Welcome to Spring Forward 2006

www.springforward2006.com
September 26, 2006 Penn State Great Valley

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

Securing Your Applications with CAS and Acegi

Dmitriy Kopylenko
Application Developer
Architecture & Framework
Rutgers University

Scott Battaglia
Application Developer
Enterprise Middleware
Rutgers University

www.springforward2006.com
September 26, 2006 Penn State Great Valley

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

Overall Presentation Goal

Learn How to Use Acegi Security and CAS to secure your Spring-based Applications

Qualifications

- Dmitriy Kopylenko
  - Senior Architect on Architecture & Framework Team
  - Committer to various open source projects including Spring and Acegi
- Scott Battaglia
  - Application Developer for Enterprise Middleware
  - Lead Developer/Architect for JA-SIG CAS
  - Committer for Acegi Security

Presentation Overview

- Why Use Acegi Security?
- Why use JA-SIG CAS?
- Adding Acegi and CAS to YOUR Application
- How Acegi Works
- How CAS Works
- Rutgers Experience with Acegi/CAS
- Conclusion

Why Use Acegi Security?

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

Acegi Overview

- Official Spring Project
- Used in projects for over 2 ½ years now
- Over 70,000 downloads before 1.0 release
- High test coverage
- 14 active committers
- Apache 2.0 licensed

Authentication Features

- LDAP
- BASIC
- Digest
- JAAS
- CAS
- X.509 Certificates
- DAO
- Run-as Replacement
- Form-based login
- Anonymous

- Remember-Me
- SiteMinder
- HTTP Switch User
- Concurrent User Limiting
- Container Adapters
  - JBoss
  - Jetty
  - Tomcat
  - Resin
- Write your own
- Decide at deployment

Authorization Features

- Web requests
  - Http://my.server.com/some/secure/path
- Java methods
  - AspectJ compile-time weaving
  - Spring AOP runtime weaving
- Domain object instance security
- Write your own
- All with authentication independence!

Other Features

- Localization
- Channel security (HTTPS)
- Human user detection (JCAPTCHA)
- Filter to bean proxy capabilities
- Tag libraries
  - JSP and Velocity
- Two sample applications
- Quality documentation

Technical Design

- Uses Spring IoC container
  - DI, events, localization and JdbcTemplate
- Completely interface-driven
- High cohesion, loosely coupled
- Encourage customization and extension
- Java 1.3+ compatible
  - Java 5 code packaged in “Tiger” JAR

Why Use JA-SIG CAS?

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

CAS Overview

- Official JA-SIG Project
- Used in production for over a year
- High test coverage
- 8 active committers
- JA-SIG License

Authentication Features

- LDAP
- DAO
- NTLM (3.1)
- SPNEGO (3.1)
- RADIUS (3.1)
- File System
- X.509
- “Trusted”
- JAAS
- Acegi
- Create your own…
- Chain them together

Other Features

- Localization
- Clustering (3.1)
- Client Libraries (PHP, Java, etc.)
- Demo-able/Quickstart WAR file
- Quality Documentation
- Active community mailing lists

Technical Design

- Use Spring IoC Container
  - DI, Localization, events, JdbcTemplate, LdapTemplate, etc.
- Completely interface driven
- Encourage customization and extension
- Java 1.4+/Servlet 2.4 compatible

Adding Acegi and CAS to YOUR Application

www.springforward2006.com
September 26, 2006 Penn State Great Valley

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

Steps

Download

- Spring 2.0 RC4
- Acegi Security 1.0.1
- CAS Server 3.0.5
- Java 1.5
- Apache Tomcat 5.5.17

