RIPE NCC
RIPE NETWORK COORDINATION CENTRE

HTTPS in Trust Anchor Locators (TALs)

Tim Bruijnzeels | IETF101

The change

Can now do this

```
rsync://rpki.example.org/rpki/hedgehog/root.cer
https://rpki.example.org/rpki/hedgehog/root.cer

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAovWQL2lh6knDx
GUG5hbtCXvvh4AOzjhDkSHlj22gn/1oiM9IeDATIwP44vhQ6L/xvuk7W6
Kfa5ygmqQ+xOZOwTWPcrUbqaQyPNxokuivzyvqVZVDecOEqs78q58mSp9
nbtxmLRW7B67SJCBSzfa5XpVyXYEgYAjkk3fpmefU+AcxtxvvHB5OVPIa
BfPcs80ICMgHQX+fphvute9XLxjfJKJWkhZqZ0v7pZm2uhkcPx1PMGcrG
ee0WSDC3fr3erLueagpiLsFjwwpX6F+Ms8vqz45H+DKmYKvPSstZjCCq9
aJ0qANT9OtnfSDOS+aLRPjZryCNyvvBHxZXqj5YCGKtwIDAQAB
```

- ➡ Seems we had consensus on allowing one or more https or rsync URIs
- ➡ Obsoletes RFC7730 for readability

Why?

- Easier to host Trust Anchor certificates
- Easier to fetch for Relying Parties

Please review HTTPS Considerations

- Text adapted from delta protocol (RFC8182)
- Best effort TLS validation
  - Object security, verify that certificate matches “subjectPublicKeyInfo”
  - Using alternatives left to local policy

- Done?