

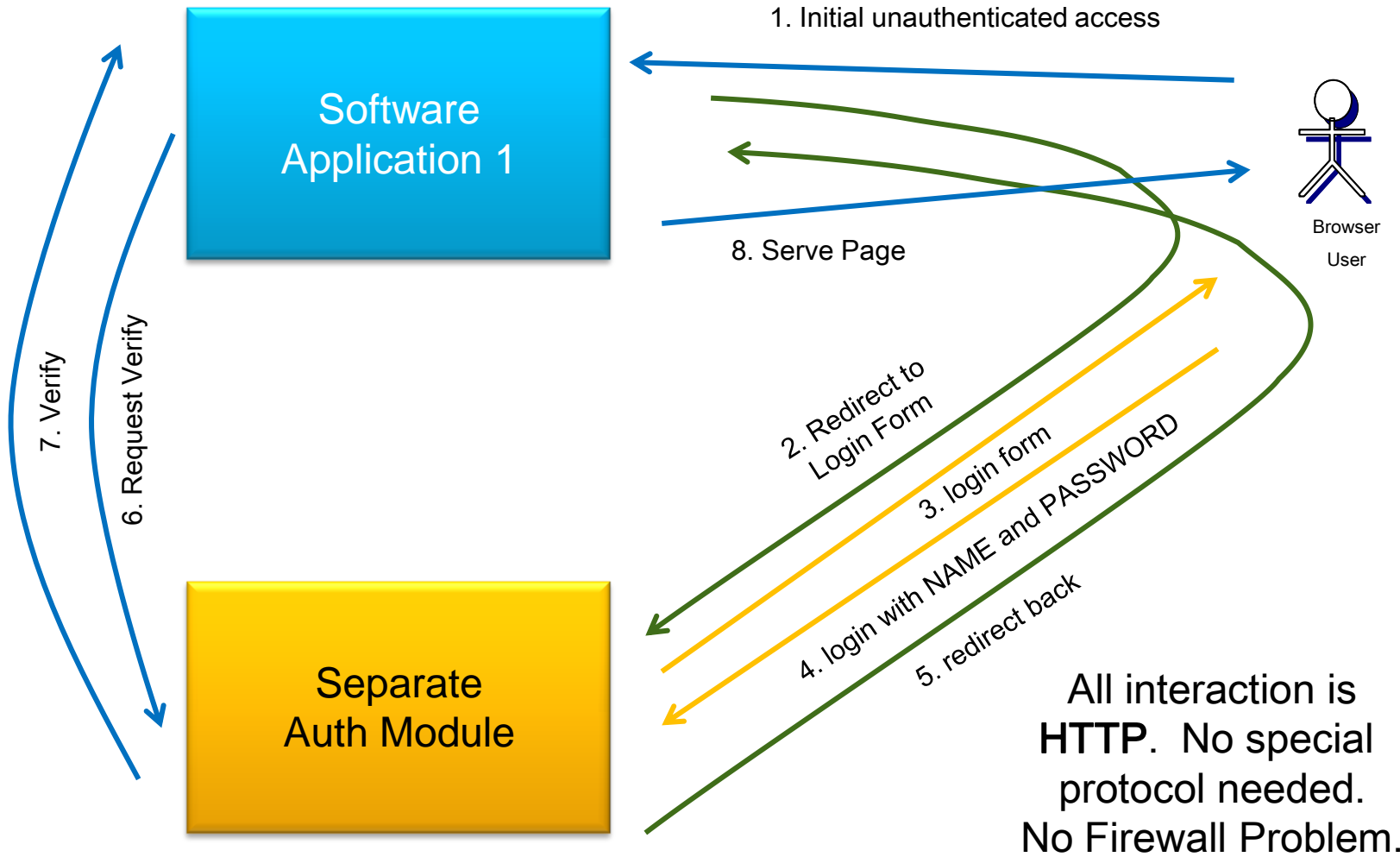
Advanced Software Design Team

Fujitsu Middleware SSO Support

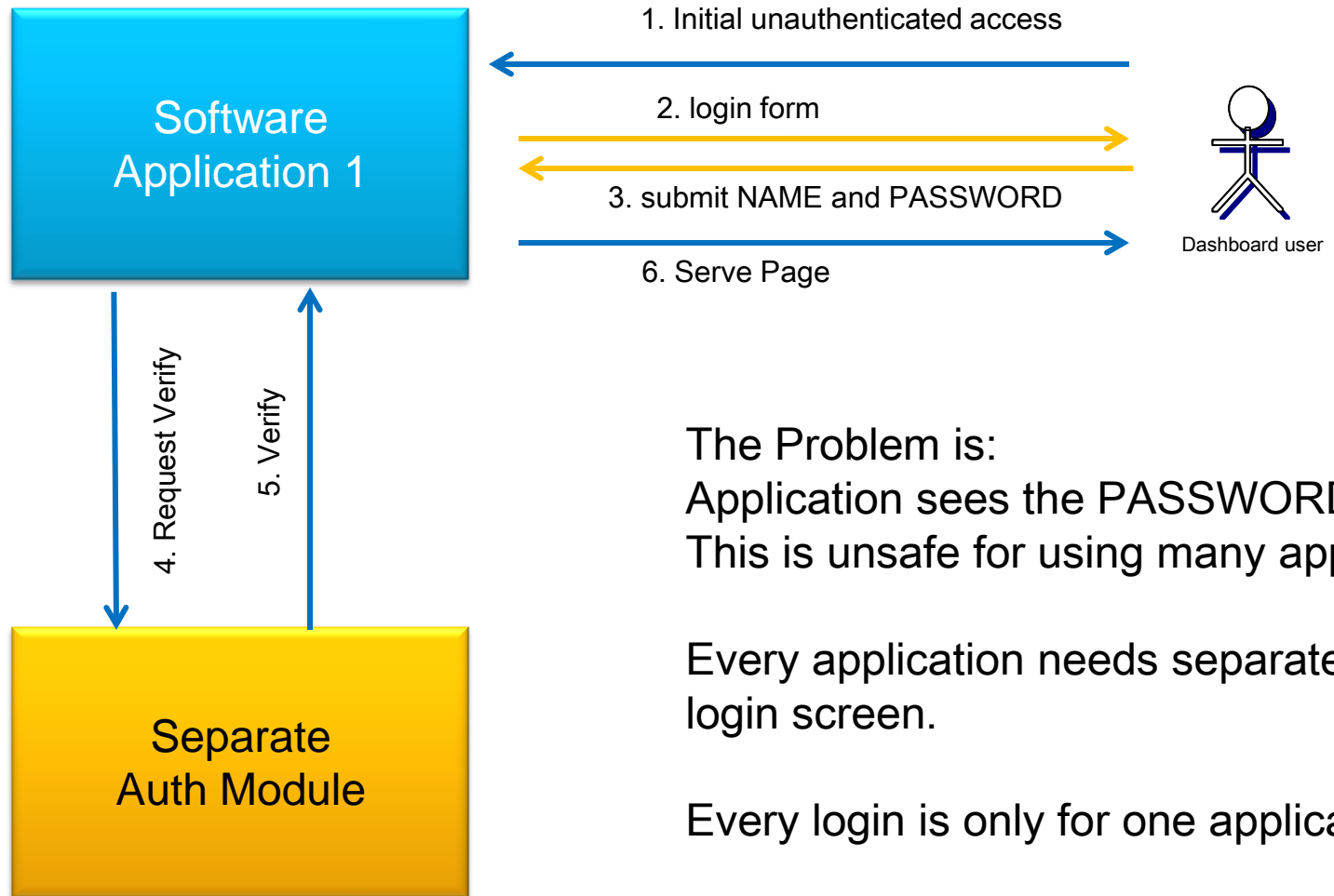
Keith Swenson
April 2012

- Fujitsu sells multiple middleware product developed separately
- Cloud deployments as well
- Users was to log in once
- There is an opportunity for Fujitsu to show leadership in allowing users to log in once, and access multiple cloud or non-cloud applications, without having to re-log in.
- Fujitsu should leverage standards in this area

General Scheme Architecture



OLD – Unsafe – Way



No Restriction on Physical Host



Many applications can share one authentication module.

