CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

Gli aspetti organizzativi per la gestione delle identità e del controllo degli accessi

Ing. Gianfranco Pontevolpe
Responsabile Ufficio Dematerializzazione

Centro Nazionale per l'Informatica nella Pubblica Amministrazione

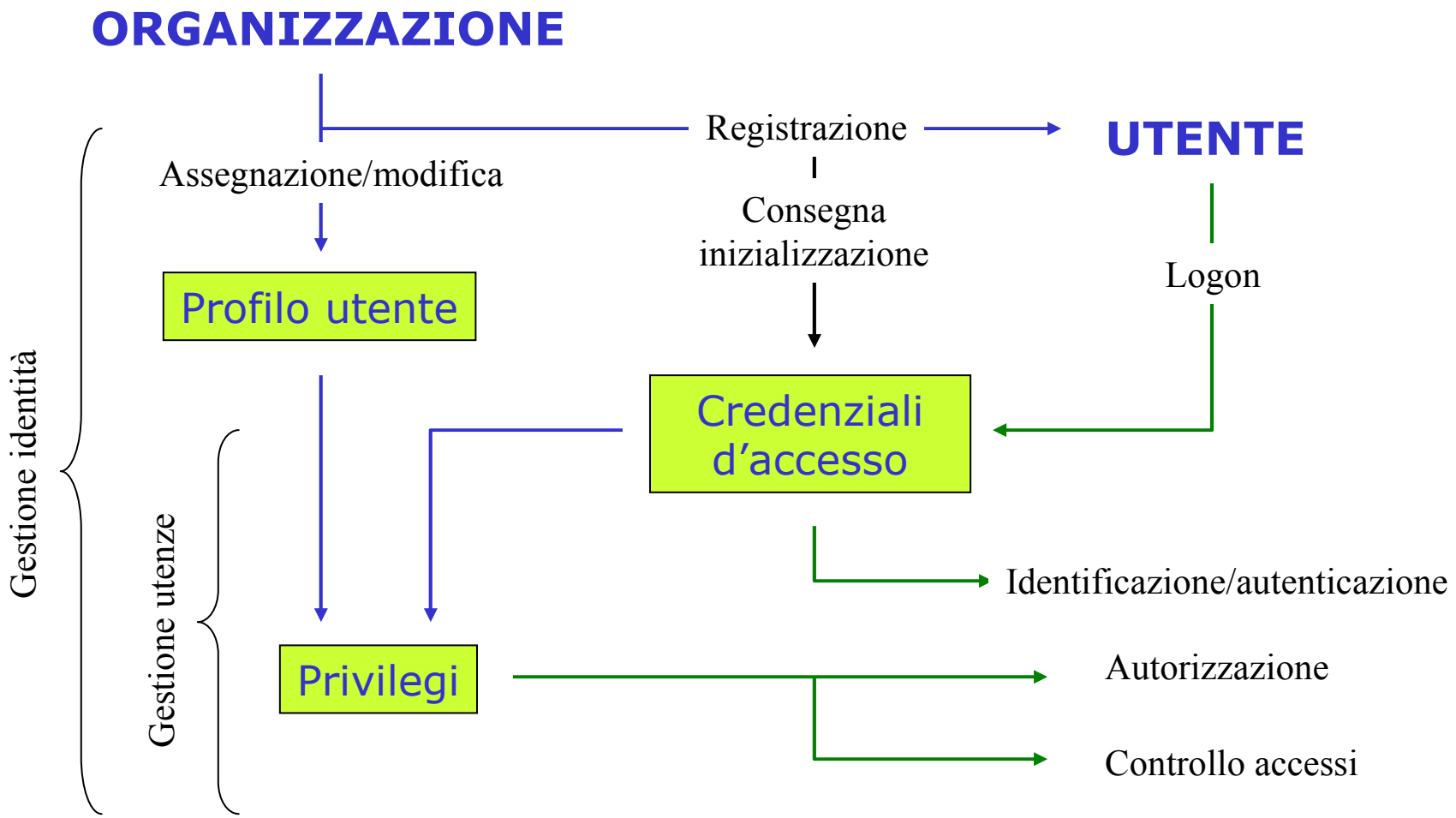
Premessa

Gestione delle identità

Gestione dati identificativi personali
(*Id management*)

Gestione utenze
(*account management*)

