Using X.509 Authentication with ARIN's Database

Mike Loevner

Tim Christensen

Overview

- How X.509 Protects You
- Requesting a Certificate
- Identity Checking Procedures & Privacy
- Installing Certificates and Deprecating Mail-From
- Signing Mail to ARIN

How X.509 Protects You

- **ARIN currently uses MAIL-FROM authentication to authenticate template submissions.**
  - Registration Services processes templates received from the e-mail address listed as:
    - Administrative or Technical POCs associated with an Organization, and
    - Technical POCs associated with a resource.
- **This is a less secure way of authenticating users.**
  - Susceptible to mail header spoofing.
  - Open to domain (ergo, e-mail) hijacking.

How X.509 Protects You

- ARIN now provides X.509-based authentication to safeguard records. The authentication process allows certain POCs to obtain unique X.509 certificates that verify the identity of the sender.
  - Issued to individuals and roles.
  - Authenticated through an extensive process.

How X.509 Protects You

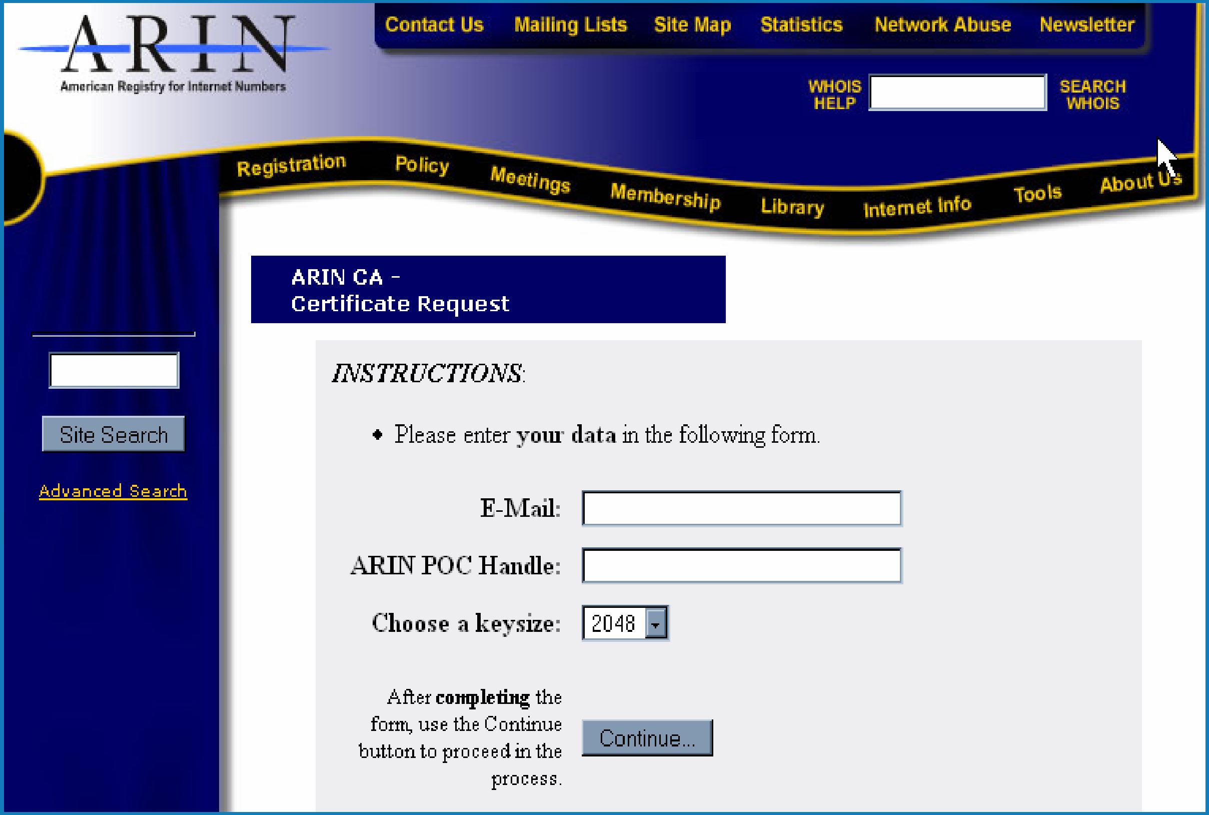
- **To be eligible for a certificate from ARIN, the POC applying must be the Administrative or Technical POC associated with a Subscriber Member Org ID.**
  - **The Administrative POC of the member's ORG ID <u>must</u> be an individual, not a role account.**
  - ORG IDs with a role account as the Administrative POC will be unable to use this feature.
  - Technical POCs may be role accounts and may receive certificates.