Authentication module can be on any server, any address.

Authentication does not depend on the physical host that the application is run on.



Cloud based applications as well



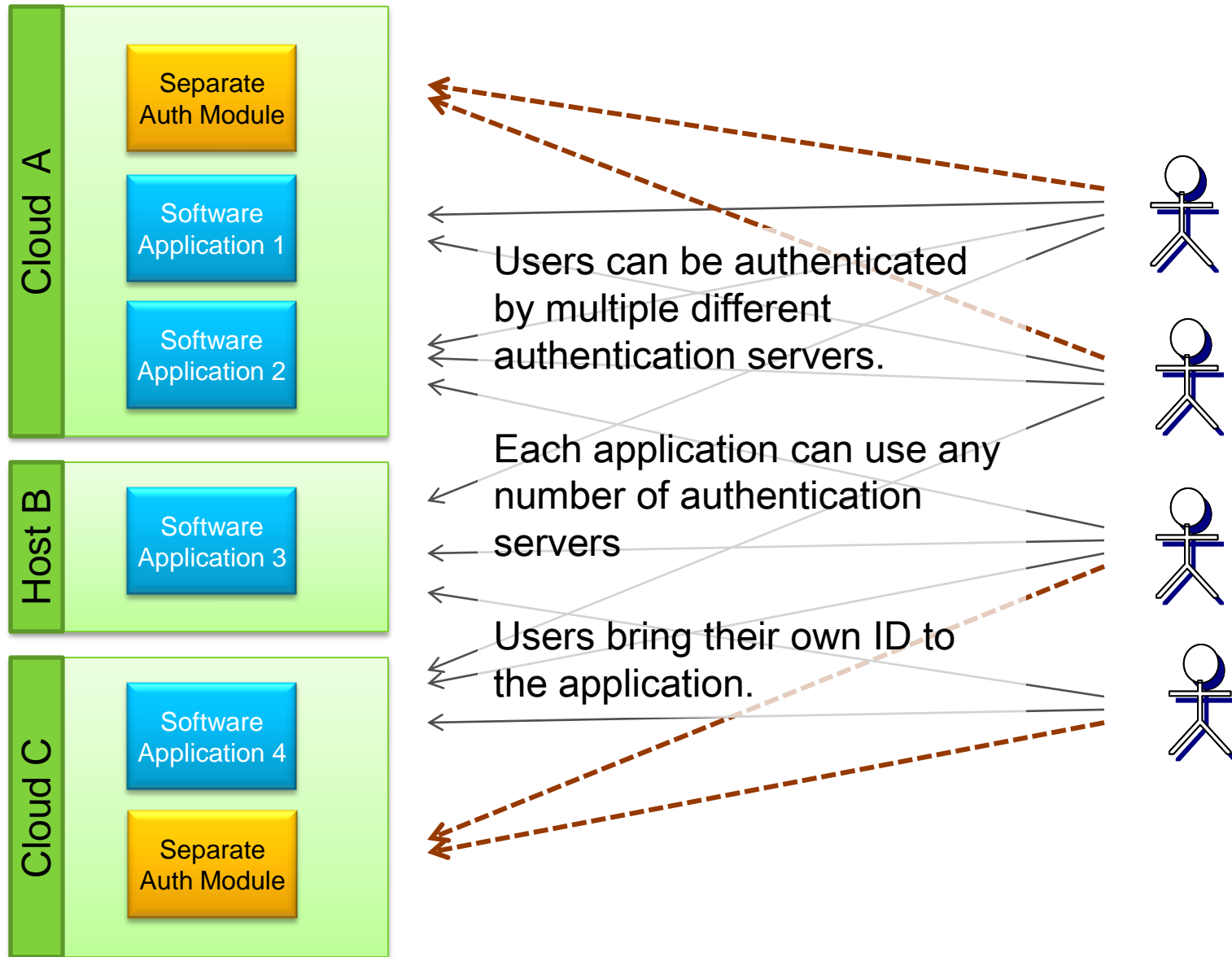
Many applications can share one authentication module even when they are running in the cloud!

Authentication module can be on any server, any address.

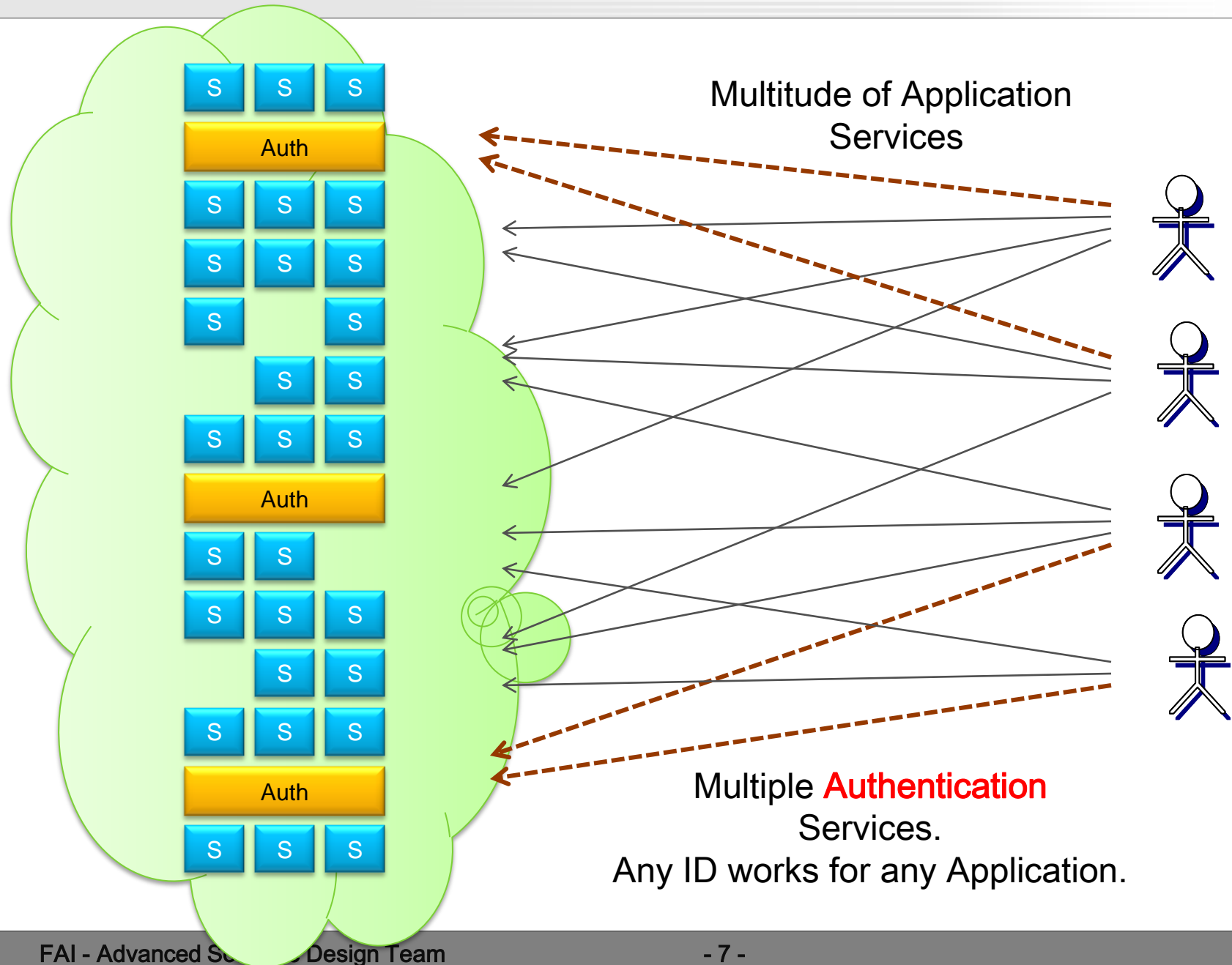
Authentication does not depend on the physical host that the application is run on.



