



Governo italiano

Presidenza del Consiglio dei Ministri

Gli strumenti di semplificazione dei rapporti tra professionisti e PA

Francesco Tortorelli

22 Gennaio 2010

Ministro per la pubblica amministrazione e l'innovazione



Governo italiano

Presidenza del Consiglio dei Ministri

Gli strumenti di semplificazione dei rapporti tra professionisti e PA



Sottoscrizione



Attestazione del ruolo



spedizione



Archiviazione





- La posta elettronica certificata**
- La firma digitale**
- La gestione dei ruoli professionali**



- La posta elettronica certificata**
- La firma digitale**
- La gestione dei ruoli professionali**



Nel corso dei prossimi mesi il grado di diffusione della posta elettronica certificata subirà un forte impulso:

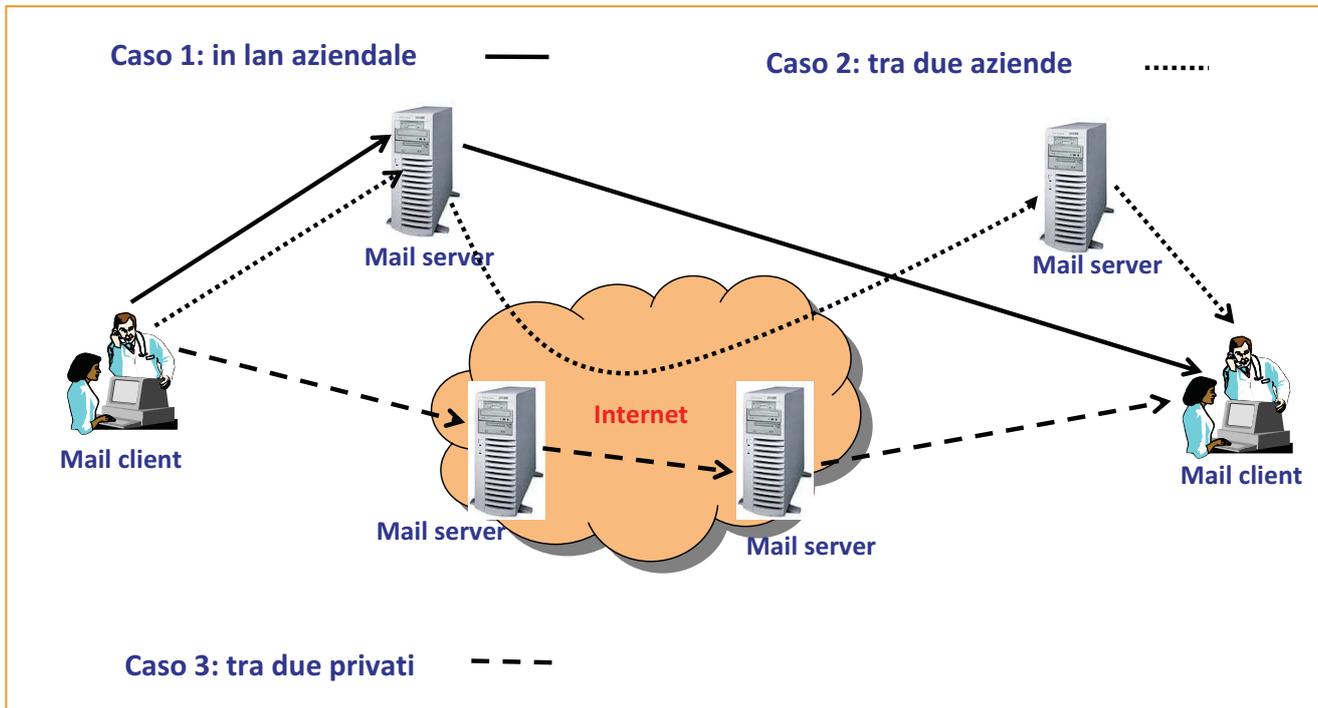
- ✓ dal 29/11/2008 tutte le nuove imprese debbono dotarsi di PEC
- ✓ Dal 28/11/2009 tutti i professionisti debbono dotarsi di PEC
- ✓ Nelle prossime settimane sarà avviato il servizio di PEC ai cittadini, grazie al quale tutti coloro che ne faranno richiesta potranno avere, gratuitamente, una casella di posta elettronica certificata per le comunicazioni con la PA



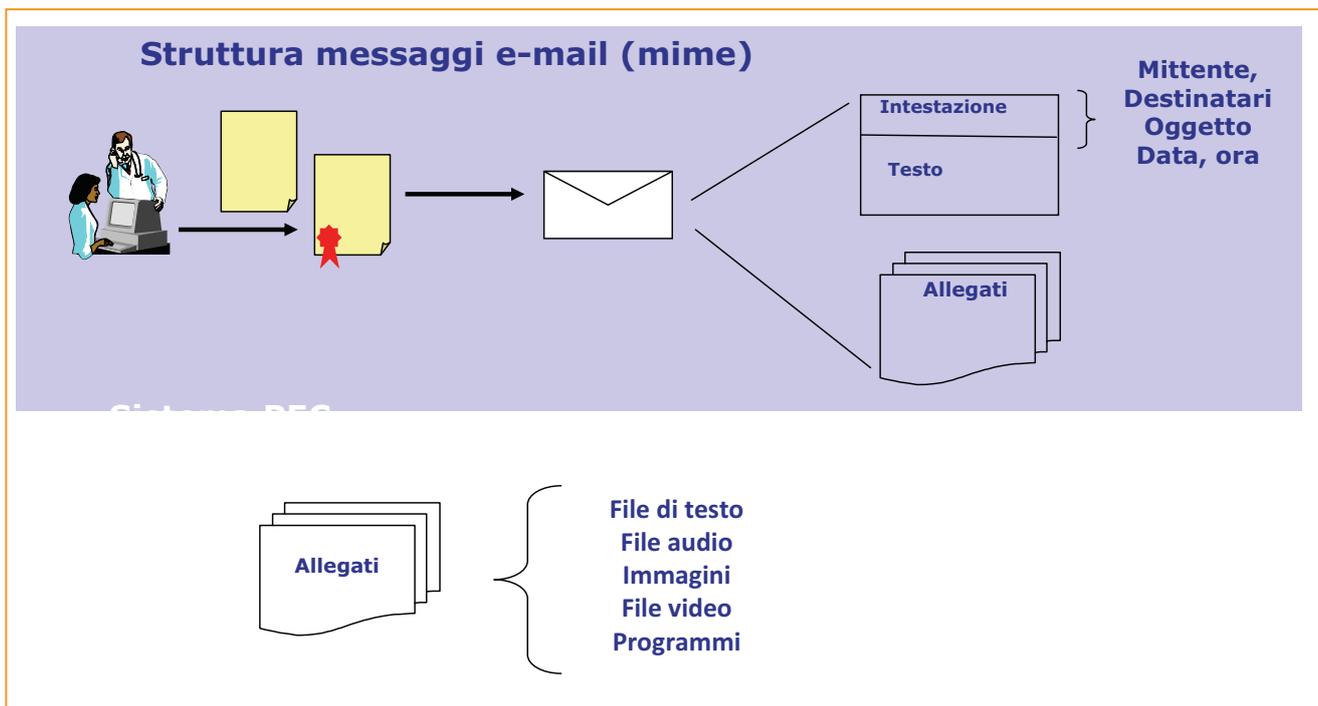
La posta elettronica certificata (PEC) è uno strumento con valore legale, basato sulla posta elettronica, per la trasmissione di documenti informatici attraverso la rete internet.



