

Using InCommon Client Certs for eduroam

Jeff Hagley and Ryan Martin

January 23rd, 2012

Internet2 Winter Joint Techs

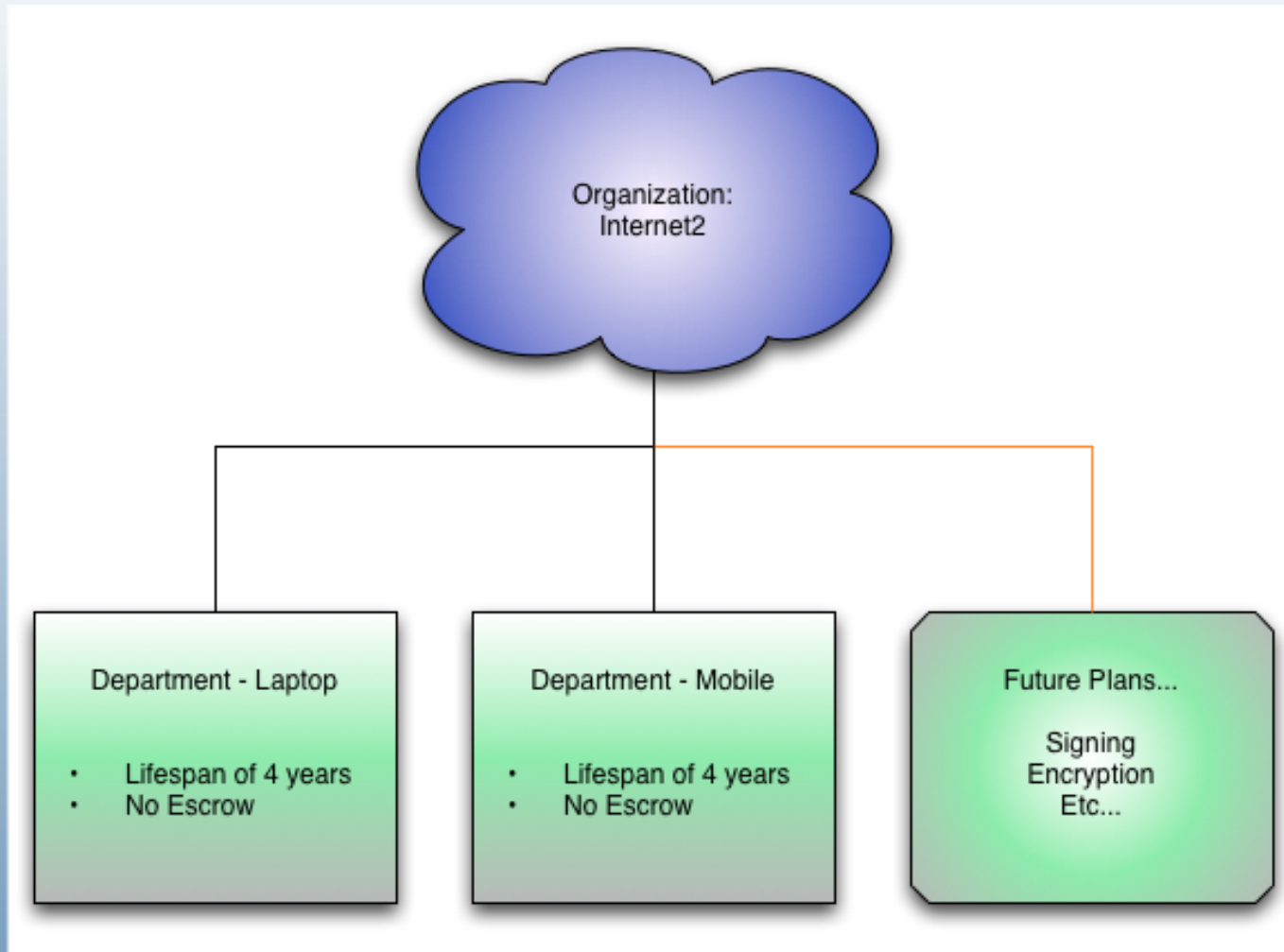
Why we Chose to use InCommon Certs

- Provide implementation details and lessons learned for the R&E community
- Cost
- Infrastructure
- Same interface as all of our SSL certs
- Ability to integrate future InCommon / Comodo products

RADIUS Setup

- FreeRADIUS
 - CRL Checking
 - BASH script to update this
 - One issue is that Comodo doesn't have a set time of day to issue CRL, supposedly happens every 23 hours
 - Common CA Cert Chain across InCommon
 - All InCommon Members have same signing Intermediate Cert
 - Only allowing Internet2 authentication
 - Proxy controls this
 - Cert Fragmentation Size

