

La sicurezza nel Sistema Pubblico di Connettività

Ing. Gianfranco Pontevolpe
Responsabile Ufficio Tecnologie per la sicurezza

Centro Nazionale per l'Informatica nella Pubblica Amministrazione



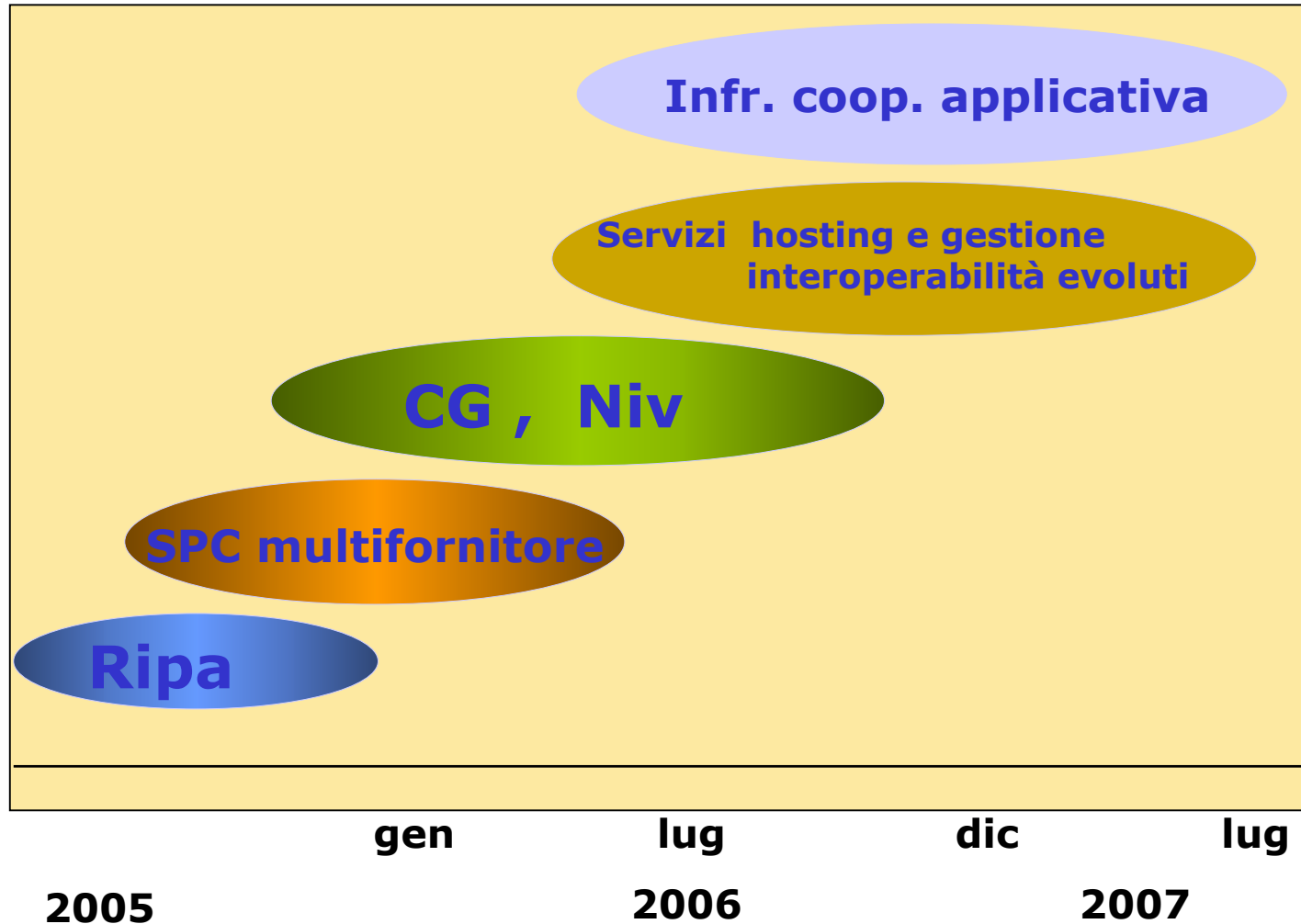
Sistema pubblico di connettività

Art 73 del CAD

Il SPC è l'insieme di **infrastrutture tecnologiche** e di **regole tecniche**, per lo sviluppo, la condivisione, l'integrazione e la diffusione del patrimonio informativo e dei dati della pubblica amministrazione, **necessarie per assicurare l'interoperabilità** di base ed evoluta e la **cooperazione applicativa** dei