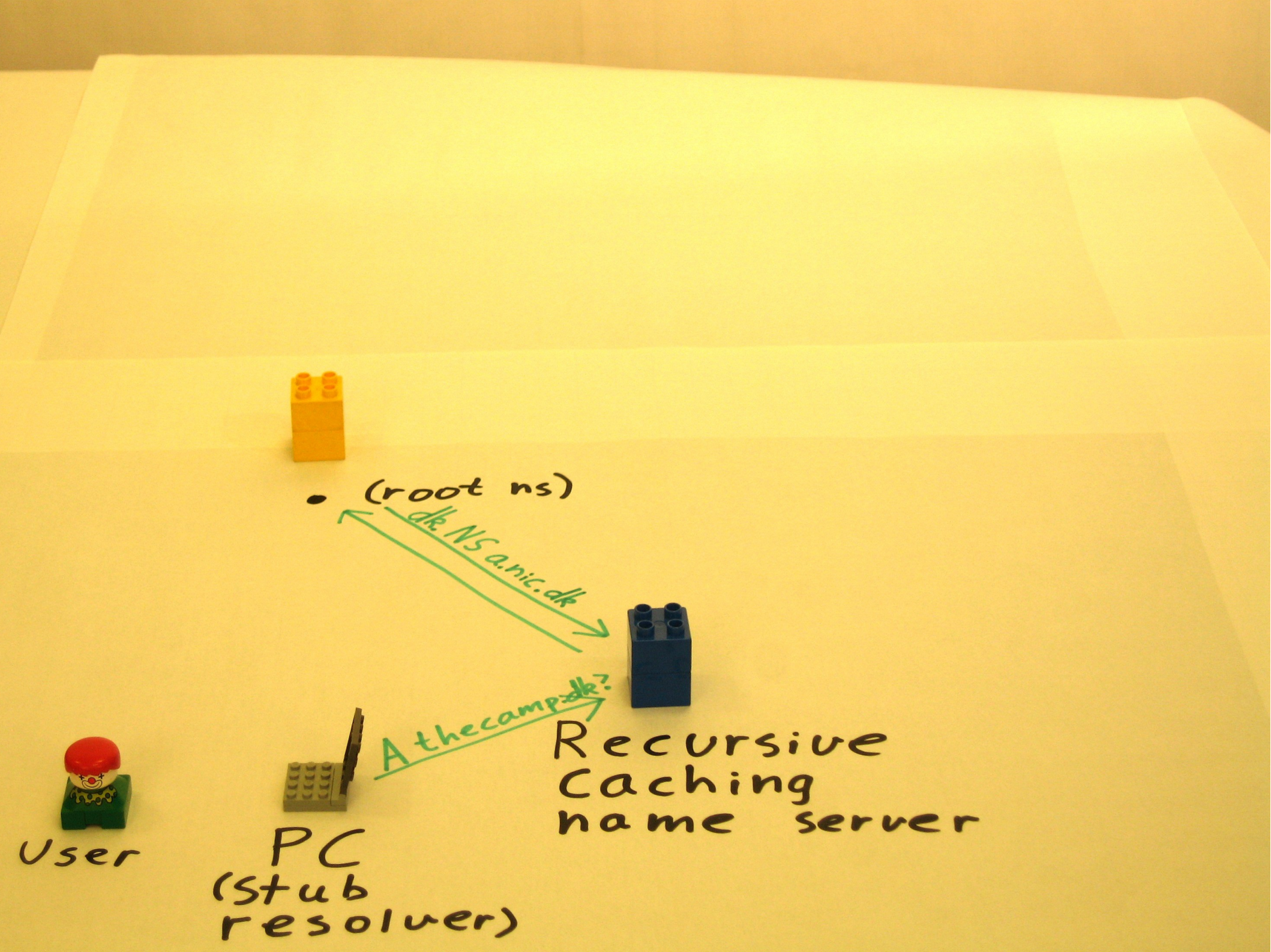

User
PC
(Stub
resolver)

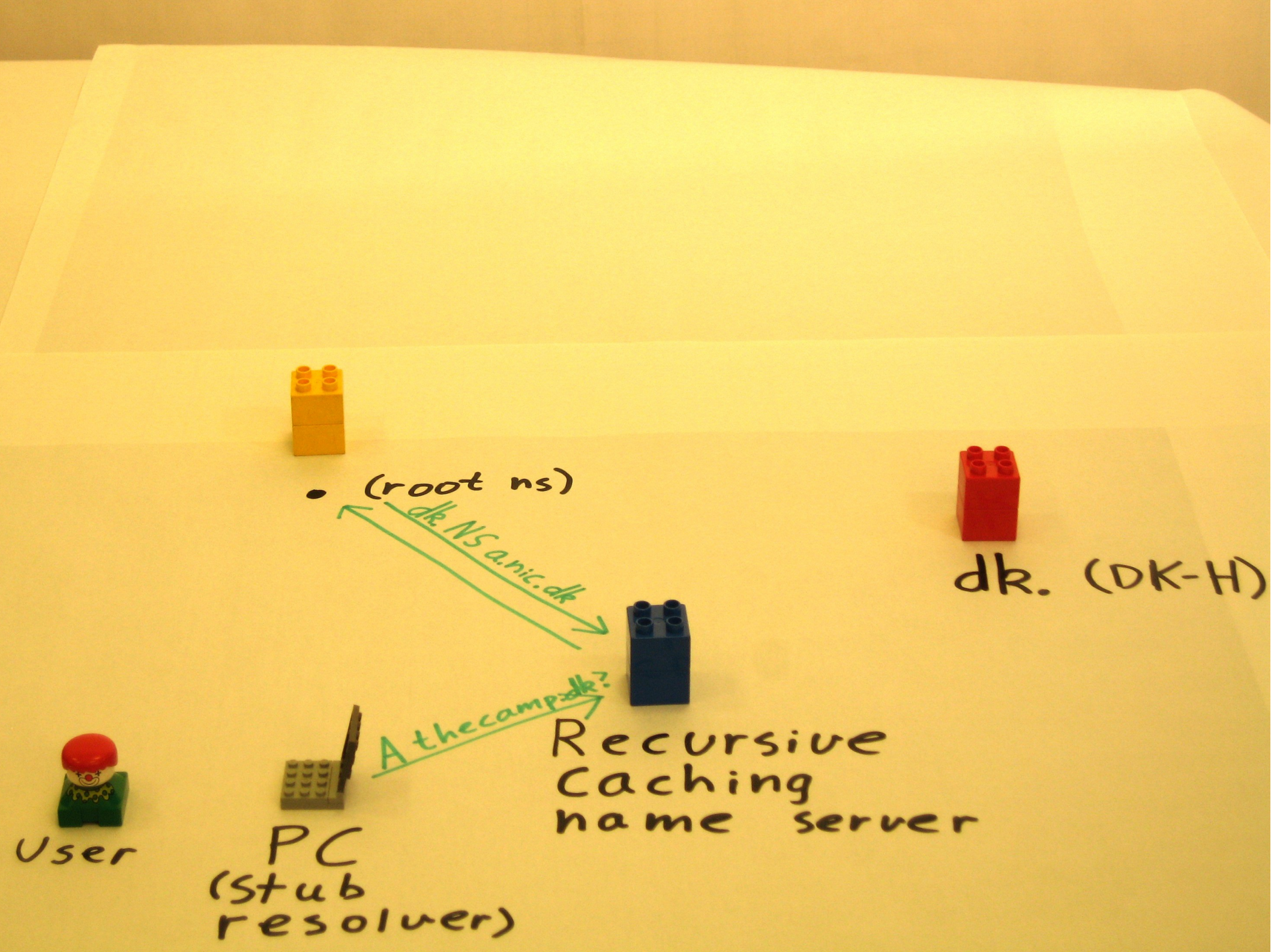

User
PC
(Stub
resolver)
Recursive
Caching
name server

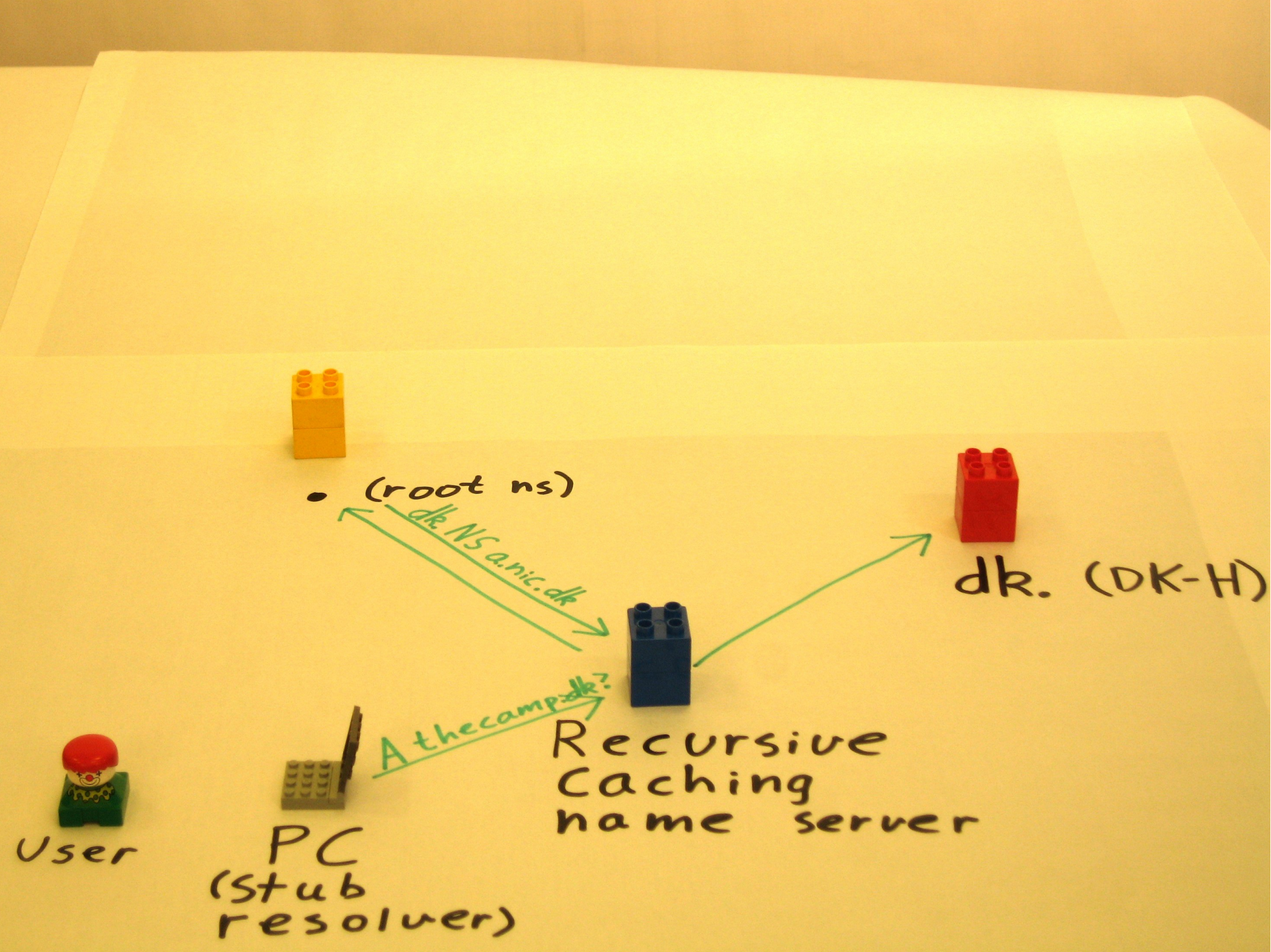

A thecamp.dk?
Recursive
Caching
name server
User
PC
(Stub
resolver)

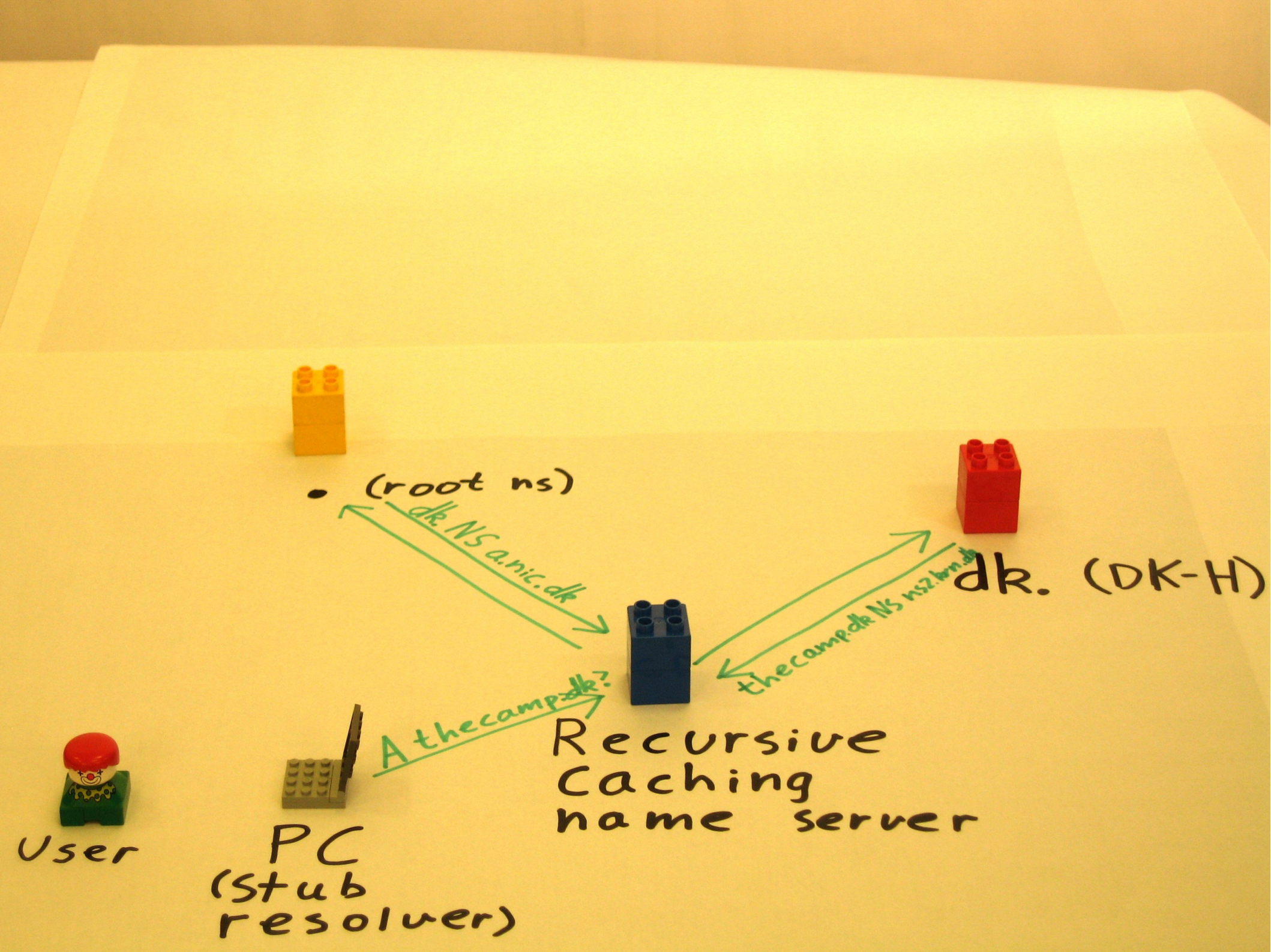

. (root ns)
A thecamp.dk?
Recursive
Caching
name server
User
PC
(Stub
resolver)

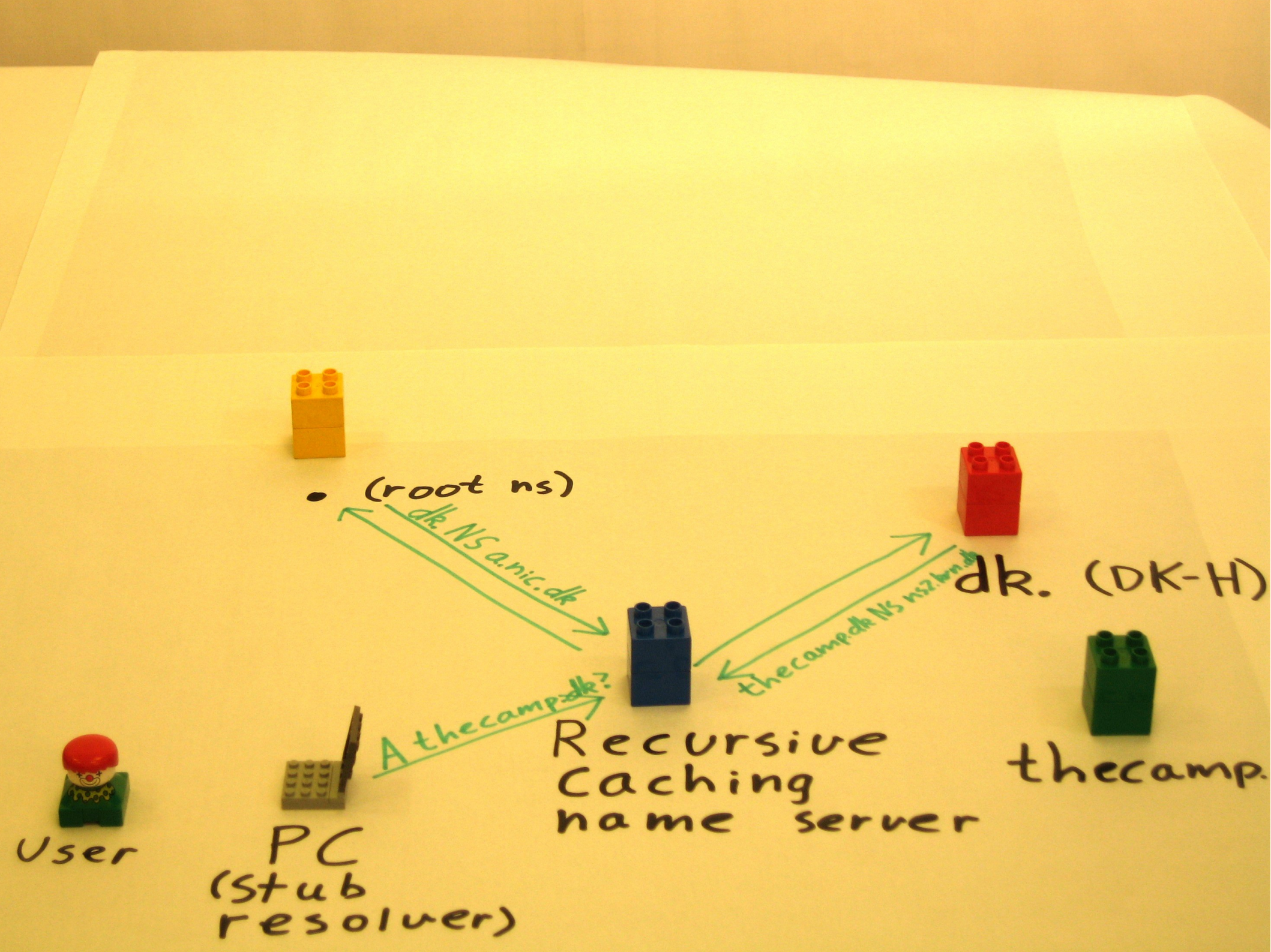

. (root ns)
A thecamp.dk?
Recursive
Caching
name server
User
PC
(Stub
resolver)

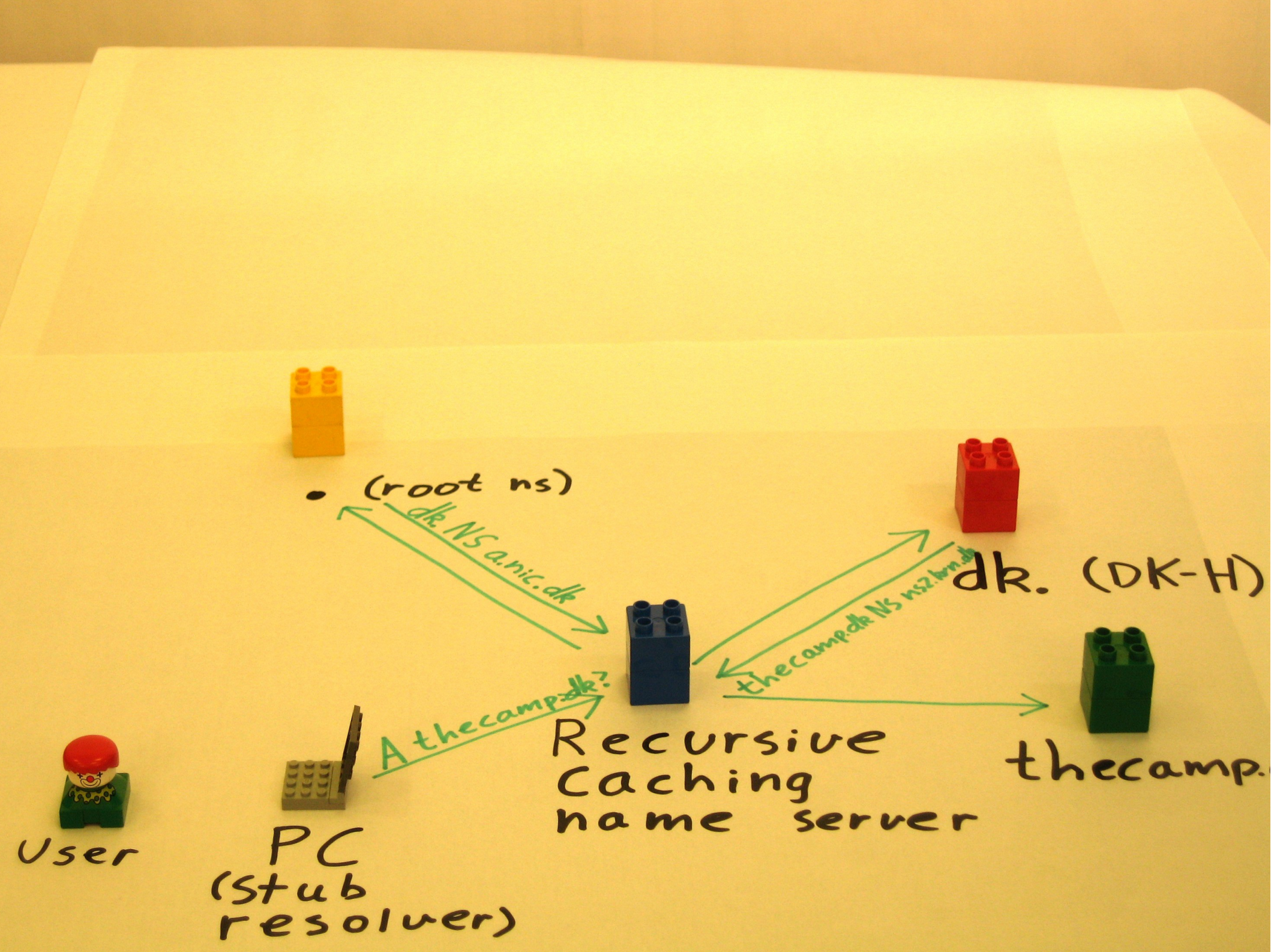

. (root ns)
dk. NS a.nic.dk
A thecamp.dk?
Recursive
Caching
name server
User
PC
(Stub
resolver)

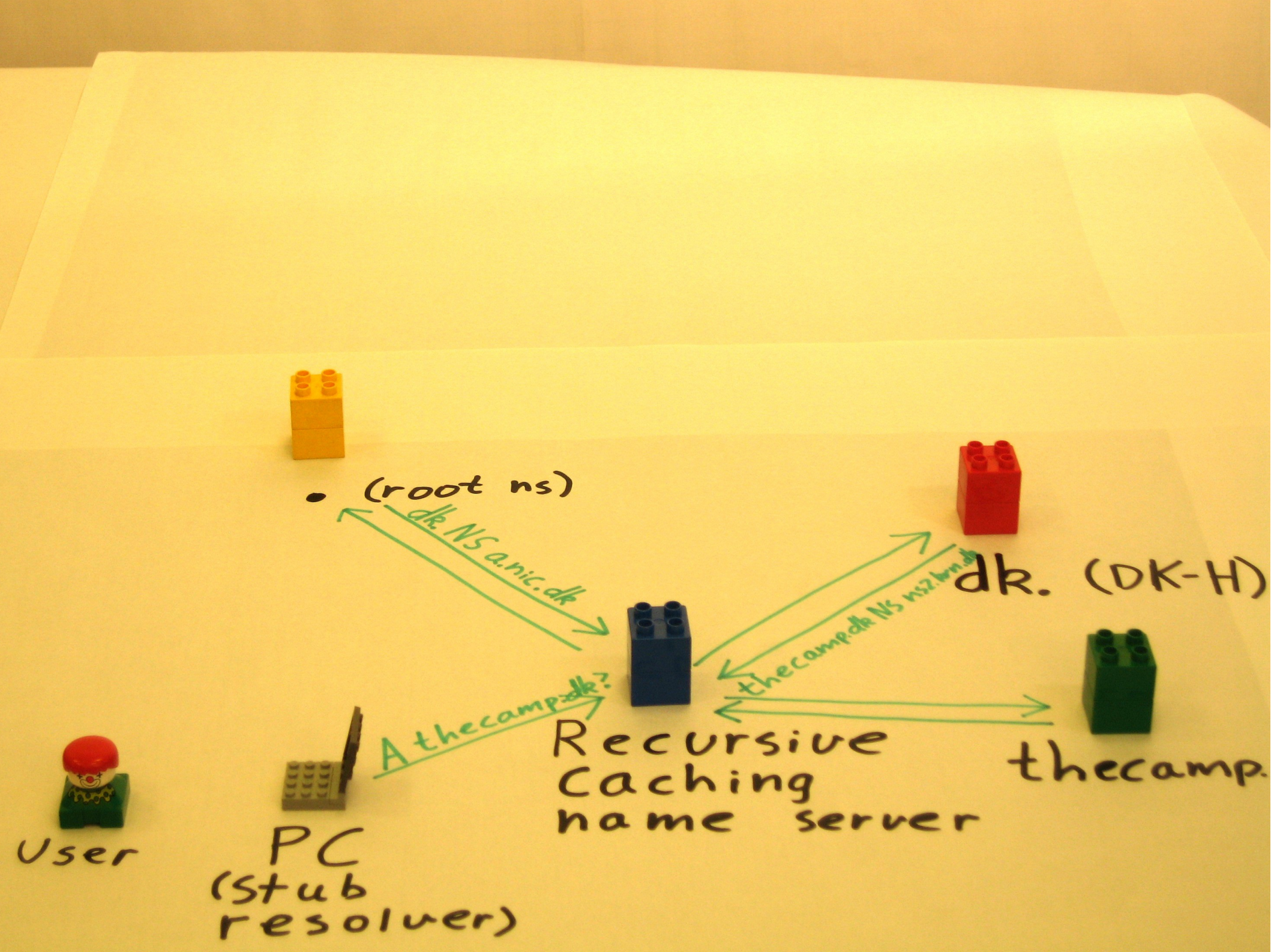

. (root ns)
dk NS a.nic.dk
dk. (DK-H)
A thecamp.dk?
Recursive
Caching
name server
User
PC
(Stub
resolver)