Cert Deployment Hierarchy



Documentation and Policies

- Master Key Escrow Policy
- Certificate Revocation Policy
- FreeRADIUS setup information
- Installation on Clients

Client Setup

- Used “+” sign in email address to issue multiple certs
 - Comodo added this after a bug report from us, ticket ID ETJ-152871
 - Using “+” sign to get one user in more than one department
 - Keeps email client from automatically using the cert for signing and encryption
 - Issues separate role based certificates
 - Easier than email aliases

OS Deployment

- iOS 4.3.5 and newer doesn't work, previous versions do
- Mac OS 10.6 and 10.7 works
 - We were having trouble with eap-tls on 10.6 and it seems much more stable in 10.7
- Windows 7 works (limited experience, we are Mac people)

Issues

- iOS 4.3.5, and iOS 5.x issue
 - We would love to have others test this and report it to Apple
 - Bug ID 10080052
 - Now have an open ticket with Apple on this
 - It is currently under review by Apple Engineering
- OCSP and FreeRADIUS vulnerability
 - CVE-2011-2701
 - Fixed in newest version of FreeRADIUS
- Users can only be assigned to one department (Comodo is aware of this issue)

Issues

- After our pilot ended in the middle of October, we used the csv import function to add the rest of our users
 - The automatically send invitation created and sent invitations that were invalid
 - Needed to manually send invites to users
 - Comodo has fixed this bug now

Issues

- PIN vs Password on web enrollment form
 - Ticket ID NHQ-579831
 - Password is a required field, only used to self revoke a cert
 - PIN is what is needed to install the cert on a client, not a required field
 - We have asked that these be merged to a single password to manage the cert
 - Comodo has added a help field, but most users won't notice that
 - Our suggestion is for our users to use the same password in both the PIN and password fields

Documentation Discrepancies

- Comodo Support Ticket RHK-693913 covers the following issues:
 - Documentation states you can only have one cert per email address, we have found you can have 2.
 - Document is ambiguous about a key usage template of “none”
 - Document shows multiple terms are available for a given department, yet only the default term is used.

