# DNSSEC key maintenance

Jelte Jansen

# Overview

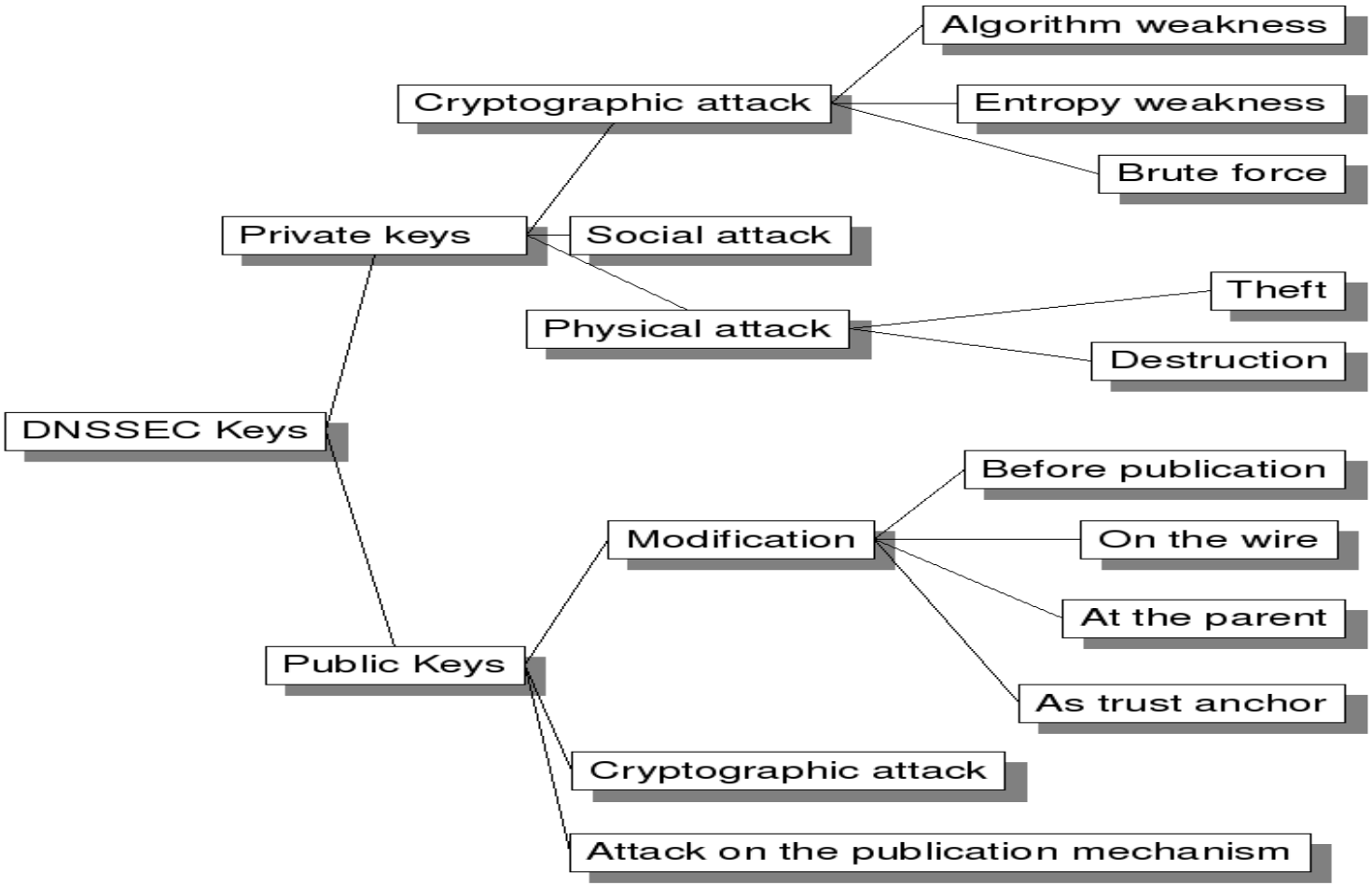
- 'Desk-study'
- Failure modes:
  - Attacks on keys
  - Operational mishaps
- Key management:
  - Deployment choices
  - Rollover
  - Storage
  - Publication

# There's more to DNS(SEC)

- Repository corruption
- Domain Hijacking
- Compromised machines
- Man-in-the-Middle
- DOS attacks
- Snooping
- NSEC walking
- Monitoring
- And more

- But I won't go into those

# Attacks!



# Private keys

- Cryptographic attack
  - Algorithm weakness
  - Entropy weakness
  - Brute force
- Social attack
- Physical attack
  - Theft
  - Destruction

# Public keys

- Modification attack
  - Before publication
  - On the wire
  - At the parent
  - As trust anchor
- Cryptographic attack
- Attack on the publication mechanism

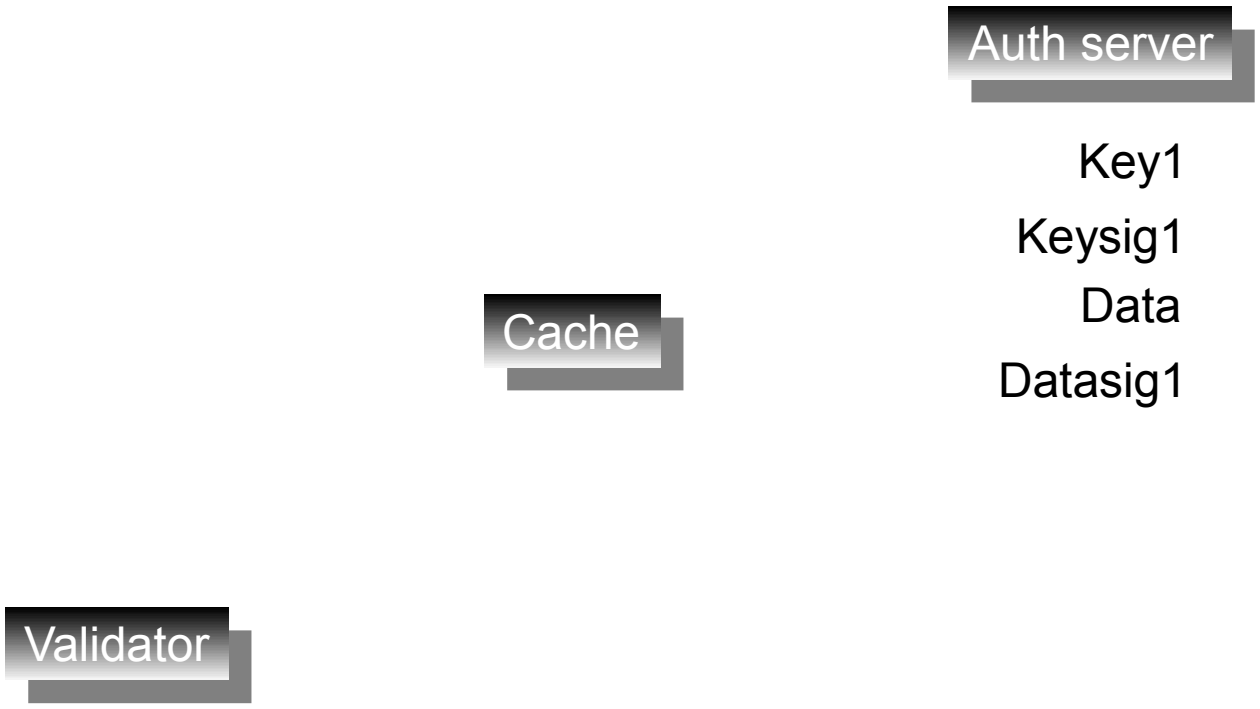
# Deployment choices

- Policy, policy, policy
- Staff
- Algorithm(s)
- Key lifetimes
- Rollovers
- Automation

