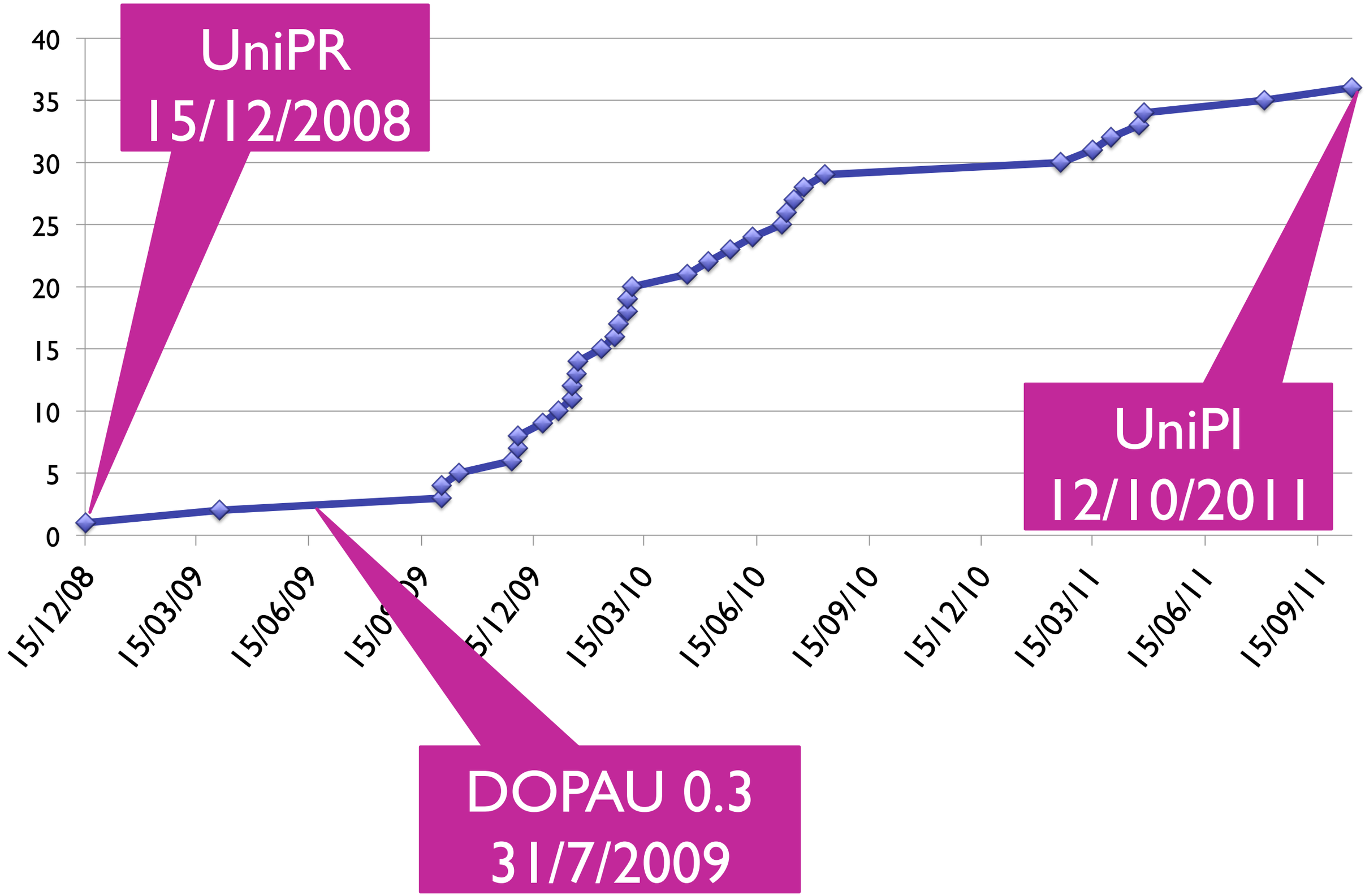
Fiducia nelle federazioni e garanzie sulle identità

Tiziana Podestà – CSITA – Università degli Studi di Genova

IdP e DOPAU


UniPR
15/12/2008
UniPI
12/10/2011
DOPAU 0.3
31/7/2009
40
35
30
25
20
15
10
5
0
15/12/08
15/03/09
15/06/09
15/12/09
15/03/10
15/06/10
15/09/10
15/12/10
15/03/11
15/06/11
15/09/11

DOPAU e Organizzazioni

Atenei	24
CNR	6
Altri enti di ricerca	1
Altri	5

NB I dati presentati fra 5 slide sono ricavati dai DOPAU degli Atenei

DOPAU : cosa è

Consortium GARR

24-25 Novembre 2009
Roma, Sede centrale ENEA

idem day

Che cosa è un DOPAU

Il DOPAU (DOcumento del Processo di Accreditamento degli Utenti) è un documento che illustra schematicamente il sistema di accreditamento del personale contrattualizzato ed esterno dell'organizzazione.