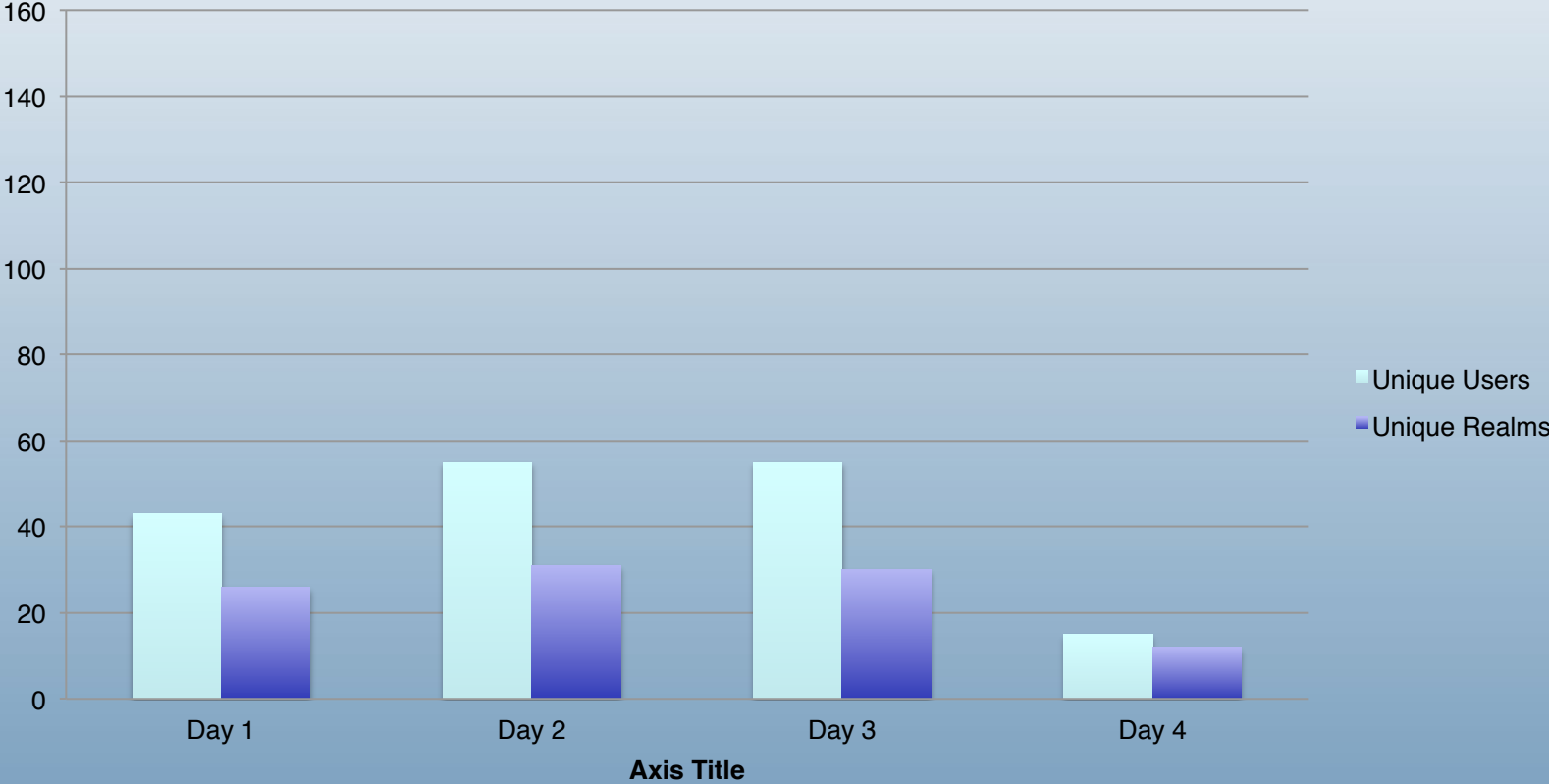
Future Plans

- OCSP implementation
- Email signing
- Email encryption

QUICK INTERNET2 MEETING EDUROAM UPDATE

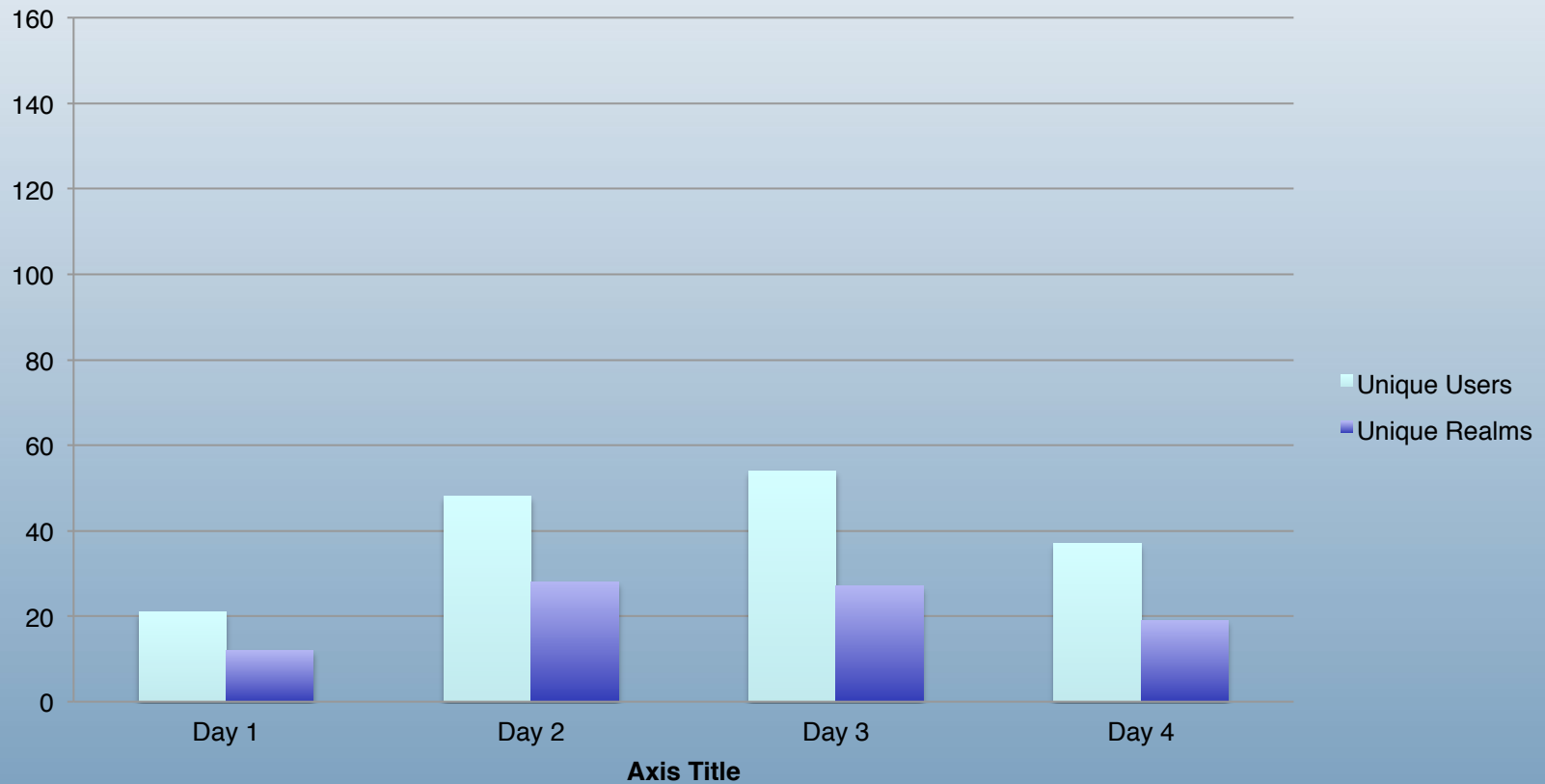
eduroam Growth at Internet2 Meetings

