User Authentication using the Client Principle Object

PUG Challenge America

Presented By:
Chris Longo
Senior Consultant
clongo@bravepoint.com

Agenda

- Define Authentication Authorization and the role of the CP Object
- Security Domains and how they effect Authentication Strategies
- Creating CP Object
- Best practice for integration into application context
- Using Authentication Callback Procedures

Authentication

- A process that establishes a valid identity.
- Validation of a UserID and Password combination.
- Security Token provides a durable persistent means of establishing an identity for a period of time.

Authorization

- Process that grants or revokes access to application data, functionality or workflow.
- Based upon an established Identity.

Client Principal Object

- Provides a means of establishing an authenticated identity.
  - Durable
  - Repeatable
- Validate UserID / Password
  - Depends on the domain type associated with a user.

Importance of a CP Object

- Establish identity on and AppServer (WebSpeed or Open AppServer).
- Establish Tenancy.
- Establish and identity for auditing.
- Establishing single sign-on

What is a Client Principal Object?

- Dynamic ABL Object
  - Created and maintained using ABL code.
  - Methods
  - Attributes

What is a Security Token?

- Unique value that represent an identity.
- Generated once and identity is established and used to re-establish and identity.
- Encrypted String
- Not the CP Object itself, but used to re-constitute a CP Object.

Security Domains

- Effect the way in which Users Authenticate.
- Required for creating a Client Principal Object.
- Domains Establish Tenancy.

Domain Types

- _oeusertable: User profiles maintained via the _User table in an OpenEdge Database.
  - Web, AppServer, GUI, TTY

Domain Types

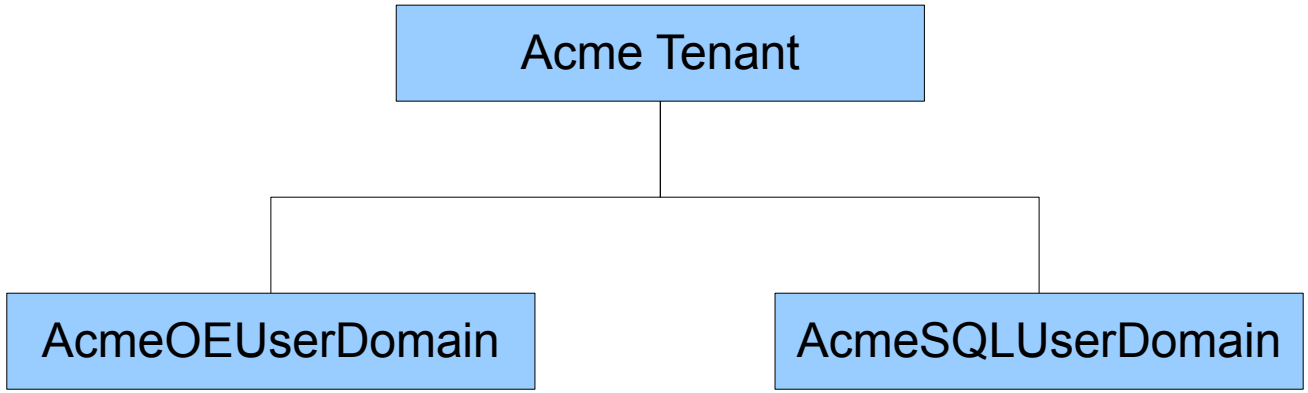
- _oslocal: User profiles maintained via the host operating system.
  - GUI, TTY

Domain Types

- _extsso: User Profiles maintained via and application table or external source (Possibly LDAP).
  - Web, AppServer, GUI, TTY

Domain Tenant Relationship

- A Tenant is associated with one or more Domains.
- A Domain is associated with a single Tenant.



Pre-configured Domains

- Default (blank) Domain
  - For backward compatibility.
  - Associated with the Default Tenant.
  - Uses the _oeusertable Domain Type.
  - Can't be deleted.

Pre-configured Domains

- Reserved for command line utilities
  - WINDOWS
  - WINDOWSID
  - UNIX
  - UNIXID

3 Ways to Load Domain for a Session

- Domains defined within a database are loaded as DB Connections are made.

3 Ways to Load Domain for a Session

- Domains can be defined in a single database and manually loaded and applied across multiple DB Connections
  - For those databases relying on the domains defined in another database, turn on “Use Application Domain Registry” setting.
  - Then, use SECURITY-POLICY:LOAD-DOMAINS(dbname) to load the domains defined in the <dbname> database.