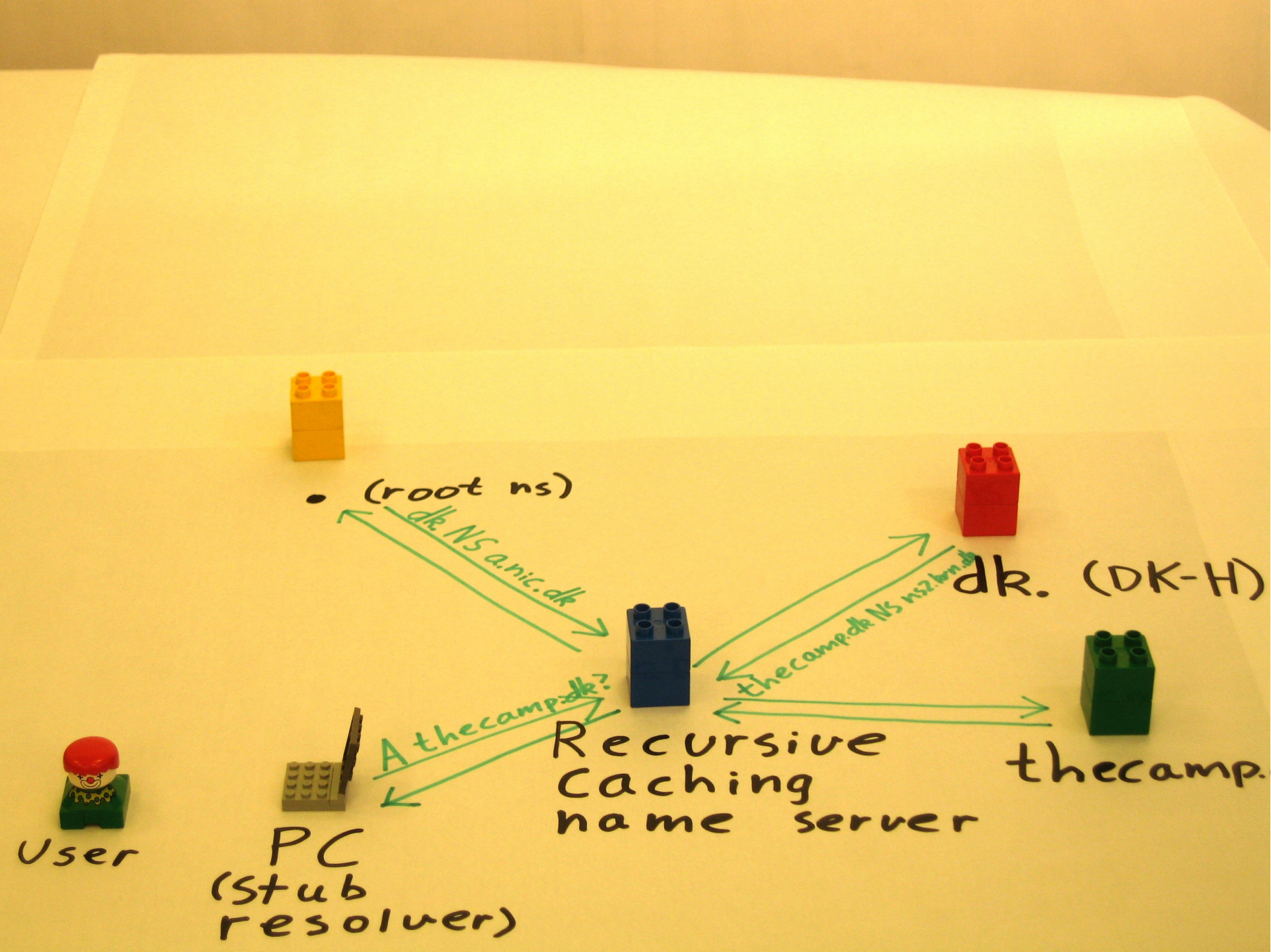

. (root ns)
dk. NS a.nic.dk
dk. (DK-H)
A thecamp.dk?
Recursive
Caching
name server
User
PC
(Stub
resolver)

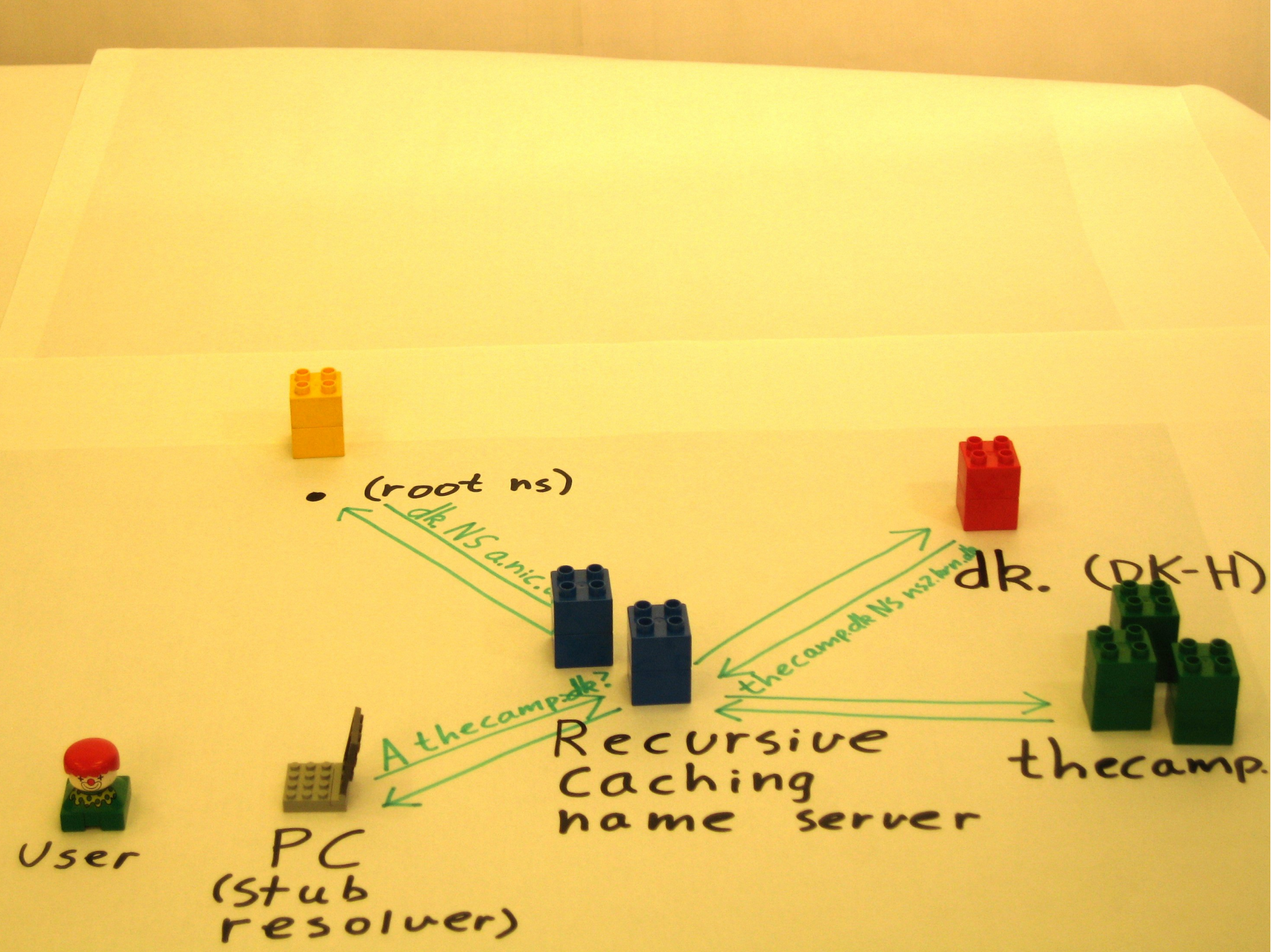

. (root ns)
dk NS a.nic.dk
dk. (DK-H)
thecamp.dk NS ns2.bsn.dk
A thecamp.dk?
Recursive
Caching
name server
User
PC
(Stub
resolver)

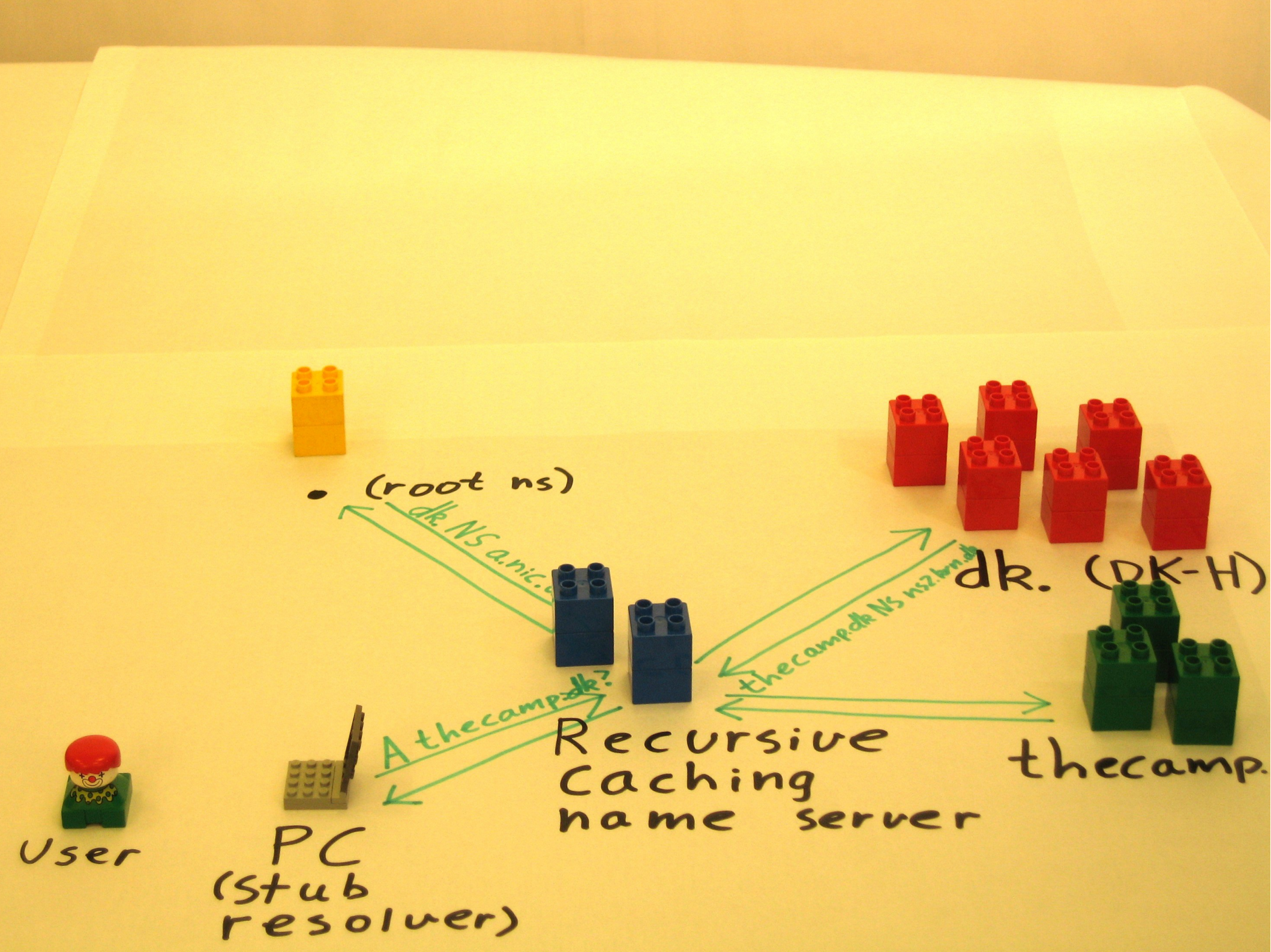

. (root ns)
dk. NS a.nic.dk
dk. (DK-H)
thecamp.dk NS ns2.bwn.dk
A thecamp.dk?
Recursive
Caching
name server
thecamp.
User
PC
(Stub
resolver)

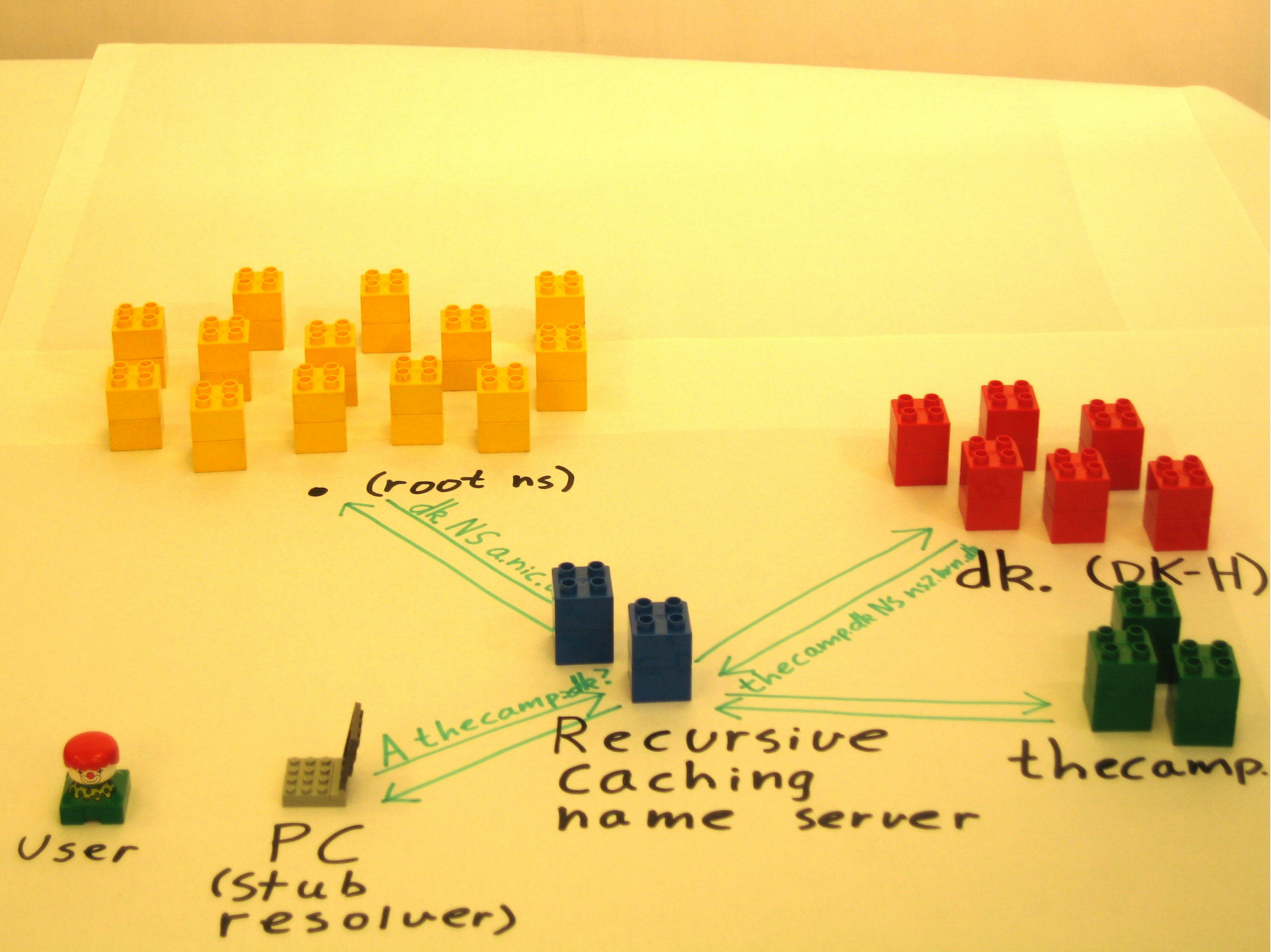

. (root ns)
dk NS a.nic.dk
dk. (DK-H)
thecamp.dk NS ns2.bun.dk
A thecamp.dk?
Recursive
Caching
name server
thecamp.
User
PC
(Stub
resolver)


. (root ns)
dk. NS a.nic.dk
dk.
(DK-H)
thecamp.dk NS ns2.bwn.dk
A thecamp.dk?
Recursive
Caching
name server
thecamp.
User
PC
(Stub
resolver)


. (root ns)
dk. NS a.nic.dk
dk. (DK-H)
thecamp.dk NS ns2.bsn.dk
A thecamp.dk?
Recursive
Caching
name server
thecamp.
User
PC
(Stub
resolver)

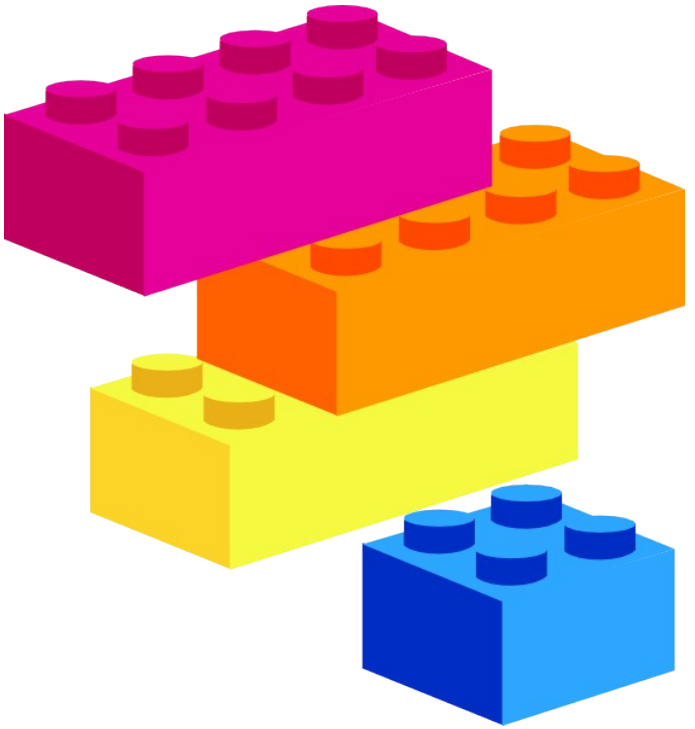

. (root ns)
dk. (DK-H)
thecamp.
User
PC
(Stub
resolver)
Recursive
Caching
name server

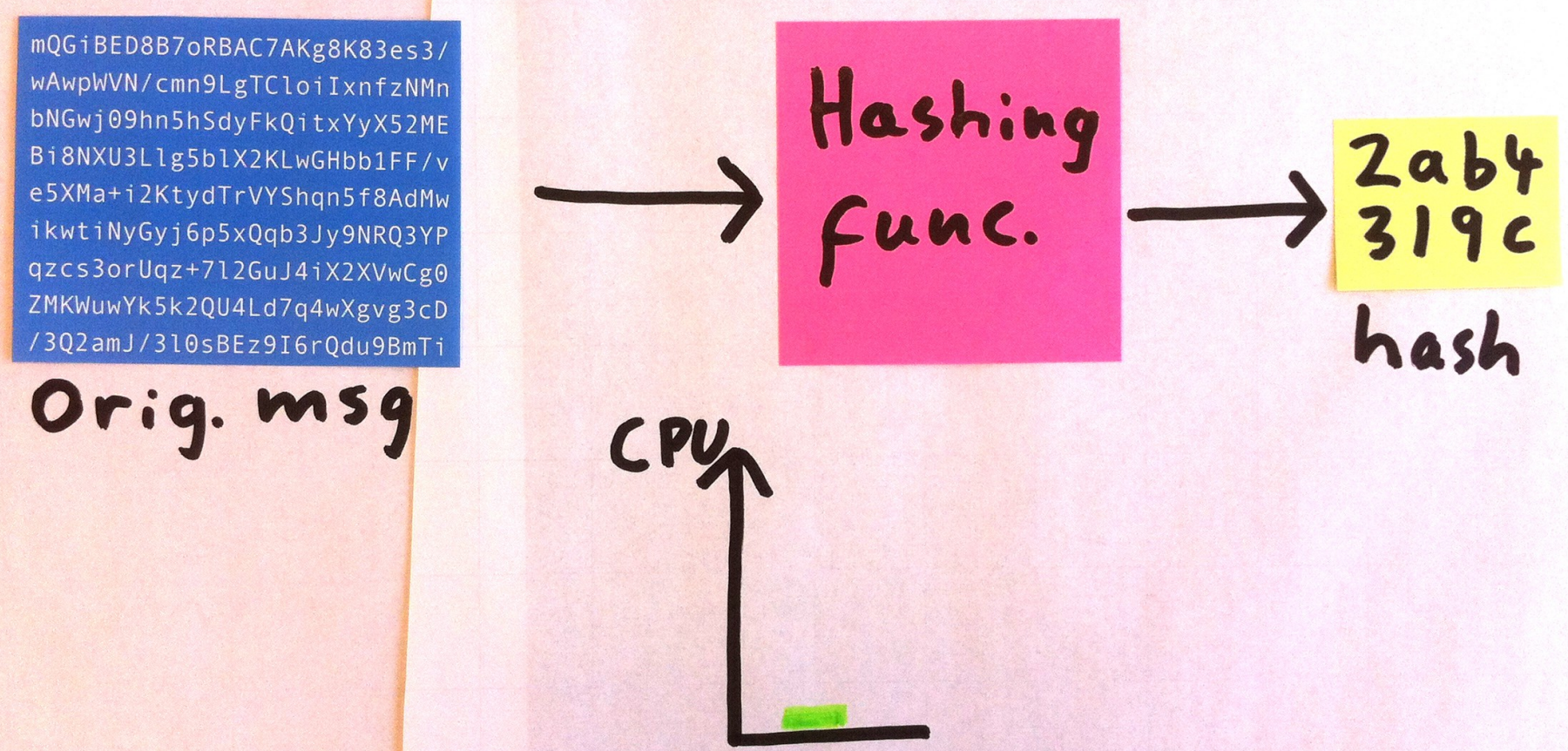

. (root ns)
dk NS a.nic.
dk. (DK-H)
thecamp.dk NS ns2.
A thecamp.dk?
Recursive
Caching
name server
thecamp.
User
PC
(Stub
resolver)

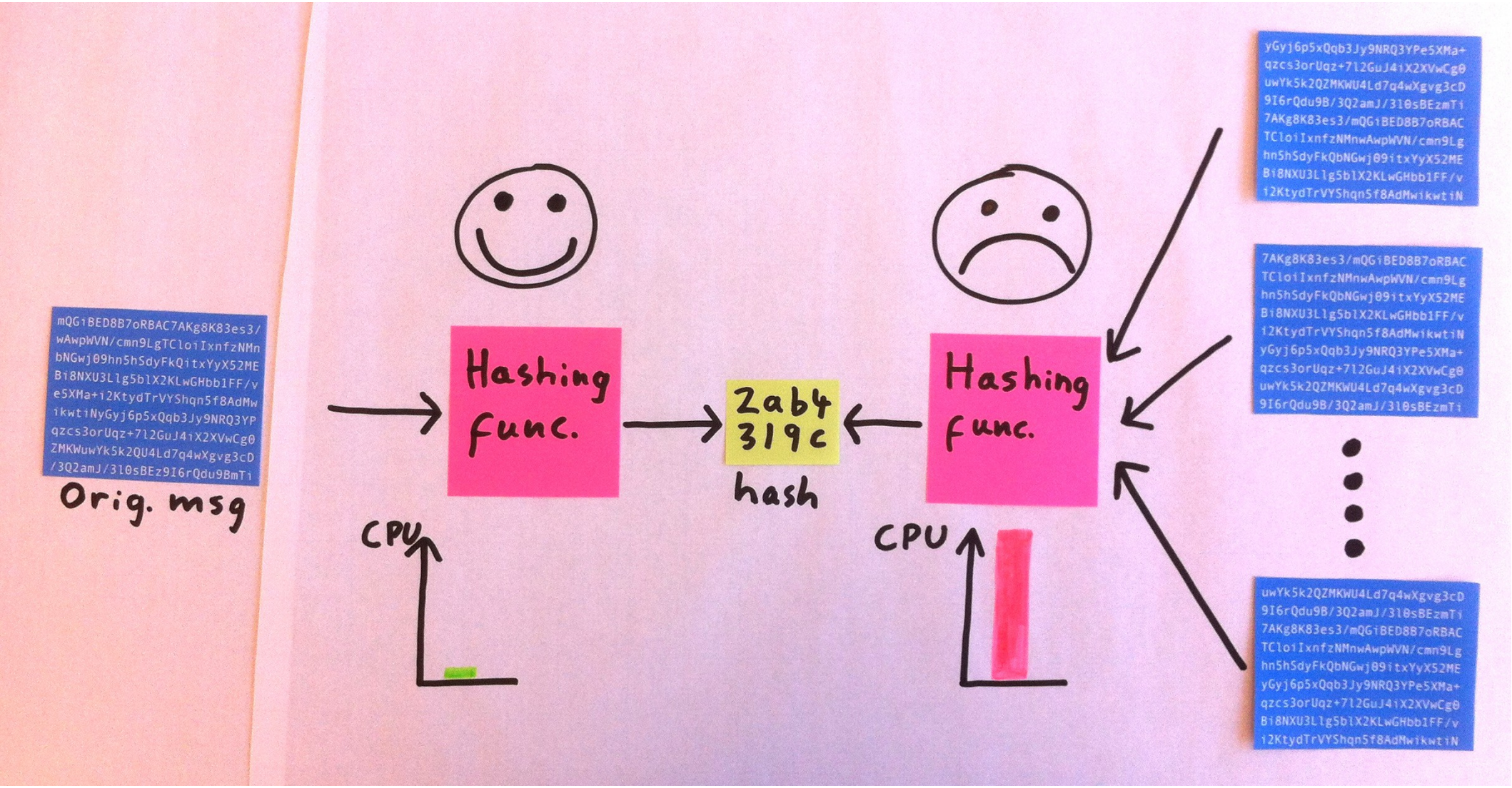

. (root ns)
dk. (DK-H)
thecamp.
User
PC
(Stub
resolver)
Recursive
Caching
name server

Cryptography primer

- Cryptographic hash functions
- Public-key cryptography
  - Public/private key pair
  - Encryption/decryption
  - Signing/validating




mQGiBED8B7oRBAC7AKg8K83es3/
wAwpWVN/cmn9LgTCloiIxnfzNMn
bNGwj09hn5hSdyFkQitxYyX52ME
Bi8NXU3Llg5blX2KLwGHbb1FF/v
e5XMa+i2KtydTrVYShqn5f8AdMw
ikwtiNyGyj6p5xQqb3Jy9NRQ3YP
qzcs3orUqz+7l2GuJ4iX2XVwCg0
ZMKWuwYk5k2QU4Ld7q4wXgvg3cD
/3Q2amJ/3l0sBEz9I6rQdu9BmTi
Orig. msg
Hashing func.
2ab4 319c
hash
CPU


mQGiBED8B7oRBAC7AKg8K83es3/
wAwpWVN/cmn9LgTCloiIxnfzNMn
bNGwj09hn5h5dyFkQitxYyX52ME
Bi8NXU3Llg5blX2KLwGHbb1FF/v
e5XMa+i2KtydTrVYShqn5f8AdMw
ikwtiNyGyj6p5xQqb3Jy9NRQ3YP
qzcs3orUqz+7l2GuJ4iX2XVwCg0
ZMKWuwYk5k2QU4Ld7q4wXgvg3cD
/3Q2amJ/3l0sBEz9I6rQdu9BmTi
Orig. msg
Hashing func.
2ab4 319c
hash
Hashing func.
CPU
CPU
yGyj6p5xQqb3Jy9NRQ3YPe5XMa+
qzcs3orUqz+7l2GuJ4iX2XVwCg0
uwYk5k2QZMKWU4Ld7q4wXgvg3cD
9I6rQdu9B/3Q2amJ/3l0sBEzmTi
7AKg8K83es3/mQGiBED8B7oRBAC
TCloiIxnfzNMnwAwpWVN/cmn9Lg
hn5hSdyFkQbNGwj09itxYyX52ME
Bi8NXU3Llg5blX2KLwGHbb1FF/v
i2KtydTrVYShqn5f8AdMwikwtiN
7AKg8K83es3/mQGiBED8B7oRBAC
TCloiIxnfzNMnwAwpWVN/cmn9Lg
hn5hSdyFkQbNGwj09itxYyX52ME
Bi8NXU3Llg5blX2KLwGHbb1FF/v
i2KtydTrVYShqn5f8AdMwikwtiN
yGyj6p5xQqb3Jy9NRQ3YPe5XMa+
qzcs3orUqz+7l2GuJ4iX2XVwCg0
uwYk5k2QZMKWU4Ld7q4wXgvg3cD
9I6rQdu9B/3Q2amJ/3l0sBEzmTi
uwYk5k2QZMKWU4Ld7q4wXgvg3cD
9I6rQdu9B/3Q2amJ/3l0sBEzmTi
7AKg8K83es3/mQGiBED8B7oRBAC
TCloiIxnfzNMnwAwpWVN/cmn9Lg
hn5hSdyFkQbNGwj09itxYyX52ME
yGyj6p5xQqb3Jy9NRQ3YPe5XMa+
qzcs3orUqz+7l2GuJ4iX2XVwCg0
Bi8NXU3Llg5blX2KLwGHbb1FF/v
i2KtydTrVYShqn5f8AdMwikwtiN

Cryptographic hash functions

- The ideal CHF:
  - Easy to compute
  - Infeasible to generate message with a given hash
  - Infeasible to modify message without changing the hash
  - Infeasible to find two different messages with the same hash
- Used for digital signatures, authentication, hash tables, checksumming, etc.

