CASifying the Big Green

A Grassroots Enterprise Project

Steve Cochran

JA-SIG Summer Conference

June 25th 2007

Who Am I

Manger, Special Projects
Dartmouth College

- Ongoing Responsibilities:
  - Directory
  - Authentication
  - Email
  - Calendaring
  - Web and File Services
- Recent Projects
  - WebAuth, Paperless Admissions Office, “Smart” System Status Notification, Authenticated Network Access

A Grassroots Enterprise Project

I. Gain support from Administration

II. Build consensus from technical staff

III. Receive allocation of resources needed

IV. The Easy Part: Build it

A Grassroots Enterprise Project

I. Gain support from Administration

II. Build consensus from technical staff

III. Receive allocation of resources needed

IV. The Easy Part: Build it

Support from the Top

- Security
  - Standardization of UI
  - Limiting Password Access
- Compatibility
  - Kerberos/Sidecar Limitations
  - Intel Macs & Vista
- New Features

A Grassroots Enterprise Project

I. Gain support from Administration

II. Build consensus from technical staff

III. Receive allocation of resources needed

IV. The Easy Part: Build it

A Grassroots Enterprise Project

I. Gain support from Administration

II. Build consensus from technical staff

III. Receive allocation of resources needed

IV. The Easy Part: Build it

Building The Team

- Technical Services
  - PM, Directory Admin, Webmaster
- Administrative Computing
  - DBA, Application Programmer
- Library Computing
- Academic Computing
- Graduate Schools

Project Overview

Purpose

Create a standard framework to handle user authentication for web applications.

Scope

Only address web application authentication.

Goals and Requirements

- Based on open standards
- Provide equivalent security to Kerberos
- Compatible with common web servers
- Work with standard compliant browsers
- Support multiple identity stores (realms)
- Multiple authentication protocol support
- Client support for common languages

A Grassroots Enterprise Project

I. Gain support from Administration

II. Build consensus from technical staff

III. Receive allocation of resources needed

IV. The Easy Part: Build it

A Grassroots Enterprise Project

I. Gain support from Administration

II. Build consensus from technical staff

III. Receive allocation of resources needed

IV. The Easy Part: Build it

A Grassroots Enterprise Project

I. Gain support from Administration

II. Build consensus from technical staff

III. Receive allocation of resources needed

IV. The Easy Part: Build it

A Grassroots Enterprise Project

I. Gain support from Administration

II. Build consensus from technical staff

III. Receive allocation of resources needed

IV. The Easy Part: Build it

The WebAuth System

WebSSO

- Using CAS3 from JA-SIG
  - Cookie based
- Handles user authentication
  - PKI, Kerberos/SPNEGO, Web Form
  - LDAP, JDPB, DND
- Provides client code
  - Java, C, Perl, PHP, Ruby, Cold Fusion, etc

Shibboleth

Internet2 project to handle federated authentication. Builds on top of the WebSSO.

