



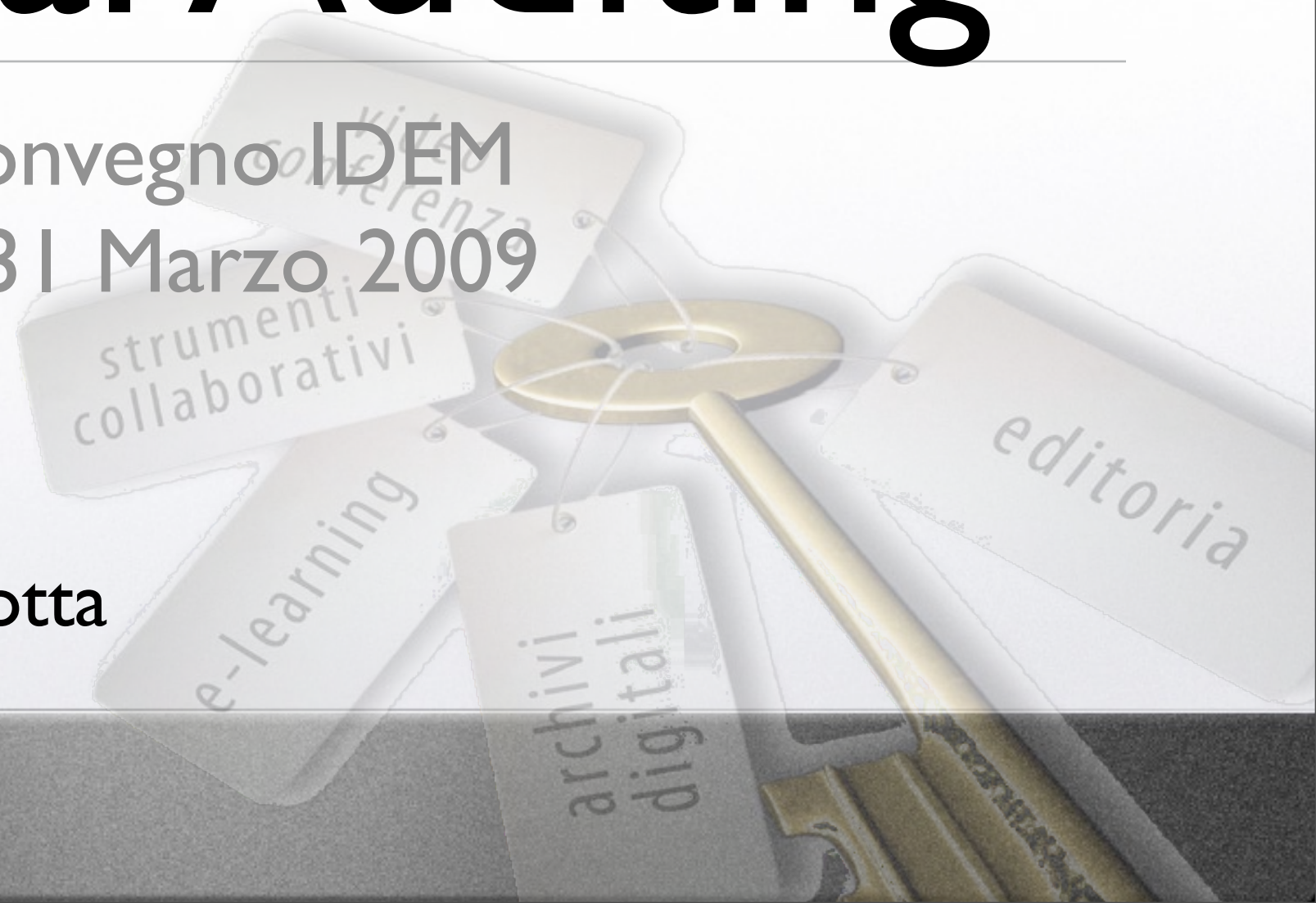
CNR - Istituto di studi sui
sistemi intelligenti per l'automazione



