UI Digital Certificate Service

IT Security Office – September 08, 2010

Agenda

- Current University SSL process
- What is the InCommon Federation?
- Digital certificates
- What is in scope
- New buzz words
- The Process
- Next Steps
- Who were the early adopters
- Questions

Current UI SSL Service

Biggest Change – not only with Thawte

System Administrators have to generate CSRs with a 2048-bit key

Chained certificate hierarchy i.e. root, intermediate, and SSL certificates

Ground control to Major Tom

When generating a NEW CSR (system specific) you have to make sure you supply the following information in order to avoid additional vetting or revocation of your request.

Common Name: **Domain Name of the registered system**
Organization Name: **The University of Iowa**
OrgUnit: (**Your department name**)
City/Location: **Iowa City**
State: **Iowa**
Country: **US**

- Once you have the information you submit the request via the Certificate Request Form
  - Here we require you add/confirm a technical, billing and organizational contact.

Ground control to Major Tom

Once the ITSO receives the CSR it is processed on behalf of the requesting unit.

Historical impetus behind this was mostly tied to business end process, as this was a charged service there was a need to have a stop gap in-place to avoid unnecessary costs that both central IT and the requesting department would have to bear.

Most requests are signed within a 30 minute period once processed through the CA.

Best thing since sliced bread

- Various factors influenced the need to look around for a better and more economical service.
  - Support and communication
  - Total Cost per certificate
  - Overhead - administrative and billing costs
- Most Higher Ed institutions use the same CA we do and all had similar unsatisfactory reports.
- Enter – The InCommon Federation.

Who is the InCommon Federation

- InCommon is a higher education collective whose mission is to create and support a common framework for trustworthy shared management of access to on-line resources in support of Education and Research in the United States.

InCommon Cert Service

- Service created by and for the higher education community to provide unlimited server and personal certificates for one low fee.

Unlimited Digital Certificate Offerings

- SSL Certificates - *ready to go, post test phase*
- SAN Certificates
- Wild Card Certificates
- Client
- Personal Certificate

In Scope – first steps…

- Deploy a replacement service for issuing digital certificates.
  - First and foremost is the need to migrate from the current vendor to the new vendor for SSL certificate issuance.
  - During the pilot phase of the project plan, the project team will test the SSL service on different systems. Some have volunteered – others may like to jump on the band-wagon?

InCommon Nomenclature

- CSM – Certificate Services Manager
- RAO – Registration Authority Officer
  - The RAO for the University is the IT Security Office
- DRAO- Departmental Registration Authority Officers
- End-User

InCommon Digital Certificate Service @ The University of Iowa

There are a few changes to the service that would hopefully ease the process and end user experience for all.

- *FREE* - cant beat that now can you?
- Structure change: creation & inclusion of an RAO, DRAO & End-User

Who gets to become an RAO, DRAO or End-User, owner and requestor?

What are their responsibilities?

InCommon Digital Certificate Service @ The University of Iowa

An RAO would basically be the ITSO – with higher permission levels mainly to audit and run reports at an enterprise level.

A DRAO would be an administrator who has the rights to access manage and request SSL certificates for the domains that have been delegated by the RAO.

- They have no access to manage SSL certificates belonging to other departments
- They can create other DRAO SSL admins but only for the departments they have access to.
- They can view reports, edit access control lists and modify email templates ONLY for the department they have access to.

InCommon Digital Certificate Service @ The University of Iowa

An End-User would be a person who has made an application for an SSL certificate using the self enrollment form.

- The owner would be the Administrator that approved the certificate
- The requestor would be the person that filled out the initial application for the certificate