Finalità

(Fiducia, Consapevolezza, Trasparenza, Realtà)

- Realizzare una Federazione su una rete di fiducia
- "Consapevolezza" per l'ente che partecipa alla Federazione del proprio processo di accreditamento

Il DOPAU in NdP (1/2)

(da 3.2 Registrazione di un IdP)

Il Partecipante invia alla Federazione il documento descrittivo del processo di accreditamento dei propri utenti compilato secondo lo schema DOPAU predisposto dalla Federazione: a seguito della registrazione dell'IdP la Federazione renderà disponibile tale documento ai Partecipanti che ne facciano richiesta;

In pratica: copia del DOPAU firmata dal Referente Organizzativo va allegata al modulo per la registrazione dell'IdP IPRR (Identity Provider Registration Request)

Il DOPAU in NdP (2/2)

(da 3.4 Impegni dei Partecipanti)

Il Partecipante che registra un IdP si impegna a verificare periodicamente la conformità a quanto dichiarato tramite il DOPAU

(6 Auditing)

Il Partecipante accetta e consente che vengano effettuate dalla Federazione verifiche periodiche della conformità dei servizi registrati ai requisiti tecnici, come specificati in ST e ST-A e a quanto dichiarato in DOPAU

Il DOPAU in DOPAU

Il Documento DOPAU prodotto dal Partecipante DEVE contenere le informazioni elencate nel presente modello.

In caso di modifica delle procedure o informazioni descritte nel documento, esso DEVE essere prontamente aggiornato e ne deve essere data comunicazione alla Federazione.

In pratica : non esiste l'obbligo di aggiornarlo periodicamente (ma forse dovrebbe esserci ..)

Gestore dell'accreditamento

[Dove viene descritto chi è il responsabile (quale area o servizio) del processo di accreditamento degli utenti che afferiscono al proprio Ente. Dove cioè viene detto chi è responsabile dell'assegnazione, del mantenimento e della cancellazione di un' identità digitale presso il proprio Ente.]

Area Personale e Area Studenti	5
Area ICT	6
Area Personale, Area Studenti e Area ICT	1
Area Personale, Area Studenti + altre strutture	8
responsabilità ICT	12
responsabilità conferita dal DA	3

Utenti gestiti

Dove vengono descritte tutte le categorie di utenti gestite dal proprio ente. Specificare a quali categorie viene dato l'accesso ai servizio della Federazione (cioè sono incluse nell'IdP) Specificare anche la cardinalità degli insiemi indicati.

staff	24
student	24
alum	12
affiliate	18

Visione d'insieme (1/3)

[Dove si descrive (possibilmente con un diagramma) l'architettura complessiva di provisioning degli utenti: dalle applicazioni che alimentano i DB fino alla loro propagazione nei Directories Service. Vanno descritti inoltre i punti in cui l'utente utilizza le credenziali ottenute]

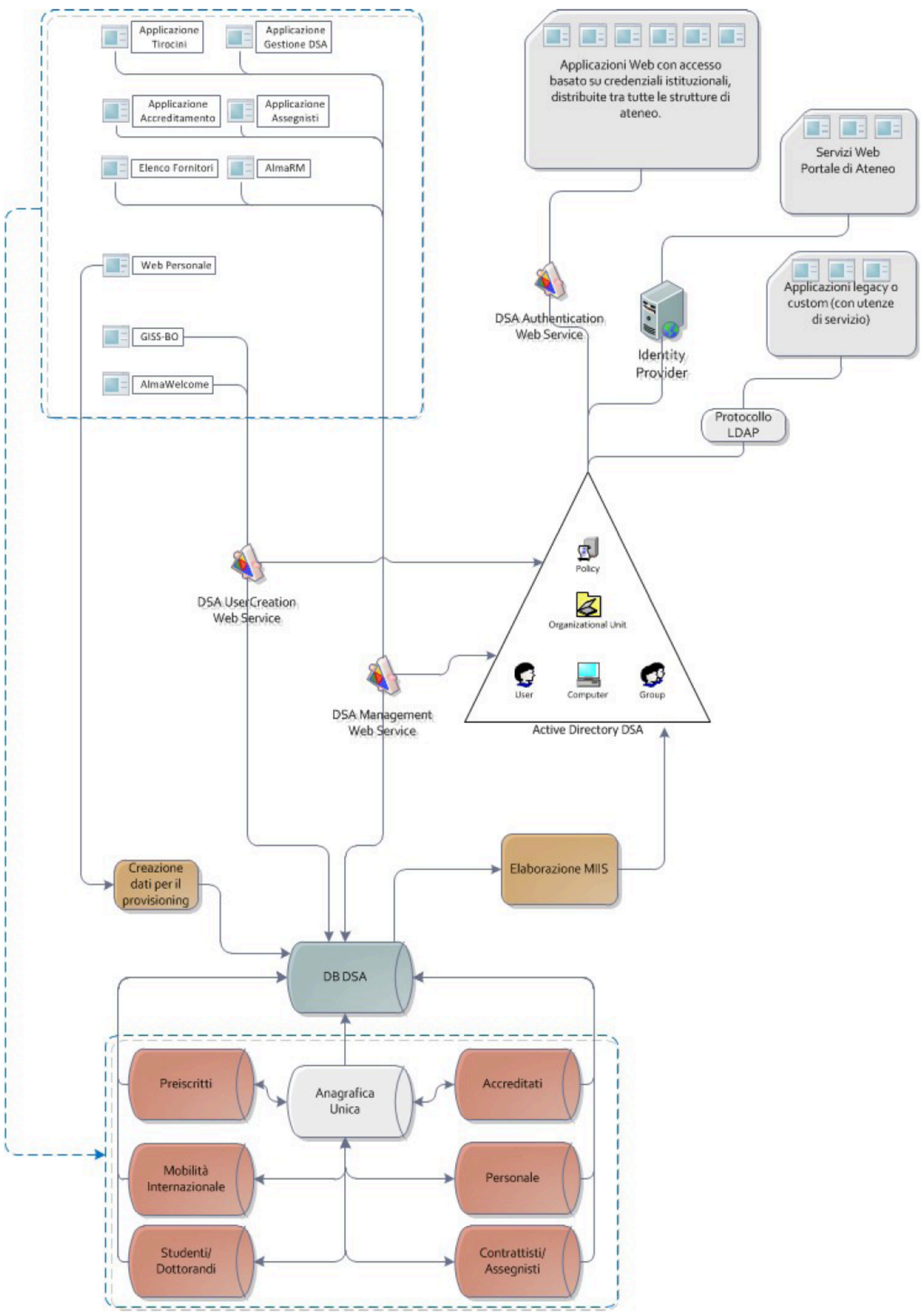
FONTE AUTORITATIVA	N. ATENEI
ESSE3	15
CSA	15
GISS	4
U-GOV	2
GEDAS, GISS-BO, altri *in house*	1x
CIA, GIADA, SIRIUM, SUPER, VISPER	1x
PI, PAE, ADELINE, altri in house	1x