sistemi informatici e dei flussi informativi, **garantendo la sicurezza**, la riservatezza delle informazioni, nonché la salvaguardia e l'autonomia del patrimonio informativo di ciascuna pubblica amministrazione.

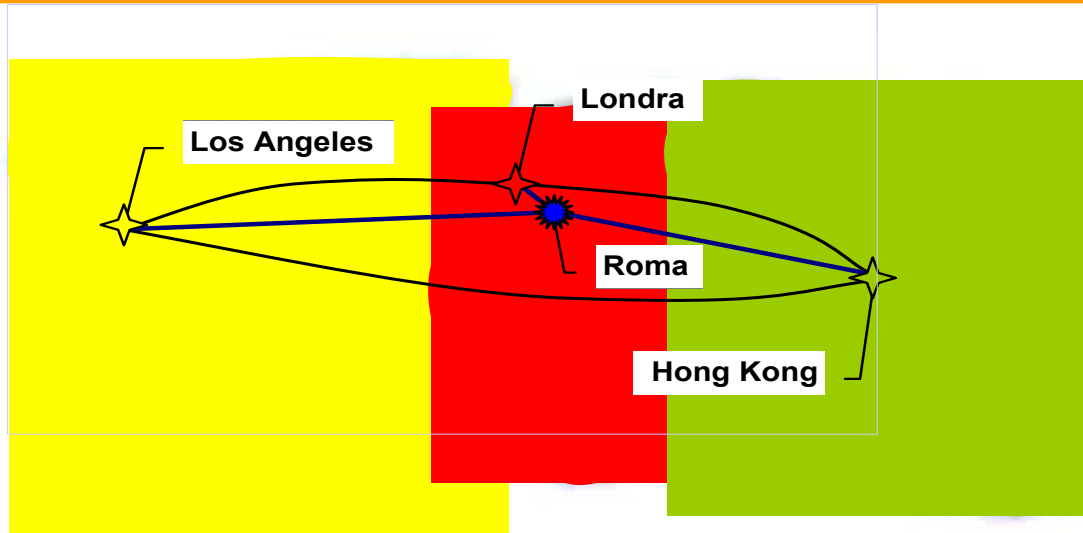


Gare per la realizzazione delle componenti del SPC





La rete internazionale (RIPA)



- Il partner è RTI EDS-Infonet
- E' in corso di realizzazione con le amministrazioni MAE e Min. Difesa alle quali si sono aggiunte Dogane, ICE ed ENIT
- Sono attive 300 sedi su 352 del MAE e 55 su 70 del Min Difesa ed il piano di realizzazione si completerà nel 2006



