# Mettere insieme i pezzi

## Esempi di funzionamento e controllo degli accessi

Giacomo Tenaglia

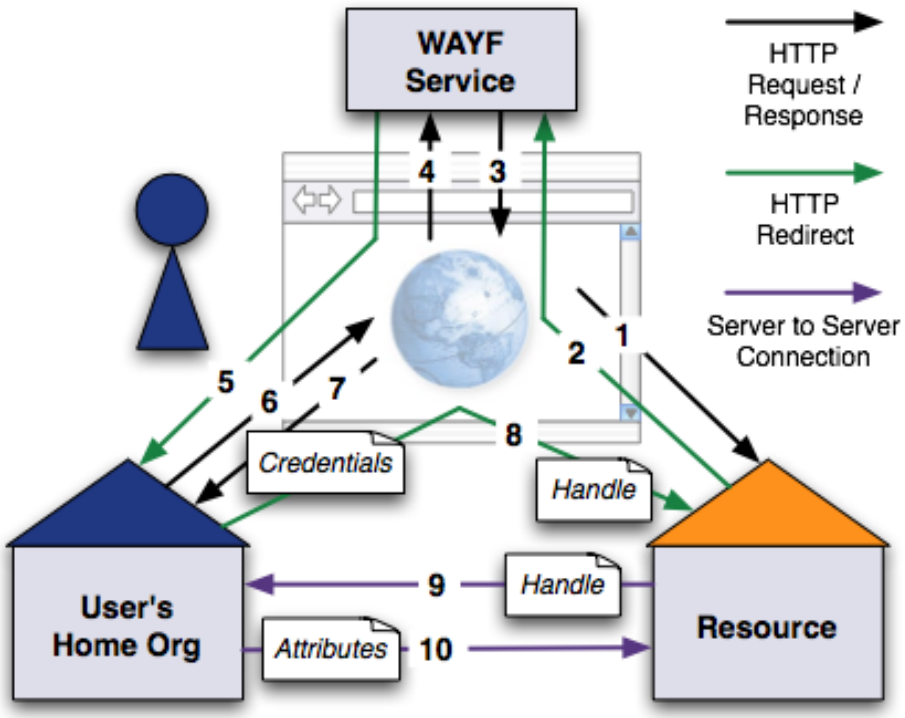
CNR Bologna

5 Marzo 2007

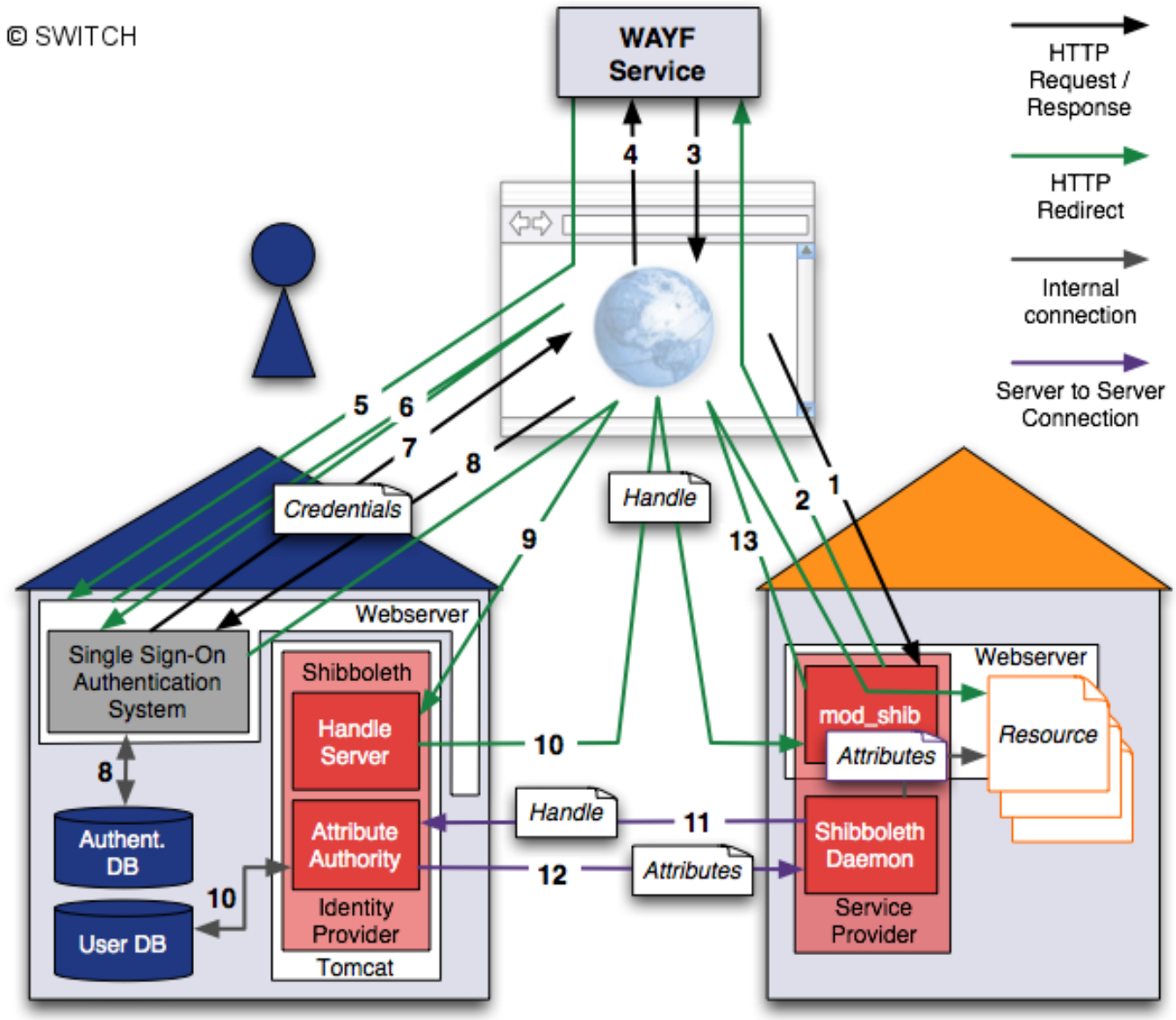
# Mettere insieme i pezzi

## Esempi di funzionamento e controllo degli accessi

# Punto della situazione (semplice)



# Punto della situazione (approfondito)



# Metadati della federazione

## Informazioni di base:

[ file:///etc/shibboleth/metadata.xml ]

```
<EntitiesDescriptor
    xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
    xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
    xsi:schemaLocation="urn:oasis:names:tc:SAML:2.0:metadata ../schemas/saml-schema-metadata-2.0.x
    Name="urn:mace:test.shib:federation"
    validUntil="2010-01-01T00:00:00Z">

    <Extensions>
        <shibmd:KeyAuthority>
            <ds:KeyInfo>
                <ds:X509Data>
                    <ds:X509Certificate>MIIDnDCCAwWgAwIBAgIJAIRfHySYxlFvMA0GCSqGSIb3DQEBBAUAMIGRMQ
VQQKEwNDTlIxEDAOBgNVBAsTB1Rlc3QgQ0ExKTAnBgkqhkiG9w0BCQEWGmdpYWNv
....
                    </ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </shibmd:KeyAuthority>
    </Extensions>
```

# Metadati della federazione (2)

## Dati dell'Identity Provider:

[ file:///etc/shibboleth/metadata.xml ]

```
<EntityDescriptor entityID="https://idp.test.shib/shibboleth">

    <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol urn:mace:sh
        <Extensions>
        <shibmd:Scope>idp.test.shib</shibmd:Scope>
        </Extensions>

        <KeyDescriptor use="signing">
            <ds:KeyInfo>