Cryptographic hash functions

- The ideal CHF:
  - Easy to compute
  - Infeasible to generate message with a given hash
  - Infeasible to modify message without changing the hash
  - Infeasible to find two different messages with the same hash
- Used for digital signatures, authentication, hash tables, checksumming, etc.

Take a look at http://codahale.com/how-to-safely-store-a-password/ and PHK's column at http://queue.acm.org/detail.cfm?id=2254400

Cryptographic hash functions

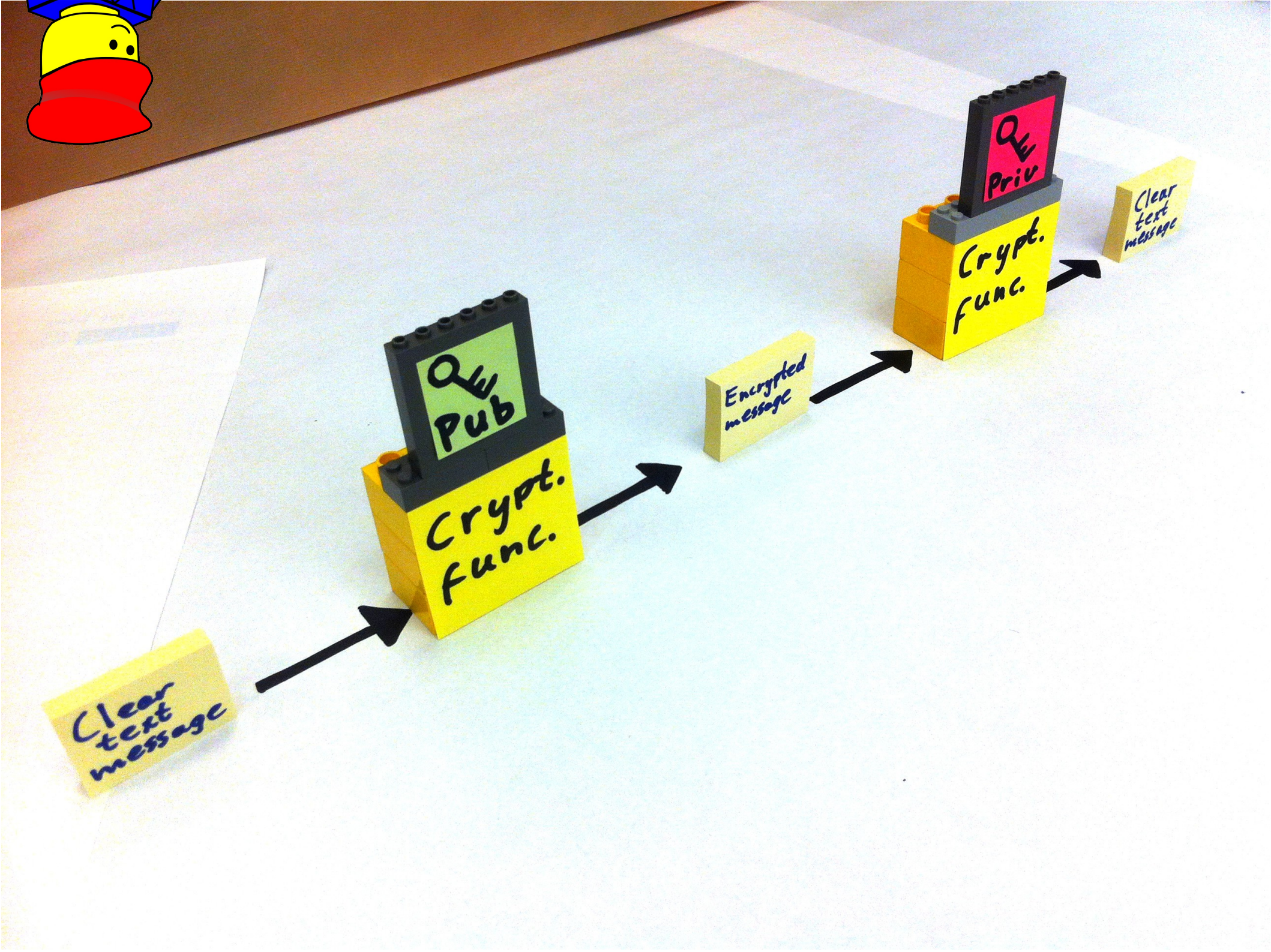
MD5 (128 bits), SHA-1 (160 bits), SHA-256, SHA-512
MD = ”Message Digest”, SHA = ”Secure Hashing Alg.”

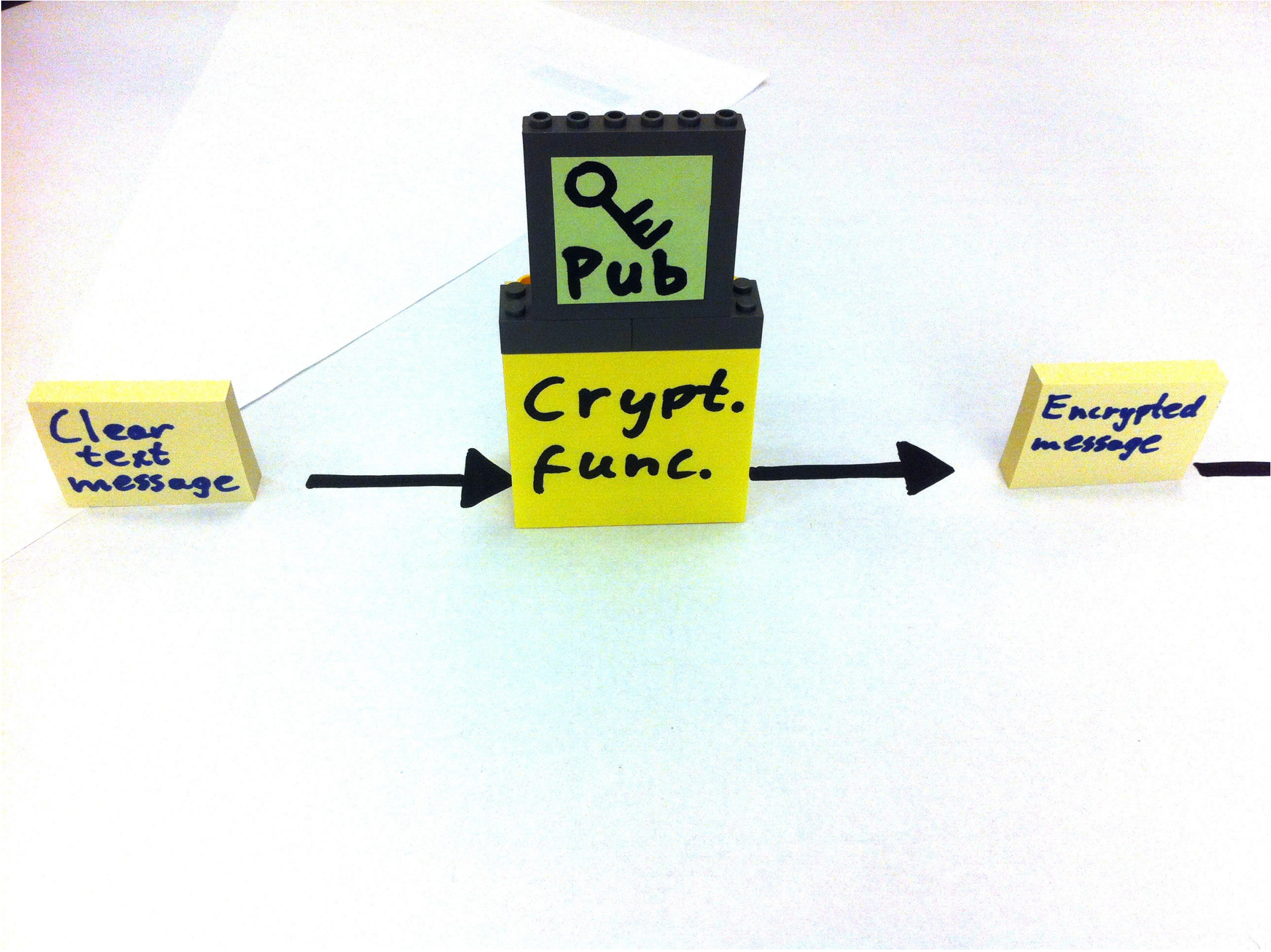
Public-key cryptography

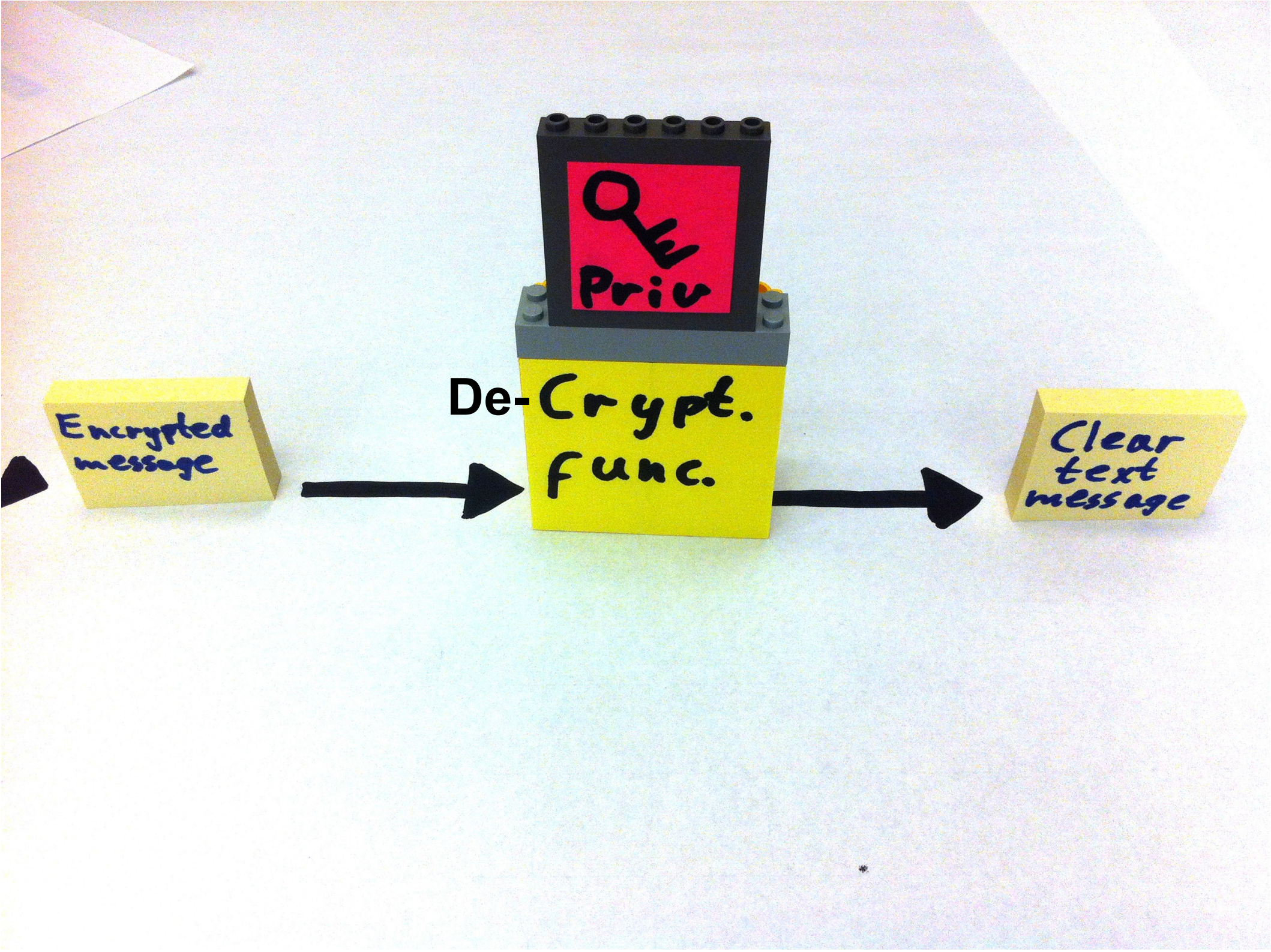
- Generate key pair: a public and a private key
- Mathematically linked, i.e. data encrypted with one can be decrypted with the other
- Publish the public key as widely as possible
- Keep the private key secret
- Asymmetric rather than symmetric, i.e. no problematic key exchange for each session
- … But, initially, a public key must be obtained from an authentic source!

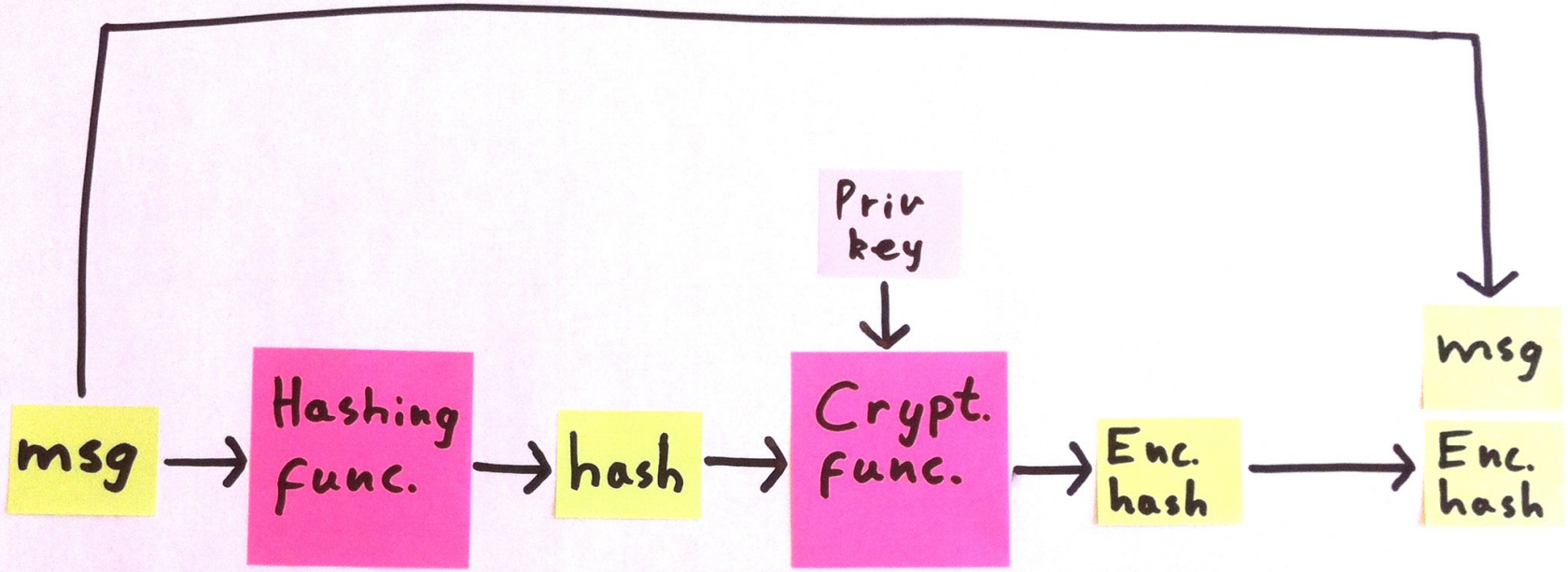
Public/ Private key pair

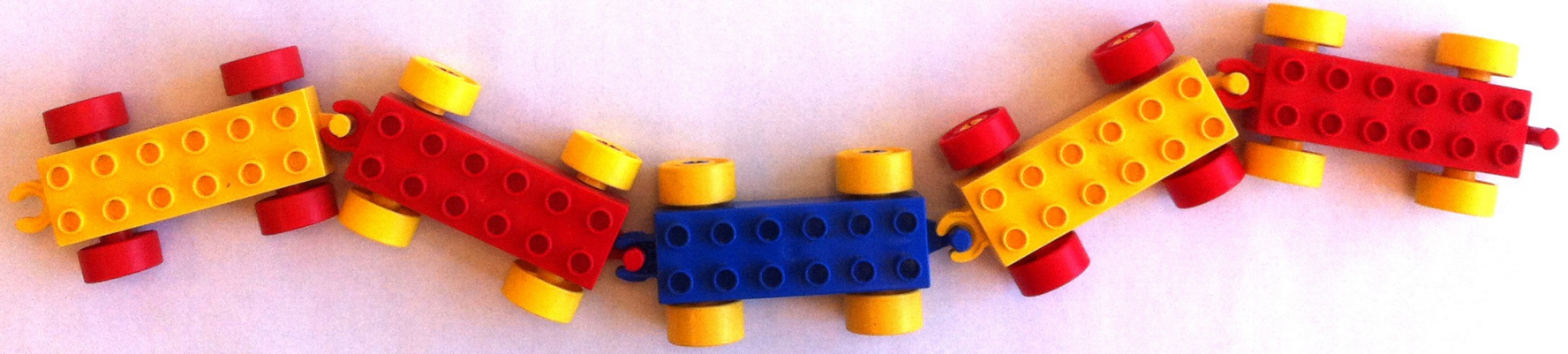

Pub


Clear text message
Pub
Crypt. func.
Encrypted message
Priv
Crypt. func.
Clear text message

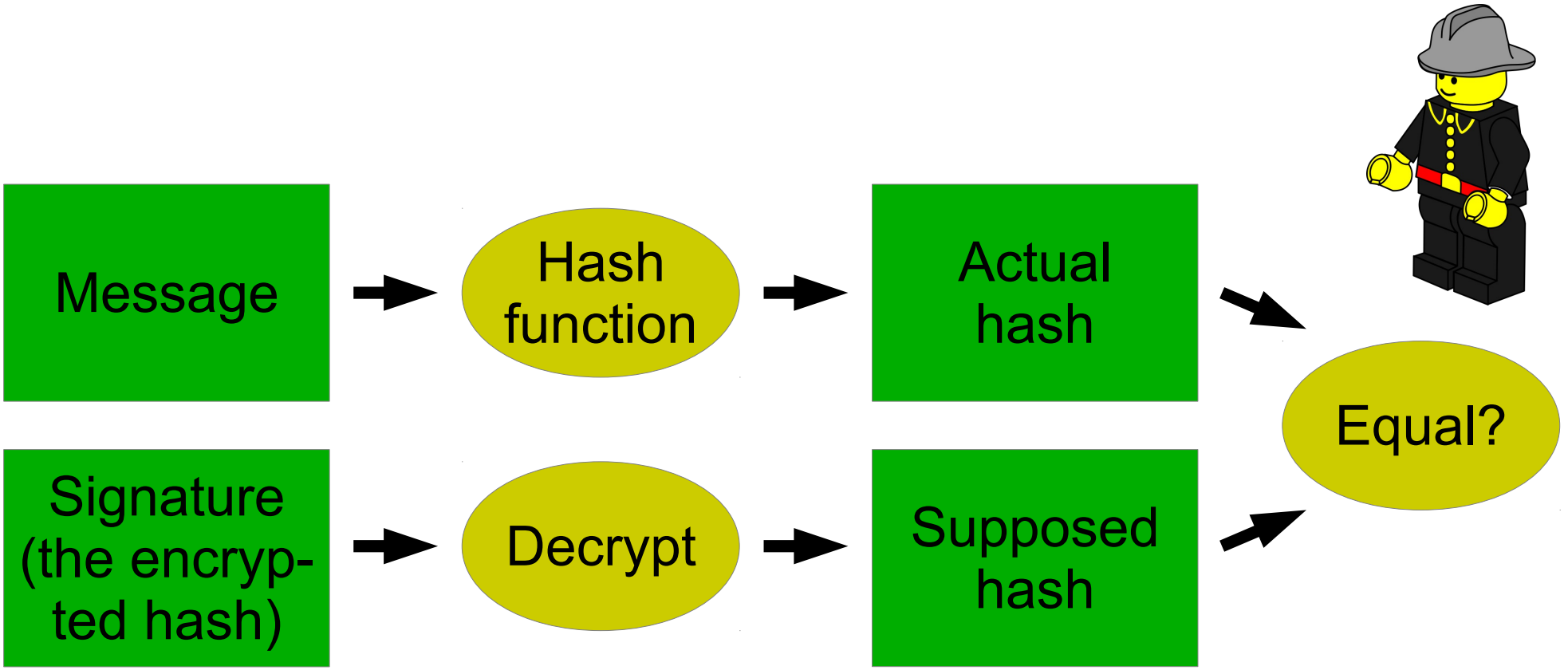

Pub
Clear text message
Crypt. Func.
Encrypted message


Priv
Encrypted message
De-Crypt. Func.
Clear text message

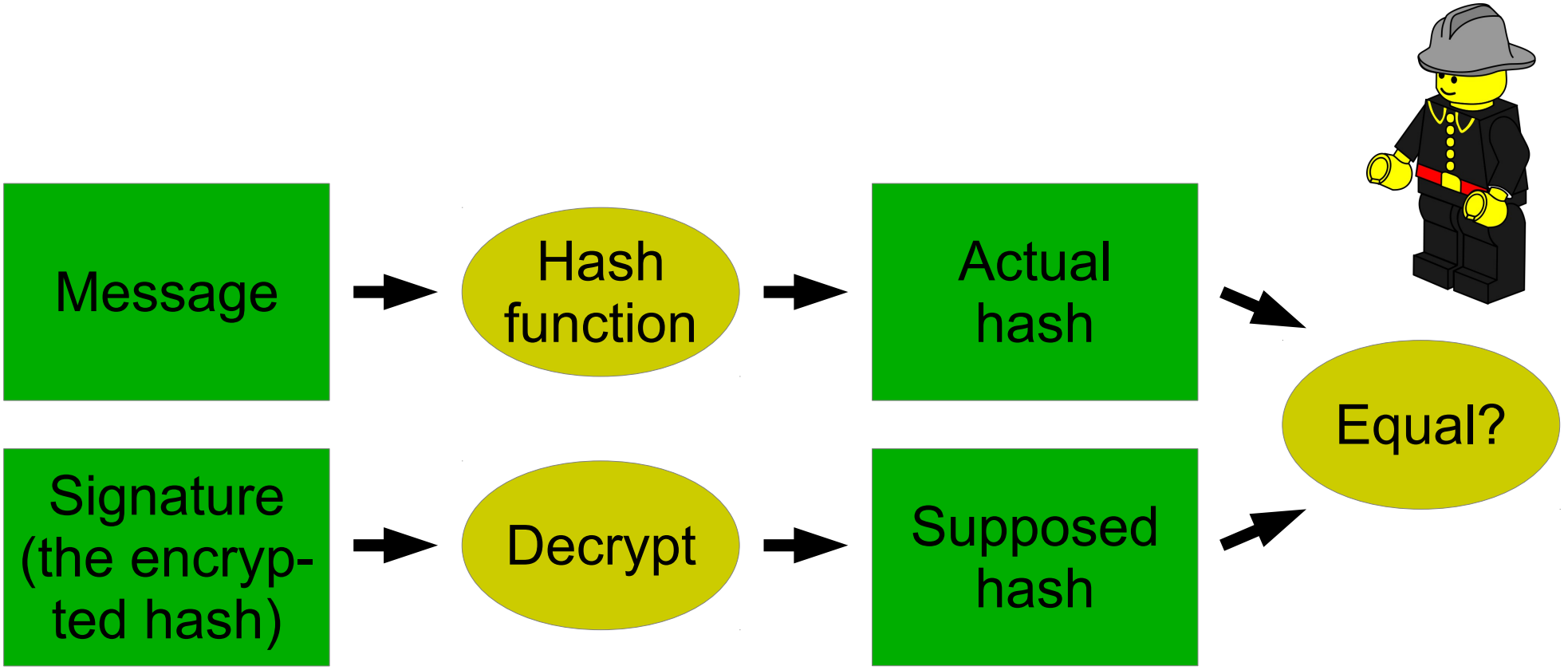

msg
Hashing func.
hash
Priv key
Crypt. func.
Enc. hash
msg
Enc. hash



Validating a signature



Validating a signature



DNSSEC

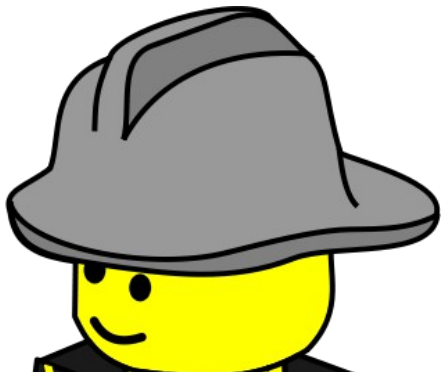
- Two sides of the coin:
  - A tree of signed zones being served by authoritative name servers
  - Validating resolvers/name servers
- We will return to the latter later
- DNS + some new stuff:
  - Ressource records
  - Chain of trust
  - New header flags and bits
  - Maintenance

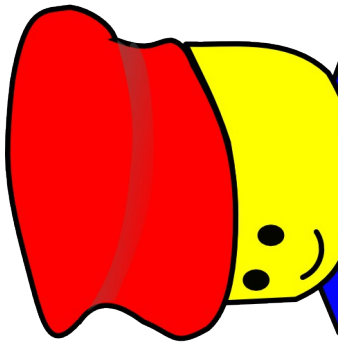
In a nutshell

- Generate two key pairs:
  - Key signing key pair (KSK)
  - Zone signing key pair (ZSK)
- Add public keys of KSK and ZSK to zone
- Sign public keys with KSK and add signature to zone
- Sign remaining ressource record sets (RRsets) with ZSK and add signatures to zone
- Hash public key of KSK and add value to parent zone (e.g. dk.)