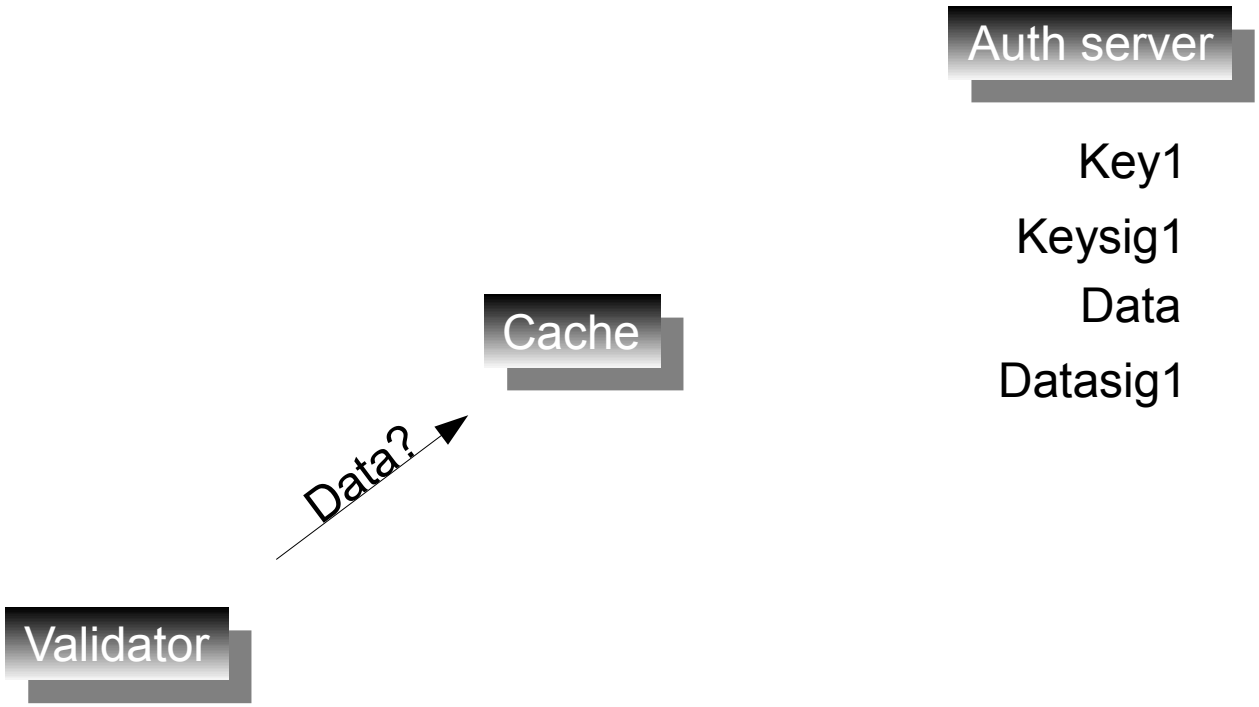
# Rollover

- Periodic rollover
- Emergency rollover
- Algorithm rollover

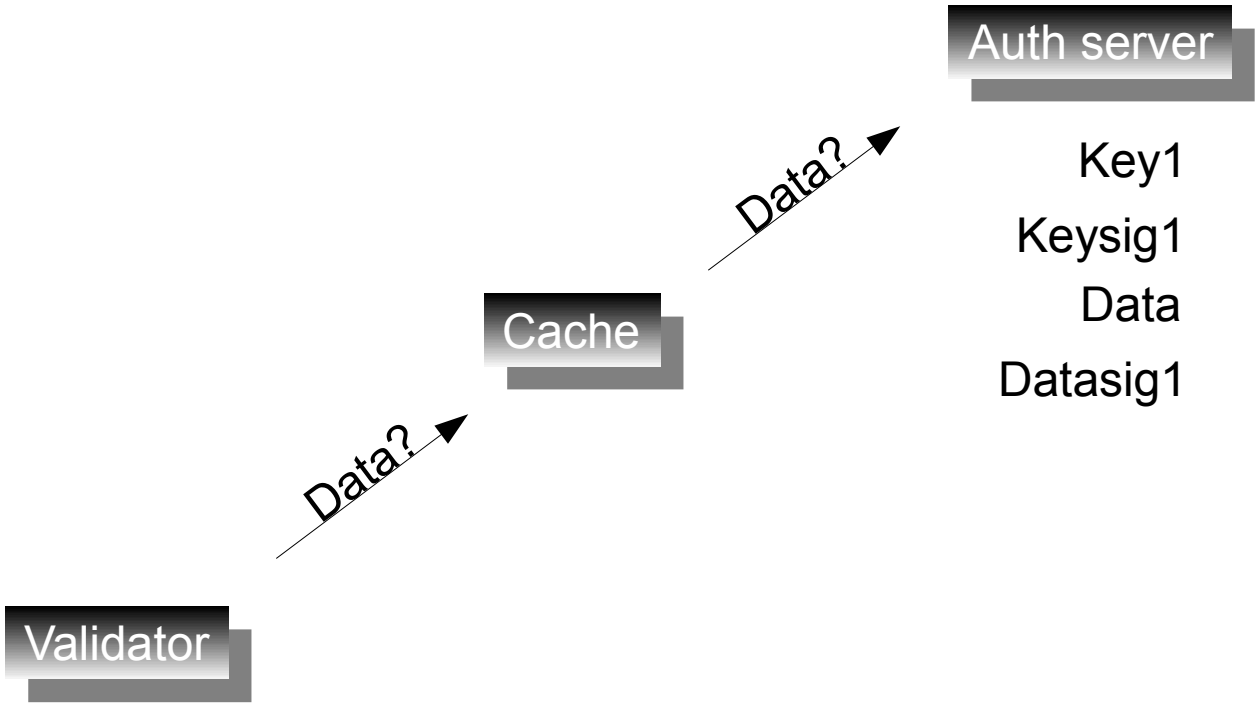
# Simple example



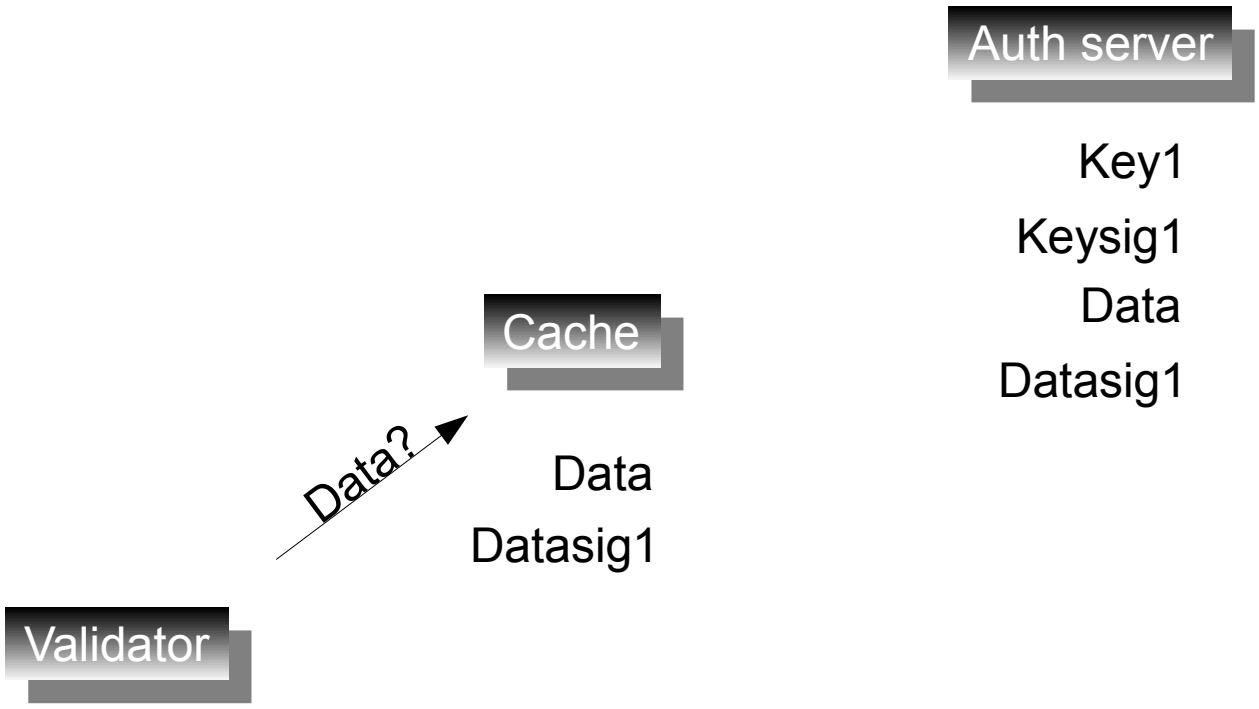
# Simple example



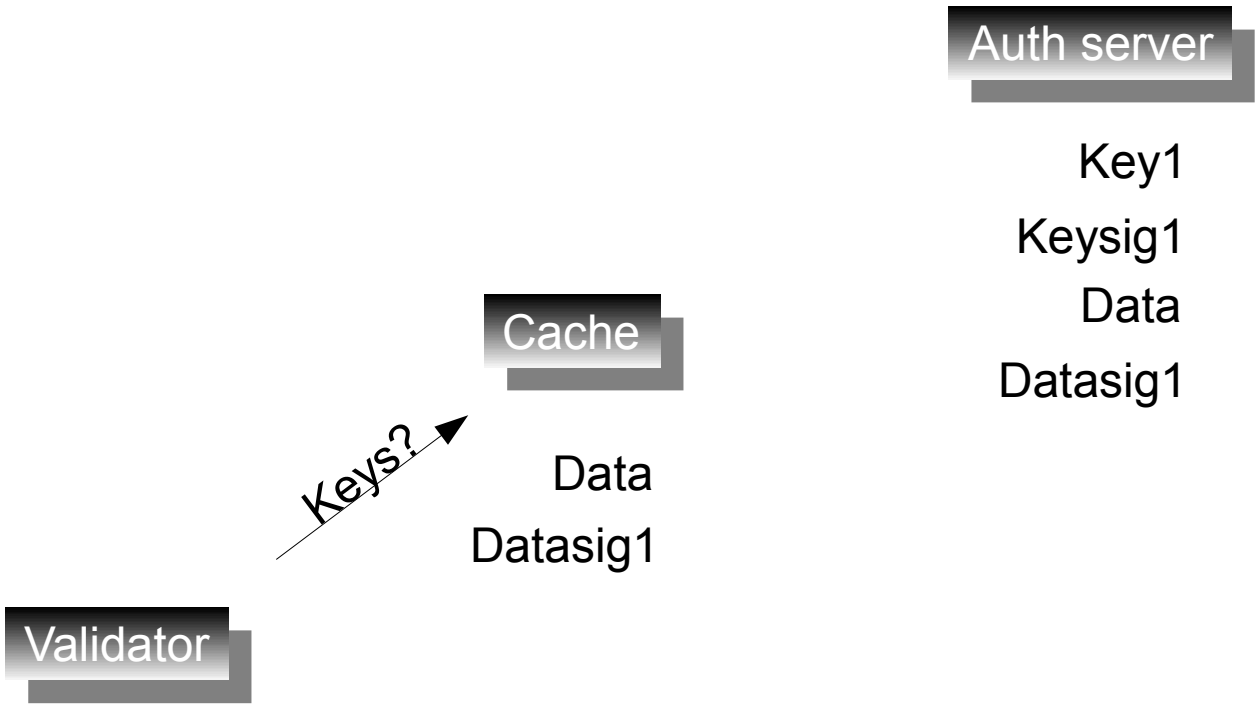
# Simple example



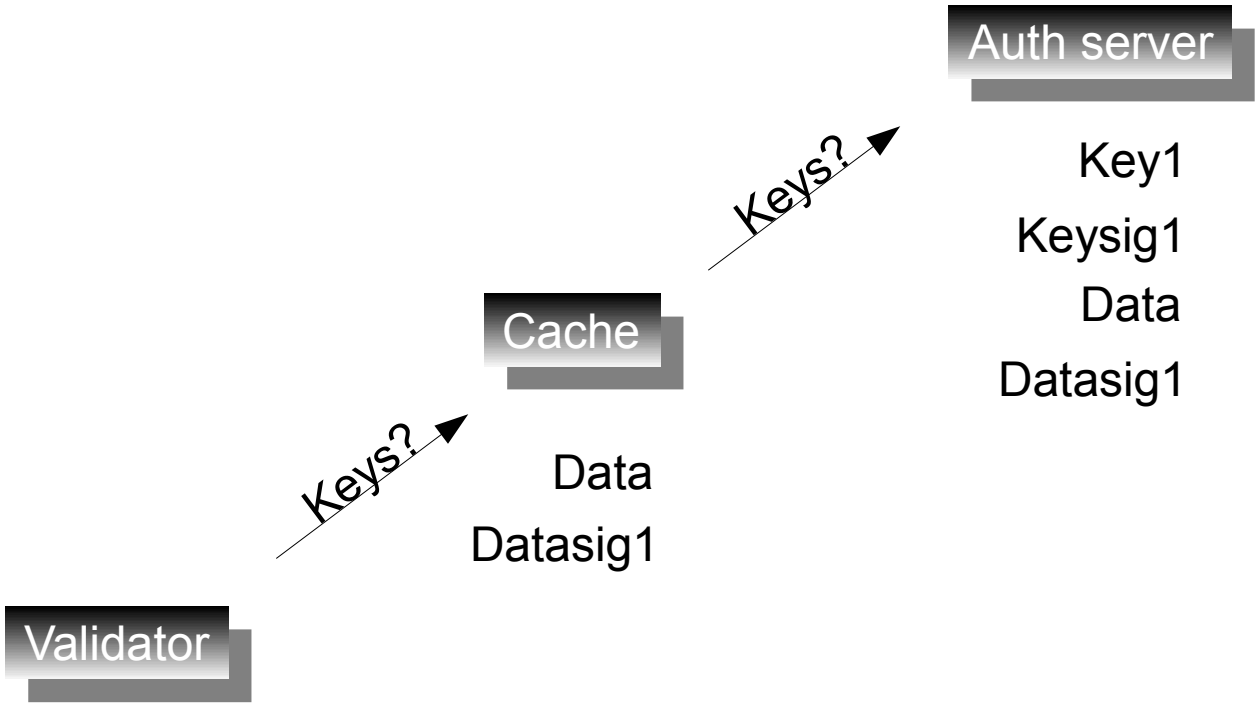
# Simple example



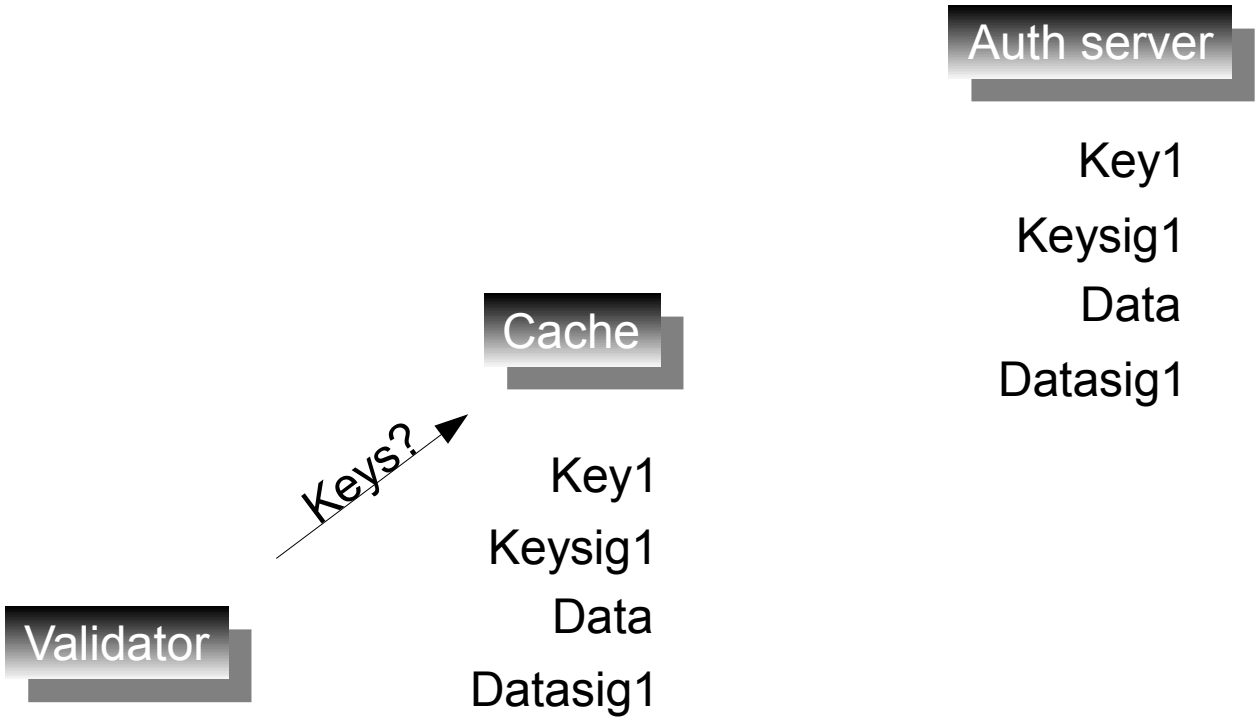
# Simple example



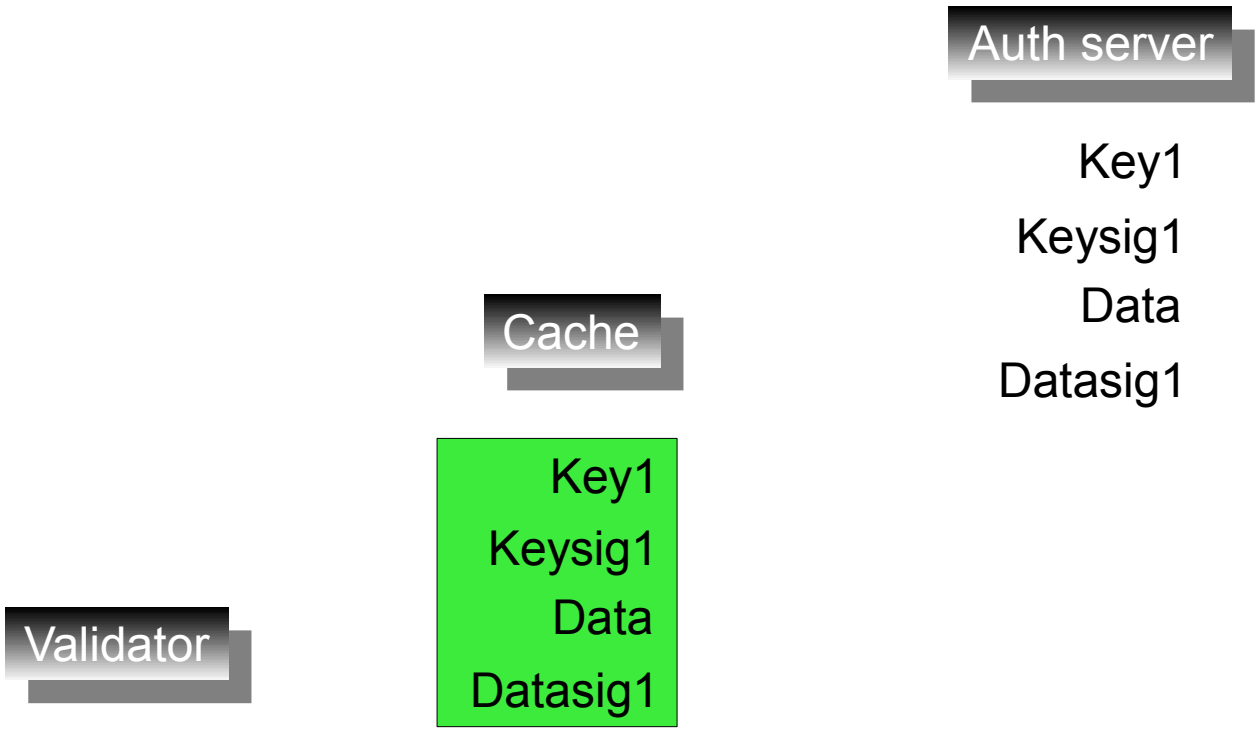
# Simple example



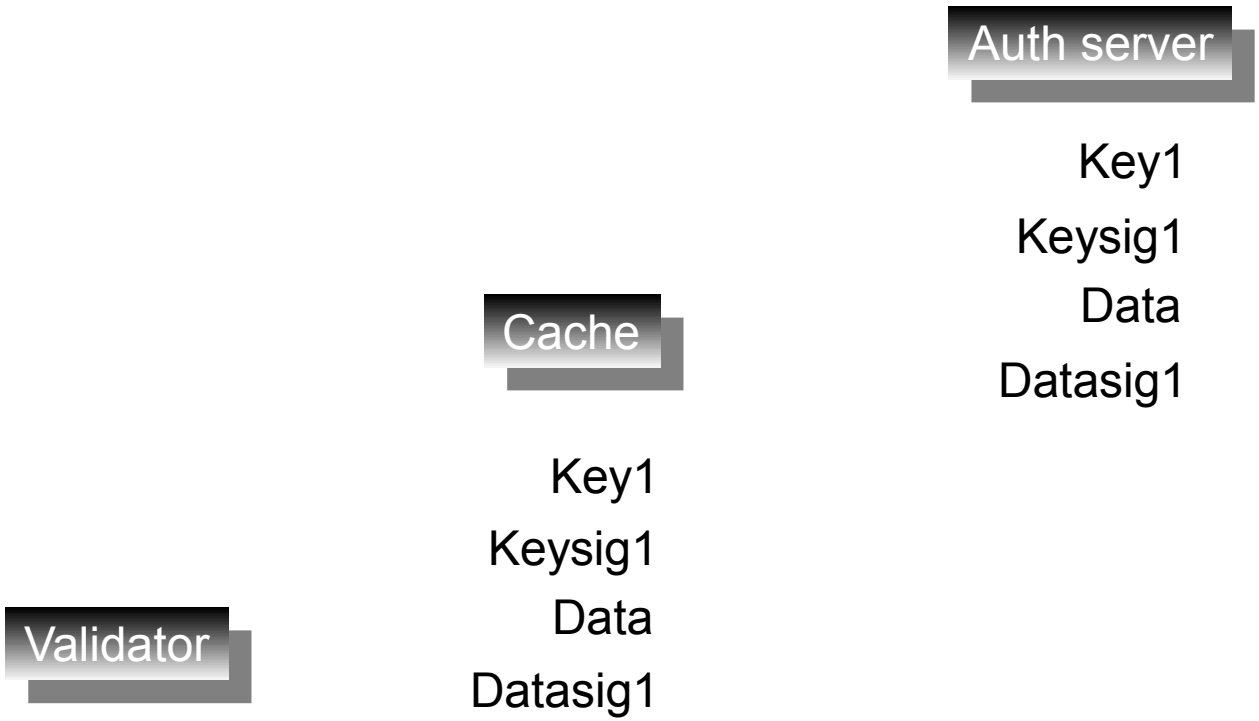
# Simple example



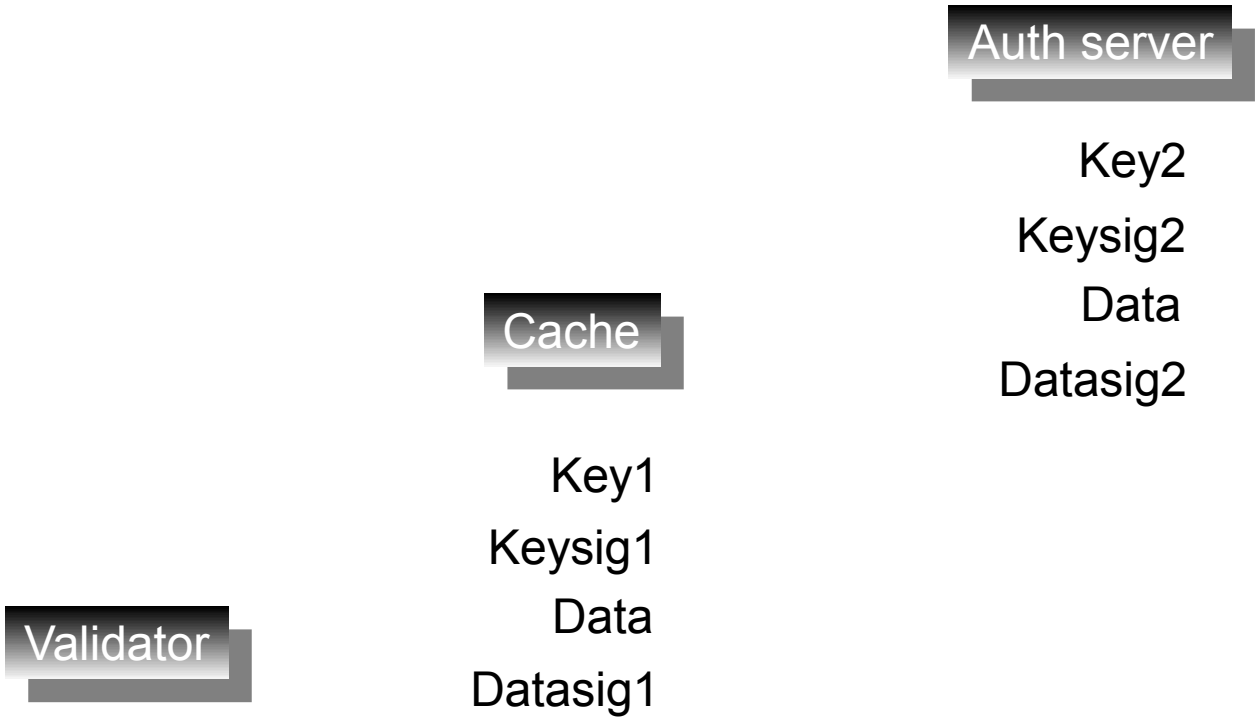
# Simple example



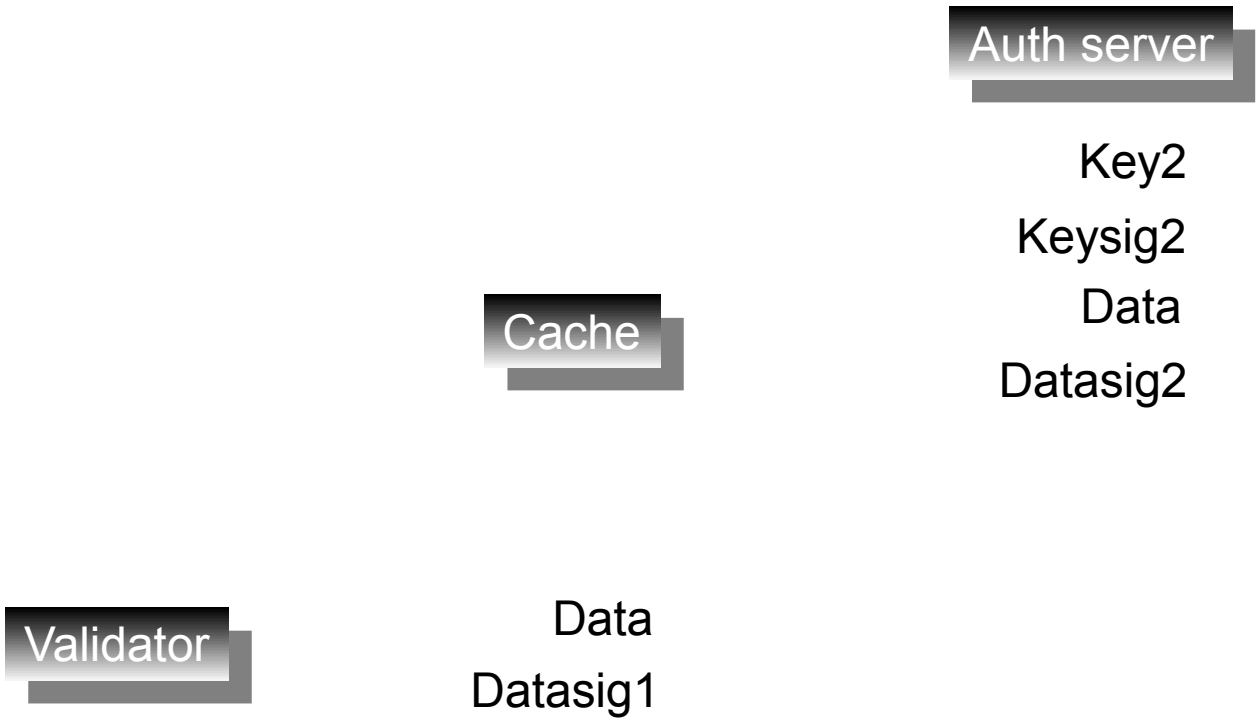
