Identity Management 10 anni dopo

Agenda

- Provisioning e ciclo di vita dell'identità digitale
- Sviluppo strumenti di gestione
- Esistono buone pratiche condivisibili?

Accreditamento

Ambiente universitario: all'inizio avevamo quasi esclusivamente **studenti**, **personale** e qualche **ospite**...

Strategie tradizionali di creazione degli account:

- manuale (duplicazione dati)
- importazione da DB (sincronizzazione)

Accreditamento

Possibile soluzione: **pre e auto accreditamento**

- account indipendenti da posizione nell'ente
- self-provisioning
- perfezionamento di fronte a *pubblico ufficiale* (LOA)

  ...ma

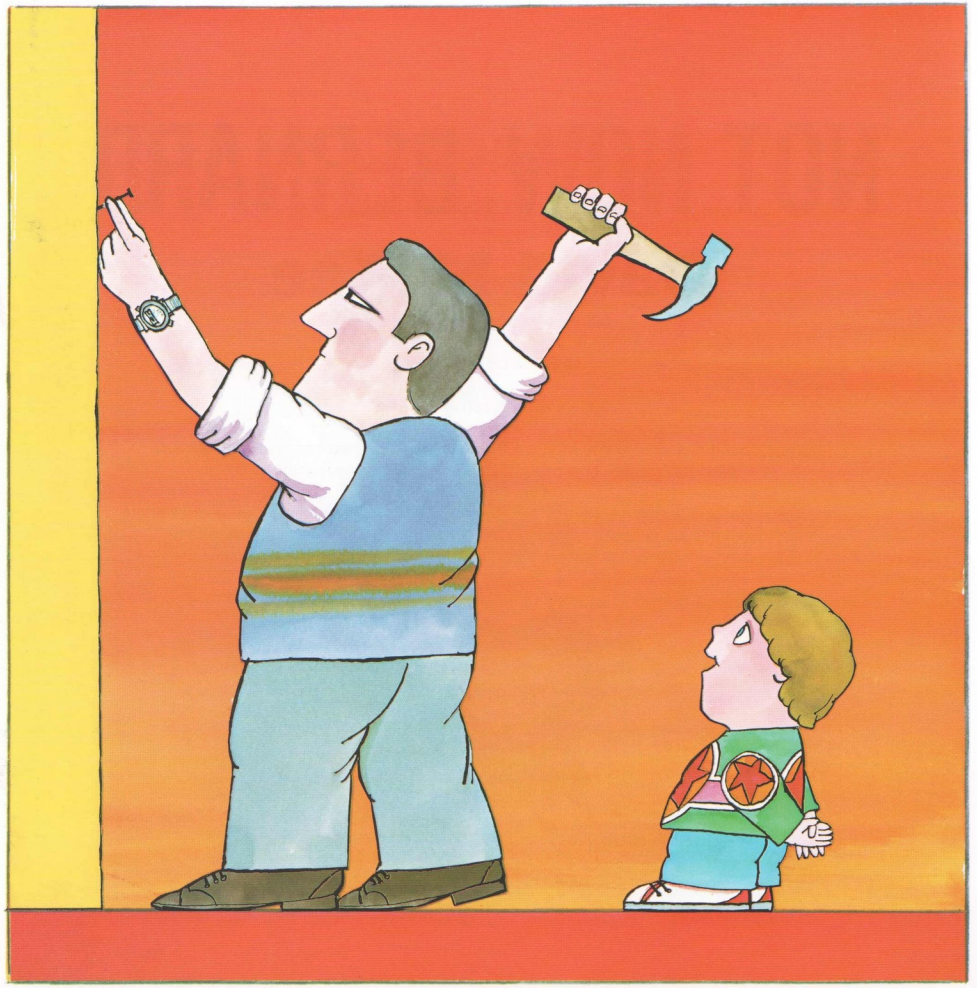
- quale strato di persistenza?

Evoluzione

Due storie paradigmatiche:

- Not now, Bernard (David McKee)
- Den grimme ælling (Il brutto anatroccolo, Hans Christian Andersen)

Evoluzione: Not now, Bernard



''Hello, Dad,'' said Bernard.

''Not now, Bernard,'' said his father.

