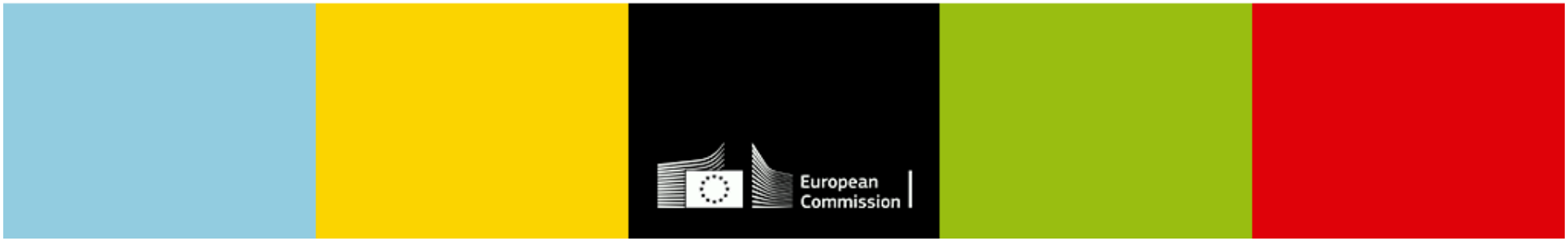
On line Training Material on AAI development

Identity Provider Concepts and Implementation

Luciano Fernandes Rocha / Francisco Leonardo Mota | RNP | 27-02-16 | WP2



Shibboleth

- What is Shibboleth?
  - *Middleware* project from Internet2
    - SAML (Security Assertion Markup Language)
      - Standard defined by OASIS (Organization for the Advancement of Structured Information Standards)
  - Federated access
    - Authentication
    - Authorization
  - SSO (Single Sign-On)

Shibboleth

- What is Shibboleth?
  - Components:
    - Identity Provider (IdP)
    - Service Provider (SP)
    - Discovery Service / WAYF (Where Are You From?)
    - Metadata

Shibboleth

- Why Shibboleth?
  - Developed to address the following challenges:
    - Multiple passwords required for multiple applications
    - Scalability in managing multiple applications
    - Security issues related to third-party services access
    - Privacy
    - Interoperability within and between organizations
    - Freedom of choice Authentication technologies for institutions
    - Access control made from the service providers

Shibboleth

- Why Shibboleth?
  - Compatible applications:
    - Google Apps
    - Media Wiki
    - Moodle, Joomla, Drupal
    - Blackboard
    - ProQuest
    - Confluence

Identity Provider (IdP)

- Identity
  - Authentication
    - Web SSO
  - Atributes

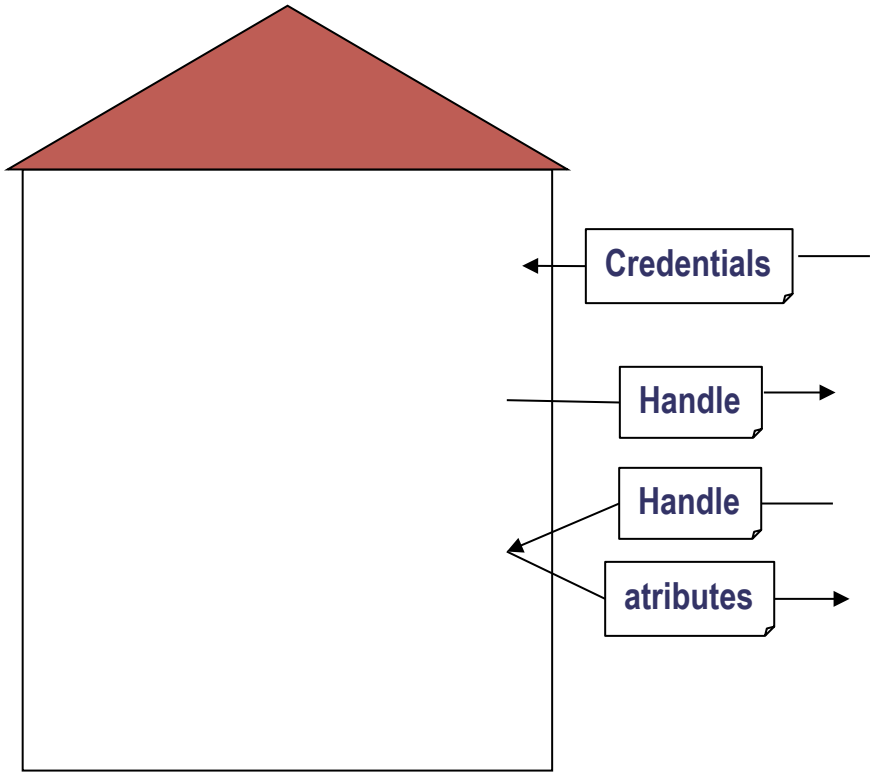


Figura 7.1

Identity Provider (IdP)

- Identity
  - Authentication
    - Web SSO
  - Atributes

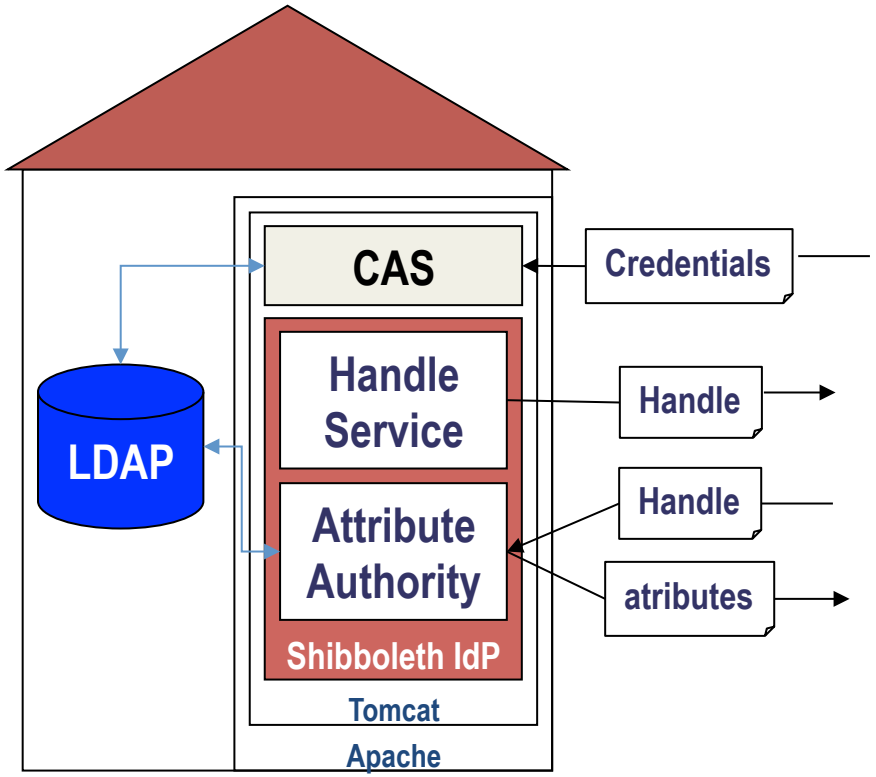


Figura 7.2

Identity Provider (IdP)

- Shibboleth Identity Provider
  - Handle Service
  - Attribute Authority
- CAS
  - Web SSO
- LDAP
  - Authentication
  - Atributes

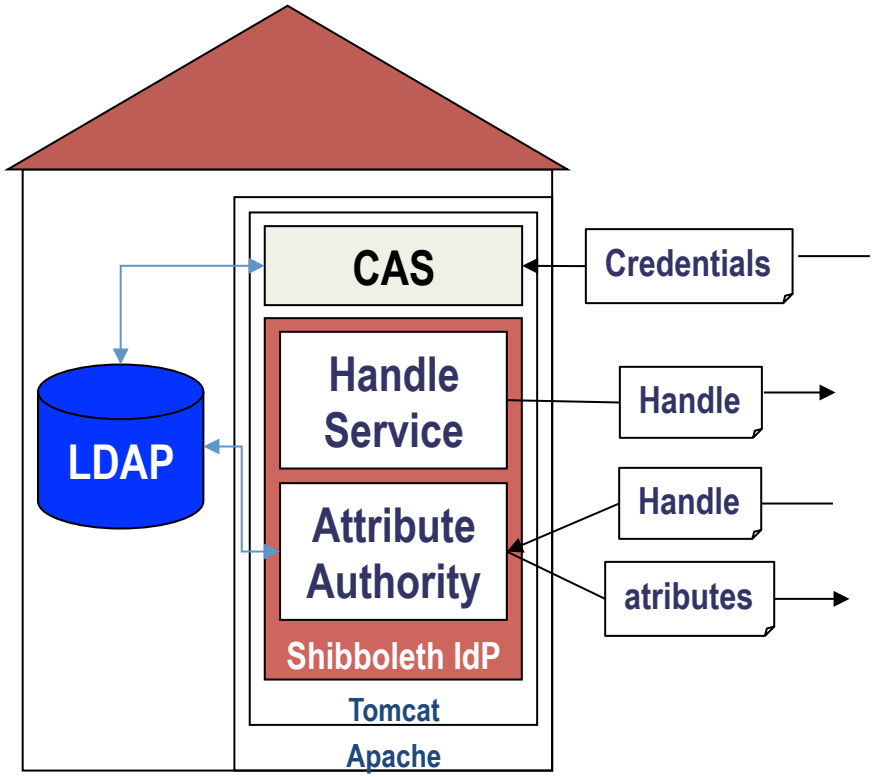


Figura 7.3

Service Provider (SP)

- Service
  - Resource
  - Authorization

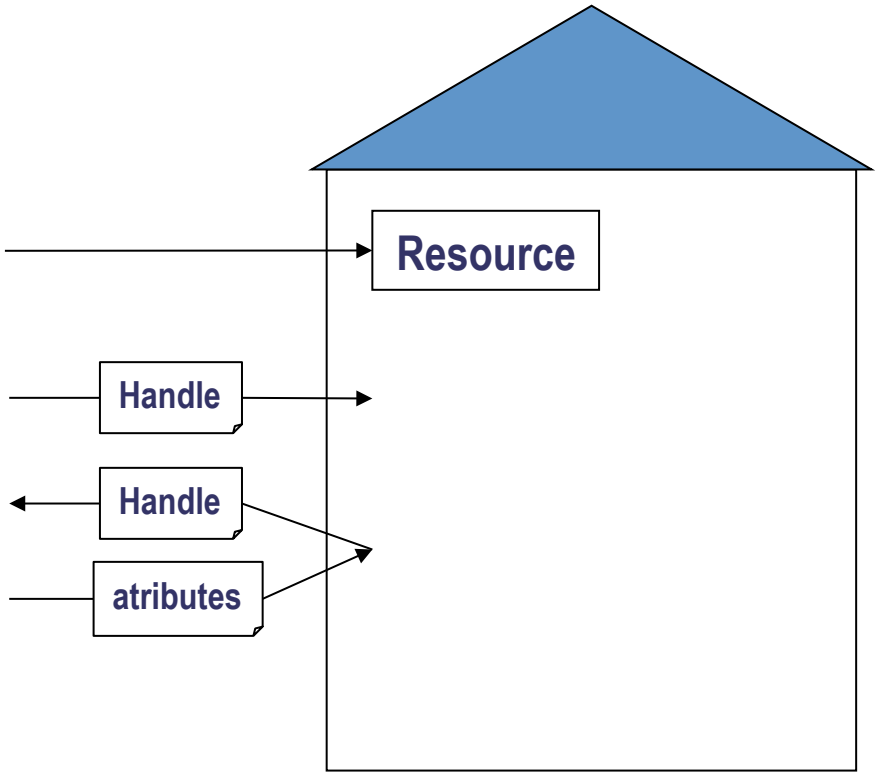


Figura 7.4

Service Provider (SP)

