

## UC Authentication Workgroup Meeting

UC Office of the President

February 26, 1999

10:00 a.m. - 3:00 p.m.

Attendees: Marina Arseniev (UCI), Peter Brantley, Denis DeLaRoca (UCLA), Mike Friedman (UCB), Joan Gargano (UCOP), Sal Gurnani (UCOP), Russ Harvey (UCR), Ron Klatchko (UCSF), Benny Minn (UCOP), Pete Neilson (UCLA), Brian Roode (UCI), Vance Vaughan (UCB), Ken Weiss (UCD), Frank Whittemore (UCSD)

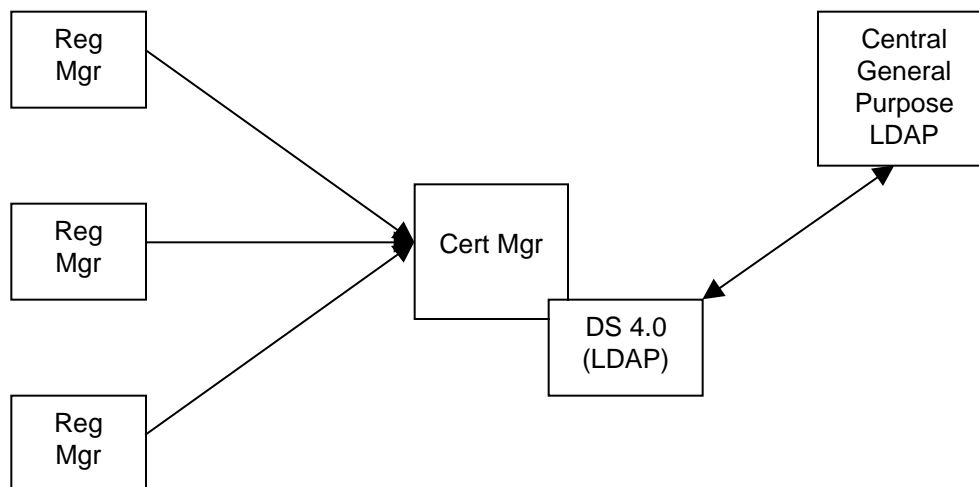
### I. Netscape Presentation - Certificate Management System 4.0

Currently available in beta test.

#### Scalability

New architecture for the certificate authority supports:

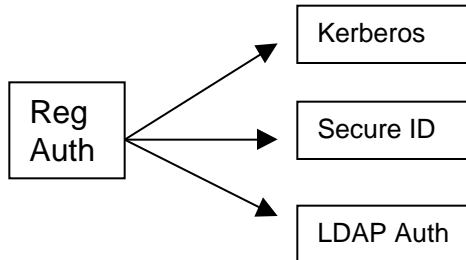
- □ PKCSH 11 Hardware Acceleration
- □ Multiple registration authorities link to central certificate authority.
- □ DS 4.0 (LDAP server) can manage 50 million entries, 6500 reads/second
- □ Key Recovery Authority - Data Recovery Manager
- □ Browser independent issuance of certificates



## **Extensibility**

### Authentication API

Registration Authority has APIs to Kerberos, Secure ID, LDAP authentication, one time PIN interface or other systems



## **Customization**

- Policy API/Policy Module for rules based issuance.  
Supports validity periods up to the second.
- Job scheduling notification engine  
Event based - email notification of events which require human intervention such as certificate renewal.

## **PKI**

PKI features are targeted for full deployment in the 5.0 browser. Plugins will be available for the 4.5 browser.

- Certificate Revocation List publishing to an LDAP directory
- CRL checker
- CRL distribution points
- Online Certificate Status Protocol (OCSP)
- CMC over CMS (PKIX)  
(CRMF/CMMF)
- CRS/CEP - Cisco router protocol authentication
- Virtual Private Network certificates

## **Metadirectory 1.0 - available late 1999**

- Join engine
- 20 pre-built connectors
- 2 way synchronization to Oracle

### **Certificate Portability Options**

- Floppy Disk with PKCS-11 plugins
- Hard Token
- USB device - Aladdin

### **Netscape Brower 5.0 (Open Source)**

- Will include a feature which restricts the presentation of a particular certificate to a limited domain.
- Will delete old root CAs and reinstall new root CAs.
- Dual key generation, signing and encryption. Keys are stored in the Data Recovery Manager.

### **Root CA Signing**

Netscape has agreements with Verisign and Thawt to provide root CA services.

### **Contact Information**

Mmullany@netscape.com

## **II. University Directory**

The workgroup had an informal discussion with Benny Min to get answers to questions about the University Directory as it relates to their system development work for authentication and authorization.

## **III. Review of the UC Authentication and Authorization Architecture Statement**

The workgroup reviewed the latest draft of the UC Authentication and Authorization Statement. Recommended changes:

Add a definition for a Certificate Authority Server.

Add a section on the process to issue anonymous certificates.

Add a section on IP address authentication.

## **IV. Review and Update the Workgroup Workplan**

The workgroup reviewed the workplan for work through June 15, 1999. Most items are progressing according to the schedule.

## **V. Next Meeting**

The group will meet on May 17, 1999 by videoconference to plan the work for the last four months of the workgroup.