

*Reverse proxy &
Identity services*

(St. Patrick's Day edition)

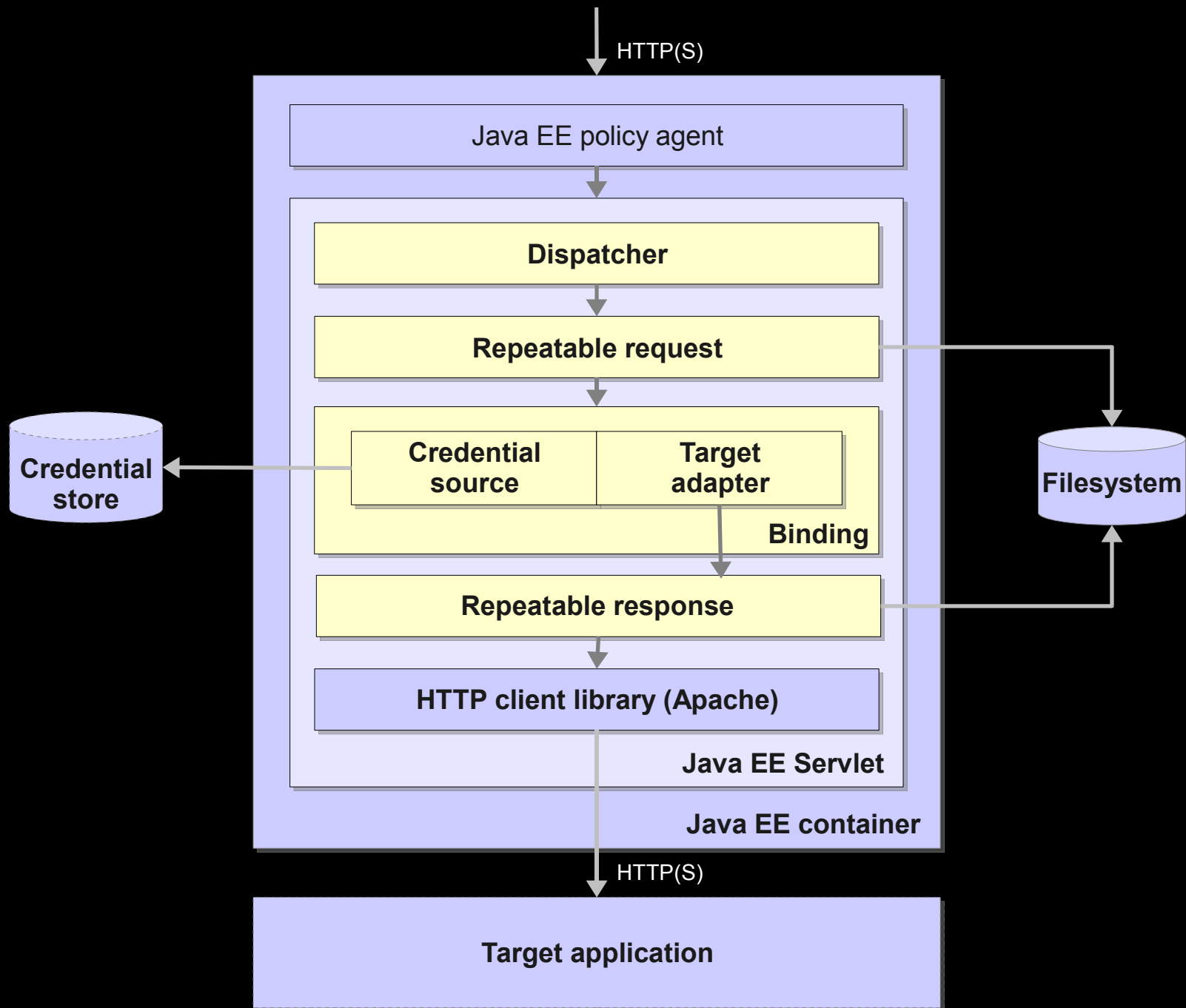
Paul C. Bryan
Sun Microsystems

1. Reverse proxy

Reverse proxy

- Stands in front of target application
- Authenticates using application user credentials
- Detects session state in target application
- Flexible credential source implementation
- Transparent session management
- Standard Java EE Servlet implementation

Architectural overview



When not to use the reverse proxy

- Policy agent integration is a valid option
- Integration through federation is an option
- Application maintained by another organization
- You don't control DNS resolution to application
- Unreasonably large content to cache

Issues w. external applications

- SSL/TLS and issues w. certificates
- Impact of modifications to target application

Target adapter

- Detect absence or loss of session
- Knows how to authenticate on behalf of user
- Detects authentication failures
- Determines what cookies need to propagate

Credential source

- Fetches credentials from data store (e.g. vault)
- Handles authentication failures

Types of credentials supported

- So far: username & password
- Expandable for future credential types

Steps to deploy reverse proxy

- Bind a target adapter with a credential source
- Configure target explicitly in reverse proxy
- Point DNS for application to the reverse proxy
- Profit!

