

The slide features a header with the Consortium GARR logo on the left, the text "Roma, 2-3 dicembre 2010" and "Ministero dell'Istruzione, dell'Università e della Ricerca" in the center, and the "idem day" logo on the right. The main title "uApprove e Consent: due strumenti per il consenso informato" is displayed in green. A red grid logo is positioned on the left side of the slide. The names "Virginia Calabritto - Ilaria De Marinis" and "CASPUR" are listed in red text. The footer contains the email addresses "Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it" and the number "2".

Consortium
GARR

Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca

idem
day

uApprove e Consent: due strumenti
per il consenso informato



Virginia Calabritto - Ilaria De Marinis CASPUR

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it 2



The slide features a header with logos for Consortium GARR, the event location and date (Roma, 2-3 dicembre 2010), the organizing ministry (Ministero dell'istruzione, dell'Università e della Ricerca), and the 'idem day' logo. The main title 'Agenda' is centered in green. A bulleted list of four items is presented in green text. The footer contains contact email addresses and a page number '3'. A faint background illustration shows a hand holding a pen over a document with a smiley face above it.

Consortium
GARR

Roma, 2-3 dicembre 2010
Ministero dell'istruzione, dell'Università e della Ricerca

idem
day

Agenda

- Introduzione
- Punto di vista dell'utente
- Funzionalità a confronto
- Installazione e configurazione

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it

3



Consortium
GARR

Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca



idem
day

Problema

- I servizi di Identity Management gestiscono le identità e hanno accesso a dati personali
- I servizi di Identity Management scambiano dati con Risorse del medesimo gestore o di altri gestori
- Sono in vigore delle direttive Comunitarie e leggi nazionali, sul “trattamento dei dati personali”, che siamo tenuti a rispettare

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it

4

Per esempio:

Il soggetto cui si riferiscono i dati ha il diritto di accesso alle informazioni, che lo riguardano, da altri detenute e tale diritto comprende la facoltà di richiedere: quali dati vengono trattati;

come e con quali fini avviene il trattamento;

l'autore del trattamento;

i soggetti a cui detti dati possono essere comunicati;

che i dati i detenuti corrispondano al vero e quindi pretenderne l'aggiornamento o la cancellazione.

Risposta

- **Degli strumenti che**
 - mostrano agli **utenti** gli attributi rilasciati dal gestore di Identità
 - raccolgono, dagli **utenti**, il consenso al trasferimento dei loro dati ai gestori delle risorse
 - per i **gestori dei servizi** di Identità, tengono traccia degli attributi rilasciati e delle risorse accedute

Consortium GARR

Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca

idem day

Quali?

- uApprove (Shibboleth)
- Consent & Consent Administration (simpleSAMLphp)

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it

6

SimpleSAMLphp è un'applicazione scritta in PHP per gestire l'autenticazione. Il progetto è guidato da UNINETT (la National Research & Education Network Norvegese - <http://uninett.no/>).

Lo scopo principale di SimpleSAMLphp è fornire supporto per:

- * SAML 2.0 Service Provider.
- * SAML 2.0 Identity Provider.

Consortium
GARR

Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca

idem
day

Vantaggi

- Aiutano ad implementare/rafforzare la protezione della privacy dei dati e la verificabilità dei dati
- Dando il controllo del rilascio degli attributi all'utente, migliorano il gradimento che questo ha del sistema
- Consentono di rendere i nostri sistemi rispondenti alla legge dell'identità di Kim Cameron:

User Control and Consent: *"Technical identity systems must only reveal information identifying a user with the user's consent."*

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it 7

Al II convegno IDEM l'avv. Andrea MONTI nel suo intervento

"Identità, identificazione e privacy. Tre atomi o una molecola?"

(http://helix940.rm.cnr.it/ramgen/GARR/IDEM/Convegno_02/05_Monti.rm) ci insegna che la "legge sul Corretto trattamento di dati personali" L. 193/03, più nota come "legge sulla Privacy") si basa 3 principi:

- "need to know"
- attendibilità
- disponibilità

I dati devono essere corretti e disponibili per verifiche all'interessato

uApprove

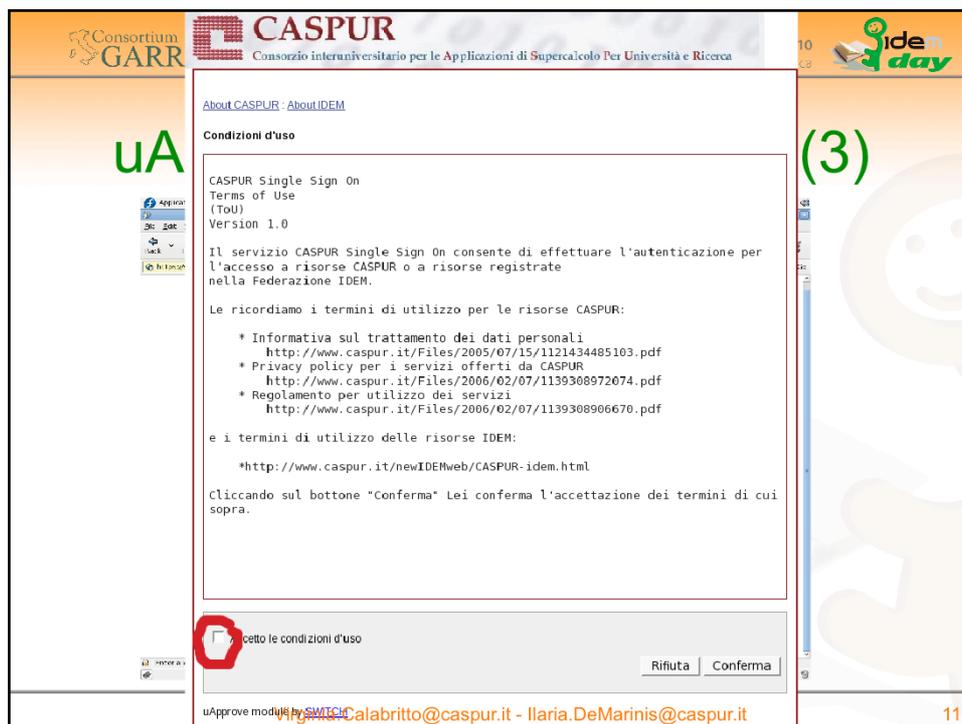
- Plug-in per Shibboleth Identity Provider, sviluppata in java, da Switch
- Gestisce i termini d'utilizzo del "Servizio di Identità" ed il relativo versioning
- Mostra la "Digital ID Card" con gli attributi da trasferire e richiede il consenso al loro trasferimento
- Gestisce il consenso globale
- Permette di azzerare il consenso dato