Copyright David McKee 1980

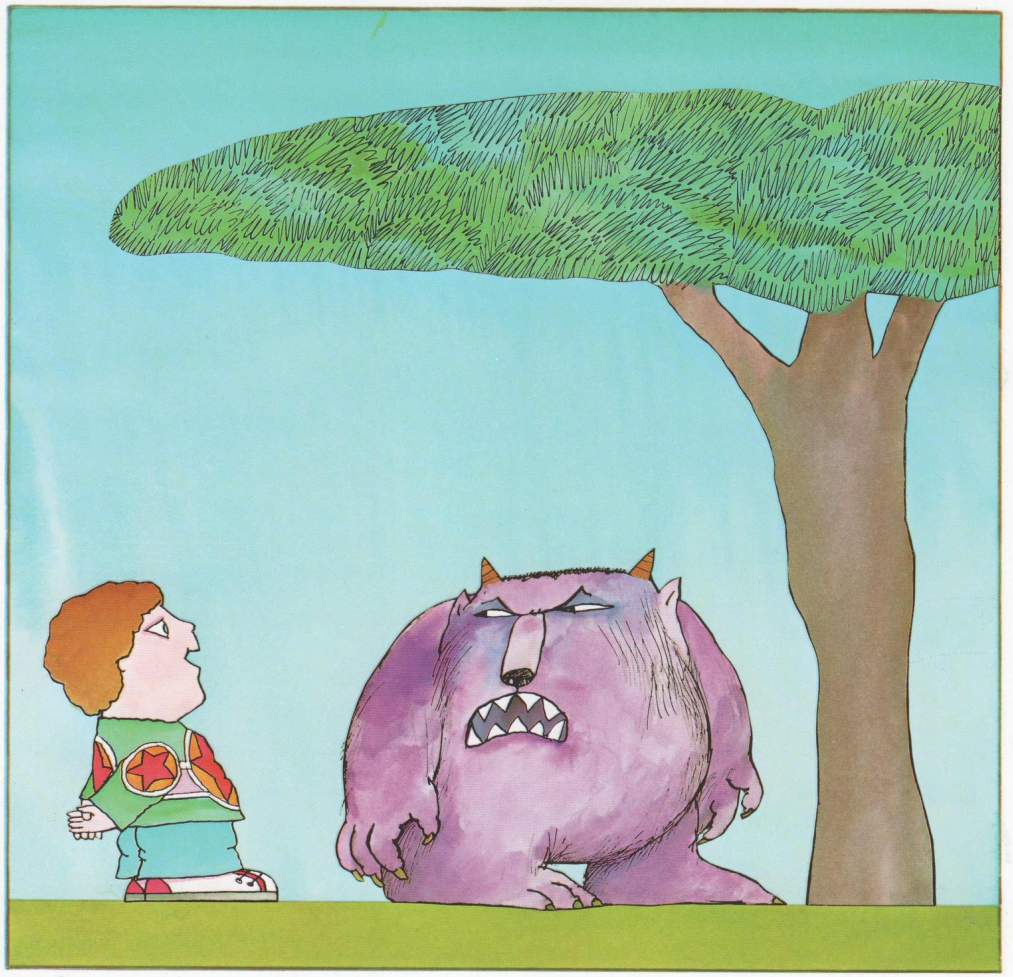
Evoluzione: Not now, Bernard

"There's a monster in the garden and it's going to eat me," said Bernard.