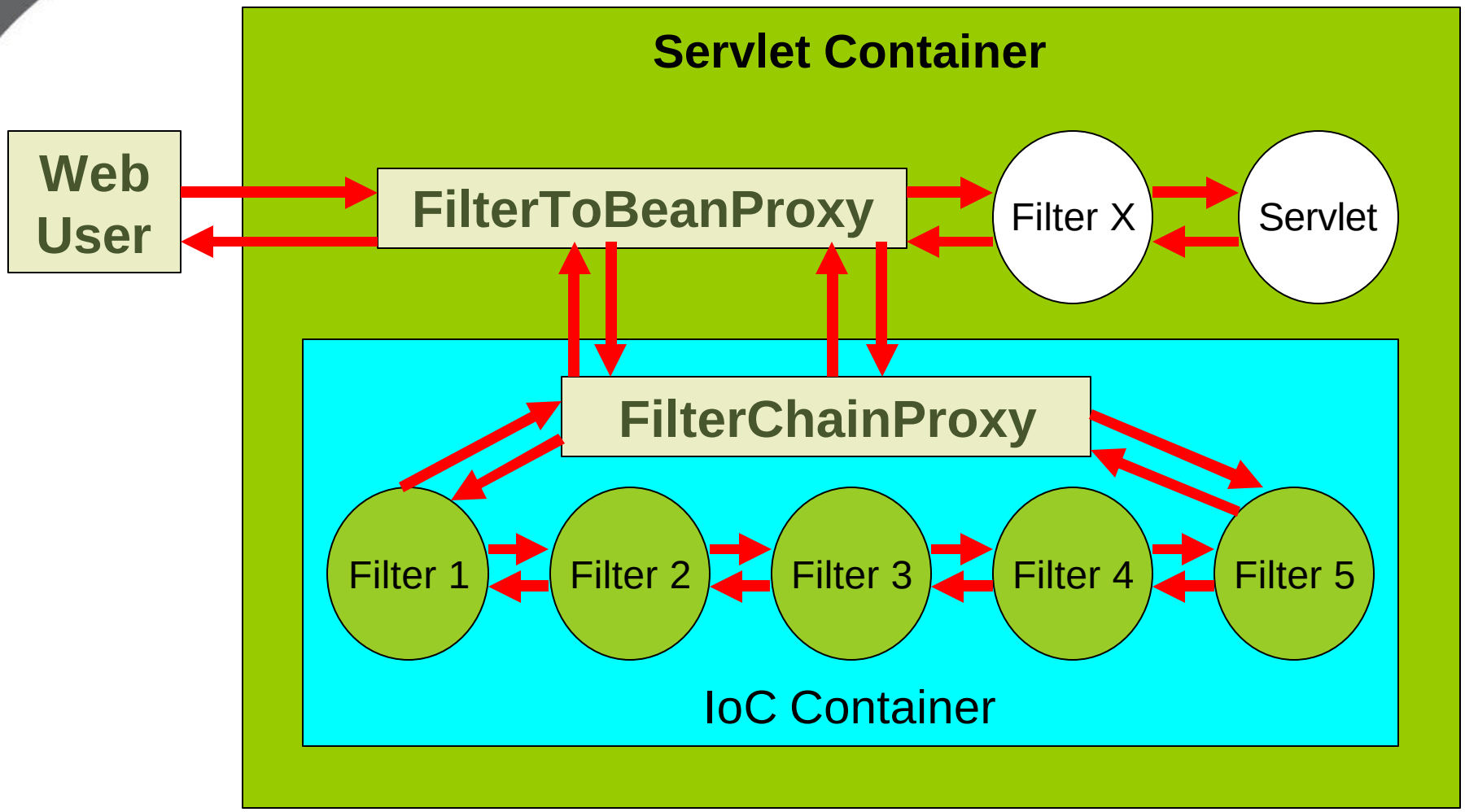
- Add files from Acegi's "tutorial" sample
- Edit Spring Petclinic XML and JSP files

