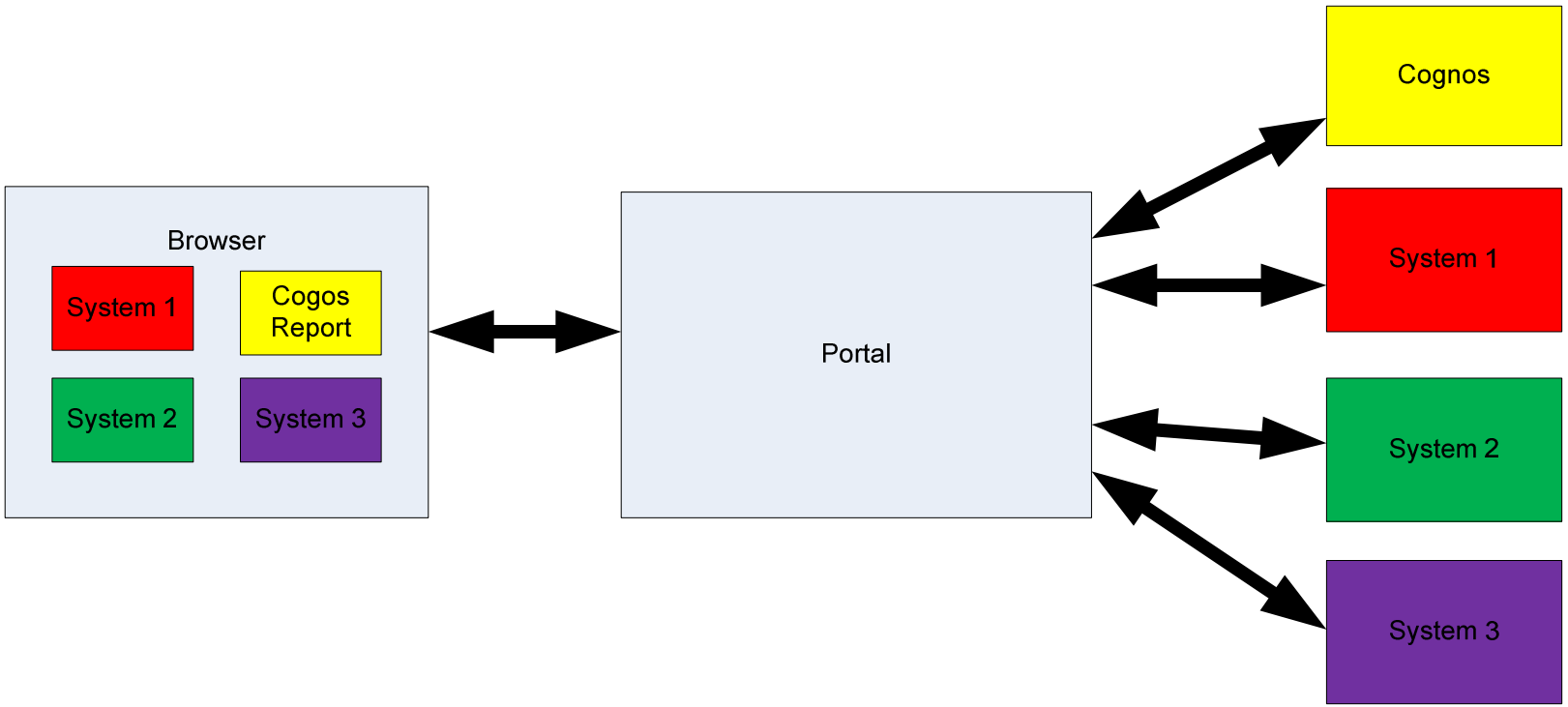
Integrating WebSphere Portal and Cognos Identities

On a WebSphere Application Server Platform

Core Presentation Pattern



Portlet options

- Cognos provides portlet – “Cognos Portal Services”
  - Portlet is IFRAME based
- Cognos provides APIs
  - Portlets can be written
- Access to data must be controlled
  - Need to consider security model

We are assuming use of “Cognos Portal Services” out of the box portlets

Commonality

Portal

- Authorization is per-user but commonly aggregated into roles.
- Roles are commonly implemented using registry groups.
- Must run under WebSphere Application Server.

