

# Documento descrittivo del processo di accreditamento degli utenti della SISSA

Le informazioni fornite in questo documento sono accurate alla data del 06/05/2013



## Sommario

Abbreviazioni.....	2
Gestore dell'accREDITamento .....	2
Utenti gestiti .....	2
Visione di insieme del processo di accREDITamento degli utenti .....	2
Il processo di accREDITamento per la categoria di utenti: personale tecnico/amm.vo a tempo det/indeterminato, ricercatori/ricercatori a contratto, personale docente.....	3
Il processo di accREDITamento per la categoria di utenti: studenti PhD, Postgraduate, Undergraduate .....	5
Il processo di accREDITamento per la categoria di utenti: studenti dei Master.....	7
Il processo di accREDITamento per la categoria di utenti: visitatori .....	9
Il processo di accREDITamento per la categoria di utenti: personale esterno.....	11
Il sistema di autenticazione e autorizzazione interno.....	13
Partecipazione ad altre federazioni .....	13

## Revisions

Data	Versione	Descrizione modifica	Autore
06/05/2013	1.0	Prima stesura	Ritossa M.

## Abbreviazioni

ITCS – Information Technology and Computing Services  
URU – Ufficio Risorse Umane  
ILAS – Interdisciplinary Laboratory for Advanced Studies)

## Gestore dell'accreditamento

L'accreditamento viene gestito da:

- Ufficio Risorse Umane per il personale tecnico-amministrativo nonché i docenti e ricercatori.
- Ufficio Economato e Patrimonio per il personale tecnico esterno (manutentori, guardie giurate,..) appartenenti a servizi dati in out-sourcing.
- Segreteria degli Studenti per gli studenti iscritti a PhD e Lauree.
- Segreteria ILAS per gli studenti dei Master
- Responsabili degli account di Area/Settore per gli ospiti visitatori.

Le identità digitali vengono create, mantenute ed eventualmente cancellate, unicamente dal Servizio Informatico della SISSA.

## Utenti gestiti

Categorie di utenti	Cardinalità	Affiliazione IDEM
Personale tecnico/amministrativo a tempo det./indet.	100	Staff, Member
Personale docente: <ul style="list-style-type: none"><li>- Professori</li><li>- Professori associati</li><li>- Assistenti</li><li>- Professori visitatori</li></ul>	50	Staff, Member
Ricercatori	10	Staff, Member
Collaboratori	15	Member
Executive	1	Staff, Member
Collaboratori esterni	10	Member
Personale esterno	10	Member
Fellowship Holder	20	Member
Studenti: <ul style="list-style-type: none"><li>- Studenti PhD</li><li>- Studenti Master</li><li>- Postgraduate</li><li>- Undergraduate</li></ul>	250	Student, Member
Postdoc	120	Member
Professori emeriti	1	Member
Visitatori	30	Affiliate

## Visione di insieme del processo di accreditamento degli utenti

Ogni utente è tenuto a compilare e sottoscrivere il modulo di richiesta di creazione account, in forma cartacea. La sottoscrizione del modulo presuppone l'aver letto ed accettato la "GARR AUP" (Acceptable Use Policy) e la "SISSA Network Computer Policy", oltre a rispettare le regole del documento RFC 1855 "Netiquette Guidelines". Assieme al modulo di account l'utente deve fornire una copia del documento di identità valido.

La base dati utenti viene conservata sia su server LDAP che AD. La gestione delle credenziali viene gestita tramite script a linea di comando. I servizi web, per l'autenticazione, si appoggiano principalmente al server LDAP (utilizzano l'AD solo dove non è possibile fare altrimenti). Gli utenti utilizzano le proprie credenziali per accedere alle workstation ed ai servizi messi a disposizione dalla Scuola, compreso l'accesso alla rete wireless e wired (IEEE 802.1x) con i laptop personali.

## **Il processo di accreditamento per la categoria di utenti:**

- **Personale tecnico/amministrativo a tempo det./indet.**
- **Ricercatori / Ricercatori a contratto**
- **Personale docente**

## **Il processo**

L'URU presenta all'ITCS il modulo di richiesta creazione dell'identità digitale. Lo stesso URU notifica all'ITCS eventuali variazioni sulla scadenza del contratto del personale tecnico/amministrativo.

## **Modalità di riconoscimento della persona**

Al momento dell'assunzione viene fatto compilare e sottoscrivere il modulo cartaceo di richiesta creazione account. Il modulo, completo di copia di documento di identità viene quindi fatto recapitare all'ITCS che si occupa di creare l'account per l'accesso alle macchine ed ai servizi della Scuola. Il modulo quindi viene archiviato.