- Service
  - Resource
  - Authorization

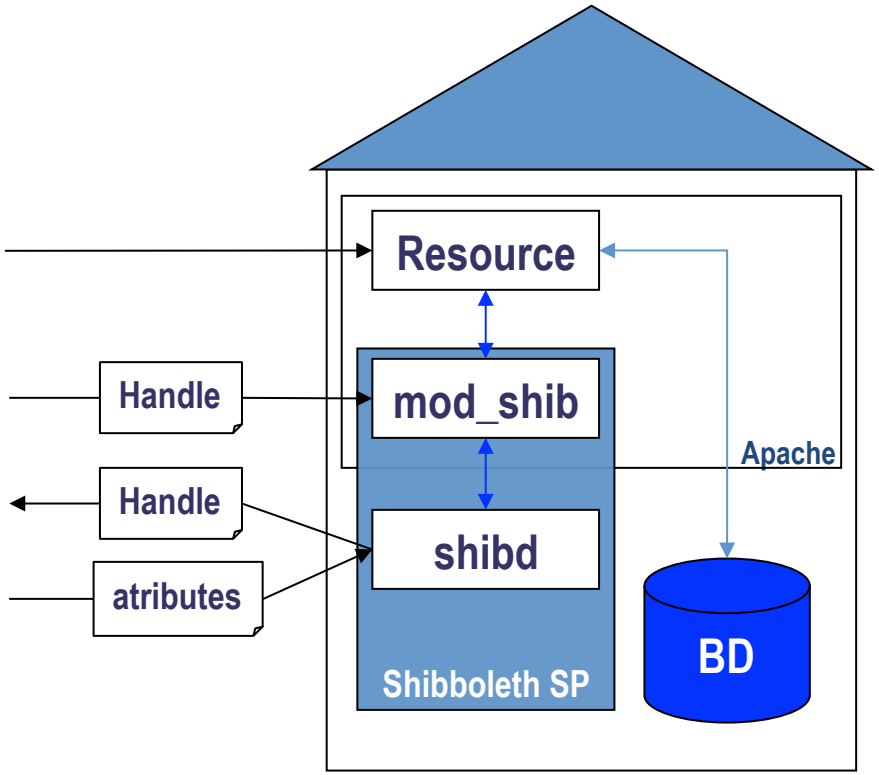


Figura 7.5

Service Provider (SP)

- Shibboleth Service Provider
  - mod_shib
    - Apache Module
  - shibd
    - Daemon

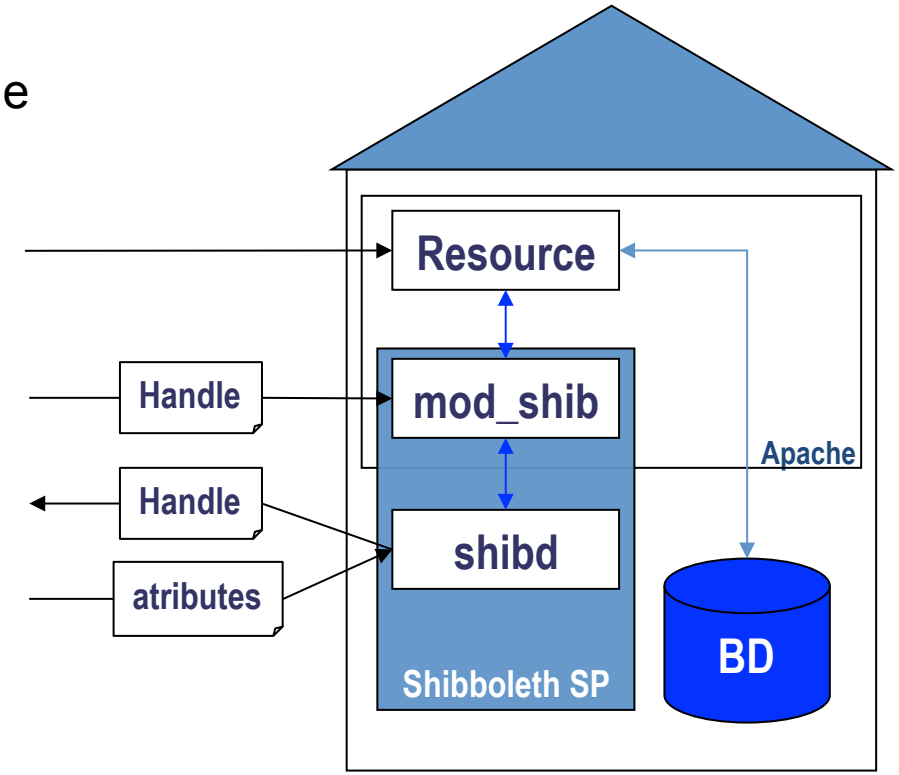


Figura 7.6

DS/ WAYF

- Where are you from?
  - Wha is your identity provider?

Metadata

- Configuration file
  - SAML Metadata (schema) + Extensions Shibboleth
  - Shared between federation providers

Metadata

- Metadata
  - Trust relationship between providers
    - Certificates
    - Public keys
  - Informations for communication between providers
    - IDs
    - URLs
    - Protocols

Identity Federation Operation

- Phase 1

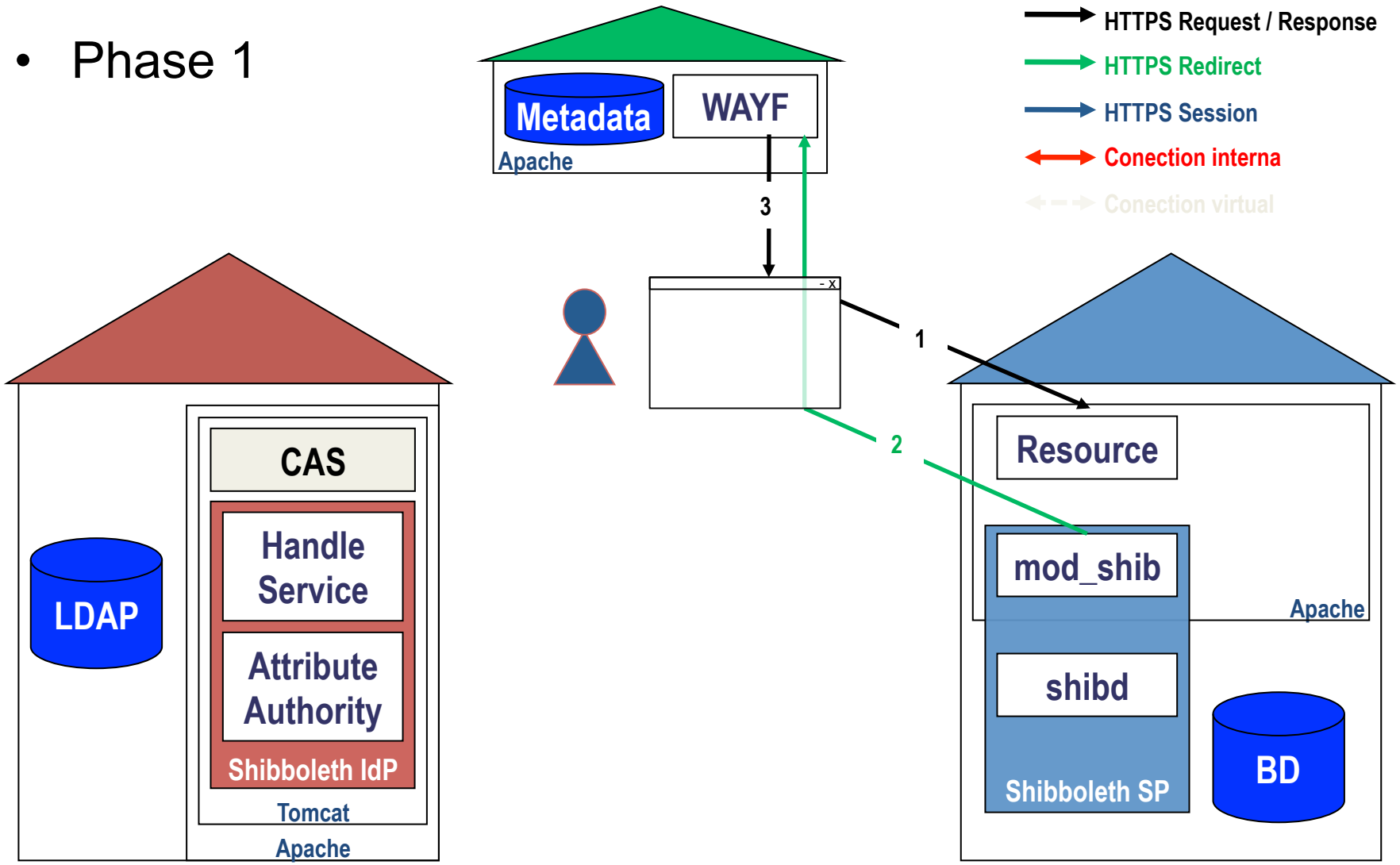
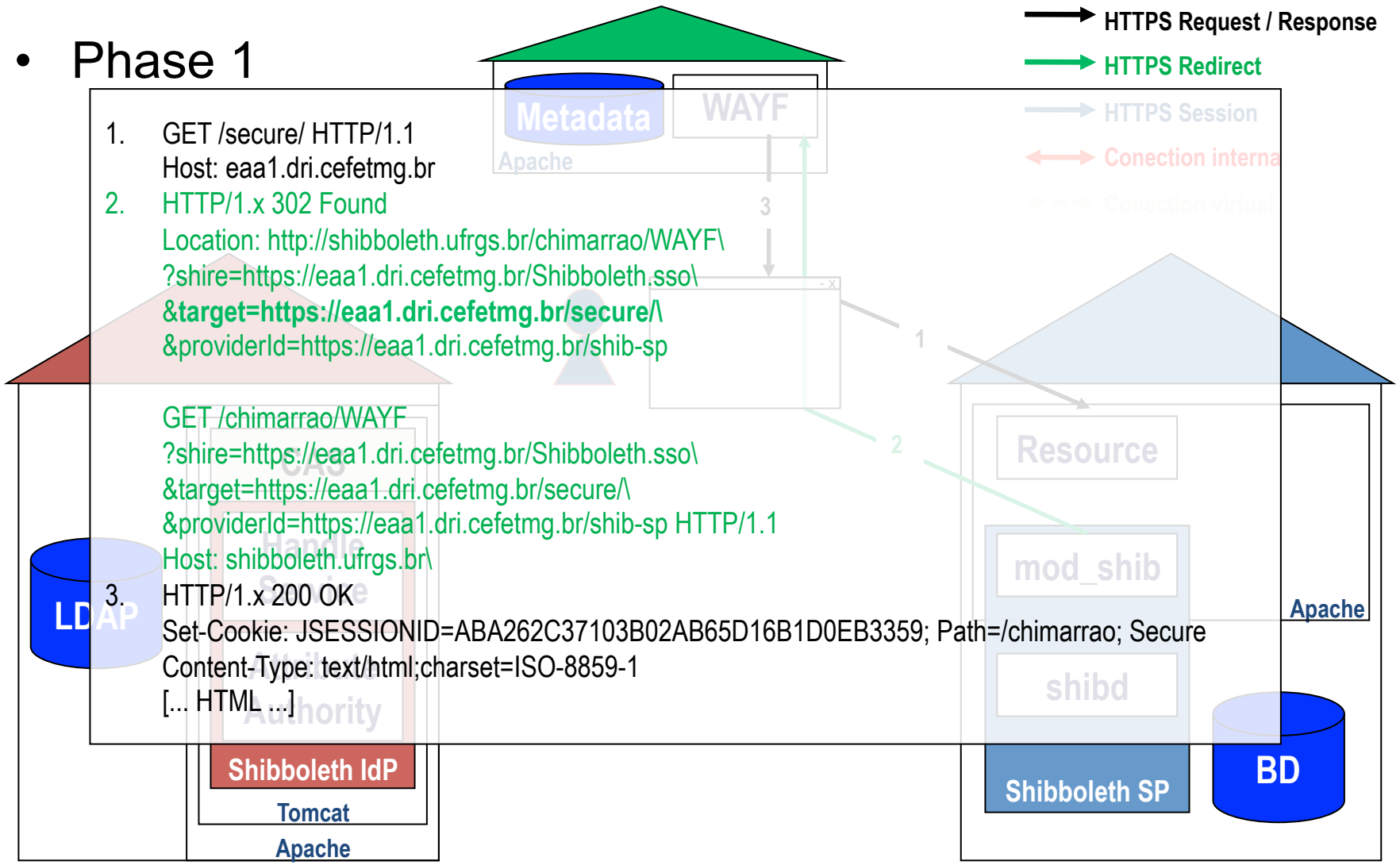