Come vengono trasmesse le e-mail



Struttura dei messaggi e-mail





Alcune riflessioni di partenza

L'e-mail tradizionale presenta problemi

Sul piano tecnico di:

- integrità (il messaggio arrivato è esattamente quello spedito?),
- riservatezza (qualcuno ha letto il messaggio durante il percorso?),
- certezza dell'origine (il messaggio proviene esattamente dall'indirizzo mittente?).

Sul piano giuridico di:

- obblighi specifici per i fornitori del servizio (chi fornisce servizi e-mail ha obblighi di prestazione, di conservazione?),
- opponibilità (l'avvenuta spedizione e la ricezione di messaggi e-mail sono eventi opponibili a terzi?).



Il quadro normativo

Le norme

- L. 59/97
- DPR 445/2000
- DPR 68/2005 "Posta certificata"
- Il D.lgvo 82/2005 "Codice dell'Amministrazione Digitale"
- L. 2/2009 (conversione decreto legge n. 185/2008)
- L. 69/2009



La norma primaria

art 15, comma 2, della legge 59/97:

“Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge”



I principi stabiliti dal DPR 68/05 - 1

- **L’ambito di utilizzo all’interno delle P.A., nei rapporti tra pubbliche amministrazioni e privati e tra i privati**
- **La disciplina della figura del gestore del servizio**
- **I contenuti probatori della trasmissione del documento informatico e la disciplina delle ricevute**
- **Il valore dell’invio e della ricezione della posta elettronica [Art. 3]:**
 - a) **il documento, trasmesso per via telematica, si intende spedito dal mittente se inviato al proprio Gestore**
 - b) **il documento si intende consegnato al destinatario se disponibile all'indirizzo elettronico da questi dichiarato, nella casella di PEC messa a disposizione dal Gestore**



I principi stabiliti dal DPR 68/05 - 2

- **Le modalità di trasmissione e le ricevute;**
- **La sicurezza del sistema;**
- **Istituzione dell'elenco pubblico dei gestori, requisiti e modalità di iscrizione;**
- **La vigilanza;**
- **Regole tecniche.**



IL DM 2 novembre 2005

Definisce:

- **standard tecnici e compatibilità;**
- **comunicazione disponibilità uso PEC e variazione;**
- **caratteristiche dei messaggi gestiti e delle tipologie di ricevute:**
- **il riferimento temporale;**
- **conservazione dei log dei messaggi;**
- **il trattamento dei virus;**
- **livelli di servizio;**
- **i documenti necessari all'iscrizione;**
- **il circuito dei domini PEC e i certificati di accesso e firma delle ricevute;**
- **disciplina dei compiti del CNIPA;**
- **organizzazione del personale del gestore;**
- **struttura del manuale operativo.**



Decreto Legislativo del 7 marzo 2005, n. 82

- **Art. 6** Le pubbliche amministrazioni utilizzano la posta elettronica certificata (DPR 68/2005) per ogni scambio di documenti e informazioni con i soggetti interessati che ne fanno richiesta e che hanno preventivamente dichiarato il proprio indirizzo di posta elettronica certificata.
- **Art. 47** Le pubbliche amministrazioni devono istituire almeno una casella di posta elettronica istituzionale ed una casella di posta elettronica certificata.
- **Art. 48** La trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna avviene mediante la posta elettronica certificata

La trasmissione del documento informatico per via telematica, effettuata mediante la posta elettronica certificata (DPR 68/2005), equivale, nei casi consentiti dalla legge, alla notificazione per mezzo della posta