# Plain replacement



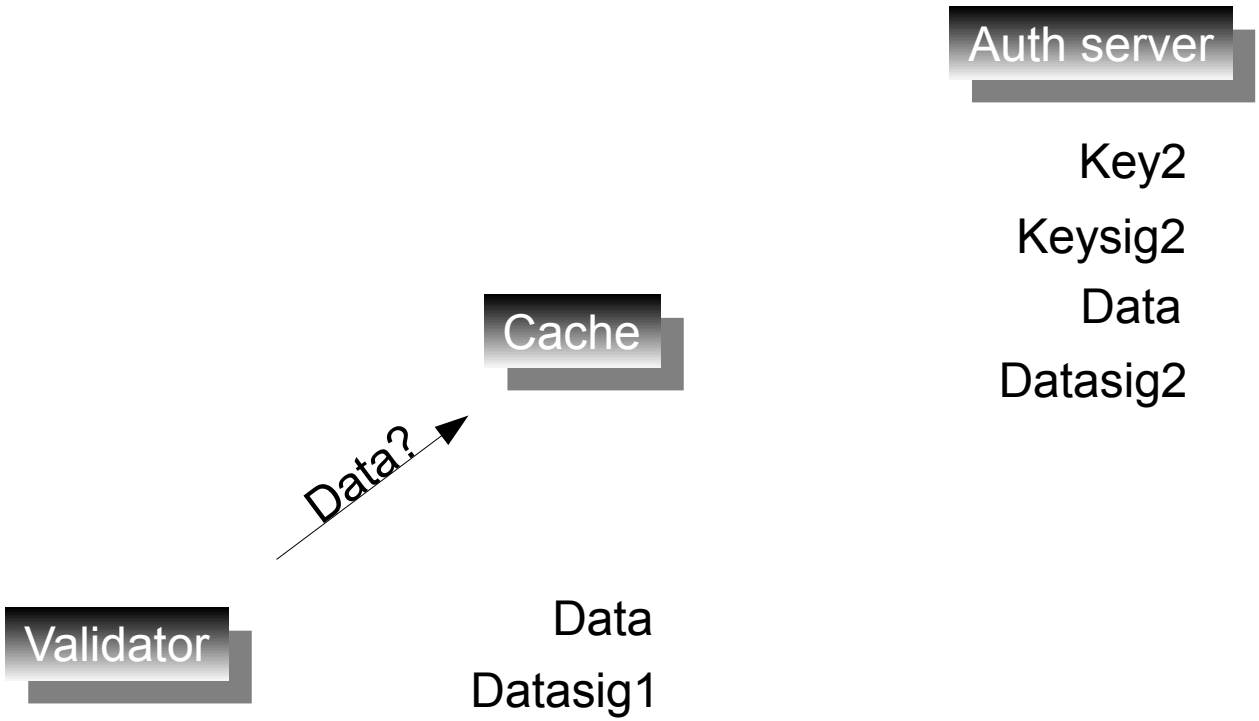
# Plain replacement



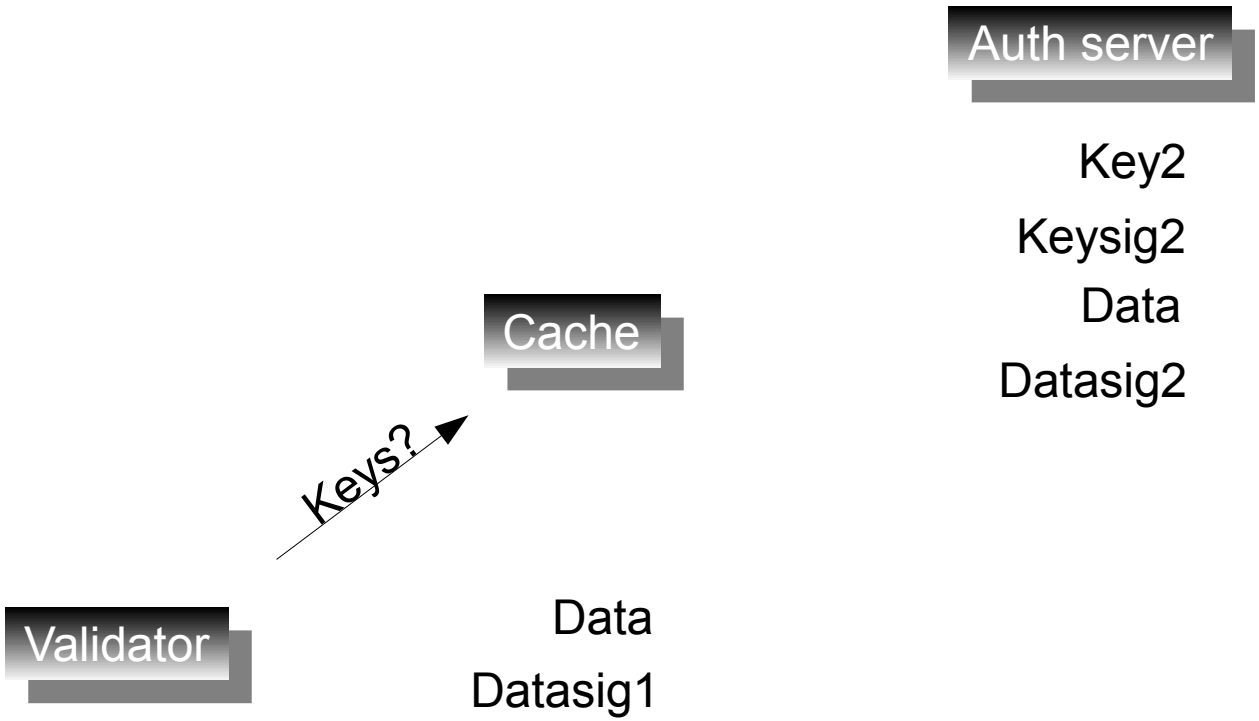
# Plain replacement



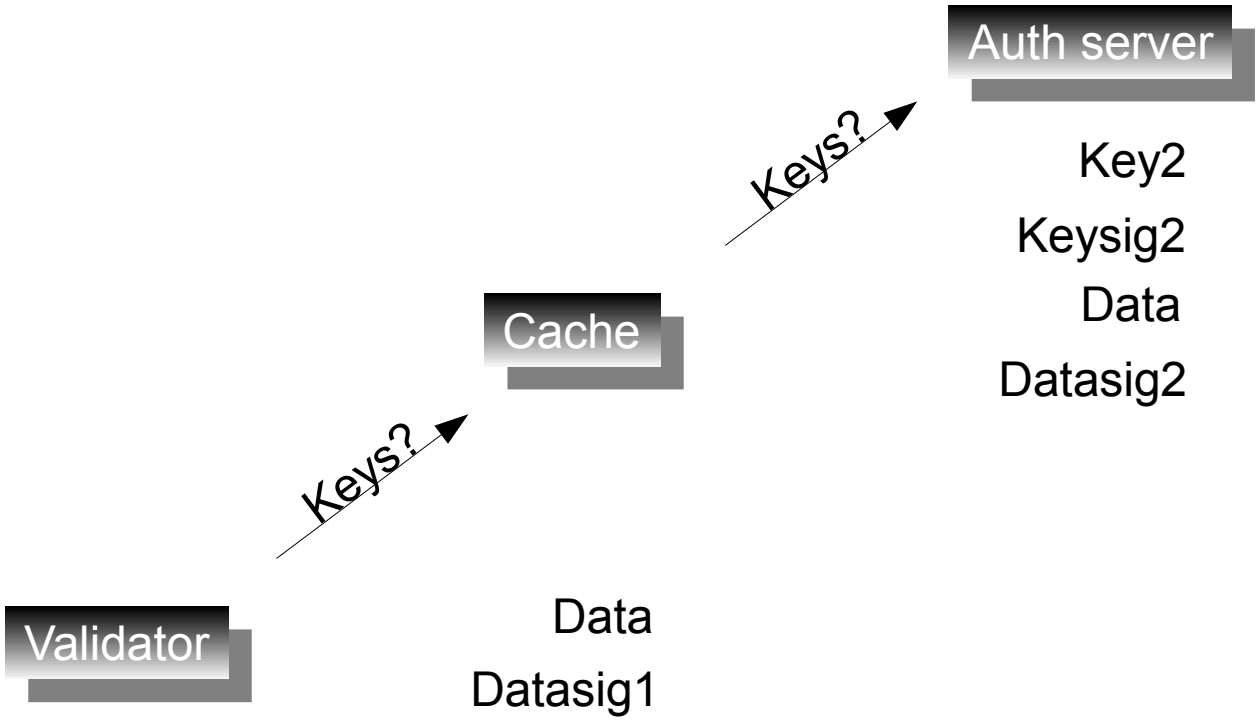
# Plain replacement



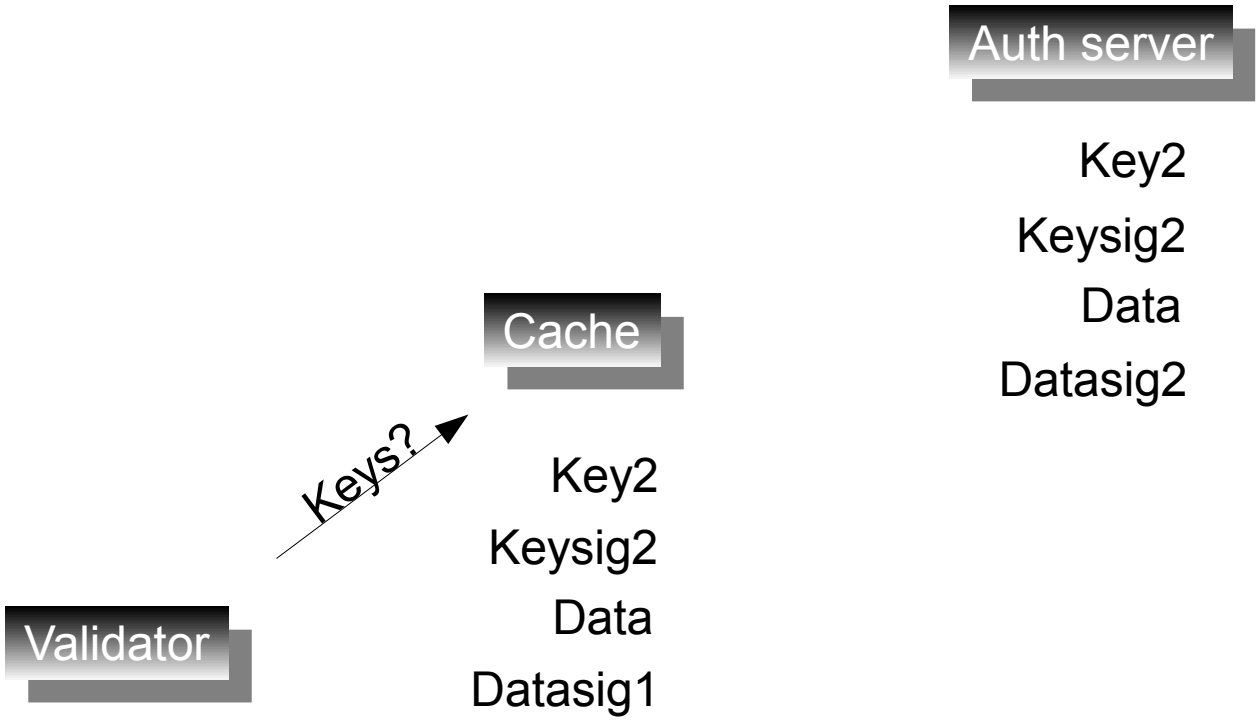
# Plain replacement



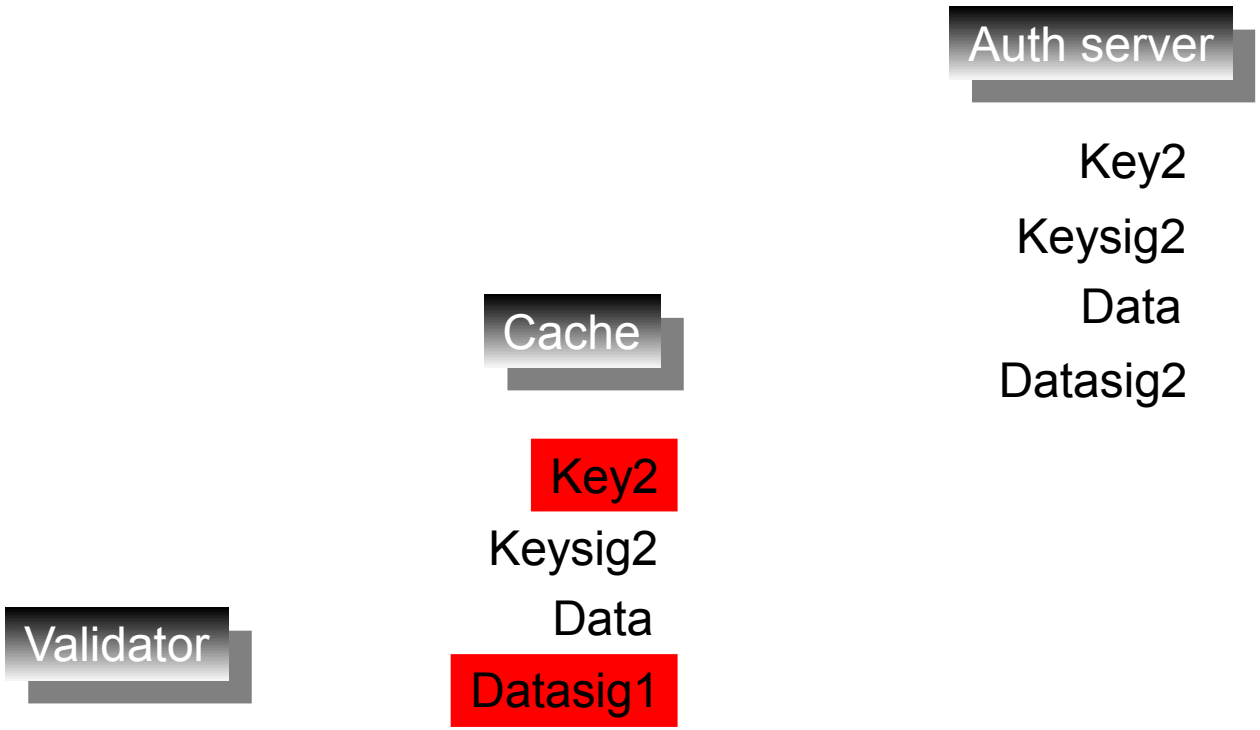
# Plain replacement



# Plain replacement



# Plain replacement



# ZSK Rollover: Double signatures

- Starting status:
  - Original keys and signatures in zone
- Add new:
  - Both old and new keys and sigs in zone
- Remove old:
  - Only new keys and signatures in zone

# Double signature rollover

| ----------time-------> | | |