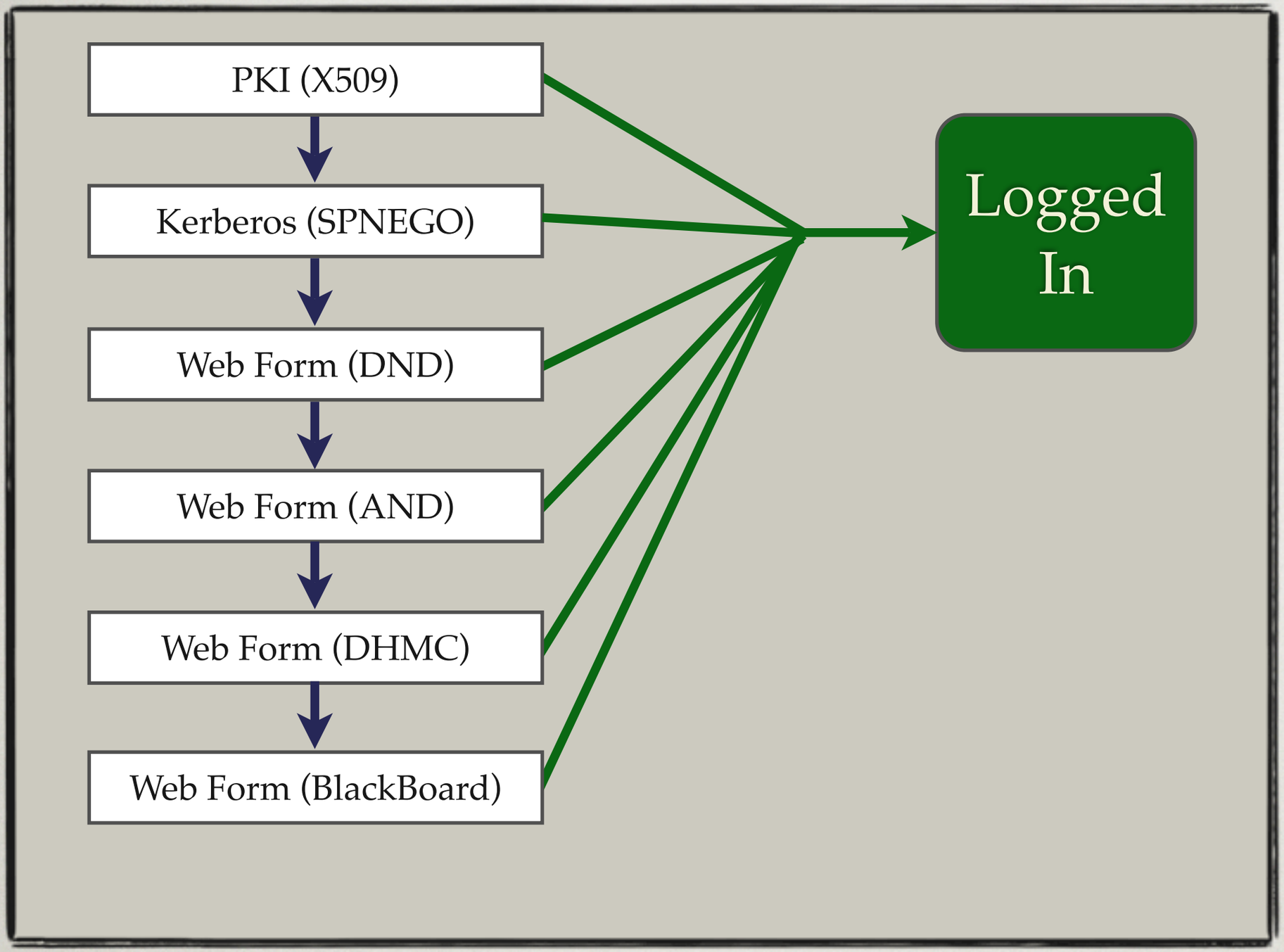
The WebAuth System

- Redundant Servers
  - Dell 1855 Blades, dual 3GHz CPUs, 4GB RAM
- Tomcat 5.5.x fronted by Apache 2.0.x
- Test/Development Server