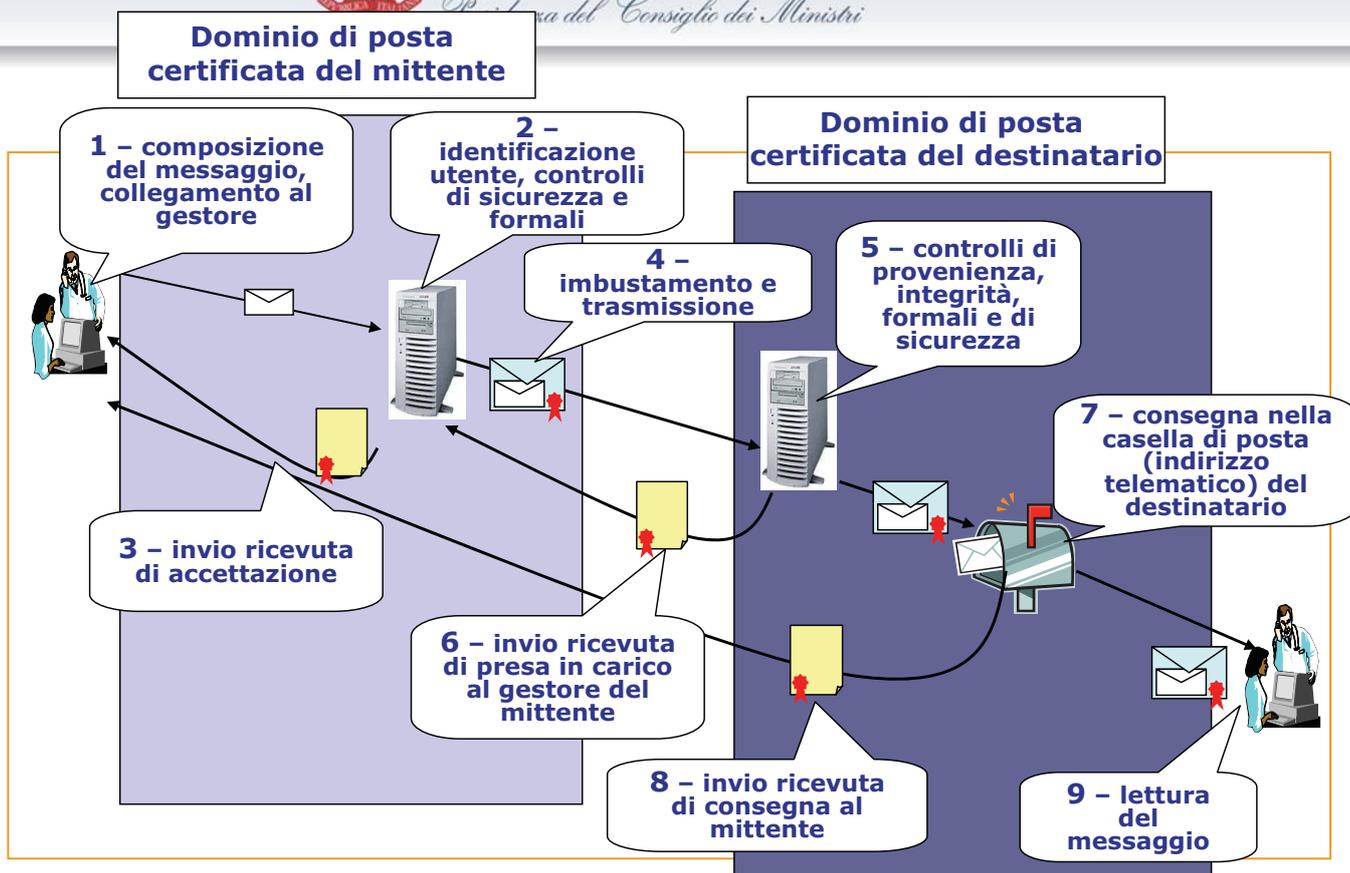
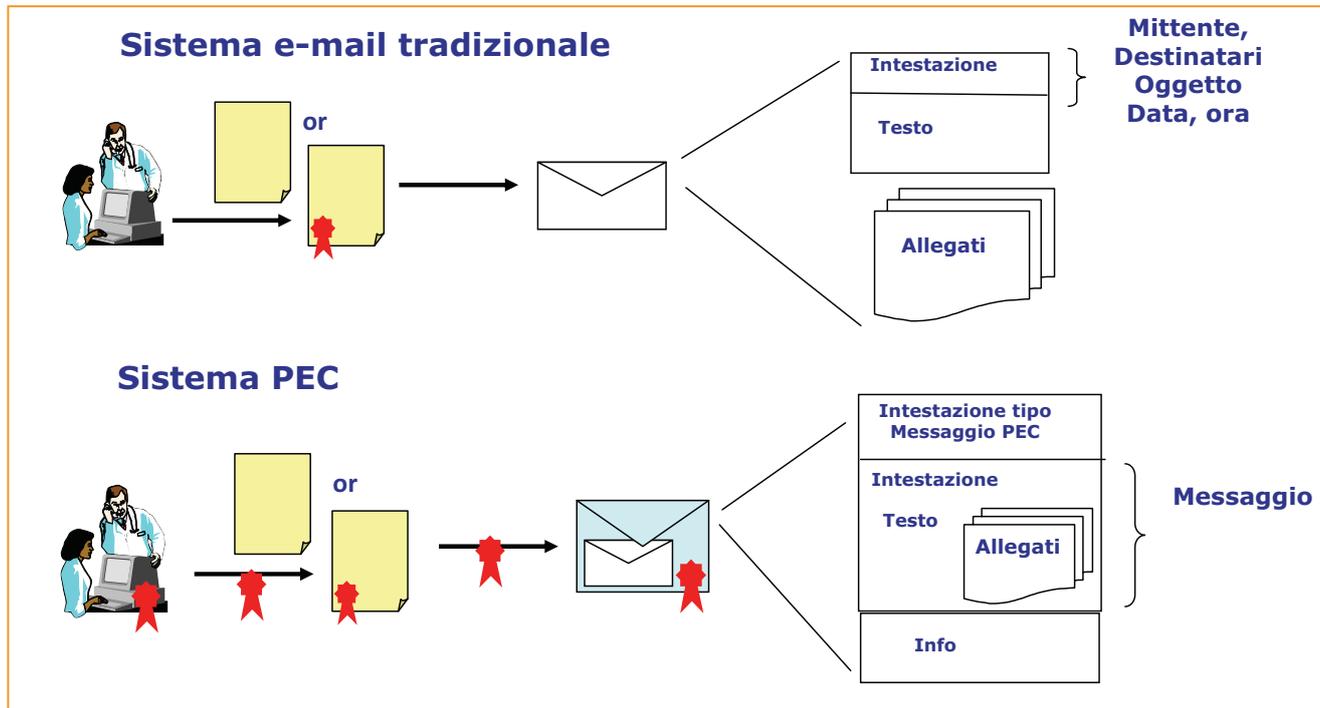


L. 2/2009

• **I professionisti** iscritti in albi ed elenchi istituiti con legge dello Stato **comunicano ai rispettivi ordini o collegi il proprio indirizzo di posta elettronica certificata**

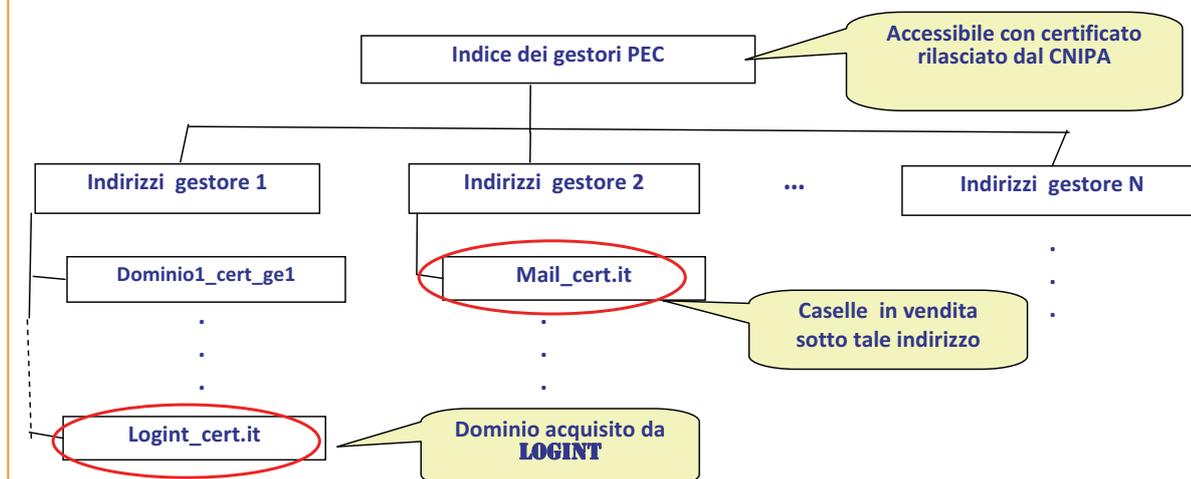
• **le comunicazioni tra Pa professionisti ed imprese**, che abbiano provveduto agli adempimenti ivi previsti, **possono essere inviate attraverso la posta elettronica certificata, senza che il destinatario debba dichiarare la propria disponibilità ad accettarne l'utilizzo.**

• **La consultazione per via telematica dei singoli indirizzi di posta elettronica certificata** nel registro delle imprese o negli albi o elenchi costituiti ai sensi del presente articolo **avviene liberamente e senza oneri. L'estrazione di elenchi di indirizzi è consentita alle sole pubbliche amministrazioni** per le comunicazioni relative agli adempimenti amministrativi di loro competenza.