|---|---|---|
| initial | new DNSKEY | DNSKEY removal |
| SOA0 | SOA1 | SOA2 |
| RRSIG10(SOA0) | RRSIG10(SOA1) | RRSIG11(SOA2) |
| | RRSIG11(SOA1) | |
| DNSKEY1 | DNSKEY1 | DNSKEY1 |
| DNSKEY10 | DNSKEY10 | DNSKEY11 |
| | DNSKEY11 | |
| RRSIG1(DNSKEY) | RRSIG1(DNSKEY) | RRSIG1(DNSKEY) |
| RRSIG10(DNSKEY) | RRSIG10(DNSKEY) | RRSIG11(DNSKEY) |
| | RRSIG11(DNSKEY) | |

# ZSK Rollover: Pre-publish

- Starting status
  - Original keys and signatures in zone
- Add new key
  - Original and new keys in zone
  - Only old signatures in zone
- Switch signatures
  - Original and new keys in zone
  - Only new signatures in zone
- Remove old key

# Pre-publish rollover

| initial | new DNSKEY | new RRSIGs | DNSKEY removal |
|---|---|---|---|
| SOA0 | SOA1 | SOA2 | SOA3 |
| RRSIG10(SOA0) | RRSIG10(SOA1) | RRSIG11(SOA2) | RRSIG11(SOA3) |
| DNSKEY1 | DNSKEY1 | DNSKEY1 | DNSKEY1 |
| DNSKEY10 | DNSKEY10 | DNSKEY10 | DNSKEY11 |
| | DNSKEY11 | DNSKEY11 | |
| RRSIG1(DNSKEY) | RRSIG1(DNSKEY) | RRSIG1(DNSKEY) | RRSIG1(DNSKEY) |
| RRSIG10(DNSKEY) RRSIG11(DNSKEY) | RRSIG10(DNSKEY) | RRSIG11(DNSKEY) | |

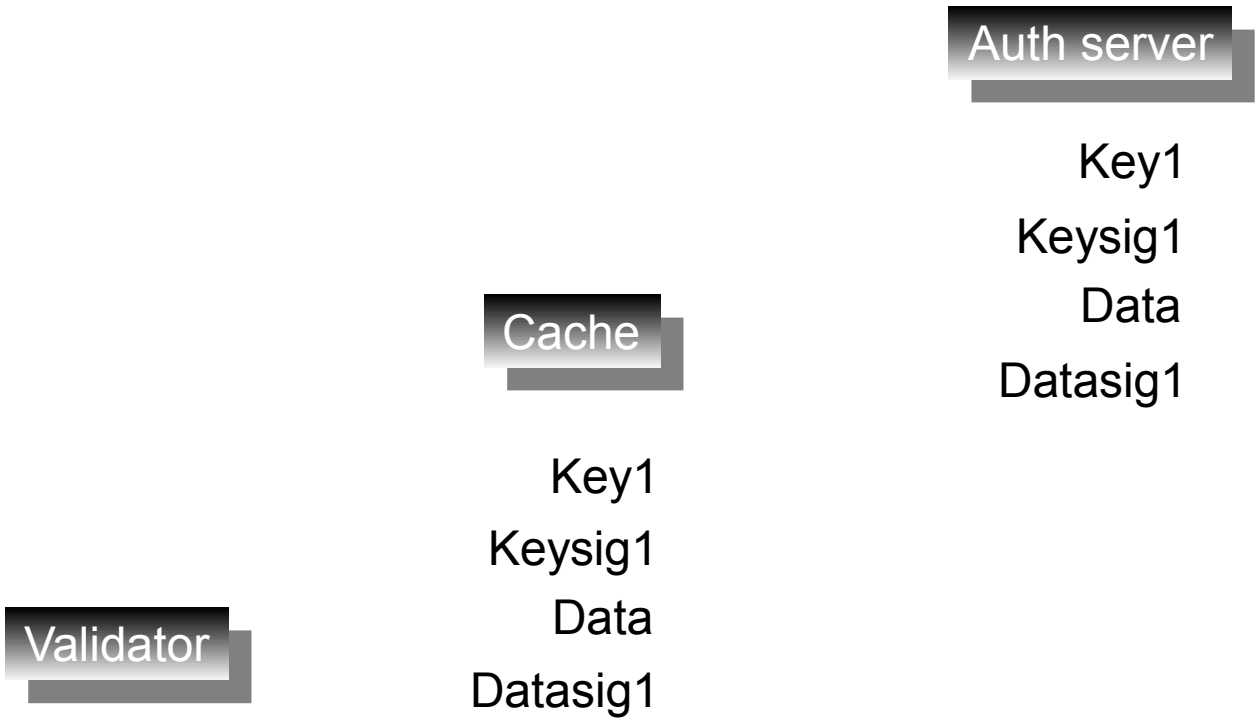
# KSK Rollover

- New keys must be published
  - To parent
    - Depends on their procedures
  - To clients
    - Out of band
    - RFC5011