Some thoughts

- DNSSEC provides authenticity and integrity, not confidentiality
- The two key pairs create a decoupling
- Space is saved by adding a hash to the parent zone rather than the key





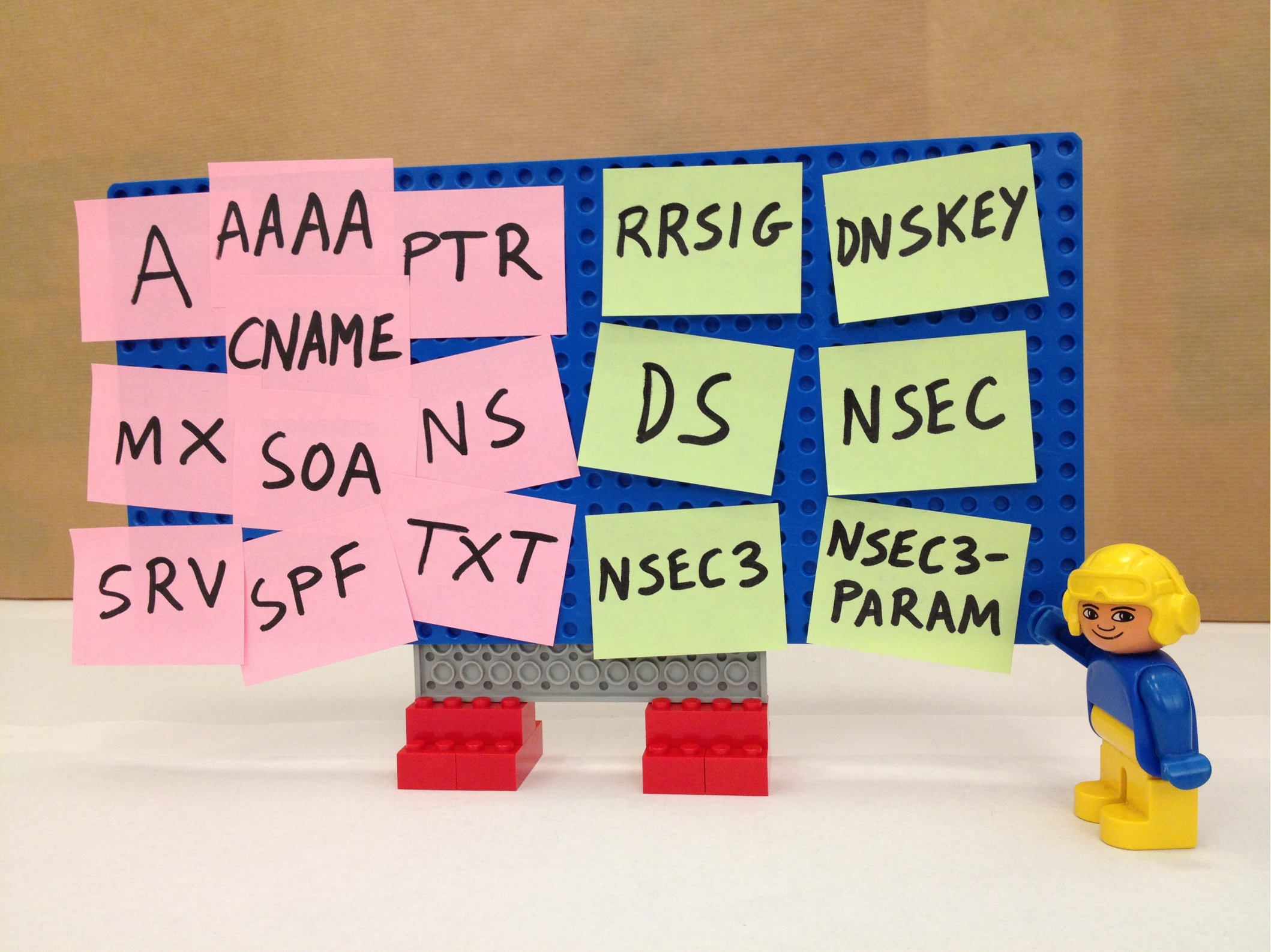
Relevant RFCs

- **2535**: Domain Name System Security Extensions
- **2845**: Secret Key Transaction Authentication for DNS (TSIG)
- **2931**: DNS Request and Transaction Signatures (SIG(0)s)
- **4033**: DNS Security Introduction and Requirements
- **4034**: Ressource Records for the DNS Security Extensions
- **4035**: Protocol Modifications for the DNS Security Extensions
- **4470**: Minimally Covering NSEC Records and DNSSEC On-line Signing
- **5155**: DNS Security (DNSSEC) Hashed Authenticated Denial of Existence

Relevant RFCs

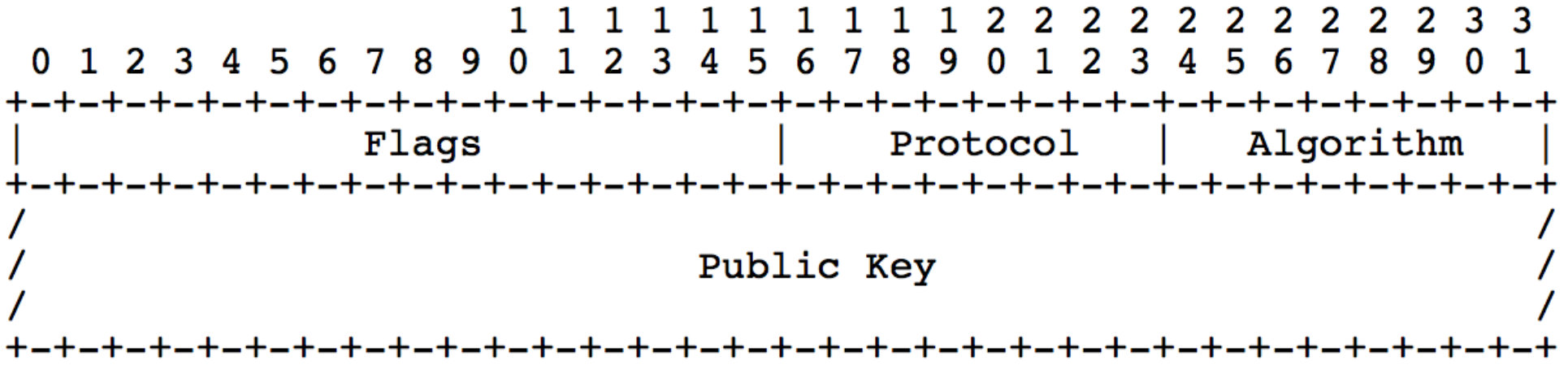
- **2535**: Domain Name System Security Extensions
- **2845**: Secret Key Transaction Authentication for DNS (TSIG)
- **2931**: DNS Request and Transaction Signatures (SIG(0)s)
- **4033**: DNS Security Introduction and Requirements
- **4034**: Ressource Records for the DNS Security Extensions
- **4035**: Protocol Modifications for the DNS Security Extensions
- **4470**: Minimally Covering NSEC Records and DNSSEC On-line Signing
- **5155**: DNS Security (DNSSEC) Hashed Authenticated Denial of Existence

We have not read all of them :-P


A
AAAA
PTR
CNAME
MX
SOA
NS
SRV
SPF
TXT
RRSIG
DNSKEY
DS
NSEC
NSEC3
NSEC3-
PARAM

DNSKEY

The RDATA for a DNSKEY RR consists of a 2 octet Flags Field, a 1 octet Protocol Field, a 1 octet Algorithm Field, and the Public Key Field.

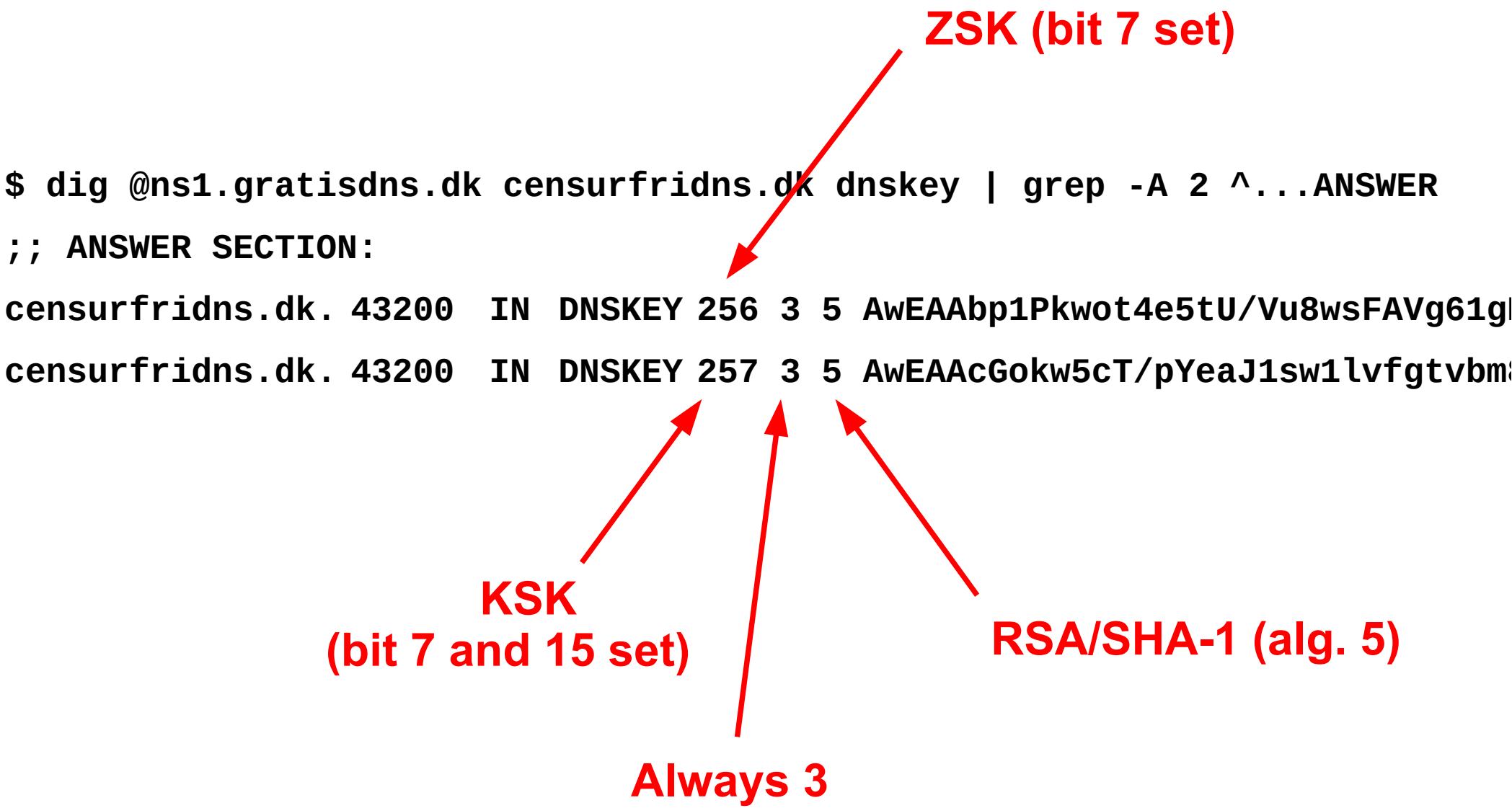


Source: RFC 4034

DNSKEY

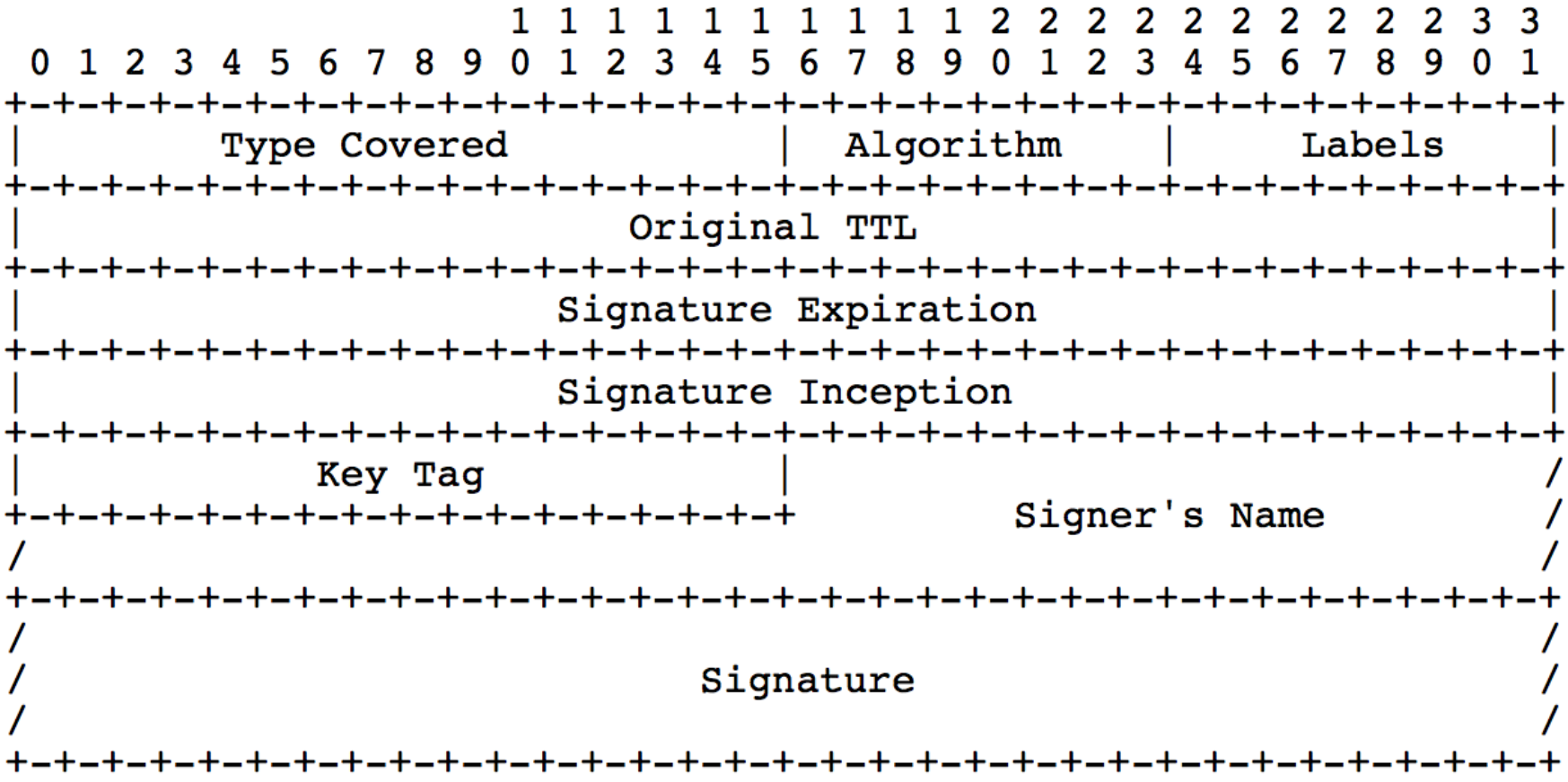
```
$ dig @ns1.gratisdns.dk censurfridns.dk dnskey | grep -A 2 ^...ANSWER

;; ANSWER SECTION:

censurfridns.dk.    43200  IN     DNSKEY 256 3 5 AwEAAbp1Pkwot4e5tU/Vu8wsFAVg61gBWvZqb1tKgaJZdDU27arWzjHF i0EhKKun3c7e65UQZT1Y88pXSCTi5rfHiUU=

censurfridns.dk.    43200  IN     DNSKEY 257 3 5 AwEAAcGokw5cT/pYeaJ1sw1lvfgtvbm8t7M19XYTIy0wtob9kJZFnapy r4ch9gNyzUIe4Ks9ItvT/hiuDv7GJk/6NEc=
```

DNSKEY


ZSK (bit 7 set)
$ dig @ns1.gratisdns.dk censurfridns.dk dnskey | grep -A 2 ^...ANSWER
;; ANSWER SECTION:
censurfridns.dk. 43200 IN DNSKEY 256 3 5 AwEAAbp1Pkwot4e5tU/Vu8wsFAVg61g
censurfridns.dk. 43200 IN DNSKEY 257 3 5 AwEAAcGokw5cT/pYeaJ1sw1lvfgtvbm
KSK
(bit 7 and 15 set)
Always 3
RSA/SHA-1 (alg. 5)

RRSIG

The RDATA for an RRSIG RR consists of a 2 octet Type Covered field, a 1 octet Algorithm field, a 1 octet Labels field, a 4 octet Original TTL field, a 4 octet Signature Expiration field, a 4 octet Signature Inception field, a 2 octet Key tag, the Signer's Name field, and the Signature field.



Source: RFC 4034

RRSIG

```
$ dig @ns1.gratisdns.dk censurfridns.dk rrsig | grep -A 9 ^...ANSWER

;; ANSWER SECTION:

censurfridns.dk. 43200 IN RRSIG DNSKEY 5 2 43200 20120820132225 20120721132225 39453 censurfridns.dk. Mti1G/P7G4cgM9Kj3sBKik50bRGfQXGqx2bWgdhWjxRDfWFdpZzpyHcp tIGpfl/pD/gZ2kdj2qzIwHk7s4U

censurfridns.dk. 43200 IN RRSIG DNSKEY 5 2 43200 20120820132225 20120721132225 59671 censurfridns.dk. ruNo6HT3R+Ll6wlptfKaAMt0cYM8BiYo3ZmcqZEdcngFpo87NxpD/khG 3aJfFWiHg73K91M+T68C6RjXcbM

censurfridns.dk. 43200 IN RRSIG NSEC 5 2 43200 20120820132225 20120721132225 39453 censurfridns.dk. SB/KFjL6k/J2+sc4AWPwDiUfo7qNeFXbeCPluKgGCCnxNjr5YXOMnBjH emB7/nlWZ/ooDLaSkfAMWOYm6PDnF

censurfridns.dk. 43200 IN RRSIG AAAA 5 2 43200 20120820132225 20120721132225 39453 censurfridns.dk. BNw8aD1hy6VRmd73X6/otBq3nkIko7i0FD93gMlhCeEVTzbXcefUpqQU CxQMrAhTHIJVlj3bVFTlXNc537fIl

censurfridns.dk. 43200 IN RRSIG TXT 5 2 43200 20120820132225 20120721132225 39453 censurfridns.dk. XNrclGxuwscAB5QNYpcDRuQRxMXh1y527WPmvP875t72VZmmOmNvsiub 4nTOS2Z1gKUU/kIDoRpilHAKbox5Gw

censurfridns.dk. 43200 IN RRSIG MX 5 2 43200 20120820132225 20120721132225 39453 censurfridns.dk. qDafz5gRUVddJi4gZc7y2rUdkOkTgOOKybbKQygoO1JYfF2WiZguRhG9 efl7VnaWOa4rP38+9DrZpkbFFhZsBw=

censurfridns.dk. 43200 IN RRSIG A 5 2 43200 20120820132225 20120721132225 39453 censurfridns.dk. K8i2sbv7C7PPjvToJBk2aKcNXQY8+Ke91FsjQpDpZLKgyoX3KGyOS6Yb CsIp4qPo4TNZI6d9+XXuh69NvC0mUw==

censurfridns.dk. 43200 IN RRSIG NS 5 2 43200 20120820132225 20120721132225 39453 censurfridns.dk. jQfNDEEuuhqRnpufk0v9FVxUbsZEbeWPz8rdkBNu8IJDh0SxJ0pZLbp6 Yd0EJFMbYj+Avvg33veLcnVl02YvRA=

censurfridns.dk. 43200 IN RRSIG SOA 5 2 43200 20120820132225 20120721132225 39453 censurfridns.dk. aE8kAn4QErkf7K405gqhgkZIqUtVjWKVbnht8R8AhsyeJ0X6V85qWVTK 6S9brwMOD9vjsrEcqZf6ZaLfjmw4Fg
```

RRSIG

RSA/SHA-1 (alg. 5)

2 labels, ”dk” and ”censurfridns”

```
$ dig @ns1.gratisdns.dk censurfridns.dk rrsig | grep -A 9 ^...ANSWER
;; ANSWER SECTION:
censurfridns.dk. 43200 IN RRSIG DNSKEY 5 2 43200 20120820132225 20120721132225 39453 censurfridns.dk. Mti1G/P7G4cgM9K
censurfridns.dk. 43200 IN RRSIG DNSKEY 5 2 43200 20120820132225 20120721132225 59671 censurfridns.dk. ruNo6HT3R+Ll6wl
censurfridns.dk. 43200 IN RRSIG NSEC 5 2 43200 20120820132225 20120721132225 39453 censurfridns.dk. SB/KFjL6k/J2+sc4A
censurfridns.dk. 43200 IN RRSIG AAAA 5 2 43200 20120820132225 20120721132225 39453 censurfridns.dk. BNw8aD1hy6VRmd73X
censurfridns.dk. 43200 IN RRSIG TXT 5 2 43200 20120820132225 20120721132225 39453 censurfridns.dk. XNrclGxuwscAB5QNYp
censurfridns.dk. 43200 IN RRSIG MX 5 2 43200 20120820132225 20120721132225 39453 censurfridns.dk. qDafz5gRUVddJi4gZc7
censurfridns.dk. 43200 IN RRSIG A 5 2 43200 20120820132225 20120721132225 39453 censurfridns.dk. K8i2sbv7C7PPjvToJBk2
censurfridns.dk. 43200 IN RRSIG NS 5 2 43200 20120820132225 20120721132225 39453 censurfridns.dk. jQfNDEEuuhqRnpufk0v
censurfridns.dk. 43200 IN RRSIG SOA 5 2 43200 20120820132225 20120721132225 39453 censurfridns.dk. aE8kAn4QErkf7K405g
```

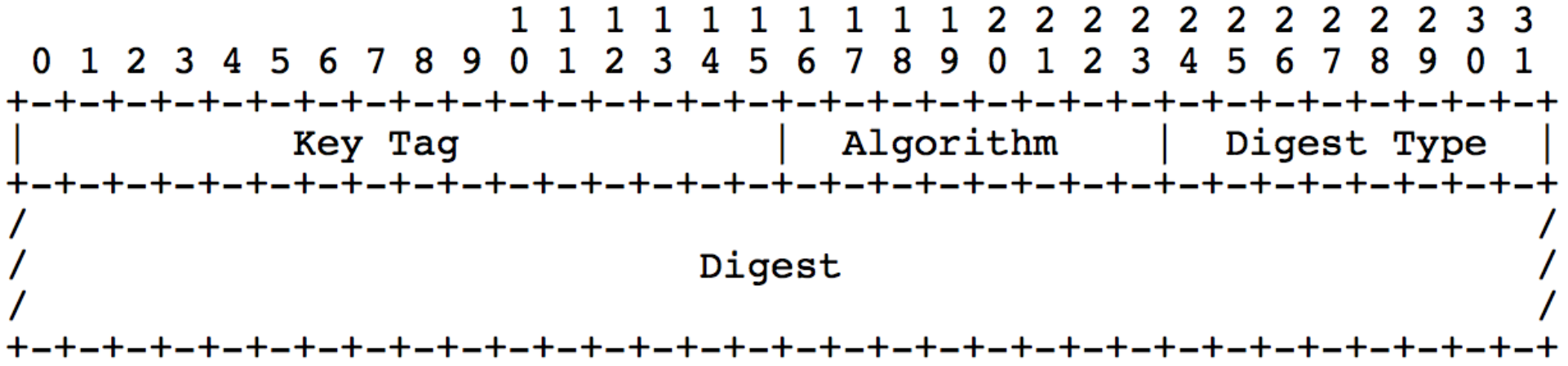
ID of KSK

ID of ZSK

DS

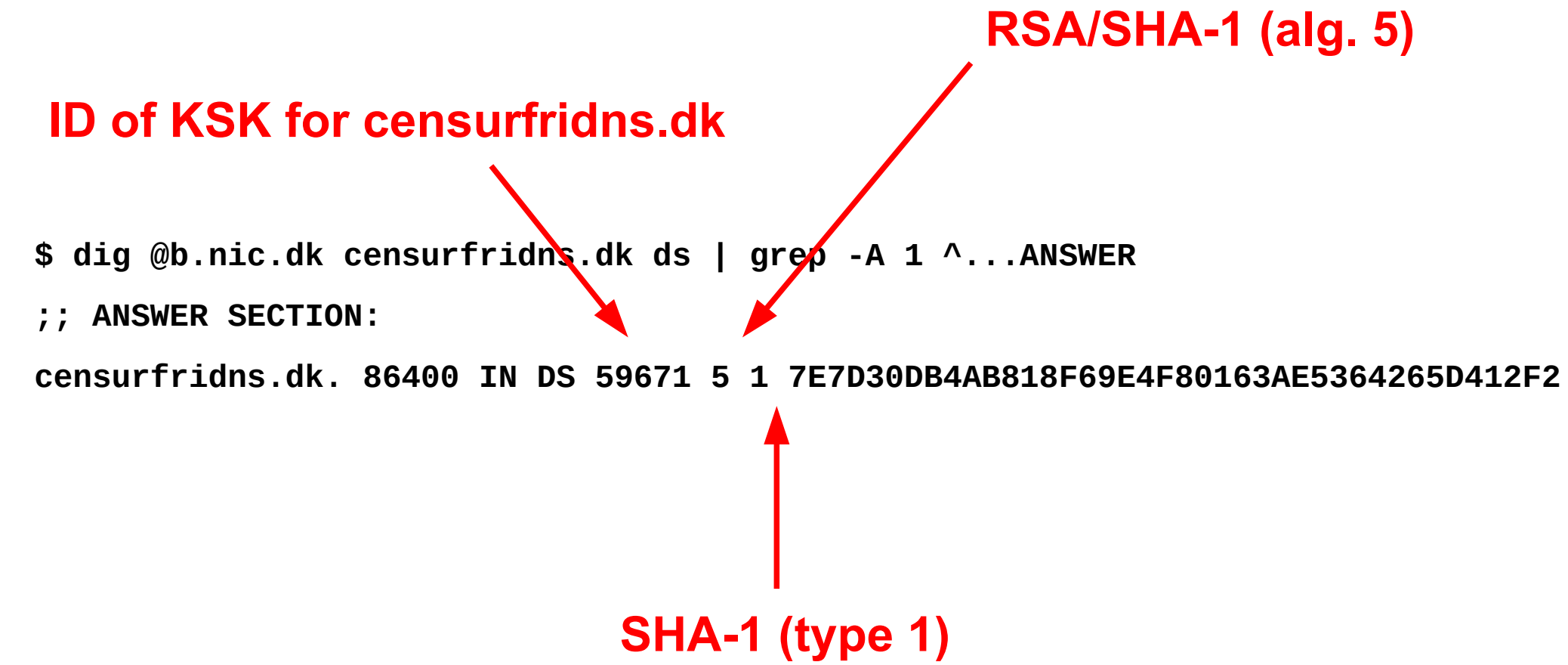
(Delegation Signer)

The RDATA for a DS RR consists of a 2 octet Key Tag field, a 1 octet Algorithm field, a 1 octet Digest Type field, and a Digest field.