Visione d'insieme (2/3)

Tempi di creazione delle credenziali a partire dai DB autoritativi:

CATEGORIA	TEMPO DI CREAZIONE	TEMPO DI AGGIORNAMENTO
PERSONALE	<1h (1) 24 h (7) 7 gg(1) 1 mese(1)	<1h (1) 24 h (6) 7 gg(1) 1 mese(1)
STUDENTI	<1h (3) 24 h(8) 7 gg(1)	<1h (3) 24 h(7) 7 gg(1)
ALTRI		

Almeno 7 atenei utilizzano un DB centralizzato di appoggio



In 14 dei 24 DOPAU è riportato il diagramma

Formato delle credenziali

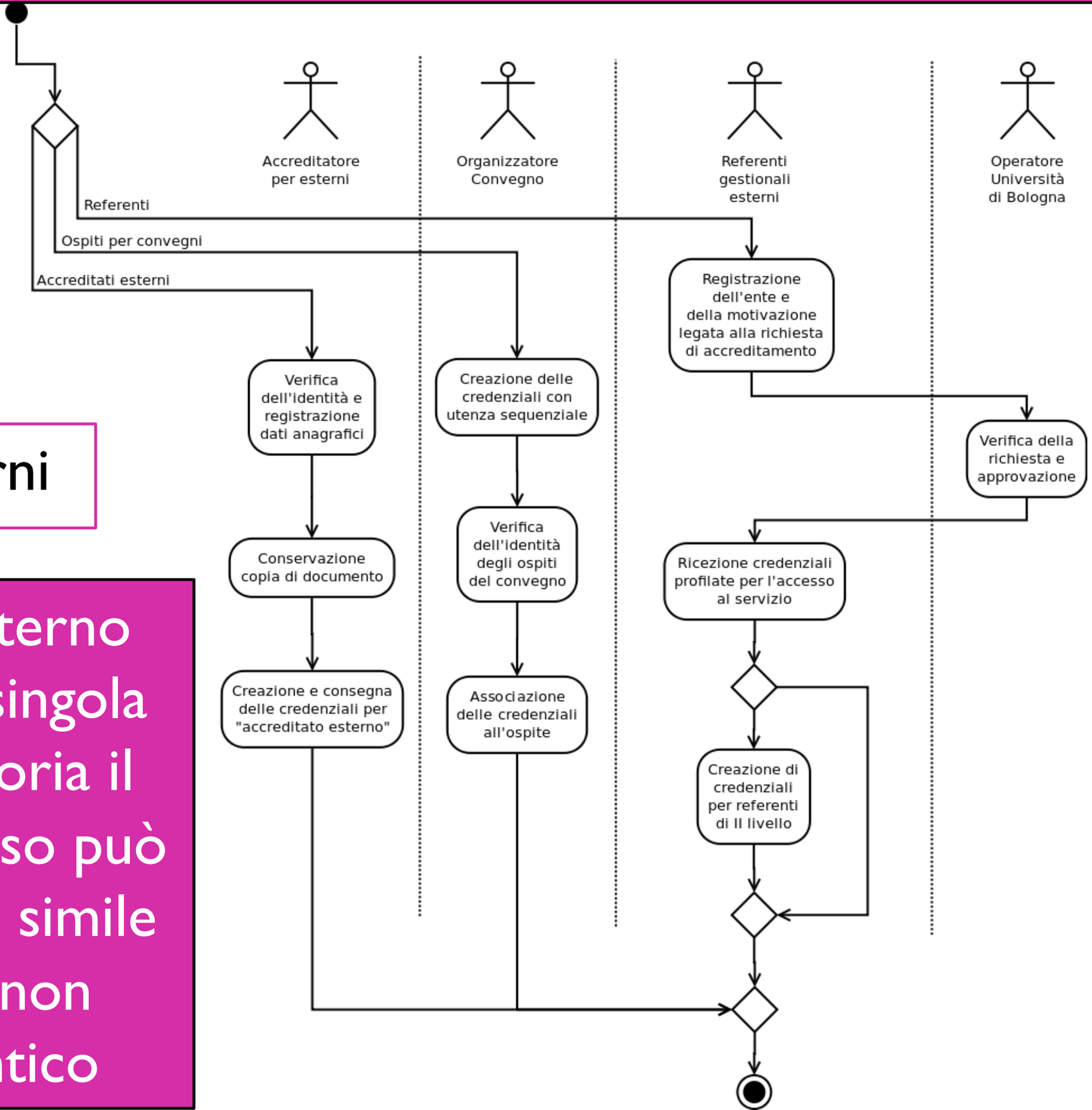
[[Dove si descrive la tipologia delle credenziali utilizzate nell'organizzazione credentials (e.g., Kerberos, userID/password, PKI, ...) il loro formato, la loro durata, ecc]