Schema di riferimento

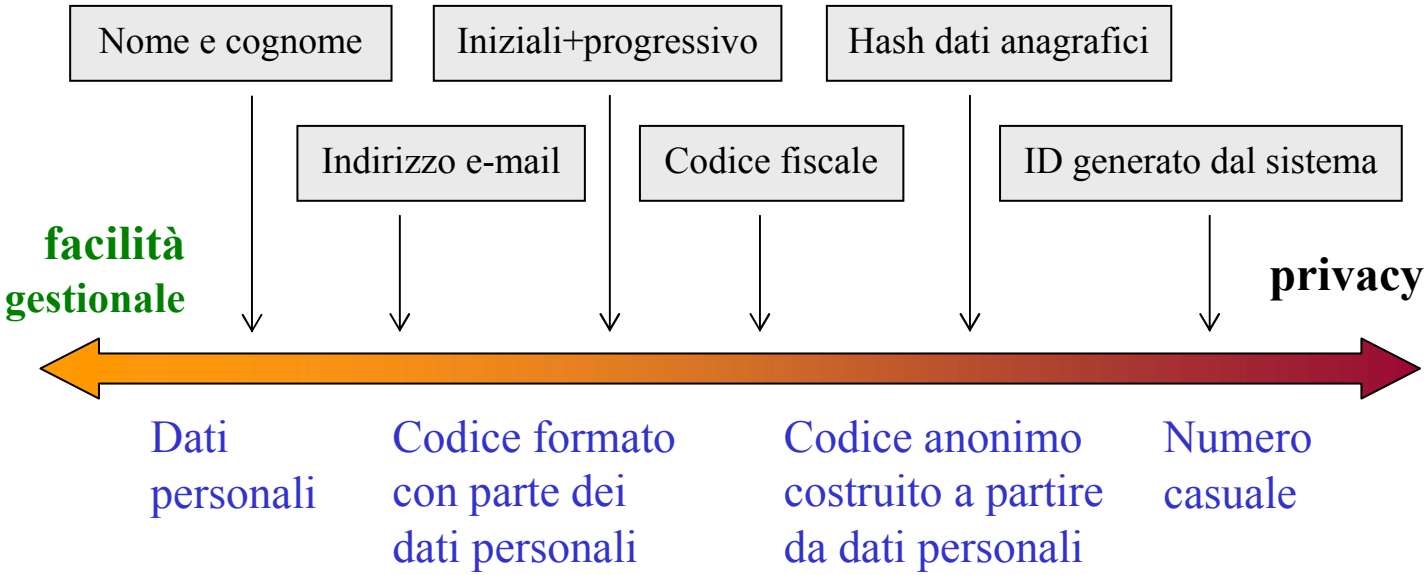


FONTE: Quaderno CNIPA n.23 – Modello organizzativo nazionale di sicurezza ICT per la PA – Appendice A.2

Gestione identificativi personali e gestione delle utenze

- In un sistema ideale
  - La gestione delle utenze è separata dalla gestione degli identificativi personali
  - L'utenza viene associata ad un soggetto/entità ed aggiornata per cambiamenti che implicano la modifica dei privilegi (es. modifica ruolo)
  - L'utente fornisce credenziali che attestano la titolarità ad ottenere il servizio ma non fornisce identificativi personali
  - E' possibile mettere in relazione l'utenza con il soggetto o i soggetti che ne sono responsabili solo in caso di problemi operativi o di sicurezza
  - Le informazioni di collegamento tra utente e utenza sono detenute da soggetti terzi affidabili

Criteri per la formazione dell'identificativo utente (userid)



FONTE: Quaderno CNIPA n.23 – Modello organizzativo nazionale di sicurezza ICT per la PA – Appendice A.2

Il modello italiano per la gestione dell'identità

- Un sistema istituzionale affidabile per l'identificazione in rete

  Carta d'Identità elettronica (CIE) e
  Carta Nazionale dei Servizi (CNS)

- Un insieme di regole per la cooperazione applicativa

  Sistema Pubblico di Connettività (SPC)

La Carta d'Identità Elettronica e Carta Nazionale dei Servizi

- La Carta d'Identità Eletronica (CIE)
  - È una carta ibrida composta da due differenti tecnologie: un circuito elettronico e una banda ottica
  - Contiene la foto e i dati personali del titolare
  - Sul retro della carta, oltre ad altri dati personali, sono installati il circuito elettronico, la banda ottica e un ologramma di sicurezza
- La Carta Nazionale dei Servizi (CNS)
  - Come la CIE, è uno strumento di autenticazione in rete: consente l'accesso ai servizi resi disponibili per via telematica dalle PP.AA.
  - Ma non è un documento per l'identificazione "a vista"