Source: RFC 4034

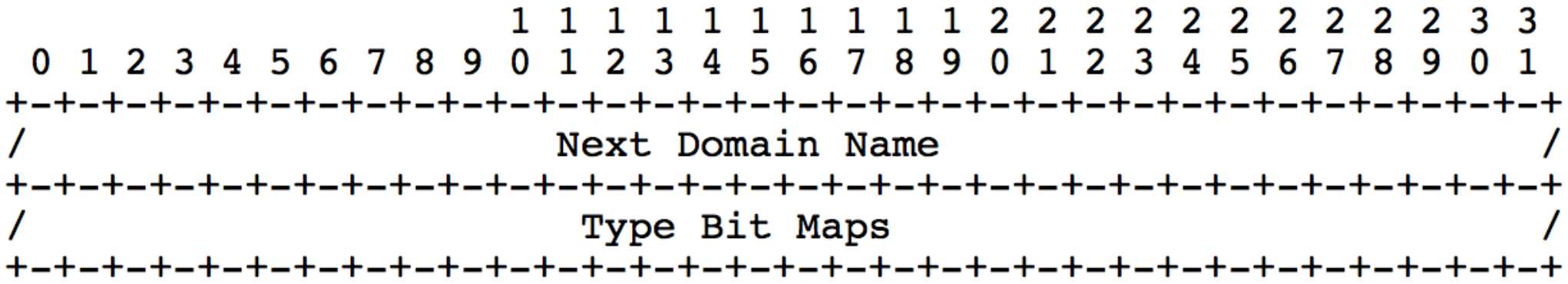
DS


RSA/SHA-1 (alg. 5)
ID of KSK for censurfridns.dk
$ dig @b.nic.dk censurfridns.dk ds | grep -A 1 ^...ANSWER
;; ANSWER SECTION:
censurfridns.dk. 86400 IN DS 59671 5 1 7E7D30DB4AB818F69E4F80163AE5364265D412F2
SHA-1 (type 1)

NSEC

(Next SECure - authenticated denial of existence)

The RDATA of the NSEC RR is as shown below:



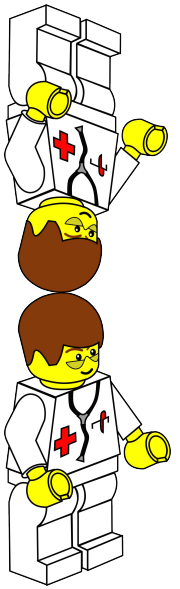
Source: RFC 4034

NSEC

```
$ dig @ns1.gratisdns.dk censurfridns.dk nsec | grep -A 1 ^...ANSWER
;; ANSWER SECTION:
censurfridns.dk. 43200 IN NSEC default._domainkey.censurfridns.dk. A NS SOA MX TXT AAAA RRSIG NSEC DNSKEY

$ dig @ns1.gratisdns.dk default._domainkey.censurfridns.dk nsec | grep -A 1 ^...ANSWER
;; ANSWER SECTION:
default._domainkey.censurfridns.dk. 43200 IN NSEC blog.censurfridns.dk. TXT RRSIG NSEC

$ dig @ns1.gratisdns.dk blog.censurfridns.dk nsec | grep -A 1 ^...ANSWER
;; ANSWER SECTION:
blog.censurfridns.dk. 43200 IN NSEC localhost.censurfridns.dk. A AAAA RRSIG NSEC

...
```

NSEC

```
$ NEXT=censurfridns.dk; while true; do echo $NEXT; NEXT=`dig @ns1.gratisdns.dk $NEXT
nsec +short | cut -d ' ' -f 1`; if [ "$NEXT" = "censurfridns.dk." ]; then break; fi;
done

censurfridns.dk

default._domainkey.censurfridns.dk.

blog.censurfridns.dk.

localhost.censurfridns.dk.

ns1.censurfridns.dk.

ns1a.censurfridns.dk.

ns1b.censurfridns.dk.

ns2.censurfridns.dk.

www.censurfridns.dk.
```



NSEC

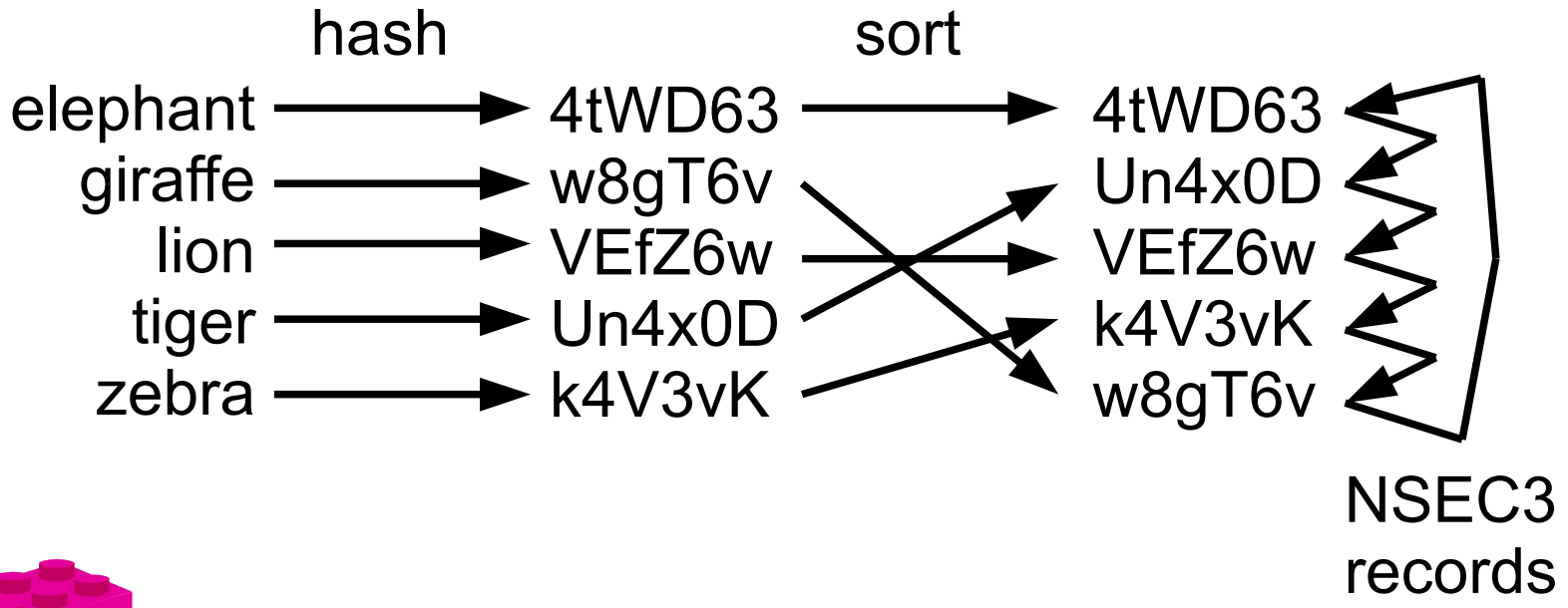
```
$ dig @ns1.gratisdns.dk elephant.censurfridns.dk a +dnssec | tr '\t' ' ' | grep -A 6
^...AUTH | egrep '(AUTH|IN NSEC)' | grep -v ^censurfridns.dk

;; AUTHORITY SECTION:

blog.censurfridns.dk. 43200 IN NSEC localhost.censurfridns.dk. A AAAA RRSIG NSEC
```

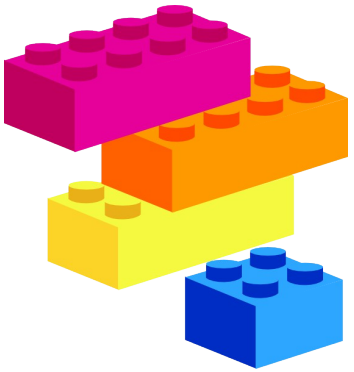
```
$ dig @ns1.gratisdns.dk virus.censurfridns.dk a +dnssec | tr '\t' ' ' | grep -A 6
^...AUTH | egrep '(AUTH|IN NSEC)' | grep -v ^censurfridns.dk

;; AUTHORITY SECTION:

ns2.censurfridns.dk. 43200 IN NSEC www.censurfridns.dk. A AAAA RRSIG NSEC
```

NSEC3

- NSEC3 solves two problems with NSEC:
  - Zone enumeration
  - High cost: ”the cost to secure delegations to unsigned zones is high, relative to the perceived benefit” (source: RFC 5155)
- Both are especially relevant for registries, e.g. DK-Hostmaster for dk.
- One new delegation at a registry:
  - New NSEC RR in an already long NSEC RRset (maintain the order of the linked list)
  - Regenerate RRSIG for NSEC RRset

NSEC3


hash
sort
elephant
giraffe
lion
tiger
zebra
4tWD63
w8gT6v
VEfZ6w
Un4x0D
k4V3vK
4tWD63
Un4x0D
VEfZ6w
k4V3vK
w8gT6v
NSEC3
records

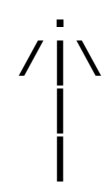


NSEC3

```
$ ldns-nsec3-hash -t 17 -s 092EF3E7975CB1EE nonexistent-domain.dk
S380h9pg6mbd0m87011bdv8icagr1994.
```

```
$ dig @b.nic.dk nonexistent-domain.dk a +dnssec | tr '\t' ' ' |
grep -A 10 ^...AUTH | egrep '(AUTH|rv1.*IN NSEC3)'
;; AUTHORITY SECTION:
rv1glegdcruclq64jr4tqem1u0eaefba.dk. 3600 IN NSEC3 1 1 17
092EF3E7975CB1EE S3F532FN55ASTA3MVMTGEIG80S12G8PC NS DS RRSIG
```

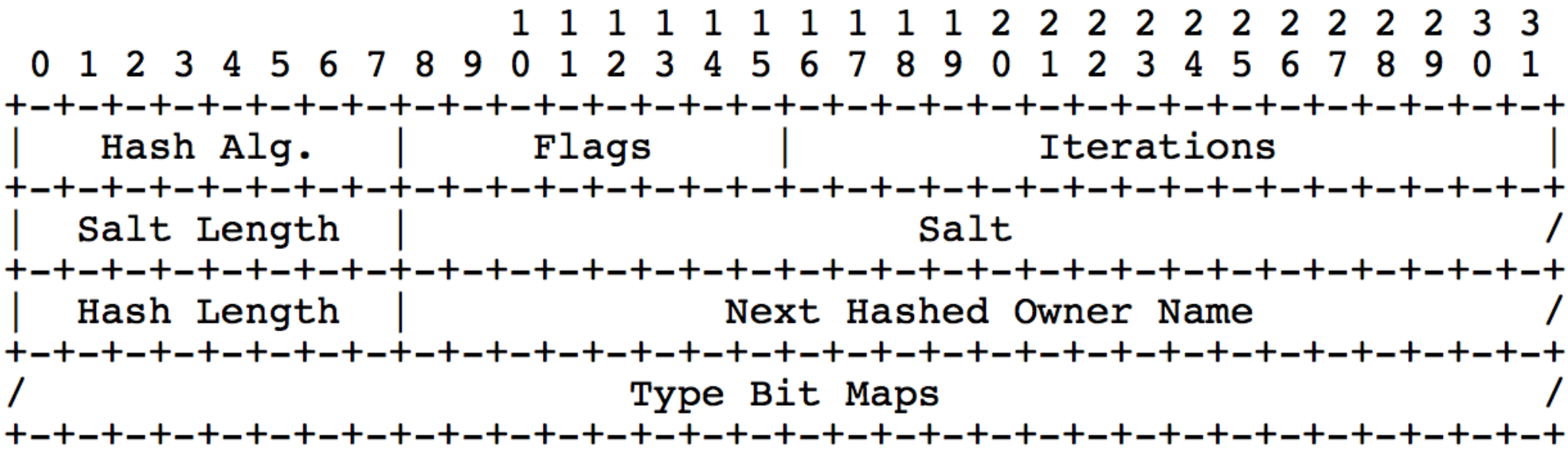
```
rv1... --> s38... --> s3f...
```



Cannot exist

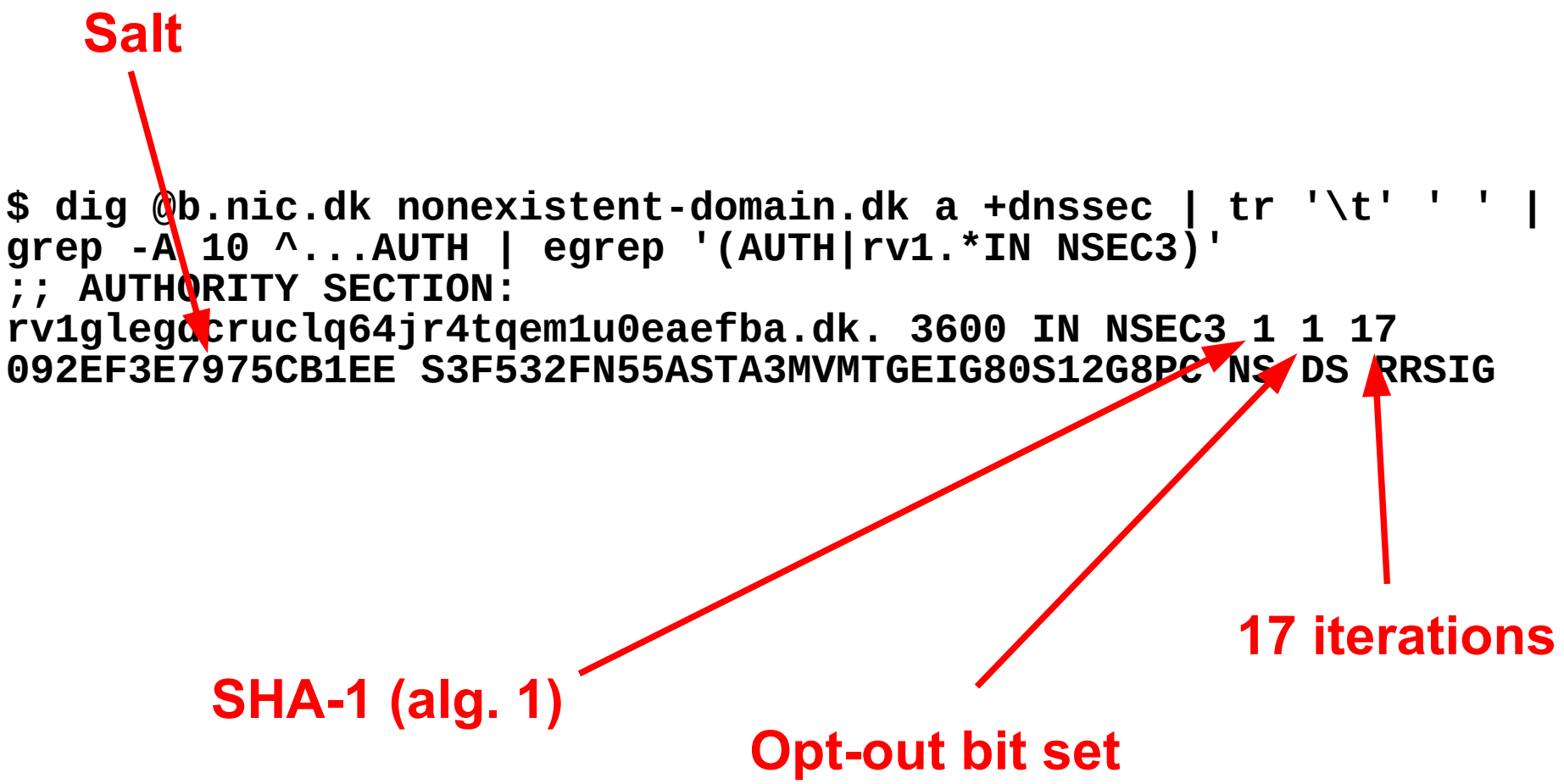
NSEC3

The RDATA of the NSEC3 RR is as shown below:



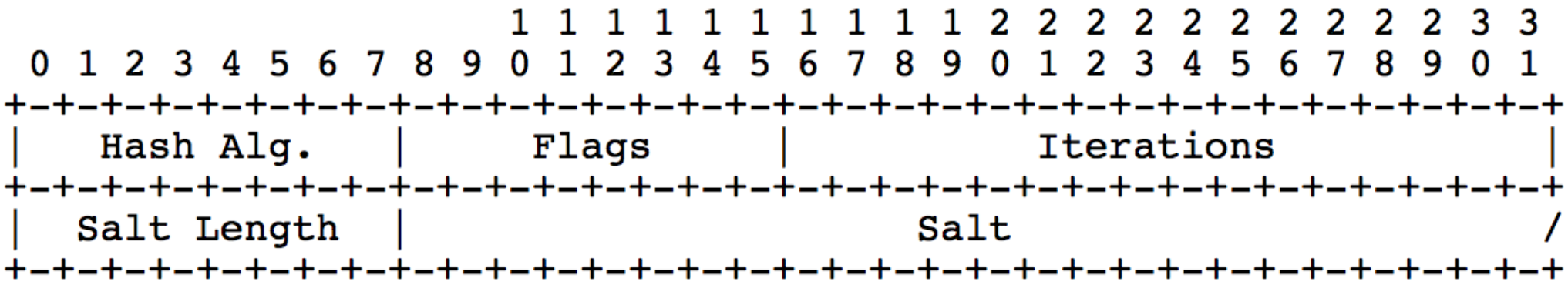
Source: RFC 5155

NSEC3


Salt
$ dig @b.nic.dk nonexistent-domain.dk a +dnssec | tr '\t' ' ' |
grep -A 10 ^...AUTH | egrep '(AUTH|rv1.*IN NSEC3)'
;; AUTHORITY SECTION:
rv1glegdcruclq64jr4tqem1u0eaefba.dk. 3600 IN NSEC3 1 1 17
092EF3E7975CB1EE S3F532FN55ASTA3MVMTGEIG80S12G8PC NS DS RRSIG
SHA-1 (alg. 1)
Opt-out bit set
17 iterations

NSEC3PARAM

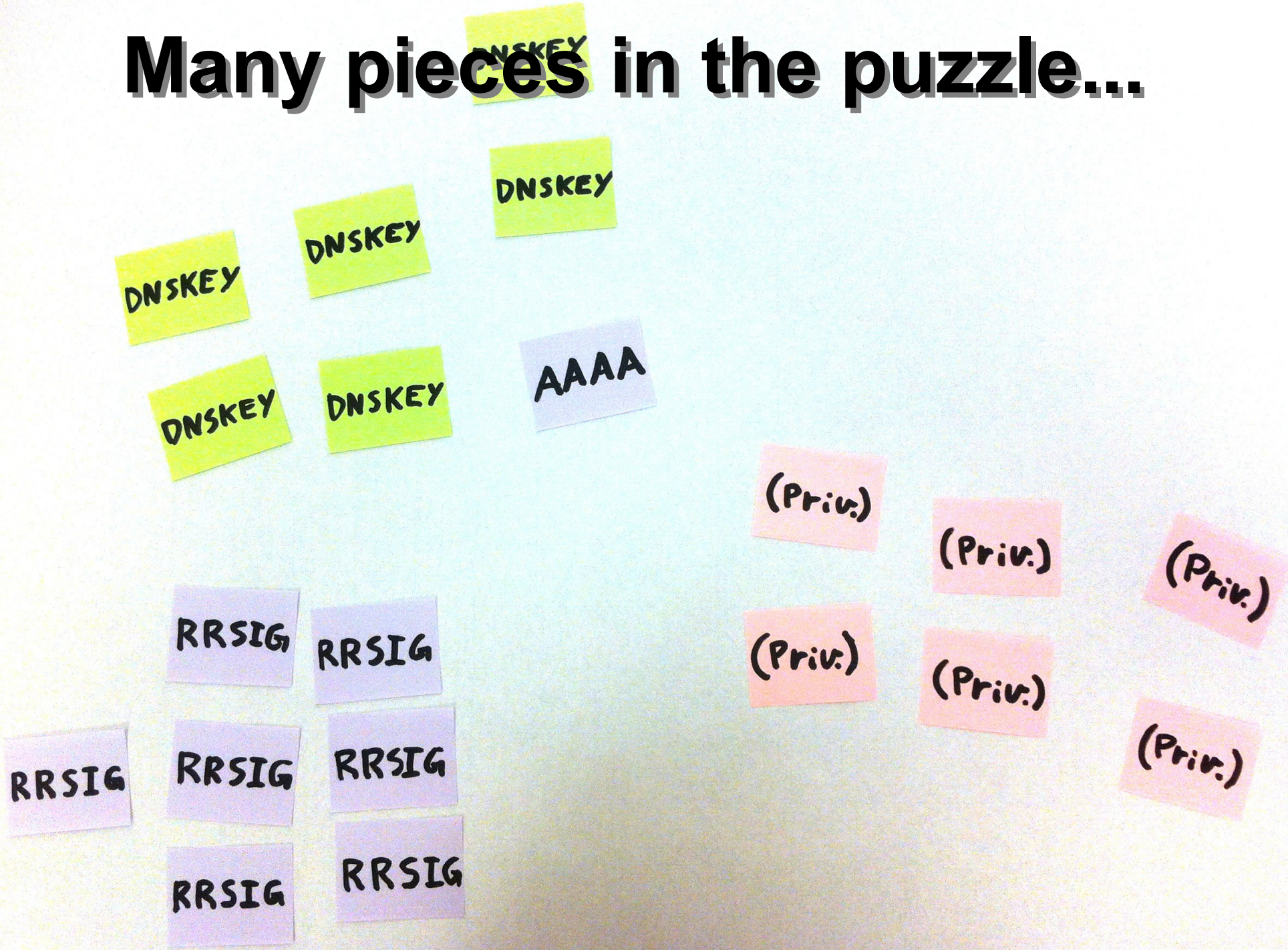
The RDATA of the NSEC3PARAM RR is as shown below:



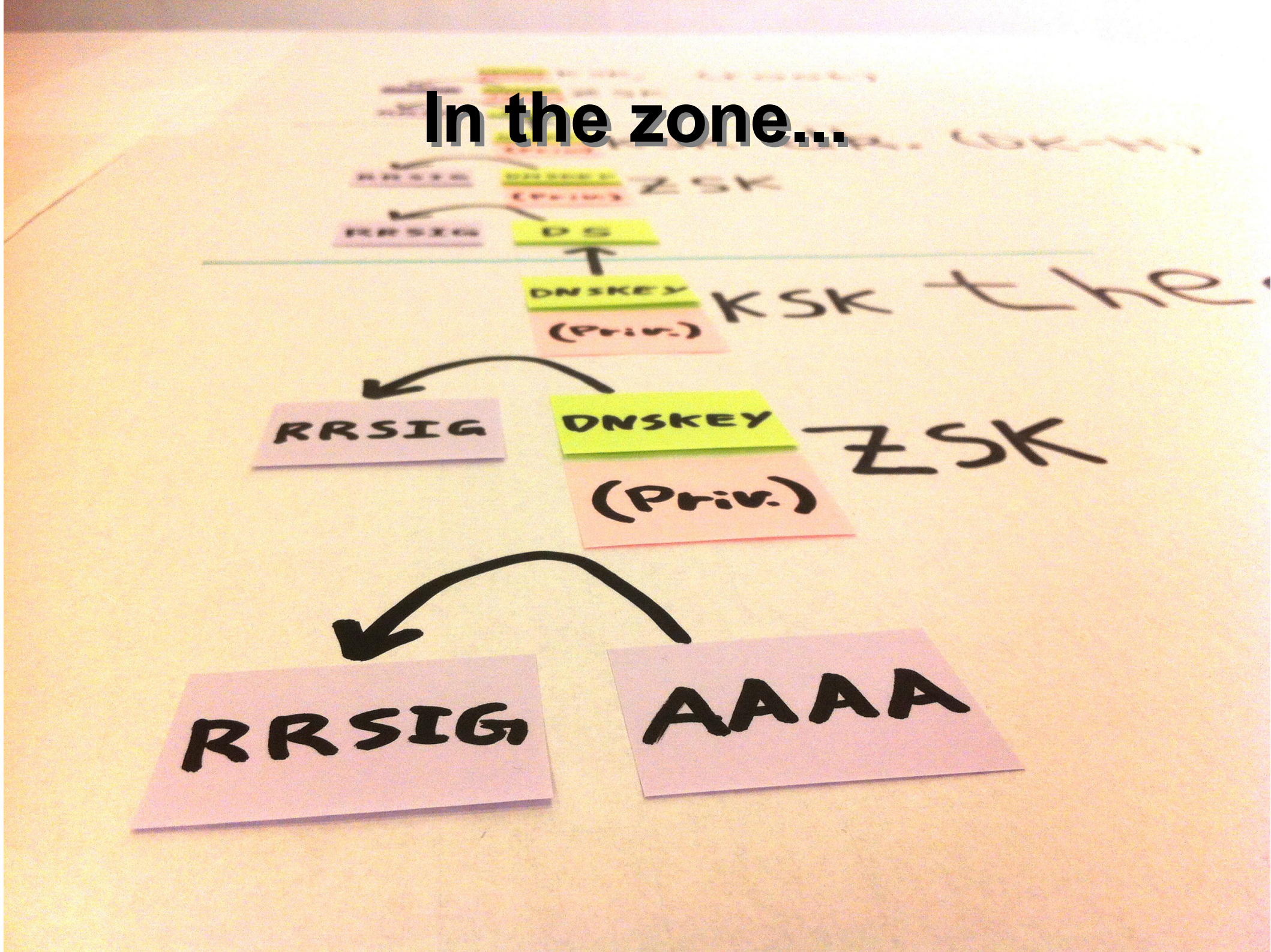

```
$ dig @b.nic.dk dk. nsec3param | tr '\t' ' ' | grep -A 1 ^...ANSWER
;; ANSWER SECTION:
dk.   3600 IN NSEC3PARAM 1 0 17 092EF3E7975CB1EE
```

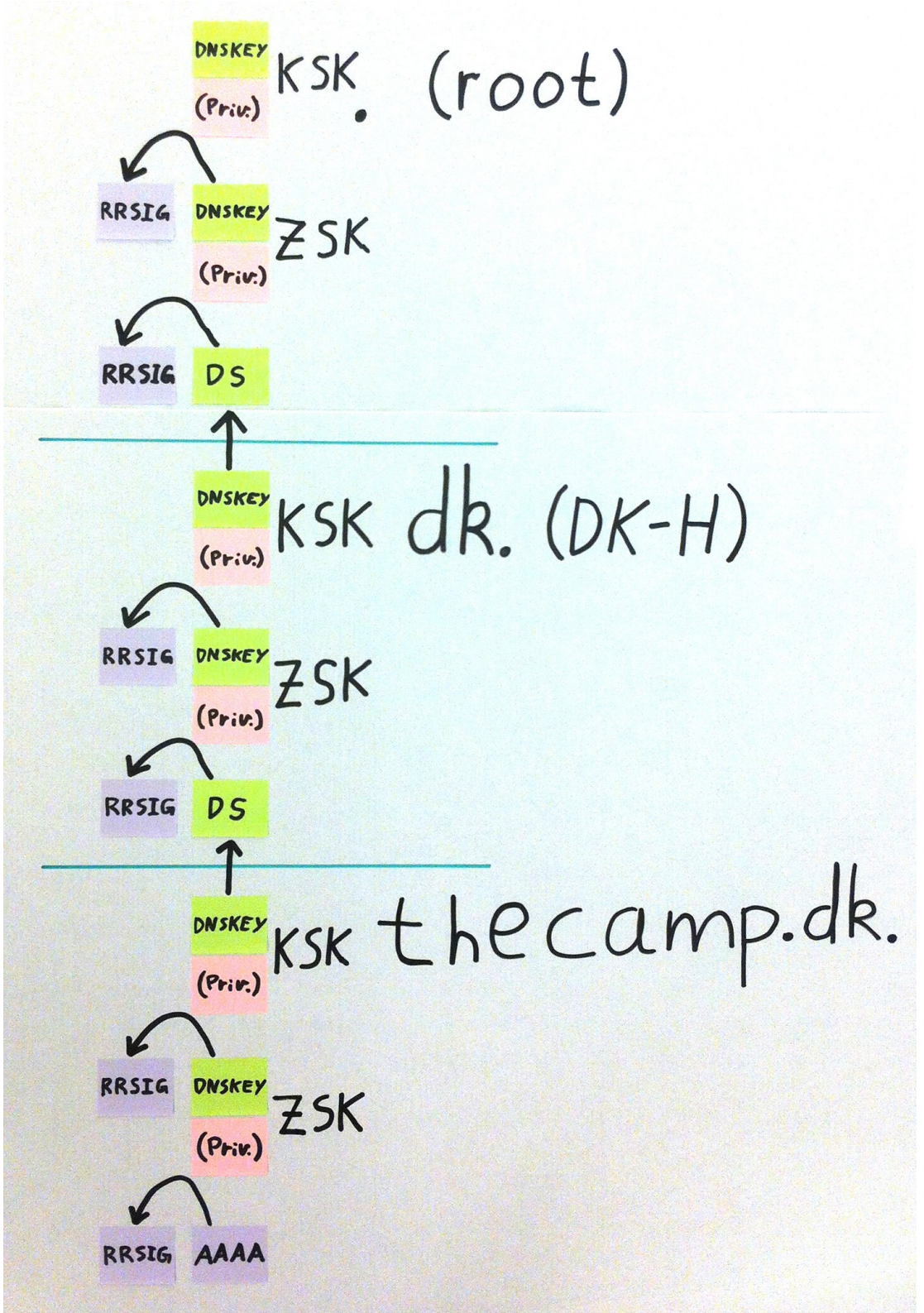
Source: RFC 5155

Many pieces in the puzzle...