Tutorial Auditing

I convegno IDEM
30-31 Marzo 2009

Speaker: Claudio Marotta





- Auditing & Operatività
- Problemi & Soluzioni
- Tips'n'Tricks sparsi (come aderire alle specifiche tecniche)

Auditing & Operatività



- Cosa è l'auditing
- Gruppo di auditing: M. Ianigro, F. Malvezzi, M.L. Mantovani, C. Marotta
- Auditing in fase sperimentale: test dei sistemi e delle procedure
- Auditing in produzione

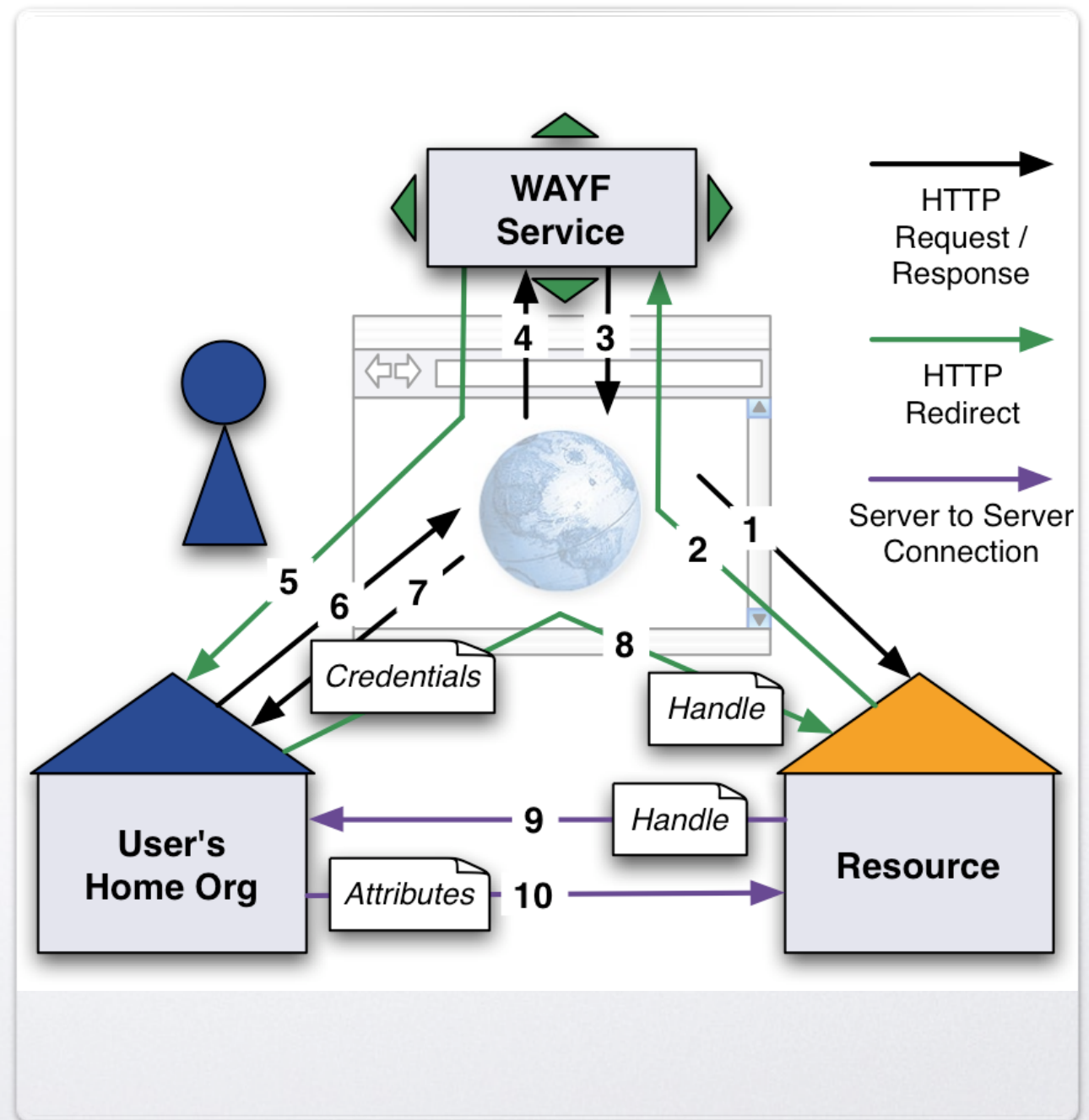


Strumento di indagine:

- Server di monitoring AAIEYE
- Sviluppato nel contesto della federazione Finlandese Haka (thanks to Mika Suvanto)
- Approccio basato sui test-case

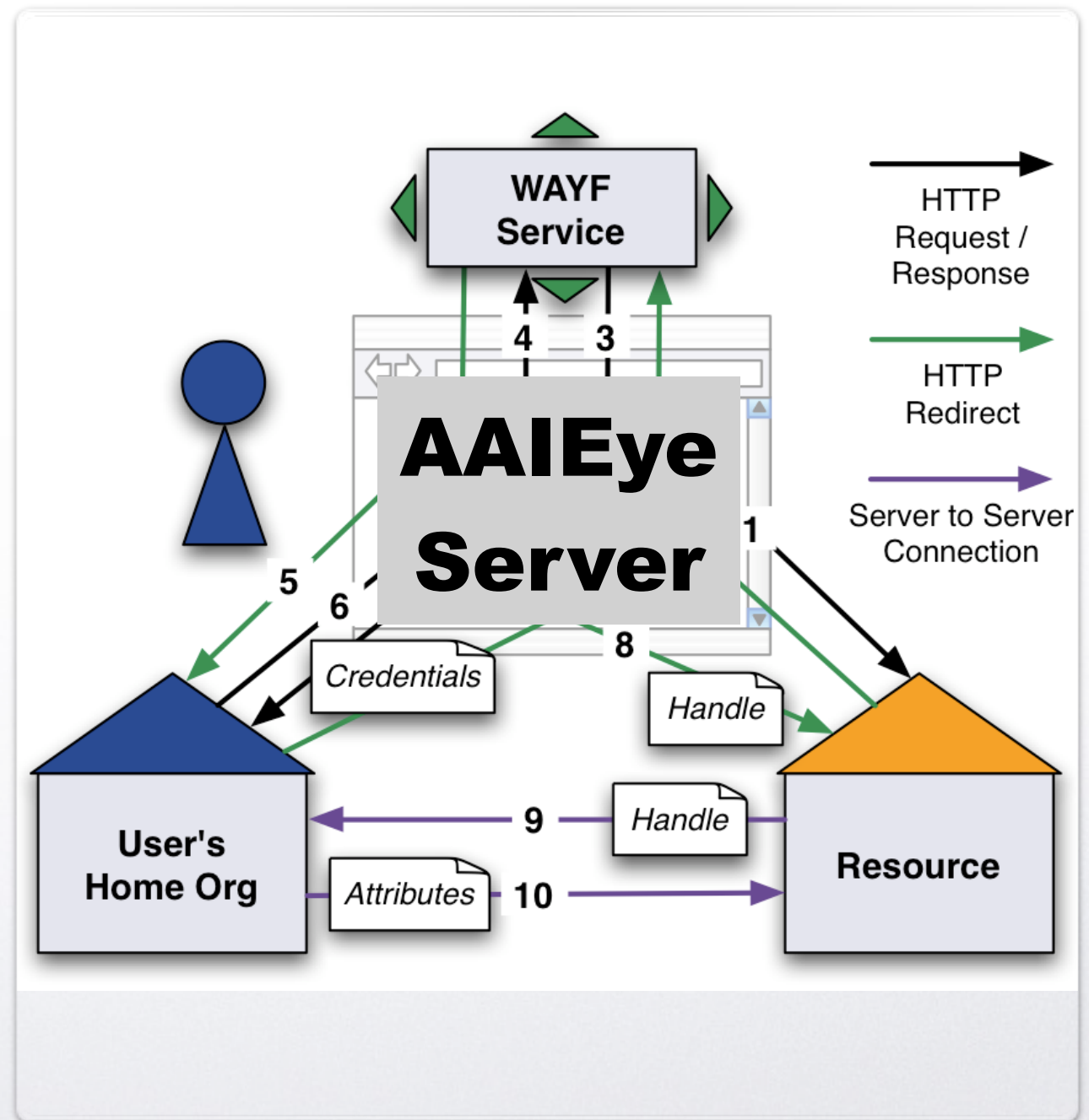
- Simulazione del login di un utente
- Tutti contro tutti (IdP vs. SP)