Consortium GARR Roma, 2-3 dicembre 2010 Ministero dell'Istruzione, dell'Università e della Ricerca **iden day**

uApprove: come funziona (2)

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it 10

2 – l'utente si autentica presso il Servizio di gestione delle Identità della propria organizzazione



3 – se il gestore del servizio di Identità abilita l'uso dei termini di utilizzo del servizio (ToU, Terms Of Use), l'utente, per poter proseguire è obbligato ad accettare I ToU

The screenshot shows a web page for uApprove. At the top, there are logos for Consortium GARR, Roma (2-3 dicembre 2010), Ministero dell'istruzione, dell'Università e della Ricerca, and idem day. The main heading is "uApprove: come funziona (4)". Below it is the CASPUR logo and the text "Consorzio interuniversitario per le Applicazioni di Supercalcolo Per Università e Ricerca".

There are two links: "About CASPUR" and "About IDEM". The text says: "Questa è la tua Carta di identità digitale da inviare a 'aai.caspur.it':".

Digital ID Card	
email	virgi2@caspur.it
eduPersonPrincipalName	virgi2@caspur.it
eduPersonScopedAffiliation	staff@caspur.it

Below the table is a checkbox with the text: "Non mostrarmi più questa pagina. Sono d'accordo che in futuro la mia Carta d'identità digitale (che potrebbe contenere alcuni attributi in più di quelli mostrati qui sopra) sarà inviata automaticamente." There are "Annulla" and "Conferma" buttons.

At the bottom, it says "uApprove module by SWITCH" and "Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it" with the page number "12".

4 – all'utente viene mostrata la scheda (digital Id Card) con tutti gli attributi, che devono essere passati alla risorsa affinché questa possa autorizzare l'accesso, e gli viene richiesto di dare il suo consenso al trasferimento. Se il gestore del servizio di identità abilita la gestione del consenso globale, all'utente viene data anche la possibilità di impostare un checkbox per rilasciare il consenso una volta per tutte

Consortium GARR

Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca

idem day

uApprove: come funziona (6)

CASPUR
Consorzio Interuniversitario per le Applicazioni di Ricerca Per Università e Ricerca

CASPUR Identity Provider Login to Service Provider https://sai.caspur.it/shibboleth

Username:

Password:

Login

Reset my attribute release approvals

Single Signon

Shibboleth

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it 14

6 – se l'utente vuole revisionare e/o revocare il consenso, precedentemente dato al trasferimento dei suoi attributi alla risorsa, al momento dell'autenticazione deve impostare il quadratino “Reset my attribute release approvals”

The image is a screenshot of a presentation slide titled "uApprove: come funziona (7)". At the top left, it shows the Consortium GARR logo. At the top right, it says "Roma, 2-3 dicembre 2010" and "Ministero dell'Istruzione, dell'Università e della Ricerca" next to the "idem day" logo. The main content area features the CASPUR logo (Consorzio interuniversitario per le Applicazioni di Supercalcolo Per Università e Ricerca) and a dialog box with the text: "Cancella le mie preferenze di login: Questo comporterà il mostrarmi la mia Carta di identità digitale ogni volta che accedo a una risorsa web per la prima volta." Below this text are "Annulla" and "Conferma" buttons. A link "uApprove module by SWITCH" is also visible. The slide footer contains the email addresses "Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it" and the number "15".

7 – a questo punto gli verrà chiesto di confermare la cancellazione del suo precedente consenso (verranno rimossi tutti i consensi già rilasciati per risorse diverse)

Consortium GARR Roma, 2-3 dicembre 2010 Ministero dell'Istruzione, dell'Università e della Ricerca idem day

Consent & Consent administration

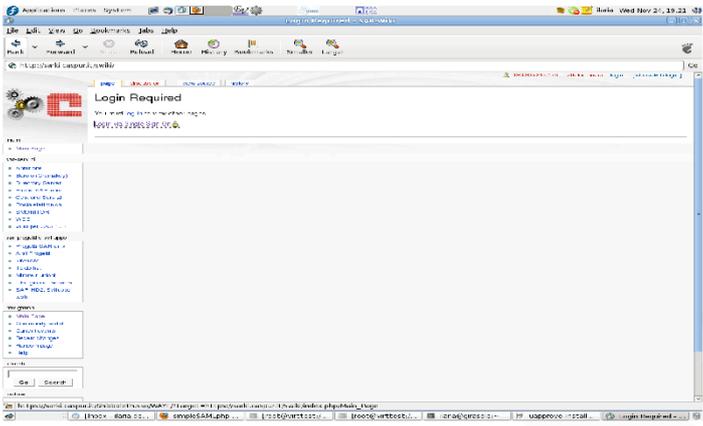
- Consent è un modulo integrato di simpleSAMLphp
- Mostra la scheda degli attributi rilasciati, richiedendo il consenso al trasferimento
- Consent administration è un'applicazione sviluppata da WAYF.dk, implementa un servizio separato
- Permette la gestione selettiva dei consensi rilasciati

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it 16

WAYF è la Federazione danese di identità elettroniche (<https://www.wayf.dk>)