Federated ID – Multiple Pools of People



True Cloud Model



Who Are You (WAY) Page



Most of application is the “page logic” that generates the normal pages.

Pages receive requests, either unauthenticated or authenticated based on application session.

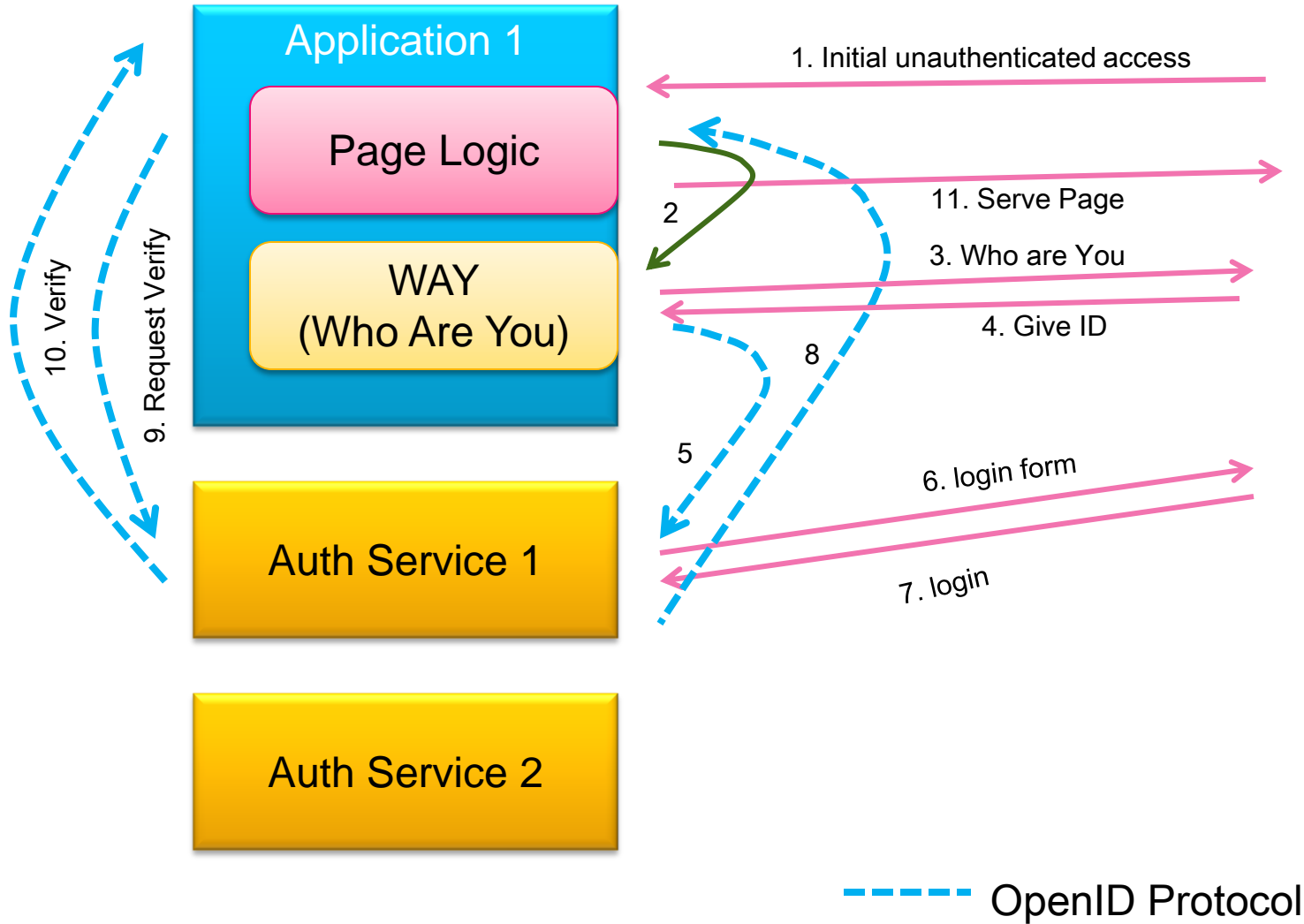
When user clicks login, the browser is directed to the “Who Are You” page.

The WAY page is a standard form inside an application to ask for the user ID.

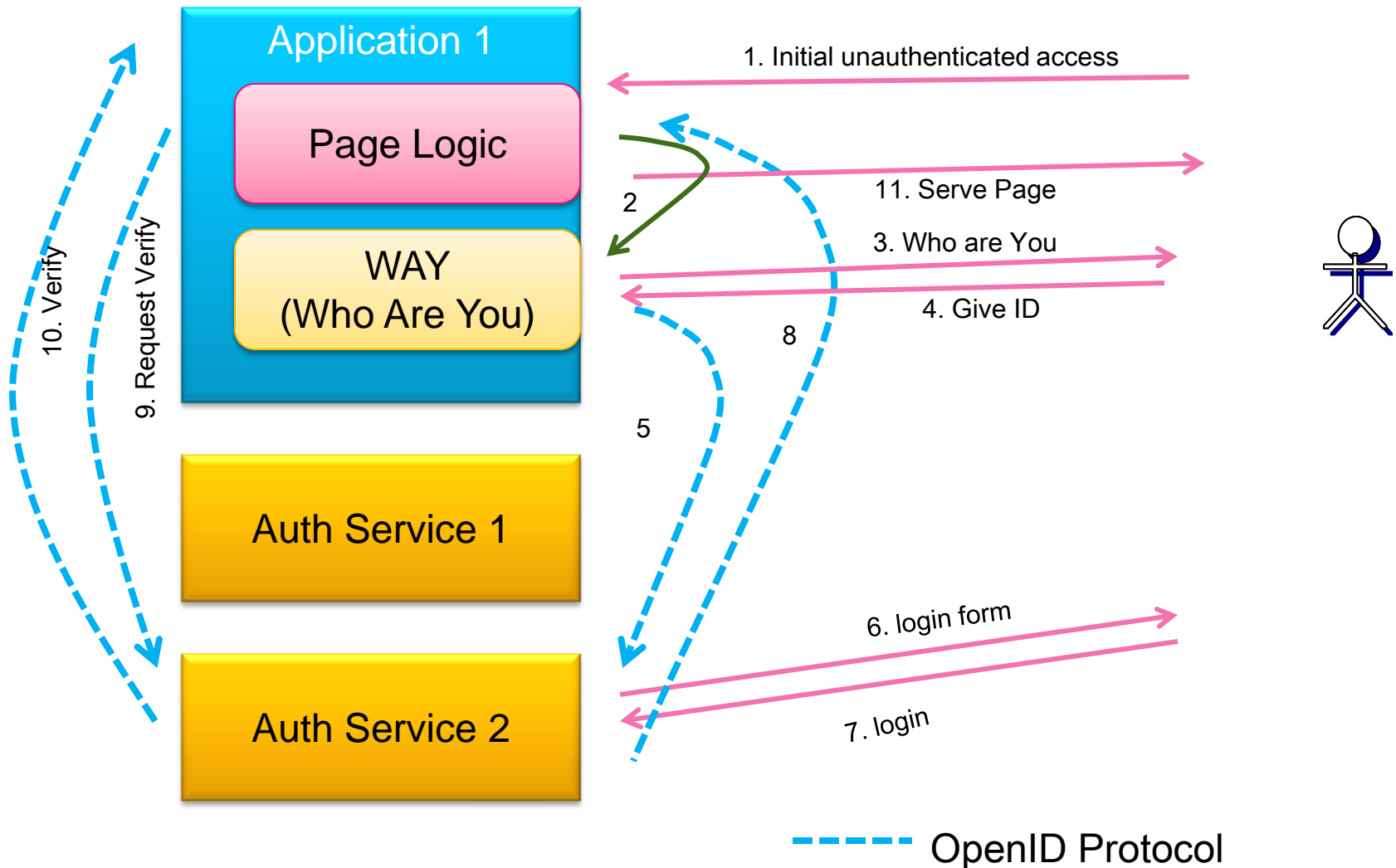
Then, depending upon the ID, the correct external authentication service is used for that ID using OpenID protocol.