3 Ways to Load Domain for a Session

- Register a Domain defined outside a OE Database.
  - Use SECURITY-POLICY:REGISTER-DOMAINS(*domain-name, access-code*) method.

CP Object

- The CP Object becomes part of a user's session context.

- It can be used to set the UserIDs of all connected databases at run-time

Steps to Using CP Object

- Define Security Domains
- Load Security Domain (Session)
- Create CP Object
- Assign three key attribute
  - UserID
  - Domain Name
  - SessionID
- Seal CP Object
  - Domain AccessKey
- Establish Identity

Sample Create CP (_extsso)

```
CREATE CLIENT-PRINCIPAL hClientPrincipal.
/* Set CP Object Values */
hClientPrincipal:SESSION-ID = BASE64-ENCODE(GENERATE-UUID).
hClientPrincipal:USER-ID = pcUserID.
hClientPrincipal:DOMAIN-NAME = 'bravepoint.com'.
hClientPrincipal:DOMAIN-TYPE = 'Internal'.
hClientPrincipal:LOGIN-EXPIRATION-TIMESTAMP =
                                ADD-INTERVAL(NOW, 60, 'seconds').
```

Sample Create CP

- Initialize Method
  - –

```
CREATE CLIENT-PRINCIPAL hClientPrincipal.


IF NOT hClientPrincipal:INITIALIZE (pcUserID,                              /* UserID     */
                                    ?,                                     /* SessionID  */
                                    ADD-INTERVAL(NOW, 60, 'seconds'),      /* Expiration */
                                    pcPasswd)                              /* Password   */
```

Sample Create CP

- The Domain Access Key was previously defined using the Data Admin tool or setup manually using register-domain().

```
hClientPrincipal:SEAL(cDomainAccessKey)
```

Sample Create CP (_extsso)

- SET-DB-CLIENT will set the effective UserID for all connected databases or those explicitly specified.

```
SET-DB-CLIENT(hClientPrincipal)
```

CP Object Portability

- CP Object provides methods to import and export it's values.
  - CP Object exports and imports from a raw data type.

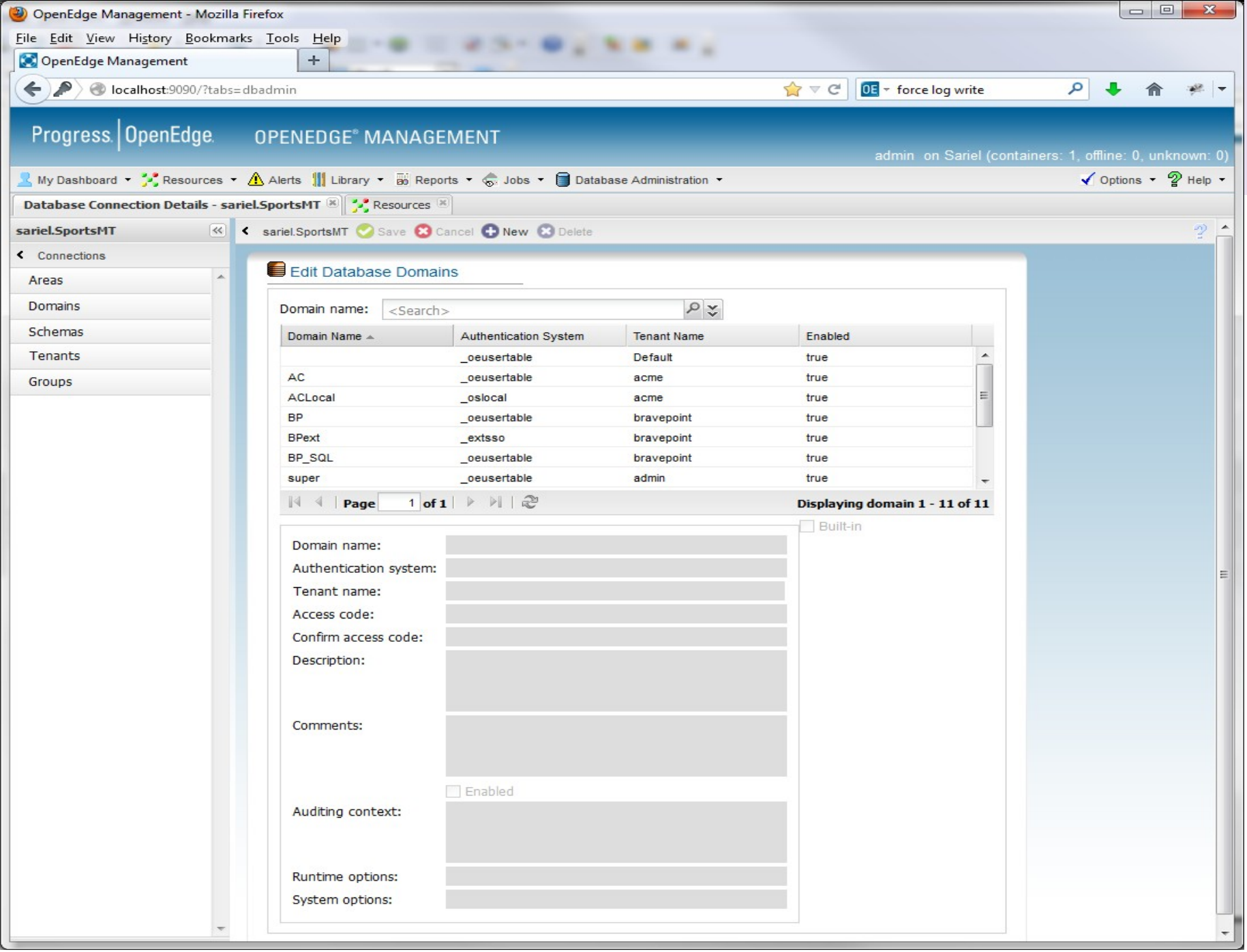
```
DEFINE VAR rCP AS RAW NO-UNDO.

rCP = hClientPrincipal:EXPORT-PRINCIPAL().
```