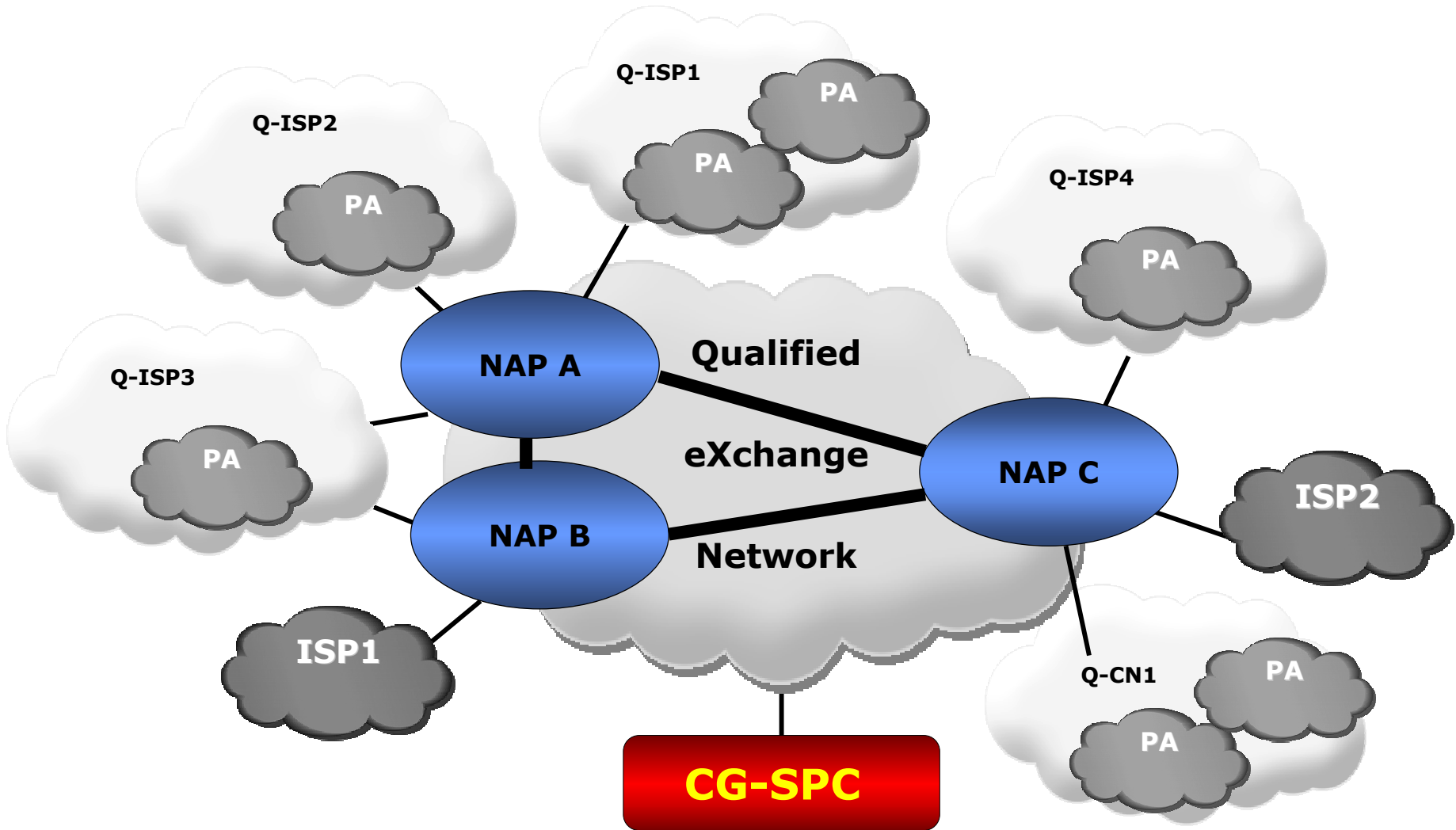
SPC multifornitore

Il Sistema multifornitore comprende:

- Servizi di trasporto
- Servizi di supporto (indirizzamento, gestione indirizzi pubblici ,domain name service)
- VoIP
- Interoperabilità di base : posta elettronica, trasporto di protocolli proprietari e web hosting/housing/mirroring
- Manutenzione ed assistenza
- Servizi di sicurezza



Infrastruttura di comunicazione multifornitore





Servizi di hosting e gestione

Hosting

- Realizzazione di siti web
- Servizi di redazione per siti web
- Adattamento delle applicazioni in modalità web
- Hosting di siti web