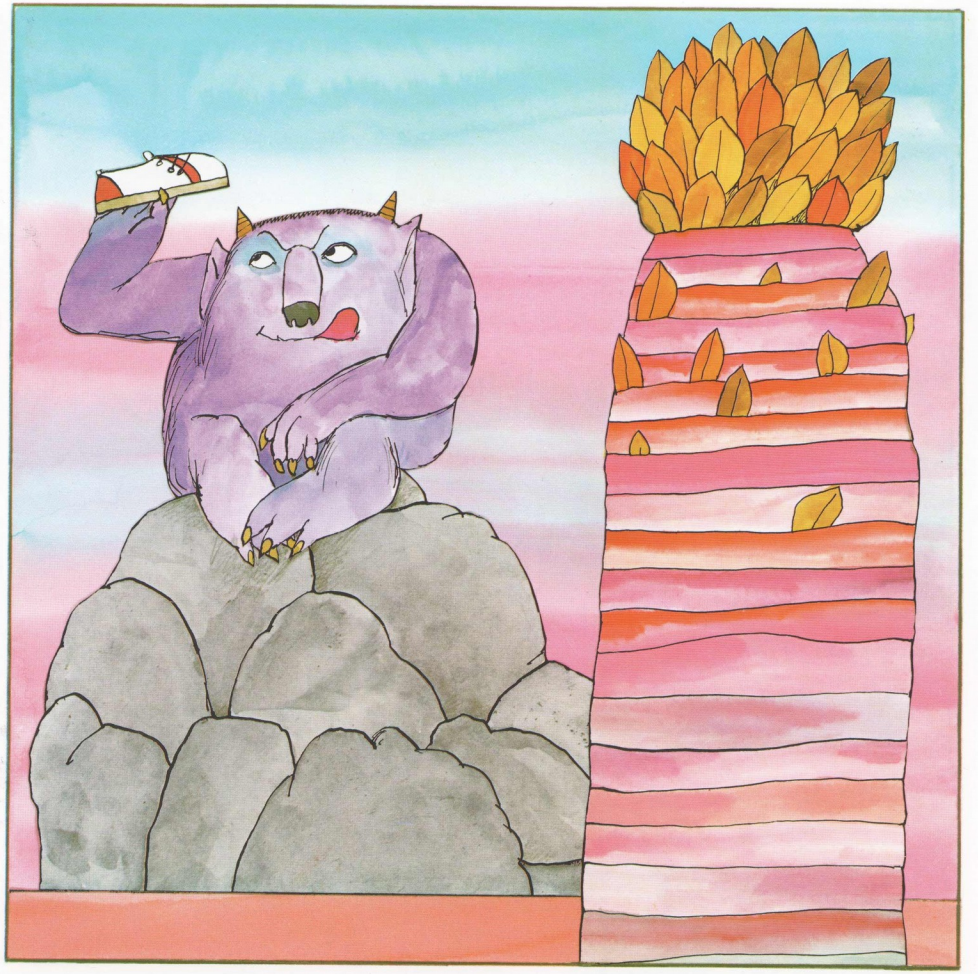
"Not now, Bernard," said his mother.

Copyright David McKee 1980

Evoluzione: Not now, Bernard



"Hello, monster," he said to the monster.



The monster ate Bernard up, every bit.

Evoluzione: Not now, Bernard

''But I'm a monster,'' said the monster.

''Not now, Bernard,'' said Bernard's mother.

Copyright David McKee 1980

Evoluzione

Cosa succede se non prestiamo attenzione alle nostre identità digitali:

- Senescenza
- Indigestione di attributi
- Modifiche organizzative
- Passaggi di ruolo