The WebAuth System

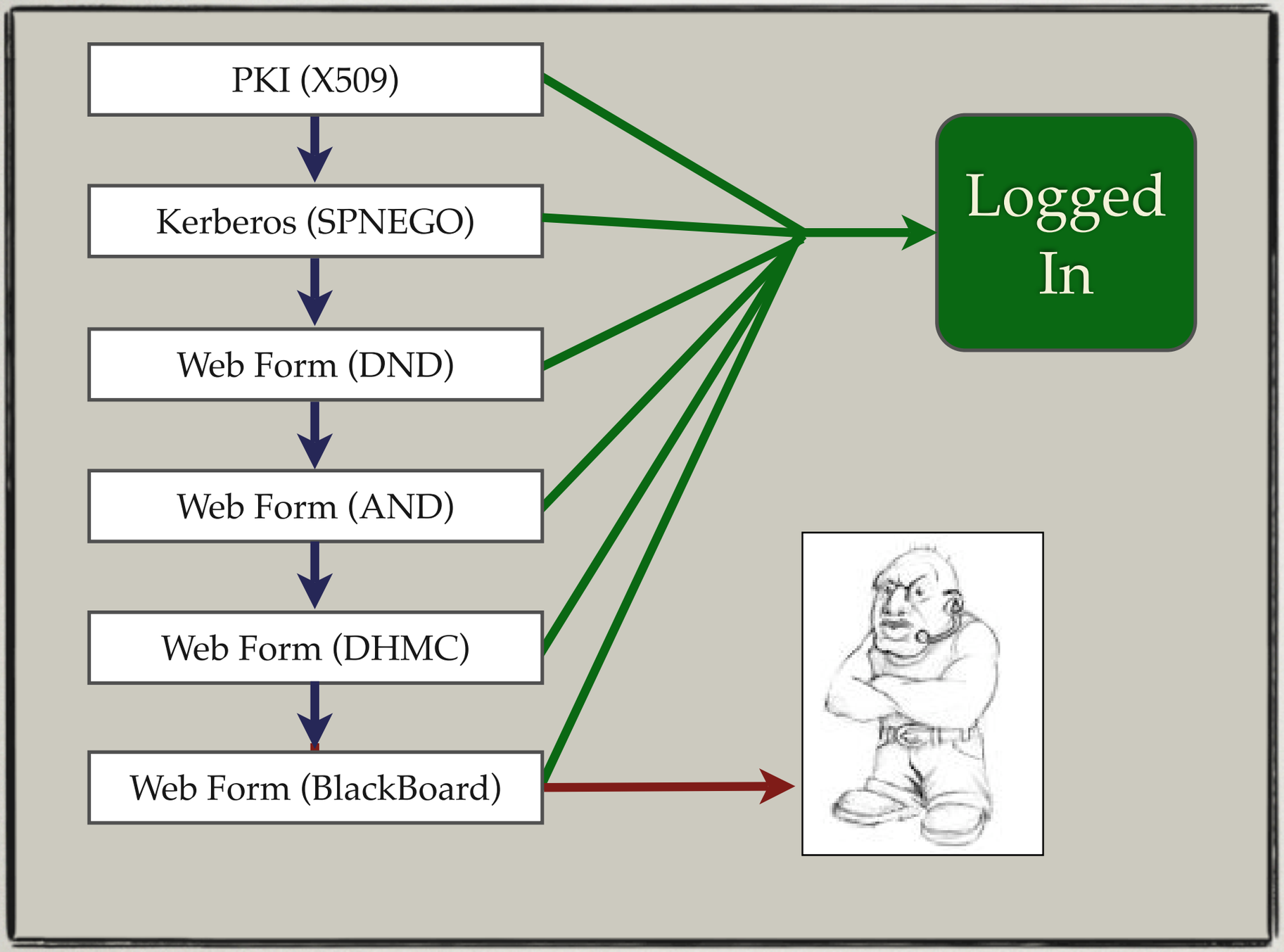
- Redundant Servers
  - Dell 1855 Blades, dual 3GHz CPUs, 4GB RAM
- Tomcat 5.5.x fronted by Apache 2.0.x
- Test/Development Server
- F5 Load Balancer
- Clustered using JBossCache

Dartmouth Enhancements



Authentication Handlers

Authentication handlers perform the actual steps to authenticate a user. The diagram above shows the current order of handlers.



Authentication Handlers

Authentication handlers perform the actual steps to authenticate a user. The diagram above shows the current order of handlers.

Realms

Handler	Realm	authType
Dartmouth PKI	DARTMOUTH.EDU	PKI
Dartmouth SPNEGO	DARTMOUTH.EDU	SPNEGO
Dart Name Directory	DARTMOUTH.EDU	USERPASS
Alumni Name Directory	DARTMOUTH.ORG	USERPASS
DHMC Name Directory	HITCHCOCK.ORG	USERPASS
BlackBoard	BB.DARTMOUTH.EDU	USERPASS
??	??	??

Unique UIDs

Handler	Realm	UID
Dartmouth PKI	DARTMOUTH.EDU	
Dart SPNEGO	DARTMOUTH.EDU	
Dart Directory	DARTMOUTH.EDU	
Alumni Directory	DARTMOUTH.ORG	AL-
DHMC Directory	HITCHCOCK.ORG	DH-
BlackBoard	BB.DARTMOUTH.EDU	BB-
??	??	??