Gestione

- lan
- postazioni di lavoro
- server
- applicazioni

Supporto

- Help desk
- Risorse professionali
- Formazione



Servizi di interoperabilità evoluti e cooperazione applicativa

Messaggistica

- Posta elettronica (esclusiva, certificata)
- Archiving
- Unified messaging

Cooperazione applicativa

- Porta di dominio
- Integrazione applicativa
- Composizione e coordinamento di servizi

Sicurezza applicativa

- Identity & Access management
- Firewall applicativo

Supporto

- Risorse professionali, help desk, formazione



Infrastruttura nazionale per la cooperazione applicativa

Servizi di infrastruttura (SICA)

- Registro di servizi (**comprende Indice PA**)
- Catalogo di schemi/ontologie
- Gestione delle identità federate
- Indice dei soggetti (**comprende Rubrica PA**)
- Servizi di certificazione (rilascio e gestione dei certificati SpCoop)
- Servizi di monitoraggio, gestione e sicurezza interna

Qualificazione

- Porta di dominio campione
- Qualificazione SICA secondari



Confronto modelli RUPA ed SPC

■ Modello RUPA

- Pensata per PAC →
- Centralizzata →
- Monofornitore →

■ Modello SPC

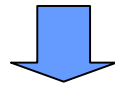
- Federata (PAC + PAL)
- Distribuita
- Multifornitore
- Nuove tecnologie
 - Cooperazione applicativa (SOA)
 - VOIP
 - Wireless
- Infrastrutture condivise
- Centri servizi

Una MAGGIORE COMPLESSITÀ necessita di una MAGGIORE ATTENZIONE ALLA SICUREZZA da parte di tutti i soggetti aderenti. Previsto un MAGGIORE SUPPORTO da parte del CNIPA, dei centri servizi e dei fornitori.



La strategia di sicurezza

- L'intero SPC deve avere caratteristiche di sistema fidato



Ridotte vulnerabilità
Accesso controllato

- Tutti gli attori che partecipano al SPC devono impegnarsi ad assicurare tale requisito, anche curando la separazione con ambienti non fidati
- I procedimenti più "critici" possono avvalersi di ulteriori servizi di sicurezza



Servizi di sicurezza gara multifornitore

- Servizi base (servizi di cui ogni amministrazione nel SPC deve dotarsi per garantire il livello minimo di sicurezza previsto)
 1. Firewall Management
 2. Network Intrusion Detection System Management
 3. Event & Log Monitoring Management
- Servizi evoluti (servizi di cui ogni amministrazione nel SPC può dotarsi qualora intenda dotarsi di un livello di sicurezza superiore al minimo stabilito)
 1. Antivirus & Content Filtering Management
 2. VPN (in ambito SPC) Management
 3. Hardening dei sistemi
 4. Network Address Translation Management
 5. Host Intrusion Detection System Management
 6. Vulnerability Assessment