Gli indirizzi PEC



La PEC consente (cfr. riflessioni di partenza)

Sul piano tecnico:

- l'integrità dei messaggi trasportati,
- la riservatezza dei messaggi trasportati che non possono essere letti durante il percorso,
- la certezza dell'origine (titolare della casella mittente).

Sul piano giuridico:

- i gestori hanno obblighi specifici e sono sottoposti a vigilanza,
- le ricevute di spedizione e di avvenuta consegna sono opponibili a terzi.

Inoltre:

- le ricevute sono legate univocamente al contenuto del messaggio spedito,
- in caso di smarrimento delle ricevute il "log" del gestore fa fede,
- può essere usata da persone o da applicazioni informatiche.



DigitPA

Come viene effettuata la vigilanza a regime da parte di DigitPA ?

- Con controlli periodici;
- Attraverso l'acquisizione di informazioni ricevute periodicamente dai gestori ai sensi della circolare 51;
- Su segnalazione.

Esistono registri, elenchi pubblicamente consultabili delle caselle PEC ?

- SI per le PA, il sito www.indicepa.gov.it contiene tra l'altro tali informazioni relative alle PA, a breve sarà disponibile un sito dedicato;
- Per i privati solo in caso di consenso esplicito;
- Per i professionisti e le imprese consultazione singola, elenchi completi solo a disposizione delle PA



Gli utenti

Cosa devono fare gli utenti per usare la PEC ?

- Informarsi sul servizio iniziando a consultare l'apposita sezione del sito DigitPA: [http://www.cnipa.gov.it/site/it-IT/In primo piano/Posta Elettronica Certificata \(PEC\)/](http://www.cnipa.gov.it/site/it-IT/In_primo_piano/Posta_Elettronica_Certificata_(PEC)/)
- Consultare le caratteristiche dei servizi offerti, pubblicizzati attraverso i rispettivi siti internet dei gestori iscritti nell'indice DigitPA e rivolgendosi direttamente agli stessi.

Quali servizi si possono richiedere ai gestori ?

- Domini PEC (anche con nomi a scelta del richiedente);
- Singole caselle (talvolta su nomi di dominio definiti);
- Servizi complementari non regolamentati.



Gli utenti - 2

Cosa prevede un servizio-tipo ?

- Servizi di gestione di caselle di posta nel rispetto dei requisiti normativi del servizio;
- Emissione di ricevute opponibili;
- Accesso ai log in caso di smarrimento ricevute o contestazioni.

Come dichiarano le imprese la volontà di utilizzare la PEC ?

- Le imprese, nei rapporti tra loro intercorrenti, possono dichiarare la esplicita volontà di accettare l'invio di posta elettronica certificata mediante indicazione della relativa casella PEC, nell'atto di iscrizione al registro delle imprese.



La PEC: dimensione del mercato

- 24 gestori PEC iscritti;
- Oltre 10.000 indirizzi PEC delle PA pubblicati su "indicePA.gov.it";
- circa 60.000 domini PEC registrati a dicembre 2009 per oltre 1.200.000 caselle;
- Oltre 25.000.000 PEC/mese scambiate;
- La distribuzione dei domini ha toccato praticamente tutti i settori di mercato: PA, Banche, Piccole medie e grandi Aziende, professionisti, cittadini.



INDICE PA

iPA indice delle
Pubbliche Amministrazioni

indicePA.gov.it



Sito ufficiale previsto dal D.P.C.M. del 31.10.2000 G.U. 272 del 21.11.2000



Struttura preposta a contenere per tutte le Amministrazioni Pubbliche:



le strutture organizzative,



gli uffici di protocollo (AOO),



le caselle di posta certificata.



Conclusioni

- La posta elettronica certificata (PEC) può essere vista come una raccomandata elettronica e può essere utilizzata anche in sostituzione della notificazione nei casi in cui la legge prevede la possibilità di utilizzare la posta.
- E' un sistema maturo e già di larga diffusione che si diffonderà ulteriormente nei prossimi mesi.
- Più che un obbligo è una eccellente opportunità per i professionisti che potranno vedere la loro pratica viaggiare più velocemente, con minori costi, con certezza di consegna e con la possibilità di inviare (e ricevere) documenti da un qualunque punto connesso ad una rete telematica in qualunque ora e giorno dell'anno.
- I professionisti devono acquisire le proprie caselle PEC e comunicare i relativi indirizzi ai rispettivi ordini, che pubblicheranno tali indirizzi attraverso sistemi di consultazione sui singoli iscritti ed in maniera complessiva solo verso le PA.



- La posta elettronica certificata**
- La firma digitale**
- La gestione dei ruoli professionali**



LA FIRMA DIGITALE



Informazione crittografata che, allegata ad un documento informatico, ne garantisce:

- **integrità**, ossia l'assenza di modifiche successive alla sottoscrizione;
- **provenienza**, ossia l'identità del sottoscrittore.

Il sottoscrittore usa la sua chiave crittografica privata (segreta) per firmare.

I destinatari usano la chiave crittografica pubblica del sottoscrittore per verificare la firma.



GLI ATTORI

CERTIFICATORE

ALICE



Genera e fa certificare le chiavi con cui firma moduli di richiesta di servizi



Certifica e rende pubblico il fatto che le chiavi generate da Alice appartengono effettivamente a lei

BRUNO



Impiegato che riceve le richieste e le verifica



IL CERTIFICATORE

- Identifica il soggetto proprietario di una coppia di chiavi di sottoscrizione.
- Verifica che il proprietario delle chiavi abbia le caratteristiche necessarie per divenire titolare del certificato richiesto.
- Emette il certificato che attesta la corrispondenza tra chiavi di sottoscrizione ed identità del titolare.
- Pubblica il certificato nel proprio elenco dei certificati che può essere consultato telematicamente.



ATTIVAZIONE DEI CERTIFICATORI

- Il Certificatore comincia ad operare dopo l'inserimento nell'elenco pubblico dei certificatori.
- L'inserimento nell'elenco permette al Certificatore di emettere certificati qualificati (all. I - Direttiva CEE 93/CE/1999).
- Non è vietato operare sul mercato senza essere inseriti nell'elenco pubblico.

