

Napoli – 12 novembre 2010
WORKSHOP ICT4UNIVERSITY
Università Federico II, Complesso San Marcellino e Festo

Autenticazione federata per l'accesso ad Internet



Alessandro Bogliolo
Università di Urbino
alessandro.bogliolo@uniurb.it

Caso d'uso

- 1. L'utente**, registrato presso un soggetto, detto "**Organizzazione di appartenenza**" (**OdA**), che gli ha fornito un'identità digitale e le relative credenziali (username e password, o certificato),
2. utilizza le credenziali fornite dall'OdA
3. per accedere ad Internet attraverso le risorse di rete di un secondo soggetto, detto "**Fornitore di servizio**" (**FdS**).

Condizione 1

1) registrazione:

la procedura di registrazione adottata dall'OdA per **assegnare e/o abilitare le credenziali** all'utente deve garantire la **riservatezza** delle credenziali e l'**identificazione certa** dell'utente nel rispetto della normativa vigente in materia di antiterrorismo e di sicurezza informatica.

Condizione 1 (continua)

a. Identificazione diretta:

procedure di registrazione a seguito di identificazione diretta **de visu** attraverso l'acquisizione dei dati di un documento di identità personale,

b. Identificazione indiretta esterna:

procedure di registrazione a seguito di identificazione indiretta basata sull'acquisizione dei dati di una **carta di credito** o di una **SIM card** rilasciata in Italia,

c. Identificazione indiretta interna:

- c. procedure di registrazione a seguito di identificazione indiretta basata sull'acquisizione di token o la verifica di **credenziali precedentemente rilasciati dalla OdA** stessa con modalità di tipo a) o b).

Condizione 2

2) gestione dell'identità digitale:

l'OdA deve garantire il trattamento dei dati e delle credenziali dell'utente nel rispetto della normativa vigente in materia di **sicurezza informatica** e di **privacy** e, nel caso in cui l'identità digitale comprenda username e password, l'OdA deve mettere a disposizione dell'utente procedure sicure per **modificare o reimpostare la propria password**.

Condizione 3

3) autenticazione:

la procedura di autenticazione deve prevedere l'utilizzo di **canali sicuri** per la trasmissione delle credenziali ed **evitare di esporre le credenziali al Fornitore di servizio o a terzi**.

Condizione 4

4) **accesso:**

la procedura di accesso deve prevedere lo **scambio** tra l'OdA e il FdS **dei dati minimi indispensabili** a permettere:

- l'**identificazione** dell'utente presso l'OdA,
- la **verifica** del possesso dei **requisiti** di accesso,
- l'**erogazione** del servizio nel rispetto della normativa vigente e delle usage policies della rete del FdS e della rete (ad esempio NREN) a cui questo è connesso;

Condizione 5

5) **tracciamento:**

l'OdA e il FdS devono collaborare ai fini del **tracciamento** e dell'**identificazione** dell'utente, nel rispetto della normativa vigente in materia di antiterrorismo, di privacy e di sicurezza informatica.

A tal fine l'OdA e il FdS devono **condividere riferimenti univoci** associati alle tracce mantenute dal FdS e all'identità dell'utente mantenuta dall'OdA.

Condizione 6

6) **fiducia:**

L'OdA e il FdS devono darsi garanzie reciproche di rispetto delle condizioni espresse ai precedenti punti 1), 2), 3), 4) e 5).

Tali garanzie possono essere formalizzate da un **accordo bilaterale** tra OdA e FdS, o dalla adesione dell'OdA e del FdS ad una **federazione** o confederazione che preveda il rispetto delle suddette condizioni.

Condizione 7

7) **informazione:**

L'utente deve essere informato:

- delle finalità e delle modalità di **trattamento dei propri dati** personali eventualmente richiesti;
- **dei servizi**, delle federazioni e delle confederazioni a cui le credenziali danno accesso;
- dell'**identità** del soggetto che fornisce il servizio (**FdS**) e dell'identità del soggetto che opera la validazione delle credenziali all'atto dell'autenticazione (**OdA**);
- dello **scambio di informazioni** tra OdA e FdS ai fini della fornitura del servizio;
- delle **condizioni di utilizzo** del servizio di accesso;
- delle modalità di interruzione dell'accesso (**logout**).

Condizione 8

8) consenso:

prima di effettuare l'accesso l'utente deve acconsentire, caso per caso o una tantum:

allo scambio di informazioni tra OdA e FdS eventualmente necessarie ai fini della fornitura del servizio.

Condizione 9

9) controllo:

l'utente deve avere controllo della durata della connessione ad Internet e deve poterne verificare in ogni momento la sussistenza o la cessazione.