**OBBLIGATORI PER
CONNESSIONI A
RETI NON TRUSTED**

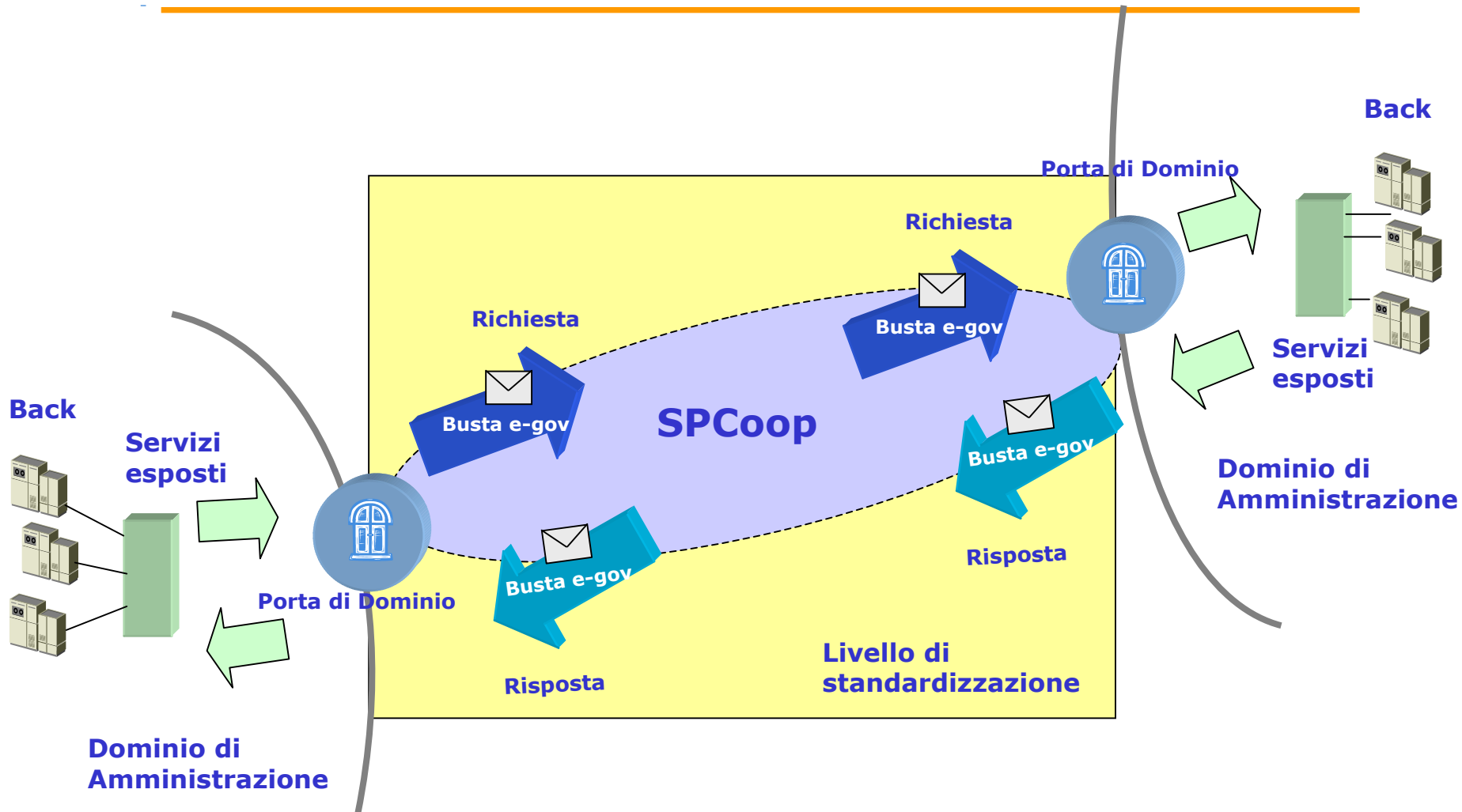


Servizi di sicurezza obbligatori

- Porta verso rete trusted (ambito intranet/infranet)
 - ELM
- Porta verso rete untrusted (ambito internet)
 - ELM
 - Firewall
 - NIDS
- Co-locazione degli ambiti infra/inter-net
 - Possibilità di filtraggio del traffico interamministrazione