TIP: Account di test - occhio al popolamento di tutti gli attributi



- Simulazione del login di un utente
- Tutti contro tutti (IdP vs. SP)

TIP: Account di test - occhio al popolamento di tutti gli attributi



Identity Providers

	Provider	Tests passed	Last tested on	Message
!	CASPUR	4 / 5	2009-03-26 08:38:13	[GARR Vconf] -- FAILED: [IdP] Refresh Aborted by HtmlUnit: Attempted to refresh a page using an ImmediateRefreshHandler which could have caused an OutOfMemoryError Please use WaitingRefreshHandler or ThreadedRefreshH
!	CNR Bari	4 / 5	2009-03-26 08:38:16	[GARR Vconf] -- FAILED: [IdP] Refresh Aborted by HtmlUnit: Attempted to refresh a page using an ImmediateRefreshHandler which could have caused an OutOfMemoryError Please use WaitingRefreshHandler or ThreadedRefreshH
!	CNR Ceris	5 / 6	2009-03-26 08:38:12	[GARR Vconf] -- FAILED: [IdP] Refresh Aborted by HtmlUnit: Attempted to refresh a page using an ImmediateRefreshHandler which could have caused an OutOfMemoryError Please use WaitingRefreshHandler or ThreadedRefreshH
✓	CNR Istituto di Virologia Vegetale	5 / 5	2009-03-26 08:38:11	
✓	CNR IVV	1 / 1	2009-03-26 08:38:13	
✓	POLIMI	1 / 1	2009-03-26 08:38:14	
!	Politecnico di Milano	4 / 5	2009-03-26 08:39:04	[GARR Vconf] -- FAILED: [IdP] Refresh Aborted by HtmlUnit: Attempted to refresh a page using an ImmediateRefreshHandler which could have caused an OutOfMemoryError Please use WaitingRefreshHandler or ThreadedRefreshH
✓	Università degli Studi di Modena e Reggio Emilia	5 / 5	2009-03-26 08:38:20	
✗	Università degli Studi di Padova	0 / 5	2009-03-26 08:38:07	[Moodle Idem] -- FAILED: [WAYF] HtmlUnit Error submitting form using default submit button, check th [GARR Vconf] -- FAILED: [WAYF] HtmlUnit Error submitting form using default submit button, check th [SP di Test GARR] -- FAILED: [WAYF] HtmlUnit Error submitting form using default submit button, check th [Idem Wiki] -- FAILED: [WAYF] HtmlUnit Error submitting form using default submit button, check th [Idem Blog] -- FAILED: [WAYF] HtmlUnit Error submitting form using default submit button, check th
!	Università degli Studi di Torino	4 / 5	2009-03-26 08:38:17	[GARR Vconf] -- FAILED: [IdP] Refresh Aborted by HtmlUnit: Attempted to refresh a page using an ImmediateRefreshHandler which could have caused an OutOfMemoryError Please use WaitingRefreshHandler or ThreadedRefreshH