CAS XML Extensions

- user, uid, did, affil, authType

```
<cas:serviceResponse xmlns:cas='http://www.yale.edu/tp/cas'>
    <cas:authenticationSuccess>
        <cas:user>Stephen A. Cochran@DARTMOUTH.EDU</cas:user>
        <cas:uid>66035</cas:uid>
        <cas:did>HD1205K7</cas:did>
        <cas:affil>DART</cas:affil>
        <cas:authType>PKI</cas:authType>
    </cas:authenticationSuccess>
</cas:serviceResponse>
```

CAS XML Extensions

- user, uid, did, affil, authType

```
<cas:serviceResponse xmlns:cas='http://www.yale.edu/tp/cas'>
    <cas:authenticationSuccess>
        <cas:user>Stephen A. Cochran@DARTMOUTH.EDU</cas:user>
        <cas:uid>66035</cas:uid>
        <cas:did>HD1205K7</cas:did>
        <cas:affil>DART</cas:affil>
        <cas:authType>PKI</cas:authType>
    </cas:authenticationSuccess>
</cas:serviceResponse>
```

CAS XML Extensions

- user, uid, did, affil, authType

```
<cas:serviceResponse xmlns:cas='http://www.yale.edu/tp/cas'>
    <cas:authenticationSuccess>
        <cas:user>Stephen A. Cochran 05@DARTMOUTH.ORG</cas:user>
        <cas:uid>AL-1488065548</cas:uid>
        <cas:did>0000234339</cas:did>
        <cas:affil>AL-1488065548</cas:affil>
        <cas:authType>USERPASS</cas:authType>
    </cas:authenticationSuccess>
</cas:serviceResponse>
```

CAS XML Extensions

- user, uid, did, affil, authType

```
<cas:serviceResponse xmlns:cas='http://www.yale.edu/tp/cas'>
    <cas:authenticationSuccess>
        <cas:user>Stephen A. Cochran 05@DARTMOUTH.ORG</cas:user>
        <cas:uid>AL-1488065548</cas:uid>
        <cas:did>0000234339</cas:did>
        <cas:affil>AL-1488065548</cas:affil>
        <cas:authType>USERPASS</cas:authType>
    </cas:authenticationSuccess>
</cas:serviceResponse>
```

CAS XML Extensions

- user, uid, did, affil, authType

```
<cas:serviceResponse xmlns:cas='http://www.yale.edu/tp/cas'>
    <cas:authenticationSuccess>
        <cas:user>Stephen A. Cochran 05@DARTMOUTH.ORG</cas:user>
        <cas:uid>AL-1488065548</cas:uid>
        <cas:did>0000234339</cas:did>
        <cas:affil>AL-1488065548</cas:affil>
        <cas:authType>USERPASS</cas:authType>
    </cas:authenticationSuccess>
</cas:serviceResponse>
```

Tomorrow

Technical Details

- Extension of the CAS v2 XML Response
- Integration in Oracle Applications
- Working with Multiple Identity Stores
- Clustering
- Handling of Public Workstations
- Increased Security Requirements for some Apps
- Dartmouth's Logout Best Practices

Results

Current Environment

- Capacity
  - 1.2 million SSL connections per hour per server
- 35+ Applications Converted
  - Blackboard, NolijWeb, Resource25, Oracle Calendar, Web Servers, Event Calendar, Oracle Apps, Trac
- Currently supporting four user groups
  - Dartmouth, Alumni, Medical Center, Blackboard

Community Development

- Guest System
  - Network Authentication
  - Self Account registration
  - “Sonar” at Medical Center
  - Client Enhancement

Lessons

Keys To Success

- Open Process
- Top Level Support
- Inclusion During Design
- Ease of Integration
- Reliability and User Friendly

More Information

Project Website

http://dev.dartmouth.edu/projects/softdev/webAuth/

CAS v3

http://www.ja-sig.org/products/cas/

Shibboleth

http://shibboleth.internet2.edu/

Questions