Nuts n' Bolts

Ways to request an SSL certificate

1. Web form and
2. via the application

A DRAO and End-user can all request an SSL cert via the web enrollment form

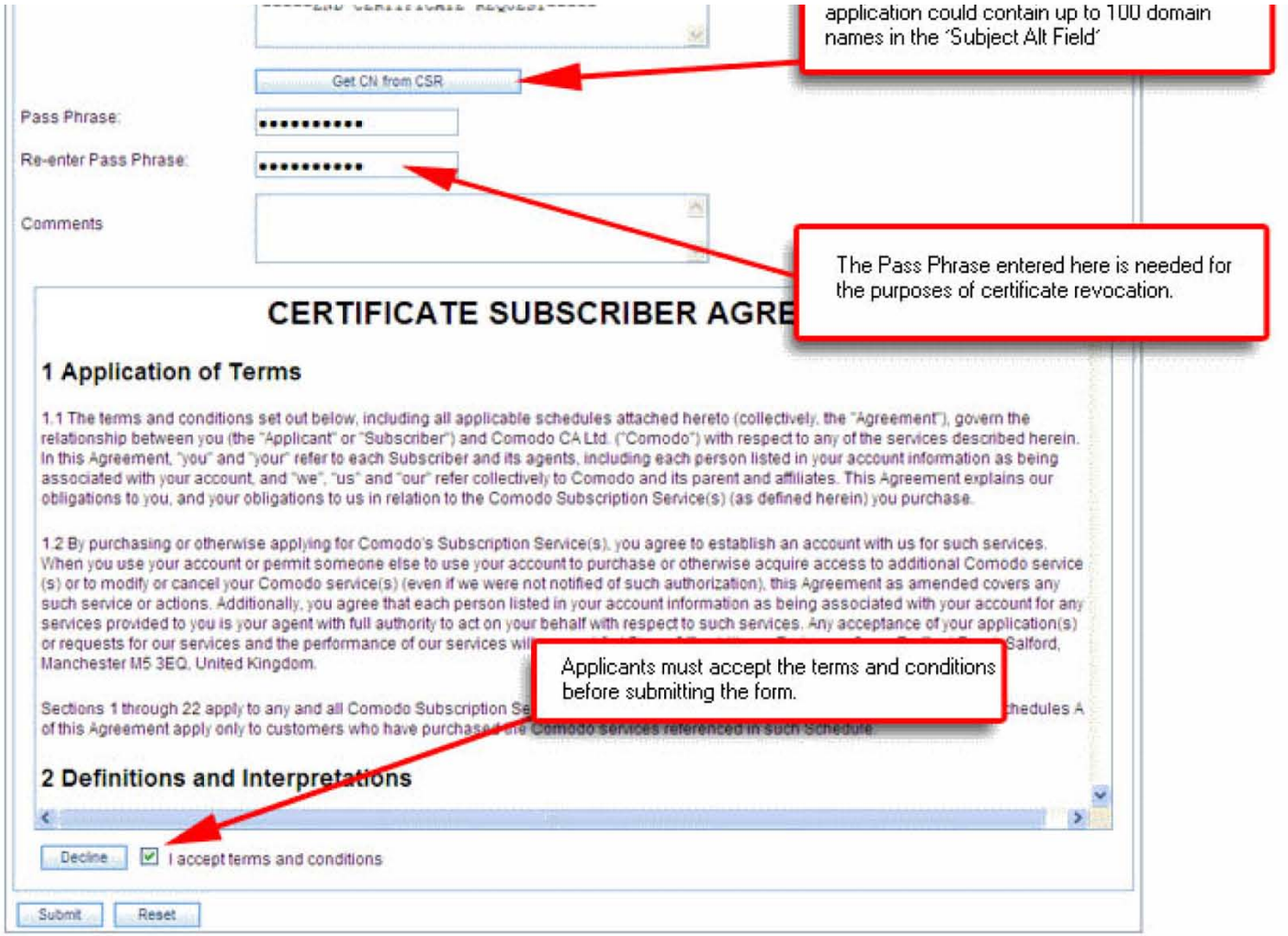
The DRAO can only issue SSL certs through the application for the departments under their control