Service Providers

	Provider	Tests passed	Last tested on	Message
✓	Cilea Digital Library	3 / 3	2009-03-26 08:38:14	
!	GARR Vconf	2 / 8	2009-03-26 08:38:14	[Università degli Studi di Padova] -- FAILED: [WAYF] HtmlUnit Error submitting form using default submit button, check th [Università degli Studi di Torino] -- FAILED: [IdP] Refresh Aborted by HtmlUnit: Attempted to refresh a page using an ImmediateRefreshHandler which could have caused an OutOfMemoryError Please use WaitingRefreshHandler or ThreadedRefreshH [CNR Ceris] -- FAILED: [IdP] Refresh Aborted by HtmlUnit: Attempted to refresh a page using an ImmediateRefreshHandler which could have caused an OutOfMemoryError Please use WaitingRefreshHandler or ThreadedRefreshH [CNR Bari] -- FAILED: [IdP] Refresh Aborted by HtmlUnit: Attempted to refresh a page using an ImmediateRefreshHandler which could have caused an OutOfMemoryError Please use WaitingRefreshHandler or ThreadedRefreshH [Politecnico di Milano] -- FAILED: [IdP] Refresh Aborted by HtmlUnit: Attempted to refresh a page using an ImmediateRefreshHandler which could have caused an OutOfMemoryError Please use WaitingRefreshHandler or ThreadedRefreshH [CASPUR] -- FAILED: [IdP] Refresh Aborted by HtmlUnit: Attempted to refresh a page using an ImmediateRefreshHandler which could have caused an OutOfMemoryError Please use WaitingRefreshHandler or ThreadedRefreshH
!	Idem Blog	7 / 8	2009-03-26 08:39:04	[Università degli Studi di Padova] -- FAILED: [WAYF] HtmlUnit Error submitting form using default submit button, check th
!	Idem Wiki	7 / 8	2009-03-26 08:38:19	[Università degli Studi di Padova] -- FAILED: [WAYF] HtmlUnit Error submitting form using default submit button, check th
!	Moodle Idem	7 / 8	2009-03-26 08:38:20	[Università degli Studi di Padova] -- FAILED: [WAYF] HtmlUnit Error submitting form using default submit button, check th
!	SP di Test GARR	7 / 8	2009-03-26 08:38:15	[Università degli Studi di Padova] -- FAILED: [WAYF] HtmlUnit Error submitting form using default submit button, check th

Date un'occhiata: <http://cluedo5.ba.issia.cnr.it/idem/webui/status.php>



Ogni Identity provider deve realizzare una pagina web (linkata dalla pagina di SSO) contenente:

- Denominazione dell'organizzazione
- Riferimenti per il supporto agli utenti
- Nominativi, indirizzi e-mail e numeri telefonici dei contatti tecnici per IDEM.
- Numero di fax e di telefono cellulare (opzionale)

TIP: Host pagina supporto != Host IdP



Ipotesi in discussione

Obiettivi di qualità	Intertempo di verifica [gg]	Downtime tollerato [gg]
Uptime dei server (IdP/SP):	7	30
Pagina web di supporto	7	15
Indirizzo email per l'helpdesk	30	60

Il partecipante si impegna a mantenere una registrazione delle attività legate ai propri servizi (Idp o SP) al fine di poter fornire un migliore supporto nella risoluzione di problemi tecnici o nella gestione di eventuali incidenti di sicurezza.
(Accordo di Partecipazione)

Problemi & Soluzioni



Certificati buoni....

```
> openssl s_client -connect sp-test.garr.it:443
```

```
...
```

Certificate chain

```
0 s:/C=IT/O=GARR/OU=GARR/OU=Firenze/CN=sp-test.garr.it/emailAddress=xxxx@garr.it  
i:/C=BE/O=Cybertrust/OU=Educational CA/CN=Cybertrustbertrust Educational CA
```

```
1 s:/C=BE/O=Cybertrust/OU=Educational CA/CN=Cybertrust Educational CA  
i:/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root
```

```
2 s:/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root  
i:/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root
```

```
...
```



