Cryptographic Authentication Update
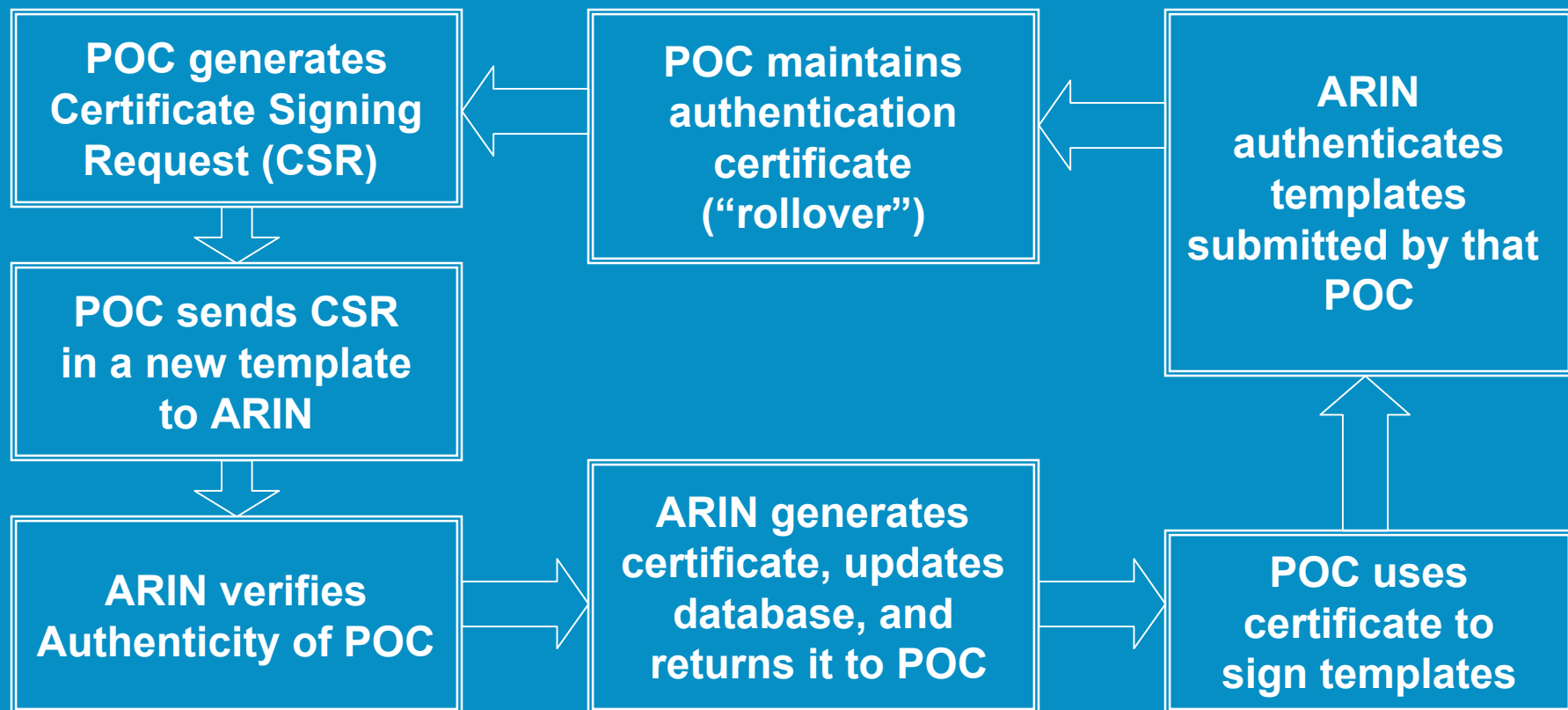
ARIN DBWG

Tim Christensen

Overview

- Background
- X.509 Authentication deployment overview
- Current Status
- What's Next?

Background

- **Community has asked for spectrum of authentication choices**
  - Password (md5-pw, des, etc.)
  - PGP
  - X.509

- **Implement one at a time, evaluate, and repeat**

- **Consider mail-from deprecation after evaluating adoption progress**

X.509 Authentication at ARIN

POC generates Certificate Signing Request (CSR) ←	**POC maintains authentication certificate ("rollover")** ←	**ARIN authenticates templates submitted by that POC** ↑
↓		
POC sends CSR in a new template to ARIN		
↓		
ARIN verifies Authenticity of POC →	**ARIN generates certificate, updates database, and returns it to POC** →	**POC uses certificate to sign templates**

Current Status

- **X.509 authentication mechanism deployed**

- **Workshop conducted at this public policy meeting on Sunday – available on your CD**

- **Templates, FAQ, and other resources available at http://ca.arin.net/request**

- **Several POCs are in the process of adopting X.509 strong authentication at this time**

What's Next?

- Expand use of X.509 to include other authentication needs
- Add another strong-auth type
  - Password (md5-pw, des, etc.)
  - PGP
- Expand X.509 to include more POCs, not just POCs associated with Subscriber Members

Thank You!