The CERT-REQUEST Template

```
Template: ARIN-CERT-REQUEST-0.1.0
## As of October 2003
############## IDENTIFICATION SECTION #################
1. POC Handle:
      ## Enter POC handle. **REQUIRED**
2. Additional Information:
      ## Provide additional information to clarify the
      ##registration request.
################ REQUEST SECTION########################
3. CSR:
        ## **REQUIRED**
        ## ARIN accepts PKCS#10 CSR or SPKAC formats
```

Requesting a Certificate (CSR)

- Visit http://ca.arin.net/request



ARIN CA - Certificate Request

INSTRUCTIONS:

- Please enter your data in the following form.

E-Mail:

ARIN POC Handle:

Choose a keysize: 2048

After completing the form, use the Continue button to proceed in the process.

Continue...

Requesting a Certificate (CSR)

- Visit http://ca.arin.net/request.
- Fill out the form and submit your data.
- You’ll receive an e-mail with a pre-filled template.
- Forward template to hostmaster@arin.net.

Identity Checking Procedures

- **ARIN will go through exhaustive identity checking procedures to verify the identity of a POC. This will include, but is not limited to, submission of documentation:**
  - identifying the applicant as the POC. This will include the submission of a challenge question and answer.
  - showing that the POC is associated with the ORG ID for which the POC is an Administrative or Technical POC.
  - showing that the Organization is a legal business entity.

How ARIN Protects Your Info

- ARIN permanently stores private information related to certificate requests in a secured location, to which only ARIN staff have access.

- ARIN releases no private information collected in the certification process to third parties except when subpoenaed by law enforcement authorities.

Certifying Role Accounts

- Remember, to use any X.509 authentication with ARIN, it is necessary for your organization’s Administrative POC to be an individual, not a role account.

- The Administrative POC must hold an ARIN certificate before a role account POC applies for a certificate.

Certifying Role Accounts

- Role account POC certificate requests are forwarded to Administrative POCs for their endorsement before ARIN continues with its certification process.

- Role account POC’s certificates may be shared among members of the role, or a certificate for each role user can be requested. It is the responsibility of the role account holder to administer and make decisions about who holds certificates.

Understanding ARIN's CA

- **ARIN asked me for documentation showing association with an organization, so it must be certifying my organization, right?**
  - ► Certificates validate the identity of the POC only.
  - ► Association with an organization is used initially to help determine and lend credibility to a POC's identity.
  - ► After the certificate is assigned, the POC has no required association with any Organization or resource.
  - ► The POC's certificate grants no special rights with respect to authority.

Understanding ARIN's CA

- **ARIN asked me for documentation showing association with an organization, so it must be certifying my organization, right?**
  - ►Certificated POCs may continue to use certificates to authenticate their identity even if their relationship with their original organization terminates.
  - ►The termination of relationship would remove authority over records, but not authenticity of the POC.

Understanding ARIN’s CA

- **I received a certificate for my POC. Which records can I update in the database now?**
  - ►The authorization model of ARIN’s WHOIS database does not change whether or not a POC is using certificate-based authentication.
  - ►If you are currently authorized to make specific changes to the database, that privilege does not change just because you have obtained a certificate.
  - ►For more information on the authorization model in ARIN’s database, check out the next workshop this afternoon, entitled “Managing Your ARIN Data.”

Installing the Certificate

- When ARIN issues your certificate, you will receive e-mail notification.
- Be sure to use the same computer and browser that you used to request the certificate, otherwise you will have difficulty in retrieving your certificate!

