

Cosign

A Web Credential Management Solution

Mark Earnest
Lead Systems Programmer
Emerging Technologies
The Pennsylvania State University

What is Cosign

- Kerberos integrated Login Server
 - Runs on Unix/Linux
 - “central hub” of the Credential management system
- Apache Auth Module
 - Provides authenticated access
 - Communicates with the Login Server
 - Receives Kerberos credentials from Login Server
- ISAPI Auth Module
 - Provides authenticates access
 - Communicates with the Login Server

Features

- Web single-sign on
- Kerberos credential passing (apache only)
- Prevents password from being exposed to the web server
- Cookie based persistent identity
 - Session cookies
 - Server-only scope (not domain)
- Universal Logout
- DFS access via Kerberos->DCE credential conversion (PSU developed)
- Planned integration with FPS

Login Flow

- User hits a Cosign protected web server
 - Web server cookie set, passed to Login Server
- Redirect to Cosign Login Server
- User authenticates via Kerberos
 - Login server cookie set, matched to web server cookie
- User redirected back to web server
- Via an out-of-band SSL connection, the login server tells the webserver the user's principal name and (optionally) Kerberos credentials
- The user is granted (or denied) access

Demo