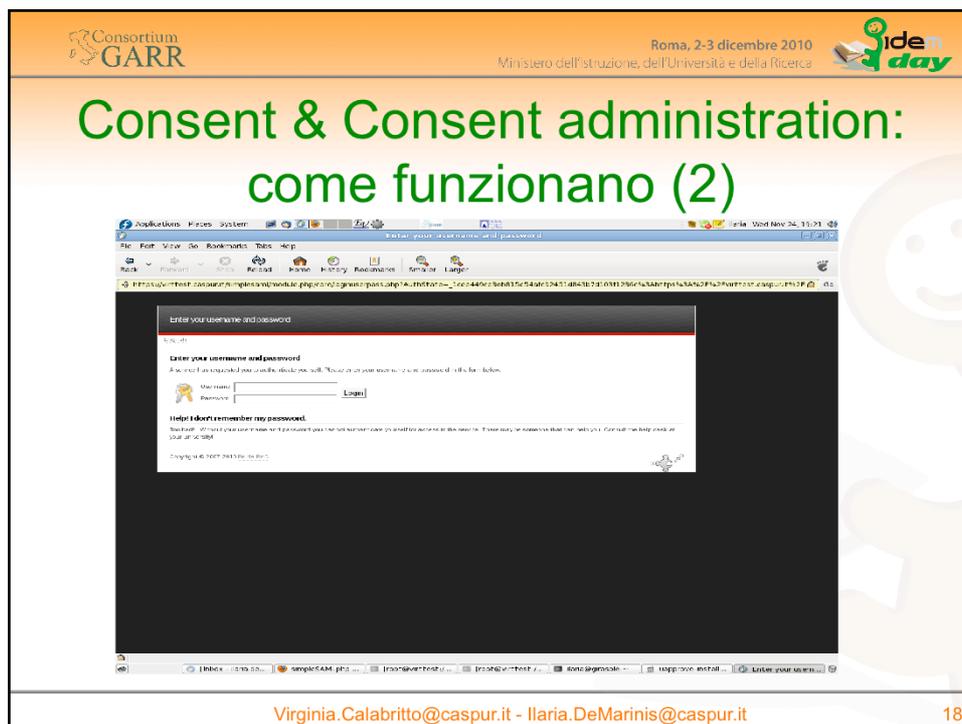
Consortium GARR Roma, 2-3 dicembre 2010 Ministero dell'Istruzione, dell'Università e della Ricerca 

Consent & Consent administration: come funzionano (1)



Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it 17

1 – l'utente chiede accesso alla risorsa



2 - l'utente si autentica presso il Servizio di gestione delle Identità della propria organizzazione

Più avanti mostreremo un'altra finestra di autenticazione per il servizio di gestione revocche qui e piu' avanti mostriamo la URL e ne evidenziamo la differenza:

https://virttest.caspur.it/simplesaml/module.php/consent/getconsent.php?StateId=_0238e4e1feec4a5d3f5f6ffea899fb3300a3a6e56%3Ahttps%3A%2F%2Fvirttest.caspur.it%2Fsimplesaml%2Fsaml2%2Fidp%2FSSOService.php%3Fspentityid%3Dhttps%253A%252F%252Fsarki.caspur.it%252Fshibboleth%26cookieTime%3D1290699961%26RelayState%3Dcookie%253Ae02babdf

Consortium GARR Roma, 2-3 dicembre 2010 Ministero dell'istruzione, dell'Università e della Ricerca **idem day**

Consent & Consent administration:

Consent about releasing personal information

English

<https://sarki.caspur.it/shibboleth> requires that the information below is transferred.

Remember

Information that will be sent to <https://sarki.caspur.it/shibboleth>

Affiliation at home organization	staff@caspur.it
Person's principal name at home organization	virginia@caspur.it
Mail	Virginia.Calabritto@caspur.it
Persistent pseudonymous ID	... Show content

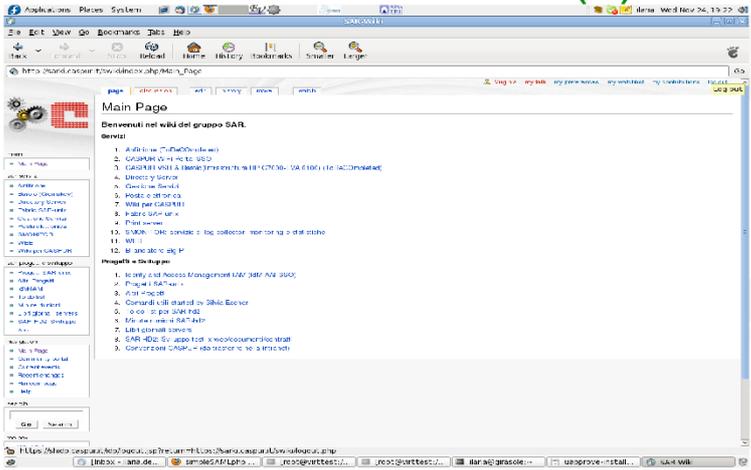
Copyright © 2007-2010 Feide RnD

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it 19

3 – all'utente viene mostrata la scheda con tutti gli attributi, che devono essere passati alla risorsa affinché questa possa autorizzare l'accesso, e gli viene richiesto di dare il suo consenso al trasferimento

Consortium GARR Roma, 2-3 dicembre 2010 Ministero dell'Istruzione, dell'Università e della Ricerca **idem day**

Consent & Consent administration: come funzionano (4)



The screenshot shows a web browser window displaying a wiki page. The page title is "Main Page" and it contains a list of items under the heading "Benvenuti nel wiki del gruppo SAR". The list includes items like "1. Addizione (1+1=2)", "2. GARR", "3. GARR", "4. GARR", "5. GARR", "6. GARR", "7. GARR", "8. GARR", "9. GARR", "10. GARR", "11. GARR", "12. GARR". The browser's address bar shows "http://www.caspur.it/wiki/index.php/Main_Page". The browser's status bar at the bottom shows "http://www.caspur.it/wiki/index.php/Main_Page".