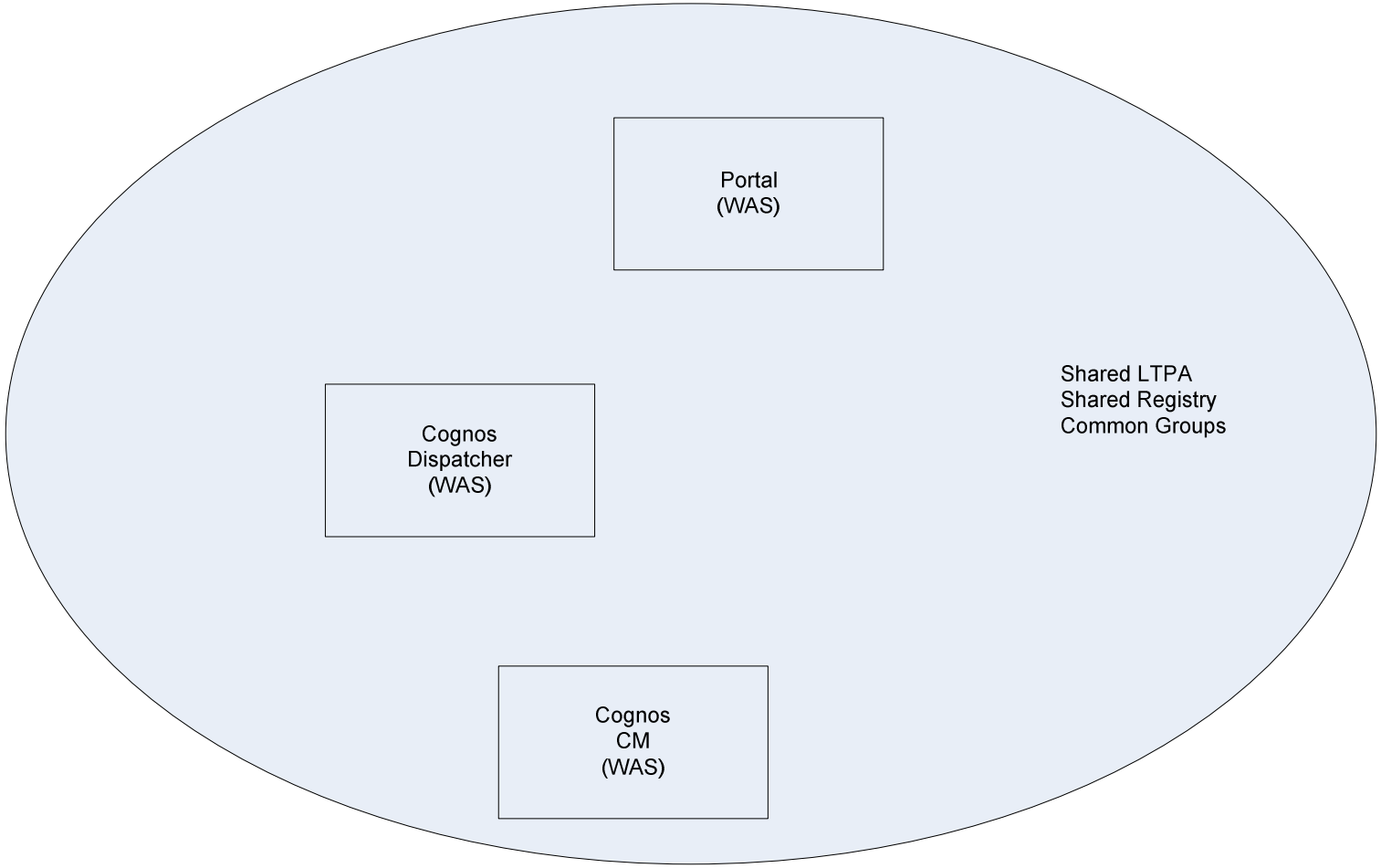
Cognos

- Authorization is per-user but commonly aggregated into roles.
- Roles are commonly implemented using registry groups.
- Can run under WebSphere Application Server.