... e un po' meno buoni....

```
> openssl s_client -connect fire.rettorato.unito.it:443
```

```
...
```

```
Certificate chain
```

```
0 s:/C=IT/O=GARR/OU=UNITO/CN=fire.rettorato.unito.it/emailAddress=xxxx@unito.it
```

```
  i:/C=BE/O=Cybertrust/OU=Educational CA/CN=Cybertrust Educational CA
```

```
1 s:/O=Cybertrust Inc/CN=Cybertrust SureServer StandardValidation CA
```

```
  i:/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root
```

```
2 s:/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root
```

```
  i:/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root
```

```
3 s:/C=BE/O=Cybertrust/OU=Educational CA/CN=Cybertrust Educational CA
```

```
  i:/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root
```

```
4 s:/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root
```

```
  i:/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root
```

```
5 s:/C=BE/O=Cybertrust/OU=Educational CA/CN=Cybertrust Educational CA
```

```
  i:/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root
```

```
6 s:/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root
```

```
  i:/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root
```

```
7 s:/C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority - G2/OU=(c) 1998VeriSign, Inc. - For authorized use only/OU=VeriSign Trust Network
```

```
  i:/C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority - G2/OU=(c) 1998VeriSign, Inc. - For authorized use only/OU=VeriSign Trust Network
```

```
8 s:/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=Terms of use at https://www.verisign.com/rpa (c)03/CN=VeriSign Class 3 Secure Intranet Server CA
```

```
  i:/C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority - G2/OU=(c) 1998VeriSign, Inc. - For authorized use only/OU=VeriSign Trust Network
```

```
9 s:/O=VeriSign Trust Network/OU=VeriSign, Inc./OU=VeriSign International Server CA - Class 3/OU=www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97VeriSign
```

```
  i:/C=US/O=VeriSign, Inc./OU=Class 3 Public Primary Certification Authority
```

```
...
```



Come posso verificare la catena che rilascio?

```
#> openssl s_client -connect <hostname>:<port>
```



Attributi non accettati:

- Nelle prime fasi dell'auditing abbiamo scoperto che alcuni SP falliscono se gli attributi contengono caratteri non alfanumerici: “_”, “-”
- I service provider DEVONO rendere note le proprie anomalie, e RISOLVERE il problema nel minor tempo possibile.