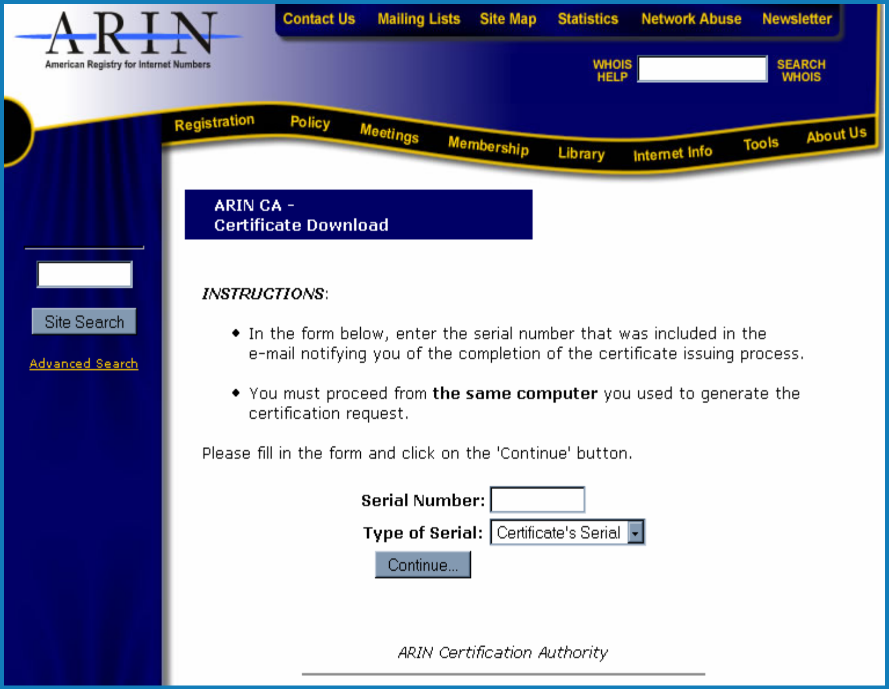
Installing the Certificate

- Follow the instructions – click the link to retrieve the certificate.

```
From: Hostmaster <hostmaster@arin.net>
To: <recipient e-mail>
Subject: Re: [ARIN-20040000.000] forward to hostmaster@arin.net |
    CERT-REQUEST template (fwd)

Your certificate for use with ARIN's registration system has
been generated. The certificate is identified by the
following attributes:

Serial number xx     DN serialNumber=xx,CN=HANDLE-
ARIN,O=arin,C=US

You may retrieve your certificate directly from:

https://ca.arin.net/cgi-
bin/pub/pki?cmd=getcert&key=XX&type=CERTIFICATE

…
Regards,
Registration Services
American Registry for Internet Numbers
```

Installing the Certificate

- When ARIN issues your certificate, you will receive e-mail notification.
- Follow the instructions – click the link to retrieve the certificate to your browser.
- Or visit http://ca.arin.net/pickup.



ARIN CA -
Certificate Download

INSTRUCTIONS:

- In the form below, enter the serial number that was included in the e-mail notifying you of the completion of the certificate issuing process.
- You must proceed from **the same computer** you used to generate the certification request.

Please fill in the form and click on the 'Continue' button.

Serial Number:

Type of Serial: Certificate's Serial

Continue...

ARIN Certification Authority

Installing Cert / Deprecating Mail-From

- Don’t forget to download ARIN’s CA certificate, so that you ‘trust’ ARIN (which makes your certificate ‘work’).

- If necessary, export the certificate from your browser into a file, and transport and install that certificate file into the X.509-enabled MUA of your choice.

Installing Cert / Deprecating Mail-From

- When complete, send a signed confirmation e-mail to hostmaster@arin.net, who will check that your signed e-mail can be authenticated.
- You will receive an e-mail response notifying you to submit all templates using a signature generated by the use of the certificate for all further ARIN communication (this deprecates Mail-From authentication for your POC).

Signing E-mail

- **Using common MUAs?**
  - Refer to ARIN’s FAQ to find out which MUAs are X.509-enabled.
  - Install and use the certificate according to your MUA’s instructions.
- **Using scripts?**
  - Consider using OpenSSL in your script process to sign script-generated templates.
  - Refer to ARIN’s FAQ on using OpenSSL to sign messages generated in a process.

Using My Certificate

- **What can my certificate be used for?**
  - Only for signing e-mails sent to ARIN.
  - Not for encrypting e-mail sent to ARIN.
  - Only authenticates the sender's identity.
  - No third party use.
  - See http://ca.arin.net/cps for ARIN's Certification Practices Statement.

Questions?