In the zone...




DNSKEY
(Priv.)
KSK .
(root)
RRSIG
DNSKEY
(Priv.)
ZSK
RRSIG
DS
DNSKEY
(Priv.)
KSK dk.
(DK-H)
RRSIG
DNSKEY
(Priv.)
ZSK
RRSIG
DS
DNSKEY
(Priv.)
KSK thecamp.dk.
RRSIG
DNSKEY
(Priv.)
ZSK
RRSIG
AAAA

New headers flags and bits

- DNS header flags:
  - Checking Disabled (CD)
    Client says: ”Please to not perform DNSSEC validation”
  - Authenticated Data (AD)
    Client says: ”Please tell me whether all answer and authority data has been validated”
- Extension mechanisms for DNS (EDNS) header bits:
  - DNSSEC OK (DO)
    A resolver can indicate that it wishes to receive DNSSEC RRs in response messages
- EDNS0 is the first set of EDNS
  - From 512 byte to 4 kB packets, among other things...
- DNSSEC requires the possibility for larger packets

Support in dig

```
$ man dig | grep -B 1 -A 1 -i checking
       +[no]cdflag
           Set [do not set] the CD (checking disabled) bit in the query. This
           requests the server to not perform DNSSEC validation of responses.
```

```
$ man dig | grep -B 1 -A 6 -i 'authentic data'
       +[no]adflag
           Set [do not set] the AD (authentic data) bit in the query. This
           requests the server to return whether all of the answer and
           authority sections have all been validated as secure according to
           the security policy of the server. AD=1 indicates that all records
           have been validated as secure and the answer is not from a OPT-OUT
           range. AD=0 indicate that some part of the answer was insecure or
           not validated.
```

Maintenance

- The more data, a key signs, the more exposed the key is
- KSK switched e.g. every year
- ZSK switched e.g. every week
- As ZSK is switched more often, it can be shorter, yielding smaller DNSKEY/RRSIG RRs
- Key rolling/rollover is the process of switching keys
- Complicated – you don't want to do it by hand

Bind as a recursive caching name server

```
Options {
...
 dnssec-enable yes;
 dnssec-validation yes;
 dnssec-lookaside auto;
}
```

DNSSEC as an authorative name server

- Three approaches
  - GratisDNS.dk (or similar services)
  - Bind >= 9.9
  - OpenDNSSEC


Intet SIM-kort
web.gratisdns.dk/?q=node/105
Google
Larsen Data ApS
GratisDNS
Login
Domæne
SSL
Hosting
Prisliste
Support
Kontrolpanel
Om os
DNS
Europa
Amerika
Afrika
Asien/Pacific
gTLD
Køb domæne
Flyt domæne
Forny domæne
DNS
Vi sætter en ære i at levere Danmarks teknisk bedste DNS service, vel og mærke helt gratis. Vores setup er blandt de større set i norden og lever op til sidste nye RFC'er og sikkerhedsstandarder. Vores servere anvender forskellige operativsystemer, kører alle med både IPv4 og IPv6 og har understøttelse for DNSSEC.
GratisDNS har 5 navneservere, men reelt dækker det over mere end 44 forskellige servere.
NS1.gratisdns.dk
Hostet i vores eget racks hos Interxion i Ballerup. Interxion har datacentre over hele Europa og er en af de største datacenter leverandører i Europa. Linien er sponsoreret af Solido Networks. Solido Networks hoster og leverer også linie til danmarks eneste root dns server.
NS2.gratisdns.dk
Hostet hos softlayer i Washington
NS3.gratisdns.dk
Hostet af CommunityDNS på deres Anycast 1, med over 40 servere spredt ud over hele verden. F.eks. Ballerup, Wien, Singapore, Chicago, London, Kiev, Bruxelles og mange andre steder. Se evt: http://communitydns.eu/map/
Antal brugere ialt: 51742
Antal domæner ialt: 240782
1. dk 178787
2. com 20212
3. net 5915
4. eu 5605
5. org 3717
6. se 3598
7. info 2674
8. no 2081
9. nu 1836
10. de 998
11. biz 850
12. fo 600
13. gl 465
14. uk 451
15. pl 413
16. es 366

DNS kontrolpanel

Logud | ReLogin | Opret ny bruger | Info | DNS ordbog | Sikkerhed

Bruger Setup | Primær DNS | Sekundær DNS | Registrar | IPv4 rDNS | IPv6 rDNS

System besked:
Primær DNS domæner

hal9k.dk	Ændre DNS	Whois	Tilkøbs produkter	DNSSEC	SLET DNS

Antal domæner: 1

Nyt domæne der skal have både primær og sekundær DNS:

nytprimærtdomæne.dk

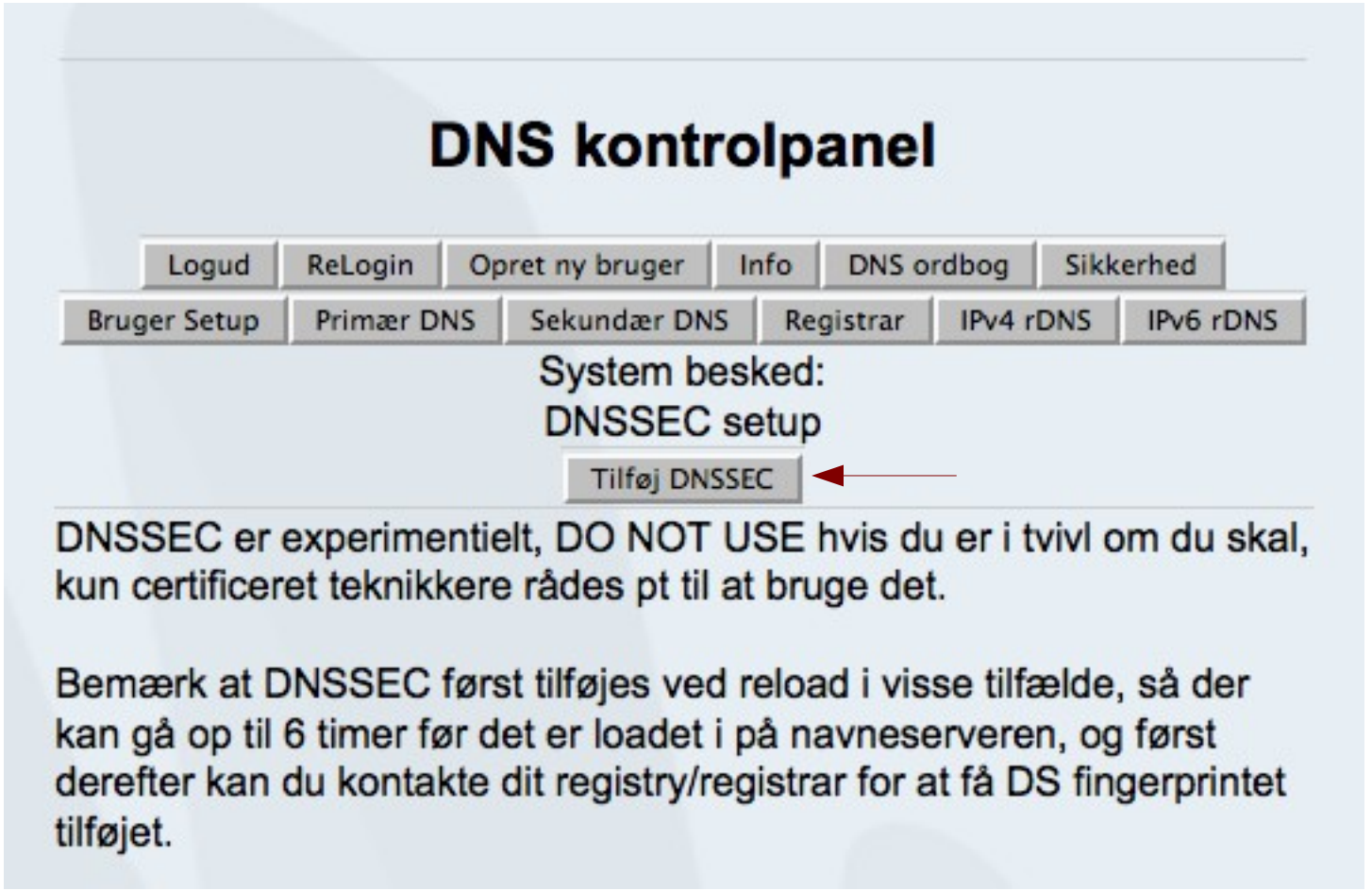
Opret primær & sekundær DNS for dette domæne

Ny template til domæner der skal have både primær og sekundær DNS:

Navn på template

Opret primær & sekundær DNS for denne template

Forklaring:
Du skal oprette dit domæne med primær og sekundær DNS, hvis du ikke har DNS til dit domæne i


DNS kontrolpanel
Logud
ReLogin
Opret ny bruger
Info
DNS ordbog
Sikkerhed
Bruger Setup
Primær DNS
Sekundær DNS
Registrar
IPv4 rDNS
IPv6 rDNS
System besked:
DNSSEC setup
Tilføj DNSSEC
DNSSEC er experimentielt, DO NOT USE hvis du er i tvivl om du skal, kun certificeret teknikkere rådes pt til at bruge det.
Bemærk at DNSSEC først tilføjes ved reload i visse tilfælde, så der kan gå op til 6 timer før det er loadet i på navneserveren, og først derefter kan du kontakte dit registry/registrar for at få DS fingerprintet tilføjet.

DNS kontrolpanel

Logud | ReLogin | Opret ny bruger | Info | DNS ordbog | Sikkerhed

Bruger Setup | Primær DNS | Sekundær DNS | Registrar | IPv4 rDNS | IPv6 rDNS

System besked:

DNSSEC setup (tilføjer til domæne)

DNSSEC er tilføjet/opdateret på zonen Hvis der eksisterede mere end 2 ZSK nøgler, og disse ZSK nøgler er mere end 14 dage gamle, så er de nu fjernet.

DNSSEC tilføjelsen kommer senest med på næste reload (dette sker hver 6. time). Det er vigtigt at efter dette reload skal du kontakte din Registrar/Registryet for at tilføje DS recorden hos TLD'et. Bemærk at kun følgende TLD'er er DNSSEC aware: .se, .br, .cz, .bg, .org og få andre.

Er din registrar Larsen Data, så vil vi i de fleste tilfælde kunne tilføje din DS record helt gratis, skriv til os på support@gratisdns.dk. Bemærk at du kun ved NYOPRETTELSE af DNSSEC skal kontakte os, da det er KSK nøglen der laver DS recorden, som registyet skal have.. dette gøres kun en gang.På .dk domæner skal du selv opdatere DS KSK nøgle hos DK-Hostmaster. Vi yder kun support på dette mod betaling.

For at få informationerne om DS records, og de andre værdier du skal bruge til DK-Hostmaster site, så skal du vende tilbage til DNSSEC siden for hvert enkelt domæne, efter næste reload. Siden vil da vise de nøjagtige informationer du skal tilføje hos DK-Hostmaster, eller din registrar.
Har du Spørgsmål til hvordan du angiver nøglen hos DK-Hostmaster, så skal du ringe på 33646060.

DNS kontrolpanel

Logud | ReLogin | Opret ny bruger | Info | DNS ordbog | Sikkerhed

Bruger Setup | Primær DNS | Sekundær DNS | Registrar | IPv4 rDNS | IPv6 rDNS

System besked:
DNSSEC setup

Domæne: hal9k.dk
Nøgle-ID:
Algoritme:
Hashingalgoritme:
Hash:

Information will appear after up to 6 hours

Hvis du IKKE ser nogle værdier ovenover, så er det fordi din DNSSEC nøgle IKKE er i DNS endnu!

Er du ved at sætte DNSSEC på et .dk domæne, så ret spørgsmål til hvordan du indtaster og opdaterer dette på tlf: 33646060, tak!

DNSSEC på andre TLD'er skal du kontakte din registrar, de kan MÅSKE hjælpe dig med at sætte disse informationer i et interface..
Hvis det IKKE er muligt, kan dit domæne blive utilgængeligt pga keyoftrust er brudt! Be aware!
Support på DNSSEC faktureres af Larsen Data med minimum 1 teknikker supporttime.

Ny ZSK nøgle til DNSSEC

Fjern DNSSEC

DNSSEC er experimentielt, DO NOT USE hvis du er i tvivl om du skal, kun certificeret teknikkere rådes pt til at bruge det.

Bemærk at DNSSEC først tilføjes ved reload i visse tilfælde, så der kan gå op til 6 timer før det er loadet i på navneserveren, og først derefter kan du kontakte dit registry/registrar for at få DS fingerprintet tilføjet.

Bind and DNSSEC

- Bind 9.9: A subset of the functionality that OpenDNSSEC offers.
  - E.g. no automatic key rollover
  - Automatic signing of zones
  - More features may (very likely?) come in the future

Bind and DNSSEC

- named.conf on authorative name server

```
options {
…
key-directory "/var/bind/keys";
Dnssec-enable yes;
}
```

Bind and DNSSEC

- For each zone

```
zone {
…
auto-dnssec maintain;
inline-signing yes;
}
```

Bind and DNSSEC

- Generate KSK

```
cd /var/bind/keys

key=$(dnssec-keygen -3 -a RSASHA256 -b
4096 -f KSK $zone)

dnssec-dsfromkey $key > $key.ds

chown named:named $key*
```

- Generate ZSK

```
dnssec-keygen -3 $zone

chown named:named K*
```

Bind and DNSSEC

- Upload to parent
  - dnssec-dsfromkey $keyfile
- Key rollover

Bind and DNSSEC

- That was way to easy and not feature rich enough, so lets move on to OpenDNSSEC :-)

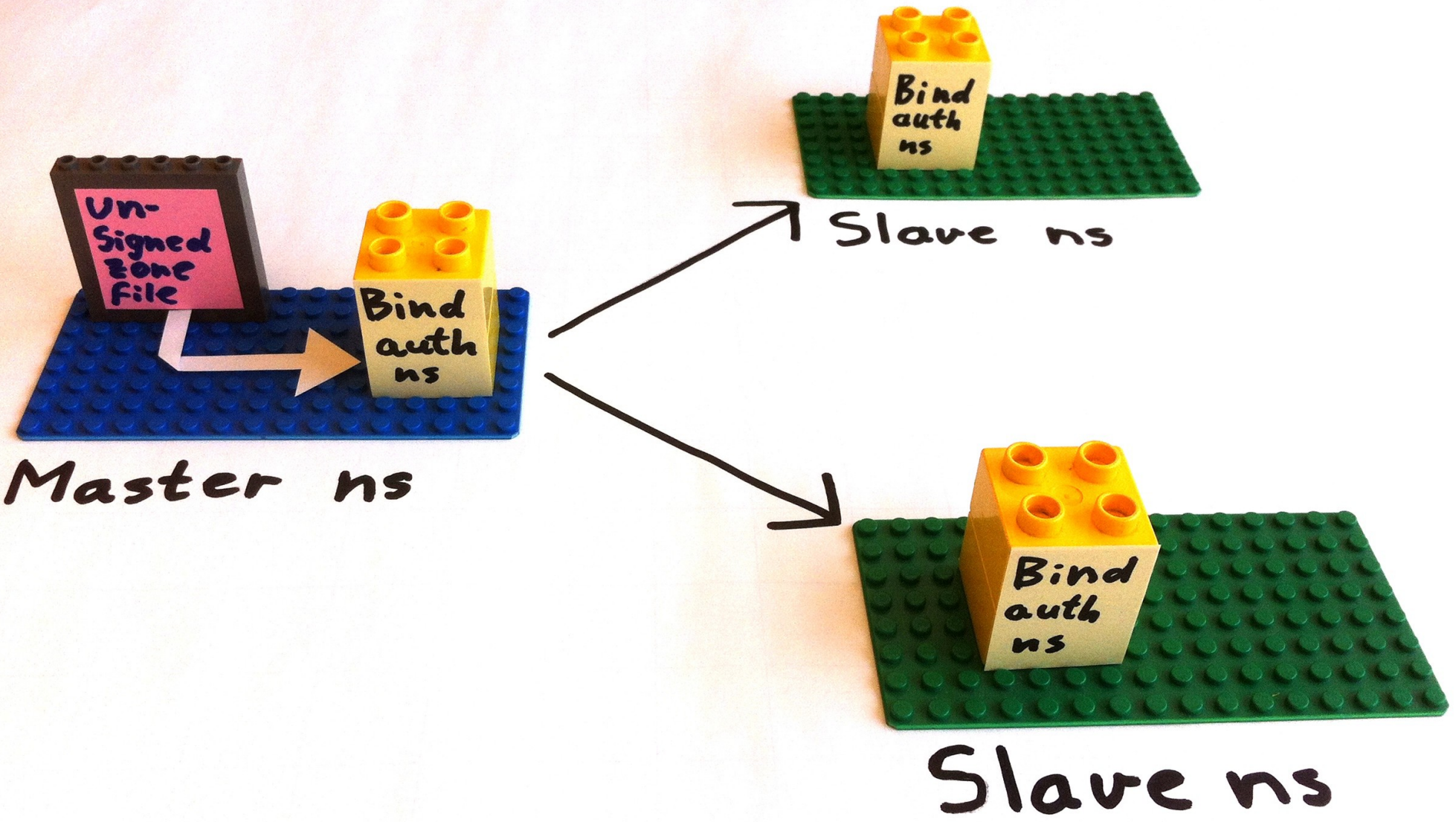
OpenDNSSEC

- What is OpenDNSSEC
- Why OpenDNSSEC
- Architecture
- Configuration
- Manual upload of keys to parent
- Validator
- HSM's (Hardware Security Module)

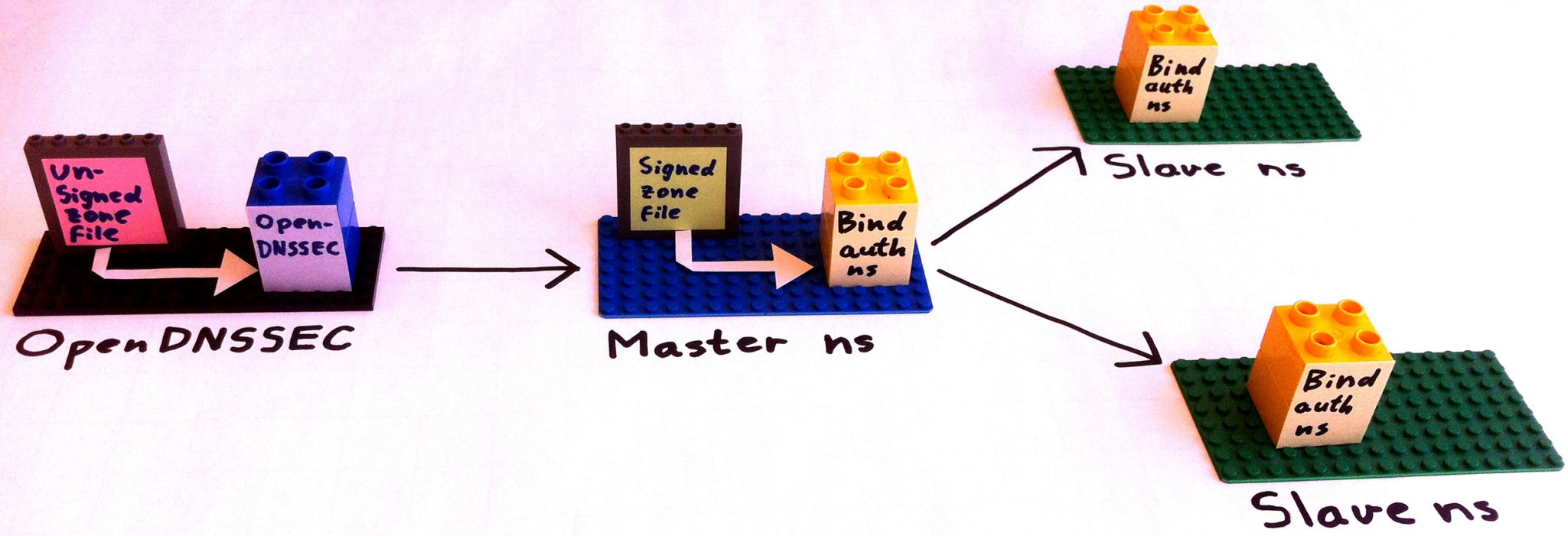
What is OpenDNSSEC

- OpenDNSSEC maintains the signing of your zones.
- It is not a name server
- Used by .se, .dk, .nl and .co.uk registries
- Originally a .se registry project but is now backed by, among other, the above registries.

Before DNSSEC


Un-
Signed
Zone
File
Bind
auth
ns
Master ns
Bind
auth
ns
Slave ns
Bind
auth
ns
Slave ns

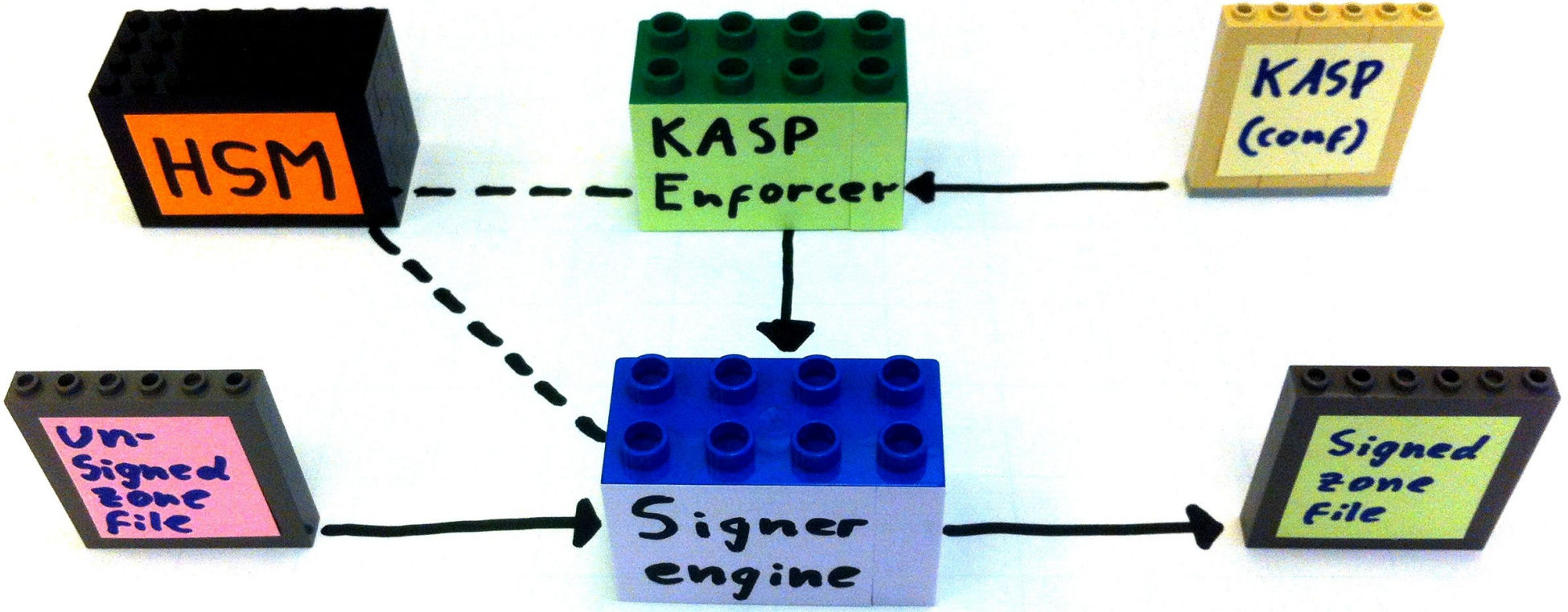
Introducing OpenDNSSEC


Un-
Signed
Zone
File
Open-
DNSSEC
OpenDNSSEC
Signed
Zone
File
Bind
auth
ns
Master ns
Bind
auth
ns
Slave ns
Bind
auth
ns
Slave ns

Why OpenDNSSEC

- Using Bind's tools does not take care of rolling keys (KSK, ZSK)
- OpenDNSSEC automating the process of keeping track of DNSSEC keys and the signing of zones
- Communication to parent zone (e.g. epp-client)
- Scalability (multiple threads, multiple HSM's)
- Security (HSM)

OpenDNSSEC architecture


HSM
KASP Enforcer
KASP (conf)
Un-Signed Zone File
Signer engine
Signed Zone File

KASP enforcer

- KASP: Key and Signature Policy
- Reads configuration (policy, list of domains etc.).
- Key management
  - Creation of keys in HSM
  - Key rolling
- Instructs what keys etc. ods-signer should use

Key rolling

ZSK key rolling
DK-Hostmaster
Parent zone
dk
DS
KSK
ZSK
ZSK
RRSIG
RRSIG
RRSIG
RRSIG
Your zone
thecamp.dk
DS

KSK
KEY ROLLING

DK-Hostmaster

Parent zone
dk

DS
KSK
ZSK
RRSIG
RRSIG

DS
KSK
ZSK
RRSIG
RRSIG

Your zone

the.rest.dk

HSM

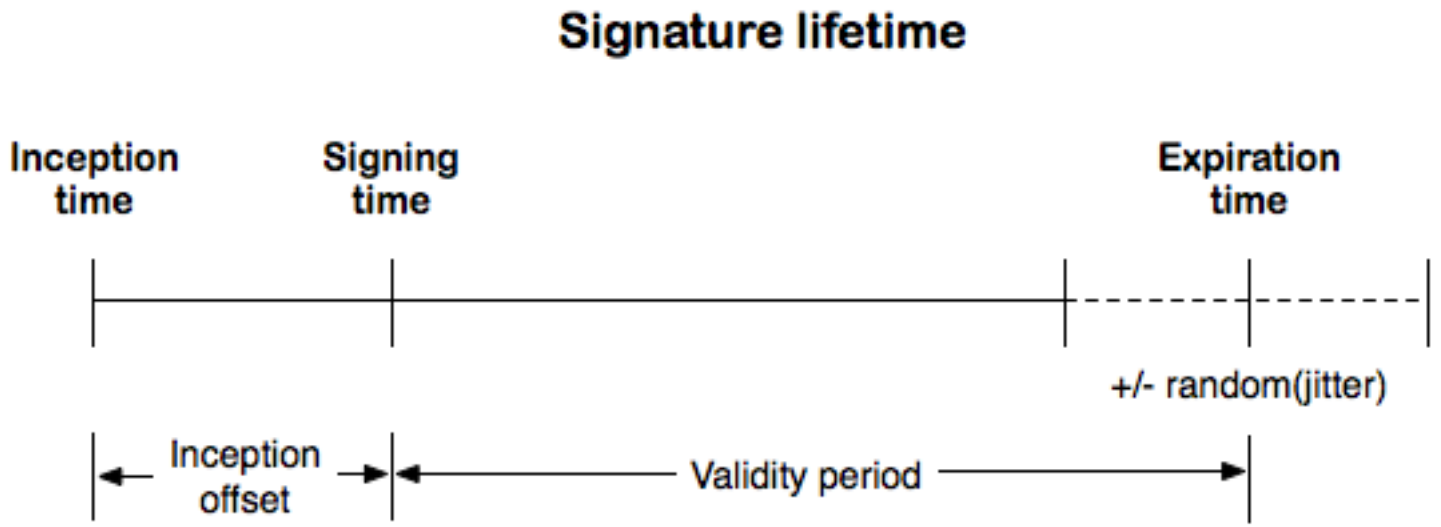
- Hardware Security Module
  - Stores and generates keys
  - Signs records
  - Hardware accellerated signing and key generation
- PKCS#11 interface
- SoftHSM
  - No hardware required
  - Simple configuration
  - Developed for OpenDNSSEC
  - Not as über secure as some hardware based HSM's

Configuration files

- conf.xml
  - Overall configuration
- kasp.xml
  - Key and signature policy
- zonefetch.xml
  - Optional: Receive zones via AXFR
- zonelist.xml
  - List of zones, how to fetch and publish them and a pointer to policy in kasp.xml. Maintained by OpenDNSSEC, but manual editing is possible.