WAY page is reusable in different apps.

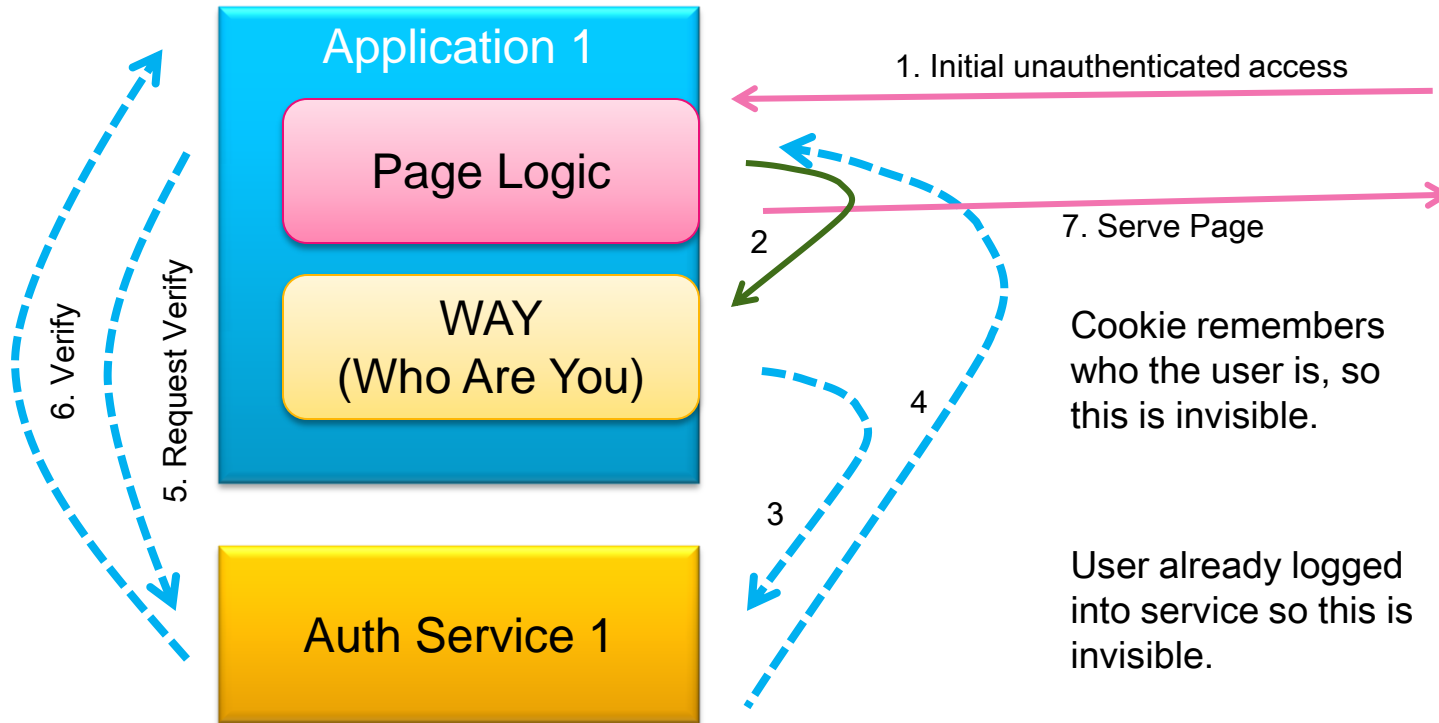
Who Are You Page != Login Page



ID (in WAY) specifies the Auth Service



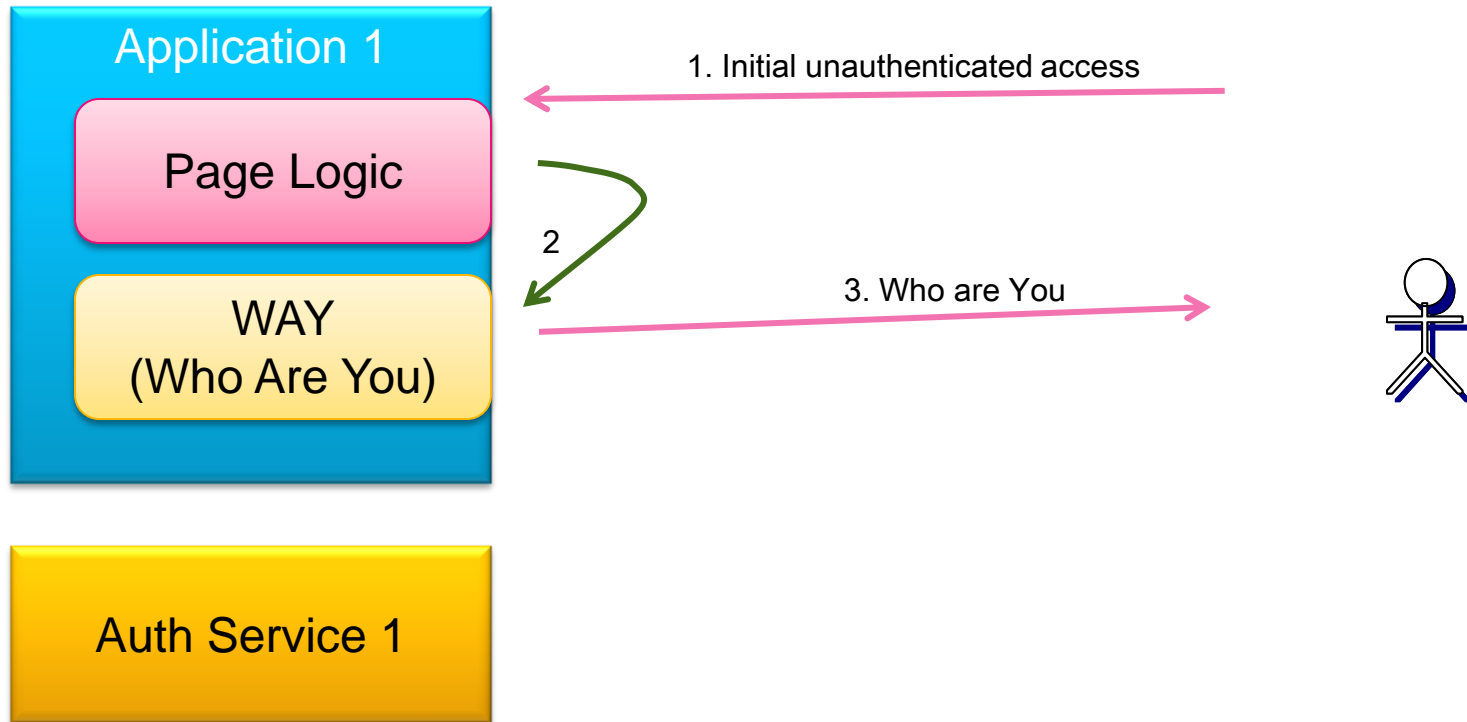
Login → automatic & transparent



Ready to start, click “log in”

The screenshot shows the Interstage Cognoscenti web application interface. At the top left is the Interstage COGNOSCENTI logo. To its right, the account information reads: "Account: Interstage Product Management" and "Interstage BPM V12 MRD". In the top right corner, the text "Welcome Page | Log in" is displayed, with the "Log in" link circled in red. Below the header is a navigation bar with five tabs: "Project Stream", "Project Notes" (which is active), "Project Tasks", "Project Documents", and "Project Settings". The main content area is divided into a left sidebar and a main panel. The sidebar contains several expandable sections: "General Links" (with a "Please log-in or register" link), "Recently Visited Projects", "To This Project", "From This Project", and "Tags". The main panel shows a "Public (1)" tab selected, with other tabs for "Member (1)", "Deleted Notes (0)", and "Draft Notes (0)". Below these tabs is a "Goals" section, which includes the text: "This page tracks the Version 12 MRD and PRD. Look in folder under attachments tab. Related to Interstage Product Management". At the bottom right of the "Goals" section, it says "- Last edited by Keith Swenson 11/13/2010" with an edit icon.