Further considerations

- What credentials to use
- Secure storage of user credentials
- Identity Manager for managing credentials
- Programmatic credentials
- Null credentials

Uncertain, possible future directions

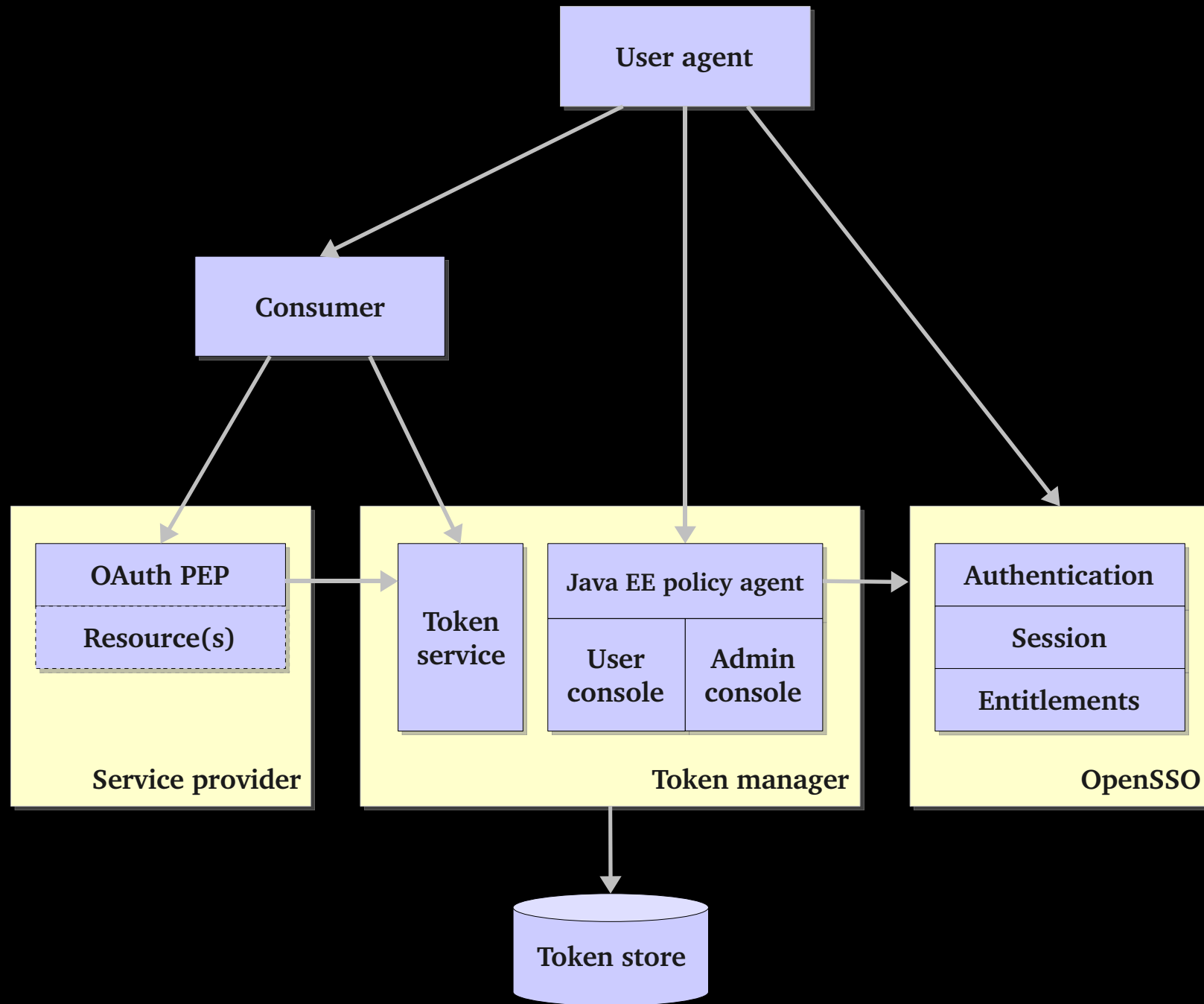
- Generic, configurable target adapters
- Secure storage of credentials in a vault
- In-flight detection of credential changes

2. Identity services

Identity services

- Full compliance with any adopted standards
- Full API access through RESTful web services
- Policies can enforce identity service access
- WADL for generation of access API
- Full Java client API shipping with product
- Secured through the OAuth core protocol
- Includes OAuth policy enforcement point

OAuth policy enforcement point



OAuth policy enforcement point

- Designed to Protect RESTful web services
- Supplies subject, token, attributes to service
- Supports 2 and 3-legged OAuth profiles
- Users can manage issued tokens
- Administrators can manage consumer keys, token issuance policies, etc.
- Even better than the ShamWow®

Potential OAuth PEP future

- User-defined access control policies
- Vendor relationship management (VRM)

Fin