# X.509 Authentication in the RIPE Database

Shane Kerr

RIPE NCC

<shane@ripe.net>

# PGP Authentication

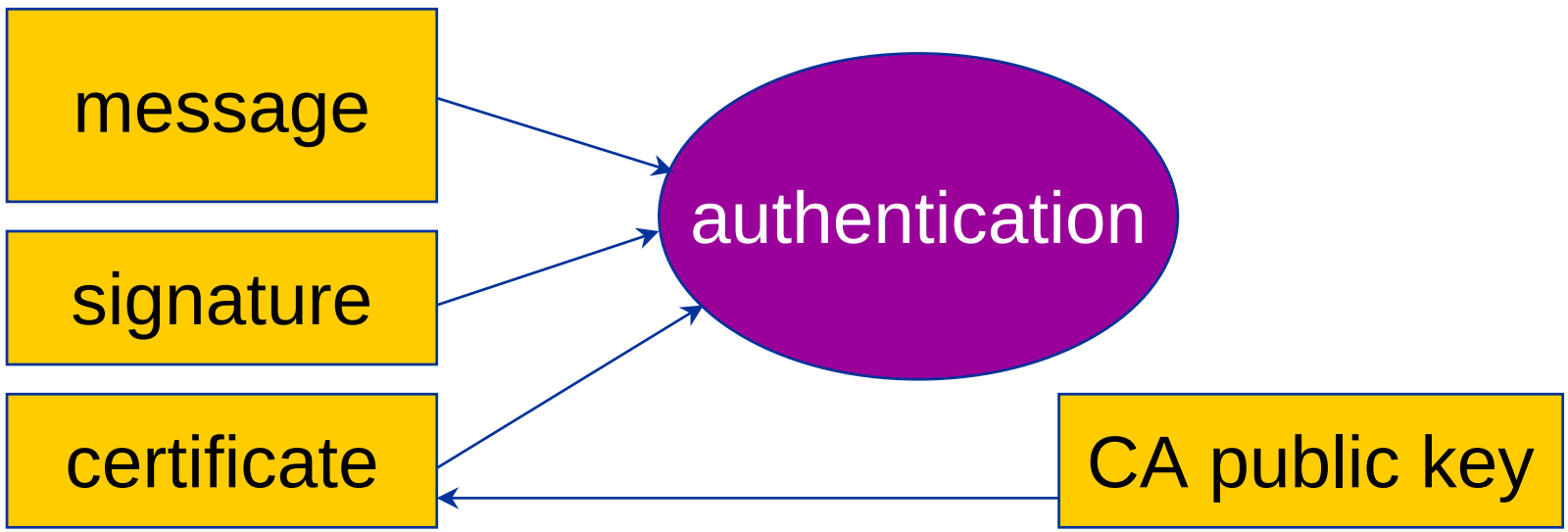
- The Database's existing strong authentication
- `key-cert` objects hold PGP public keys
- Widely supported (at least through extensions)
- E-mail only…

# Motivation for X.509

- *Improved Secure Communication* effort
  - Easier/more secure LIR-RIPE NCC communication
  - Single authentication token
  - Leverage existing technology and standards
- Use these client-side certificates with DB
- Web updates with strong authentication

# Proposal, Take 1

- Add a new "`auth:`" value
  - Contains the Distinguished Name in the certificate
- Get DN from certificate in messages
  - SSL and S/MIME messages include certificate
  - Certificates are signed by RIPE NCC CA