Step 1: request login



The “Who Are You” page

Interstage
COGNOSCENTI

Welcome Page | Log in
FUJITSU

Fujitsu Id

Open ID

Email Address

Register for New

Login with Open ID

Open Id:

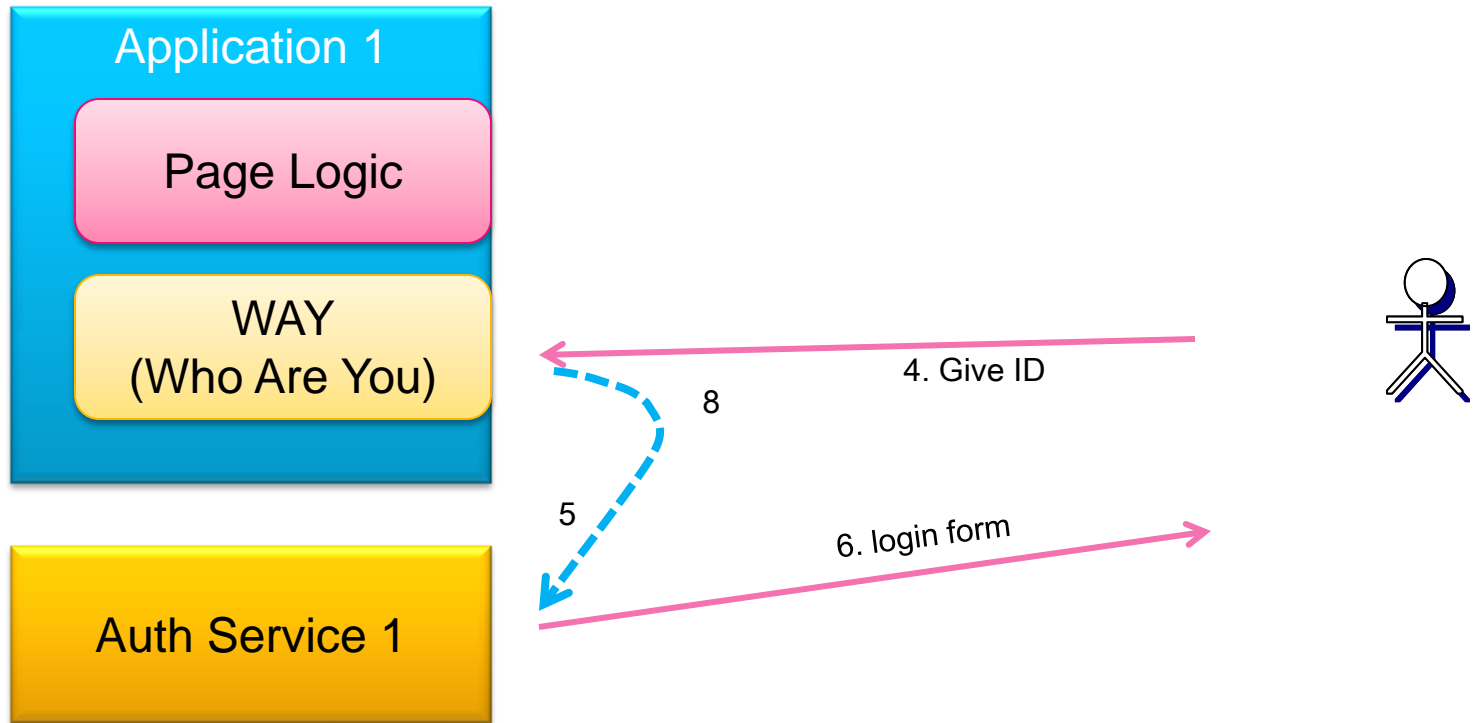
Login

[What is Open ID ?](#)

Validate HTML | Old UI

Copyright 2011 Fujitsu America Incorporated. All rights reserved.

Step 2: Specify ID, get login form



Log in to ID Provider (myopenid)



SIGN IN

 Notice [Dismiss](#)

You must sign in to authenticate to <http://leaves.interstagebpm.com:8080/nugen/t/Cognoscenti.htm> as <http://kswenson.myopenid.com/>

Username <http://kswenson.myopenid.com/>

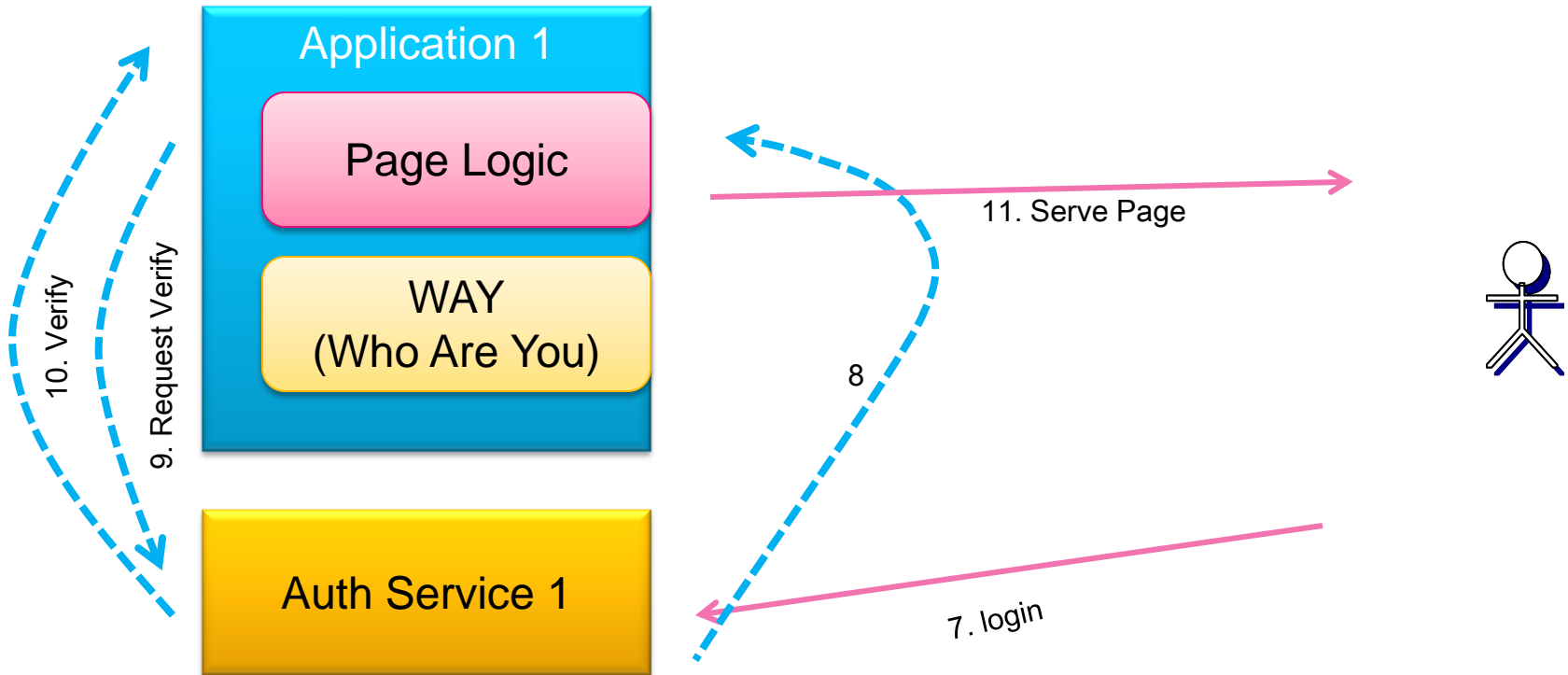
Password

☐ Stay signed in

[Sign In](#) [Cancel](#)