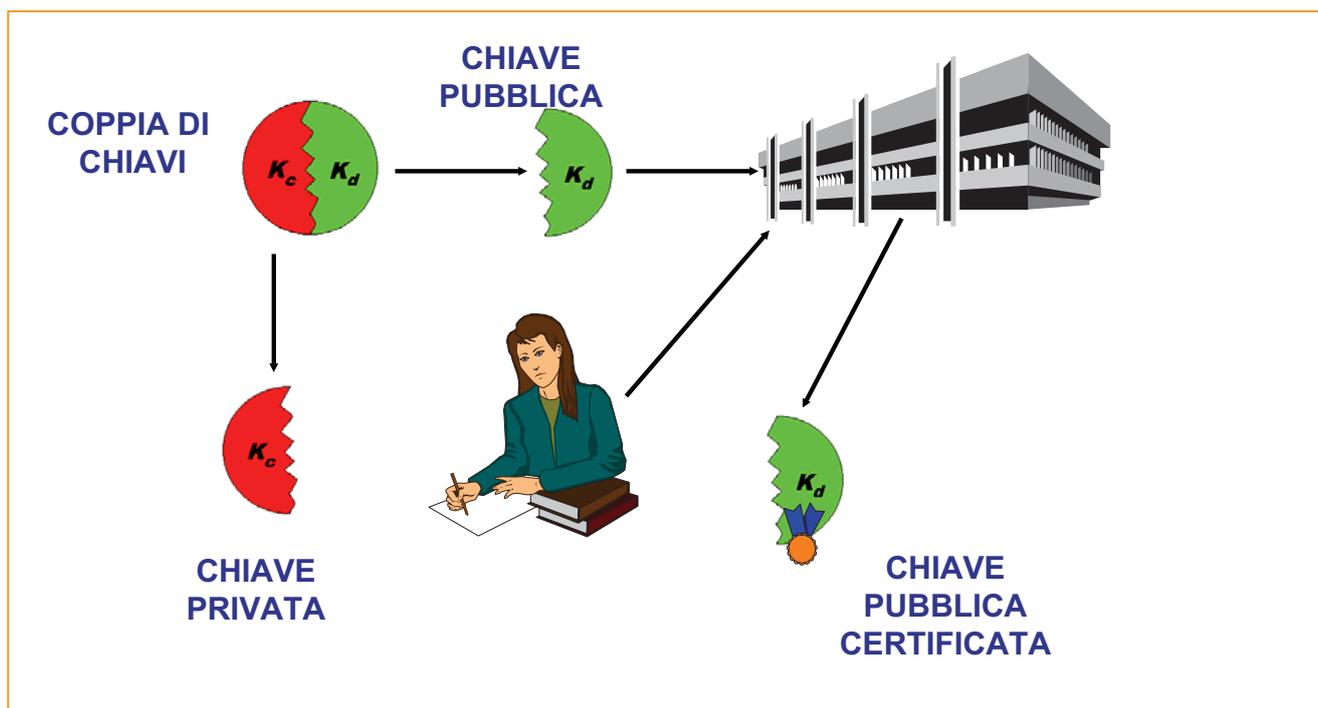


LA REGISTRAZIONE

- È l'operazione che stabilisce il rapporto tra titolare delle chiavi e certificatore.
- Comporta le seguenti azioni:
 - Compilazione della richiesta da parte del titolare.
 - Generazione della coppia di chiavi di sottoscrizione.
 - Verifica dell'identità e dei requisiti del titolare.
 - Emissione del certificato relativo alla coppia di chiavi generate.



LA REGISTRAZIONE





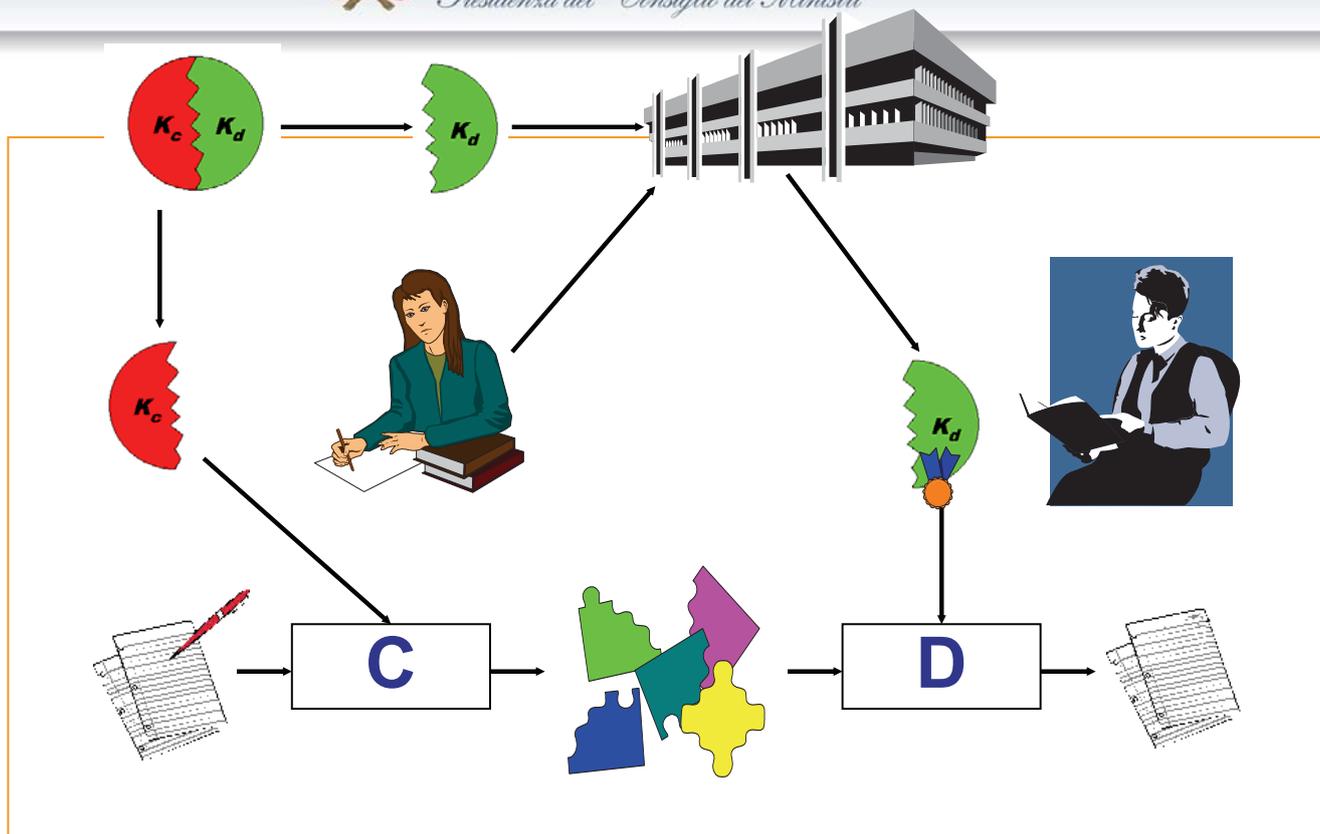
SOTTOSCRIZIONE E VERIFICA

SOTTOSCRIZIONE

- Il documento viene elaborato con la **CHIAVE SEGRETA** producendo un valore cifrato che costituisce la **FIRMA DIGITALE**.
 - La **FIRMA DIGITALE** è unica perché dipende dal documento e dalla chiave segreta.
 - La **FIRMA DIGITALE** viene allegata al documento.