Solution v1

1. Run everything on WebSphere Application Server
2. Use standard WebSphere LTPA functionality to assert identity at a WAS level.
3. Use shared registry & groups to maintain consistent authorization and roles.

Simple!


Portal
(WAS)
Cognos
Dispatcher
(WAS)
Cognos
CM
(WAS)
Shared LTPA
Shared Registry
Common Groups

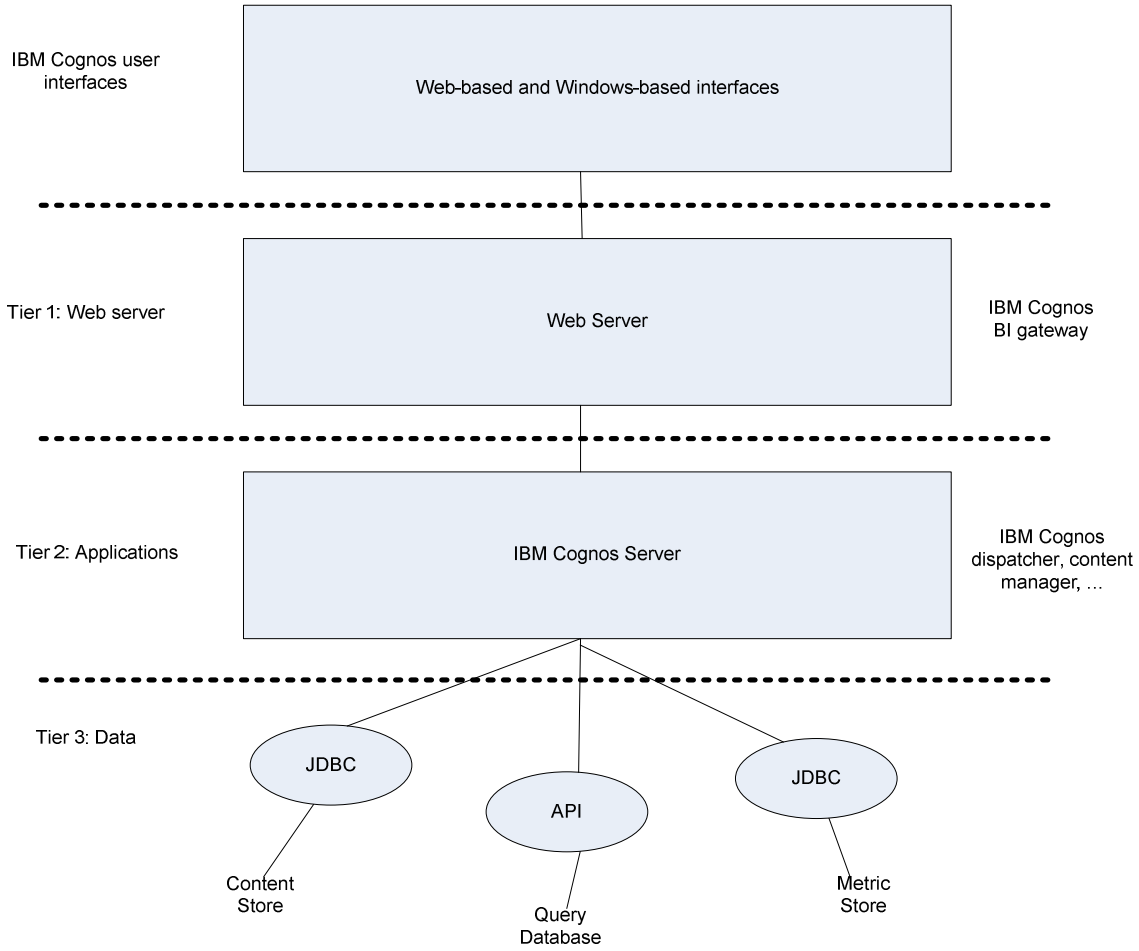
Challenge

- Standard WebSphere Security/LTPA can provide access to the Cognos applications across WebSphere cell(s)

  BUT!