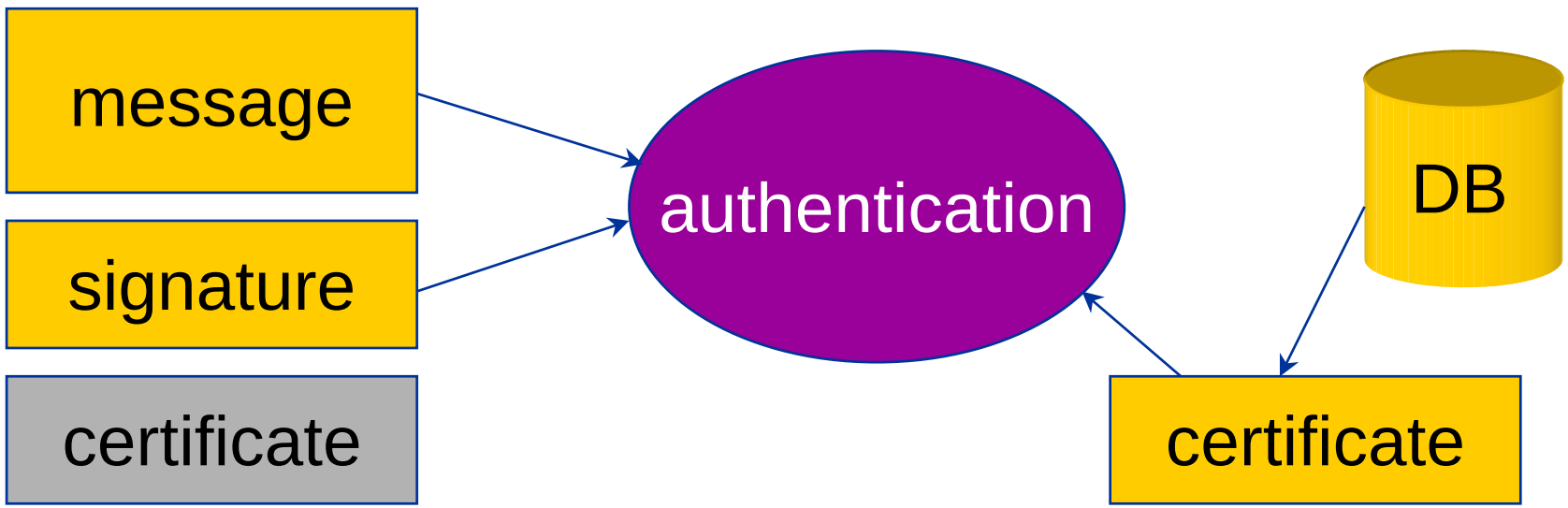


# Problems with Approach

- Database is not self-contained
  - Requires separate, non-public, CA configuration
- Certificates only from specific CA(s) allowed
  - Non-LIR users still want strong web authentication
  - Users may already have certificates

# Proposal, Take 2

- Add a new "`auth:`" value
  - Contains the identifier of a `key-cert` object
- Add a new type of `key-cert` object
- Don't verify certificates, verify messages



# New `key-cert` type

- Similar to PGP `key-cert` objects
  - "`method:`" attribute distinguishes PGP and X.509
- Unique identifier
  - Auto-generated, like "`nic-hdl:`"
  - No collisions possible
  - No DoS possible

# Example X.509 key-cert

```
key-cert:    X509-14
method:      X.509
owner:       C=NL, O=RIPE NCC, OU=Members, CN=zz.example.user1
fingerprint: CF:88:4F:CB:C2:E0:15:51:68:45:DC:10:E1:F7:4A:4D
certif:      -----BEGIN CERTIFICATE-----
certif:      MIIDmzCCAwSgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBljELMA
   …
certif:      u+ABjCVGvUDjU2QP/D+B
certif:      -----END CERTIFICATE-----
mnt-by:      RIPE-NCC-PORTAL-MNT
changed:     lir-portal@ripe.net 20030830
source:      RIPE
```

# “auth:” value change

```
mntner:         EXAMPLE-MNT
descr:          mntner with X.509 auth
admin-c:        SK15964-RIPE
auth:           X509-14
mnt-by:         EXAMPLE-MNT
referral-by:    RIPE-DBM-MNT
changed:        user@ripe.net 20030830
source:         RIPE
```

# Usage

- Maintainer setup similar to PGP use today
  - Create `mntner` object
  - Create `key-cert` object
  - Add new "`auth:`" attribute to mntner object
- Web and synchronous updates
  - Use client-side certificate with SSL
- Mail updates
  - Send message clear-signed as S/MIME

# Making it Transparent

- LIR Portal can make it easier for members
  - Reduce learning curve for secure database work
  - Any CA can adopt similar techniques
- Create key-cert objects
  - LIR Portal create when issued, delete if revoked
  - Maintained by LIR Portal
- Make adding to maintainers easier
  - “maintainer manager” screen
  - Get certificate from SSL connection
  - Override not required, use existing passwords