Tutti forniscono agli utenti credenziali del tipo UserID/password

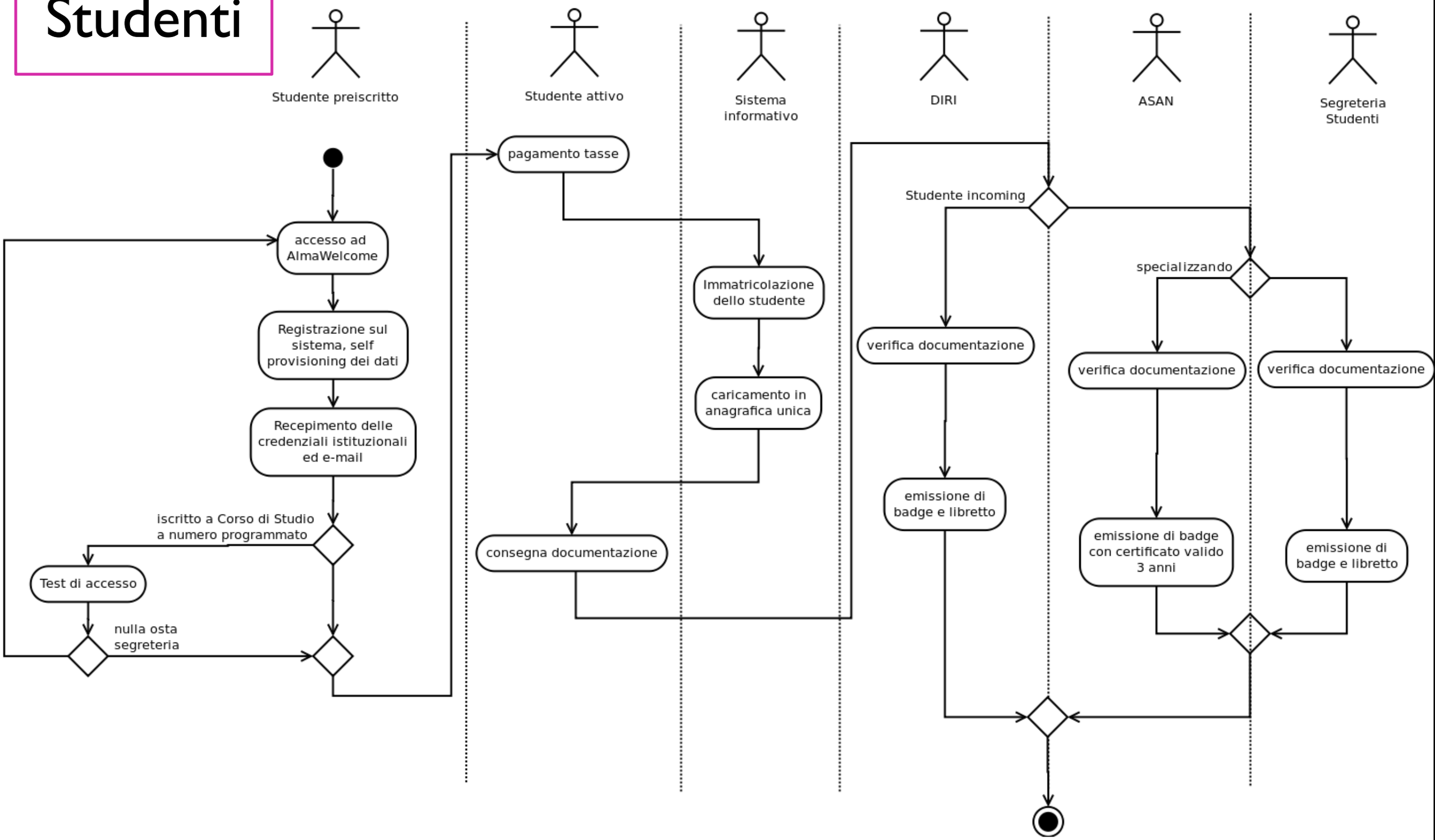
10 atenei forniscono ai propri utenti smart card e certificati