- Cognos does not use WAS's registry internally
- Cognos is unaware of user's WebSphere identity -> access to WAS application with no identity and hence rights!
- User is challenged for authentication information

Generic Cognos Architecture



IBM Cognos Gateway

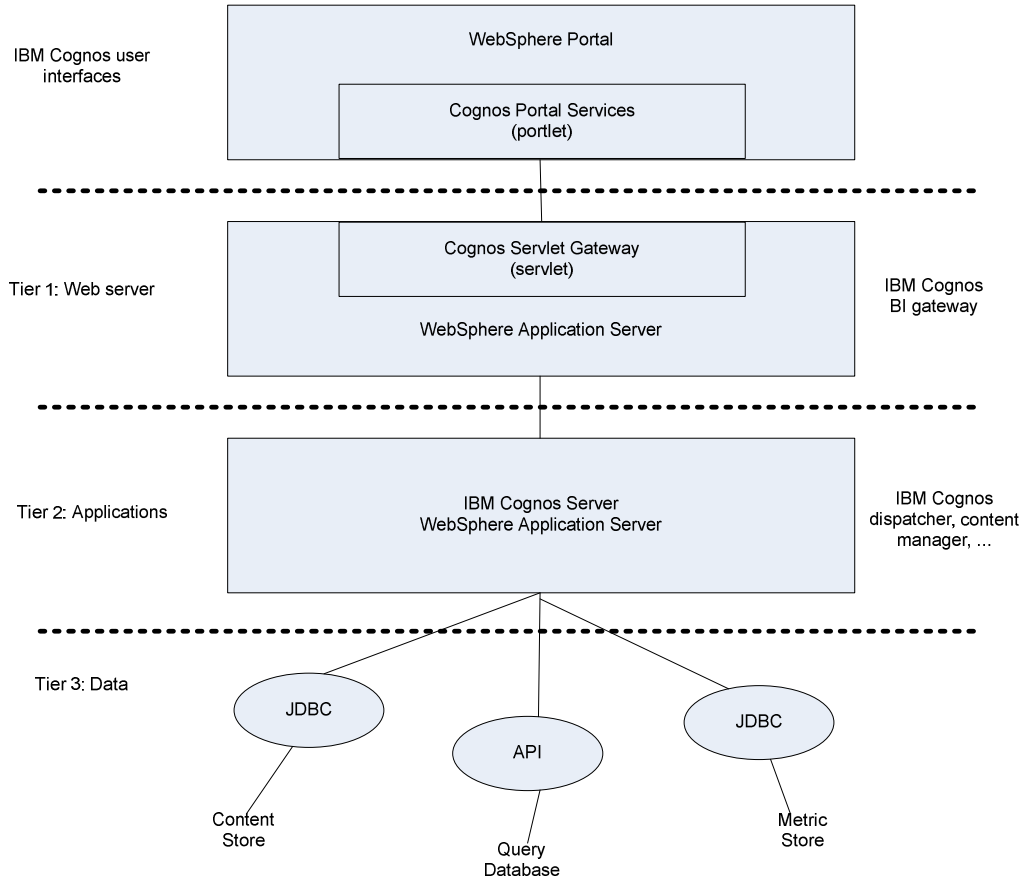
When an IBM Cognos BI gateway receives a request, it:

1. Encrypts passwords to ensure security
2. **Extracts information needed to submit the request to an IBM Cognos BI server**
3. Attaches environment variables for the Web server
4. Adds a default namespace to the request to ensure that the server authenticates the user in the correct namespace
5. Passes requests to an IBM Cognos BI dispatcher for processing

Solution v2

1. Use standard WebSphere LTPA functionality to assert identity at a WAS level.
2. Assert WebSphere identity to Cognos
    1. Use a Cognos BI Gateway
    2. Use of LTPA by Gateway requires IBM product -> IBM Cognos Servlet BI Gateway (WAS based)
3. Configure portlet(s)
    1. IBM WSRP WSDL Location: Gateway
    2. Active Credential Type: LtpaToken
    3. (cps_auth_namespace: Cognos namespace hint)
4. Use shared registry & groups to maintain consistent authorization and roles.