Signer engine

- Performs the actual signing
  - Reuses signatures if they are not too old
  - Can spread signature generation (jitter)



The above picture is copied from https://wiki.opendnssec.org/display/DOCS/kasp.xml with the copyright as indicated by the site.

- Maintains NSEC/NSEC3 chain
- Updates SOA serial number

Bind

- named.conf
  - `dnssec-enable yes;`
- Restart bind
- Configure firewall to accept 4096 Byte UDP-packets on port 53 due to EDNS0.

Installing and running OpenDNSSEC

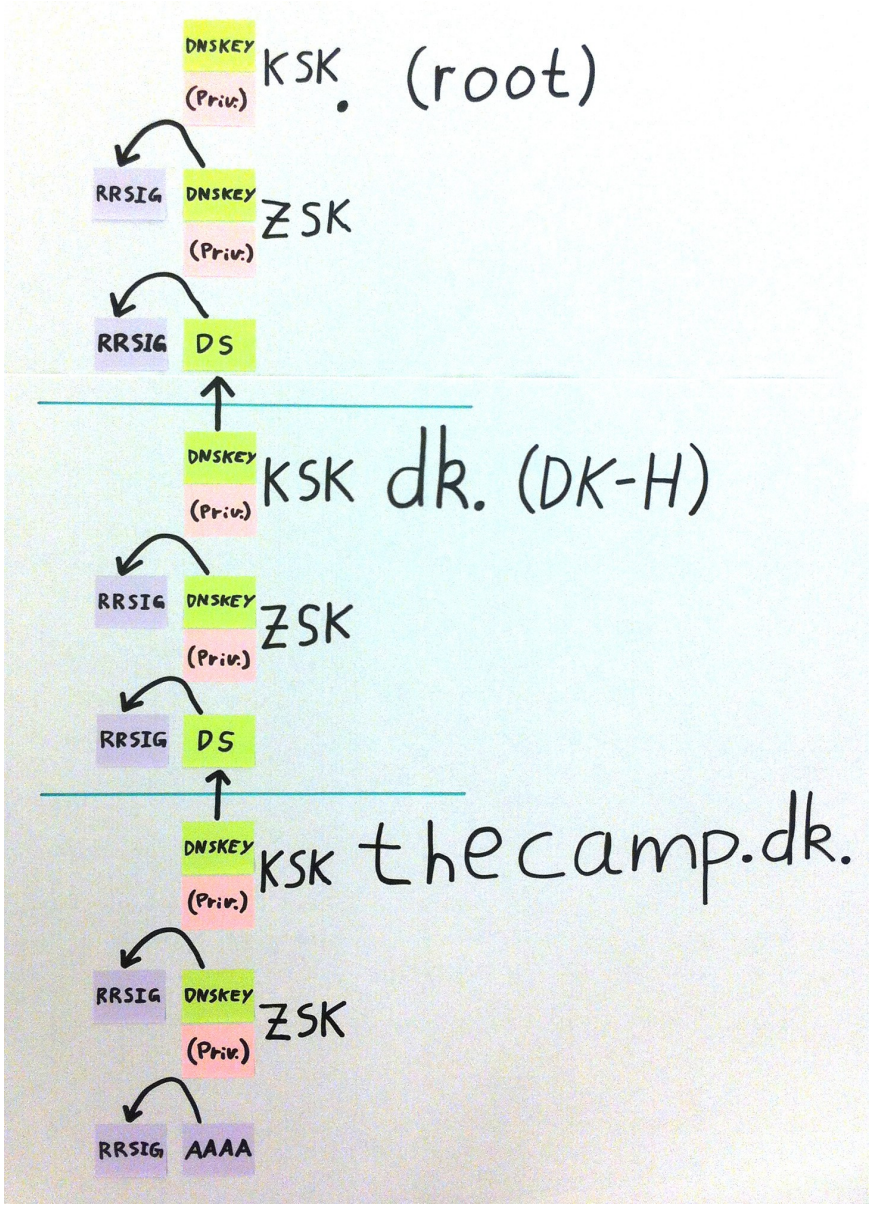
- Lets jump to the wiki
  - Will be put online together with the video as a .pdf

OpenDNSSEC Roadmap

- From verison 1.4 the KASP auditor is obsolete
  - We will show an example with validns
- Version 2.0: Support for passing through unsigned zones
- My wishlist:
  - Support for split horizon
    - https://issues.opendnssec.org/browse/OPENDNSSEC-232
    - “Please feel free to vote on this and add comments.”

Manual upload of DS to parent

Manual upload of DS to DK-Hostmaster

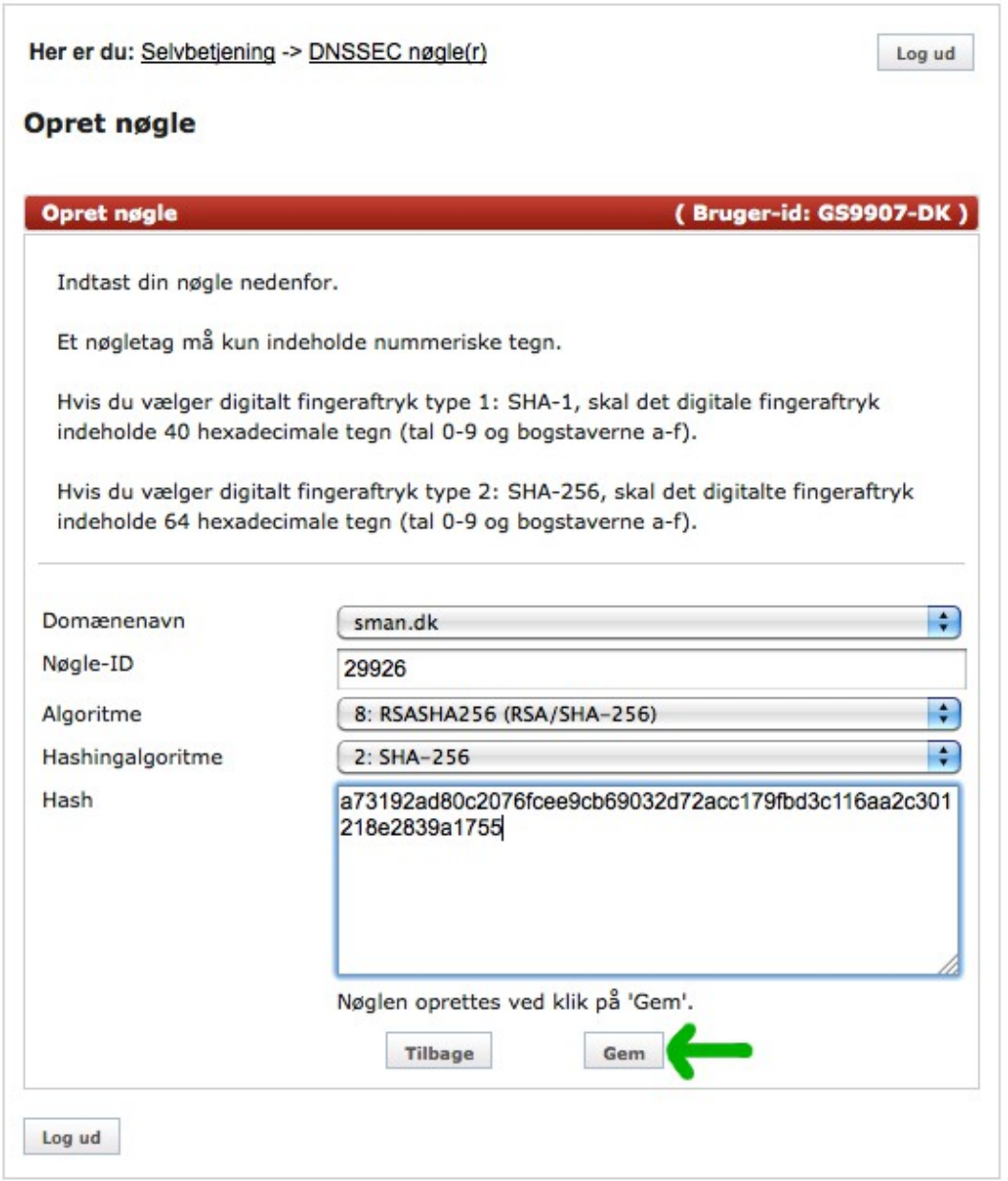


- To gain trust from parent (here DK-Hostmaster), go trhough the following steps:
  - Get DS keys from OpenDNSSEC
  - Log in to https://www.dk-hostmaster.dk and inser DS key

Manual upload of DS keys to DK-Hostmaster

Manual upload of DS to DK-Hostmaster

Manual upload of DS to DK-Hostmaster

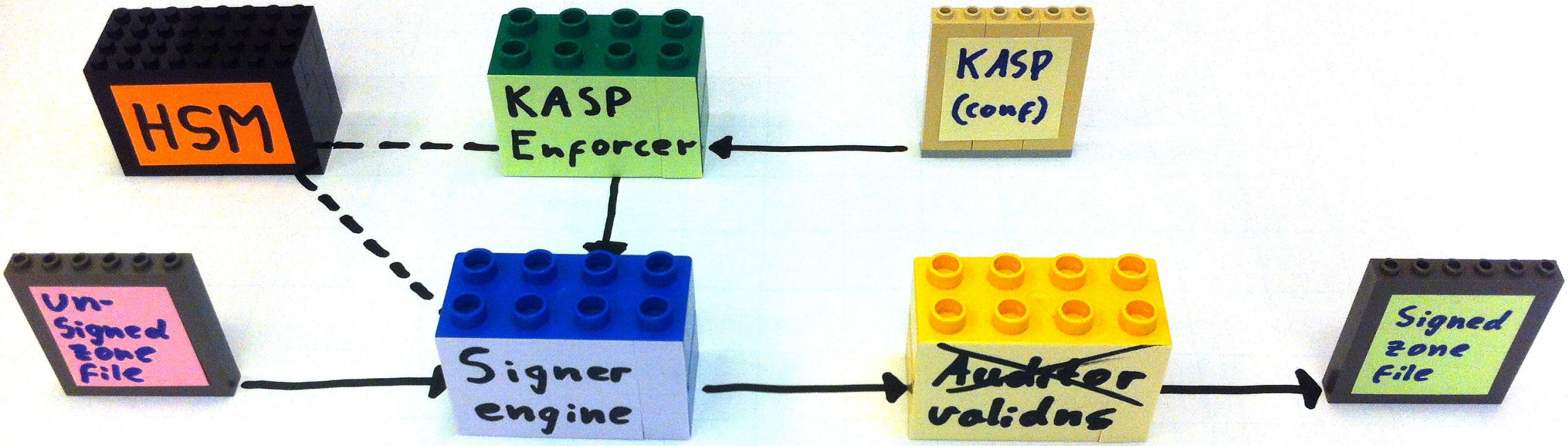


Manual upload of DS to DK-Hostmaster

Manual upload of DS to DK-Hostmaster

```
dig +dnssec sman.dk. DS @c.nic.dk | grep -v ';'


sman.dk.    86400 IN  DS  29926 8 2
A73192AD80C2076FCEE9CB69032D72ACC179FBD3C116AA2C3
01218E2 839A1755
sman.dk.    86400 IN  RRSIG DS 8 2 86400
20120730120851 20120723200442 37626 dk.
BIAt9QxZxbtOiXdK+dt2YizOsZXa+GBKRbaKvQAsRyilYUExB
SAcjcPK
bruVhcqop01W5l7xJrXGNtH+fx1lbbl6+CB1o9gq0a98z0GdU
+7aqDfz
FEcPg9rf8i600DbLwUsQEyLnqUG8KqPGDU3+YGsv6uNCQnsfp
h8L//Om TvU=
```

Validation of zone files


HSM
KASP Enforcer
KASP (conf)
Un-signed zone file
Signer engine
Auditor validns
Signed zone file

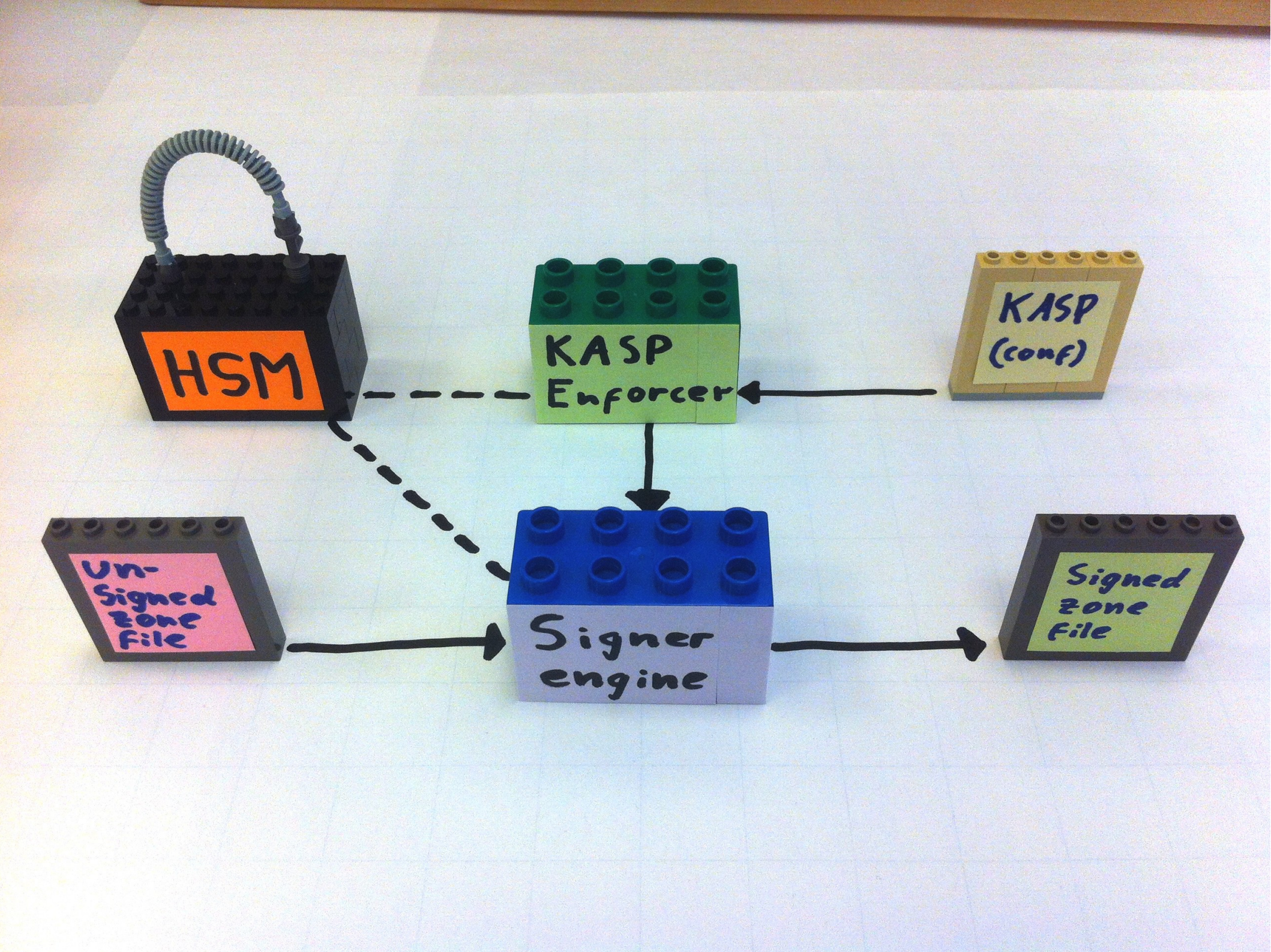
validns

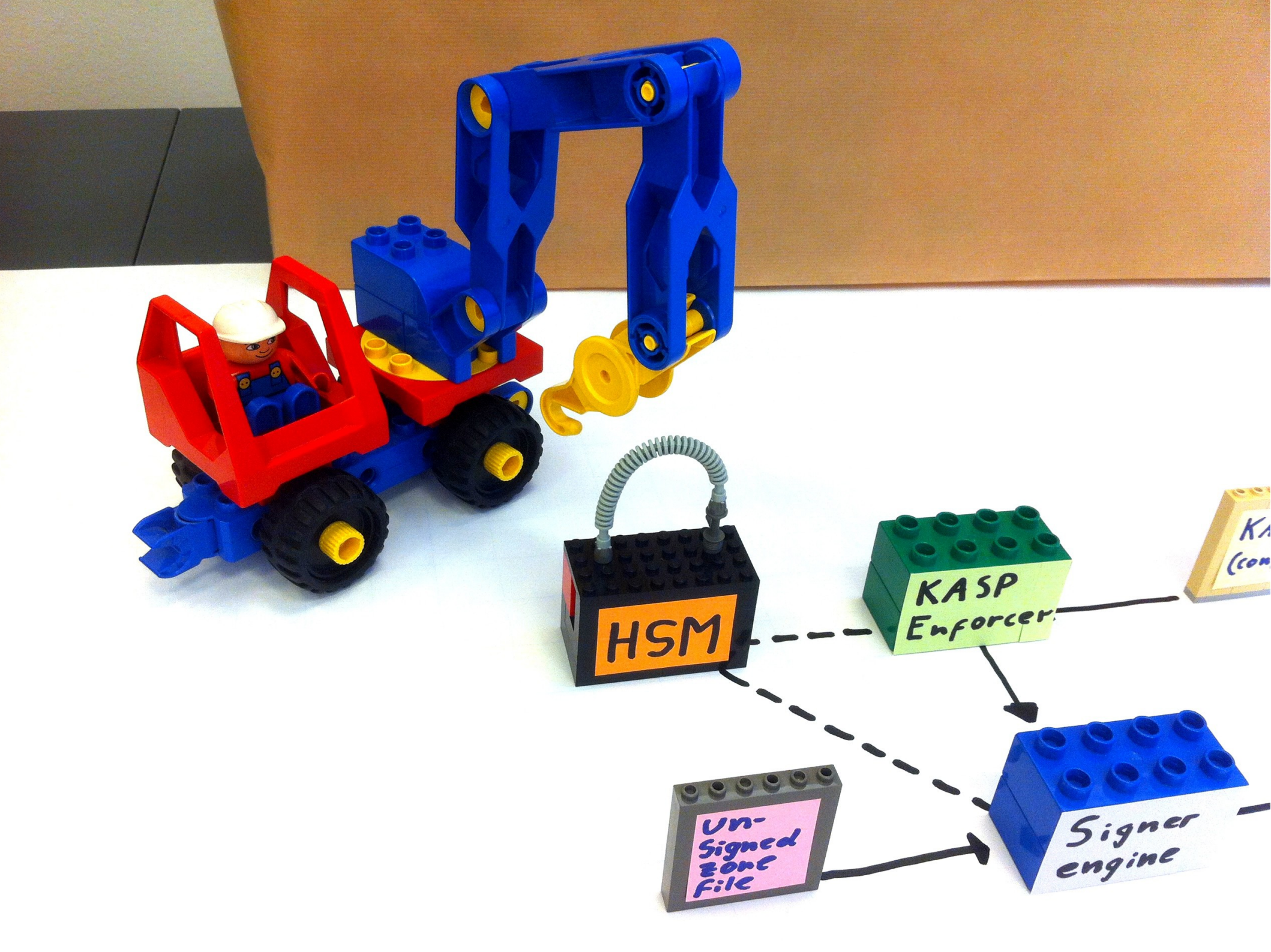
- http://www.validns.net
- Used by several major DNS operators
- Check syntax and more
- Checks for valid DNSSEC signatures, NSEC{,3} chains, outdated signatures etc.
- Not checking delegations
- Reads local files
- Written in C and scales well. Uses OpenSSL.
- Similar software: See also http://yazvs.verisignlabs.com/

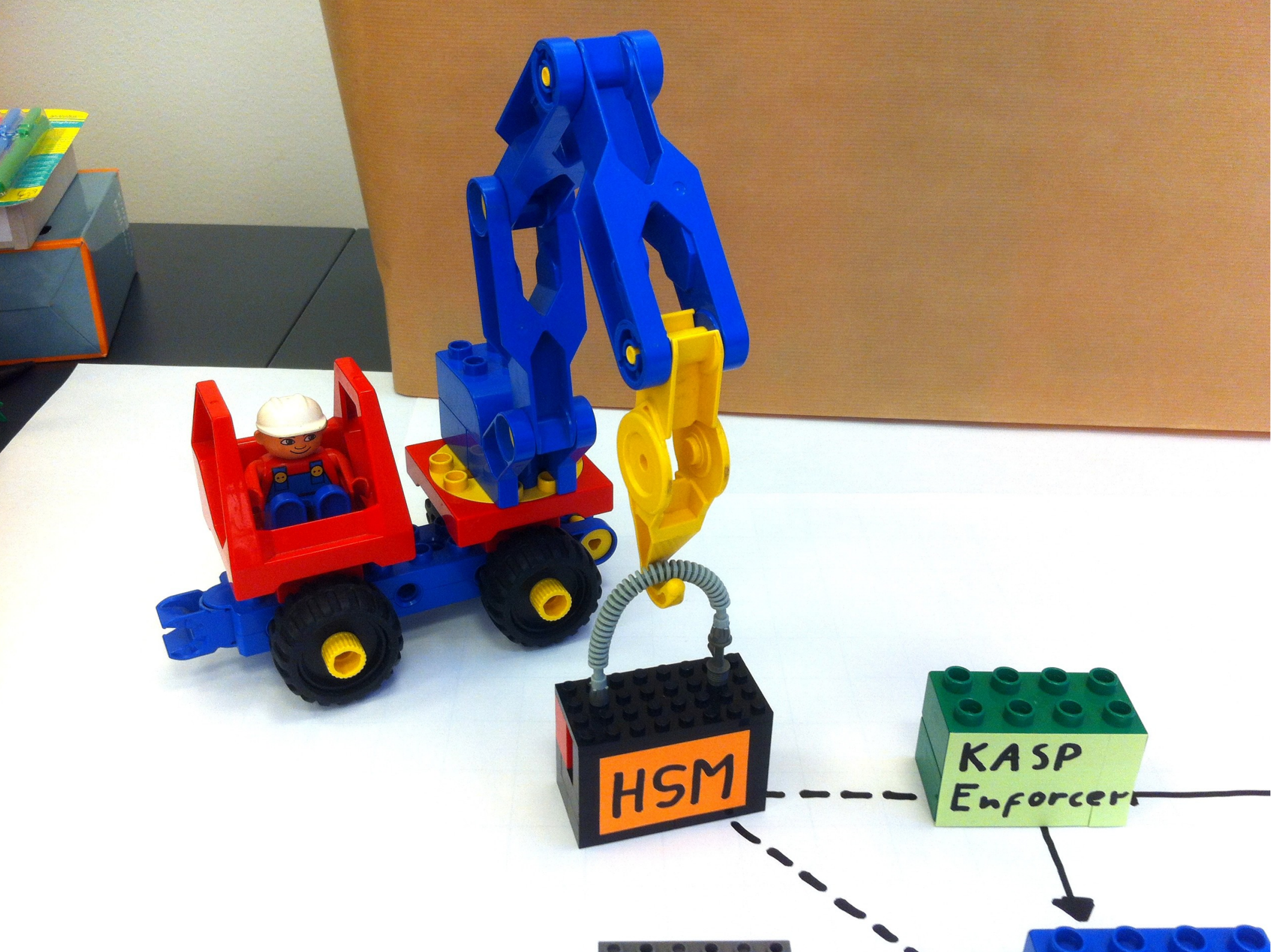
Demonstration

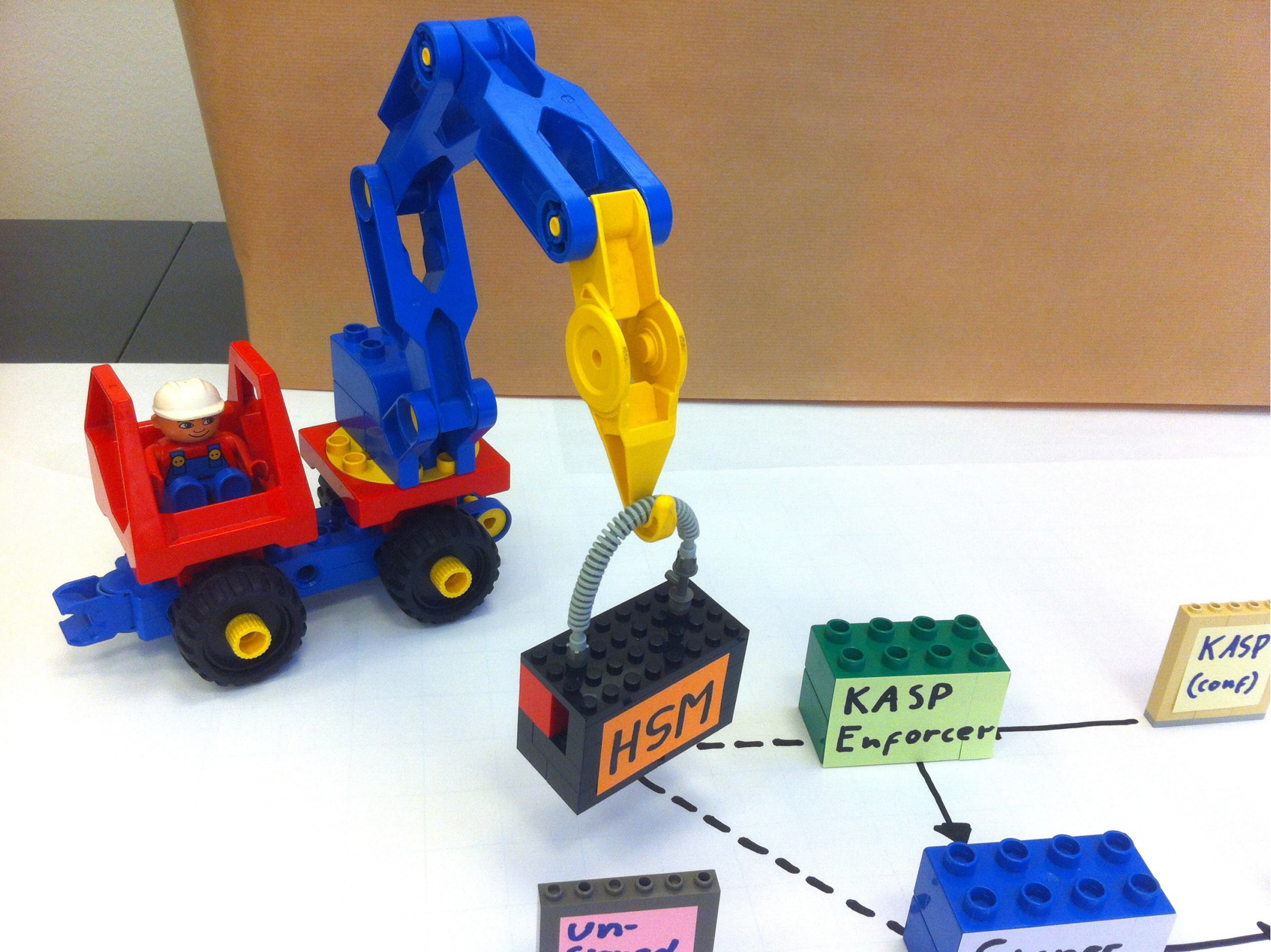
- Lets have a look at a server running OpenDNSSEC