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it 20

4 – se l'utente consente al trasferimento ottiene accesso alla risorsa

Consortium GARR

Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca

idem day

Consent & Consent administration: come funzionano (5)

ConsentAdmin

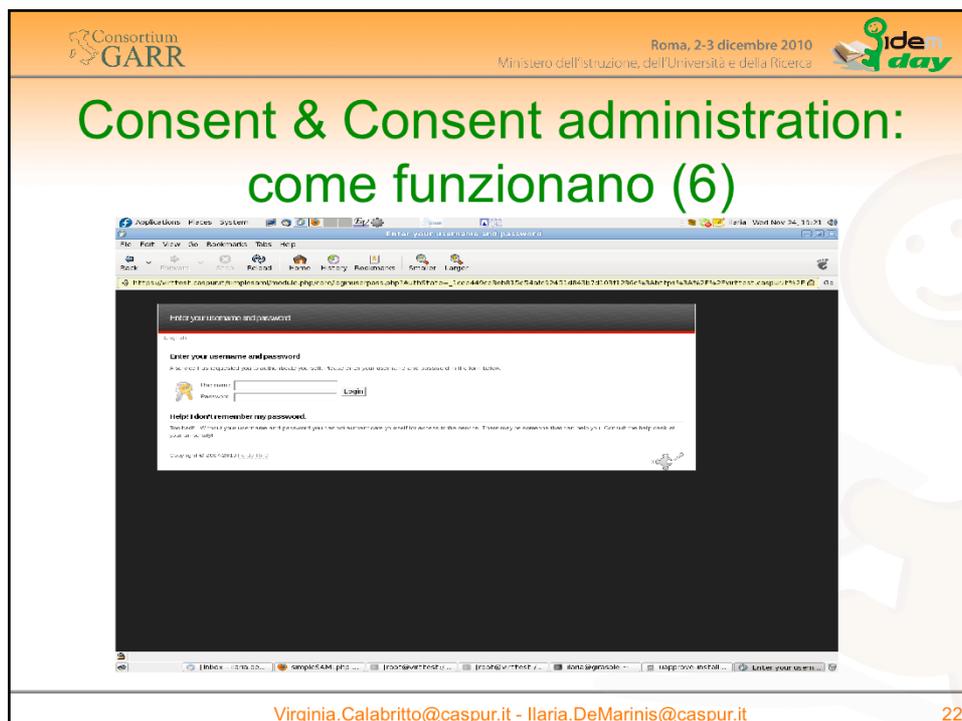
ConsentAdmin

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it

21

5 – per la gestione e revoca dei consensi è messo a disposizione un servizio dedicato la cui URL deve essere messa a disposizione dell'utente

<https://virttest.caspur.it/simplesaml/module.php/consentAdmin/consentAdmin.php>



6 – per accedere al servizio di gestione del consenso, l'utente si deve autenticare attraverso il servizio di identità

Notate, che si sta effettuando l'autenticazione per un servizio indipendente:

https://virttest.caspur.it/simplesaml/module.php/core/loginuserpass.php?AuthState=_66e0ba7a7a943aa034051a9f32c2481909c1df6d45%3Ahttps%3A%2F%2Fvirttest.caspur.it%2Fsimplesaml%2Fmodule.php%2Fcore%2Fas_login.php%3FAuthId%3Dcaspur-ldap%26ReturnTo%3Dhttps%253A%252F%252Fvirttest.caspur.it%252Fsimplesaml%252Fmodule.php%252FconsentAdmin%252FconsentAdmin.php

Consortium GARR Roma, 2-3 dicembre 2010 Ministero dell'istruzione, dell'Università e della Ricerca idem day

Consent & Consent administration: come funzionano (7)

Consent Administration

How to delete your consent

Links

- Start
- End

Logout

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it 23

7 – una volta autenticato il servizio di gestione delle identità gli mostrerà l'elenco delle risorse(oltre a SARKI WIKI ci saranno altre righe) per le quali è stato dato il consenso

8 – l'utente selezionando o deselezionando la casella corrispondente alla risorsa confermerà o revocherà il suo consenso al trasferimento dei suoi dati a quel servizio



 Roma, 2-3 dicembre 2010
 Ministero dell'Istruzione, dell'Università e della Ricerca
 

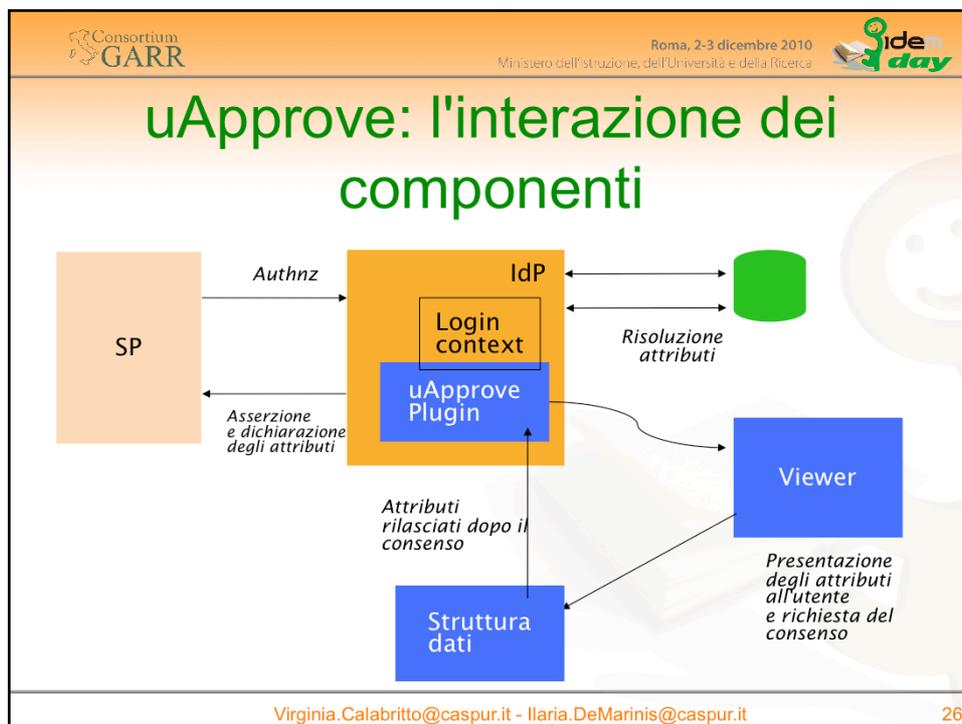
uApprove <> Consent & Consent administration