La cooperazione



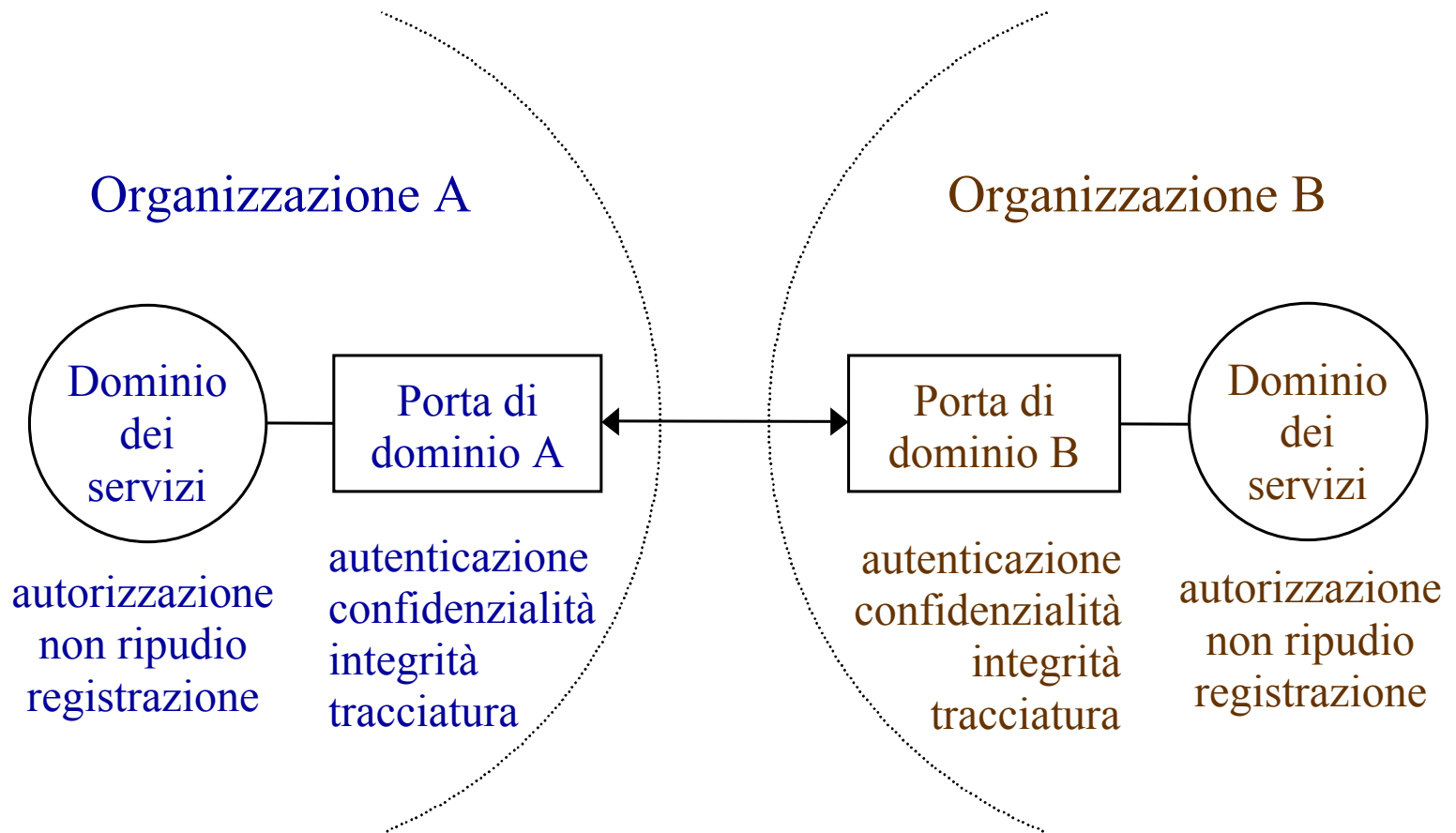


I criteri di sicurezza per la cooperazione

- 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, per fare ciò si basano sugli strumenti di autenticazione nazionali (Carta d'Identità Elettronica, Carta Nazionale dei Servizi)
- Le eventuali informazioni aggiuntive necessarie per l'autorizzazione (ruolo, funzione, ecc.) sono ottenute mediante accessi "sicuri" verso gli enti competenti
- Ciascun ente mantiene traccia delle sole operazioni di propria competenza



Modello di sicurezza per la cooperazione





L'organizzazione della sicurezza nel SPC

Le prime azioni verso la costruzione di un modello integrato per la sicurezza sono:

- La costituzione nella PA di una community di riferimento per la sicurezza ICT che si specializzerà per tipologie di problematiche
- L'individuazione dei riferimenti organizzativi per la Governance
- La coerenza ed omogeneità nelle politiche di sicurezza nelle infrastrutture condivise del SPC
- Gli accordi fra amministrazioni specifici per la sicurezza ICT