- [Sign in with an SSL certificate](#)
- [I cannot access my account](#)

Step 3: submit password to provider



Now you are logged in

The screenshot displays the Interstage Cognoscenti web application interface. At the top, the user is logged in as Keith Swenson, with a welcome message and the Fujitsu logo. The navigation bar includes links for Projects, Updates, Tasks, Settings, Administration, and Log Out. The main content area is titled 'Project Notes' and shows a list of notes under the 'Public (1)' tab. The note titled 'Goals' is selected, displaying its content: 'This page tracks the Version 12 MRD and PRD. Look in folder under attachments tab. Related to Interstage Product Management'. The note was last edited by Keith Swenson on 11/13/2010. Action links for 'Edit Note', 'Send Note By Email', and 'Zoom' are visible. A sidebar on the left contains a search bar and a list of project-related links: 'Recently Visited Projects', 'To This Project', 'From This Project', and 'Tags'. A footer section at the bottom indicates the user's role as an administrator with read and write access to all non-private project information, and includes a 'Logout' button.

Interstage
COGNOSCENTI

Account: Interstage Product Management
Interstage BPM V12 MRD

Projects | Updates | Tasks | Settings | Administration | Log Out

Welcome, Keith Swenson FUJITSU

Project Stream | **Project Notes** | Project Tasks | Project Documents | Project Settings

Search
 GO

▼ Recently Visited Projects

▼ To This Project

▼ From This Project

▼ Tags

Public (1) | Member (1) | Deleted Notes (0) | Draft Notes (0)

Create Note [+] Expand All Export to PDF

► Goals - Last edited by Keith Swenson 11/13/2010

This page tracks the Version 12 MRD and PRD.
Look in folder under attachments tab.
Related to Interstage Product Management

Edit Note Send Note By Email Zoom

You are logged in as Keith Swenson
You are an admin of this Project, you have read and write access to all (non private) information on the Project.
Logout

- Do not get confused:

- ID – a universal, global identification of a user
- Authentication – proof that the user is who they say they are
- Authorization – what they are allowed to do
- Profile – settings that are associated with the user

- These are all SEPARATE concepts
 - OLD SYSTEM often required these to be from one place
 - New design allows different servers to be responsible for different parts

- ID – a universal, global identification of a user
 - Same ID can be used in many applications, many hosts
 - Looks like a URL
- Authentication – proof that the user is who they say they are
 - OpenID provider takes care of proving who user is
 - ONLY the OpenID provider takes/handles a password
- Authorization – what they are allowed to do
 - Each application controls what user is able to do
 - Nothing to do with OpenID provider
- Profile – settings that are associated with the user
 - Each application keeps settings for each user

Application Requirements

- Each application has an “internal id” to track each user
- User may have multiple global ID
 - They can log in with more than one OpenID, for example
- First time they log in,
 - the application generates and assigns the internal ID
 - Sets up a profile for them
 - Asks for and remembers their display name
- Later they are allowed to
 - add and remove OpenIDs
 - add and remove email addresses
 - change their name

For example


Personal Settings

Contacts



Connections

Accounts

Unsubscribe



Keith Swenson's Settings
From here you can view your own profile settings.

 [Change Password](#)  [Update Settings](#)

Name: Keith Swenson

Display Name

Description: New profile for Keith, with completely unnecessary Japanese characters included in name (危機 or 名匠)

Preferred Email: keith.swenson@us.fujitsu.com

Alternate Email: kswenson@us.fujitsu.com

Multiple Email

Open Id: <http://kswenson.leaves.interstagebpm.com:8080/id/>
<http://kswenson.myopenid.com/>

Multiple OpenIDs

Last Login: 22 minutes ago. as <http://kswenson.myopenid.com/>

Unique Id: VBJIRKIHG

Internal ID

■ “Who Are You” Module

- Standard Java Servlet for inclusion in application
- Uses J2EE session to communicate with application
- Configure for simple UI for special services

■ Auth Service for LDAP

- Separately installed TomCat Application
- Configure to talk to an LDAP server


■ Auth Service for Active Directory

- Separately installed TomCat Application
- Uses NTLM to authenticate user transparently


■ Auth Service for Database

- Separately installed TomCat Application
- Stores user info in DB, has UI for changing/resetting password

Who Are You (Email)



Welcome Page | [Log in](#)



[Fujitsu Id](#)

[Open ID](#)

Email Address

[Register for New](#)

Login with Email Address

Email Address:

Password:

[Login](#)

[Forgot your Password ?](#)

[Validate HTML](#) | [Old UI](#)

Copyright 2011 Fujitsu America Incorporated. All rights reserved.

Who Are You (OpenID)

Interstage
COGNOSCENTI

Welcome Page | Log in
FUJITSU

Fujitsu Id

Open ID

Email Address

Register for New

Login with Open ID

Open Id:

Login

[What is Open ID ?](#)

[Validate HTML | Old UI](#)

Copyright 2011 Fujitsu America Incorporated. All rights reserved.

Who Are You (Specially Configured)

The screenshot shows a web application interface. At the top left is the 'Interstage COGNOSCENTI' logo. At the top right are links for 'Welcome Page' and 'Log in', and the 'FUJITSU' logo. The main content area features a sidebar with four buttons: 'Fujitsu Id' (selected), 'Open ID', 'Email Address', and 'Register for New'. The 'Fujitsu Id' section contains a title 'Login with Fujitsu Id', a text input field with 'kswenson', a URL 'http://kswenson.leaves.interstagebpm.com:8080/id/', and a 'Login' button. The footer includes 'Validate HTML | Old UI' on the left and 'Copyright 2011 Fujitsu America Incorporated. All rights reserved.' on the right.