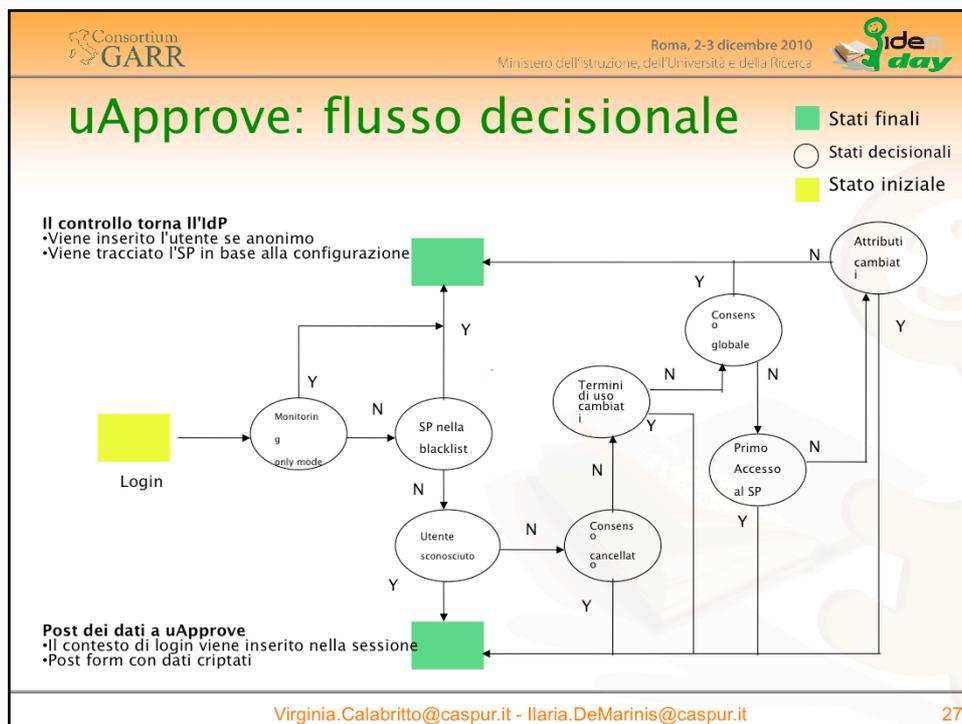
Funzionalità	uApprove	Consent & Consent Administration
Gestione Termini di	SI	NO
Consenso Globale	SI	NO
Revoca Globale	Sempre	Selezionando tutte le
Gestione selettiva revoche	NO	SI

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it 24

uApprove: i componenti

- Un plugin che verifica se uApprove debba essere invocato
- Un'applicazione web che interagisce con l'utente
- Una struttura dati per memorizzare le decisioni prese dall'utente





Consortium
GARR

Roma, 2-3 dicembre 2010
Ministero dell'istruzione, dell'Università e della Ricerca

idem
day

uApprove: Prerequisiti

- Shibboleth IdP 2.1.x
- Database SQL

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it 28

Consortium
GARR

Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca

idem
day

uApprove: Installazione (1)

- Download e unzip del software
- `wget http://www.switch.ch/aai/downloads/uApprove-2.1.3-bin.zip`
- `unzip uApprove-2.1.3-bin.zip`

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it 29

uApprove: Installazione (2)

- 2 file zip uno per il plugin e uno per il viewer

```
[tomcat@idp uApprove-2.1.3]$ ls
```

```
doc idp-plugin-2.1.3-bin.zip viewer-2.1.3-bin.zip
```

- Copia del plugin e dei file di configurazione

```
[tomcat@idp uApprove-2.1.3]$ unzip idp-plugin-2.1.3-bin.zip
```

```
[tomcat@idp uApprove-2.1.3]$ cp idp-plugin-2.1.3/conf-  
template/* /usr/local/idp/uApprove
```

```
[tomcat@idp uApprove-2.1.3]$ cp idp-plugin-2.1.3/lib/* /path/  
to/shibboleth/src/main/webapp/WEB-INF/lib/
```

uApprove: Installazione (3)

- Copia del viewer e dei suoi file di configurazione
- [tomcat@idp uApprove-2.1.3]\$unzip viewer-2.1.3-bin.zip
- [tomcat@idp uApprove-2.1.3]\$cp viewer-2.1.3/conf-template/* /usr/local/idp/uApprove/
- [tomcat@idp uApprove-2.1.3]\$cp -r viewer-2.1.3/webapp /opt/tomcat/webapps/uApprove

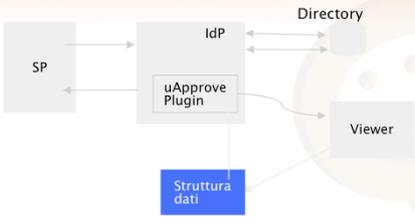


Consortium
GARR

Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca



uApprove: Configurazione (1)



```

graph LR
    SP[SP] <--> IdP[IdP]
    IdP <--> Directory[Directory]
    IdP <--> uApprove[uApprove Plugin]
    uApprove <--> Viewer[Viewer]
    uApprove <--> Struttura[Struttura dati]
    
```

- Il terzo componente è creato da noi: la struttura dati dove memorizzare le decisioni prese dall'utente
- FILE : raccomandato solo per organizzazioni molto piccole (meno di 100 utenti)
- DATABASE SQL: MySql, qualsiasi databse SQL purchè abbia un connettore JDBC

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it

32

Consortium GARR Roma, 2-3 dicembre 2010 Ministero dell'Istruzione, dell'Università e della Ricerca idem day

uApprove: Configurazione (2)

- Configurare il file `/usr/local/idp/uApprove/common.properties` come segue:

```
#storageType=database
#databaseConfig=/usr/local/idp/uApprove/
database.properties

storageType=file
flatFile = /usr/local/idp/uApprove/uApprove-log.xml
```
- Rendere `uApprove-log.xml` scrivibile da tomcat