DEMO

How Acegi Works

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

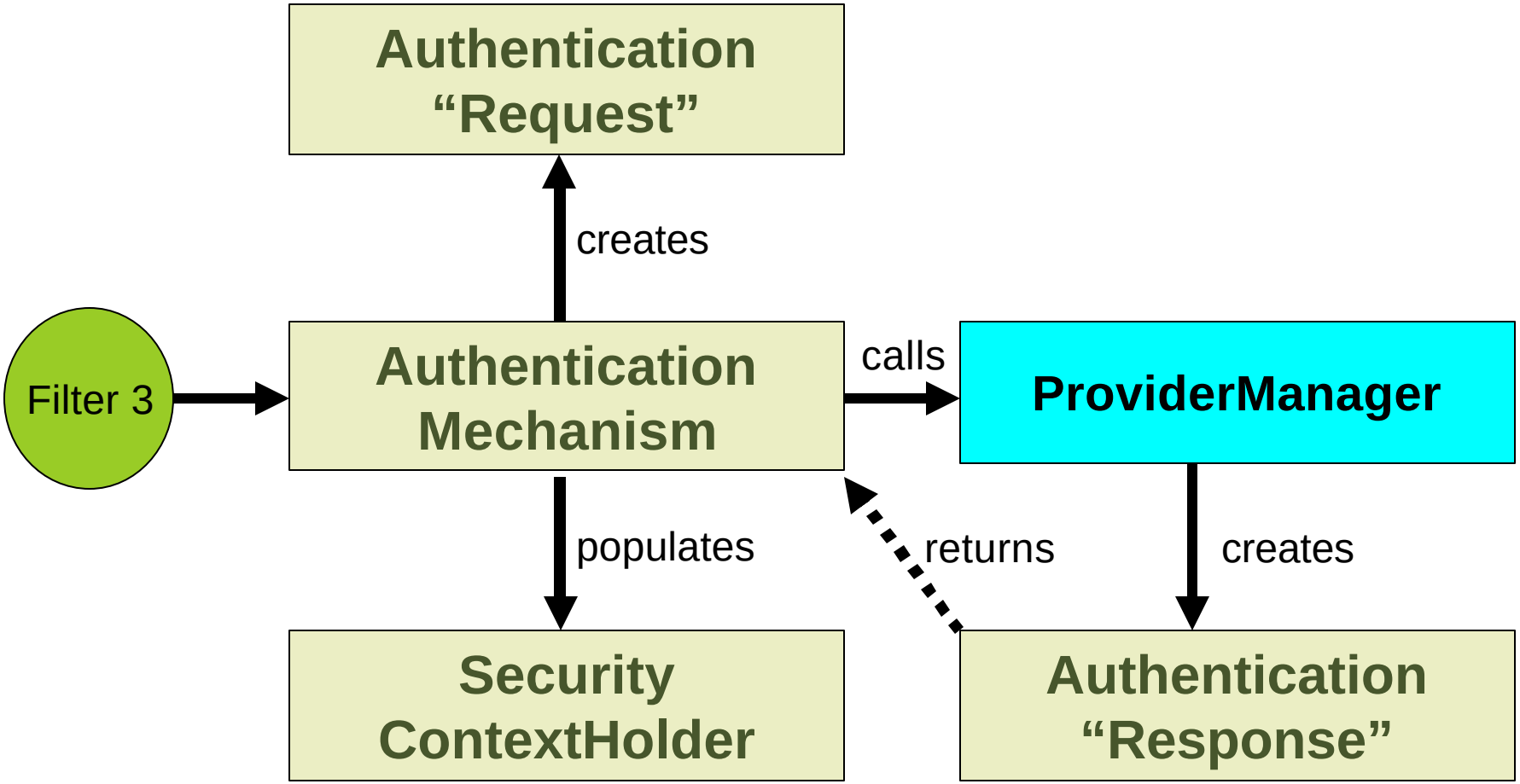
Filters Are Central



Main Filters

#	Filter Name	Main Purpose
1	HttpSessionContext IntegrationFilter	Stores SecurityContextHolder between HTTP requests
2	LogoutFilter	Clears SecurityContextHolder when logout requested
3	Authentication Mechanism Filters	Puts Authentication into SecurityContextHolder
4	Exception TranslationFilter	Converts Acegi Security exceptions into HTTP
5	FilterSecurity Interceptor	Authorizes web filter requests based on URL patterns