Example WebSphere Portal/Cognos Architecture



Solution v2 - Implementation

1. **Use standard WebSphere LTPA functionality to assert identity at a WAS level.**
2. Assert WebSphere identity to Cognos
    1. **Use Cognos BI Gateway**
    2. **Use of LTPA by Gateway requires IBM product -> IBM Cognos Servlet BI Gateway (WAS based)**
3. Configure portlet(s)
    1. IBM WSRP WSDL Location: Gateway
    2. Active Credential Type: LtpaToken
    3. (cps_auth_namespace: Cognos namespace hint)
4. Use shared registry & groups to maintain consistent authorization and roles.

LTPA Options

1. Use a single cell for WebSphere Portal and the Cognos Gateway WAS server (at least)

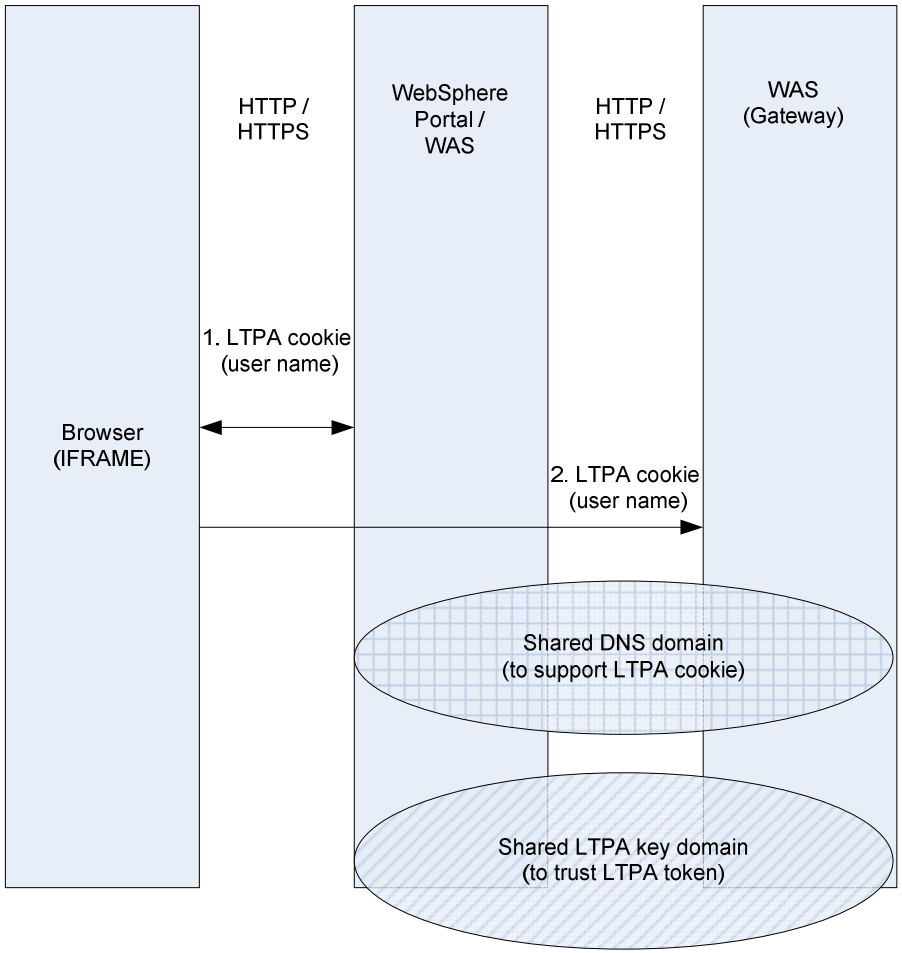
   OR

   Share the LTPA keys, cookie domain, … between the Portal and Cognos Gateway WAS servers (at least)