VERIFICA

- La **FIRMA DIGITALE** viene decifrata mediante la **CHIAVE PUBBLICA** e si verifica che corrisponda al documento.

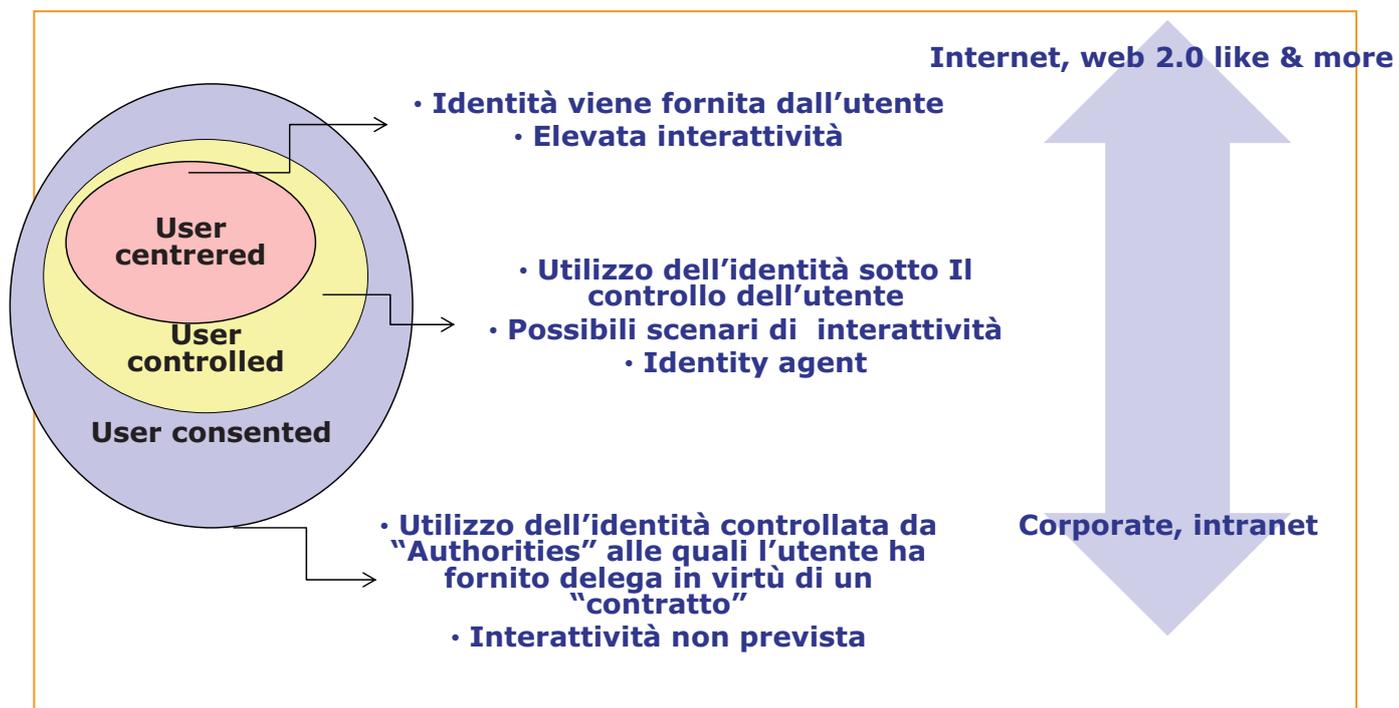




- La posta elettronica certificata
- La firma digitale
- La gestione dei ruoli professionali



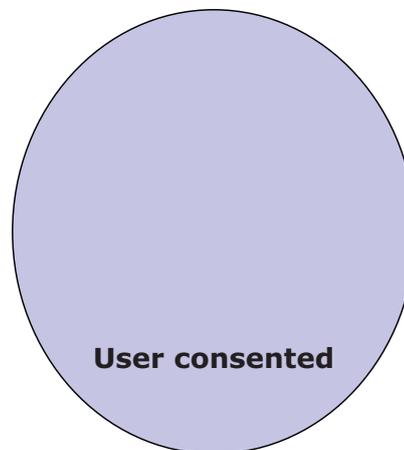
Modelli di gestione delle identità digitali





Modelli di gestione delle identità digitali / 2

Domain centric identity

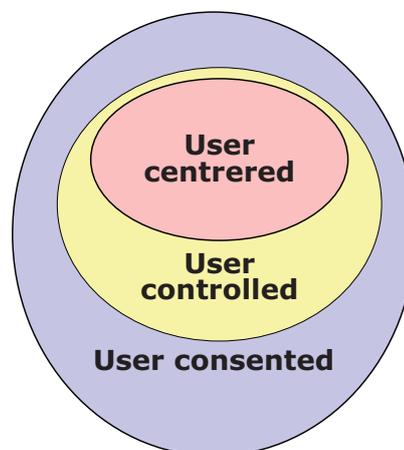
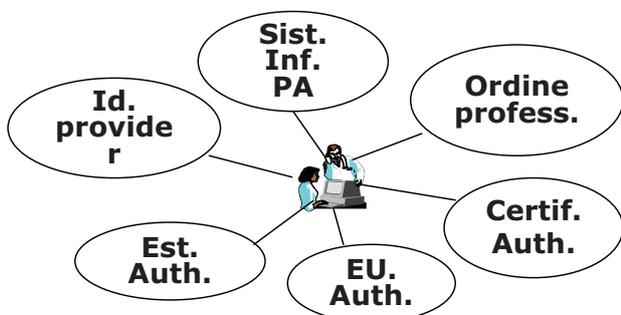


- Responsabilità dell'amministrazione
- No interoperabilità con altre PA
- Scarsa automazione
- Bassa scalabilità