Evoluzione: il brutto anatroccolo

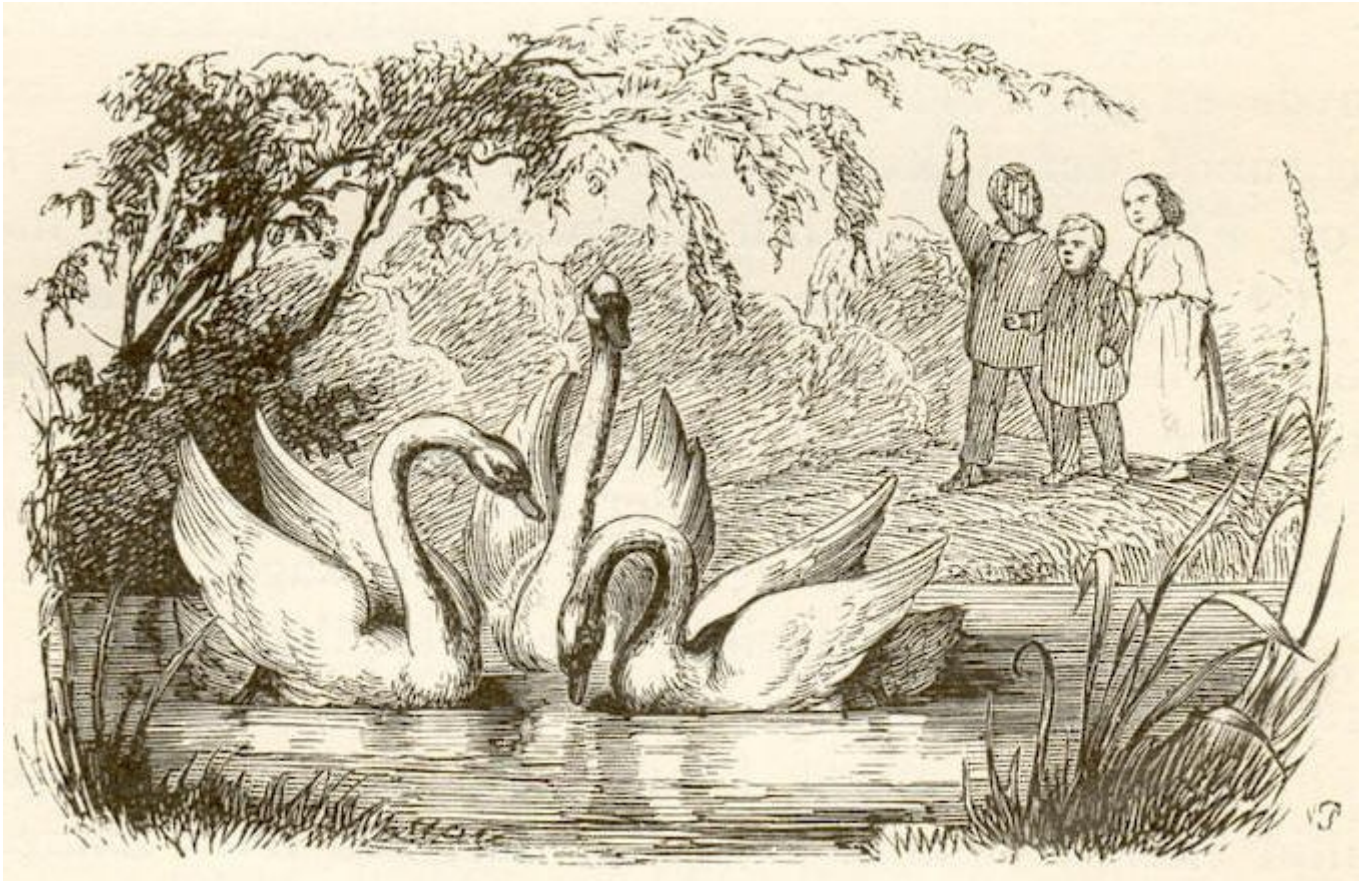


Illustrazione di Vilhelm Pedersen

Evoluzione

Utenti accreditati come **ospiti**, **contrattisti temporanei**, **ecc** da un giorno all'altro diventano utenti strutturati:

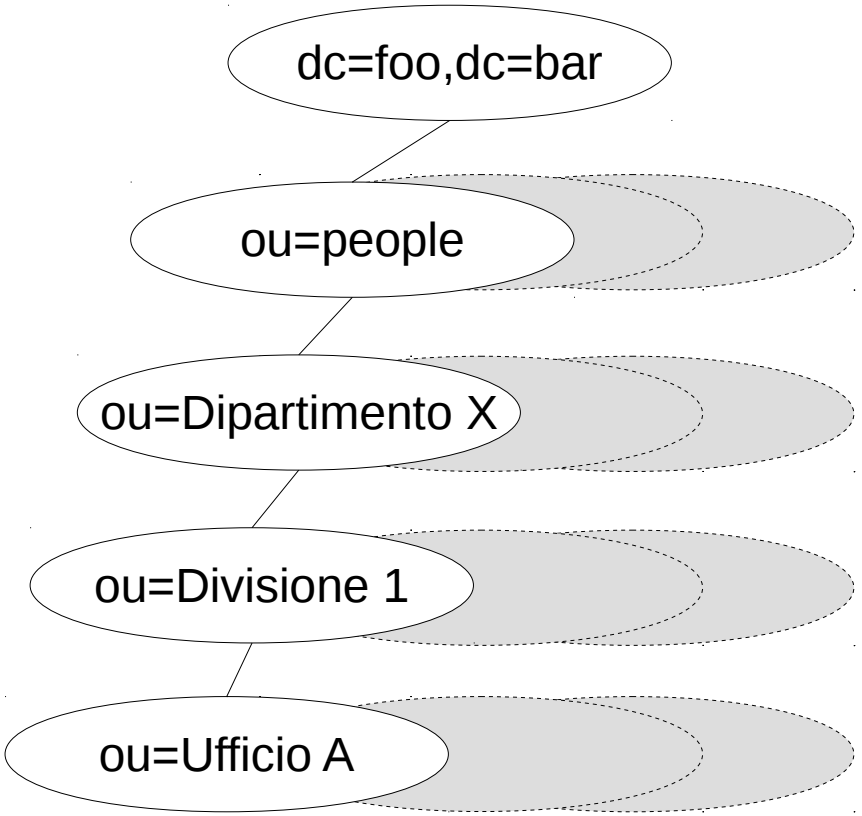
- Account ancora valido? (regole di naming)
- Servizi attivati sul profilo *minore* da migrare
- Chiavi di collegamento con il profilo strutturato (codice fiscale)