Altre carte istituzionali

- Dal Codice dell'Amministrazione Digitale
  - "Le tessere di riconoscimento rilasciate dalle amministrazioni dello Stato ai sensi del decreto del Presidente della Repubblica 28 luglio 1967, n. 851, possono essere realizzate anche con modalità elettroniche e contenere le funzionalità della carta nazionale dei servizi per consentire l'accesso per via telematica ai servizi erogati in rete dalle pubbliche amministrazioni"

I servizi di e-government mediante CIE e CNS

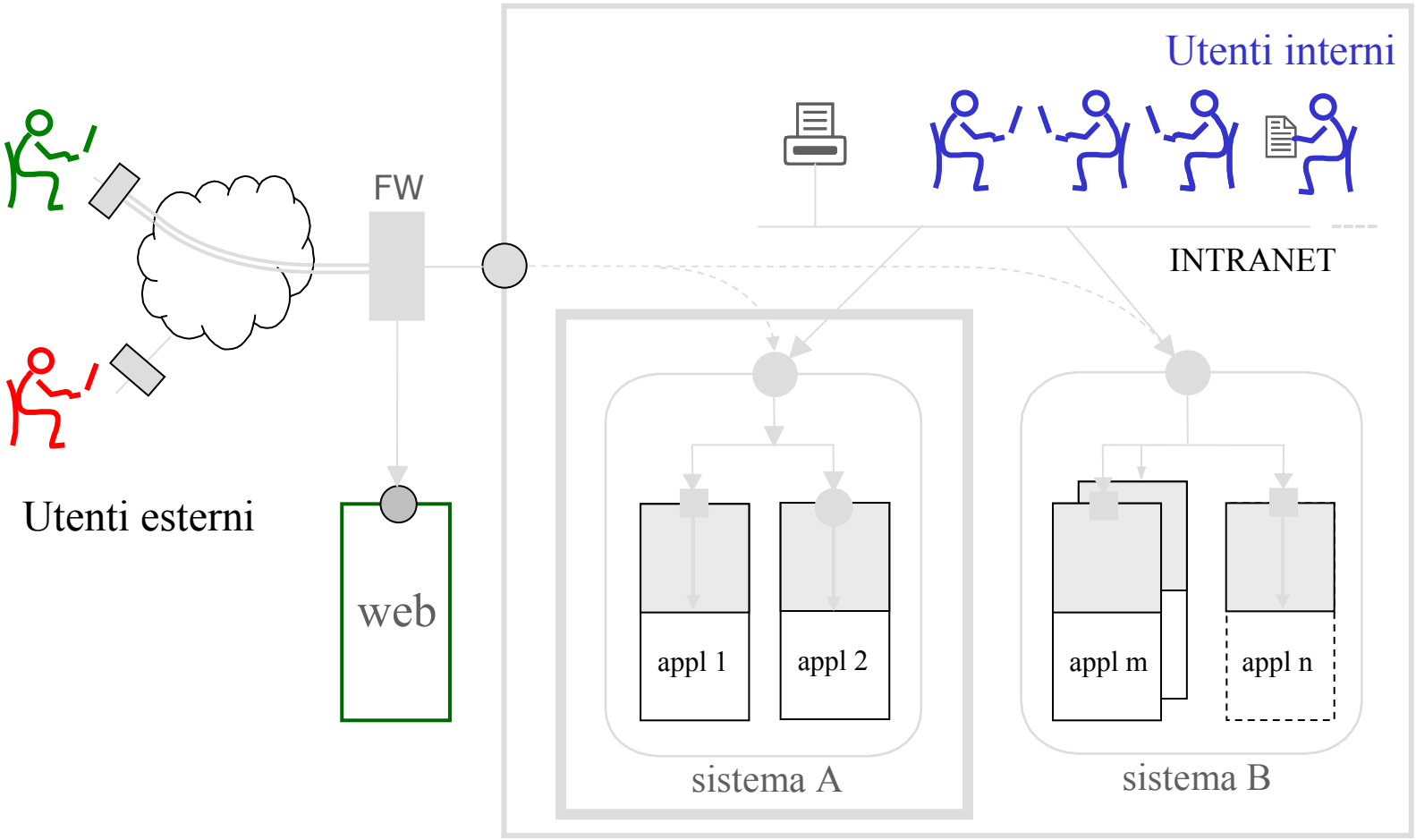
- Tutte le PP. AA. che erogano servizi in rete devono garantirne l'accesso ai titolari di CNS e CIE
- La CNS può supportare funzioni di pagamento (anche tramite la banda magnetica)
- La CIE e CNS possono contenere applicazioni "locali"