Figura 7.7

* Essa demonstração foi baseada no Expert Demo da SW

Identity Federation Operation

- Phase 1



Identity Federation Operation

Magic
Middleware for collaborative Applications and Global virtual Communities

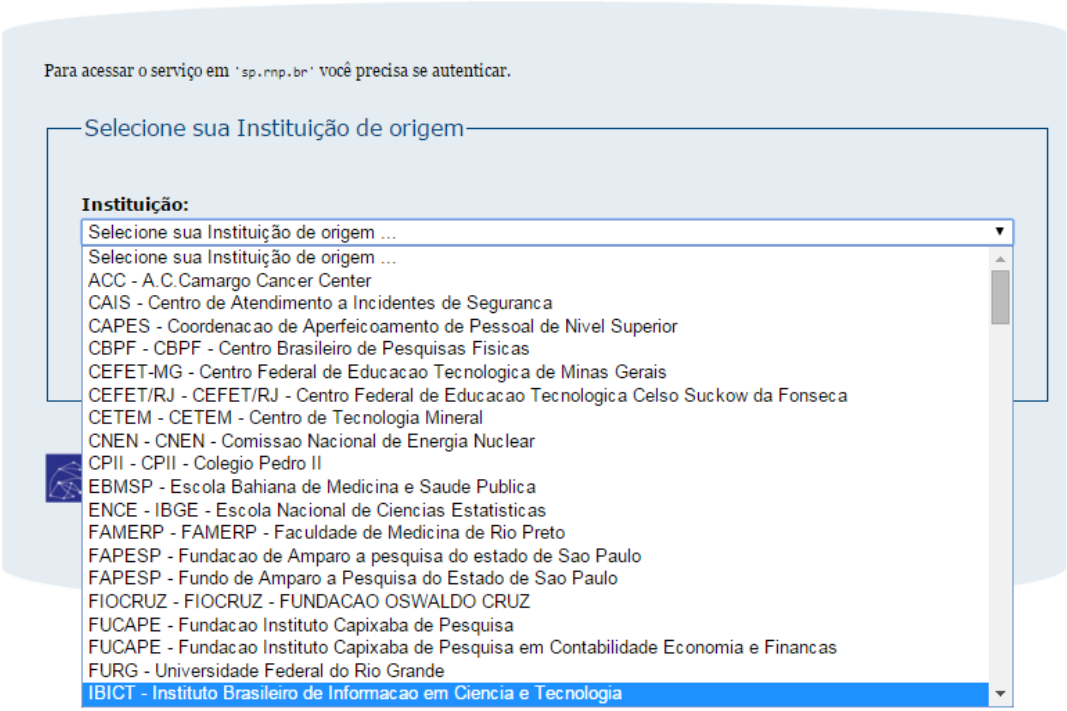
- Phase 2

Identity Federation Operation

Magic
Middleware for collaborative Applications and Global virtual Communities

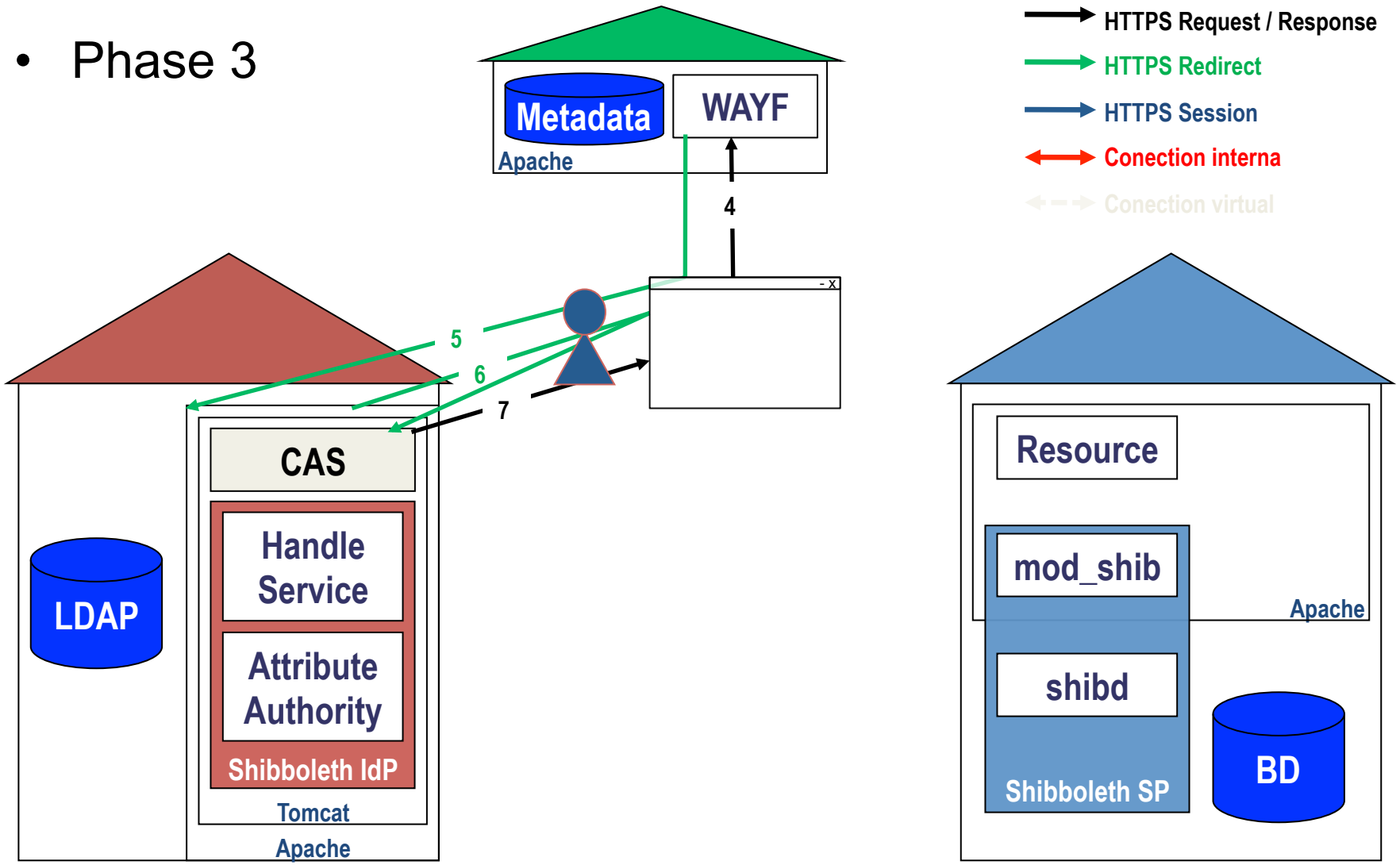
- Phase 2

Federação Chimarrão



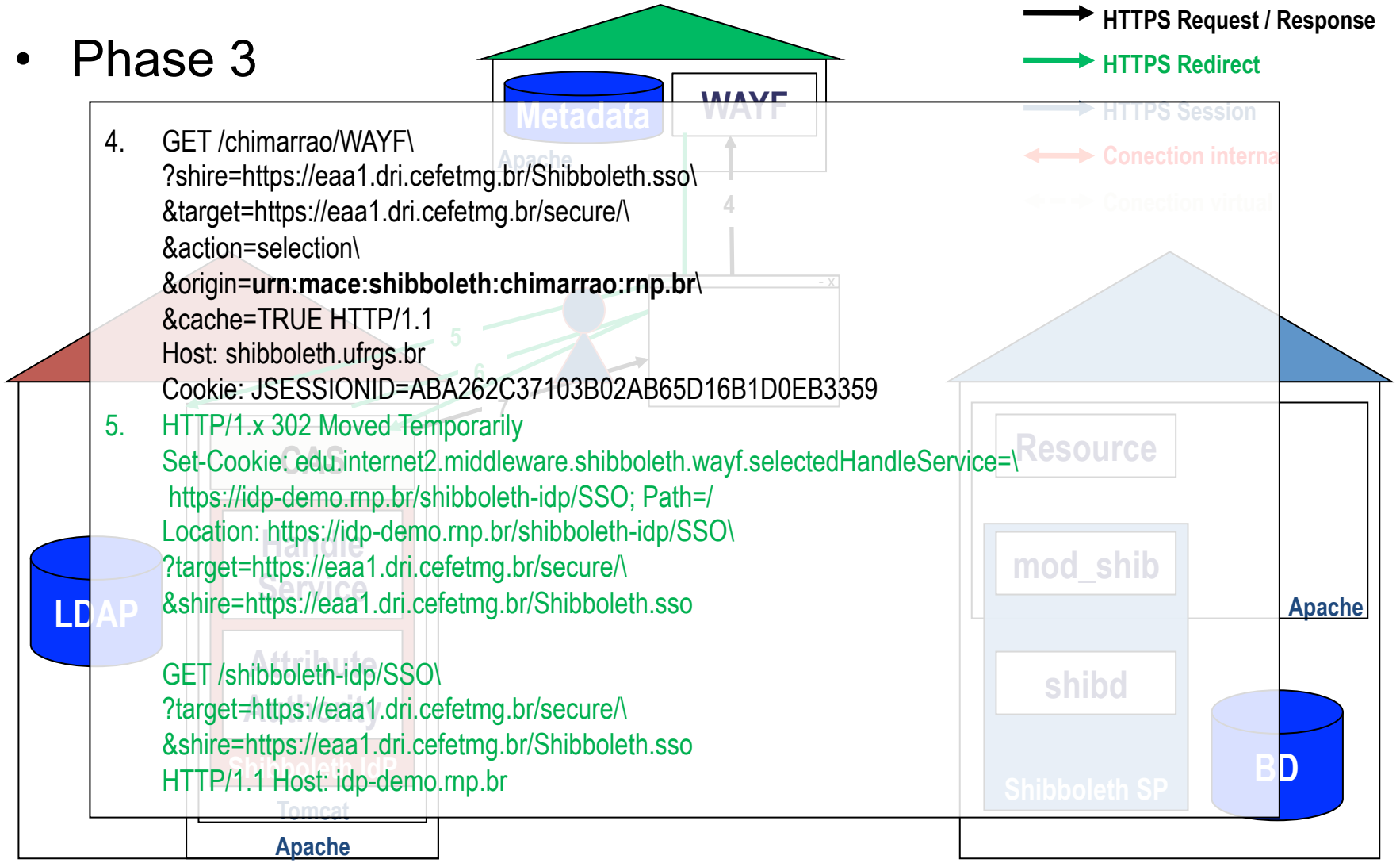
Identity Federation Operation

- Phase 3



Identity Federation Operation

- Phase 3



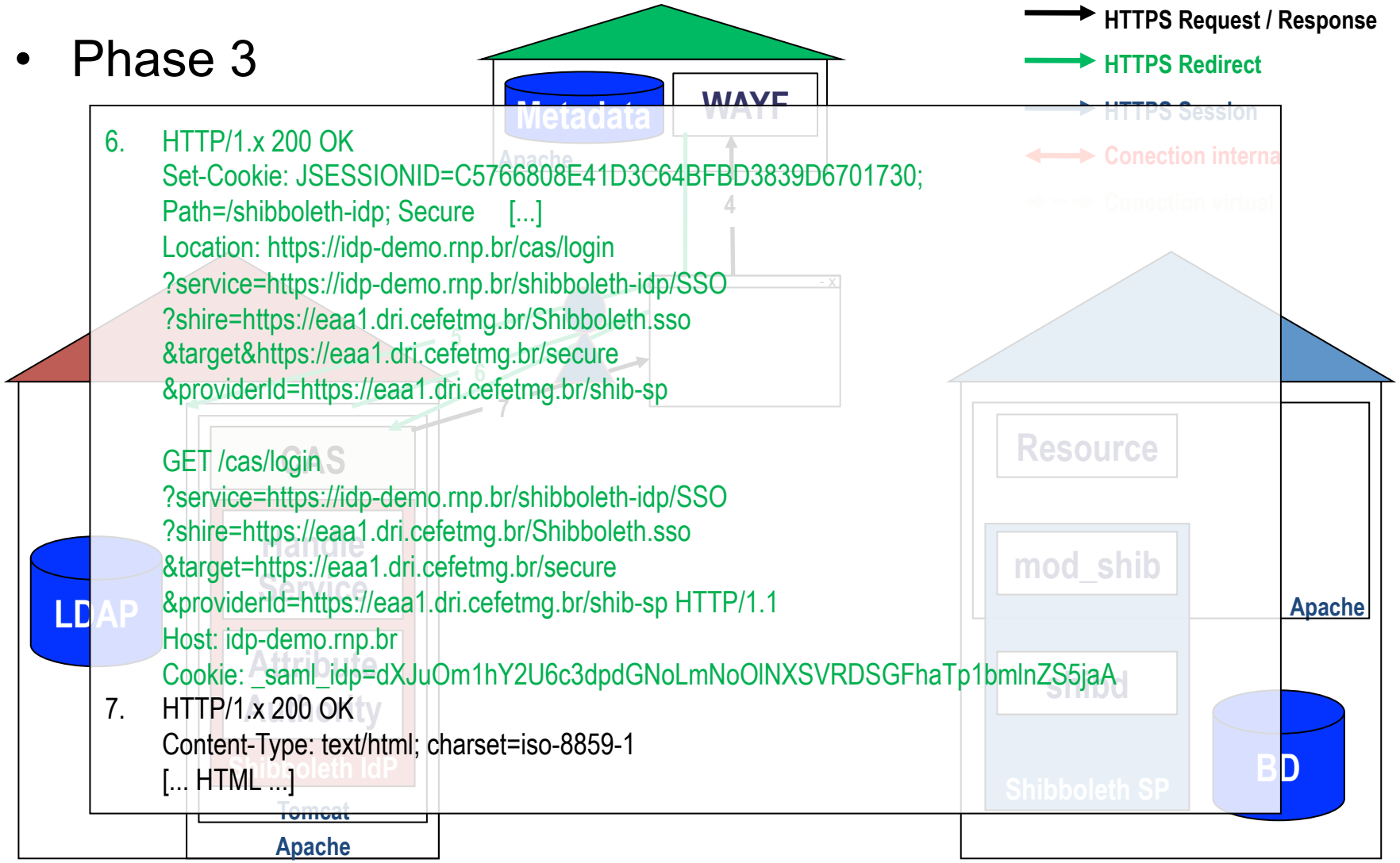
4. GET /chimarrao/WAYF\
?shire=https://eaa1.dri.cefetmg.br/Shibboleth.sso\
&target=https://eaa1.dri.cefetmg.br/secure/\
&action=selection\
&origin=**urn:mace:shibboleth:chimarrao:rnp.br**\
&cache=TRUE HTTP/1.1
Host: shibboleth.ufrgs.br
Cookie: JSESSIONID=ABA262C37103B02AB65D16B1D0EB3359