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it 33



Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca



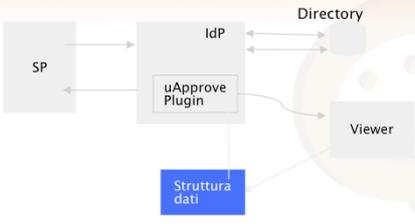
uApprove: Configurazione (3)

FILE

Un esempio

```

<?xml version="1.0" encoding="UTF-8"?>
<Users>
  <User name="virgi2">
    <Version id="1.0" terms-id="1.0" global="no" installationdate="Thu May 28 14:56:54 CEST 2009"/>
    <providerId name="https://sp.testshib.org/shibboleth-sp" attributes=":transientId:"/>
  </User>
  <User name="demarini">
    <Version id="1.0" terms-id="1.0" global="no" installationdate="Fri Oct 16 11:09:49 CEST 2009"/>
    <providerId name="https://aai.caspur.it/shibboleth"
      attributes=":eduPersonPrincipalName:transientId:eduPersonScopedAffiliation:eduPersonTargetedID:email:"/>
    <providerId name="https://sp.testshib.org/shibboleth-sp" attributes=":transientId:"/>
  </User>
</Users>
                
```



The diagram illustrates the uApprove configuration architecture. It shows a Service Provider (SP) interacting with an Identity Provider (IdP). The IdP is connected to a Directory and a Viewer. A uApprove Plugin is positioned between the SP and IdP, and is linked to a 'Struttura dati' (Data Structure) component. Arrows indicate the flow of information and interactions between these components.

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it

34



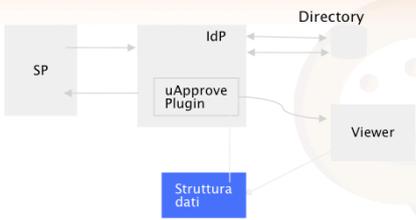
Consortium
GARR

Roma, 2-3 dicembre 2010
Ministero dell'istruzione, dell'Università e della Ricerca



idem
day

uApprove: Configurazione (4)



Database

- Creare un database ed un utente:

```
mysql>
CREATE DATABASE uApprove;
CREATE USER 'uApprove'@'localhost' IDENTIFIED BY 'uApprove';
GRANT USAGE ON *.* TO 'uApprove'@'localhost';
GRANT SELECT , INSERT , UPDATE , DELETE ON `uApprove`.* TO 'uApprove'@'localhost';
ALTER DATABASE uApprove DEFAULT CHARACTER SET utf8 COLLATE utf8_general_ci;
```

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it

35

Consortium
GARR

Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca

idem
day

uApprove: Configurazione (5)

Database

- La struttura

```
create table ArpUser (  
  idxArpUser int unsigned auto_increment primary key,  
  auUserName varchar(255) not null,  
  auLastTermsVersion varchar(255),  
  auFirstAccess timestamp,  
  auLastAccess timestamp  
);  
  
create index idxUserName on ArpUser (auUserName );  
  
create table ShibProvider (  
  idxShibProvider int unsigned auto_increment primary  
  key,  
  spProviderName varchar(255)  
);  
  
insert into ShibProvider (idxShibProvider) values (1);  
create index idxProvidename on ShibProvider  
(spProviderName);
```

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it

36



Consortium
GARR

Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca



idem
day

uApprove: Configurazione (6)

Database

- La struttura

```
create table AttrReleaseApproval (  
  idxAttrReleaseApproval int unsigned auto_increment primary key,  
  araldxArpUser int unsigned references ArpUser ( idxArpUser ),  
  araldxShibProvider int unsigned references ShibProvider( idxShibProvider ),  
  araTimeStamp timestamp not null,  
  araTermsVersion varchar(255),  
  araAttributes text(2048)  
);  
  
create table ProviderAccess (  
  idxProviderAccess int unsigned auto_increment primary key,  
  paIdxArpUser int unsigned references ArpUser( idxArpUser ),  
  paIdxShibProvider int unsigned references ShibProvider( idxShibProvider ),  
  paAttributesSent text,  
  paTermsVersion varchar(255),  
  paIdxAttrReleaseApproval int unsigned references AttrReleaseApproval ( idxAttrReleaseApproval ),  
  paShibHandle varchar(255),  
  paTimeStamp timestamp not null  
);
```

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it37



Consortium
GARR

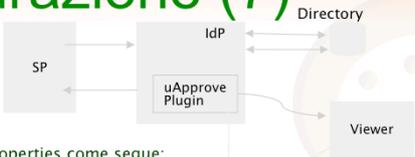
Roma, 2-3 dicembre 2010
Ministero dell'istruzione, dell'Università e della Ricerca



idem
day

uApprove: Configurazione (7)

DATABASE



Configurare il database `/usr/local/idp/uApprove/common.properties` come segue:

```
storageType=database
databaseConfig=/usr/local/idp/uApprove/
database.properties

#storageType=file
#flatFile = /opt/uApprove/data/uApprove-log.xml
```

Configurare i parametri mysql nel file `/usr/local/idp/uApprove/database.properties`:

```
driver=com.mysql.jdbc.Driver
url=jdbc:mysql://localhost:3306/uApprove?
autoReconnect=true
user=uApprove
password=uApprove
sqlCommands=/etc/shibboleth-idp/uApprove/
mysql.commands
```

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it

38



Consortium
GARR

Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca



uApprove: Configurazione (8)

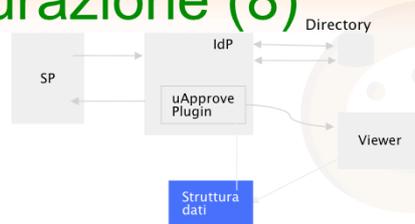
DATABASE

Un esempio

```

ArpUser
idxArpUser:          9
auUserName:          guest
auLastTermsVersion: 1.0
auFirstAccess:       2010-11-16 17:00:42
auLastAccess:        2009-07-15 13:53:02

AttrReleaseApproval
idxAttrReleaseApproval: 21
araIdxArpUser:          9
araIdxShibProvider:     caspur
araTimeStamp:           2010-08-30 16:57:14
araTermsVersion:       1.0
:eduPersonPrincipalName:commonName:
transientId:eduPersonScopedAffiliation:eduPersonTargetedID..
                    
```



```

graph LR
    SP[SP] <--> IdP[IdP]
    IdP <--> Directory[Directory]
    IdP --> uApprove[uApprove Plugin]
    uApprove --> Viewer[Viewer]
    uApprove --> Struttura[Struttura dati]
    
```