   AND

2. Use a common DNS domain for user access to Portal and the Gateway – Cognos portlets are IFRAME based.

LTPA & DNS Interaction



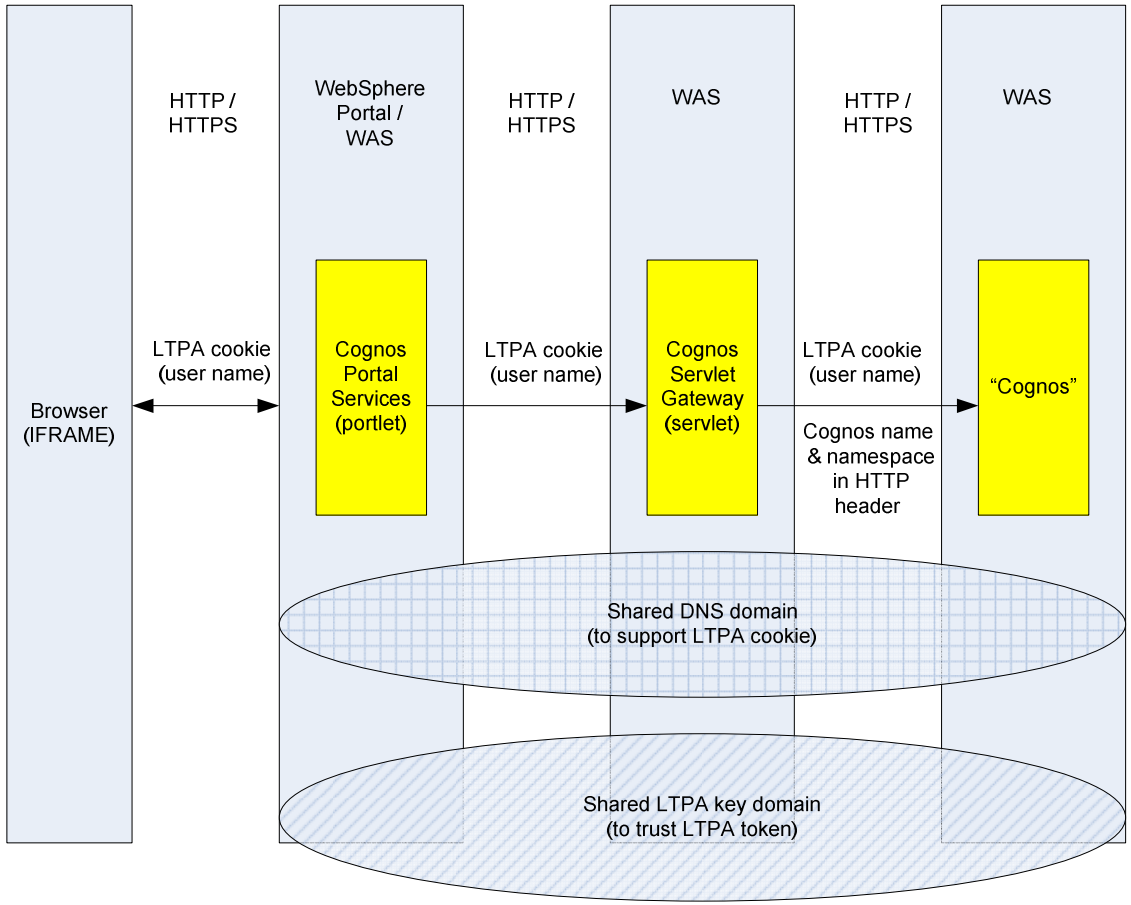
LTPA behaviour

- User is authenticated by ‘portal.example.com’ and receives an LTPA token/cookie for example.com
- Cognos portlet IFRAME references the gateway ‘gateway.example.com’
- Browser sends the cookie to the gateway (as domains match)
- Gateway WAS server accepts LTPA token and authenticates the user.

IBM Cognos Servlet Gateway

- WAS aware:
  - Retrieves the user's WAS identity (provided using LTPA) and encodes it in the HTTP header for Cognos
- Sets the user's Cognos namespace (based on a configuration setting of the gateway)
  - Encodes it in the HTTP header for Cognos
- Forwards (proxies) the request