5. HTTP/1.x 302 Moved Temporarily
Set-Cookie: edu.internet2.middleware.shibboleth.wayf.selectedHandleService=\
https://idp-demo.rnp.br/shibboleth-idp/SSO; Path=/
Location: https://idp-demo.rnp.br/shibboleth-idp/SSO\
?target=https://eaa1.dri.cefetmg.br/secure/\
&shire=https://eaa1.dri.cefetmg.br/Shibboleth.sso

GET /shibboleth-idp/SSO\
?target=https://eaa1.dri.cefetmg.br/secure/\
&shire=https://eaa1.dri.cefetmg.br/Shibboleth.sso
HTTP/1.1 Host: idp-demo.rnp.br

Identity Federation Operation

- Phase 3

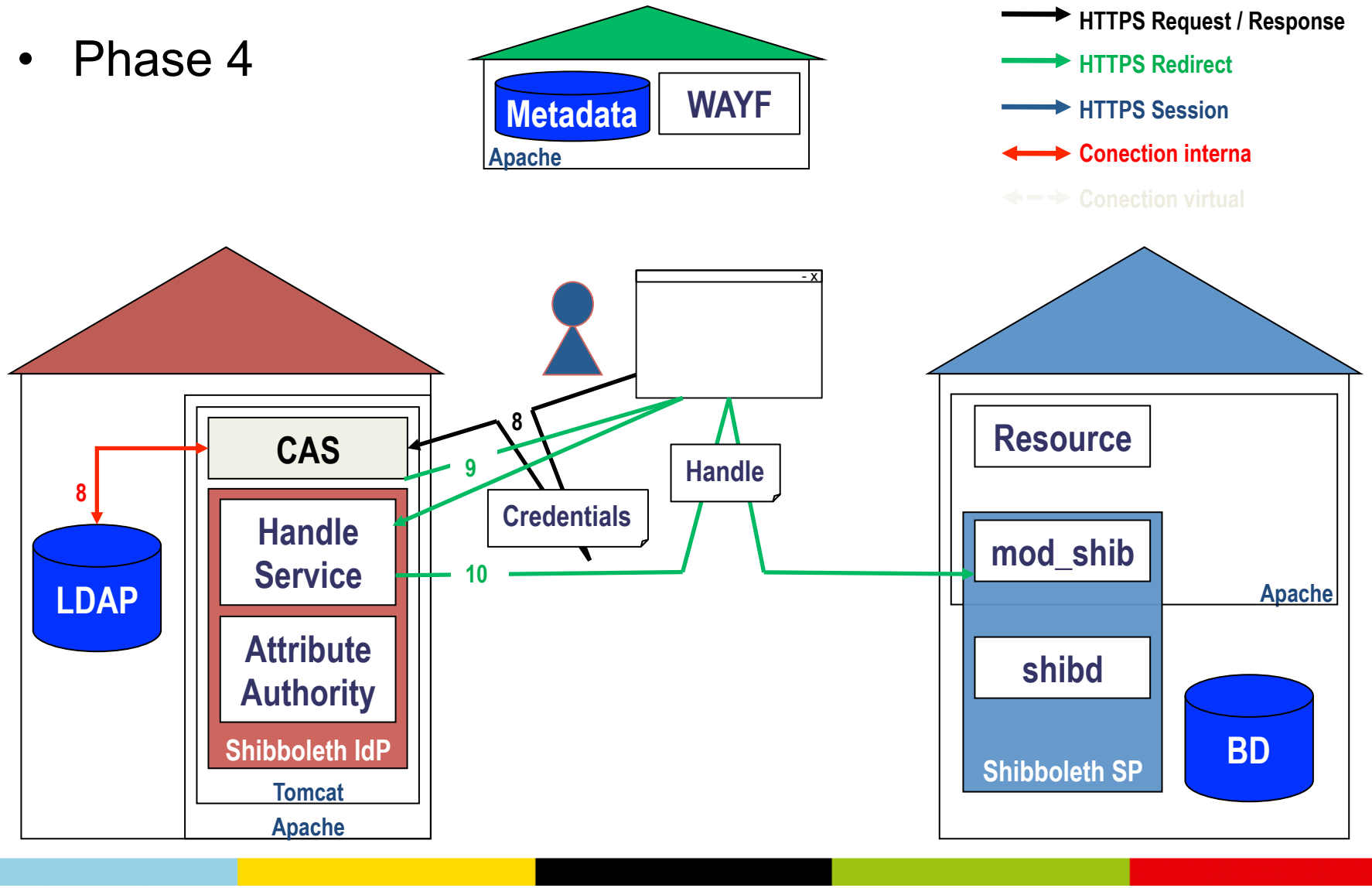


6. HTTP/1.x 200 OK
   Set-Cookie: JSESSIONID=C5766808E41D3C64BFBD3839D6701730;
   Path=/shibboleth-idp; Secure [...]
   Location: https://idp-demo.rnp.br/cas/login
   ?service=https://idp-demo.rnp.br/shibboleth-idp/SSO
   ?shire=https://eaa1.dri.cefetmg.br/Shibboleth.sso
   &target&https://eaa1.dri.cefetmg.br/secure
   &providerId=https://eaa1.dri.cefetmg.br/shib-sp