Implementazioni Allegati tecnici alle linee guida

- **IDEM**

Non si forniscono dettagli poiché è stato oggetto di uno specifico intervento

- **EDUROAM**

Non si forniscono dettagli poiché è stato oggetto di uno specifico intervento

Ultim'ora: Con o senza il Decreto Pisanu La licenza per il WiFi

Legge 31 luglio 2005, n. 155

"Conversione in legge, con modificazioni, del decreto-legge 27 luglio 2005, n. 144, recante misure urgenti per il contrasto del terrorismo internazionale"

Art. 7. Integrazione della disciplina amministrativa degli esercizi pubblici di telefonia e internet

1. A decorrere [...] e **fino al 31 dicembre 2007**, chiunque intende aprire un pubblico esercizio o un circolo privato di qualsiasi specie, nel quale sono posti a disposizione del pubblico, dei clienti o dei soci apparecchi terminali utilizzabili per le comunicazioni, anche telematiche, **deve chiederne la licenza al questore** [...]
2. Per coloro che già esercitano le attività di cui al comma 1, la licenza [...]
3. La licenza si intende rilasciata trascorsi [...] **Restano ferme le disposizioni** di cui al decreto legislativo 1° agosto 2003, n. 259, *nonche' le attribuzioni degli enti locali in materia.*

Ultim'ora: Con o senza il Decreto Pisanu Monitoraggio e identificazione

Legge 31 luglio 2005, n. 155

"Conversione in legge, con modificazioni, del decreto-legge 27 luglio 2005, n. 144, recante misure urgenti per il contrasto del terrorismo internazionale"

Art. 7. Integrazione della disciplina amministrativa degli esercizi pubblici di telefonia e internet

4. Con decreto [...] sono stabilite le misure che il titolare o il gestore di un esercizio in cui si svolgono le attività di cui al comma 1, è tenuto ad osservare per il **monitoraggio delle operazioni dell'utente e l'archiviazione dei relativi dati** [...] nonché le misure di **preventiva acquisizione di dati anagrafici** riportati su un documento di identità dei soggetti che utilizzano postazioni pubbliche non vigilate per comunicazioni telematiche ovvero punti di accesso ad Internet utilizzando tecnologia senza fili.
5. [...] il **controllo** sull'osservanza del decreto di cui al comma 4 e l'accesso ai relativi dati sono effettuati dall'organo del Ministero dell'interno preposto ai servizi di polizia postale e delle comunicazioni.

Ultim'ora: Con o senza il Decreto Pisanu Il Consiglio dei Ministri

Consiglio dei Ministri n. 113 del 05/11/2010

La Presidenza del Consiglio dei Ministri comunica:

Il Consiglio dei Ministri ha approvato un **decreto legge**, su proposta del Presidente del Consiglio, Silvio Berlusconi, e del Ministro dell'interno, Roberto Maroni, che contiene diverse disposizioni in materia di sicurezza pubblica [...] il Governo ha varato, tra le altre, le seguenti misure:

[...]

L'intervento del Governo in materia di sicurezza pubblica è stato completato e rafforzato da un **disegno di legge**, approvato su proposta del Ministro Maroni, che, fra l'altro:

[...]

- **in materia di accesso alla rete Wi-Fi: prevede il superamento delle restrizioni al libero accesso alla rete contenute nel cosiddetto "decreto Pisanu", mantenendo tuttavia adeguati standard di sicurezza.**

[...]

(Il testo del disegno di legge non è ancora disponibile)

Ultim'ora: Con o senza il Decreto Pisanu Le dichiarazioni

Dichiarazioni del Ministro:

- Liberalizzazione **dal primo gennaio 2011**
- **Superamento delle restrizioni** imposte dal decreto di cinque anni fa, che ora sono state **oltrepassate dall'evoluzione tecnologica**
- Liberalizzazione dei collegamenti Wi Fi attraverso gli smartphone o attraverso altri collegamenti offline **senza bisogno**, come succede oggi, **di preventivamente registrarsi con la fotocopia del documento d'identità**
- **Contemperamento delle esigenze** della libera diffusione del collegamento WiFi con quelle legate alla sicurezza e alle misure antiterrorismo

Dichiarazione del Procuratore Antimafia Grasso

- Credo che ci si debba rendere conto che **dietro questi internet point e queste reti wi-fi ci si possa nascondere benissimo** nella massa degli utenti non più identificabili. Si possono trovare anche terroristi, pedofili e mafiosi

Ultim'ora: Con o senza il Decreto Pisanu Cosa aspettarsi

Osservazioni:

- Si tratta di un **disegno di legge**, che a quanto mi risulta non ha ancora iniziato l'iter parlamentare.
- Il riferimento al **primo gennaio 2011** lascia intendere che non si tratti di un'abrogazione dell'articolo 7, che potrebbe avere decorrenza da qualsiasi momento, ma della **mancata proroga del comma 1**, l'unico ad avere un riferimento temporale.
- L'abrogazione in toto dell'Art. 7 del decreto Pisanu creerebbe un vuoto normativo che mal si concilia con il "mantenimento di adeguati standard di sicurezza".
- Il riferimento di Maroni all'evoluzione tecnologica che permetterebbe di superare il vincolo alla registrazione di un documento di identità, sembra alludere a soluzioni molto vicine alle linee guida del tavolo tecnico, che sono già ammesse dal ministero dell'interno.

Conclusioni:

- Non mi aspetto significative ricadute per le università
- Il termine liberalizzazione credo vada riferito alla mancata proroga dell'obbligo di licenza (comma 1 art. 7)
- Senz'altro liberalizzazione non significa quello che l'opinione pubblica si aspetta: wifi gratis per tutti