SMM10



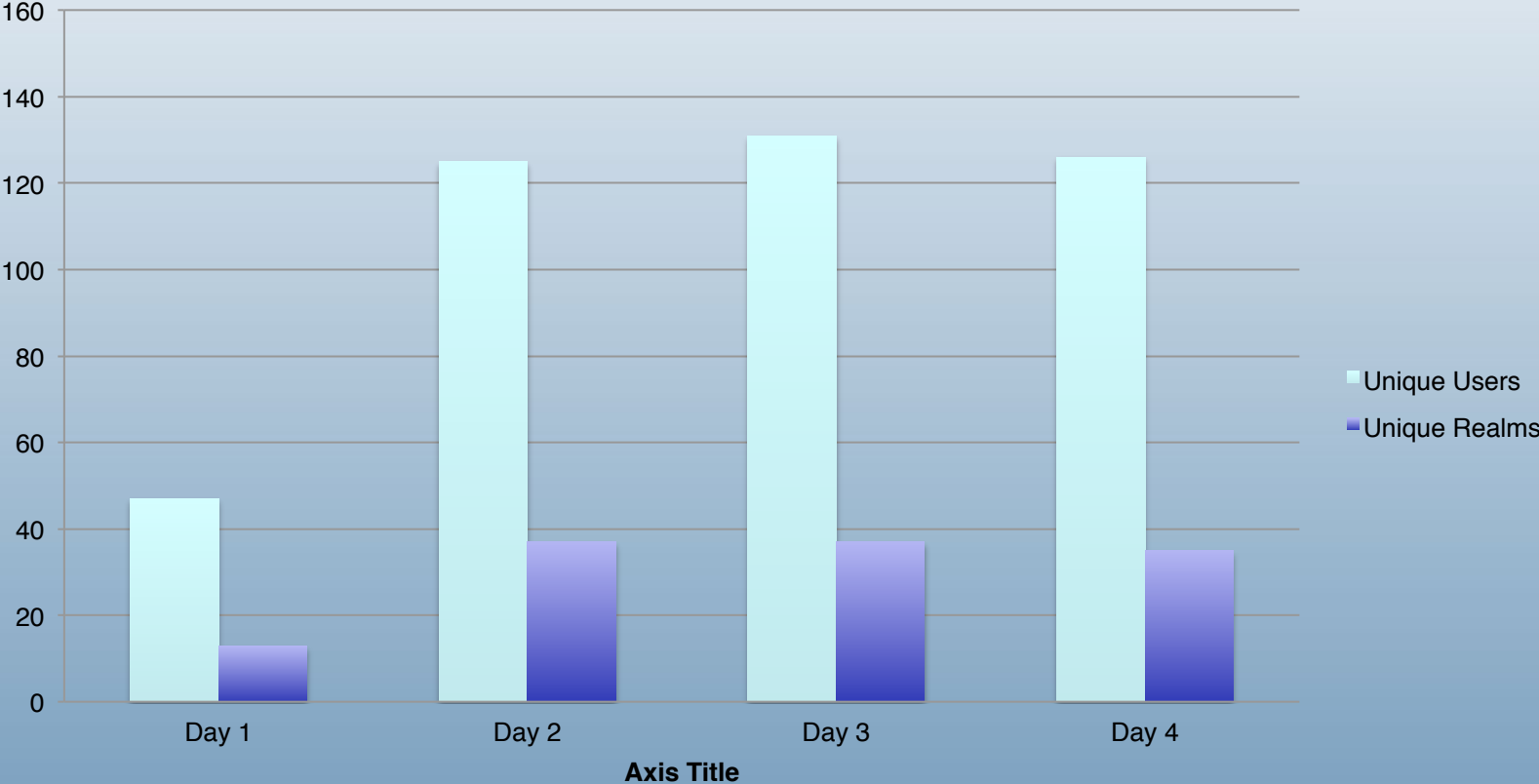
eduroam Growth at Internet2 Meetings

FMM10



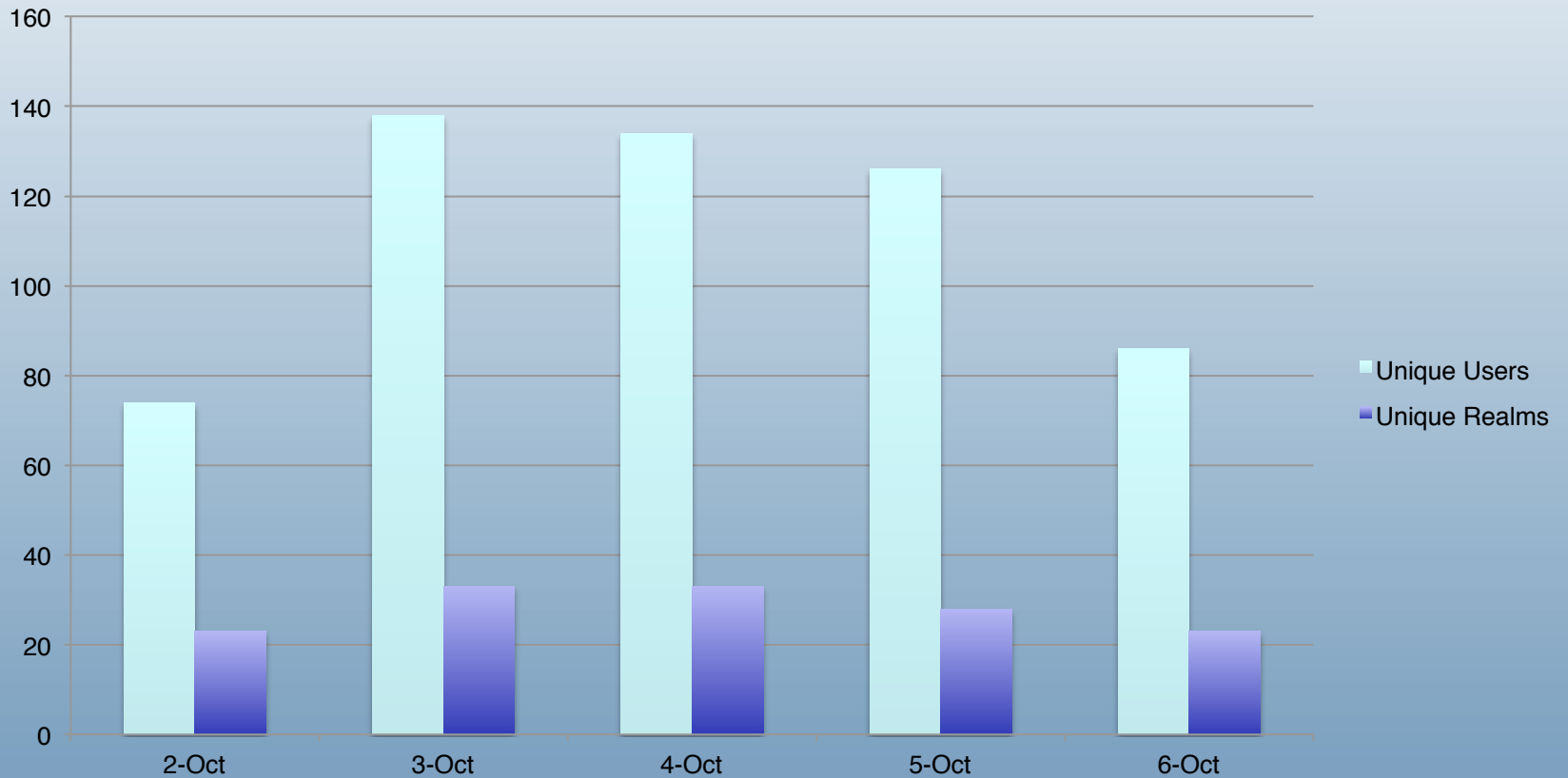
eduroam Growth at Internet2 Meetings

SMM11



eduroam Growth at Internet2 Meetings

FMM11



EDUROAM IS AVAILABLE HERE

Thanks to the meeting hosts for getting this up and running

Contact Info

- Jeff Hagley – hagleyj@internet2.edu
- Ryan Martin – rmartin@internet2.edu