NOTA: Il Codice dell'Amministrazione Digitale all'articolo 4 comma 1 prevede: "La carta d'identità elettronica e la carta nazionale dei servizi costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'autenticazione informatica

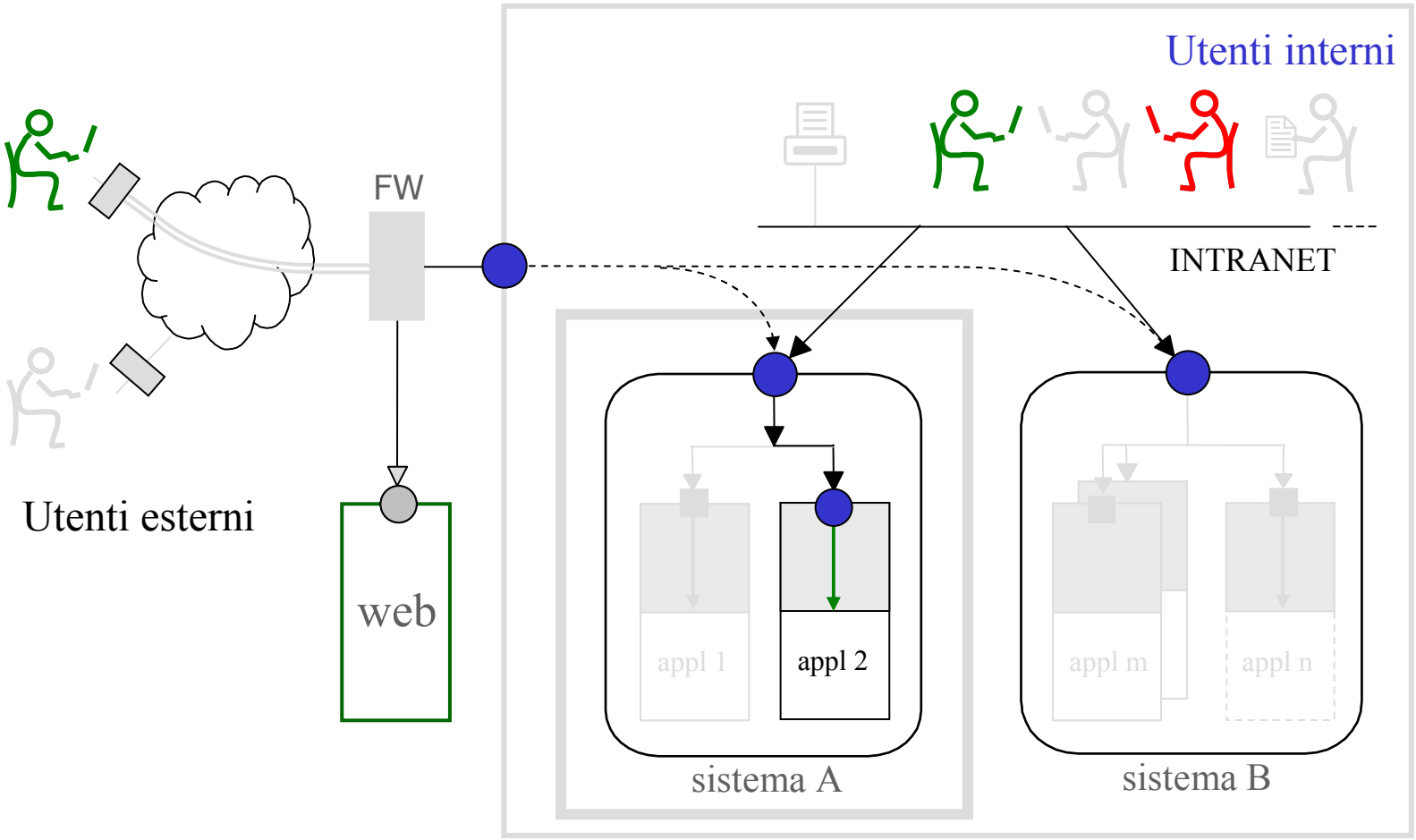
CIE/CNS e anonimato

- Il campo “common name” del certificato di autenticazione della CIE contiene l’hash dei dati personali
- Il campo “common name” del certificato di autenticazione della CNS contiene il codice fiscale