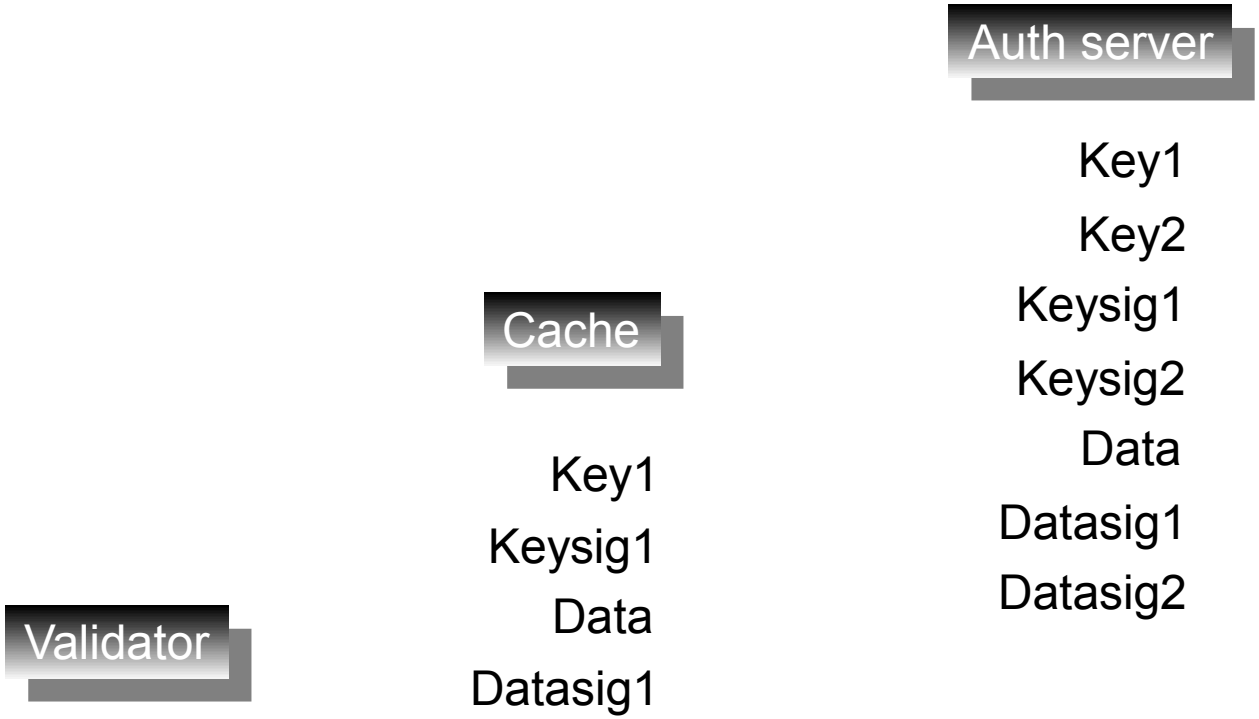
# Algorithm rollover

- Downgrade protection:
- There MUST be an RRSIG for each RRset using at least one DNSKEY of each algorithm in the zone apex DNSKEY RRset.
  - RFC4035 Section 2.2
- Caches may only have old signatures
- They will get a key for which there are no sigs
- So, additional steps are needed