CP Object and Session Context

- Best Practice
  - Store the CP Object in a session context DB Table.
    - SessionContext.SessionID AS CHARACTER
    - SessionContext.ContextObject AS RAW
  - Pass an encrypted token containing the associated sessionID back to the client.
    - SecureToken is used to reconstitute the CP Object each time a user interacts with an agent.
    - SecureToken is a character string.

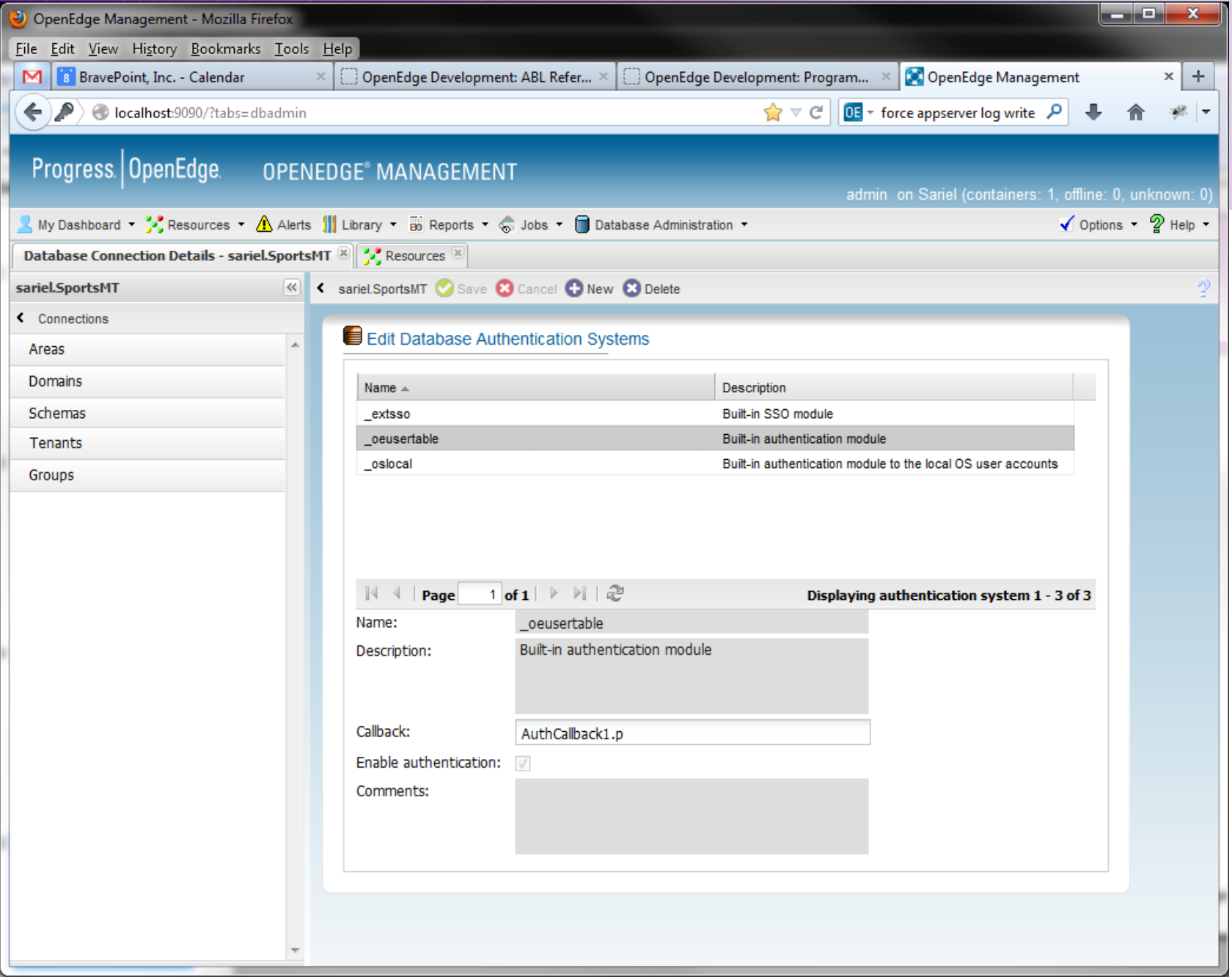
Demo App Domains

Tenant	Domain	Type
Bravepoint	BP	_oeusertable
Bravepoint	BPext	_extsso
Acme	AC	_oeusertable
Acme	ACLocal	_oslocal
Admin	Super	_oeusertable


OpenEdge Management - Mozilla Firefox
File Edit View History Bookmarks Tools Help
OpenEdge Management
localhost:9090/?tabs=dbadmin
force log write
Progress OpenEdge
OPENEDGE® MANAGEMENT
admin on Sariel (containers: 1, offline: 0, unknown: 0)
My Dashboard
Resources
Alerts
Library
Reports
Jobs
Database Administration
Options
Help
Database Connection Details - sariel.SportsMT
Resources
sariel.SportsMT
Connections
Areas
Domains
Schemas
Tenants
Groups
sariel.SportsMT
Save
Cancel
New
Delete
Edit Database Domains
Domain name:
<Search>
Domain Name
Authentication System
Tenant Name
Enabled
_oeusertable Default true
AC _oeusertable acme true
ACLocal _oslocal acme true
BP _oeusertable bravepoint true
BPext _extsso bravepoint true
BP_SQL _oeusertable bravepoint true
super _oeusertable admin true
Page 1 of 1
Displaying domain 1 - 11 of 11
Built-in
Domain name:
Authentication system:
Tenant name:
Access code:
Confirm access code:
Description:
Comments:
Enabled
Auditing context:
Runtime options:
System options:

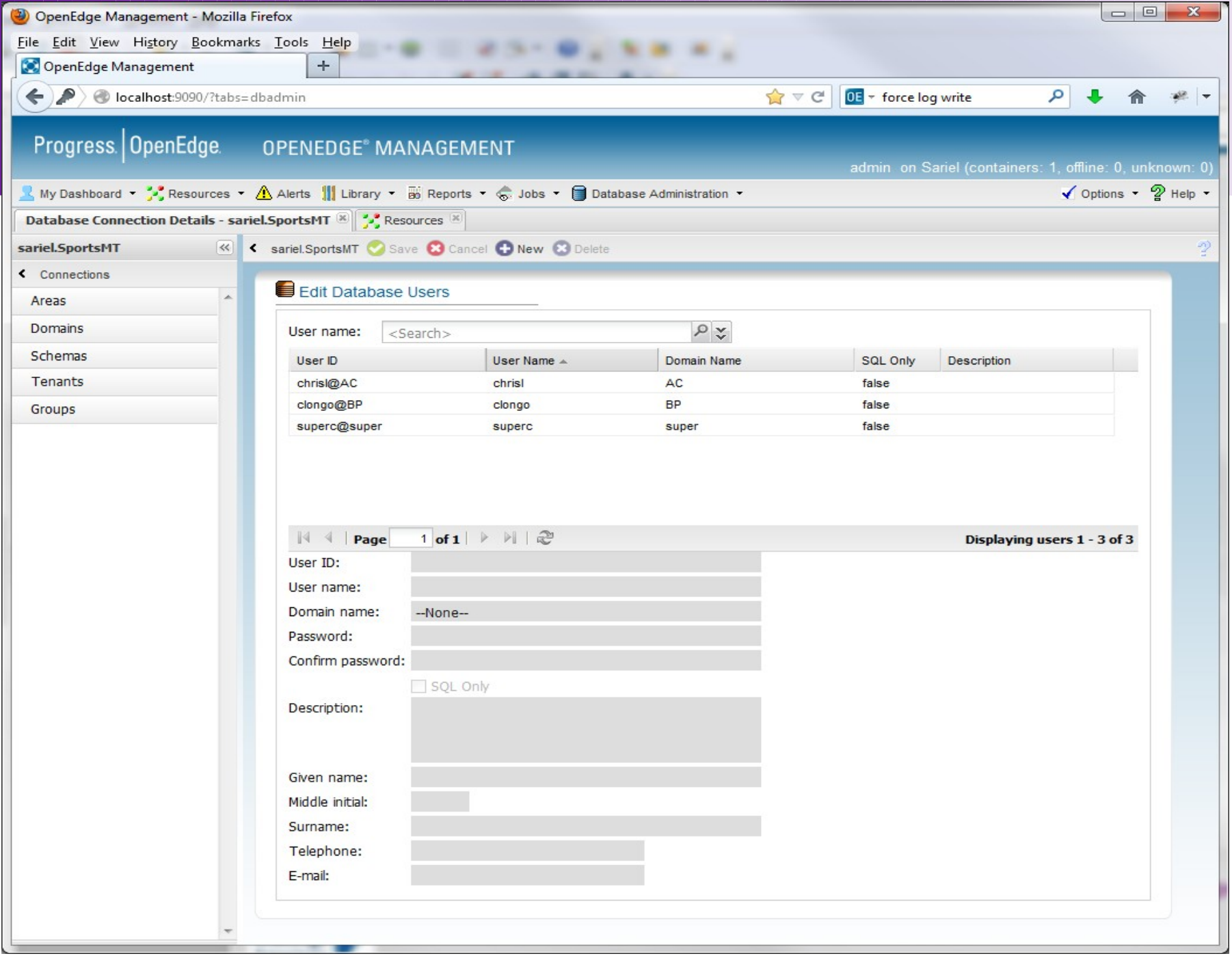
Authentication CallBack Procedure

- Associated with a Domain Type
- AuthenticateUser
  - Executes prior to sealing the CP Object
  - Provide custom user validations
- AfterSetIdentity
  - Create or Set additional Application Context