            <ds:KeyName>idp.test.shib</ds:KeyName>
            </ds:KeyInfo>
        </KeyDescriptor>

        <ArtifactResolutionService index="1"
            Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"
            Location="https://idp.test.shib/shibboleth-idp/Artifact"/>

        <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>

        <SingleSignOnService Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest"
            Location="https://idp.test.shib/shibboleth-idp/SSO"/>
    </IDPSSODescriptor>
```

# Metadati della federazione (3)

## Dati dell'Identity Provider (2):

[ file:///etc/shibboleth/metadata.xml ]

```
    <AttributeAuthorityDescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol
        <Extensions>
        <shibmd:Scope>idp.test.shib</shibmd:Scope>
        </Extensions>

        <AttributeService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"
            Location="https://idp.test.shib:8443/shibboleth-idp/AA"/>

        <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
    </AttributeAuthorityDescriptor>

    <Organization>
        <OrganizationName xml:lang="en">Test Shibboleth</OrganizationName>
        <OrganizationDisplayName xml:lang="en">Test Shibboleth</OrganizationDisplayName>
        <OrganizationURL xml:lang="en">http://www.test.shib/</OrganizationURL>
    </Organization>
    <ContactPerson contactType="technical">
        <SurName>Technical Support</SurName>
        <EmailAddress>giacomo.tenaglia@area.bo.cnr.it</EmailAddress>
    </ContactPerson>

</EntityDescriptor>
```