Interstage
COGNOSCENTI

Welcome Page | Log in
FUJITSU

Fujitsu Id

Open ID

Email Address

Register for New

Login with Fujitsu Id

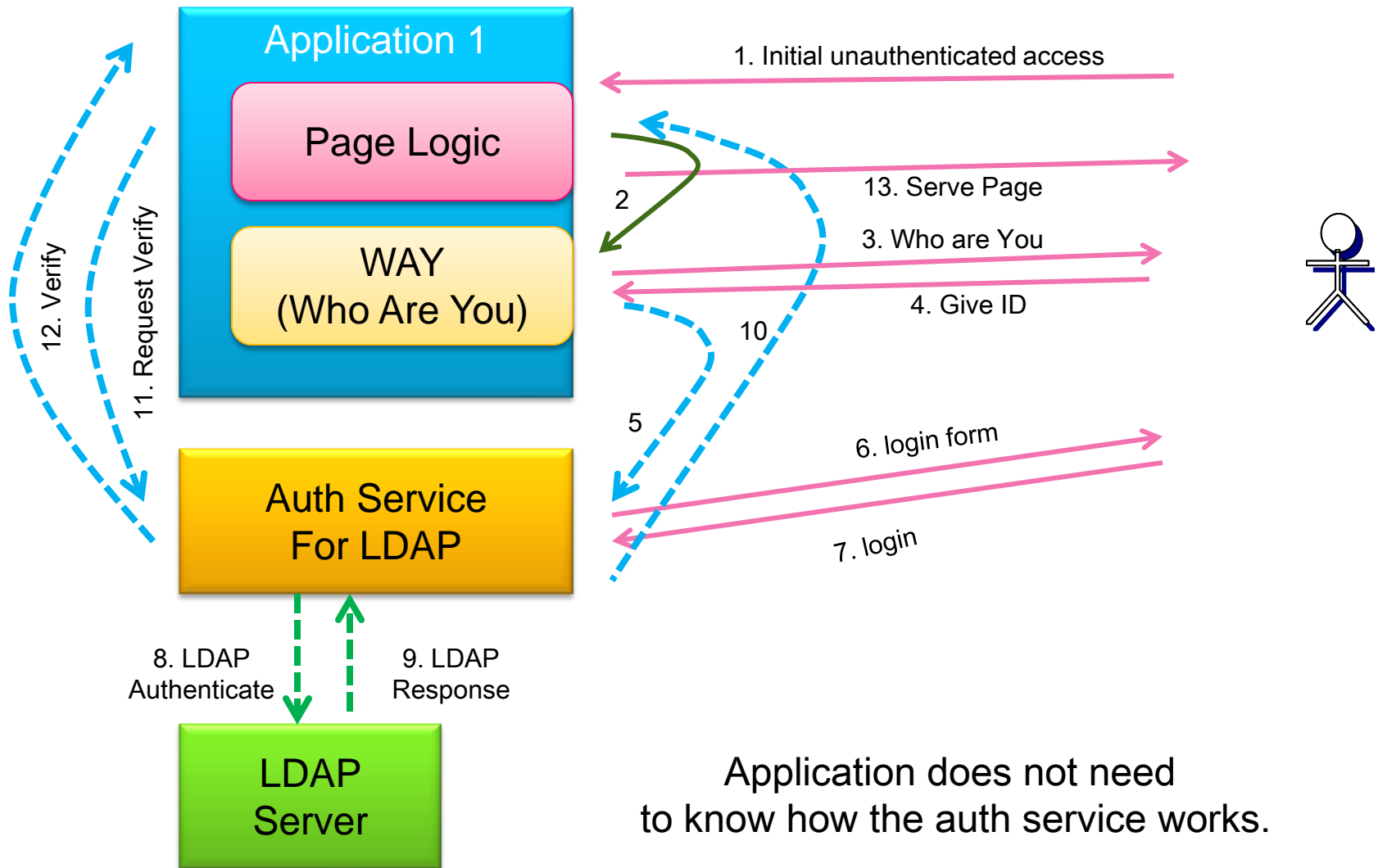
Fujitsu Id
kswenson

http://kswenson.leaves.interstagebpm.com:8080/id/

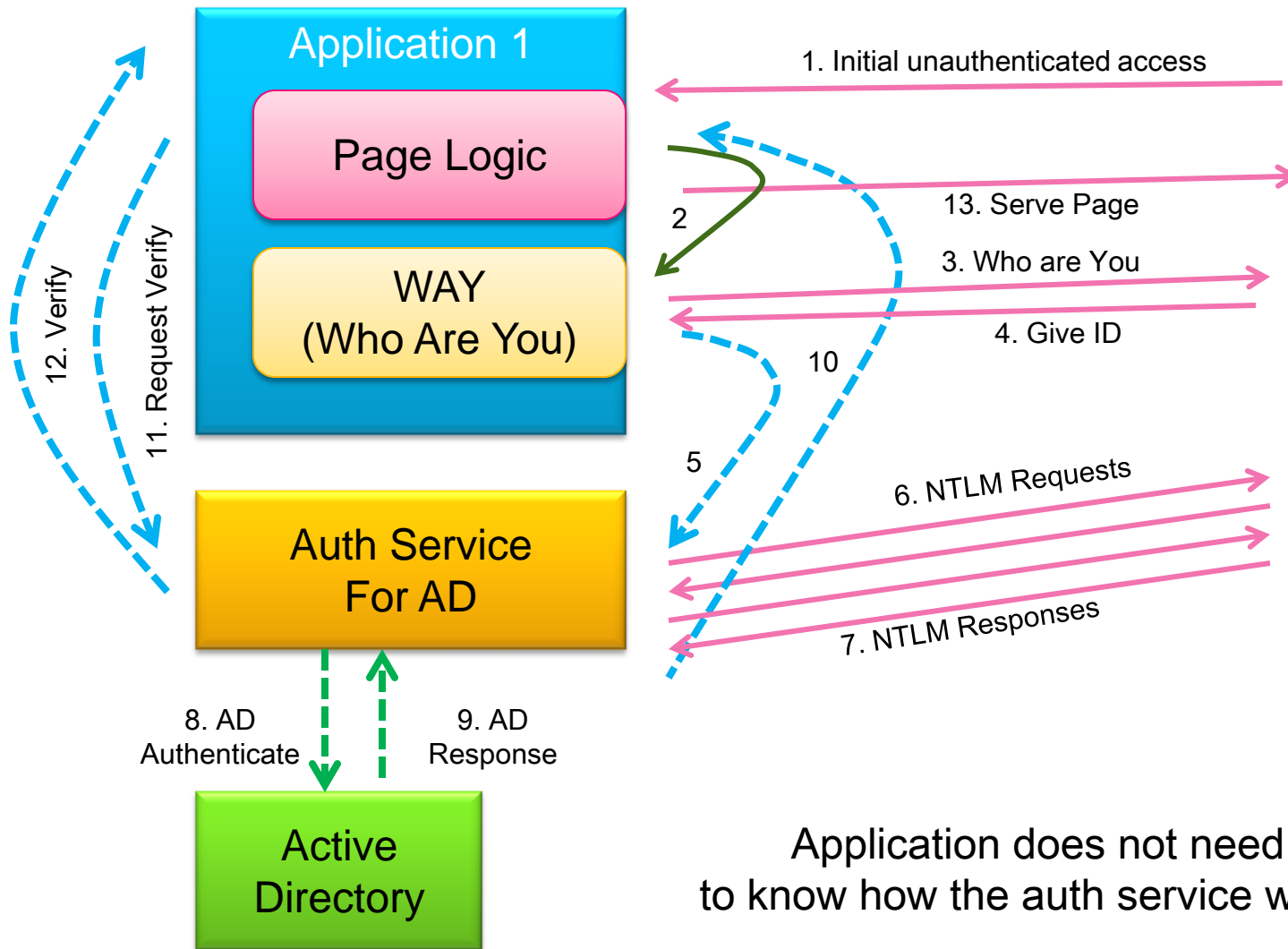
Login

Validate HTML | Old UI

Copyright 2011 Fujitsu America Incorporated. All rights reserved.