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it
39



Consortium
GARR

Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca



uApprove: Configurazione (9)

DATABASE

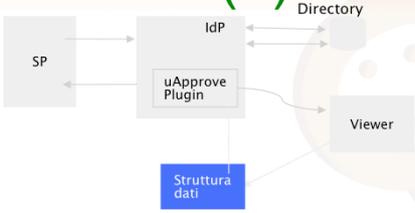
Un esempio

ShibProvider

idxShibProvider
spProviderName

ProviderAccess

paIdxAppUser
paIdxShibProvider
paAttributesSent
eduPersonPrincipalName:commonName:transientId:
eduPersonScopedAffiliation:eduPersonTargetedID:email:
paTermsVersion
paIdxAttrReleaseApproval:
paShibHandle:
paTimeStamp:



8
<https://aai.caspur.it/shibboleth>

9
8

1,0
21
NULL
2010-11-23 12:26:53

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it
40



Consortium
GARR

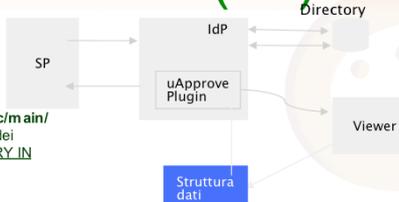
Roma, 2-3 dicembre 2010
Ministero dell'istruzione, dell'Università e della Ricerca



idem
day

uApprove: Configurazione (10)

- Integriamo uApprove dentro Shibboleth
- Configurare il file `web.xml` (`/opt/shibboleth-identityprovider/src/main/webapp/WEB-INF/web.xml`): relativo alla directory di installazione dei sorgenti di Tomcat (NON È IL FILE PRESENTE NELLA DIRECTORY IN PRODUZIONE)



```

<filter>
<filter-name>uApprove IdP plugin</filter-name>
<filter-class>ch.SWITCH.aai.uApprove.idpplugin.Plugin</filter-class>
<init-param>
<param-name>Config</param-name>
<param-value>
/usr/local/idp/uApprove/idp-plugin.properties;
/usr/local/idp/uApprove/common.properties;
</param-value>
</init-param>
</filter>

<filter-mapping>
<filter-name>uApprove IdP plugin</filter-name>
<url-pattern>/profile</url-pattern>
<dispatcher>REQUEST</dispatcher>
<dispatcher>FORWARD</dispatcher>
</filter-mapping>
    
```

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it
41

Consortium GARR Roma, 2-3 dicembre 2010 Ministero dell'Istruzione, dell'Università e della Ricerca idem day

uApprove: Configurazione (11)

```
graph LR; SP[SP] <--> IdP[IdP]; IdP <--> Directory[Directory]; IdP <--> uApprove[uApprove Plugin]; uApprove <--> Viewer[Viewer]; uApprove <--> Struttura[Struttura dati];
```

- Integriamo uApprove dentro Shibboleth
 - Deploy di Shibboleth

```
cd /opt/shibboleth-identityprovider/  
sh install.sh
```

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it 42



Consortium
GARR

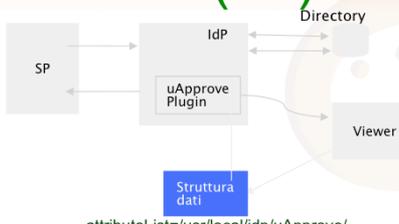
Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca



idem
day

uApprove: Configurazione (12)

- Configurazione degli attributi
 - Possiamo impostare delle regole e delle preferenze per la presentazione degli attributi all'utente per una determinata risorsa
 - Dentro il file `/usr/local/idp/uApprove/viewer.properties`:
attribute-list



attributeList=/usr/local/idp/uApprove/

```
# Ordine degli attributi
eduPersonScopedAffiliation
eduPersonPrincipalName

# Attributi da nascondere
!persistentId
```

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it

43



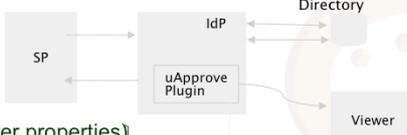
Consortium
GARR

Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca



idem
day

uApprove: Configurazione (13)



- Consenso globale (/usr/local/idp/uApprove/viewer.properties)
- globalConsentPossible=true
- Logging (/usr/local/idp/uApprove/viewer.properties)
- loggingConfig=/usr/local/idp/uApprove/logging.xml

```

<configuration>
...
<appender class="ch.qos.logback.core.FileAppender" name="RootFileAppender">
  <file>/usr/local/idp/uApprove/uApprove.log</file>
</appender>
...
</configuration>
                
```

Deve essere scrivibile da tomcat

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it
44



Consortium
GARR

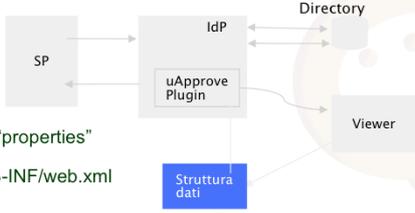
Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca



idem
day

uApprove: Configurazione (14)

- Configurazione del Viewer
- Aggiorniamo i path dei file che definiscono le nostre "properties" all'interno del viewer /opt/tomcat/webapps/uApprove/WEB-INF/web.xml



```

<web-app>
...
<context-param>
  <param-name>Config</param-name>
  <param-value>
    /usr/local/idp/uApprove/viewer.properties;
    /usr/local/idp/uApprove/common.properties;
  </param-value>
</context-param>
...
</web-app>