   GET /cas/login
   ?service=https://idp-demo.rnp.br/shibboleth-idp/SSO
   ?shire=https://eaa1.dri.cefetmg.br/Shibboleth.sso
   &target=https://eaa1.dri.cefetmg.br/secure
   &providerId=https://eaa1.dri.cefetmg.br/shib-sp HTTP/1.1
   Host: idp-demo.rnp.br
   Cookie: _saml_idp=dXJuOm1hY2U6c3dpdGNoLmNoOlNXSVRDSGFhaTp1bmlnZS5jaA
7. HTTP/1.x 200 OK
   Content-Type: text/html; charset=iso-8859-1
   [... HTML ...]

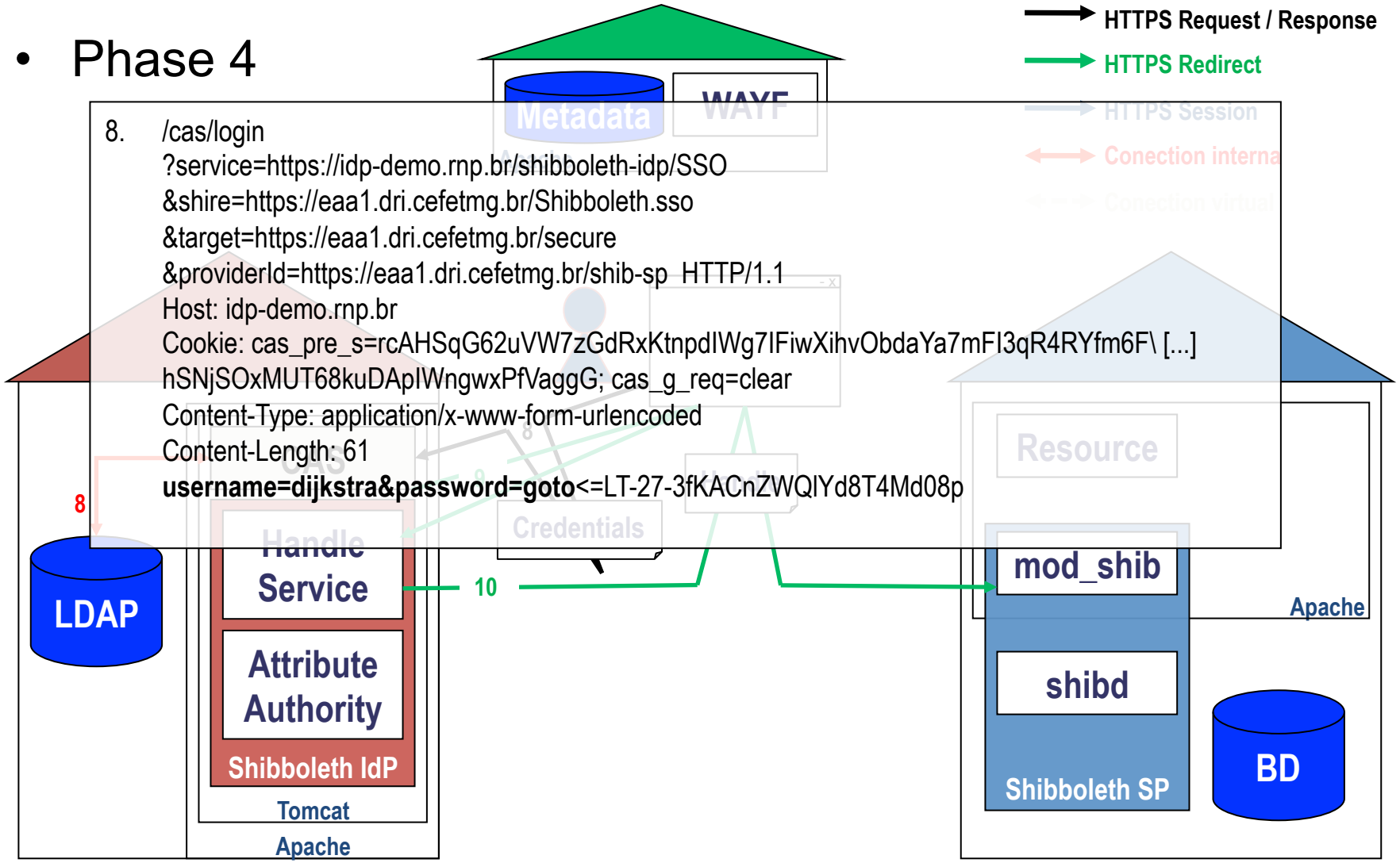
Identity Federation Operation

- Phase 4



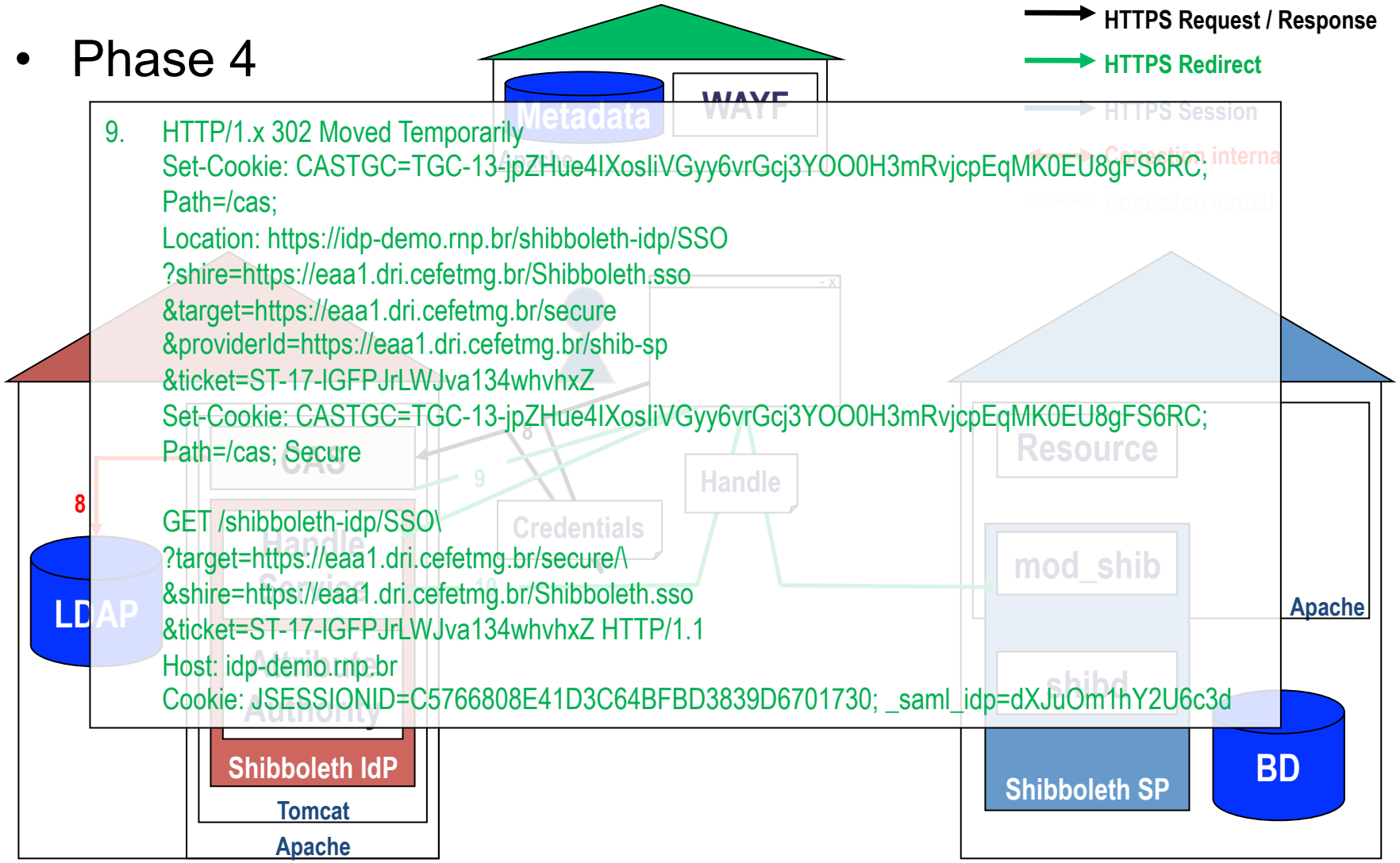
Identity Federation Operation

- Phase 4



Identity Federation Operation

- Phase 4



Identity Federation Operation

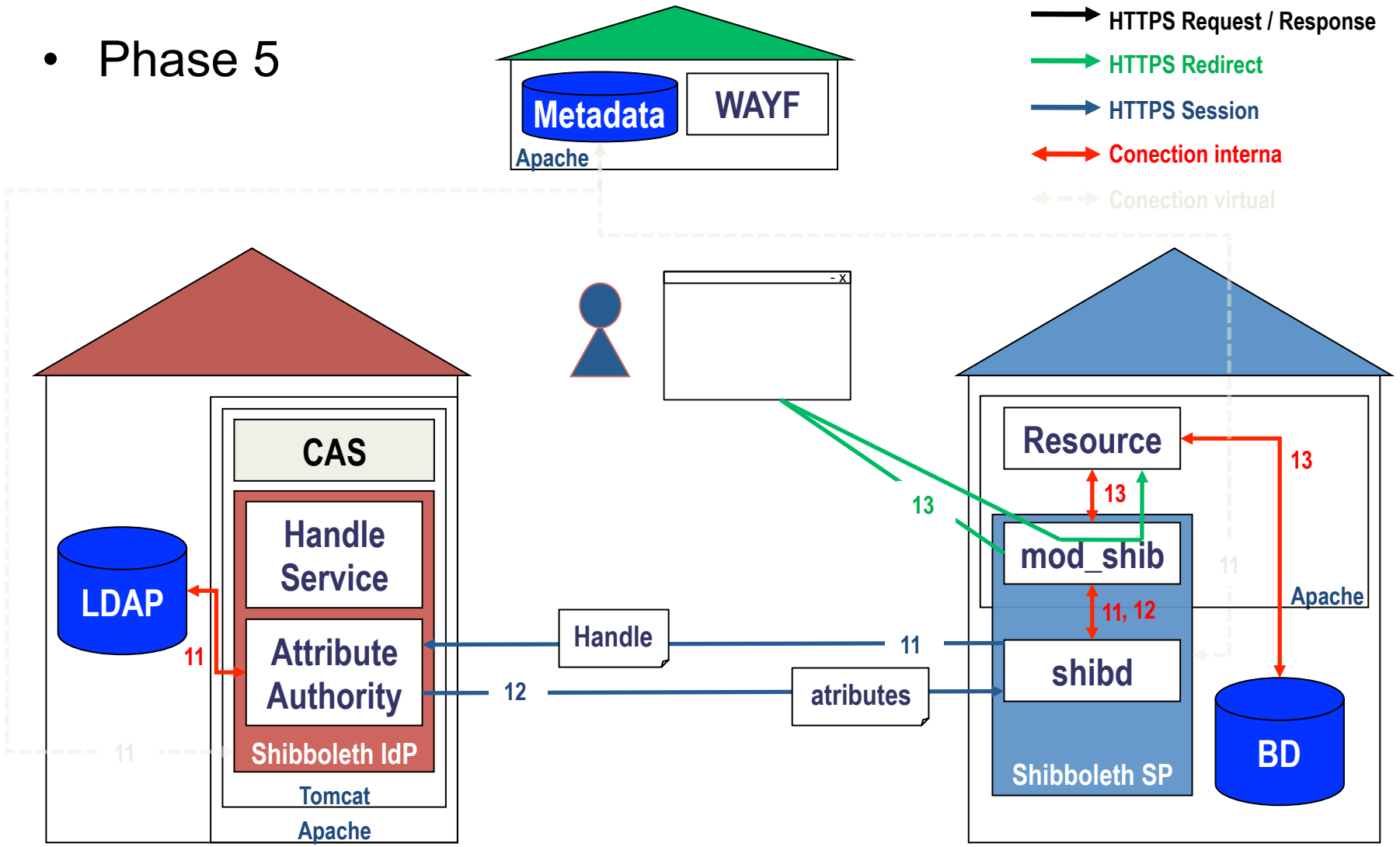
- Phase

10. HTTP/1.x 200 OK
Set-Cookie: cas_g=; domain=. rnp.br; path=/; expires=Fri,\
11-Jan-1990 00:00:01 GMT; secure
Set-Cookie: cas_pre_s=; path=/; expires=Fri, 11-Jan-1990 00:00:01 GMT; secure
Set-Cookie: cas_s__chimarrao_=C3kMOhoDCJrHivwK00FZP+8xhPFjyPVq3J8nlluLPO9\ [...] 5/xSuon/
ryauQAcKHz95IQQwe4l3eEvKRfVs; path=/; secure
Set-Cookie: JSESSIONID=4878F247EDBE5313C35397B5670413EF; Path=/chimarrao; Secure
Content-Type: text/html;charset=ISO-8859-1
[... HTML ...]
<form name="shib" action="https://eaa1.dri.cefetmg.br/Shibboleth.sso" method="POST">
<input type="hidden" name="TARGET" value="https://eaa1.dri.cefetmg.br/secure/">
<input type="hidden" name="SAMLResponse" value="PFJlc3BvbnNlIHhtbG5zPSJ1cm46\ [...]
QXNzZXJ0aW9uPjwvUmVzcG9uc2U+">
<noscript>
<input type="submit" value="Continue">
[... HTML ...]

POST /Shibboleth.sso HTTP/1.1
Host: eaa1.dri.cefetmg.br
Content-Type: application/x-www-form-urlencoded
Content-Length: 16859
TARGET=https://eaa1.dri.cefetmg.br/secure/\
&SAMLResponse=PFJlc3BvbnNlIHht\ [...] 0Pjwv%0D%0AQXNzZXJ0aW9uPjwvUmVzcG9uc2U%2B