RAOs can issue SSLs for anyone across the Organization

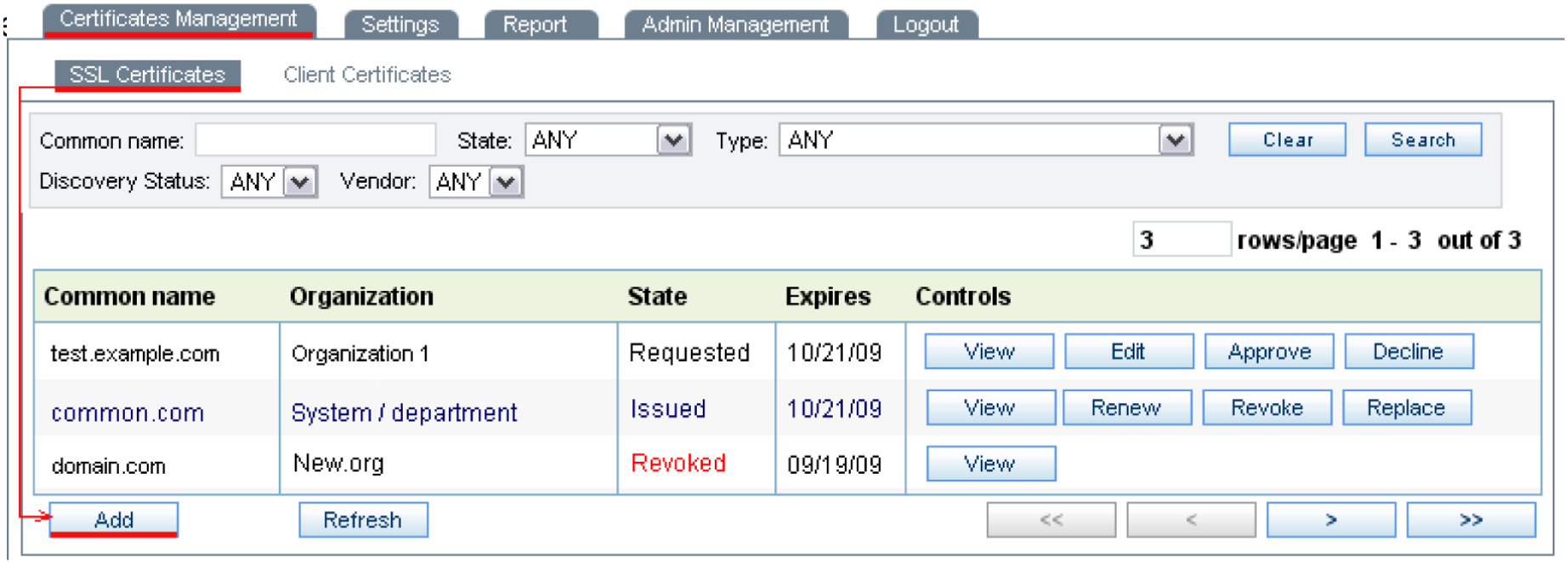
Web Form


Edit Organization:
General
Client cert
SSL
Self Enrollment
Access Code:
ak45Wywf
Sync. Expiration Date
Sync. Month
Not used
Sync. Day
(1 - 31)
Web API
SSL Types
Customize
OK
Cancel
The Access Code for the domain will have been set by the administrator in the 'SSL' tab of the 'Edit Organization' interface.
SSL Enroll
Access Code: *
E-Mail: *
applicant@mydomain.com
Common name: *
mydomain.com
Certificate Type: *
Instant SSL Certificate
Server Type: *
AOL
Certificate Term: *
1 year
CSR: *
tMkBmQY1LINShQIDAQABoAAw
DQYJKoZIhvcNAQEEBQADgYEAaYazcyZ/alqU0cEF
pyqbVKrcOdidXjy92qRy/qNR
DDOhZ0vPHFDzI6iJPGRMIQLGz4sn0aj0HG+erlqD
en0L4IkE3hl8aUTi7pPO0V4o
CN2Dz+WSbXOK9UkWG6z13JIhzTD8RqHw1xNyAgRK
vXchHfmsDYn7dNbNDKpOwtQ3
uSg=
-----END CERTIFICATE REQUEST-----
Get CN from CSR
Pass Phrase:
Re-enter Pass Phrase:
Comments
CERTIFICATE SUBSCRIBER AGRE
The external applicant need not be an existing user in Certificate Manager, but that person's email address must be from the same domain as the domain or the application cannot proceed.
Clicking 'Get CN from CSR' will automatically populate the Common Name and, if relevant, the 'Subject Alt'field with the domain name(s) in the CSR - helping to avoid errors with the application. This feature is especially useful during the application for MDC's when the application could contain up to 100 domain names in the 'Subject Alt Field'
The Pass Phrase entered here is needed for the purposes of certificate revocation.