La gestione degli utenti



Identificazione/autenticazione



Identificazione degli utenti nella PA

- Cittadini
  - Comuni (CIE)
  - Pubbliche amministrazioni (CNS)
  - Certificatori di firma digitale, limitatamente alla sottoscrizione dei documenti
- Utenti interni
  - Amministrazione di appartenenza

Autenticazione informatica

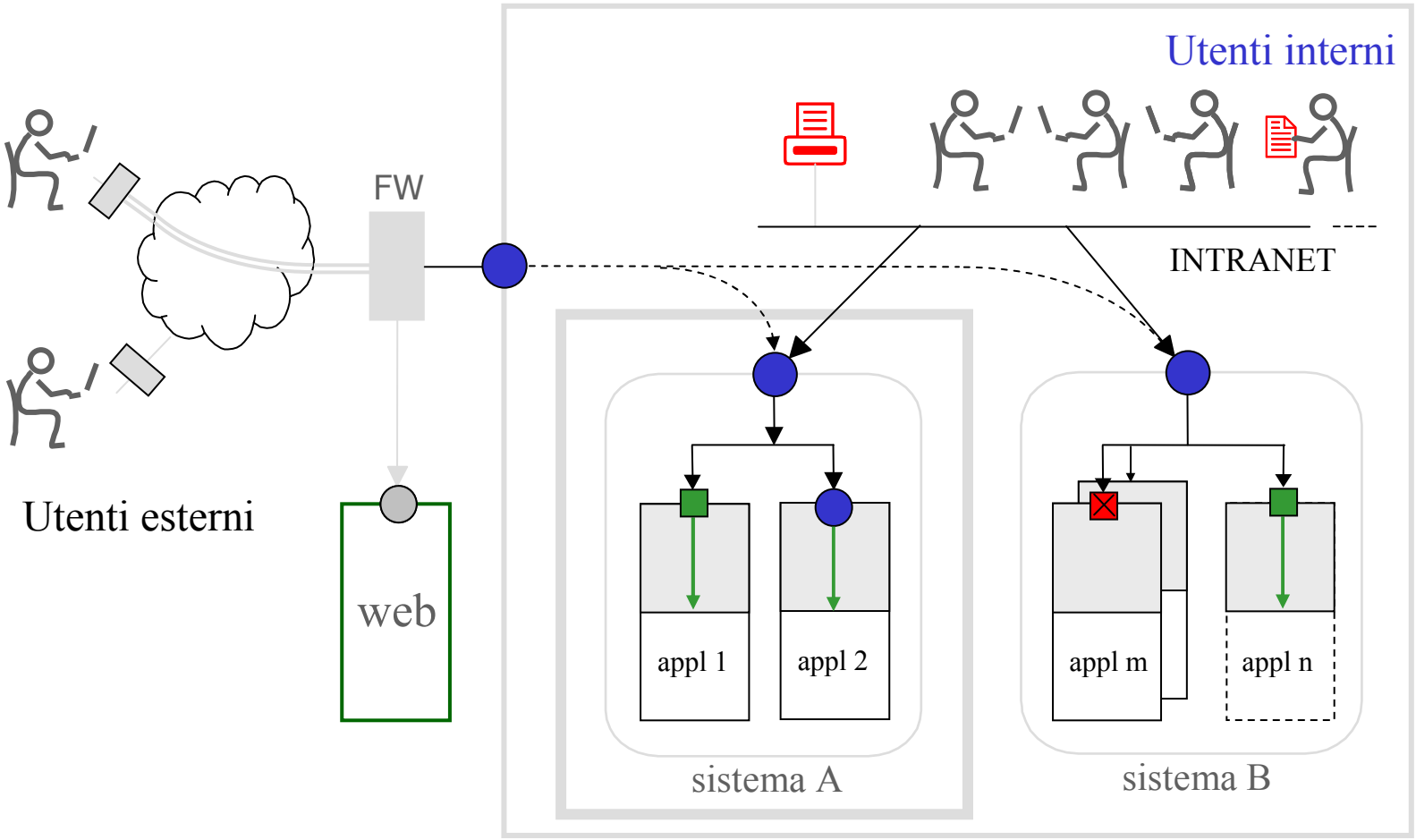
- La validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne distinguono l'identità nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso

FONTE: Codice dell'Amministrazione Digitale, articolo 1

Autenticazione degli utenti nella PA

- Cittadini
  - CIE
  - CNS e altre carte per l'accesso ai servizi in rete
  - PIN, password (*transitoriamente*)
- Utenti interni
  - Password
  - Metodi Challenge/Response
    - Certificati digitali
  - Dispositivi personali (token)
    - Smart card
  - Caratteristiche biometriche

Verifica delle autorizzazioni



Autorizzazione

- Fase in cui si verifica se l'utenza è autorizzata o meno a svolgere la funzione richiesta
  - funzioni del sistema operativo
  - funzioni dei prodotti di gestione delle utenze
  - programmi

NOTA: Autenticazione ed autorizzazione di norma sono svolte ad inizio sessione, può essere opportuno ripeterle al momento dell'accesso a funzioni critiche

Controllo accessi

- Il controllo accessi verifica se l'utenza è abilitata o meno ad eseguire operazioni elementari
- Può essere svolto da:
  - sistema operativo (ACL, RBAC)
  - DBMS
  - Programmi
- Limita i danni che possono essere provocati da programmi malevoli quali (virus, cavalli di troia, ecc.)

Organizzazione della sicurezza nelle amministrazioni

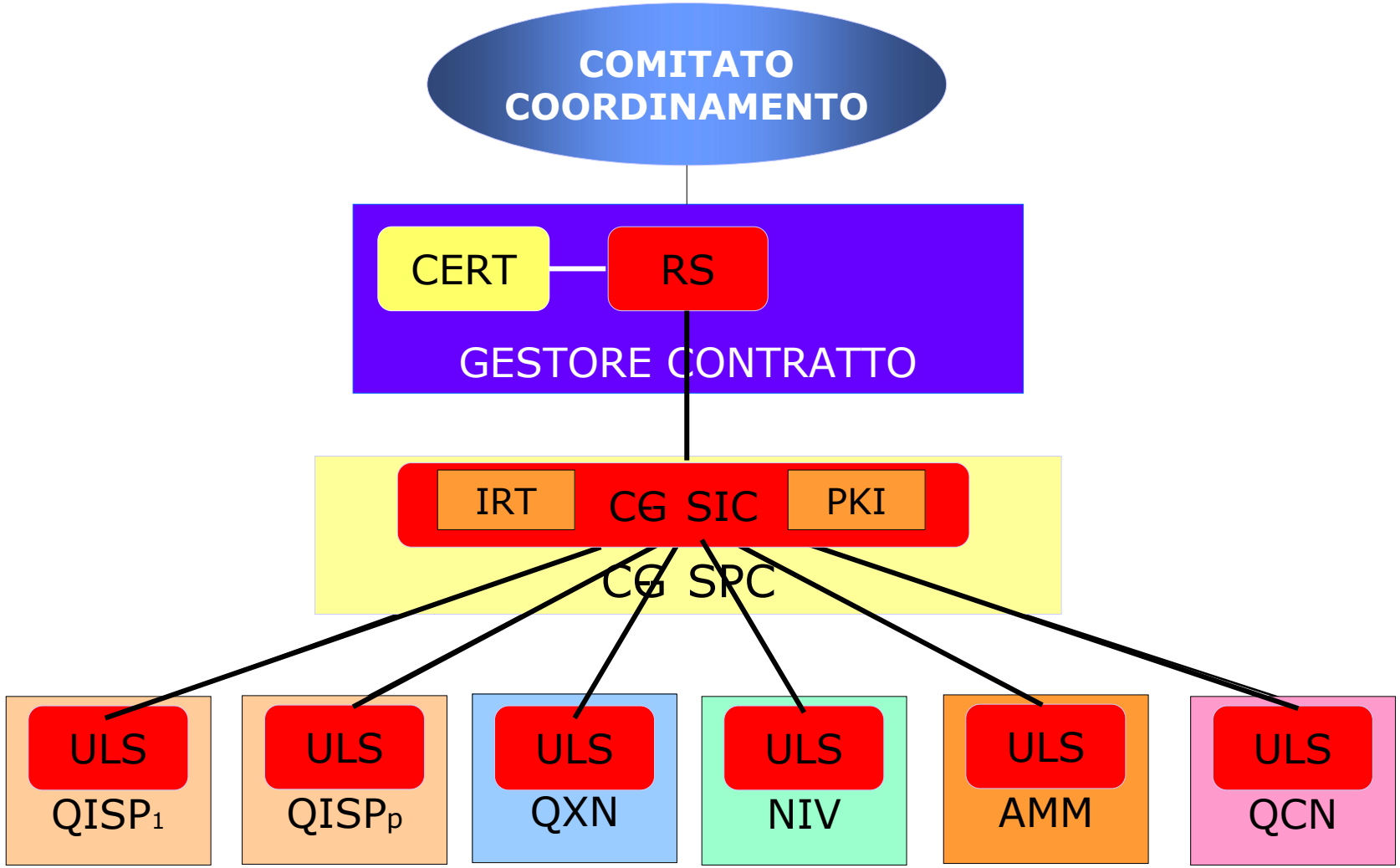
- Ruoli previsti dalla direttiva del 16 gennaio 2002
- Ulteriori strutture che dovranno partecipare all'organizzazione della sicurezza
- I ruoli non coincidono con specifici uffici o figure professionali ma, a seconda delle dimensioni e dei compiti dell'amministrazione, più ruoli possono far capo ad una stessa struttura o ad uno stesso soggetto

