

Workflow creazione account



Workshop CCR
La Biodola Isola d'Elba
17 maggio 2016



Enrico M.V. Fasanelli
R. Cecchini, F. Serafini, M. Serra

Agenda

- Workflow creazione account
- Presa visione ed accettazione disciplinare per i nuovi utenti



Identità Digitali & account I

- Il flusso logico “naturale” di assegnazione di un account ad una Identità Digitale dovrebbe essere:
 - Registrazione Identità Digitale
 - Assegnazione di un account locale e sua registrazione in AAI
protoserv2/userserv@godiva.infn.it
 - entry LDAP ramo di sede → entry LDAP ramo nazionale
 - uid locale → uid nazionale

Identità Digitali & account II

- Succede spesso che tale flusso sia invertito (per esigenze varie)
 - entry LDAP di sede rimane “orfana” → uid solo locale
 - Strumenti per “riordinare” le cose
`godivacli --sfp <CodiceFiscale>`
- Succede anche che tale flusso non sia completato dall’assegnazione di un account locale
 - entry LDAP nazionale → uid “temporanea”

Certificazione degli account



- Ogni account deve essere collegato ad una ID registrata in GODiVA ed ogni ID registrata in GODiVA deve corrispondere ad una persona che sia rintracciabile/tracciabile.
- A seconda del livello di tracciabilità di una ID possono essere definiti un certo numero di Livelli di Confidenza relativi alla veridicità dei dati registrati

Account, ID & LoA



- Ogni account relativo ad una ID registrata in GODiVA è caratterizzato da un Level of Assurance (LoA) definito in modo compatibile con SPID e con ISO/IEC29115
 - LoA0 → LoA1 dell'ISO-IEC 29115 (Little or no confidence in the asserted identity)
 - - LoA1 → LoA2 dell'ISO-IEC 29115 → livello 1 SPID



ID & ACCOUNT OGGI

Registrazione Autenticata

- La registrazione di una nuova Identità Digitale effettuata da un utente autenticato via INFN-AAI (qualunque segreteria di qualunque ufficio) NON genera automaticamente un account.
- In questo caso l'assegnazione di un account è a cura dei servizi calcolo.
 - Se effettuata successivamente alla definizione della ID, la UID viene riportata automaticamente anche nel ramo nazionale
 - Altrimenti è necessario eseguire manualmente una sincronia, una volta che viene registrata la ID

Auto-Registrazione



- L'utente si auto-registra indicando un referente INFN (filtro su e-mail infn.it)
- Il referente riceve una e-mail con la richiesta di conferma della Identità del registrando
- Se il referente conferma, il sistema genera una UID "temporanea" (NCxxxxxx) ed invia all'utente un mail con le istruzioni per definire la propria password
- L'assegnazione di un account locale con UID "normale" richiede che la UID temporanea venga cancellata via GODiVA-GUI

ID & ACCOUNT DOMANI

Presenza visione ed accettazione del
disciplinare

Nuovo flusso Registrazione ID

- Unico flusso di registrazione
 - Autenticata
 - Identità ed account con LoA 1
 - Auto-registrazione
 - Identità ed account con LoA 0 fino a certificazione identità (coerenza tra dati inseriti)
 - certificazione account solo da “staff” (Dipendenti, Associati con incarico di ricerca)
- Generata sempre una UID temporanea (NCxxxxxx)
- La registrazione di un account locale con UID “normale” sostituirà la UID temporanea con quella locale ed avviserà l’utente (via e-mail)
 - → scriptable via protoserv/userserv

Modifiche auto-registrazione I

- I nuovi utenti dovranno
 - Inserire i propri dati personali
 - Indicare la(le) risorsa(e) informatica(che) a cui vuole accedere o la conferenza a cui intendono partecipare
 - Se risorsa
 - Inserire una copia del documento di riconoscimento
 - Prendere visione ed accettare il disciplinare
 - Indicare un referente interno, che sarà definito per ogni gruppo sperimentale e struttura dal Direttore (vedi talk Bovo-Ronconi)
 - Suggerimenti (default)
 - sigla/esperimento → responsabile locale
 - servizi → staff del servizio
 - dipartimento → da definire

Modifiche auto-registrazione II

- Il sistema genera una username temporanea (NCxxxxxx), assegna all'ID un valore LoA0 ed invia al registrando le informazioni per assegnare una password a tale username temporanea
- Un account di questo tipo (NCxxxxxx & LoA0) permetterà soltanto l'accesso a selezionati servizi web (come agenda.infn.it) ai quali chiunque deve poter accedere (per esempio per registrazione a conferenze)

Modifiche auto-registrazione III

- Se il registrando ha richiesto accesso a risorse informatiche, il referente
 - riceve una mail contenente il link che gli permette di visionare il documento di riconoscimento ed i dati inseriti;
 - verifica che i dati inseriti siano coerenti con quanto ripostato il documento e quindi
 - “certifica” l’anagrafica
 - approva la richiesta di uso delle risorse informatiche
- A questo punto la ID diventa LoA1

Modifiche auto-registrazione III

- Se il registrando ha indicato di volersi semplicemente registrare ad una conferenza, la sua ID rimane LoA0 fino a quando non si reca fisicamente presso la segreteria della conferenza, che potrà effettuare il riconoscimento de-visu e quindi attivare l'utilizzo delle risorse informatiche portando l'ID ed il relativo account a LoA1

Workflow creazione account



Workshop CCR
La Biodola Isola d'Elba
17 maggio 2016



Enrico M.V. Fasanelli
R. Cecchini, F. Serafini, M. Serra