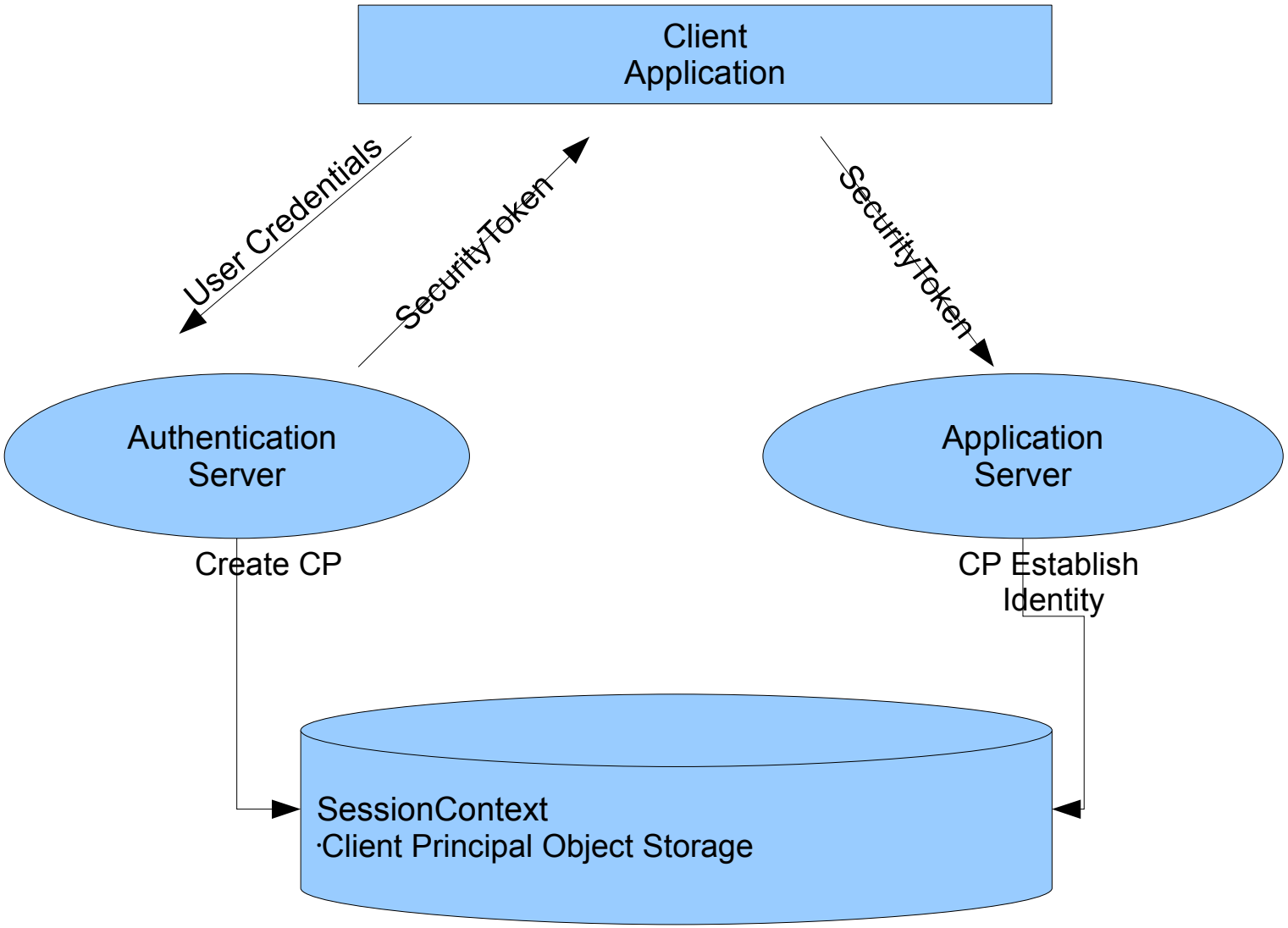

OpenEdge Management - Mozilla Firefox
File Edit View History Bookmarks Tools Help
BravePoint, Inc. - Calendar
OpenEdge Development: ABL Refer...
OpenEdge Development: Program...
OpenEdge Management
localhost:9090/?tabs=dbadmin
force appserver log write
Progress OpenEdge
OPENEDGE® MANAGEMENT
admin on Sariel (containers: 1, offline: 0, unknown: 0)
My Dashboard
Resources
Alerts
Library
Reports
Jobs
Database Administration
Options
Help
Database Connection Details - sariel.SportsMT
Resources
sariel.SportsMT
Connections
Areas
Domains
Schemas
Tenants
Groups
sariel.SportsMT
Save
Cancel
New
Delete
Edit Database Authentication Systems
Name
Description
_extsso
Built-in SSO module
_oeusertable
Built-in authentication module
_oslocal
Built-in authentication module to the local OS user accounts
Page 1 of 1
Displaying authentication system 1 - 3 of 3
Name:
_oeusertable
Description:
Built-in authentication module
Callback:
AuthCallback1.p
Enable authentication:
Comments:

Demo App Users

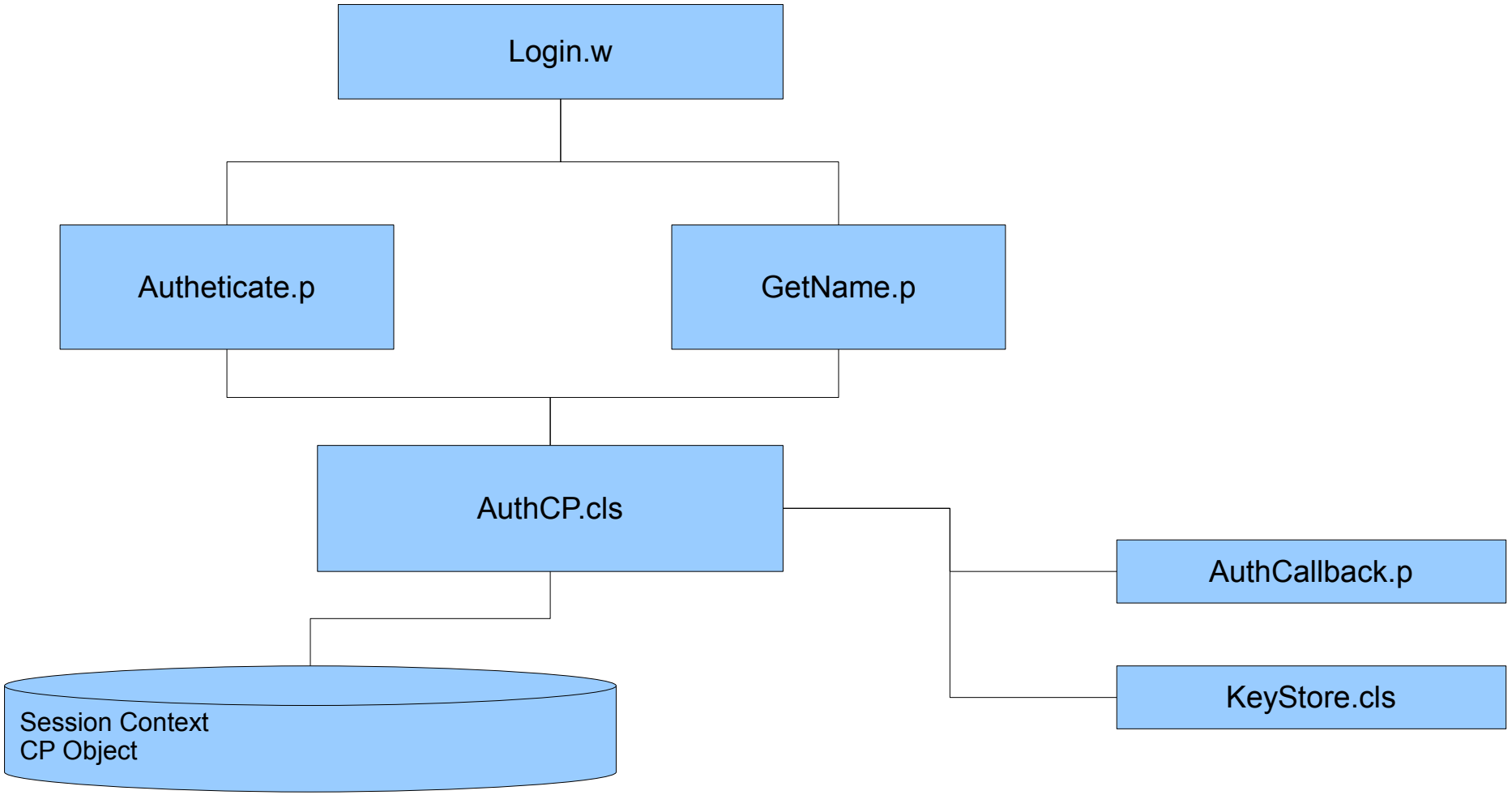
UserID	Domain
chrisl@AC	AC
clongo@ACLocal	ACLocal
clongo@BP	BP
bsmith@BPext	BPext
superc@super	super


OpenEdge Management - Mozilla Firefox
File Edit View History Bookmarks Tools Help
OpenEdge Management
localhost:9090/?tabs=dbadmin
force log write
Progress OpenEdge
OPENEDGE® MANAGEMENT
admin on Sariel (containers: 1, offline: 0, unknown: 0)
My Dashboard
Resources
Alerts
Library
Reports
Jobs
Database Administration
Options
Help
Database Connection Details - sariel.SportsMT
Resources
sariel.SportsMT
Connections
Areas
Domains
Schemas
Tenants
Groups
sariel.SportsMT
Save
Cancel
New
Delete
Edit Database Users
User name:
<Search>
User ID
User Name
Domain Name
SQL Only
Description
chrisl@AC
chrisl
AC
false
clongo@BP
clongo
BP
false
superc@super
superc
super
false
Page 1 of 1
Displaying users 1 - 3 of 3
User ID:
User name:
Domain name:
--None--
Password:
Confirm password:
SQL Only
Description:
Given name:
Middle initial:
Surname:
Telephone:
E-mail:

Authentication Flow



Demo Procedures



Questions?