## **Caratteristiche dell'identità digitale**

Attributi associati all'identità: nome, cognome, email, matricola, telefono, ufficio, numero fax, foto, unità organizzativa di appartenenza, categoria di impiego.

Attributi pubblici: nome, cognome, email, telefono, unità organizzativa di appartenenza.

## **Gestione del ciclo di vita**

L'URU comunica all'ITCS eventuali modifiche contrattuali rilevanti inerenti il mantenimento/estensione/rimozione dell'identità. L'ITCS di conseguenza procede ad aggiornare il server LDAP.

## **Formato e regole delle credenziali**

Le credenziali fornite sono del tipo userID/password e durano fino alla scadenza del contratto di lavoro. La userID è sempre formata da 8 caratteri alfanumerici. Tipicamente è composta dai primi 8 caratteri del cognome, tuttavia, in caso di collisione, alla più recente vengono aggiunte le prime lettere del nome.

Al fine di garantire la privacy e la riservatezza dei dati personali, agli utenti viene consigliato di cambiare la password secondo le direttive delle leggi vigenti.

## **Eventuale presenza di credenziali multiple per la stessa persona**

Il rilascio di ulteriori credenziali all'utente è subordinato a particolari tipologie di richieste come ad esempio creazione di account di riferimento in occasione di seminari/eventi.

È altresì possibile che l'utente abbia a disposizione delle credenziali temporanee del tipo userID/password con userID nella forma "id\*\*\*\*\*" in concomitanza con seminari ed eventi in genere. Le suddette credenziali vengono utilizzate esclusivamente per accedere via rete all'esterno della Scuola in una modalità totalmente disconnessa dalla intranet della Scuola.

### **Modalità di consegna delle credenziali**

Le credenziali vengono definite dall'utente al momento della compilazione del modulo di richiesta account. In caso di problematiche relative alla userID e/o alla password, la risoluzione viene definita a voce, di persona. Le password in ogni caso, non vengono MAI comunicate via email.

### **Modalità di recupero delle credenziali smarrite**

Per recuperare le credenziali smarrite l'utente deve rivolgersi all'ITCS che provvede a resettare la password o a comunicare la userID dimenticata.

### **Modalità di gestione smarrimento smartcard/token**

Non previsto.

### **Durata dell'accreditamento**

L'accreditamento ha validità fino alla conclusione di qualsiasi tipo di relazione lavorativa con la Scuola.

### **Disabilitazione utente**

L'utente viene automaticamente disabilitato una volta raggiunta la data di scadenza definita nel modulo di richiesta account. Il periodo di validità può essere ridotta in caso di dimissioni.

### **Cancellazione definitiva utente**

L'identità digitale viene automaticamente e definitivamente rimossa dai server LDAP dopo 6 mesi dalla data di disabilitazione. Tuttavia esiste la possibilità di recuperare l'identità qualora si venisse ad istituire un nuovo rapporto di collaborazione (anche a distanza di anni) tra l'utente titolare dell'identità digitale e la Scuola.

### **Rischi specifici associati alla categoria di utenti**

Nulla di particolare.

### **Interoperabilità tra credenziali deboli (username+pwd) ed eventuali credenziali forti (smartcard)**

Non previsto.

## **Il processo di accreditamento per la categoria di utenti:**

- **Studenti PhD**
- **Postgraduate**
- **Undergraduate**

### **Il processo**

La segreteria studenti presenta all'ITCS il modulo di richiesta creazione dell'identità digitale. Eventuali variazioni sulla scadenza dell'account o variazione di unità di appartenenza vengono comunicati dal responsabile per gli account dell'Area di appartenenza dello studente.

### **Modalità di riconoscimento della persona**

Allo studente che si presenta per la prima volta alla segreteria degli studenti, viene fatto compilare e sottoscrivere il modulo cartaceo di richiesta apertura account. Il modulo, completo di copia di documento di identità viene quindi fatto recapitare all'ITCS che si occupa di creare l'account per l'accesso alle macchine ed ai servizi della Scuola. Il modulo viene quindi archiviato.

### **Caratteristiche dell'identità digitale**

Attributi associati all'identità: nome, cognome, email, matricola, telefono, ufficio, numero fax, foto, unità organizzativa di appartenenza, categoria di impiego.

Attributi pubblici: nome, cognome, email, telefono, unità organizzativa di appartenenza.

### **Gestione del ciclo di vita**

Il responsabile dell'unità organizzativa alla quale lo studente appartiene, comunica all'ITCS eventuali modifiche inerenti il mantenimento/estensione/rimozione dell'identità. L'ITCS di conseguenza procede ad aggiornare il server LDAP.