Details - Reprise



Aside – VMM vs Cognos namespaces

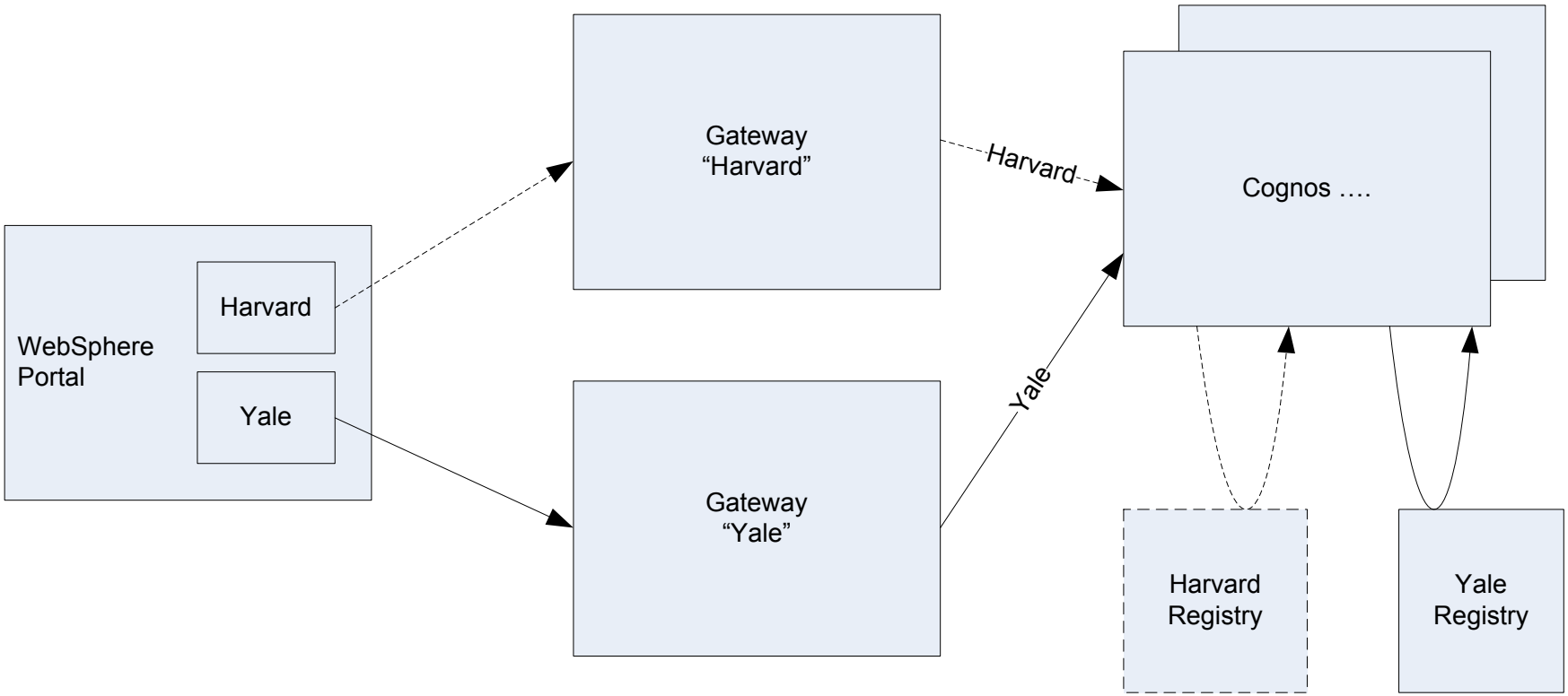
VMM

- A user is present in a specific registry
- WAS is only aware of one adapter (VMM)
  - For multiple registries the federated adapter transparently finds the user
  - No need to specify the registry

Cognos namespace

- A user is present in a specific registry
- Cognos is aware of multiple registries
  - A namespace specifies the registry
  - To logon or to assert an identity the name AND namespace must be specified
  - The gateway will add the (default) namespace

