



Authentication for Hostmaster Robot

Filiz Yilmaz, RIPE NCC

Outline

- History:
 - Secure Communications with LIRs (PKI Project)
 - What happened from last meeting to today?
- Hostmaster (HM) Robot with X.509 and PGP
 - Admin Initialisation
 - User Initialisation
 - Mails from LIR
 - Mails from RIPE NCC
- Where is it useful?
- Summary
- Possible Future Developments
- Questions & Answers



Secure Communications with LIRs a.k.a PKI Project

- Goals:
 - Security
 - Authentication, non-repudiation and confidentiality
 - Convenient and easy to use
 - Possibility of single method for security
- Documented in RIPE NCC activity plans
- “Formal” proposal to community in April 2003
 - Uses X.509 technology
 - Phased implementation
 - Phase 3: Registration Services communications (Authentication for Hostmaster Robot)

What happened from last meeting to today?

- Before RIPE 47: discussion document
<http://www.ripe.net/ripe/mail-archives/ncc-services-wg/2004/msg00016.html>
- Presentation at RIPE 47
<http://www.ripe.net/ripe/meetings/ripe-47/presentations/ripe47-db-x509.pdf>
- Discussions on ncc-services-wg list
- Collected feedback
- Not only X.509 but also PGP support!
 - Authentication for Hostmaster Robot with X.509 and PGP !



HM Robot with X.509 and PGP Admin Initialisation

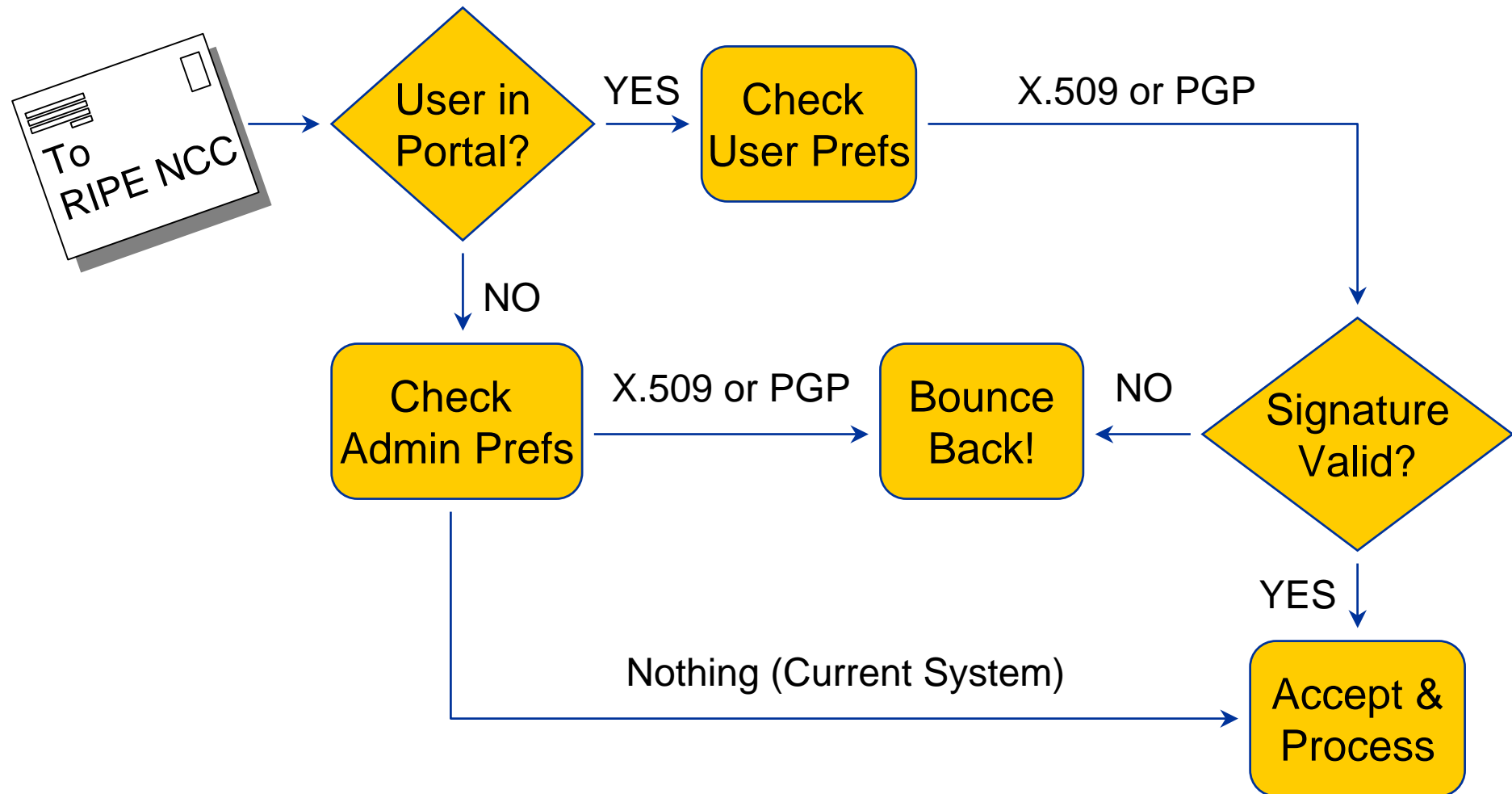
- LIR Portal Admin Account
- Admin to set “Administrative Preferences”
 - For mails from LIRs to RIPE NCC:
 - Nothing (Current System) or,
 - X.509 signed mail from member contact required or,
 - PGP signed mail from member contact required
 - For mails from RIPE NCC to LIRs:
 - PGP signed mail from RIPE NCC (Current System) or,
 - X.509 signed mail from RIPE NCC required