### **Formato e regole delle credenziali**

Le credenziali fornite sono del tipo userID/password e durano fino alla scadenza del contratto di lavoro. La userID è sempre formata da 8 caratteri alfanumerici. Tipicamente è composta dai primi 8 caratteri del cognome, tuttavia, in caso di collisione, alla più recente vengono aggiunte le prime lettere del nome.

Al fine di garantire la privacy e la riservatezza dei dati personali, agli utenti viene consigliato di cambiare la password almeno ogni 6 mesi.

### **Eventuale presenza di credenziali multiple per la stessa persona**

Il rilascio di ulteriori credenziali all'utente è subordinato a particolari tipologie di richieste come ad esempio creazione di account di riferimento in occasione di seminari/eventi e solo su espressa richiesta del responsabile dell'unità organizzativa di appartenenza.

### **Modalità di consegna delle credenziali**

Le credenziali vengono definite dall'utente al momento della compilazione del modulo di richiesta account. In caso di problematiche relative alla userID e/o alla password, la risoluzione viene definita a voce, di persona. Le password in ogni caso, non vengono MAI comunicate via email.

### **Modalità di recupero delle credenziali smarrite**

Per recuperare le credenziali smarrite l'utente deve rivolgersi all'ITCS che provvede a resettare la password o a comunicare la userID dimenticata.

### **Modalità di gestione smarrimento smartcard/token**

Non previsto.

### **Durata dell'accREDITamento**

L'accREDITamento ha validità fino alla conclusione del periodo di studi. La validità può essere ridotta in caso di rinuncia o estesa in caso di specifica richiesta da parte del responsabile dell'unità organizzativa.

### **Disabilitazione utente**

L'utente viene automaticamente disabilitato una volta raggiunta la data di scadenza definita nel modulo di richiesta account, e se non è pervenuta nessuna richiesta di estensione del periodo di validità.

### **Cancellazione definitiva utente**

L'identità digitale viene automaticamente e definitivamente rimossa dai server LDAP dopo 6 mesi dalla data di disabilitazione. Tuttavia esiste la possibilità di recuperare l'identità qualora si venisse ad istituire un nuovo rapporto di collaborazione (anche a distanza di anni) tra l'utente titolare dell'identità digitale e la Scuola.

### **Rischi specifici associati alla categoria di utenti**

Nulla di particolare

### **Interoperabilità tra credenziali deboli (username+pwd) ed eventuali credenziali forti (smartcard)**

Non previsto

## **Il processo di accreditamento per la categoria di utenti:**

### **- Studenti dei Master**

#### **Il processo**

La segreteria ILAS presenta all'ITCS il modulo di richiesta creazione dell'identità digitale. Eventuali variazioni sulla scadenza dell'account o variazione di unità di appartenenza vengono comunicati dalla segreteria ILAS.

#### **Modalità di riconoscimento della persona**

Allo studente che si presenta per la prima volta alla segreteria ILAS, viene fatto compilare e sottoscrivere il modulo cartaceo di richiesta apertura account. Il modulo, completo di copia di documento di identità viene quindi fatto recapitare all'ITCS che si occupa di creare l'account per l'accesso alle macchine ed ai servizi della Scuola. Il modulo quindi viene archiviato.

#### **Caratteristiche dell'identità digitale**

Attributi associati all'identità: nome, cognome, email, matricola, telefono, ufficio, numero fax, foto, unità organizzativa di appartenenza, categoria di impiego.

Attributi pubblici: nome, cognome, email, telefono, unità organizzativa di appartenenza.

#### **Gestione del ciclo di vita**

La segreteria ILAS comunica all'ITCS eventuali modifiche contrattuali rilevanti inerenti il mantenimento/estensione/rimozione dell'identità. L'ITCS di conseguenza procede ad aggiornare il server LDAP.

#### **Formato e regole delle credenziali**

Le credenziali fornite sono del tipo userID/password e durano fino alla scadenza del contratto di lavoro. La userID è sempre formata da 8 caratteri alfanumerici. Tipicamente è composta dai primi 8 caratteri del cognome, tuttavia, in caso di collisione, alla più recente vengono aggiunte le prime lettere del nome.

Al fine di garantire la privacy e la riservatezza dei dati personali, agli utenti viene consigliato di cambiare la password secondo le direttive delle leggi vigenti.

#### **Eventuale presenza di credenziali multiple per la stessa persona**

Non previsto.

#### **Modalità di consegna delle credenziali**

Le credenziali vengono definite dall'utente al momento della compilazione del modulo di richiesta account. In caso di problematiche relative alla userID e/o alla password, la risoluzione viene definita a voce, di persona. Le password in ogni caso, non vengono MAI comunicate via email.