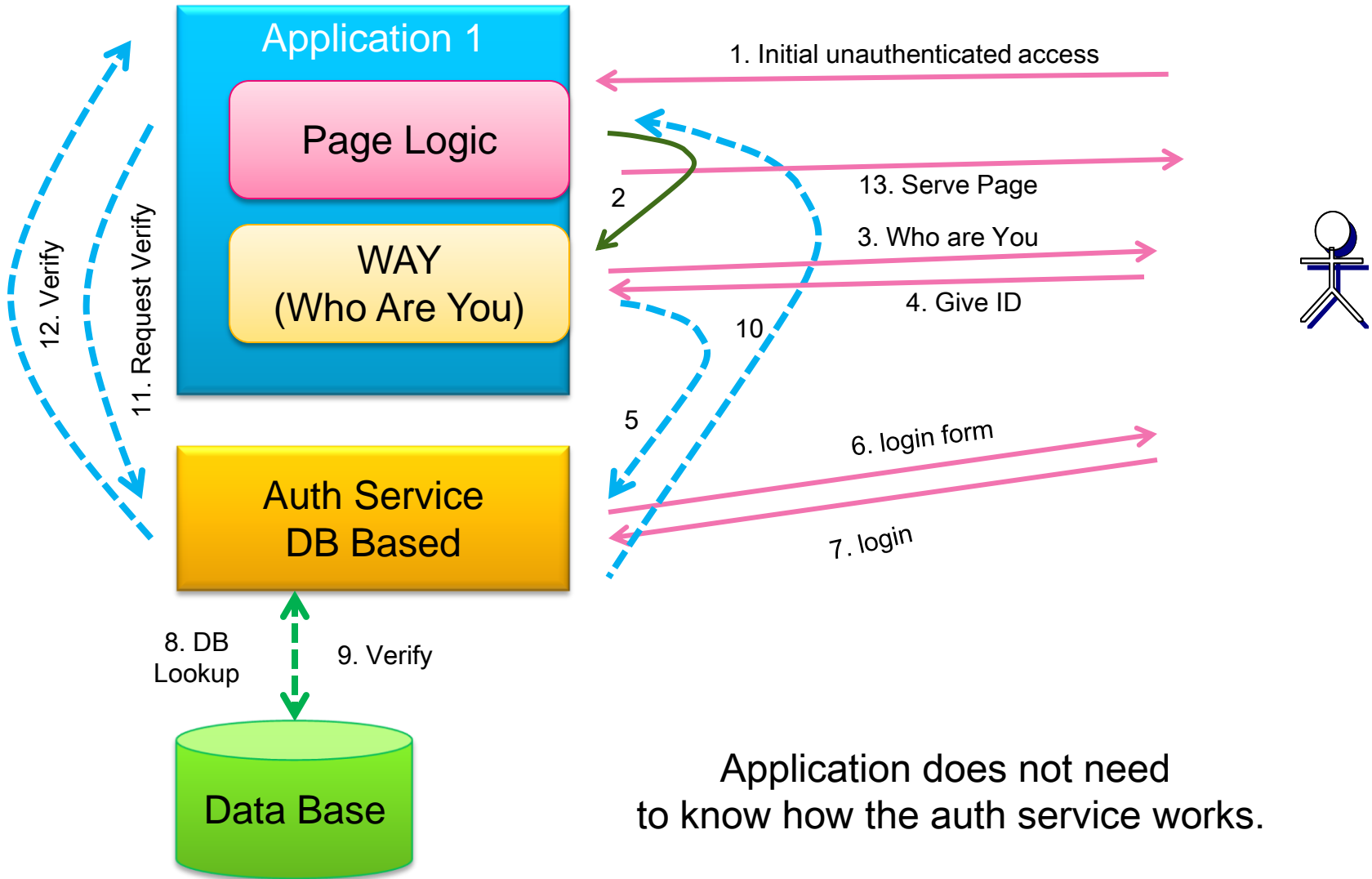


Auth Service for Active Directory

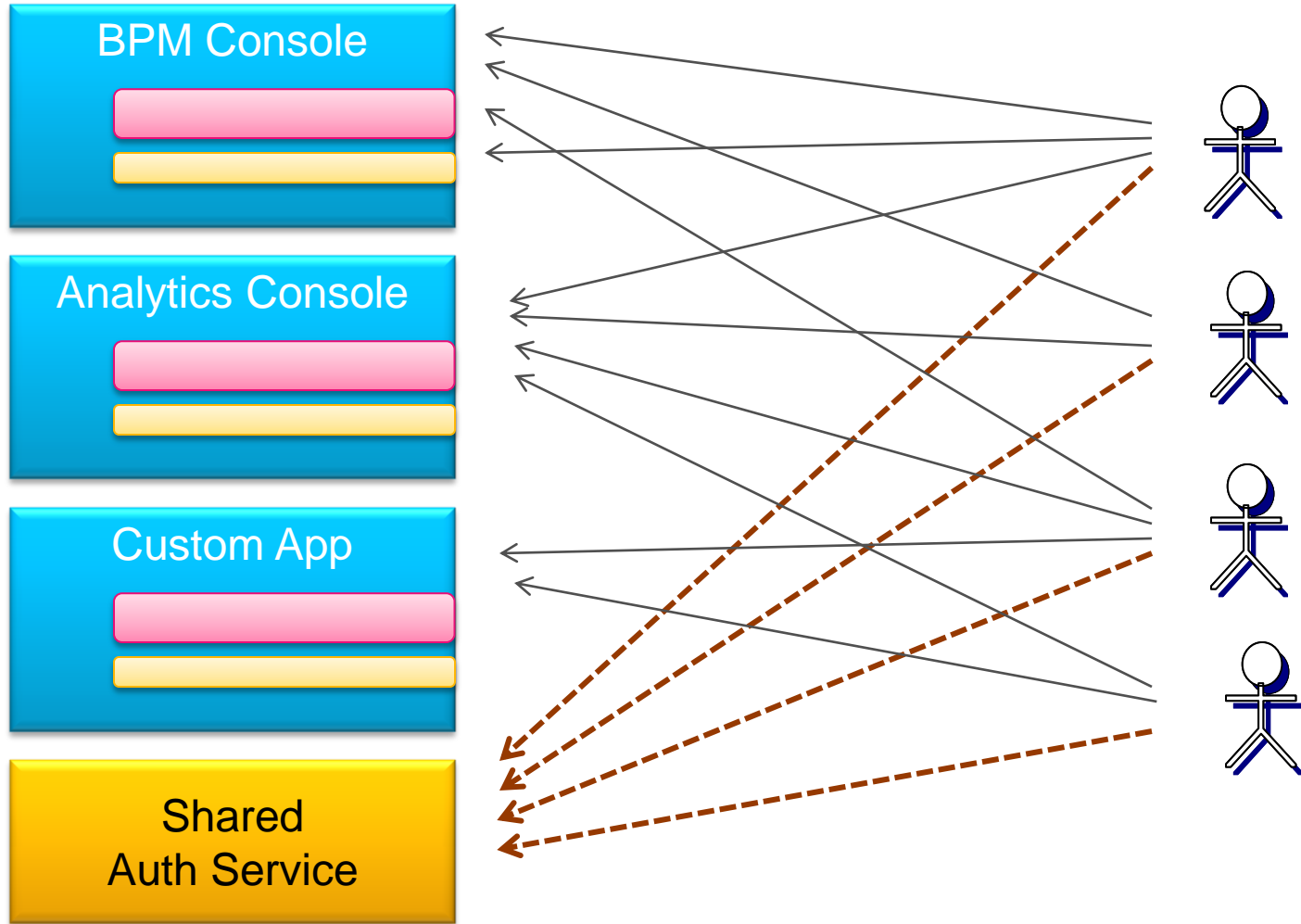


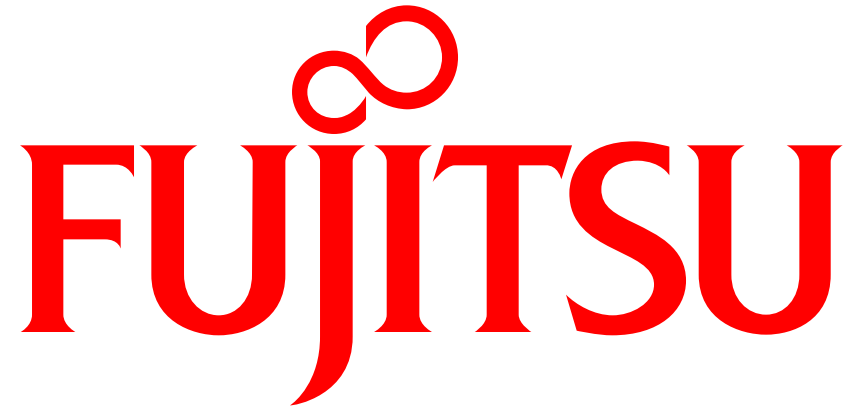
Application does not need to know how the auth service works.

Auth Service for Active Directory



Allows SSO for our Suite





shaping tomorrow with you