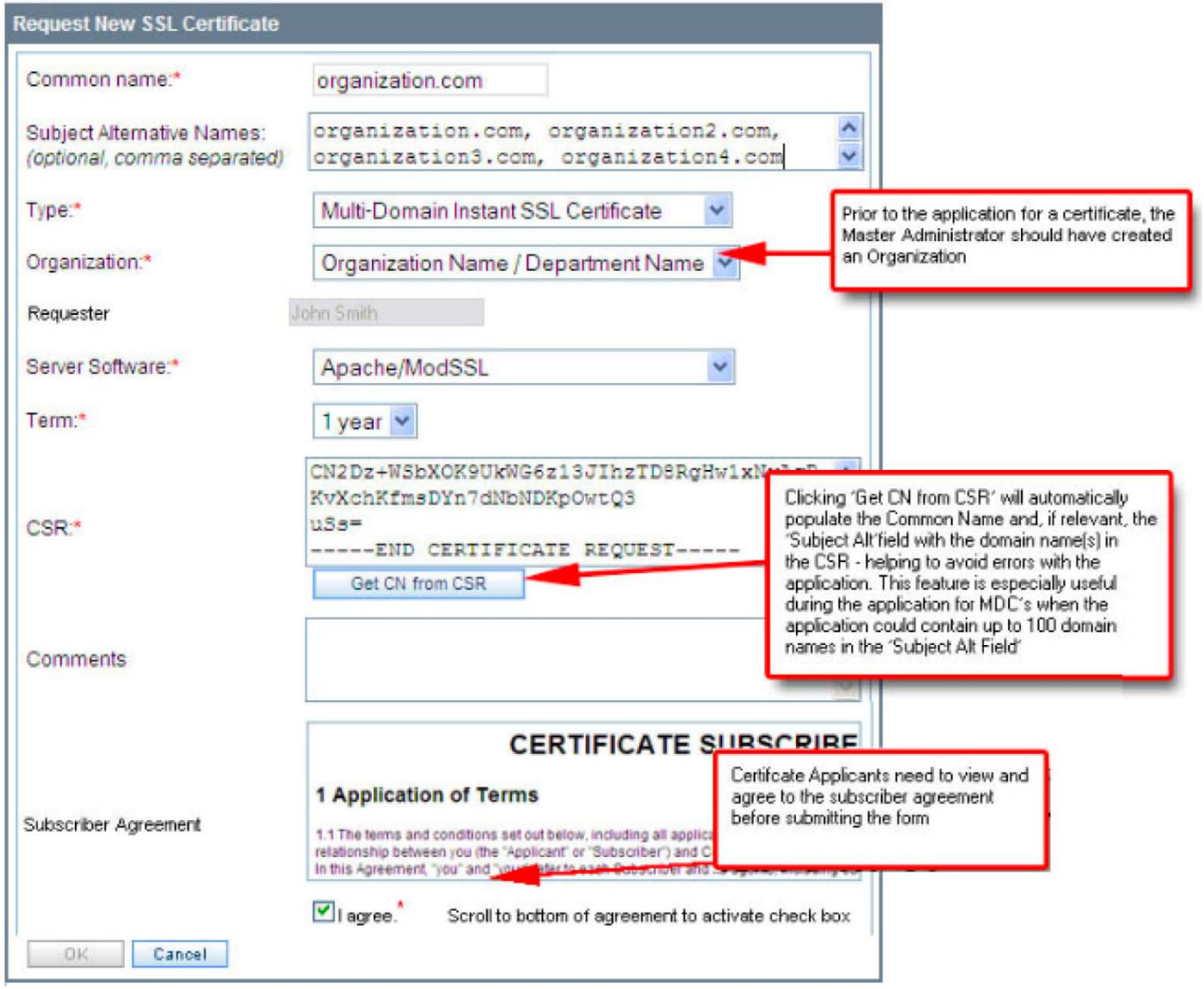
Web Form


application could contain up to 100 domain names in the 'Subject Alt Field'
Get CN from CSR
Pass Phrase:
Re-enter Pass Phrase:
Comments
The Pass Phrase entered here is needed for the purposes of certificate revocation.
CERTIFICATE SUBSCRIBER AGRE
1 Application of Terms
1.1 The terms and conditions set out below, including all applicable schedules attached hereto (collectively, the "Agreement"), govern the relationship between you (the "Applicant" or "Subscriber") and Comodo CA Ltd. ("Comodo") with respect to any of the services described herein. In this Agreement, "you" and "your" refer to each Subscriber and its agents, including each person listed in your account information as being associated with your account, and "we", "us" and "our" refer collectively to Comodo and its parent and affiliates. This Agreement explains our obligations to you, and your obligations to us in relation to the Comodo Subscription Service(s) (as defined herein) you purchase.
1.2 By purchasing or otherwise applying for Comodo's Subscription Service(s), you agree to establish an account with us for such services. When you use your account or permit someone else to use your account to purchase or otherwise acquire access to additional Comodo service (s) or to modify or cancel your Comodo service(s) (even if we were not notified of such authorization), this Agreement as amended covers any such service or actions. Additionally, you agree that each person listed in your account information as being associated with your account for any services provided to you is your agent with full authority to act on your behalf with respect to such services. Any acceptance of your application(s) or requests for our services and the performance of our services wil
Salford, Manchester M5 3EQ, United Kingdom.
Sections 1 through 22 apply to any and all Comodo Subscription Se
chedules A of this Agreement apply only to customers who have purchased the Comodo services referenced in such Schedule
Applicants must accept the terms and conditions before submitting the form.
2 Definitions and Interpretations
Decline
I accept terms and conditions
Submit
Reset