```

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it

45

Consortium GARR Roma, 2-3 dicembre 2010 Ministero dell'Istruzione, dell'Università e della Ricerca 

uApprove: Configurazione (15)

Apache, uApprove e Tomcat

```
<VirtualHost idp.example.org:443>  
...  
<Location /uApprove>  
  Allow from all  
  ProxyPass ajp://localhost:8009/uApprove  
</Location>  
...  
</VirtualHost>
```

Riavviare apache

Creare un proxy per l'applicazione web
Serve un canale di comunicazione tra Viewer e Tomcat

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it 46

uApprove: Configurazione (16)

- Cancellazione del consenso (!!! SOLO CON UN DATABASE SQL !!!)
 - Modalità *In-flow*: l'utente può cancellare le sue decisioni durante la fase di login
- (solo per JAAS UsernamePassword login handler)
- Modalità *Standalone*: pagina jsp dedicata reset-approvals.jsp

uApprove: Altre configurazioni (1)

- TermsOfUseManager: testo dei termini di utilizzo
Dentro il file `/usr/local/idp/uApprove/common.properties` definire:
`termsOfUse=/usr/local/idp/uApprove/conf/terms-of-use.xml`
Personalizzare il file `terms-of-use.xml` secondo le proprie policy
- Le informazioni che il plugin IdP e il Viewer si scambiano sono confidenziali, vengono criptate e decriptate tramite uno *sharedSecret*
Dentro il file `/usr/local/idp/uApprove/common.properties` definire:
`sharedSecret=QErDXYZEAoS6jooPvdBhQg==`

Consortium GARR Roma, 2-3 dicembre 2010 Ministero dell'istruzione, dell'Università e della Ricerca idem day

uApprove: Altre configurazioni (2)

- Configurazione di una *blacklist di SP*
Dentro il file `/usr/local/idp/uApprove/idp-plugin.properties`
specificare il file `spBlacklist=/usr/local/idp/uApprove/sp-blacklist`

```
# Example 1: specific resource  
https://sp1\domani.it/shibboleth  
  
# Example 2: all applications within a Service Provider  
https://sp2\domani.it/*  
  
# Example 3: all Service Provider within a specific domain  
https://.*\domain.it/*
```

- Monitoring only
- Supporto Multilingua per il testo statico e dinamico (ad es. gli attributi)

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it 49

consent di sSphp: i componenti

- modulo Consent
- modulo Consent Administration
- modulo di presentazione all'utente tramite interfaccia web
- Strutture dati: cookies o database

Consortium
GARR

Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca

Open
day

consent di sSphp: prerequisiti

- SimpleSAMLphp > 1.4
- php-pdo
- Database driver: (mysql, pgsql, ...)
 - php-mysqli
 - php-mysql

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it 51



Consortium
GARR

Roma, 2-3 dicembre 2010
Ministero dell'istruzione, dell'Università e della Ricerca



idem
day

modulo Consent : configurazione(1)

- Creare il file "enable" nella directory modules/consent/

Configurare il modulo config/config.php

```
90 => array(  
    'class'    => 'consent:Consent',  
    'store'    => array (  
        'consent:Database',  
        'dsn' => 'mysql:host=localhost;dbname=ssphp-consent',  
        'username' => 'user',  
        'password' => 'passwd'  
    ),  
    'hiddenAttributes' => array('eduPersonTargetedID'),  
    'focus'    => 'yes',  
    'checked'   => TRUE  
)
```

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it

52

modulo Consent : configurazione(2)

- Disabilitazione del consenso per un insieme di risorse.

Editare il file `simplesamlphp/metadata/saml2.0-idp-hosted.php`

```
'consent.disable' => array( 'sp.example.com',  
                             'sp2.example.com', ... ),
```

modulo Consent Administration: configurazione

- Abilitare il modulo: touch modules/consentAdmin/enable
- Copiare il file **/simplesamlphp/modules/consentAdmin/config-templates/module_config.php** dentro la directory **/simplesamlphp/config**

```
'consentadmin' => array(  
    'consent:Database',  
    'dsn' => 'mysql:host=localhost;dbname=ssphp-consent',  
    'username' => 'user',  
    'password' => 'passw',  
),
```

Consortium
GARR

Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca

idem
day

ToDo

Esperienza:
dopo l'installazione di uApprove sul ns IdP il server di monitoring (AAIEye), in test durante il progetto IDEM, segnalava problemi del ns IdP rispetto ad alcune risorse

Da investigare:
relazioni tra gli strumenti di consenso informato e quelli di monitoring

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it

55

Consortium
GARR

Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca

idem
day

Link utili

- uApprove:
<http://www.switch.ch/aai/support/tools/uApprove.html>
- Connettore JDBC per MySQL:
<http://dev.mysql.com/downloads/connector/j/5.0.html>
- SimpleSAMLPhp consent:
<http://simplesamlphp.org/docs/1.6/consent:consent>
- SimpleSAMLPhp consentAdmin:
<http://simplesamlphp.org/docs/1.6/consentAdmin:consentAdmin>

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it

56

The slide features a header with the Consortium GARR logo on the left, the text 'Roma, 2-3 dicembre 2010' and 'Ministero dell'Istruzione, dell'Università e della Ricerca' in the center, and the 'idem day' logo on the right. The main content area has a light orange gradient background with the word 'help' in green. Below it, three email addresses are listed: 'idem-help@garr.it', 'idem-users@garr.it', and 'aai@caspur.it'. A faint background image shows a hand holding a pen over a document. The footer contains the email addresses 'Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it' and the number '57'.

- 1 - l'indirizzo ufficiale, del Servizio GARR IDEM, per il supporto nella Federazione IDEM
- 2 - l'indirizzo della lista alla quale chiunque è interessato può iscriversi per discutere problematiche di IdM/IAM e darsi supporto reciproco. Per l'iscrizione: <http://www.garr.it/mailman/listinfo/idem-users>
- 3 - il ns indirizzo al CASPUR oltre quelli personali che trovate nel footer

Consortium
GARR

Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca

idem
day

Grazie!

Virginia.Calabritto@caspur.it - Ilaria.DeMarinis@caspur.it 58