



Privacy, sicurezza autenticazione, profilazione

Cosa dice la legge

- Nel 2003 è stata emanata una legge (D. Lgs. **196/03**) che stabilisce le regole per la protezione dei dati personali
- Dal 2005 tutti i sistemi informatici italiani devono rispettare questa legge
- Le misure di sicurezza adottate devono essere riportate in un **D**ocumento **P**rogrammatico annuale sulla **S**icurezza (**DPS**)

Adempimenti richiesti dalla legge 196/03

- Censimento e aggiornamento dei trattamenti
- Lista degli incaricati
- **Gestione delle credenziali di autenticazione**
- **Password, token o dispositivi biometrici**
- **Protezione della sessione di lavoro**
- **Profilazione dei privilegi per l'accesso**
- Prevenzione vulnerabilità e correz. difetti del software
- Protezione dei supporti rimovibili
- Misure per assicurare integrità e disponibilità dei dati
- Salvataggio e ripristino dei dati
- Ripristino dei dati e sistemi salvati
- Difesa degli accessi abusivi
- Analisi dei rischi informatici
- Relazione di conformità dell'installatore
- Formazione specifica degli incaricati

La nascita di DSA

- Si è sentita la necessità di un unico sistema di Autenticazione/Autorizzazione per profilare tutte le risorse umane presenti in Ateneo (personale, studenti, collaboratori, ospiti...)
- Motivazioni:
 - Superare le difficoltà introdotte dall'esistenza di più anagrafiche e più metodi eterogenei per la gestione dell'accesso alle risorse informatiche
 - Applicare semplicemente politiche sicure nella gestione delle credenziali in ottemperanza a quanto previsto dal D.Lgs. 196/03
 - Favorire l'utente che deve ricordarsi solo una coppia di credenziali per accedere a più risorse.
- Queste esigenze hanno portato alla realizzazione di un **Directory Service d'Ateneo (DSA)**.

AlmaWelcome e DSA

- AlmaWelcome deve gestire due modalità di accesso:
 - **Non autenticata**: per persone ignota ai sistemi informativi UNIBO (chi si vuole immatricolare per la prima volta)
 - **Autenticata**: per persone già note ai sistemi universitari → in possesso di credenziali di autenticazione)
- Requisiti di fondo:
 - **Integrità del sistema**: non duplicare le anagrafiche
 - **Rispetto della privacy**: non mostrare dati personali in assenza di certezza sull'identità dell'utente

Pagina di accesso di AlmaWelcome

UNIVERSITÀ DI BOLOGNA
ALMAWELCOME!

Sei in: AlmaWelcome

Servizio AlmaWelcome!

1. Primo Accesso

Inserisci il tuo codice fiscale:

Accedi

Per l'iscrizione ad una prova di ammissione o ad un corso di studi (immatricolazione), **nel caso in cui non si possiede già uno username e una password**, inserire il codice fiscale e cliccare sul bottone **Accedi** del riquadro 1.

Sei uno studente **straniero** e non hai un codice fiscale? Puoi iscriverti alla prova con un [codice provvisorio](#).

2. Accesso Autenticato

Inserisci il tuo nome utente:

Inserisci la tua password:

Accedi

Se si è già in possesso di uno username e una password dell'Università di Bologna, inserirle nel riquadro e cliccare sul bottone **Accedi**.

[Non conosci username e/o password?](#)

Accesso non autenticato

- Lo studente che si vuole immatricolare e non è noto a sistemi dell'Ateneo deve poter accedere all'applicazione attraverso un apposito percorso
- Le esigenze di integrità e rispetto della privacy citate nella slide precedente hanno una conseguenza diretta:
 - Chi è già presente nei sistemi dell'Ateneo non deve potere entrare attraverso questo percorso
- **Problema:** come identificare in modo certo una persona
- **Soluzione:** ogni persona residente in Italia ha un possiede un codice che la identifica in modo univoco
 - Il **codice fiscale**

Struttura del codice fiscale

- Il codice fiscale è composto da 16 caratteri
- 3 caratteri ricavati dal cognome
- 3 caratteri ricavati dal nome
- 5 caratteri che contengono giorno mese e anno di nascita e sesso
- 4 caratteri con il codice del comune di nascita (o dello stato estero)
- Un carattere di checksum

	
CODICE FISCALE	RSS MRA 75D18 A944L
COGNOME	ROSSI
NOME	MARIO
LUOGO DI NASCITA	BOLOGNA
PROVINCIA	BO
DATA DI NASCITA	18/04/1975
SESSO	M

Cognome e nome

- Cognome
 - Si utilizzano la prima, seconda e terza consonante
 - Se non ci sono 3 consonanti si cominciano ad utilizzare le vocali (Mori viene codificato come MRO)
 - Se il cognome è più corto di 3 lettere vengono aggiunte delle X (Re viene codificato come REX)
- Nome
 - Si utilizzano prima, seconda e quarta consonante
 - Se non c'è una quarta consonante si usa la terza
 - Se non c'è nemmeno la terza si fa come per il cognome: vocali ed eventualmente aggiunta di X

Data di nascita e sesso

- L'anno di nascita viene rappresentato con 2 cifre
- Il mese con una lettera (non A,B,C... c'è una codifica particolare)
- Il giorno con 2 cifre
- Il sesso viene codificato con un "trucco" nel giorno di nascita
 - Per i maschi il giorno di nascita è compreso fra 1 e 31
 - Per le femmine è compreso fra 41 e 71
- Si risparmia un carattere (maggiore compattezza)