Esterni

All’interno della singola categoria il processo può essere simile ma non identico



Studenti



In 10 dei 24 DOPAU è riportato il diagramma del processo di accreditamento per la singola categoria

Il processo di accreditamento X

Caratteristiche dell'identità digitale

[Dove si dice quali caratteristiche (attributi) vengono associate all'identità digitale che viene creata (ad es. nome, cognome, codice fiscale, matricola, email, telefono, unità organizzativa di afferenza, ecc…] [Quali delle caratteristiche/attributi possono essere considerati pubblici e vengono forniti a chiunque ne faccia richiesta?]

STAFF Attributi pubblici	**n. Atenei**
Nome	16
Cognome	16
email	16
telefono	16
ruolo	7
unità afferenza	16

STUDENTI Attributi pubblici	**n. Atenei**
Nome	5
Cognome	5
email	5

AFFILIATE Attributi pubblici	**n. Atenei**
Nome	4
Cognome	4
email	3

Gestione password

Scadenza

	staff	student
6 mesi/180 giorni	5	3
3 mesi	1 + 1(*)	1
Secondo normativa	2	1
Dal 2010 (!)	1	1
Avviso	2	2

(*) per chi tratta dati sensibili

Credenziali multiple

Casi segnalati:

- Credenziali multiple nella categoria (residuali)
- Credenziali multiple dipendente – studente
- Credenziali multiple dottorandi

Interventi:

- Controllo prima dell'attivazione
- Controllo basato su Codice Fiscale
- Su segnalazione

Durata accreditamento-STAFF

Le regole adottate sono molto diverse:

- Illimitata (2)
- Illimitata per i docenti (1)
- Fino a limite massimo età pensionabile per docenti (1)
- Correlata al rapporto di lavoro : da 0 giorni a 5 anni

Al termine del rapporto di lavoro vengono adottate misure per la parziale/totale disabilitazione (modifica stato, marcatura, data cessazione, ..)

In 7 casi “avviene la cancellazione”

La disabilitazione può dipendere dal mancato rispetto delle policy

Durata accreditamento-STUDENT

Le regole adottate sono molto diverse:

- Illimitata (2) Indefinita (3)
- Correlata al completamento degli studi
- Correlata a trasferimento/cessazione

L'intervento di disabilitazione può dipendere dal mancato pagamento delle tasse

Al completamento degli studi vengono adottate misure per la parziale/totale disabilitazione (modifica stato, marcatura, data cessazione, ..)

Rischi/criticità (1/5)

Furto di identità

richieste attivazione falsificate (2)	staff affiliate
credenziali iniziali prevedibili	
richiesta telefonica in fase di attivazione	staff affiliate
richieste urgenti di rinnovo o recupero password fatte via telefono	docenti
reset pw a quelle di ESSE3	

Rischi/criticità (2/5)

Disabilitazione

le credenziali rimangono in directory al termine del rapporto di lavoro/completamento degi studi con marcatura poco evidente	
utenze che rimangono attive anche dopo cessazione rapporto per scadenze non aggiornate/corrette(es. trasferimento, contratto breve)	staff
procedura manuale di disattivazione e cancellazione utente dipendente TI e' soggetta a errori	staff

Rischi/criticità (3/5)

Il fattore umano

sottovalutazione dell'importanza di proteggere le proprie credenziali	student
convalida richiesta di credenziali da parte del responsabile di struttura senza verifica che il richiedente abbia diritto alle credenziali	staff - affiliate
operazioni manuali (2)	
pw complicate e scadenza obbligatoria sortiscono l'effetto contrario	

Rischi/criticità (4/5)

Policy e processi operativi

manca formalizzazione regolamento per accreditamento personale non strutturato	staff
manca policy relativa a durata password	
manca policy relativa a cancellazione dalla directory al termine del rapporto di lavoro/ studi	
tempi di formalizzazione del rapporto di lavoro	staff

Rischi/criticità (5/5)

Altri rischi/criticità

gestione credenziali personale TA che tratta dati sensibili	staff
doppie credenziali (per dipendente universitario iscritto a CS)	
dottorandi con doppie credenziali	
credenziali multiple per la stessa categoria, alle quali possono corrispondere attributi diversi	

Il sistema AA interno

[Per quali applicazioni interne all'organizzazione viene utilizzato questo sistema di gestione delle identità?