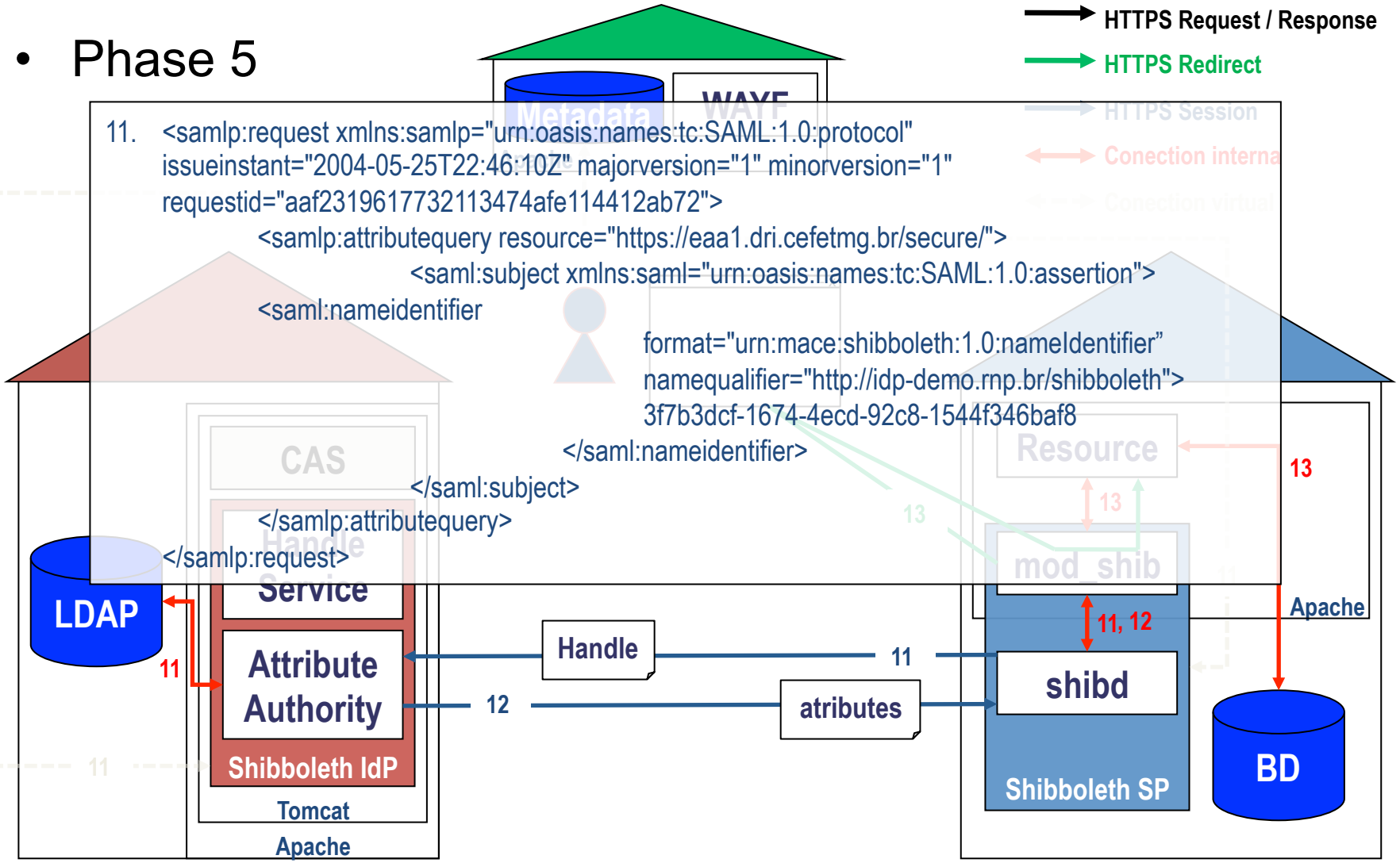
Identity Federation Operation

- Phase 5



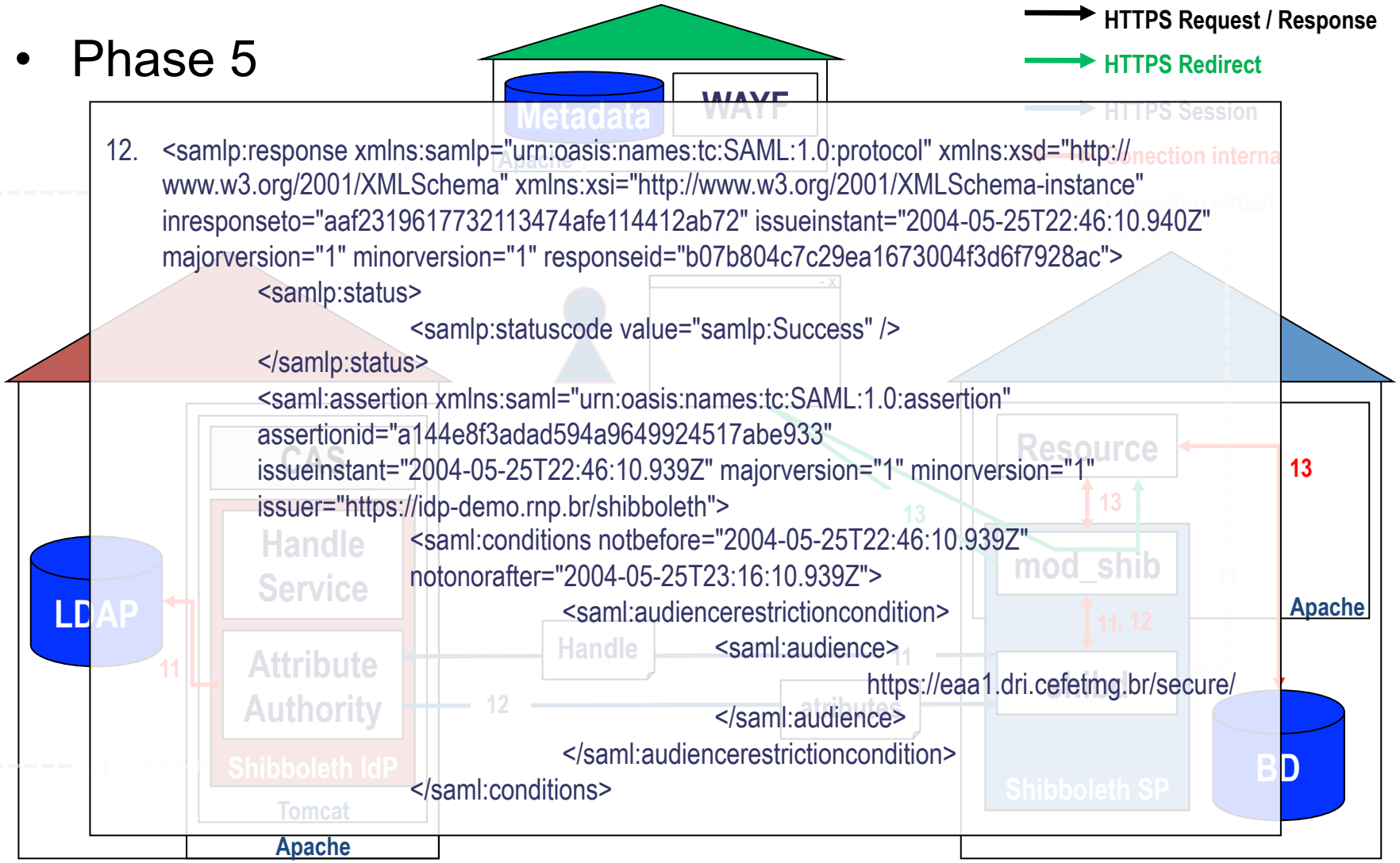
Identity Federation Operation

- Phase 5



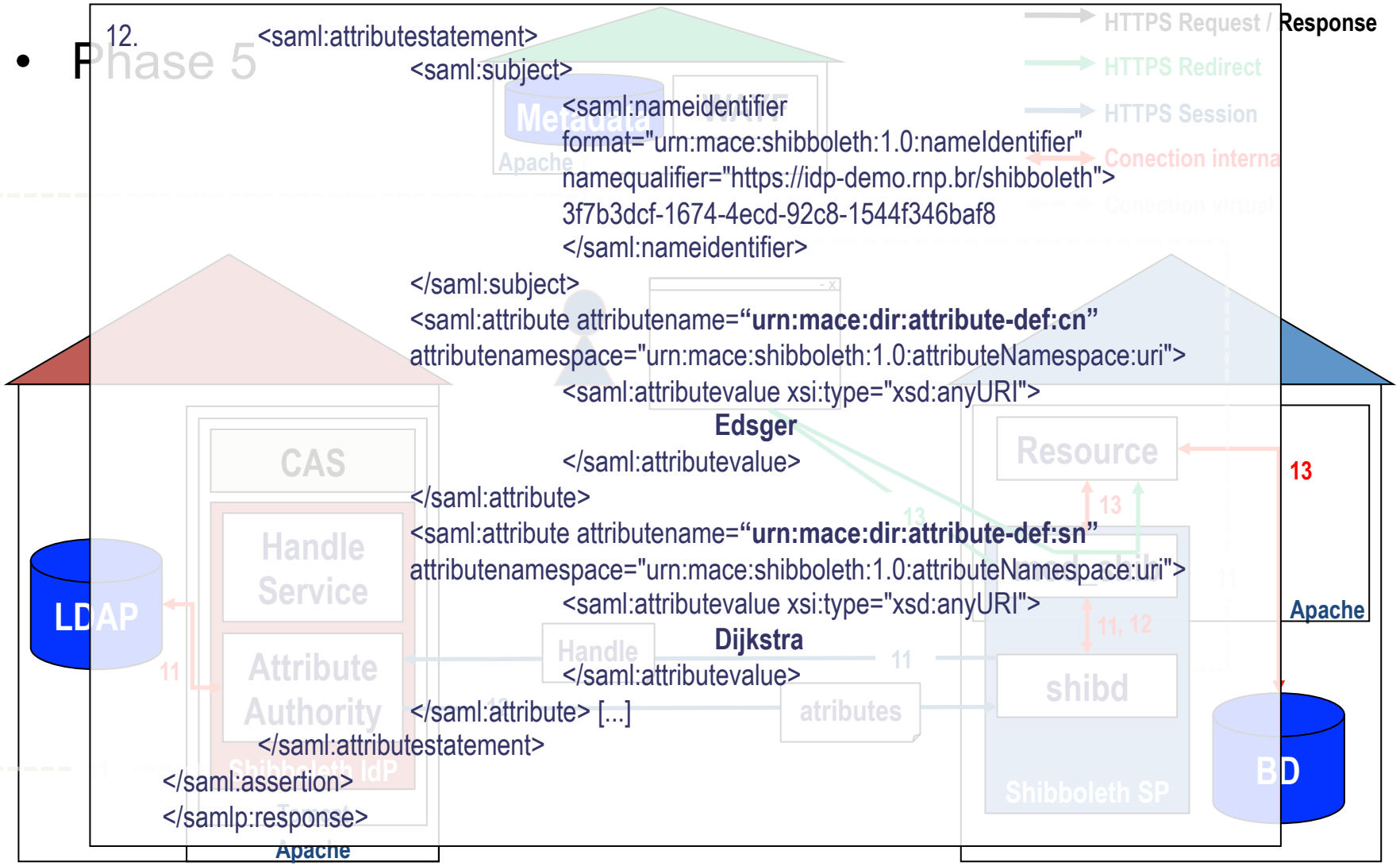
Identity Federation Operation

- Phase 5



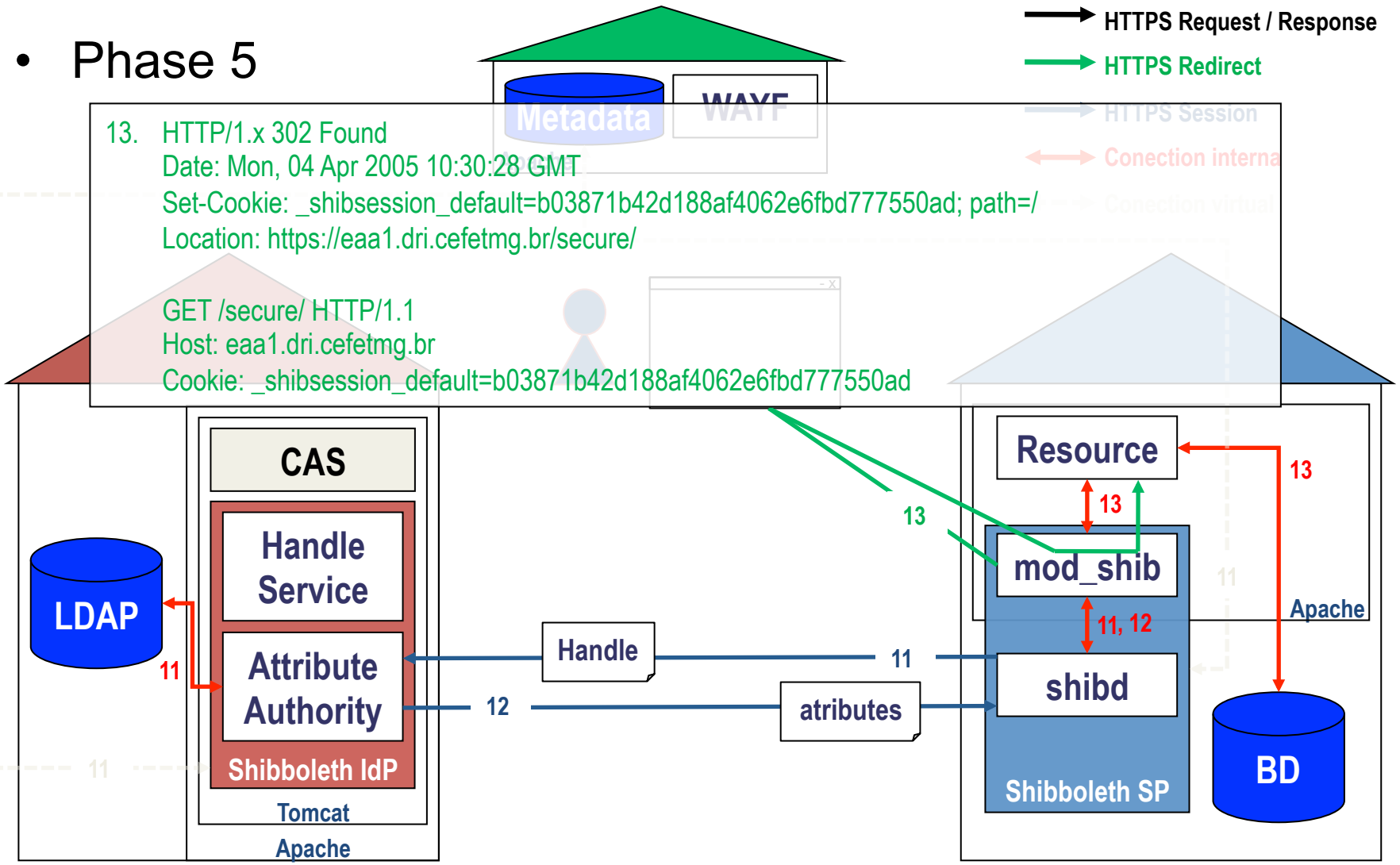
Identity Federation Operation

- Phase 5

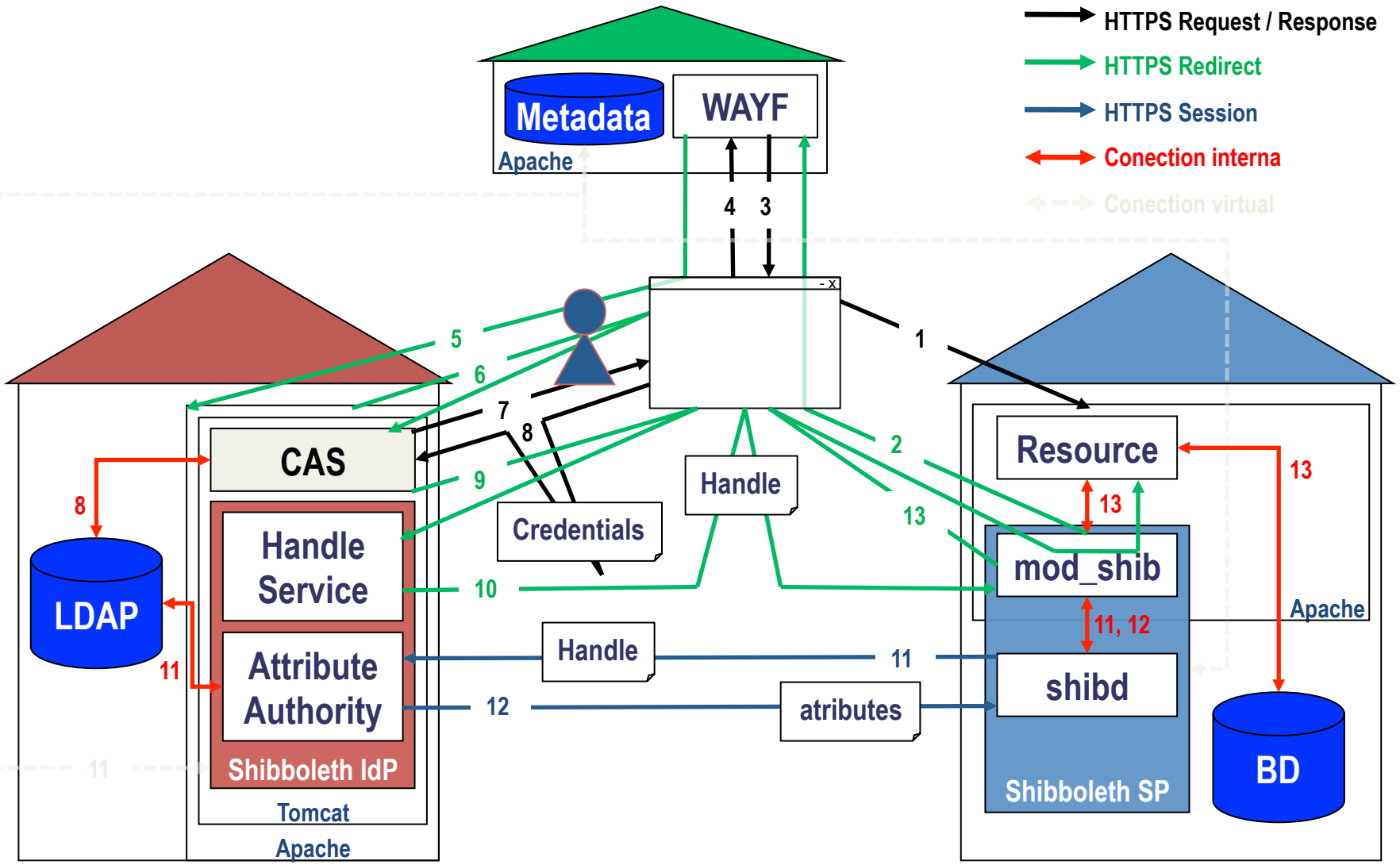


Identity Federation Operation

- Phase 5



Identity Federation Operation



Top setpoints

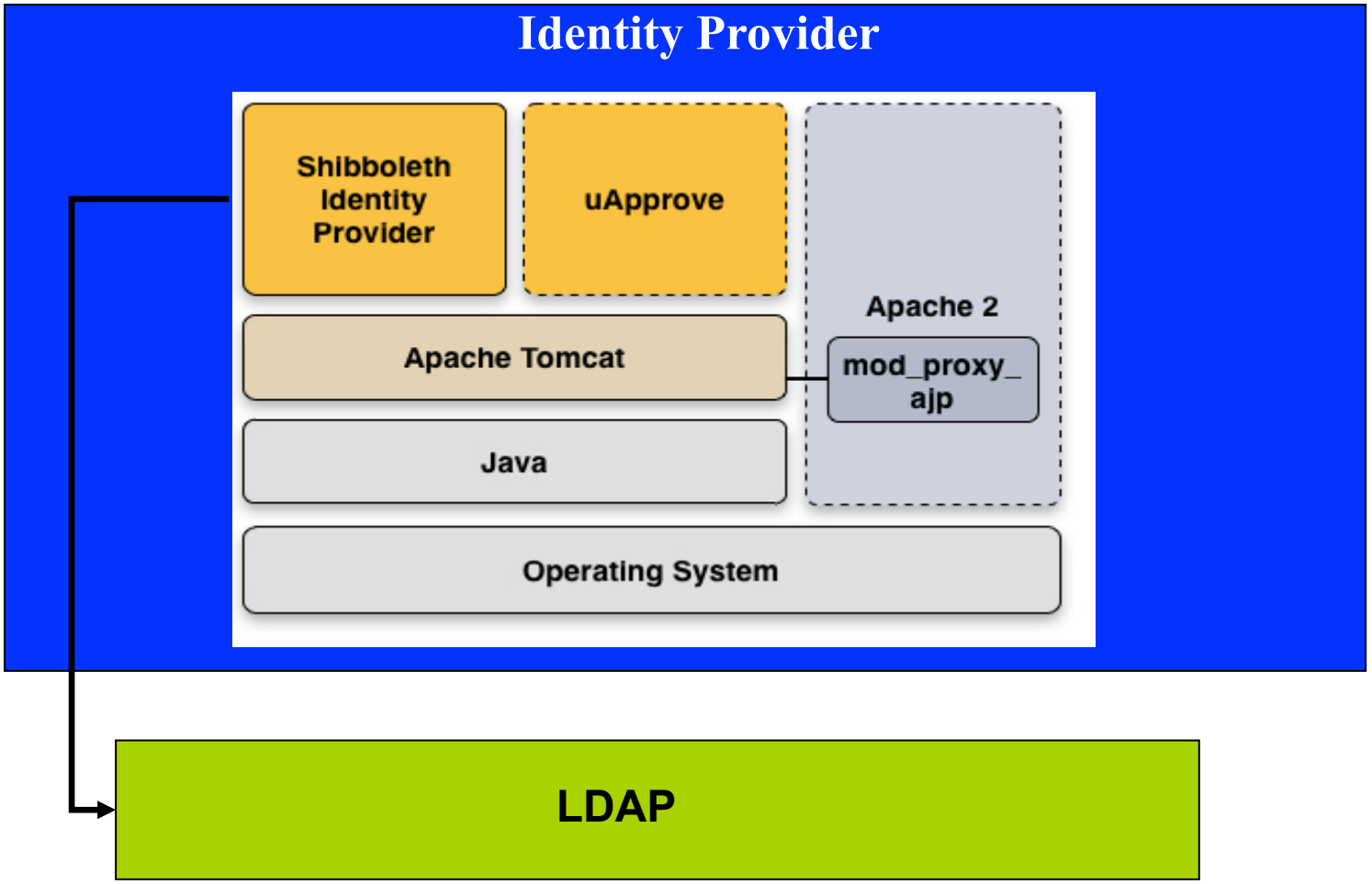


Figura 8.1

Apache Configuration

- Virtual Hosts
  - AA – Attribute Authority
    - Responsible for communication between the Attribute Authority and the Service Provider.
  - SSO – CAS e Handle Server
    - Responsible for communication between the user browser and the server and the CAS Handle.

Apache Configuration

- mod_ssl
  - Responsible for encrypting communication with the identity provider.
  - Certificate, Key and Certificate Authority
  - Mutual Authentication between AA and shibd
    - Requires shibd certificate and passtrhrough Shibboleth IdP
- mod_jk
  - Responsible for redirecting requests to Tomcat.

Tomcat Configuration

- Conector AJP 1.3
  - Apache Redirection
  - Disable other connectors
  - As a security measure, access to the Tomcat will not occur directly but through the Apache HTTP Server

Shibboleth IdP Configuration

- Identification and basic configuration of the Provider:
  - /opt/shibboleth-idp/conf/relying-party.xml
- Resolution of attributes:
  - /opt/shibboleth-idp/conf/attribute-resolver.xml
  - /opt/shibboleth-idp/conf/metadata-providers.xml
- Release of attributes:
  - /opt/shibboleth-idp/conf/attribute-filter.xml
- Authorized service providers of:
  - /opt/shibboleth-idp/metadata/<federation>-metadata.xml