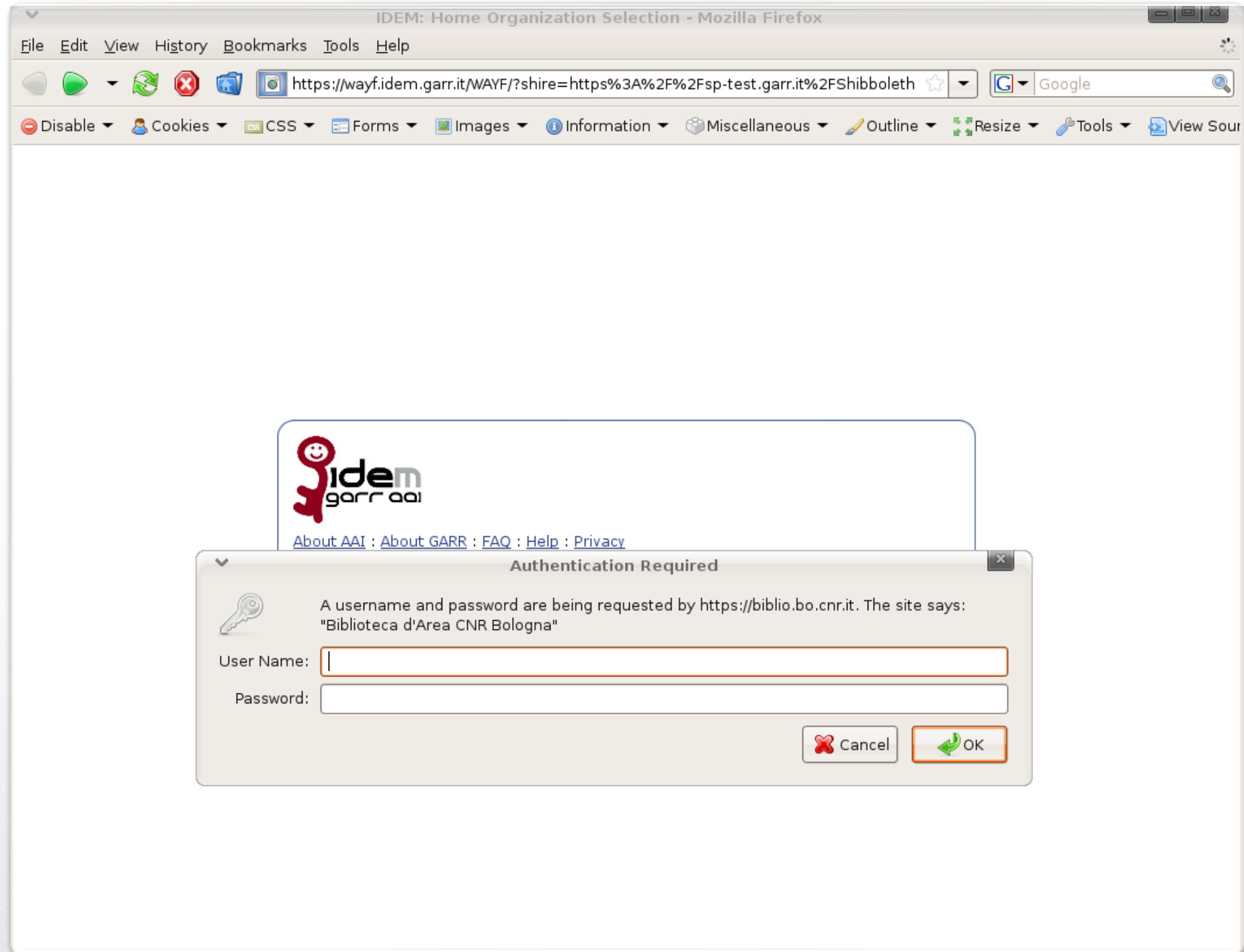


Gestori dei WAYF: occhio alla nomenclatura!

- In 2 casi la denominazione dello stesso partecipante è diversa fra i 2 WAYF 'interni' (Garr e Cilea): Politecnico di Milano, CNR IVV
- La federazione si farà carico di comunicare le denominazioni ufficiali.
- Nei metadati: `<OrganizationDisplayName>`



Autenticazione Apache-Based





Autenticazione Java-Based

Universit  degli studi
di Modena e Reggio Emilia

ATENE0 FONDATO NEL 1175

Log-in

Nome utente

Password

Entra (Login)

The resource that you have attempted to access requires that you log in with your with your UniMORE UID.
Il servizio a cui si sta accedendo richiede l'inserimento delle proprie credenziali UniMORE:

- **per gli Studenti:** le credenziali (numero tessera e PIN) le sono state rilasciate dalla segreteria studenti al momento dell'immatricolazione; lei pu  [cambiare o ripristinare la password](#) inserendo l'ultima password nota oppure il PIN originale
ulteriori informazioni: <https://posta.unimo.it/faq>
- **per tutti gli altri:** le credenziali sono state scelte da lei al momento dell'identificazione o alla presa di servizio; nel caso non le ricordi pu  rivolgersi all'incaricato dell'identificazione presso la sua Struttura di appartenenza. L'elenco degli incaricati   consultabile a questa [pagina](#)

[Elenco dei servizi accessibili con le credenziali UniMORE](#)

Single SignOn - Area CNR BA - Mozilla Firefox

File Edit View History Bookmarks Tools Help

<https://bacon.area.ba.cnr.it/shibboleth-idp/SSO?shire=h> Google

Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize

Area CNR Bari IDEM

L'area della ricerca di Bari partecipa a IDEM

Please login:

UID

Password

Login

Help	Link
Contatti tecnici	Home Area CNR BA
FAQ	Home Progetto Idem

Copyright   Area Ricerca CNR Bari 2008

Done bacon.area.ba.cnr.it FoxyProxy: Patterns

Grazie per l'attenzione!

Domande?

<mailto:marotta@ba.issia.cnr.it>



- Documento “Specifiche Tecniche” sul Wiki della Federazione:
http://aai.caspur.it/GARR-AAI-fed/index.php/Specifiche_tecniche
- Pagina del gruppo di auditing sul Wiki della Federazione:
<http://aai.caspur.it/GARR-AAI-fed/index.php/Auditing> (in pubblicazione)
- Verificate lo stato dei servizi (temporanea):
<http://cluedo5.ba.issia.cnr.it/idem/webui/status.php>
- Info e documentazione sul server di monitoring:
<http://www.csc.fi/english/institutions/haka/technology/aaieye>