Cognos Namespace and Gateways



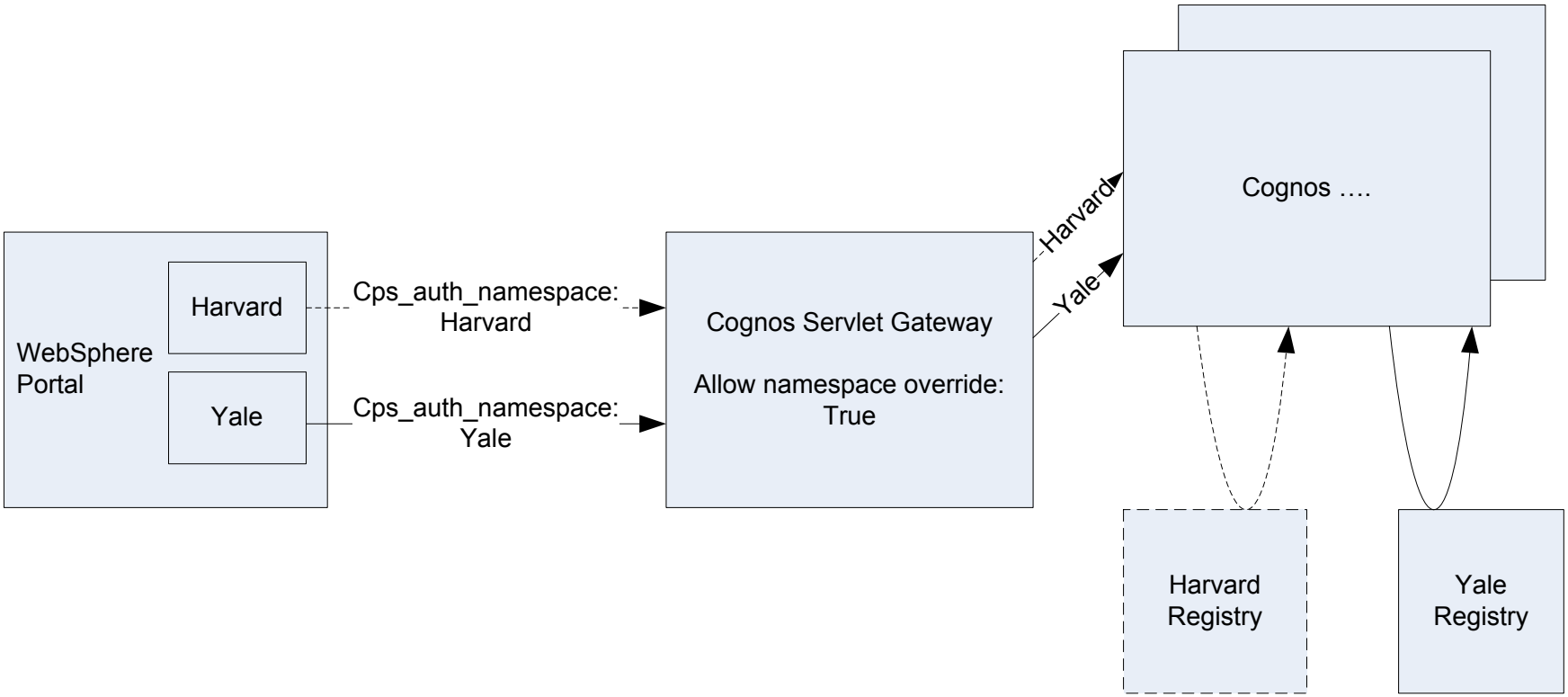
Opportunity

- The servlet gateway in combination with Portal services can support multiple namespaces with a single gateway
  - Single gateway (if portlets/Cognos Portal Services are only access mechanism)
  - Servlet gateway: **Allow namespace override: True**
  - Portlet Services: **cps_auth_namespace: <namespace>**
- The pattern is independent of the WAS authentication mechanism – SPNEGO/Windows desktop SSO can be enabled/provided at the Portal for use with Cognos

Portlet services vs WebSphere Servlet Gateway

1. Use standard WebSphere LTPA functionality to assert identity at a WAS level.
2. Assert WebSphere identity to Cognos
    1. Use a Cognos BI Gateway
    2. Use of LTPA by Gateway requires IBM product -> IBM Cognos Servlet BI Gateway (WAS based)
3. Configure portlet(s)
    1. IBM WSRP WSDL Location: Gateway
    2. Active Credential Type: LtpaToken
    3. (**cps_auth_namespace: Cognos namespace hint**)
4. Use shared registry & groups to maintain consistent authorization and roles.
5. **Cognos Servlet Gateway: Allow namespace override: True**

Servlet Gateway using namespace hints



Cognos Terminology for Portal Administrators

- Cognos Portal Services – smart WSDL configured IFRAME based portlet provided with Cognos.
- Cognos Servlet Gateway – servlet for deployment into WAS provided with Cognos.
- Namespace – a registry (realm) configured within Cognos separate to WAS's configuration.