I servizi più gettonati:

accesso alla rete wireless, posta elettronica, accesso alla rete interna (VPN), LMS, portali web, proxy, servizi di biblioteca

Applicazioni web sviluppate in casa

Gmail e Google apps

[Gli identificatori principali di ogni persona, come "net ID," eduPersonPrincipalName, o eduPersonTargetedID, sono univoci una volta assegnati? Possono venire riutilizzati? In quali casi?]

Gli identificatori principali di ogni persona, come "net ID," eduPersonPrincipalName, eduPersonTargetedID, sono univoci una volta assegnati (9)

Possono essere riassegnati alla stessa persona (2)

Lo username è univoco in un dato momento e può essere riassegnato (1) solo per utenti temporanei (1)

Torniamo a punto di partenza ..

a cosa serve il DOPAU

All'interno dell'Organizzazione

Avvalorare la rilevanza del processo di gestione delle identità :

- Supportare i tecnici nella sensibilizzazione e nel coinvolgimento della dirigenza dell'Organizzazione
- Incentivare il rafforzamento delle misure atte a sensibilizzare e responsabilizzare l'utente
- coadiuvare tecnici e responsabili nell'analisi del processo e nell'individuazione delle criticità

La stesura del DOPAU è un momento di condivisione, formalizzazione e consolidamento interno

L'Organizzazione è il principale erogatore di risorse

All'interno di IDEM

Rafforzare e armonizzare i processi di gestione delle identità:

- Fornire una traccia per adeguare e migliorare la gestione degli utenti
- Condividere soluzioni ai problemi comuni e buone prassi

Far crescere la reciproca fiducia

Far crescere i servizi

Nell'interfederazione

Consentire a IDEM di svolgere un ruolo propositivo e costruttivo nella definizione di un Identity Assurance Program per REFEDS

Costituire un punto di partenza per il riconoscimento del LoA degli IdP IDEM

Futuro prossimo

CI e CTS IDEM, in collaborazione col Servizio IDEM GARR AAI intendono:

- rendere più agevole la compilazione dello schema rendendolo più simile a un questionario e aggiungendo esempi e delucidazioni
- rivedere le regole operative relative al DOPAU

Entro marzo 2012

E, parallelamente, avviare l'evoluzione del DOPAU in strumento per l'implementazione di identity assurance profile (IAP) corrispondenti a diversi LoA

Grazie

Lo schema DOPAU nasce dalla lungimiranza di Angelo Saccà e dall'impegno di "Lalla" Maria Laura Mantovani, Paola Laguzzi e Roberto Gaffuri

La prima versione viene rilasciata il 31/7/2009

Dal 2008 ad oggi il Servizio IDEM GARR AAI ha fornito un aiuto prezioso alle organizzazioni nella compilazione del DOPAU

Gli schemi presentati sono stati realizzati dal CESIA – unibo

Fine I parte

LoA e valutazione del rischio

Il **Level of Assurance (LoA)** è la valutazione del rischio di una autenticazione digitale:

- è il grado di certezza (1) che il RP ha che la persona fisica sia stata identificata in modo adeguato prima di ricevere le credenziali da una RA, e (2) che le credenziali sono presentate dalla persona alla quale sono state assegnate

- per l'utente è un fattore di protezione dai furti di identità

LoA e NIST

NIST (National Institute of Standards and Technology) è un'agenzia governativa statunitense e Computer Security Division (CSD) è una delle 6 divisioni del NIST

In **NIST 800-63 Electronic Authentication Guideline** sono definiti 4 livelli di LoA.

La versione 1.0.2 è stata rilasciata nell'aprile 2006. Da fine giugno è disponibile la bozza della nuova versione.

NIST SP 800-63 contiene raccomandazioni e linee guida, non obblighi normativi

I 4 livelli di LoA (1/2)

NIST 800-63 integra OMB guidance, E-Authentication Guidance for Federal Agencies, che definisce 4 livelli in base alle conseguenze del non corretto uso delle credenziali fornendo le raccomandazioni per la scelta delle tecnologie una volta effettuata l'analisi dei rischi e determinato il LoA appropriato

Criteria	Level 1	Level 2	Level 3	Level 4
Confidence in asserted identity's validity	little/none	some	high	very high
Risk of inconvenience or liability	low	mod	mod	high
Risk of release of sensitive data	none	low	mod	high
Risk to personal safety	none	none	low	mod/high

Electronic authentication (E-authentication) is the process of establishing confidence in user identities electronically presented to an information system.