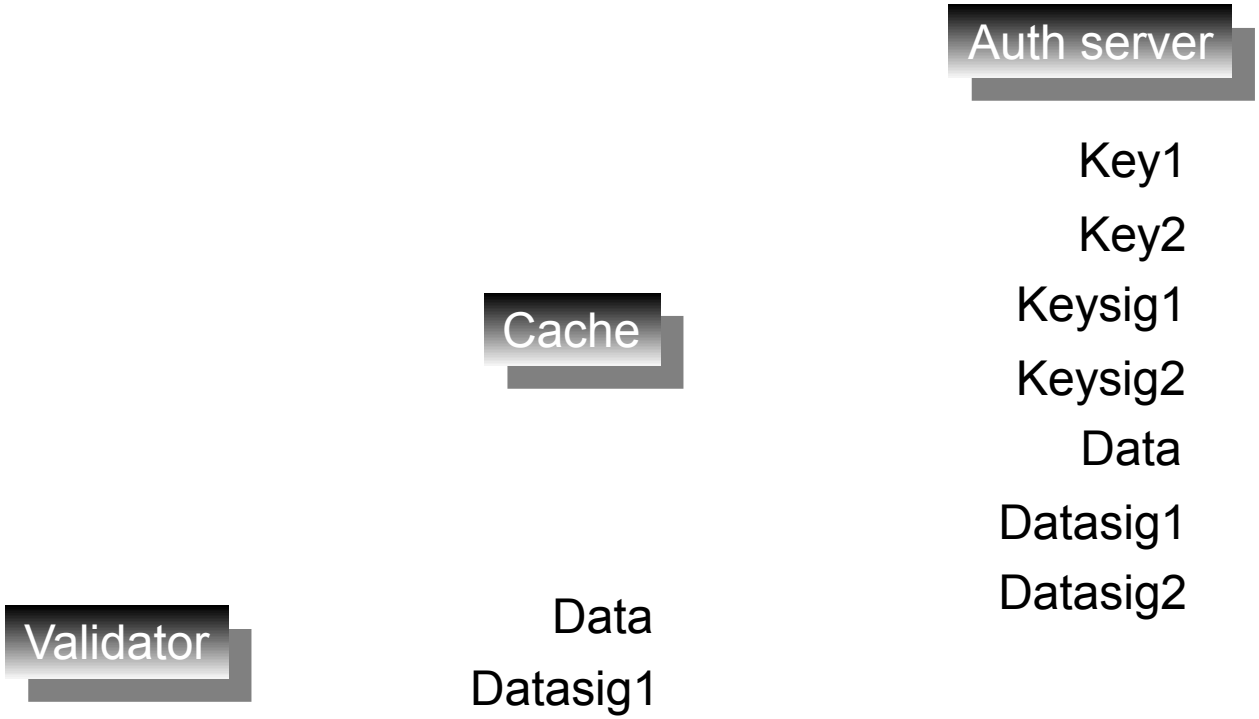
# Algorithm rollover



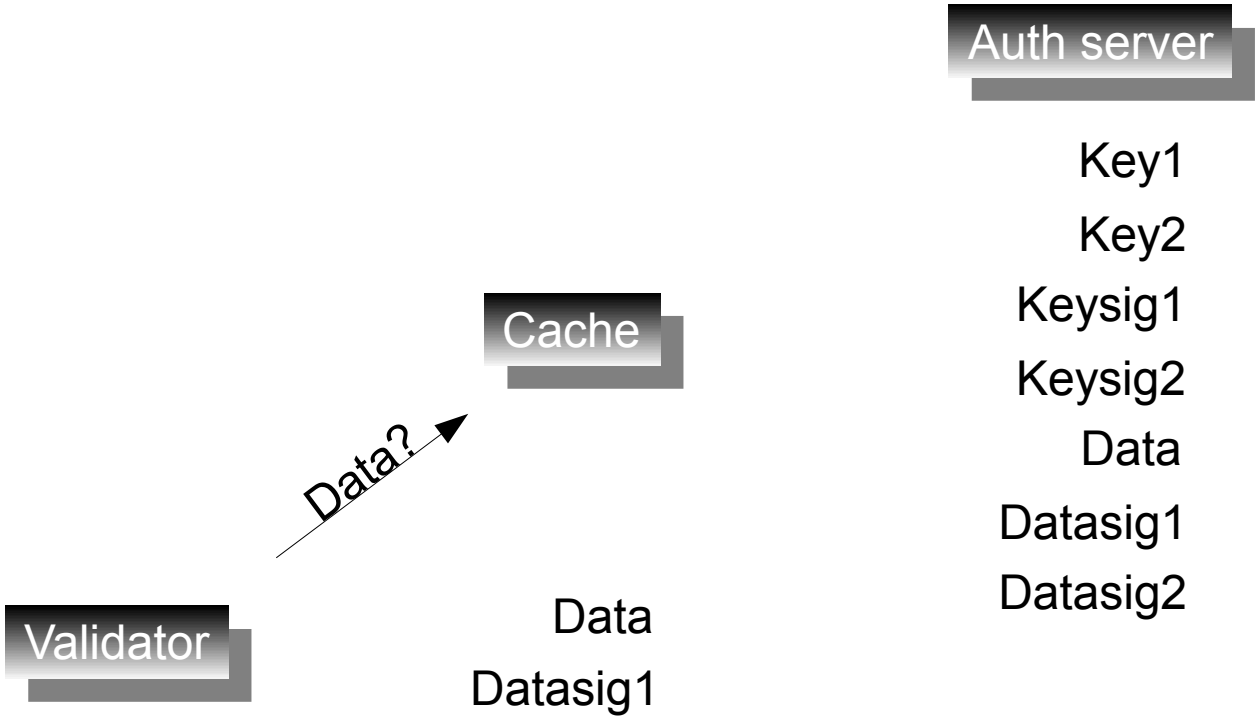
# Algorithm rollover



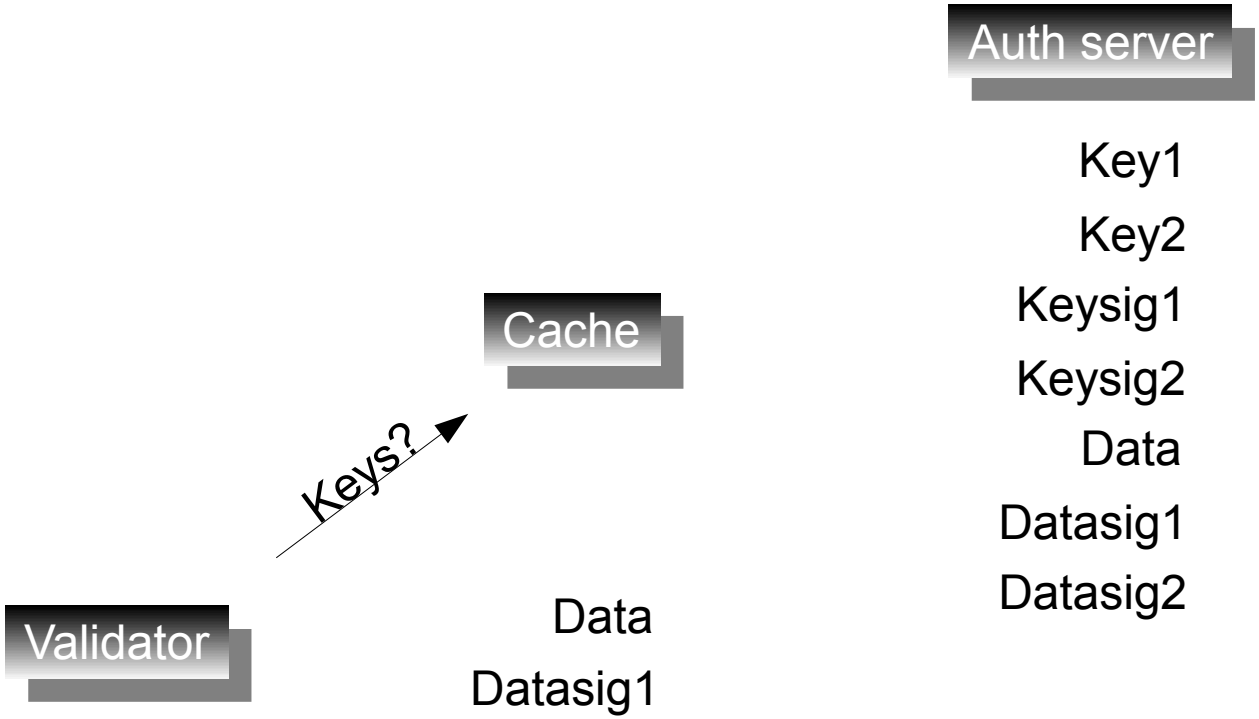
# Algorithm rollover



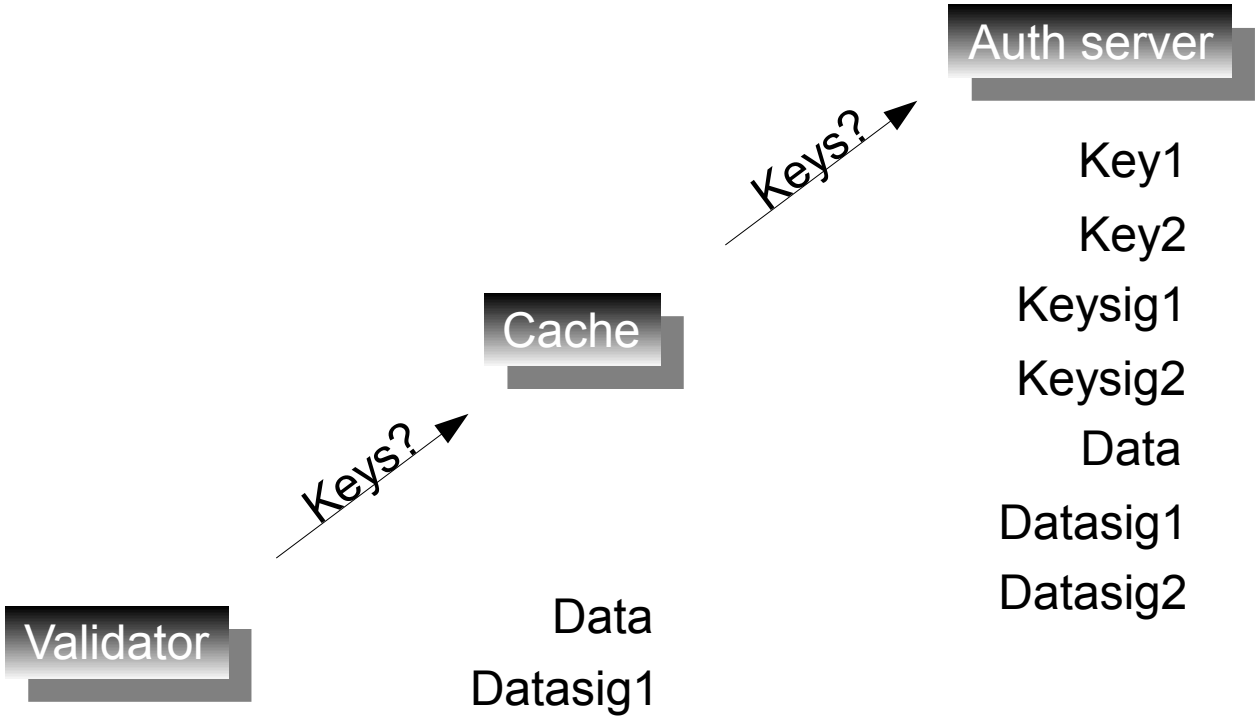
# Algorithm rollover



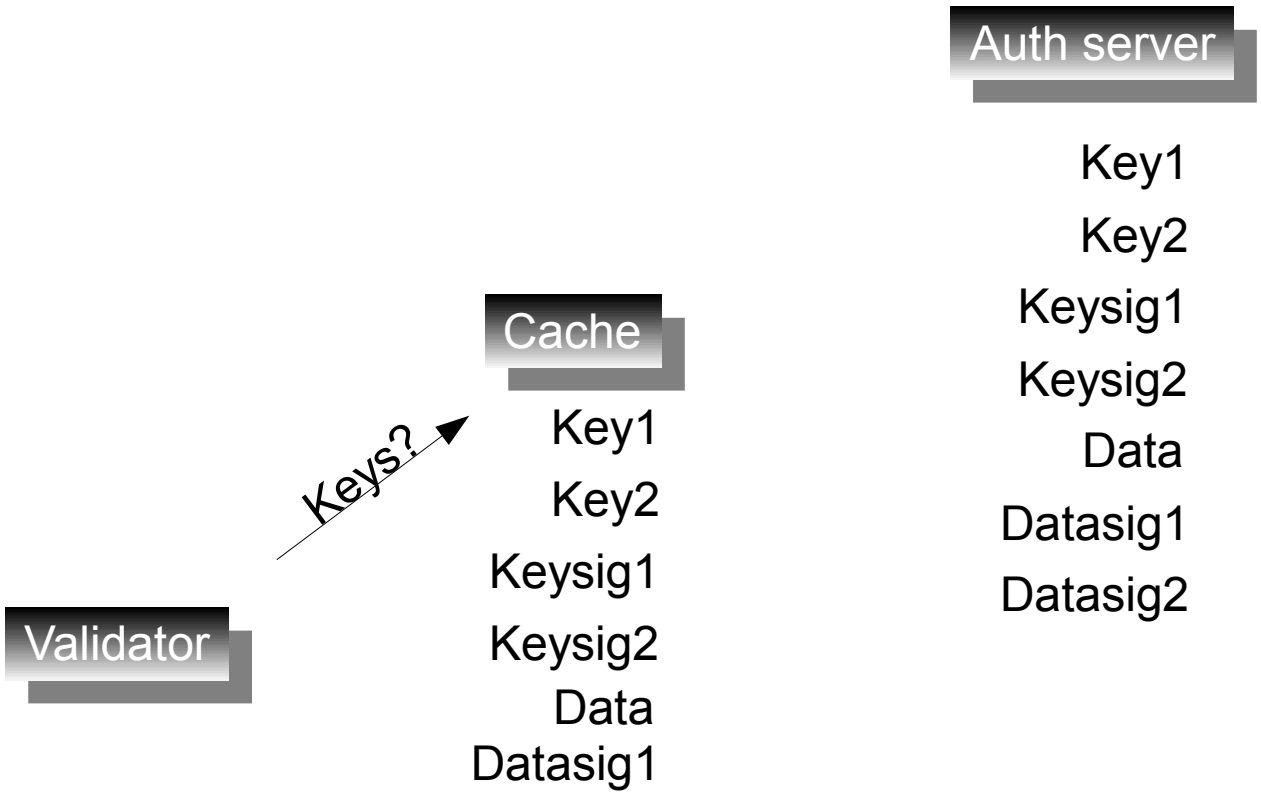
# Algorithm rollover



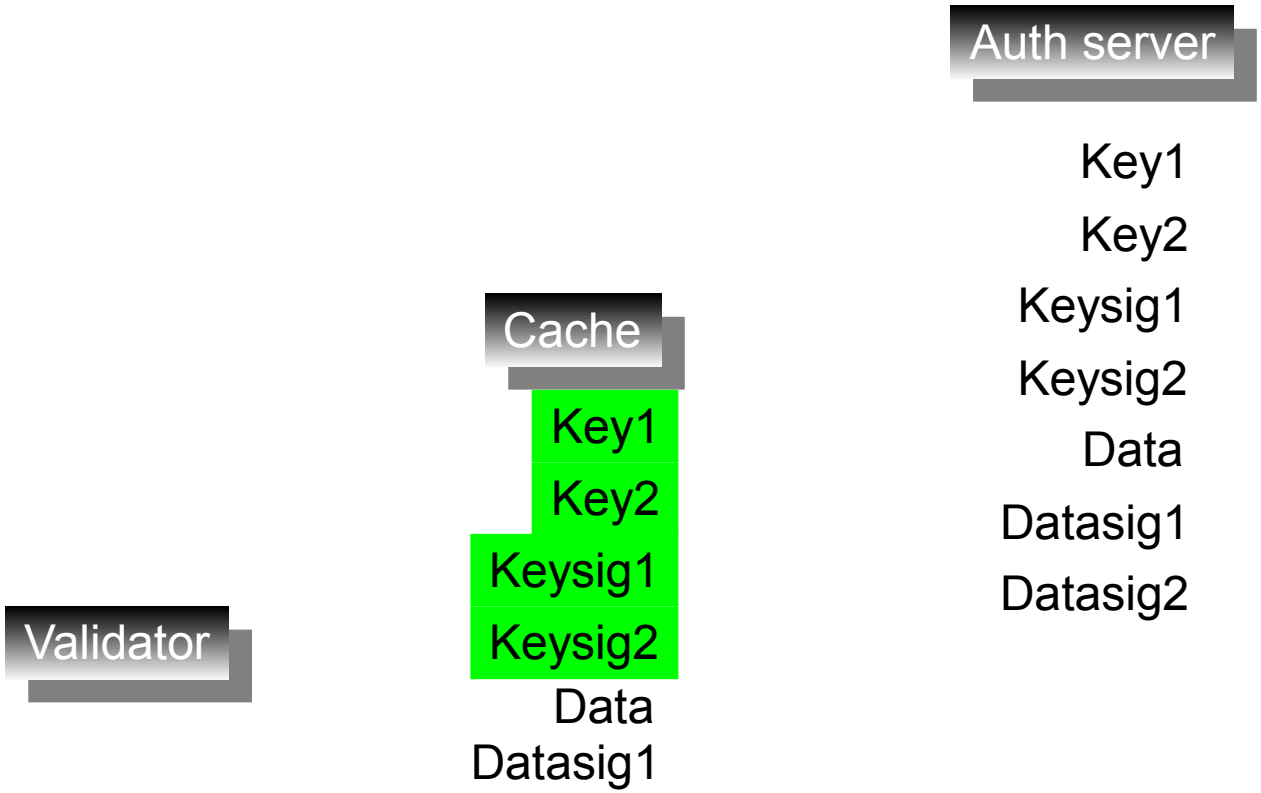
# Algorithm rollover



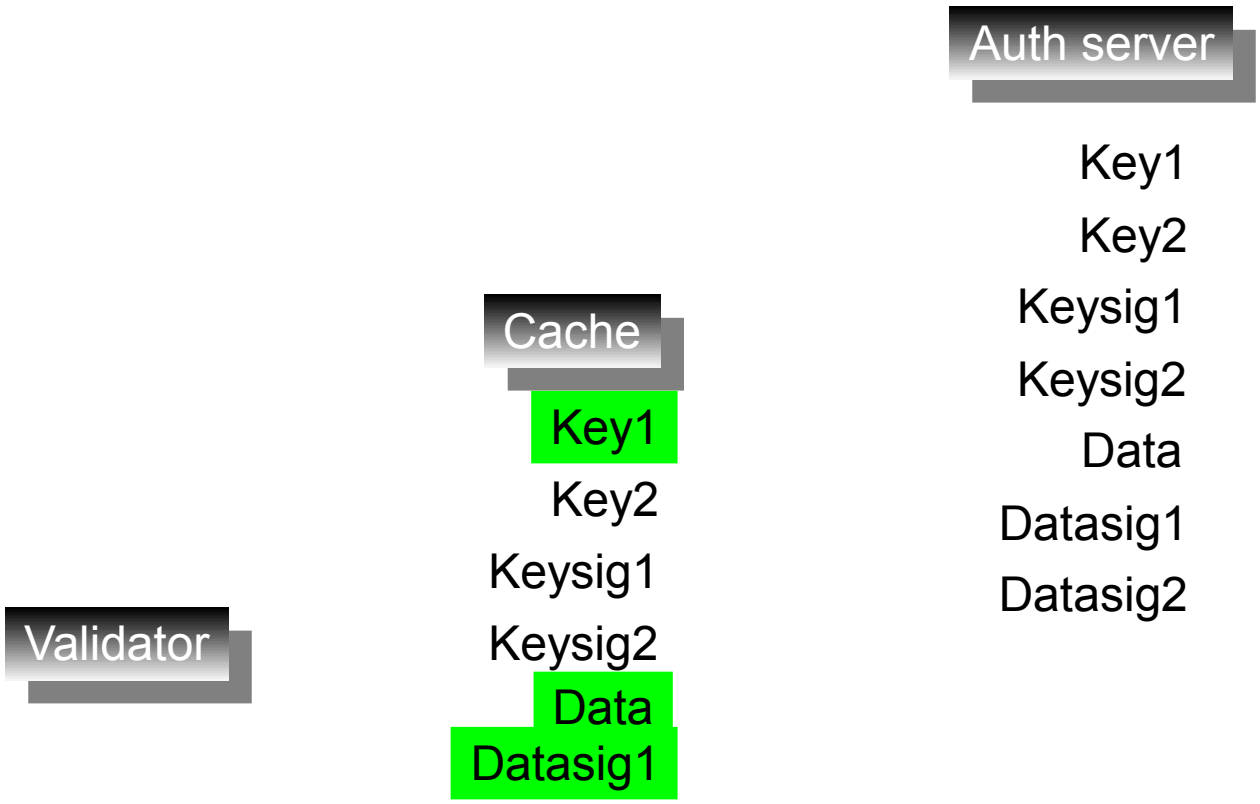
# Algorithm rollover



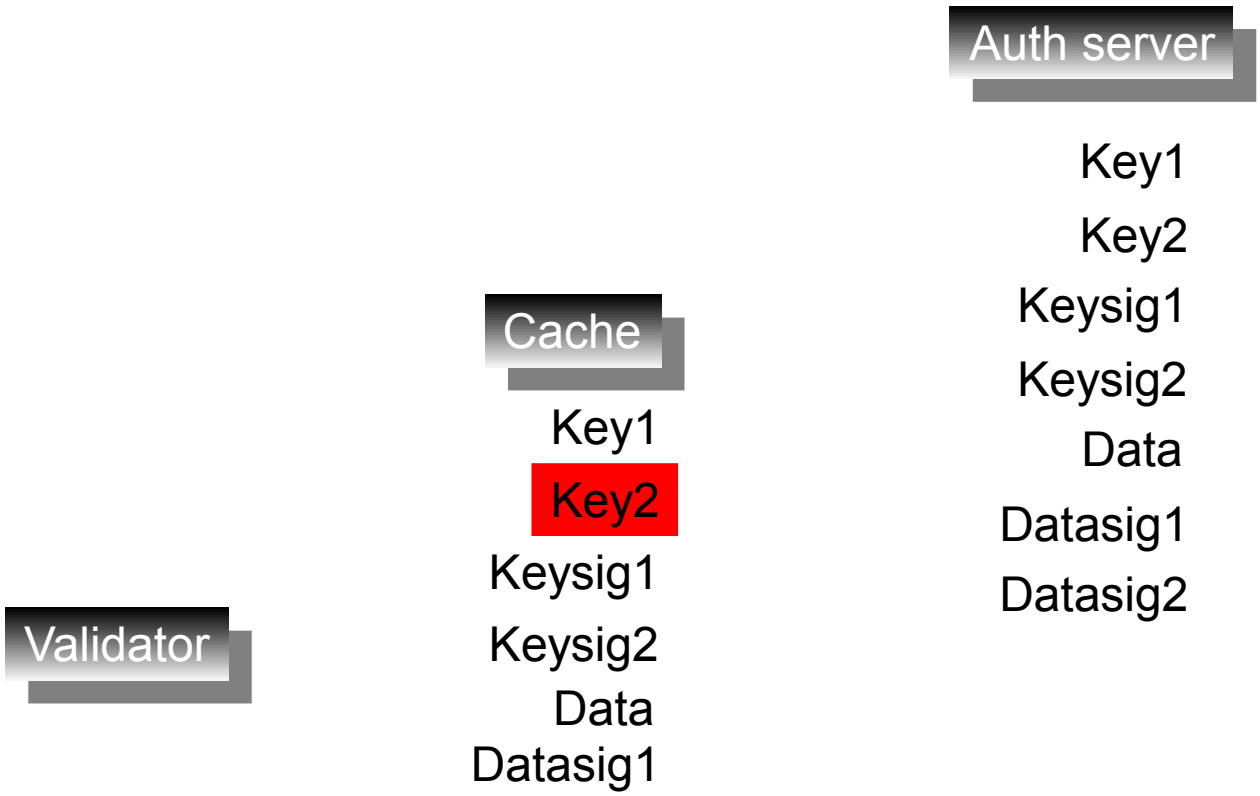
# Algorithm rollover



# Algorithm rollover

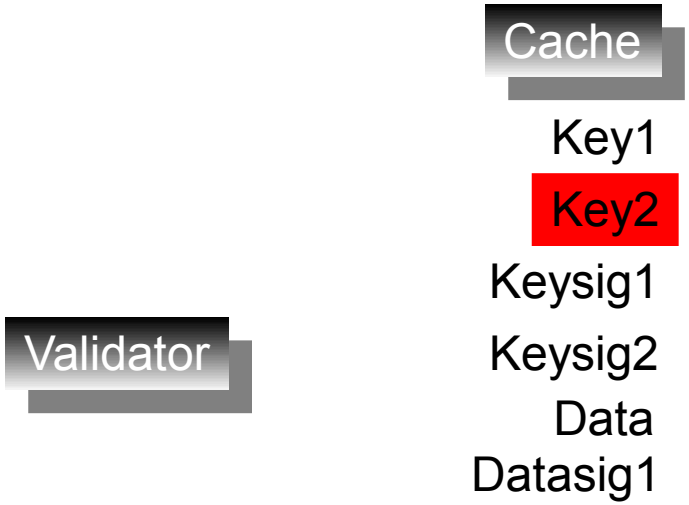


# Algorithm rollover



# Algorithm rollover

- There MUST be an RRSIG for each RRset using at least one DNSKEY of each algorithm in the zone apex DNSKEY RRset.



# Algorithm rollover: a way forward

- Starting state:
  - Old keys and signatures in the zone
- Add new signatures:
  - Old keys, both old and new sigs in zone
- Add new keys:
  - Both old and new keys and sigs in zone
- Remove old keys:
  - New keys, both old and new sigs in zone
- Remove old signatures

# Algorithm rollover I

| 1 Initial | 2 New RRSIGS | 3 New DNSKEY |
|---|---|---|
| SOA0 | SOA1 | SOA2 |
| RRSIG1(SOA0) | RRSIG1(SOA1) | RRSIG1(SOA2) |
| | RRSIG2(SOA1) | RRSIG2(SOA2) |
| DNSKEY1 | DNSKEY1 | DNSKEY1 |
| RRSIG1(DNSKEY) | RRSIG1(DNSKEY) | DNSKEY2 |
| | RRSIG2(DNSKEY) | RRSIG1(DNSKEY) |
| | | RRSIG2(DNSKEY) |

# Algorithm rollover 2

| 4 Remove DNSKEY | 5 Remove RRSIGS |
| --- | --- |
| SOA3 | SOA4 |
| RRSIG1(SOA3) | RRSIG2(SOA4) |
| RRSIG2(SOA3) | |
| DNSKEY2 | DNSKEY2 |
| RRSIG1(DNSKEY) | RRSIG2(DNSKEY) |
| RRSIG2(DNSKEY) | |

