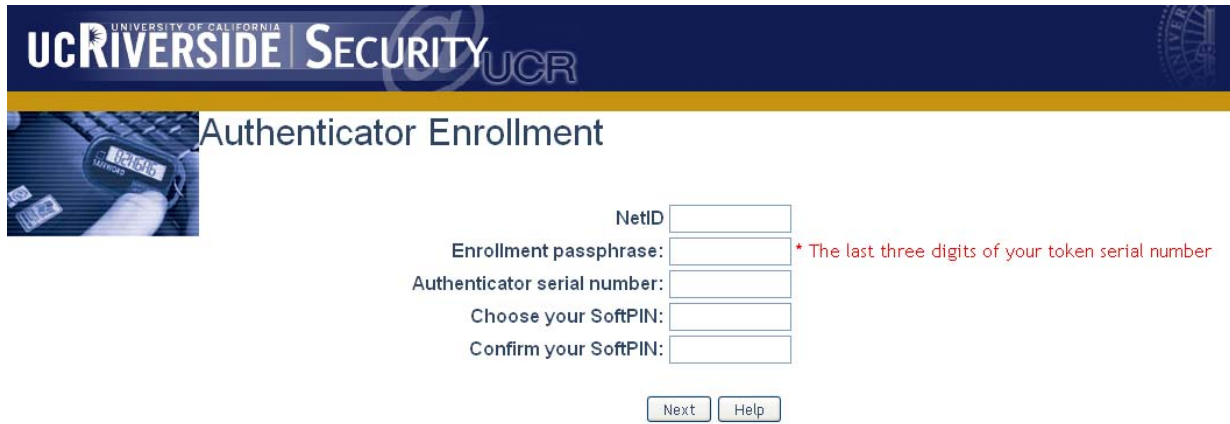


University of California, Riverside

Application for 2008 Larry L. Sautter Award for Innovation in Information Technology

University of California, Riverside – Password Token Integration with UCR's Identity Management



UCRIVERSIDE SECURITY UCR

Authenticator Enrollment

NetID:

Enrollment passphrase: * The last three digits of your token serial number

Authenticator serial number:

Choose your SoftPIN:

Confirm your SoftPIN:

For more information, please contact Russ Harvey, C&C Director of Computing Infrastructure and Security (russ.harvey@ucr.edu).

Project Summary

UCR's Two-factor Authentication project is a one time password generation technology using Secure Computing SafeWord tokens. While one time password (OTP) generation methodologies have been implemented on other university campuses, UCR has uniquely integrated the service into its single sign-on authentication environment, CAS (Central Authentication Services). The technology is open-source and works with Shibboleth. To authenticate to a user service, users can either enter their UCR Net ID password or a password generated by the Secure Computing token. Since the Secure Computing password entered at the CAS prompt also includes a 4 digit personal identification number (PIN), the process is two-factor.

Project Highlights

- Provides security against key-loggers, packet logging and general password theft.
- Computing & Communications staff have evaluated the tokens to access applications that use CAS (the UCR staff portal iViews, the campus calendaring system) and AYSO.
- Key administrative staff on campus have been identified to participate in a wider pilot, including staff that have complete access to UCR essential financial data, and regularly travel.
- Due to the success of the pilot, 150 additional Secure Computing silver tokens have been purchased.

Project Team Members

Russ Harvey
Stephen Hock
Song Bi
Andrew Tristan

Technical and System Overview

There are three main components to the integration:

1. The Secure Computing SafeWord Premier Access software
2. The Secure Computing Silver tokens
3. UCR's LDAP infrastructure

Premiere Access Software

Purchased from Secure Computing, this Solaris binary software is installed on a Sun V215 running Solaris 10. The Premiere Access software facilitates:

- User registration/enrollment
- User PIN changes
- Users can verify that their token is working properly
- Administrators can add tokens to the system

Silver Tokens

A token is a Key fob that generates a random, one-time use 6-character password when the user pushes a button. The user authenticates with the 6-character password along with a 4-digit Personal Identification Number (PIN).

LDAP Infrastructure

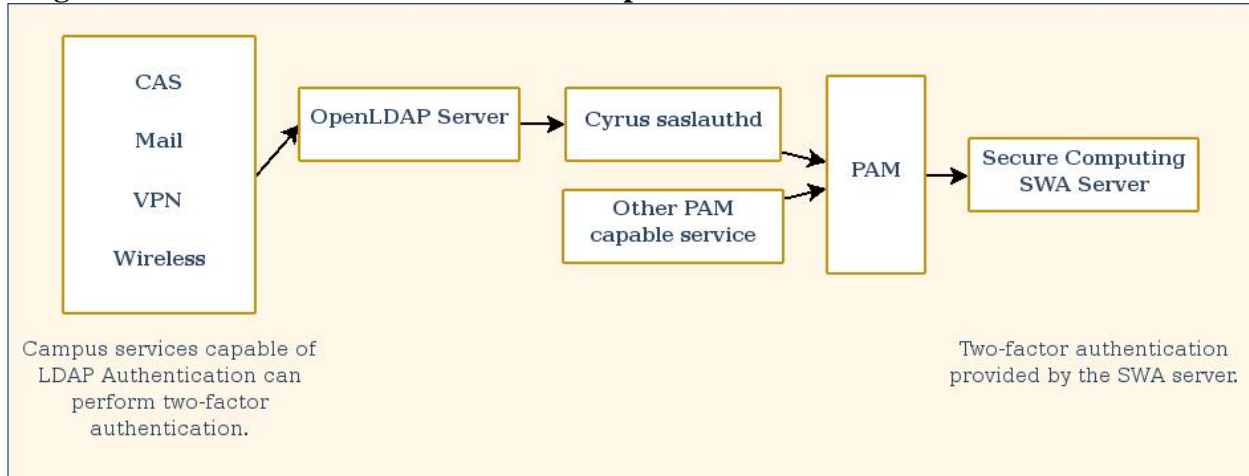
UCR's identity management infrastructure uses Open LDAP.

- Integration of Safeword with LDAP, enabling all services which currently perform LDAP authentication to use two-factor authentication. This includes CAS, VPN, wireless, dialup, campus mail services, etc. Campus Open LDAP servers were reconfigured to enable this behavior, and no modification of other authentication services was required.
- LDAP is configured to verify passwords by checking multiple ways in which a user may have provided their password. Using the Pluggable Authentication Module (PAM), LDAP can verify SafeWord generated passwords.
- No modifications were needed for CAS or VPN.
- Safeword authentication can be optional or mandatory for any user.
- A self-registration service makes Safeword token distribution easy.

Timeframe of Implementation

2007	Purchased Premiere Access software and tokens.
October – December 2007	LDAP integration complete and SafeWord environment installed.
December 2007	10 tokens distributed to C&C staff.
June 2008	Provide key UCR personnel with tokens for them to use in day-to-day activities.
September 2008	Complete Premier Access management web site for department administrative staff.

Diagram of UCR 2-Factor Authentication Implementation



Testimonials

“Very easy to use. I can now access campus applications such as Webmail from a coffee shop or public terminal and not worry about someone stealing my password.”

Bob Grant, Director of Technology

Importance and Relevance to Other Institutions

Other UC campuses have expressed interest in UCR’s implementation and requested guidance regarding their installation.

Vision for the future

Following a successful deployment to Computing & Communications staff, plans are to deploy to all campus staff and faculty (who wish to participate).

Site URL

<https://isdev1.ucr.edu>

Submitted by

Eric Martin

Project Manager

UC Riverside Computing & Communications