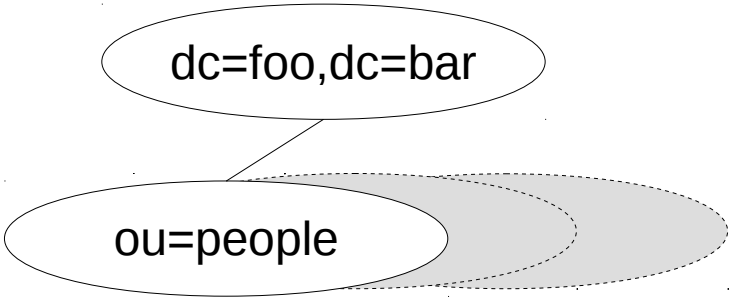
Strategie

- Evitare le forti dipendenze (tight coupling)
- Attenzione al Data model
- Minimizzare la duplicazione

In pratica... dipendenze

Directory Information Tree





Complesso vs Semplice: a quali esigenze deve rispondere il DIT?

Data model

Modellare entità complesse:

- Affiliazioni multiple nello stesso ente
- Più ruoli in ambiti diversi dello stesso ente

-> una possibile soluzione: URN

schacPersonalPosition

```
urn:schac:personalPosition:foo:bar:DivisioneX:RuoloA
urn:schac:personalPosition:foo:bar:DivisioneY:RuoloB
```

Duplicazione

Innocua (o quasi):

- Dati anagrafici (sincronizzazione)

Pericolosa (e molto):

- Dati propri del dominio del DB/Applicazione (ad esempio iscrizione ad un corso)

Duplicazione

Super Shibboleth

Se dobbiamo utilizzare dati provenienti dalla Directory e da un DB relazionale possiamo utilizzare più **connector** (LDAP data connector + relational database connector)

http://www.shibboleth4kids.com/heroes/mr-shibboleth

...se solo potessi

usare Shibboleth anche per alimentare le mie mailing list...

Shibboleth + ECP + script/tools =~

meta-directory

Sviluppo strumenti di gestione

Perchè dovrei?

(Directory and LOCAL_DB and TONS_OF_SCRIPTS and Shibboleth) != IAM

Posso usare un prodotto già pronto... magari SCIM compliant

--> la risposta semplice è NO

Sviluppo sostenibile

In anni di errori abbiamo imparato che è meglio essere SOLID che STUPID:

Singleton
Tight Coupling
Untestability
Premature Optimization
Indescriptive Naming
Duplication

Single Responsibility Principle
Open/Closed Principle
Liskov Substitution Principle
Interface Segregation Principle
Dependency Inversion Principle

…ovvero

Domain Driven Design (Eric Evans)

TDD (Kent Beck)

eXtreme Programming (Kent Beck, Martin Fowler, et al)

SCRUM (*Agile Software Development with Scrum*, Beedle, Schwaber)

Esistono buone pratiche condivisibili?

Probabilmente sì...

ma

per scoprirlo dobbiamo comunicare di più

Cosa serve? Forum/Blog/Mailing List/**TEMPO**?

Risposte?