# Private keys: storage choices

- Depending on 'value'
- Online/offline
  - Direct access
  - Physical action needed
- HSM
- Access control on storage
- Choices may differ for KSK/ZSK
- Signing Procedures

# Private key storage

| Risk | On-/Offline | System |
|---|---|---|
| High | Online | FIPS Level 4 HSM |
| High | Offline | Reviewed procedures, physical safe |
| Medium | Online | FIPS Level 2 HSM, or shielded system |
| Medium | Offline | Reviewed procedures |
| Low | Online | Normal connected or local system |
| Low | Offline | |

# HSM

- PKCS #11 API
- But most HSMs follow only a part of it
- That makes development hard
- Not much in open software available
  - OpenSSL has support
    - But tricky to get working on some systems
- But there is hope!
  - http://NLnetLabs.nl/publications/hsm
  - http://www.opendnssec.org

# Key publication

- Key publication
  - Through the parent (DS/DNSKEY)
  - DLV
  - Out of band
    - Website
    - Paper
    - Mailing list
  - In-band
    - Only updates, RFC 5011

# Policy publication

- Policy for key publication
  - Where
  - How
  - When/How often
- Policy for policy publication

# Example: RIPE NCC

- Trust anchors are published on an https website
- Trust anchors are signed with a PGP key
- Trust anchors will be rolled twice a year
  - Using the 'double signature' scheme
  - With a three-month overlap
- Procedure changes will be published on https site and signed with PGP

# Summary

- We are still in an early stage
- Lots of choices to think about
- Write down everything
- Publish what is possible
- Automate what you can, esp. rollover

# Questions?