Shibboleth IdP Configuration

- relying-party.xml
  - Provider identification in federation
  - Credentials: certificate and key
  - Attribute Authority URL
  - Protocol Handlers
  - Patch of others configuration files

Shibboleth IdP Configuration

- attribute-resolver.xml
  - Base atribute conectors for users (LDAP ou SQL)
    - DataConnectors
  - Atributes definitions
    - AttributeDefinition
  - Credentials of reader user of base attributes
- metadata-providers.xml
  - Set the metadata of IdP, addin elements (<MetadataProvider>) in *metadata-providers.xml* file

Shibboleth IdP Configuration

- attribute-filter.xml
  - release of rules attributes
    - Release of atributes by SP
    - Release of atributes by Federation
    - Release of all atributes without restriction

Shibboleth IdP Configuration

- metadata.xml
  - The metadata file is provided by federation and its function is to establish the relationship of trust between providers.
  - In this file are set to the identity provider, the relevant information about the providers of service (and vice versa).
    - Trust
      - Certificates
      - Public keys
    - Comunication
      - IDs
      - URLs
      - Protocols
  - In this way, we ensure the security and authenticity in communication between providers.
  - Relevant Informations about providers

Shibboleth IdP Configuration

- Shibboleth-IDP (Identity Provider)
  - Provides the atributes from a local database for the federation
  - Make the mapping of attributes and access control

- Data sources
  - LDAP base
  - Relational database
  - Text files
  - Custom connector (using Java)

Shibboleth IdP Configuration

- Scenario analysis
  - The purpose of the mapping is to match the federation requirements with existing atributes in LDAP base