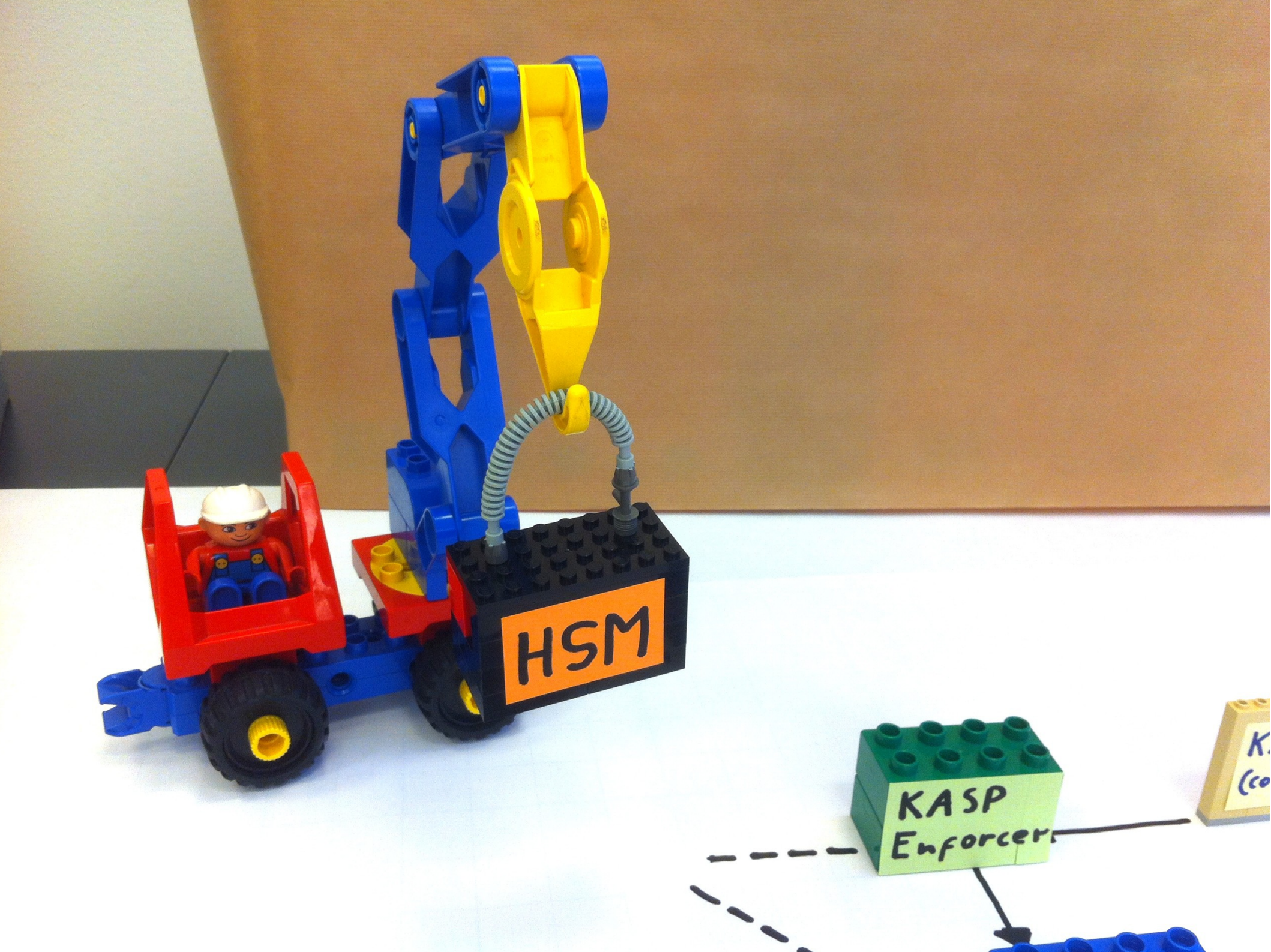
Let's have a closer look at hardware based HSM's


HSM
KASP Enforcer
KASP (conf)
Un-Signed Zone File
Signer engine
Signed Zone File


HSM
KASP Enforcer
Un-Signed zone File
Signer engine


HSM
KASP
Enforcer


HSM
KASP
Enforcer
KASP
(conf)


HSM
KASP
Enforcer


HSM


HSM

HSM

- SoftHSM
- Cheap solution (~200 DKK):
  - http://www.gooze.eu/feitian-pki-smartcard-ftcos-pk-01c
    - http://www.ewak.net/blog/?p=101
- More expencive:
  - SafeNet Luna SA
    - Faster, more secure
- See also:
  - https://wiki.opendnssec.org/display/DOCREF/HSM+Buyers%27+Guide


GEMPLUS

Fetition PKI

- Feitian PKI smartcard (FTCOS / PK-01C)
  - http://www.gooze.eu/feitian-pki-smartcard-ftcos-pk-01c
    - http://www.ewak.net/blog/?p=101


SafeNet
1
2

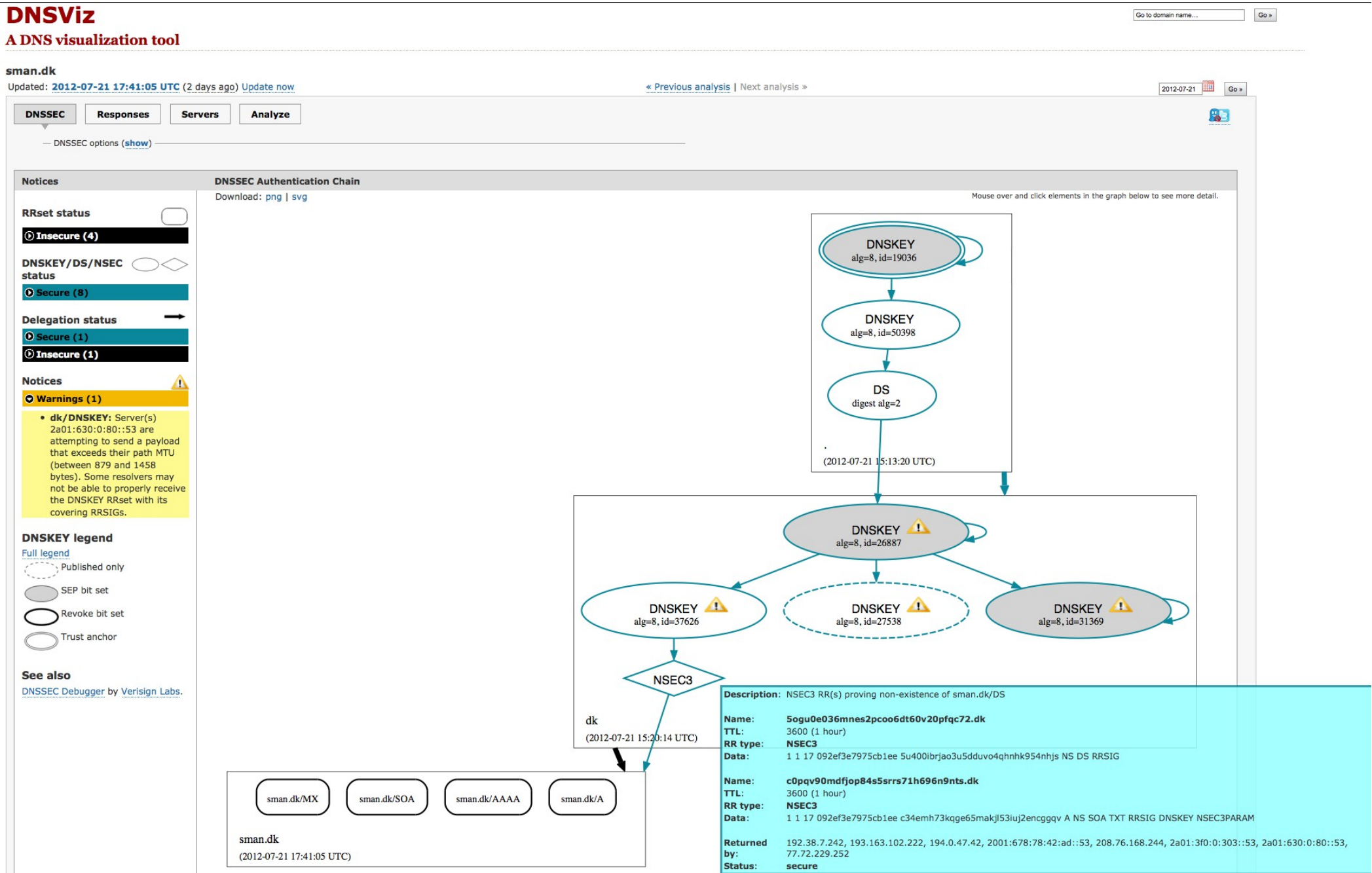
Luna SA

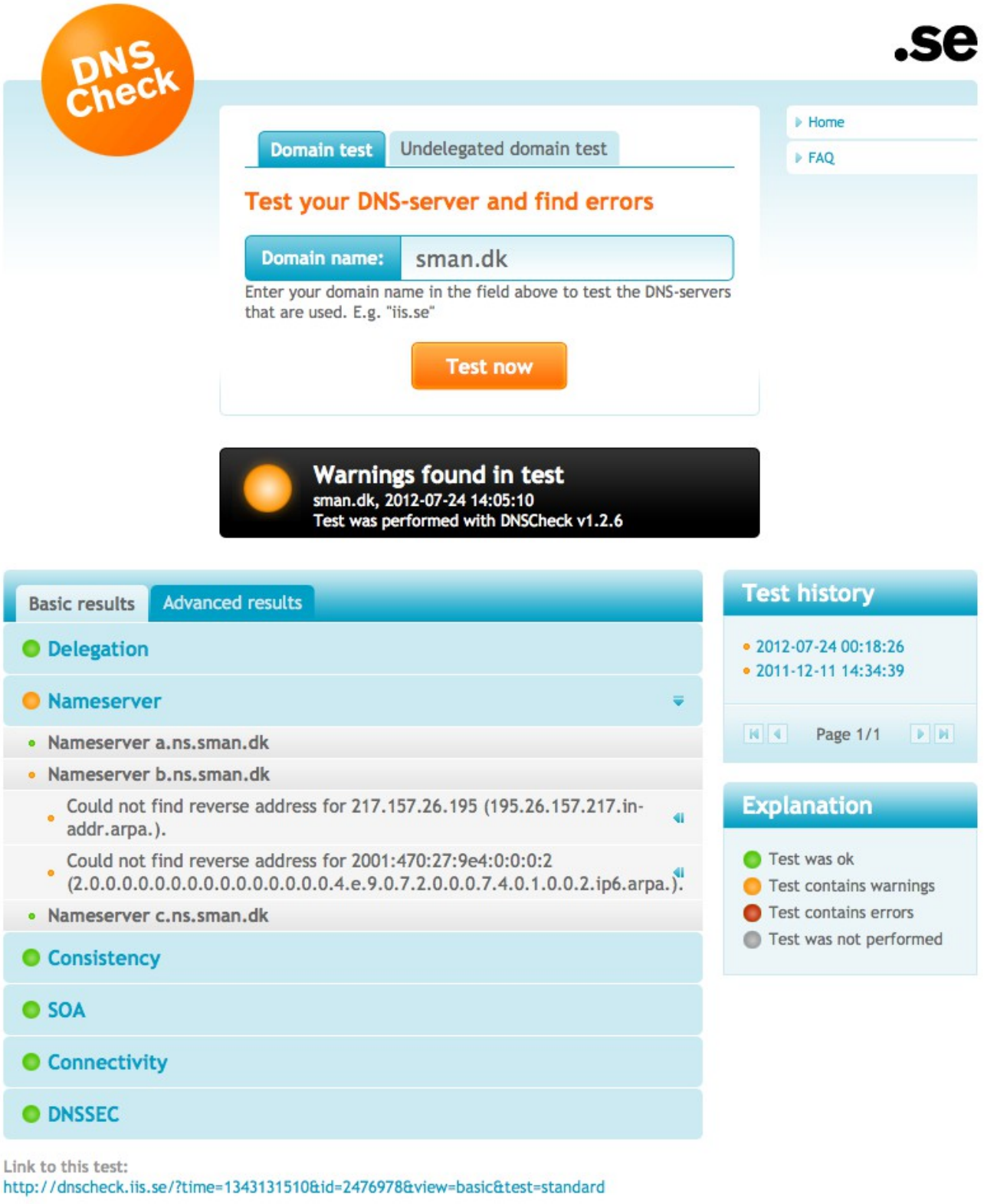
- Luna SA
  - FIPS 140-2 Level 3
    - Level 3 – includes requirements for tamper detection/resistance, data zeroisation, splitting user roles
    - Note that operating a HSM in FIPS 140-2 level 3 or higher mode may impose restrictions on on-board key generation through the PKCS #11 API that may be incompatible with OpenDNSSEC.
  - http://www.safenet-inc.com/products/data-protection/hardware-security-modules/luna-sa/

Debugging/validation

- Zone verification (we covered that earlier)
  - ods-validator
  - validns
  - yazvs
- Online tools
  - http://dnsviz.net
  - http://dnscheck.iis.se
  - http://dnssec-debugger.verisignlabs.com

dnsviz.net


DNSViz
A DNS visualization tool
Go to domain name...
Go »
sman.dk
Updated: 2012-07-21 17:41:05 UTC (2 days ago) Update now
« Previous analysis | Next analysis »
2012-07-21
Go »
DNSSEC
Responses
Servers
Analyze
DNSSEC options (show)
Notices
RRset status
Insecure (4)
DNSKEY/DS/NSEC status
Secure (8)
Delegation status
Secure (1)
Insecure (1)
Notices
Warnings (1)
dk/DNSKEY: Server(s) 2a01:630:0:80::53 are attempting to send a payload that exceeds their path MTU (between 879 and 1458 bytes). Some resolvers may not be able to properly receive the DNSKEY RRset with its covering RRSIGs.
DNSKEY legend
Full legend
Published only
SEP bit set
Revoke bit set
Trust anchor
See also
DNSSEC Debugger by Verisign Labs.
DNSSEC Authentication Chain
Download: png | svg
Mouse over and click elements in the graph below to see more detail.
DNSKEY
alg=8, id=19036
DNSKEY
alg=8, id=50398
DS
digest alg=2
.
(2012-07-21 15:13:20 UTC)
DNSKEY
alg=8, id=26887
DNSKEY
alg=8, id=37626
DNSKEY
alg=8, id=27538
DNSKEY
alg=8, id=31369
NSEC3
dk
(2012-07-21 15:20:14 UTC)
sman.dk/MX
sman.dk/SOA
sman.dk/AAAA
sman.dk/A
sman.dk
(2012-07-21 17:41:05 UTC)
Description: NSEC3 RR(s) proving non-existence of sman.dk/DS
Name: 5ogu0e036mnes2pcoo6dt60v20pfqc72.dk
TTL: 3600 (1 hour)
RR type: NSEC3
Data: 1 1 17 092ef3e7975cb1ee 5u400ibrjao3u5dduvo4qhnhk954nhjs NS DS RRSIG
Name: c0pqv90mdfjop84s5srrs71h696n9nts.dk
TTL: 3600 (1 hour)
RR type: NSEC3
Data: 1 1 17 092ef3e7975cb1ee c34emh73kqge65makjl53iuj2encggqv A NS SOA TXT RRSIG DNSKEY NSEC3PARAM
Returned by: 192.38.7.242, 193.163.102.222, 194.0.47.42, 2001:678:78:42:ad::53, 208.76.168.244, 2a01:3f0:0:303::53, 2a01:630:0:80::53, 77.72.229.252
Status: secure



dnscheck.iis.se

VERISIGN // LABS

dnssec-debugger.verisignlabs.com

Domain Name: sman.dk

Analyzing DNSSEC problems for sman.dk

.	✓ 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
dk	✓ Found 1 DS records for dk in the . zone ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=50398 and DNSKEY=50398 verifies the DS RRset ✓ Found 3 DNSKEY records for dk ✓ DS=26887/SHA256 verifies DNSKEY=26887/SEP ✓ Found 2 RRSIGs over DNSKEY RRset ✓ RRSIG=26887 and DNSKEY=26887/SEP verifies the DNSKEY RRset
sman.dk	✓ Found 1 DS records for sman.dk in the dk zone ✓ Found 1 RRSIGs over DS RRset ✓ RRSIG=37626 and DNSKEY=37626 verifies the DS RRset ⚠ Query to c.ns.sman.dk/87.51.64.235 for sman.dk/DNSKEY timed out or failed ✓ Found 2 DNSKEY records for sman.dk ✓ DS=29926/SHA256 verifies DNSKEY=29926/SEP ✓ Found 1 RRSIGs over DNSKEY RRset ✓ RRSIG=29926 and DNSKEY=29926/SEP verifies the DNSKEY RRset ✓ sman.dk A RR has value 77.243.53.201 ✓ Found 1 RRSIGs over A RRset ✓ RRSIG=25944 and DNSKEY=25944 verifies the A RRset

Monitoring

- Nagios plugins
  - http://exchange.nagios.org/directory/Plugins/Network-Protocols/DNS/check_dnssec/details
  - https://www.dnssec-deployment.org/wiki/index.php/Tools_and_Resources
  - https://www.dnssec-tools.org/wiki/index.php/Nagios_Plugin_and_Modifications

Host	Service	Status	Last Check	Duration	Attempt	Status Information
example.com/example.com	Donuts	OK	02-13-2012 11:26:41	3d 20h 30m 35s	1/3	example.com has no errors
	Zone Rollover	ROLLING	02-13-2012 11:26:40	0d 0h 17m 35s	1/3	ZSK Rollover Phase 3
ideal.com/ideal.com	Donuts	OK	02-13-2012 11:26:46	3d 20h 30m 29s	1/3	ideal.com has no errors
	Zone Rollover	ROLLING	02-13-2012 11:26:00	0d 0h 16m 15s	1/3	KSK Rollover Phase 3
instance.com/instance.com	Donuts	OK	02-13-2012 11:26:52	3d 20h 30m 23s	1/3	instance.com has no errors
	Zone Rollover	ROLLING	02-13-2012 11:26:40	0d 0h 5m 35s	1/3	ZSK Rollover Phase 1
model.com/model.com	Donuts	OK	02-13-2012 11:26:58	3d 20h 30m 17s	1/3	model.com has no errors
	Zone Rollover	ROLLING	02-13-2012 11:26:40	0d 0h 37m 35s	1/3	KSK Rollover Phase 3
paradigm.com/paradigm.com	Donuts	OK	02-13-2012 11:27:04	3d 20h 30m 11s	1/3	paradigm.com has no errors
	Zone Rollover	ROLLING	02-13-2012 11:26:20	0d 0h 37m 55s	1/3	ZSK Rollover Phase 3

The above picture is copied from https://www.dnssec-tools.org/wiki/images/7/77/Dt-nagios-dt-services0.png with the copyright as indicated by the site.

Automation of upload of DS to parent zone

- dk. / DK-Hostmaster
  - EPP test from the end of august at DK-Hostmaster
    - Only for registrars
  - DSU: https://www.dk-hostmaster.dk/noter-om-teknik/dnssec/dsu/
    - Simple protocol (which is awesome!)

DSU client implementation

- For use with Bind (with manual key rolling and key maintenance; i.e. not using OpenDNSSEC), use dsu-upload:

```
git clone git://git.svenne.dk/public/dnssec-tools.git

cd dnssec-tools

./dsu-upload $handle $keyfile
```

- For use with OpenDNSSEC
  - A slightly modified version of dsu-upload will be put online after the talk at video.thecamp.dk which will serve as an example.

SSHFP – Secure Shell Fingerprint

On the server:

```
$ ssh-keygen -r rubidium.obsd.dk
rubidium.obsd.dk IN SSHFP 1 1 60c0f7e184e3f84fac79abec73a5b5ddf3a38f6a
rubidium.obsd.dk IN SSHFP 2 1 791f6b57647a991a67d4154529cecfaaed554ce8
```

Insert records into zone.

On the client:

```
$ dig rubidium.obsd.dk sshfp | grep -A 2 ^...ANSWER | tr '\t' ' '
;; ANSWER SECTION:
rubidium.obsd.dk. 3600 IN SSHFP 1 1 60C0F7E184E3F84FAC79ABEC73A5B5DDF3A38F6A
rubidium.obsd.dk. 3600 IN SSHFP 2 1 791F6B57647A991A67D4154529CECFAAED554CE8

$ ssh -o VerifyHostKeyDNS=yes rubidium.obsd.dk
The authenticity of host 'rubidium.obsd.dk (94.146.47.1)' can't be
established.
RSA key fingerprint is 9c:13:9e:21:cc:66:c7:4f:cb:9d:08:6f:05:20:bb:48.
Matching host key fingerprint found in DNS.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'rubidium.obsd.dk,94.146.47.1' (RSA) to the list of
known hosts.
```

TLSA

- IETF wg: http://datatracker.ietf.org/wg/dane/
  - http://datatracker.ietf.org/doc/draft-ietf-dane-protocol/?inclu
- Makes it possible to include a hash for e.g. an SSL certificate in DNS:

```
echo | openssl s_client -connect blog.sman.dk:443 2>/dev/null | openssl x509 |python -c 'import sys,
hashlib; cert="".join(sys.stdin.read().strip().split("\n")[1:-1]); print
hashlib.sha256(cert.decode("base64")).hexdigest()'

3510ad32ad9d2aa02ddee3ebc0d36ce53a9cb283e02bff6cb2be26ac957d3adb

_443._tcp.blog IN TLSA 1 1 1 3510ad32ad9d2aa02ddee3ebc0d36ce53a9cb283e02bff6cb2be26ac957d3adb
```

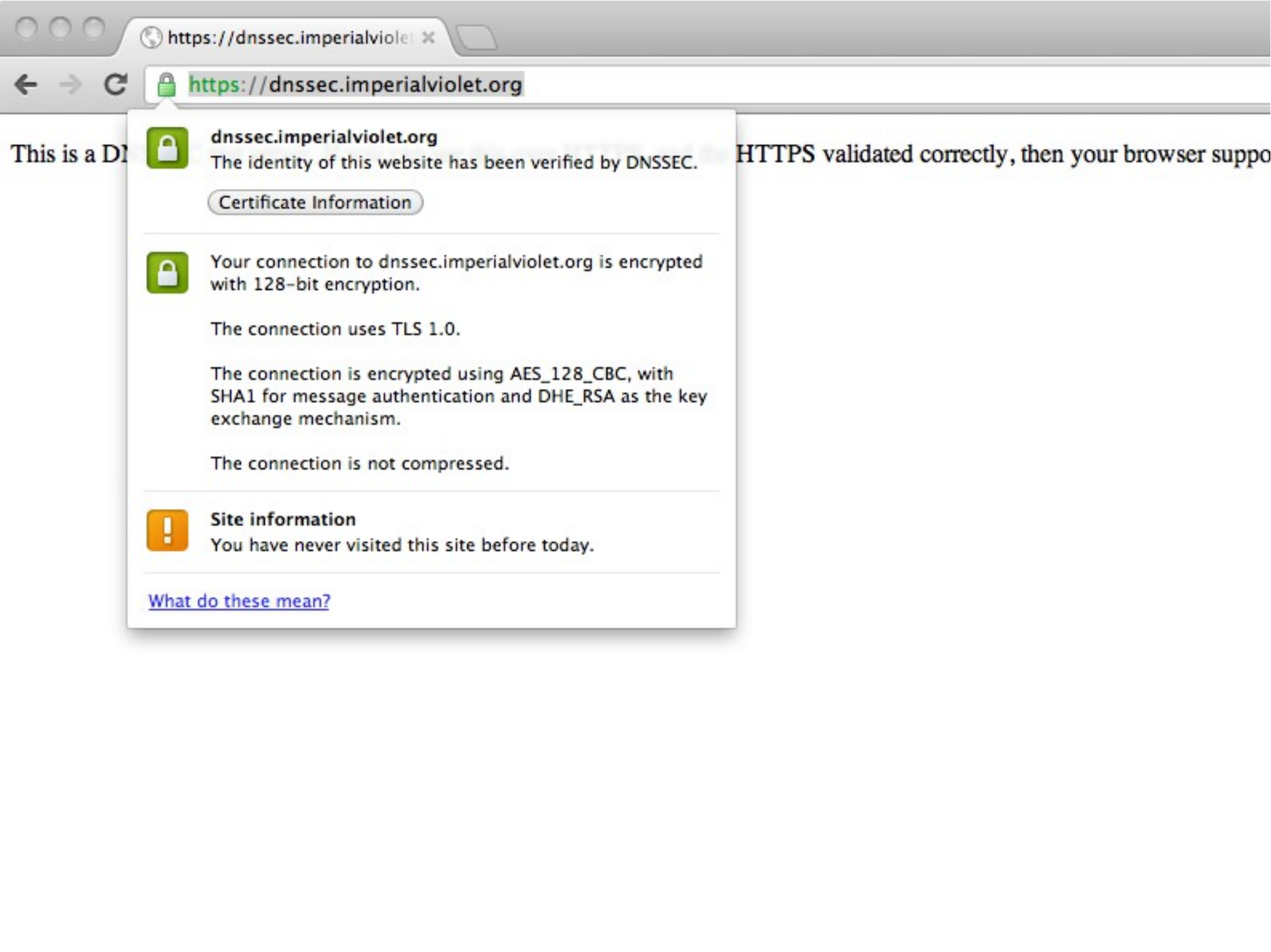
- Current status: Internet-Draft
  - Expires: December 16, 2012
- Mozilla seems to be working on support for it

TLSA example

```
./swede verify dnssec.svenne.dk
Received the following record for name _443._tcp.dnssec.svenne.dk.:
   Usage:                3 (End-Entity)
   Selector:             1 (SubjectPublicKeyInfo)
   Matching Type:            1 (SHA-256)
   Certificate for Association:
a9cdf989b504fe5dca90c0d2167b6550570734f7c763e09fdf88904e06157065
This record is valid (well-formed).
Attempting to verify the record with the TLS service...
Got the following IP: 81.7.185.93
SUCCESS (usage 3): The certificate offered by the server matches the
TLSA record
The matched certificate has Subject: /C=DK/ST=Copenhagen
/L=Copenhagen/O=Kracon Aps/CN=dns
```

CAA
Certification Authority Authorization

- IETF wg: http://tools.ietf.org/wg/pkix/
  - http://tools.ietf.org/html/draft-ietf-pkix-caa-11
- Specifies one or more CA's that may issue certificates for a domain
- Supported in Google Chrome 14
- Current status: Internet-Draft
  - Expires: January 17, 2013


https://dnssec.imperialviolet
https://dnssec.imperialviolet.org
dnssec.imperialviolet.org
The identity of this website has been verified by DNSSEC.
Certificate Information
Your connection to dnssec.imperialviolet.org is encrypted with 128-bit encryption.
The connection uses TLS 1.0.
The connection is encrypted using AES_128_CBC, with SHA1 for message authentication and DHE_RSA as the key exchange mechanism.
The connection is not compressed.
Site information
You have never visited this site before today.
What do these mean?
This is a DI
HTTPS validated correctly, then your browser suppo


SARTANO