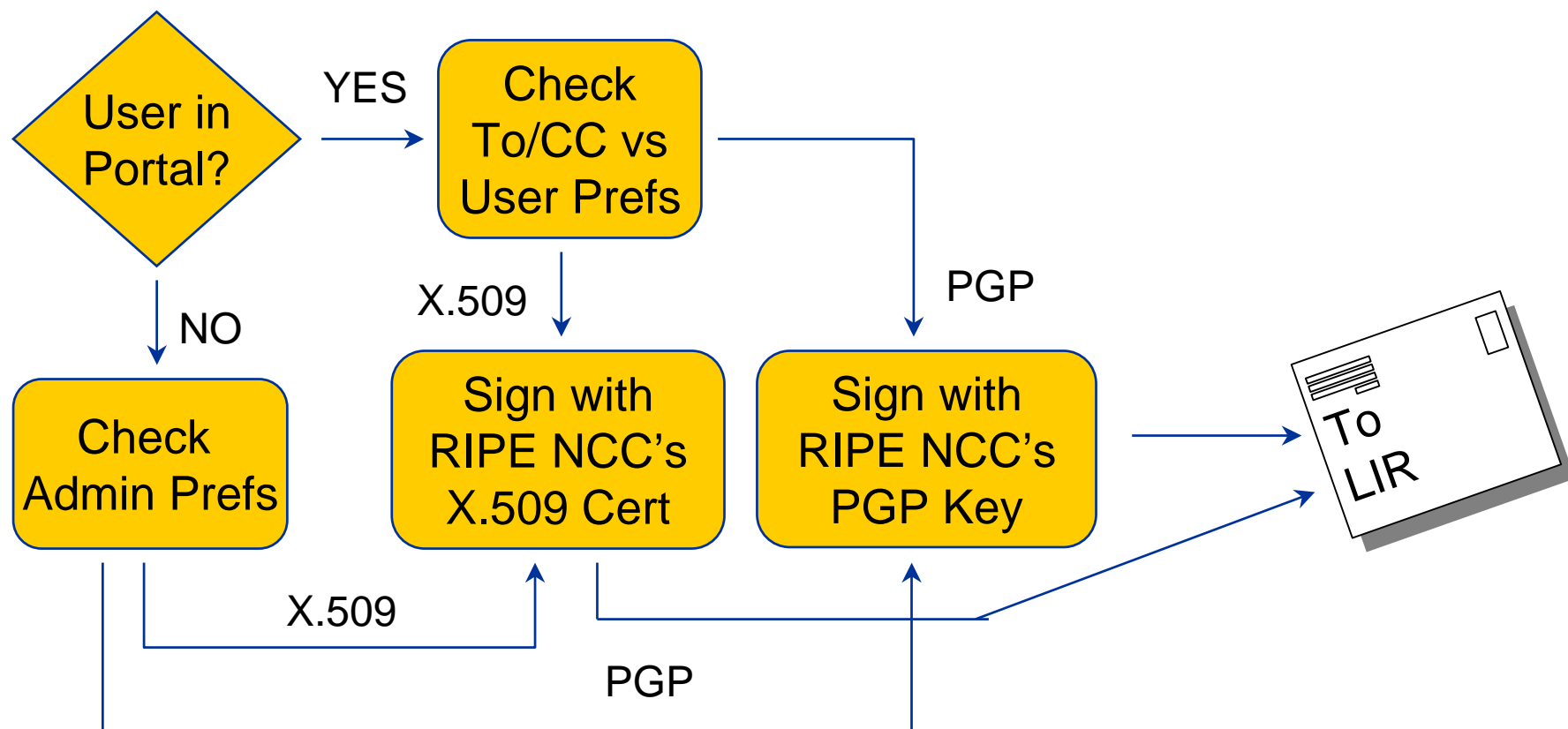
HM Robot with X.509 and PGP User Initialisation

- Users to set “User Preferences”
 - Same as admin but limited within “Admin Preferences”
 - Create X.509 certificate from portal or
 - Upload PGP key via portal

HM Robot with X.509 and PGP Mails from LIRs



HM Robot with X.509 and PGP Mails from RIPE NCC



Where is it useful?

- Non-repudiation – new employee can securely start communicating with RIPE NCC
- Employee leaves the LIR – will not be able to contact with RIPE NCC on behalf of LIR
- Member knows the reply is really coming from RIPE NCC

Summary

- Secure communication requested by community
- Suggested and Collected feedback
- Uses X.509 and PGP
- Provides authentication and non-repudiation
- Current system will still be available for those who do not want to use extra security

Possible Future Developments

- Encryption (???)
 - Need feedback !
- More areas of communication to secure:
 - Billing (Encryption ???)
 - ???

Questions & Answers