Modelli di gestione delle identità digitali / 3

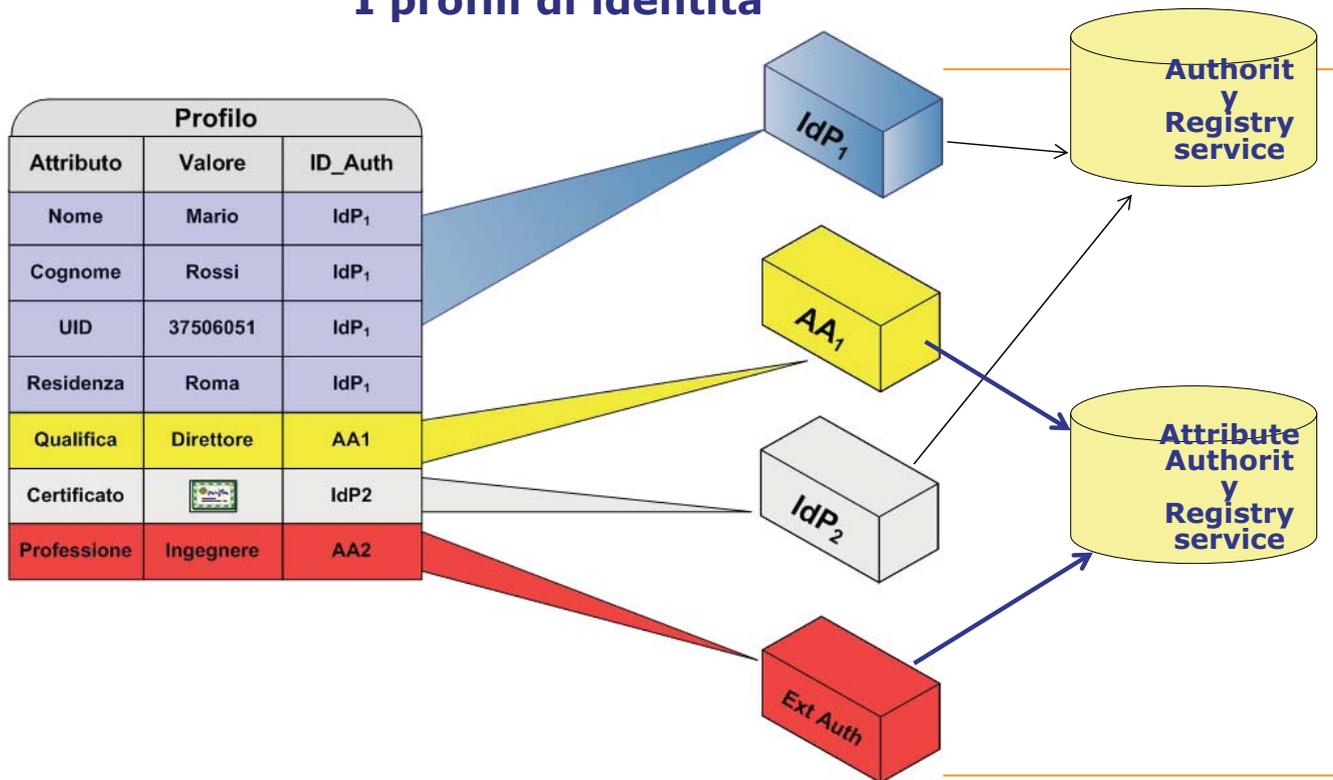
Federated identity



- Responsabilità ripartita
- Interoperabilità con altre PA
- Scalabile
- Adatto a processi automatizzabili



I profili di identità



Il modello di Gestione Federata delle Identità Digitali SPC

Coordinamento della federazione - DigitPA

Elementi della federazione
- Soggetti deputati

ID Providers, Attr. Auth.s

ID Providers Reg., Attr. Auth.s reg.
Codifiche ruoli, modelli *saml2*

Servizi sussidiari - DigitPA, Regioni

Profile Auth., Federation gateway

Per gli
utenti

Per i Service
Providers
(Amministrazioni)



Alcuni concetti di base

CAD

autenticazione informatica: la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, ...

Decreto
Regole
tecniche
SPc

autorità di autenticazione: la struttura che consente l'autenticazione in rete di un soggetto o di un sistema informatico o di un servizio

L'autenticazione in ambito SPC viene effettuata sotto la responsabilità dell'ente che eroga un servizio sulla base di un insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto

autorità di identificazione: la struttura che consente l'identificazione di un soggetto attraverso le modalità previste dall'art. 66 del Codice;

autorizzazione: l'insieme di attività che consentono l'accesso ad un servizio o una risorsa a chi, preventivamente identificato o autenticato, possiede gli attributi o il ruolo necessario;

autorità di attributo e ruolo: la struttura che ha la potestà di attestare attributi e ruoli ai fini dell'erogazione di un servizio;



DPCM Regole tecniche: principi generali

Economicità nell'utilizzo dei servizi di rete, di interoperabilità e di supporto alla cooperazione applicativa

Gli Organismi di attuazione e controllo, secondo gli indirizzi e le indicazioni della Commissione e nel rispetto delle presenti Regole tecniche, progettano e realizzano, anche attraverso la stipula dei contratti quadro di cui all'art. 83 del Codice, gli interventi che facilitino e sostengano lo sviluppo di servizi di rete, di interoperabilità e di cooperazione applicativa tra le Amministrazioni che utilizzano il SPC. A tal fine, attuano misure che favoriscano, in particolare:

l'accesso ai servizi attraverso sistemi di autenticazione distribuiti e federati, al fine di gestire con maggiore efficienza identità digitali e ruoli attribuiti e certificati dalle autorità di autenticazione e dalle autorità di attributo e ruolo;



DPCM R. tec.: gestione delle identità digitali

1. Nell'ambito del SPC l'autorizzazione all'accesso ai servizi si basa sul riconoscimento delle **identità digitali delle persone fisiche e dei sistemi informatici utilizzati** per l'erogazione dei servizi medesimi. L'autorizzazione ricade sotto la responsabilità dell'ente erogatore e può avvalersi di **meccanismi di mutuo riconoscimento nell'ambito di sistemi federati di gestione delle identità digitali**, secondo criteri e modalità stabiliti dalla Commissione.
2. I servizi disponibili in SPC possono operare secondo diversi livelli di gestione delle identità digitali:
 - servizi che non richiedono alcuna identificazione o autenticazione;
 - servizi che richiedono l'autenticazione in rete da parte di un'autorità di autenticazione;
 - servizi che richiedono, per le persone fisiche, l'identificazione in rete da parte di un'autorità di identificazione;
 - servizi che richiedono per gli utenti, oltre all'identificazione, l'attestazione di attributi e/o ruoli, che ne qualifichino ulteriormente le funzioni e/o i poteri.



Le funzioni dei Servizi Infrastrutturali di gestione id. digitali

Gestione federata delle identità digitali di quel cosiddetto "circle of trust" attraverso:

- l'accreditamento e la validazione all'interno del dominio federativo;
- la pubblicazione degli enti che ricoprono il ruolo di certificatori/validatori delle identità digitali e dei ruoli;
- la definizione di un insieme di accordi (policy) che comprendono un modello comune di cooperazione all'interno della federazione;
- la definizione delle responsabilità nell'ambito della cooperazione, utilizzando gli accordi di servizio;
- servizi di federation gateway e profile authority.