Aggregazioni consigliate per le diverse tipologie di amministraz.

	ammin. complesse presenti su più sedi su territorio nazionale	grosse ammin.. presenti su più sedi in una stessa città	grosse ammin.. presenti in una sola sede	ammin. di media complessità	piccole ammin.
Ministro, Direttore, Sindaco …	✓	✓	✓	✓	✓
Consigliere tecnico per la sic. ICT	✓				
Comitato per la sicurezza ICT	✓	✓	✓	✓	
Responsabile della sicurezza ICT	✓	✓	✓	✓	✓
Comitato tecnico	✓	✓	✓		
Ufficio di sicurezza centrale	✓				
Referente locale della sicurezza	✓	✓			
Gruppi di lavoro specifici	✓	✓	✓		
Strutture per l'emergenza	✓	✓	✓	✓	

FONTE: Quaderno CNIPA n.23 – Modello organizzativo nazionale di sicurezza ICT per la PA – Capitolo 4

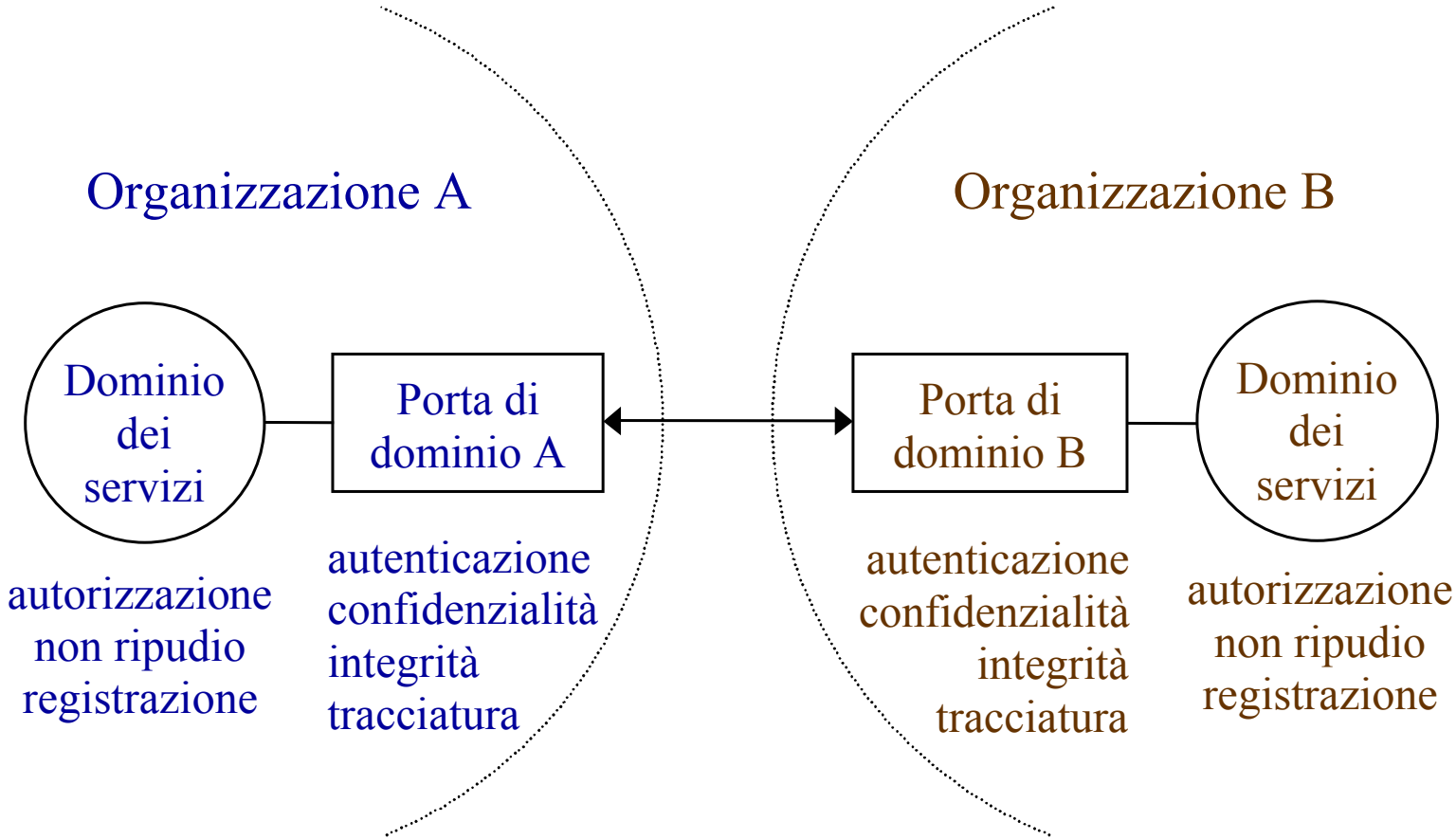
Organizzazione sicurezza SPC



I criteri di sicurezza per la cooperazione

- Le informazioni inerenti i soggetti destinatari dei servizi sono custodite esclusivamente dalle organizzazioni istituzionalmente competenti
- Le funzioni utente forniscono al sistema il minimo insieme di informazioni necessario per dimostrare la titolarità ad usufruire del servizio basandosi sugli strumenti di autenticazione nazionali (CIE, CNS)
- Le eventuali informazioni aggiuntive necessarie per l'autorizzazione (ruolo, funzione, ecc.) sono ottenute mediante accessi "sicuri" verso gli enti/autorità competenti
- Ciascun ente mantiene traccia delle sole operazioni di propria competenza

Modello di sicurezza per la cooperazione



Identificazione delle entità

- Le regole di comunicazione e cooperazione prevedono scambi di dati tra varie entità appartenenti ad organizzazioni diverse
  - soggetti
  - apparati
  - processi
- Occorre disporre di meccanismi per riconoscere ed autenticare le entità con le quali si interagisce