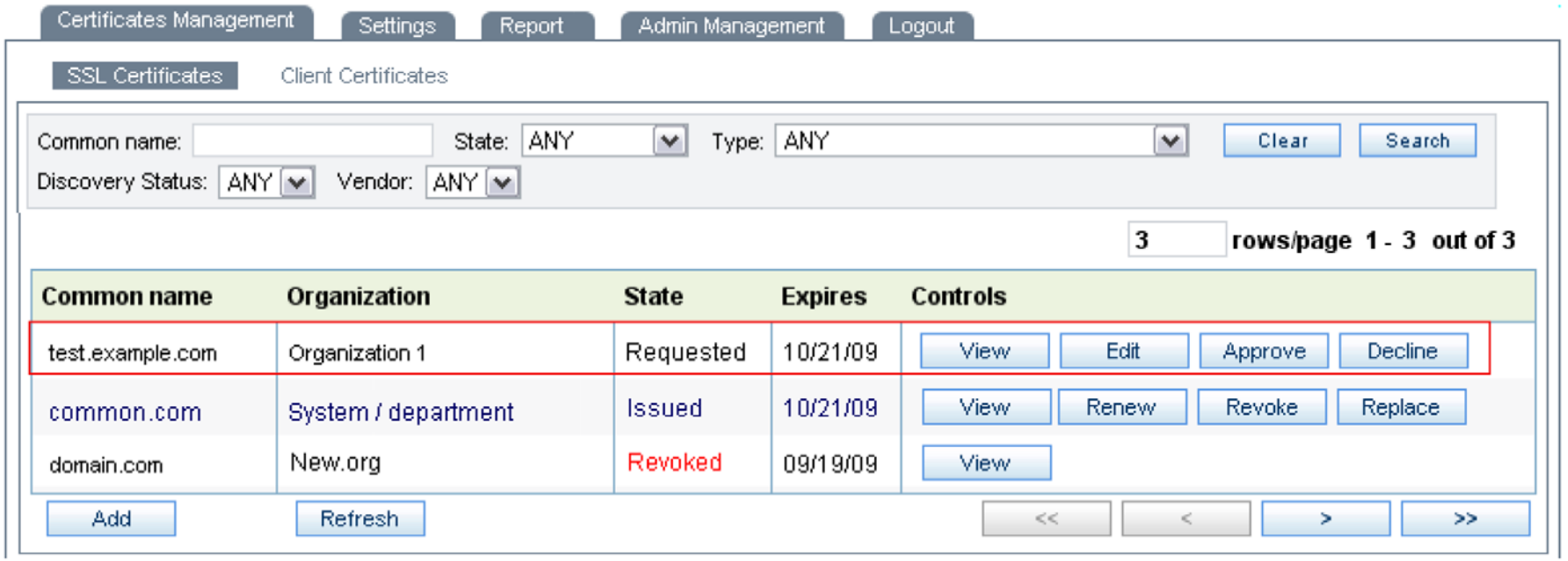
Web Application



Web Application



SSL Approval



Nuts n’ Bolts

Notifications

Notifications enable RAO and DRAO Administrators to set up and manage email notifications to various departments.

RAO –They can create new notification types and can edit settings for notification to the Organization and its Departments.

DRAO – can only see their own Department(s) in the 'Departments' column. The 'Organizations' area is not visible to DRAO's. They have rights to manage only the Department delegated to them.

In Scope – next steps…

- Define hierarchical Organizational administrative structure and process.
- Provide reporting and alerting service on validity
- Define security audit processes for issuance/renewal of SSL Certificates.
- Define types of SSL Certificates and validity periods of the Certificates.
- Define service model for the expansion of issuing SSL and other types of Certificates to the UI campus community
- Create help/FAQ documentation.

...and the early adopters are

- University of Alaska
- California Institute of Technology
- Carleton College
- University of California Berkeley
- Indiana University
- Iowa State University
- University of Minnesota
- Penn State University
- University of Texas System
- University of Virginia

Questions?

IT Security Office: security@uiowa.edu

Tel: 335 6332

Web: http://itsecurity.uiowa.edu