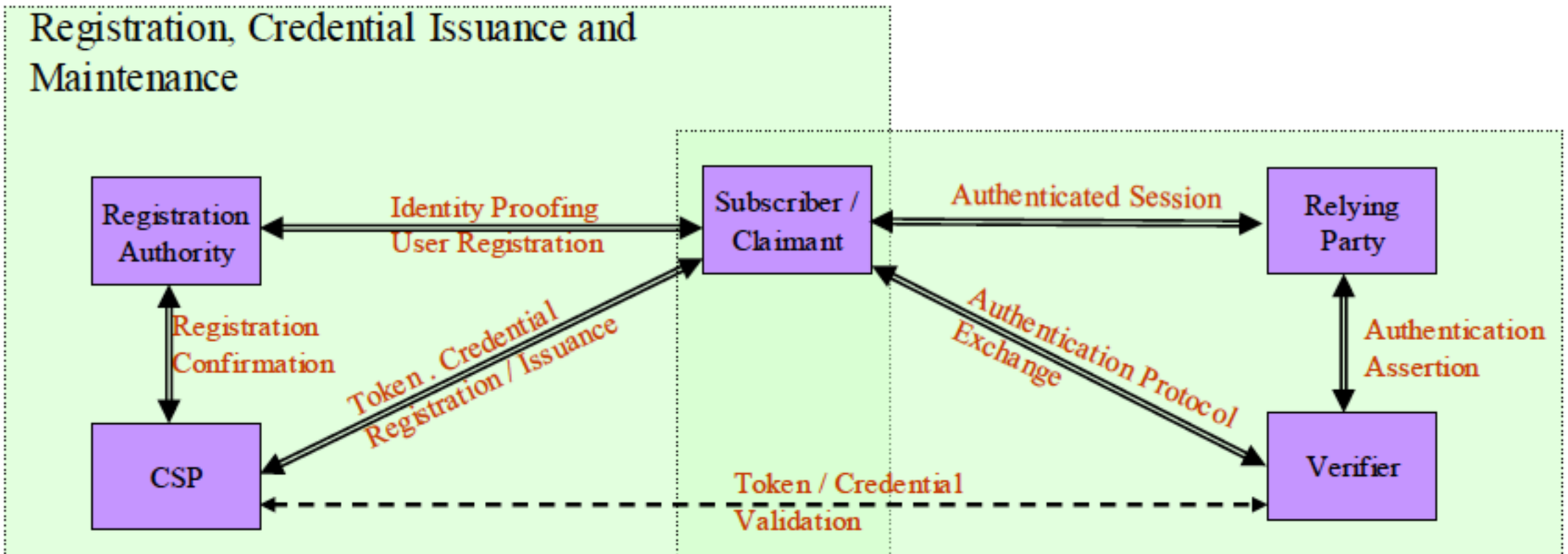
I 4 livelli di LoA (2/2)

LoA è determinato da:

1	Identity proofing and registration of Applicants
2	Tokens (typically a cryptographic key or password) for proving identity
3	Token and credential management mechanisms used to establish and maintain token and credential information
4	Protocols used to support the authentication mechanism between the Claimant and the Verifier
5	Assertion mechanisms used to communicate the results of a remote authentication if these results are sent to other parties

user	user may be referred to as the Applicant, Subscriber, or Claimant, depending on the stage in the lifecycle of the credential
Credentials Service Provider (CSP)	A trusted entity that issues or registers Subscriber tokens and issues electronic credentials to Subscribers. The CSP may encompass Registration Authorities (RAs) and Verifiers that it operates.

E-authentication e LoA



1. An individual Applicant applies to an RA
2. The RA identity proofs that Applicant
3. On successful identity proofing, the RA sends the CSP a registration confirmation message.
4. A secret token and a corresponding credential are established between the CSP and the new Subscriber.
5. The CSP maintains the credential, its status, and the registration data collected for the lifetime of the credential (at a minimum). The Subscriber maintains his or her token.

1. The Claimant proves to the Verifier that he or she possesses and controls the token through an authentication protocol.
2. The Verifier interacts with the CSP to validate the credential that binds the Subscriber's identity to his or her token.
3. If the Verifier is separate from the RP (application), the Verifier provides an assertion about the Subscriber to the RP, which uses the information in the assertion to make an access control or authorization decision.
4. An authenticated session is established between the Subscriber and the RP.

LoA level 1

1	identity proofing is not required so names in credentials and assertions are assumed to be pseudonyms.
2	Tokens: Memorized Secret Token, Pre-Registered Knowledge Token
3	Credential storage, Token and credential verification services
4	Required Authentication Protocol Threat Resistance: Online guessing, Replay
5	Threat Resistance per Assertion : Assertion manufacture/modification, Assertion reuse, Secondary authenticator manufacture

LoA level 2

1	Identity proofing is required, but the credential may assert the verified name or a pseudonym.
2	Single Tokens :Memorized Secret Token, Pre-Registered Knowledge Token, Look-up Secret Token, Out of Band Token, SF One-Time Password Device, SF Cryptographic Device Multi-Token
3	Credential storage, Token and credential verification services, Token and credential renewal/re-issuance, Token and credential revocation and destruction, Records retention
4	Required Authentication Protocol Threat Resistance: Online guessing, Replay, Session hijacking, Eavesdropping, Man in the middle
5	Threat Resistance per Assertion : Assertion manufacture/modification, Assertion disclosure, Assertion reuse, Assertion redirect, Secondary authenticator manufacture, Secondary authenticator capture, Assertion substitution

Both in-person and remote registration are permitted

LoA level 2-4

Records of registration shall be maintained either by the RA or by the CSP

Identity proofing and registration processes shall be performed according to applicable written policy or practice statement

If the RA and CSP are remotely located and communicate over a network, the entire registration transaction between the RA and CSP shall occur over a mutually authenticated protected channel. Equivalently, the transaction may consist of timestamped or sequenced messages signed by their source and encrypted for their recipient. In either case, Approved cryptography is required.