Comune/Nazione e checksum

- I comuni di nascita sono codificati con una lettera e 3 cifre
- Se la persona è nata all'estero si usa un codice di nazione che inizia sempre con Z
- Il checksum permette di evitare la maggior parte degli errori di battitura
- Viene calcolato con un algoritmo particolare che si basa sui primi 15 caratteri
- Quando si inserisce il codice si può verificarne la validità calcolando il checksum e verificando che corrisponda a quello digitato
- Si dice che il CF è **autovalidante**

Omocodie

- L'algoritmo di calcolo del CF garantisce una quasi unicità del codice ma non l'unicità in senso assoluto
- Per esempio se Mario Rossi è nato a Roma c'è una buona probabilità di collisione nel calcolo
- La presenza di due codici fiscali uguali viene definita **omocodia**, due persone con lo stesso codice vengono definite **omofiscali**
- Il codice fiscale viene attribuito dal ministero delle finanze e **non esistono due codici fiscali uguali**
 - In caso di omocodia alcune delle cifre nel codice vengono sostituite con lettere con una particolare regola che gestisce fino a 128 persone **omofiscali**

→ Il codice fiscale non deve mai essere calcolato, bisogna usare quello assegnato dal ministero

Uso corretto del CF

- Il Codice Fiscale non può essere calcolato ma può essere elaborato
 - Calcolo del checksum
 - Verifica di conformità di nome e cognome con i primi 6 caratteri
 - Estrazione di data di nascita, sesso e luogo di nascita
- Si può evitare di chiedere all'utente dati ricavabili dal CF
- Attenzione al fatto che **il CF è unico ma non immutabile**, può cambiare per diverse ragioni:
 - Errori del ministero
 - Variazioni legate ai doppi nomi
 - Cambi del cognome
 - Cambio di sesso

AlmaWelcome e CF

- Dopo aver chiesto il CF si fa una verifica che un utente non esiste già nel sistema
- Se esiste già viene invitato ad entrare in modo autenticato
- Infatti:
 - Non possiamo inserirlo una seconda volta nell'anagrafica (**integrità → no duplicazioni**)
 - Non abbiamo una certezza sulla sua identità: non possiamo consentirgli di vedere dati personali preesistenti (**privacy → riservatezza dei dati personali**)
- Se non esiste il sistema ricava dal CF data e luogo di nascita e sesso e verifica cognome e nome inseriti

Stranieri

- L'Ateneo di Bologna accoglie molti studenti stranieri
- Agli stranieri residenti o domiciliati stabilmente in Italia viene attribuito ufficialmente un codice fiscale
- Però ci sono studenti che vengono ad abitare a Bologna solo in seguito all'immatricolazione
- AlmaWelcome consente loro di fare l'intera iscrizione dal proprio paese d'origine
- In questi casi c'è la possibilità di calcolare un codice provvisorio che ha la stessa struttura del CF ma viene marcato come non ufficiale
- La prima volta che lo studente si reca in segreteria il sistema evidenzia questo fatto e lo studente deve fornire il CF ufficiale

CF provvisorio

UNIVERSITÀ DI BOLOGNA
ALMAWELCOME!

Immissione dati anagrafici per studenti stranieri

Attenzione: i dati immessi permetteranno il calcolo di un codice fiscale provvisorio **senza alcun valore legale** che verrà utilizzato per l'iscrizione.

I campi contrassegnati dal simbolo (*) sono obbligatori.

Nome (*)	<input type="text"/>
Cognome (*)	<input type="text"/>
Data di nascita (*)	<input type="text" value="01"/> <input type="text" value="gennaio"/> <input type="text" value="1989"/>
Sesso (*)	<input checked="" type="radio"/> Femmina <input type="radio"/> Maschio
Nazione di nascita (*)	<input type="text" value="Afghanistan"/>

<<Ritorna alla Home

Proseguì >>

Attribuzione delle credenziali

- Alla fine del percorso lo studente ottiene **credenziali** DSA (username e PUK)
 - Può scaricare un PDF che le contiene e stamparlo
 - Riceve via e-mail un messaggio di benvenuto che le riporta
- Usando le credenziali lo studente può rientrare in modo autenticato e svolgere un numero limitato di operazioni (ad esempio correggere eventuali errori nell'iscrizione)
- Le credenziali sono **provvisorie** e vengono rese definitive solo al completamento dell'immatricolazione dove viene verificata l'identità della persona

Username, PUK e password

- Lo username viene calcolato con un algoritmo
- Tipicamente cognome.nome:
mario.rossi@studio.unibo.it
- Se c'è un'omonimia si aggiunge una cifra in fondo:
mario.rossi2@studio.unibo.it
- Lo username completo comprende il "dominio" DSA (studio.unibo.it)
- Il sistema attribuisce un PUK che è noto sia allo studente che agli operatori autorizzati UNIBO ed è la password iniziale
- La legge sulla privacy prevede che **l'utente deve cambiare la password al primo ingresso** in modo che si nota solo a lui (la password viene memorizzata da DSA in modo da essere inaccessibile a tutti)
- **Il PUK non può essere più utilizzato**

Recupero delle credenziali

- Un utente può perdere o dimenticare le proprie credenziali
- Dal momento che la password è inaccessibile abbiamo una sola possibilità:
 - Resetare la password
 - Comunicare username e PUK all'utente
- L'utente entrerà con il PUK e gli verrà chiesto di impostare una nuova password
- Username e PUK possono essere ottenute in due modi:
 - Telefonando al servizio di assistenza
 - Utilizzare un servizio online che invia le credenziali via e-mail o SMS

Altre considerazioni su sicurezza e privacy

- La legge 196/03 prevede la protezione delle **sessioni**
→ AlmaWelcome lavora interamente in modalità sicura (protocollo HTTPS)