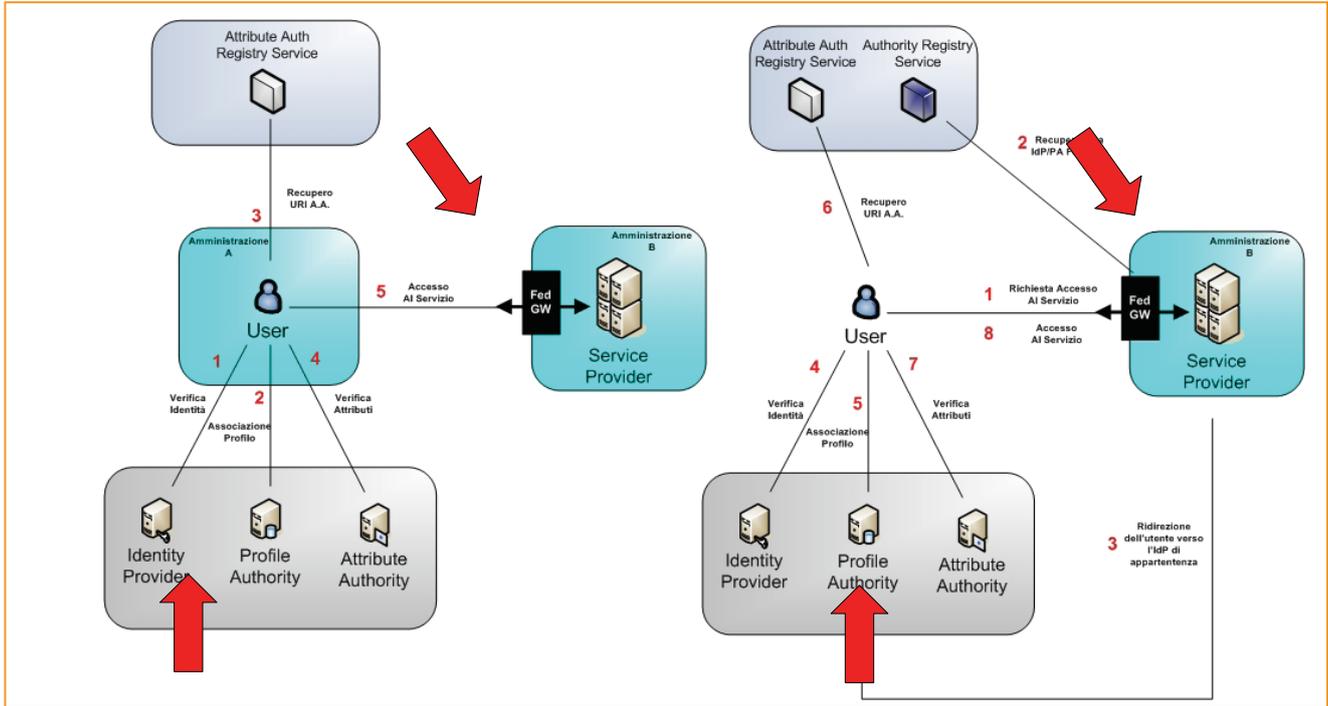


Gli scenari di Gestione Federata delle

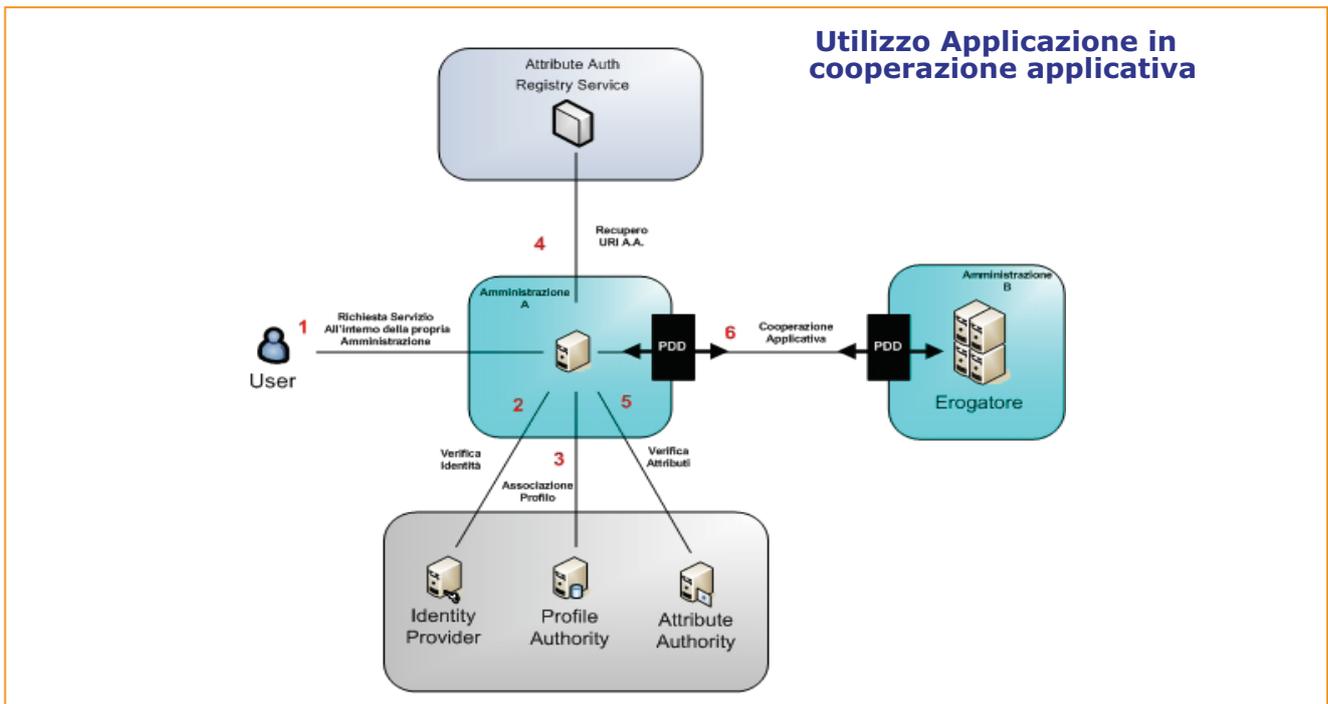
Utente interno ad un'amministrazione

Identità Digitali SPCoP

Utilizzo Applicazione Federata via Web



Gli scenari di Gestione Federata delle Identità Digitali SPCoP / 2





Governo italiano

Residenza del Consiglio dei Ministri

Grazie !