  - Basic operations:
    - Rename each attribute
    - Change the attribute value
    - Change value of a atribute sequence

Shibboleth IdP Configuration

- Atributes asked by federation
  - Minimum set of recommended attributes by the federation CAFe to identify a user :
    - eduPersonPrincipalName
    - mail
    - cn
    - sn
    - brEduAffiliation
    - brEntranceDate
    - brExitDate

Shibboleth IdP Configuration

- Mapping definition

  - Rename attribute
    - uid => brEduAffiliationType
  - Change value of a attribute
    - uid + “@ufrgs.br” => mail
  - Change value of a attribute sequence
    - atrib=“01: aluno”, atrib=“02: bolsista” => aluno;bolsista

Quiz Time

Magic
Middleware for collaborative Applications and Global vIrtual Communities

Quiz Time

1. **Which of these modules is responsible for redirecting requests to Tomcat:**
   a) Mod_ssl
   b) Mod_shibd
   c) Mod_jk
   d) Mod_redirect

2. **What is the function of the metadata.xml file?**
   a) The metadata file function is to establish the relationship of trust between providers.
   b) The metadata file function is to establish the relationship of trust only between identity providers.
   c) The metadata file function is to establish the relationship of trust only between service providers.
   d) The metadata file function is to establish the relationship of trust between members of the federation.

Quiz Time

3. **What is the main goal of a identiy provider?**

4. **Which of the following is NOT a data source for an Identity Provider?**
   a) LDAP base
   b) Relational database
   c) Excel Files
   d) Text Files

5. **Which of the following is NOT a Shibboleth component?**
   a) Identity Provider (IdP)
   b) Service Provider (SP)
   c) Discovery Service / WAYF (Where Are You From?)
   d) Assertion