#### **Modalità di recupero delle credenziali smarrite**

Per recuperare le credenziali smarrite lo studente deve rivolgersi all'ITCS che provvede a resettare la password o a comunicare la userID dimenticata.

#### **Modalità di gestione smarrimento smartcard/token**

Non previsto.

#### **Durata dell'accREDITamento**

L'accREDITamento ha validità fino alla conclusione del periodo di studi. La validità può essere ridotta in caso di rinuncia o estesa in caso di specifica richiesta da parte della segreteria ILAS.

### **Disabilitazione utente**

L'utente viene automaticamente disabilitato una volta raggiunta la data di scadenza definita nel modulo di richiesta account e se non è pervenuta nessuna richiesta di estensione del periodo di validità.

### **Cancellazione definitiva utente**

L'identità digitale viene automaticamente e definitivamente rimossa dai server LDAP dopo 6 mesi dalla data di disabilitazione. Tuttavia esiste la possibilità di recuperare l'identità qualora si venisse ad istituire un nuovo rapporto di collaborazione (anche a distanza di anni) tra l'utente titolare dell'identità digitale e la Scuola.

### **Rischi specifici associati alla categoria di utenti**

Nulla di particolare

### **Interoperabilità tra credenziali deboli (username+pwd) ed eventuali credenziali forti (smartcard)**

Non previsto



## **Il processo di accreditamento per la categoria di utenti:**

### **- Visitatori**

#### **Il processo**

Il responsabile dell'Area fornisce all'ITCS il modulo di richiesta creazione dell'identità digitale. Eventuali variazioni sulla scadenza dell'account o variazione di unità di appartenenza vengono comunicati dal responsabile stesso.

#### **Modalità di riconoscimento della persona**

All'ospite/visitatore, viene fatto compilare e sottoscrivere il modulo cartaceo di richiesta apertura account. Il modulo, completo di copia di documento di identità viene quindi fatto recapitare all'ITCS che si occupa di creare l'account per l'accesso alle macchine ed ai servizi della Scuola. Il modulo quindi viene archiviato.

#### **Caratteristiche dell'identità digitale**

Attributi associati all'identità: nome, cognome, email, matricola, telefono, ufficio, numero fax, foto, unità organizzativa di appartenenza, categoria di impiego.

Attributi pubblici: nome, cognome, email, telefono, unità organizzativa di appartenenza.

#### **Gestione del ciclo di vita**

Il responsabile comunica all'ITCS eventuali modifiche inerenti mantenimento/estensione/rimozione dell'identità. L'ITCS di conseguenza procede ad aggiornare il server LDAP.

#### **Formato e regole delle credenziali**

Le credenziali fornite sono del tipo userID/password e durano fino alla scadenza del contratto di lavoro. La userID è sempre formata da 8 caratteri alfanumerici. Tipicamente è composta dai primi 8 caratteri del cognome, tuttavia, in caso di collisione, alla più recente vengono aggiunte le prime lettere del nome.

Al fine di garantire la privacy e la riservatezza dei dati personali, agli utenti viene consigliato di cambiare la password secondo le direttive delle leggi vigenti.

#### **Eventuale presenza di credenziali multiple per la stessa persona**

Non previsto

#### **Modalità di consegna delle credenziali**

Le credenziali vengono definite dall'utente al momento della compilazione del modulo di richiesta account. In caso di problematiche relative alla userID e/o alla password, la risoluzione viene definita a voce, di persona. Le password in ogni caso, non vengono MAI comunicate via email.

#### **Modalità di recupero delle credenziali smarrite**

Per recuperare le credenziali smarrite l'utente deve rivolgersi all'ITCS che provvede a resettare la password o a comunicare la userID dimenticata.

#### **Modalità di gestione smarrimento smartcard/token**

Non previsto.

#### **Durata dell'accREDITamento**

L'accREDITamento ha validità fino alla conclusione del periodo di visita. La validità può essere ridotta in caso in cui l'ospite lasci prima la Scuola, o estesa se richiesto dal responsabile dell'Area.

### **Disabilitazione utente**

L'utente viene automaticamente disabilitato una volta raggiunta la data di scadenza definita nel modulo di richiesta account e se non è pervenuta nessuna richiesta di estensione del periodo di validità.

### **Cancellazione definitiva utente**

L'identità digitale viene automaticamente e definitivamente rimossa dai server LDAP dopo 6 mesi dalla data di disabilitazione. Tuttavia esiste la possibilità di recuperare l'identità qualora l'utente si ripresentasse in veste di ospite/visitatore o altro.