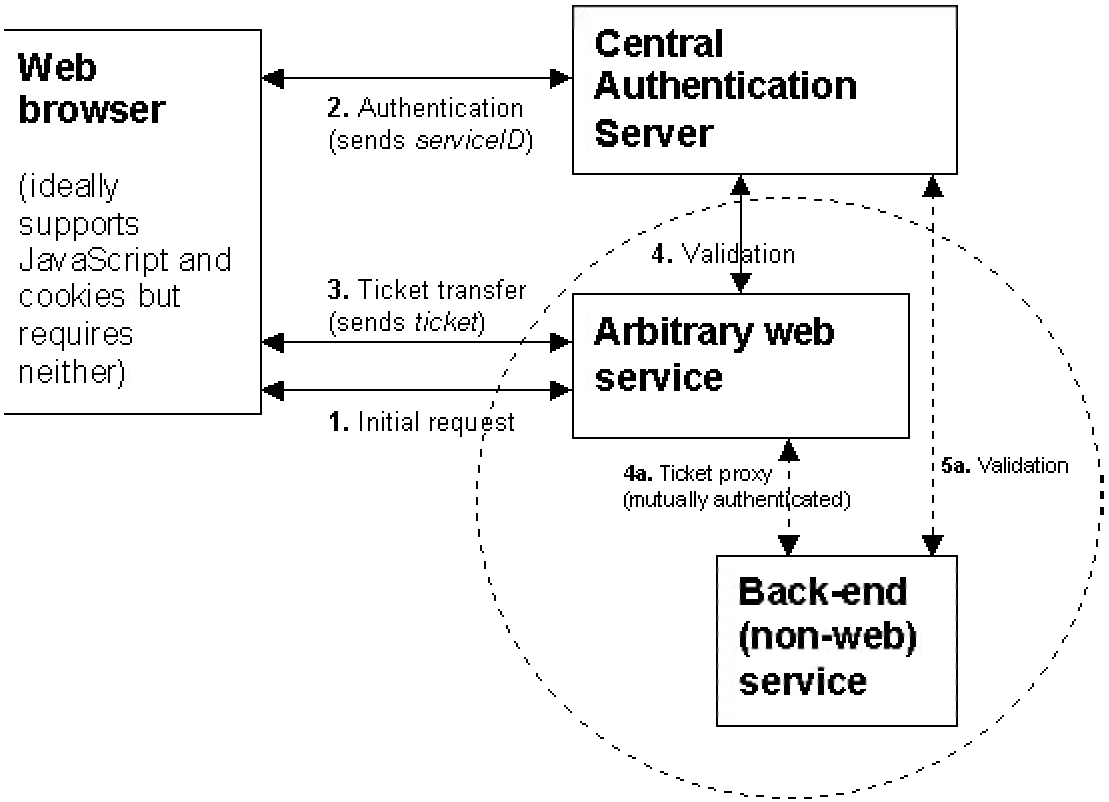
Security Context Population



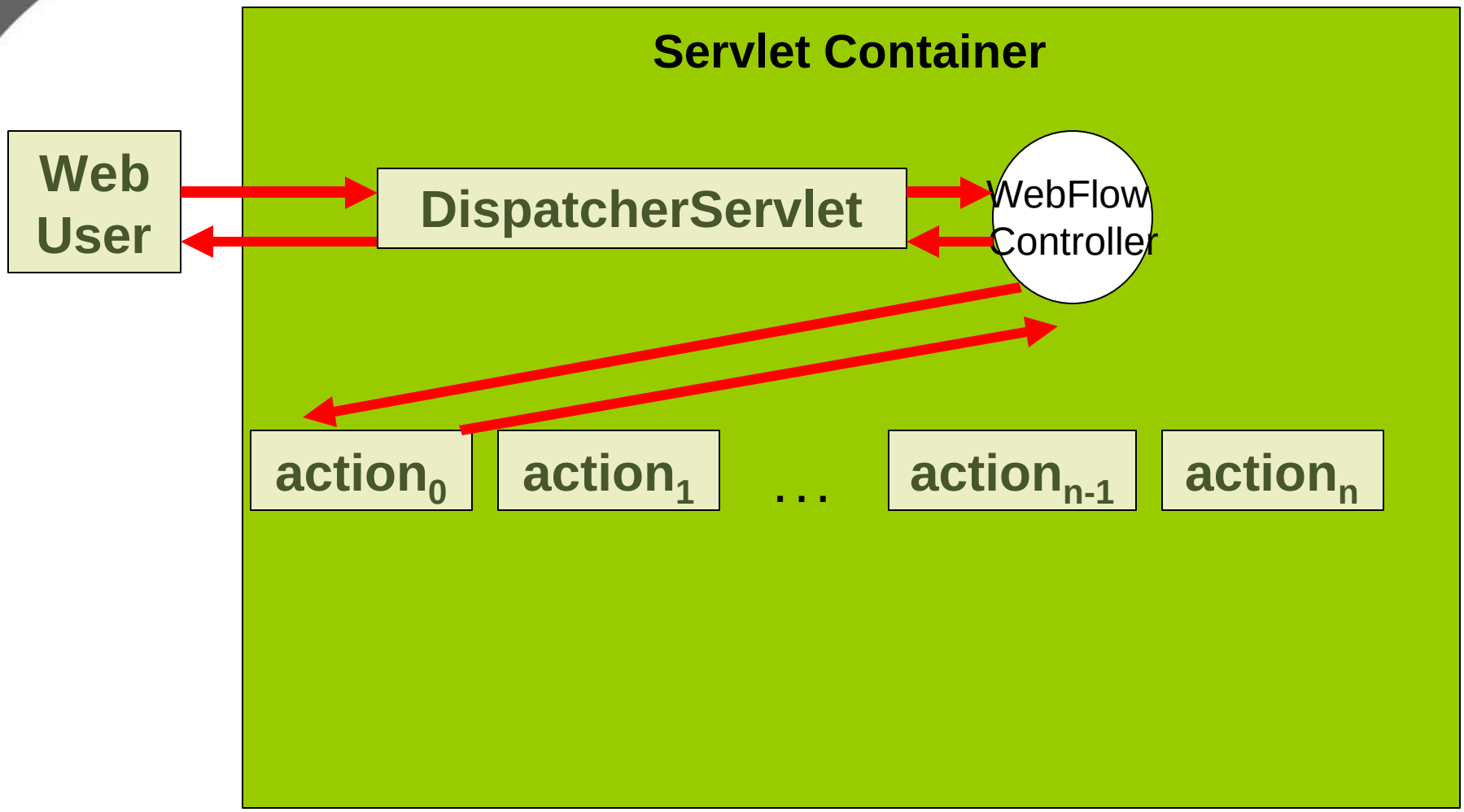
How CAS Works

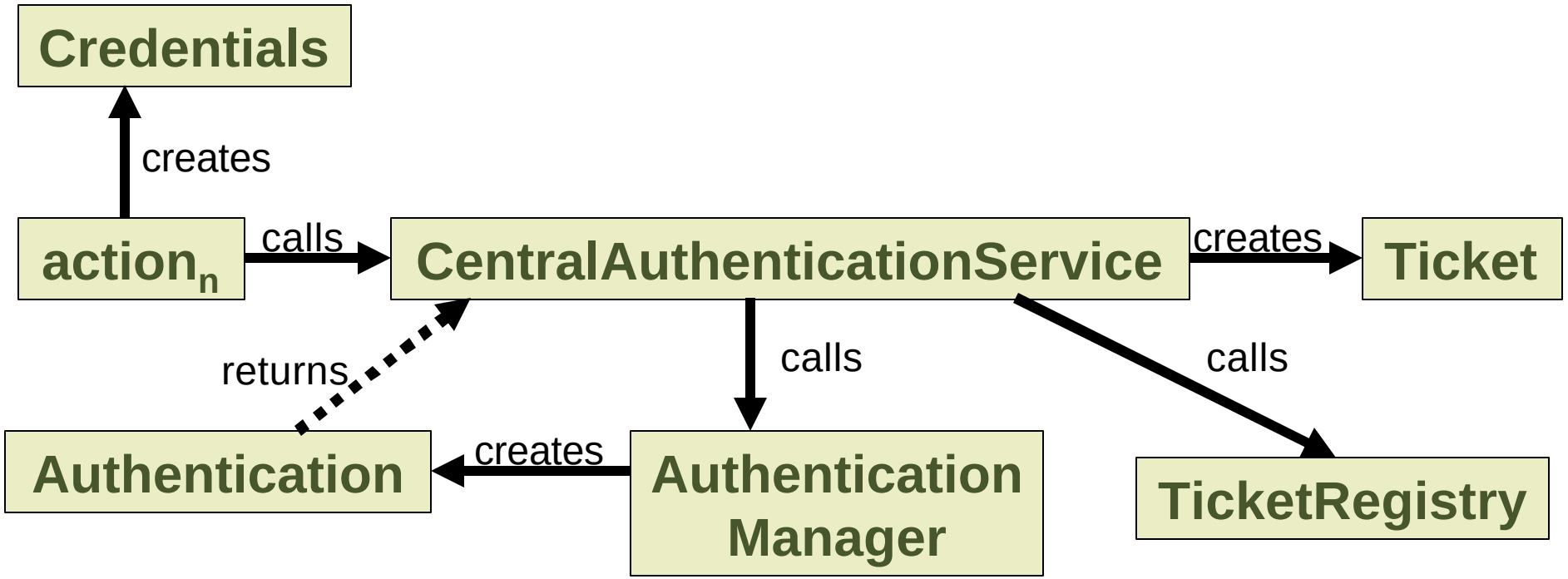
THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

CAS Protocol



Spring Web Flow




Credentials
creates
action$_n$
calls
CentralAuthenticationService
creates
Ticket
returns
calls
calls
Authentication
creates
Authentication Manager
TicketRegistry

Rutgers Experiences using Acegi/CAS

www.springforward2006.com
September 26, 2006 Penn State Great Valley

THE STATE UNIVERSITY OF NEW JERSEY
RUTGERS

What We Were Doing

- Duplicating authentication code on each application
- Multiple authentication methods
- Sign in to each application
- De-centralized authentication

What Did We Do

- Introduced a portal
- Centralized authentication
- Single Sign On
- Proxy Authentication
- Introduced Acegi into Java applications

Benefits

- Better user experience
- Minimized access to passwords
- Created “horizontal” authentication component

Conclusion

Conclusion

- Acegi Security is fully-featured solution
  - Many authentication strategies
  - Decoupled web and method authorization
  - Completely customizable by end users
  - Active community, quality documentation, etc.
- CAS is a fully-featured solution
  - Many authentication strategies
  - Easily pluggable and extensible
  - Active community, quality documentation, etc.
  - Support for multiple platforms

Conclusion

- Acegi and CAS “just work”. Go ahead and try it.

Resources

- http://www.acegisecurity.org
- http://www.ja-sig.org/products/cas/
- http://www.springframework.org
- http://www.ja-sig.org/wiki

Q&A