- I soggetti vengono riconosciuti tramite gli strumenti istituzionali per l'accesso ai servizi in rete (CIE, CNS, carta del dipendente …)
- Le altre entità sono autenticate tramite certificati di autenticazione (conformi allo standard *ws security*) gestiti da un articolato sistema di PKI

Autorizzazione, ruoli e SAML

- L'autorizzazione all'accesso a servizi o a dati spesso dipende dal ruolo del soggetto che ha innescato il processo
- Ai fini della cooperazione, è necessario disporre di strumenti per trasmettere tale informazione in modo sicuro
- Il SAML (Security Assertion Markup Language) risponde a questa esigenza poiché permette di codificare in modo standard asserzioni utilizzabili per l'autorizzazione
- E' inoltre necessario disporre di
  - una modalità standard per codificare i ruoli
  - un sistema di certificazione dei ruoli

Gestione identificativi personali e gestione delle utenze in SPC

- Il modello di gestione dell'identità prevede
  - La gestione delle utenze è separata dalla gestione degli identificativi personali GFID
  - L'utenza viene associata ad un soggetto/entità ed aggiornata per cambiamenti che implicano la modifica dei privilegi (es. modifica ruolo) Modello di cooperaz.
  - L'utente fornisce credenziali che attestano la titolarità ad ottenere il servizio ma non fornisce identificativi personali CIE, CNS, Certificati (PKI)
  - E' possibile mettere in relazione l'utenza con il soggetto o i soggetti che ne sono responsabili solo in caso di problemi operativi o di sicurezza Registry services
  - Le informazioni di collegamento tra utente e utenza sono detenute da soggetti terzi affidabili Identity providers, Attribute autorities

Per maggiori informazioni

www.cnipa.gov.it