### **Rischi specifici associati alla categoria di utenti**

Nulla di particolare

### **Interoperabilità tra credenziali deboli (username+pwd) ed eventuali credenziali forti (smartcard)**

Non previsto

## **Il processo di accreditamento per la categoria di utenti:**

### **- Personale esterno**

#### **Il processo**

L'Ufficio Economato e Patrimonio fornisce all'ITCS il modulo di richiesta creazione dell'identità digitale. Eventuali variazioni sulla scadenza dell'account o variazione di unità di appartenenza vengono comunicati da una persona autorizzata, appartenente alla stessa unità organizzativa.

#### **Modalità di riconoscimento della persona**

Al personale esterno che si presenta per la prima volta alla segreteria degli studenti, viene fatto compilare e sottoscrivere il modulo cartaceo di richiesta apertura account. Il modulo, completo di copia di documento di identità viene quindi fatto recapitare all'ITCS che si occupa di creare l'account per l'accesso alle macchine ed ai servizi della Scuola.

#### **Caratteristiche dell'identità digitale**

Attributi associati all'identità: nome, cognome, email, matricola, telefono, ufficio, numero fax, foto, unità organizzativa di appartenenza, categoria di impiego.

Attributi pubblici: nome, cognome, email, telefono, unità organizzativa di appartenenza.

#### **Gestione del ciclo di vita**

Il responsabile dell'Ufficio Economato e Patrimonio comunica all'ITCS eventuali modifiche contrattuali rilevanti inerenti il mantenimento/estensione/rimozione dell'identità. L'ITCS di conseguenza procede ad aggiornare il server LDAP.

#### **Formato e regole delle credenziali**

Le credenziali fornite sono del tipo userID/password e durano fino alla scadenza del contratto di lavoro. La userID è sempre formata da 8 caratteri alfanumerici. Tipicamente è composta dai primi 8 caratteri del cognome, tuttavia, in caso di collisione, alla più recente vengono aggiunte le prime lettere del nome.

Al fine di garantire la privacy e la riservatezza dei dati personali, agli utenti viene consigliato di cambiare la password secondo le direttive delle leggi vigenti.

#### **Eventuale presenza di credenziali multiple per la stessa persona**

Il rilascio di ulteriori credenziali all'utente è subordinato a particolari tipologie di richieste come ad esempio creazione di account di riferimento in occasione di seminari/eventi e solo su espressa richiesta del responsabile dell'unità organizzativa.

#### **Modalità di consegna delle credenziali**

Le credenziali vengono definite dall'utente al momento della compilazione del modulo di richiesta account. In caso di problematiche relative alla userID e/o alla password, la risoluzione viene definita a voce, di persona. Le password in ogni caso, non vengono MAI comunicate via email.

#### **Modalità di recupero delle credenziali smarrite**

Per recuperare le credenziali smarrite l'utente deve rivolgersi all'ITCS che provvede a resettare la password o a comunicare la userID dimenticata.

#### **Modalità di gestione smarrimento smartcard/token**

Non previsto.

### **Durata dell'accreditamento**

L'accreditamento ha validità fino alla conclusione del periodo di studi. La validità può essere ridotta in caso di dimissioni o estesa in caso di specifica richiesta da parte del responsabile dell'unità organizzativa.

### **Disabilitazione utente**

L'utente viene automaticamente disabilitato una volta raggiunta la data di scadenza definita nel modulo di richiesta account, e non è pervenuta nessuna richiesta di estensione del periodo di validità.

### **Cancellazione definitiva utente**

L'identità digitale viene automaticamente e definitivamente rimossa dai server LDAP dopo 6 mesi dalla data di disabilitazione. Tuttavia esiste la possibilità di recuperare l'identità qualora si venisse ad istituire un nuovo rapporto di collaborazione (anche a distanza di anni) tra l'utente titolare dell'identità digitale e la Scuola.

### **Rischi specifici associati alla categoria di utenti**

Nulla di particolare

### **Interoperabilità tra credenziali deboli (username+pwd) ed eventuali credenziali forti (smartcard)**

Non previsto

## **Il sistema di autenticazione e autorizzazione interno**

Tutti i servizi interni utilizzano un sistema di autenticazione basato su LDAP (ed AD, laddove non sia possibile utilizzare LDAP). Al momento i servizi della Scuola non utilizzano il single sign-on. Ciò non esclude che in futuro ci possa essere una migrazione di più servizi possibile verso una autenticazione di tipo SSO.

## **Partecipazione ad altre federazioni**

La SISSA partecipa alla Federazione Eduroam.