# Metadati della federazione (4)

## Dati del Service Provider:

[ file:///etc/shibboleth/metadata.xml ]

```
<EntityDescriptor entityID="https://sp.test.shib/sp">
    <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol">

        <KeyDescriptor>
            <ds:KeyInfo>
            <ds:KeyName>sp.test.shib</ds:KeyName>
            </ds:KeyInfo>
        </KeyDescriptor>

        <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>

        <AssertionConsumerService index="1"
            Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post"
            Location="https://sp.test.shib/Shibboleth.sso/SAML/POST"/>
        <AssertionConsumerService index="2"
            Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01"
            Location="https://sp.test.shib/Shibboleth.sso/SAML/Artifact"/>

    </SPSSODescriptor>

</EntityDescriptor>
```

# Modifica configurazioni

## Configurazione Identity Provider:

[ file:///usr/local/shibboleth-idp/idp.xml ]

```
<MetadataProvider type="edu.internet2.middleware.shibboleth.metadata.provider.XMLMetadata"
    uri="file:/usr/local/shibboleth-idp/etc/metadata-1.xml"/>
```

## Configurazione Service Provider:

[ file:///etc/shibboleth/shibboleth.xml ]

```
<MetadataProvider type="edu.internet2.middleware.shibboleth.metadata.provider.XMLMetadata"
    uri="/etc/shibboleth/metadata-1.xml"/>
```

# Esempio: protezione directory (1 IdP, 1 SP)

- `https://sp.test.shib/secure/`

# Aggiunta di un SP

## Modifica metadati della federazione:

[ file:///etc/shibboleth/metadata.xml ]

```
<EntityDescriptor entityID="https://sp2.test.shib/sp">
    <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol">

        <KeyDescriptor>
            <ds:KeyInfo>
            <ds:KeyName>sp2.test.shib</ds:KeyName>
            </ds:KeyInfo>
        </KeyDescriptor>

        <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>

        <AssertionConsumerService index="1"
            Binding="urn:oasis:names:tc:SAML:1.0:profiles:browser-post"
            Location="https://sp2.test.shib/Shibboleth.sso/SAML/POST"/>
        <AssertionConsumerService index="2"
            Binding="urn:oasis:names:tc:SAML:1.0:profiles:artifact-01"
            Location="https://sp2.test.shib/Shibboleth.sso/SAML/Artifact"/>

    </SPSSODescriptor>

</EntityDescriptor>
```

## Modifica configurazioni IdP e SP (banale).

# Aggiunta di un IdP

## Modifica metadati della federazione:

[ file:///etc/shibboleth/metadata.xml ]

`vedi slide precedenti.`

## Modifica configurazioni IdP e SP (banale).

# Esempio: protezione directory (2 IdP, 2 SP)

- `https://sp2.test.shib/secure-sp2/`
- `https://sp.test.shib/secure/`

# Uso degli attributi

- Incapsulati in header HTTP: `HTTP_$NOME_IN_AAP`
- `https://sp2.test.shib/secure-sp2/shibenv.php`
- Validità limitata all'interno della Location protetta.

# Protezione fine: lazy sessions

- L'applicazione decide quando stabilire la sessione Shibboleth.
- `ShibRequireSession` settato a `false` (in Apache).
- L'applicazione deve conscere:
  - `handlerURL`: URL dell'handler associato all'applicazione.
  - `location`: il SessionInitiator che si intende utilizzare.
  - `target`: URL dell'applicazione al quale tornare.
- Utile per affiancare o sostituire sistemi di autenticazione esistenti.
- `https://sp2.test.shib/lazy`

# Riferimenti

- Shib-users ML:
  `https://mail.internet2.edu/wws/arc/shibboleth-users`
- Shibboleth Attribute Release Policy Editor:
  `http://federation.org.au/ShARPE`
- “Non funziona!”:
  `mailto:giacomo.tenaglia@area.bo.cnr.it`