The Applicant supplies his or her full legal name, an address of record, and date of birth, and may, subject to the policy of the RA or CSP, also supply other PII.

Registration, identity proofing , token creation/issuance, and credential issuance are separate processes that can be broken up into a number of separate physical encounters and electronic transactions: the Applicant shall identify himself/herself in any new electronic transaction

LoA level 3

1	Only verified names may be specified in credentials and assertions
2	Single Tokens :MF Software Cryptographic Token Multi-Token (table 7 - NIST 800-63)
3	Credential storage, Token and credential verification services, Token and credential renewal/re-issuance, Token and credential revocation and destruction, Records retention
4	Required Authentication Protocol Threat Resistance: Online guessing, Replay, Session hijacking, Eavesdropping, Man in the middle, Phishing/pharming
5	Threat Resistance per Assertion : Assertion manufacture/modification, Assertion disclosure, Assertion repudiation by Verifier, Assertion reuse, Assertion redirect, Secondary authenticator manufacture, Secondary authenticator capture, Assertion substitution

Both in-person and remote registration are permitted

LoA level 4

1	Only verified names may be specified in credentials and assertions
2	TSingle Tokens :MF OTP Hardware Token, MF Hardware Cryptographic Token Multi-Token (table 7 - NIST 800-63)
3	Credential storage, Token and credential verification services, Token and credential renewal/re-issuance, Token and credential revocation and destruction, Records retention
4	Required Authentication Protocol Threat Resistance: Online guessing, Replay, Session hijacking, Eavesdropping, Man in the middle, Phishing/pharming
5	Threat Resistance per Assertion : Assertion manufacture/modification, Assertion disclosure, Assertion repudiation by Verifier, Assertion repudiation by SubscriberAssertion reuse, Assertion redirect,Secondary authenticator manufacture, Secondary authenticator capture, Assertion substitution

Only in-person registration is permitted.

InCommon e LoA (1/4)

Un *trust assurance framework* definisce le policy e le procedure che consentono a IdP e RP di condividere dati con un adeguato livello di reciproca fiducia

Open Identity Initiative è una organizzazione governativa statunitense incaricata della valutazione di *trust frameworks*

Fra i frameworks che vengono valutati ci sono anche quelli della federazione InCommon: Bronze (LoA 1) e Silver (LoA 2)

IAP (Identity Assurance Program) Bronze e Silver si occupano anche di verificare che i membri siano organizzazioni *trusted*

InCommon e LoA (2/4)

Un *trust assurance framework* definisce le policy e le procedure che consentono a IdP e RP di condividere dati con un adeguato livello di reciproca fiducia

Open Identity Initiative è una organizzazione governativa statunitense incaricata della valutazione di *trust frameworks*

Fra i frameworks che vengono valutati ci sono anche quelli della federazione InCommon: Bronze (LoA 1) e Silver (LoA 2)

IAP (Identity Assurance Program) Bronze e Silver si occupano anche di verificare che i membri siano organizzazioni *trusted*

InCommon e LoA (3/4)

InCommon comprende università, enti di ricerca, organizzazioni governative, non-profit e anche organizzazioni commerciali (es. NIH, NSF, TerraGrid, JSTOR, Microsoft, Apple)

La prima versione dei programmi di certificazione Bronze e Silver è del 2008

I membri di InCommon possono scegliere se aderire agli IAP

La valutazione viene effettuata da Auditor esterni

Un'organizzazione può avere un mix di utenti a livelli diversi

Un utente può avere associati livelli diversi in base al contesto

InCommon e LoA (4/4)

InCommon ha individuato SP che offrono servizi a fronte di un adeguato LoA:

Identity Assurance is useful across the academy, including research and administrative-related services:

- *National Student Clearinghouse for financial aid reporting and access for students and financial aid staff.*
- *CILogon access to CI services such as Open Science Grid*
- *Research Virtual Organizations such as LIGO*
- *NIH ERA (NIH grant submission application)*

e stabilito requisiti oltre quelli di NIST:

- *IdP Operator has sufficient staff with sufficient skills to operate according to stated policies and procedures*
- *Helpdesk available during regular hours*
- *All security policies and procedures are documented*
- ..

Per approfondire

National Strategies for Trusted Identities in Cyberspace
<http://www.nist.gov/nstic/index.html>http://www.nist.gov/nstic/index.html

NIST E-Authentication Guidelines
<http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-63-Rev.%201>SP800-63-Rev1-Draft3_June2011.pdf

OMB E-Authentication Guidance for Federal Agencies
http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

InCommon Identity Assurance
http://www.incommonfederation.org/assurance