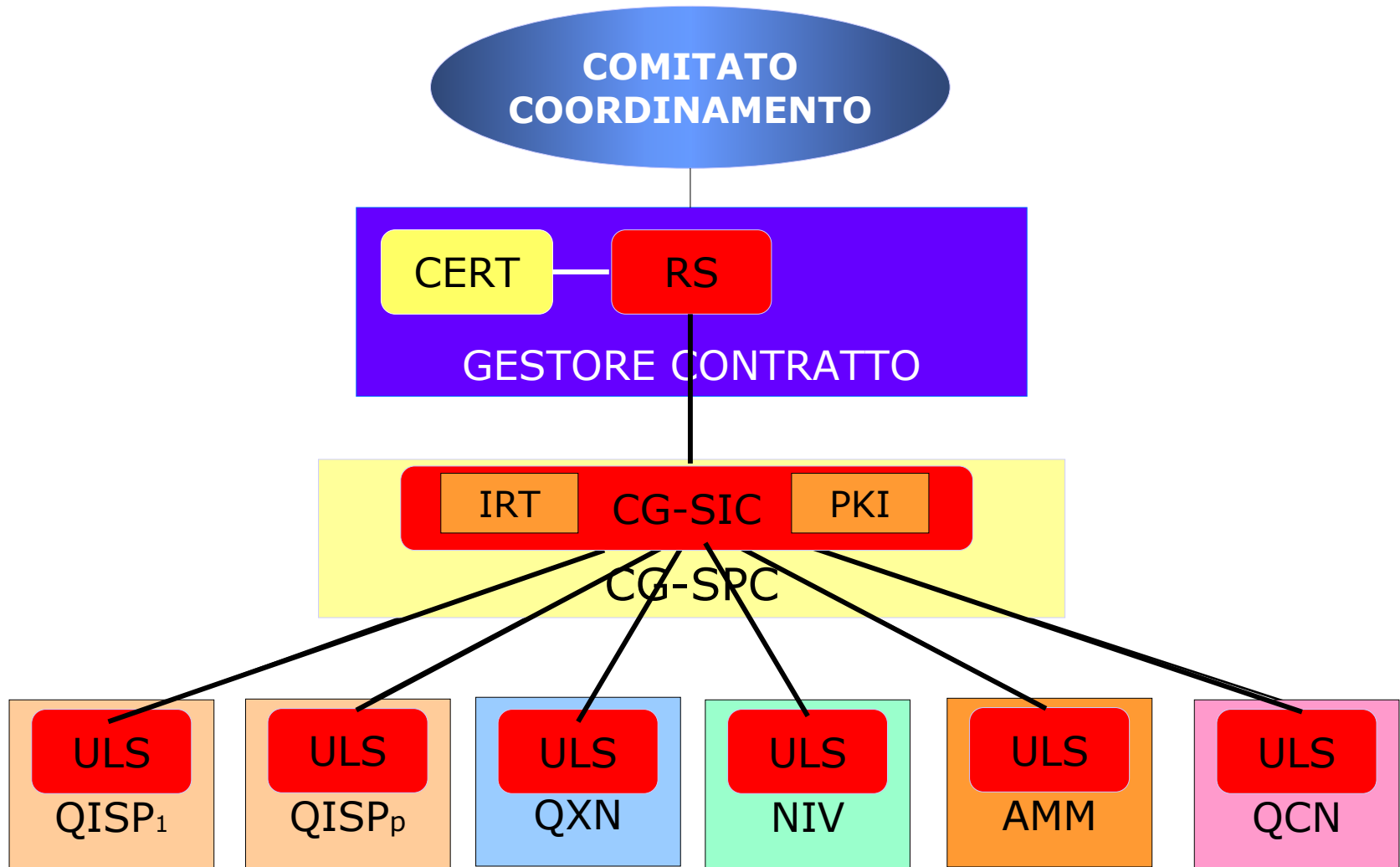


La gestione di SPC





Organizzazione sicurezza SPC





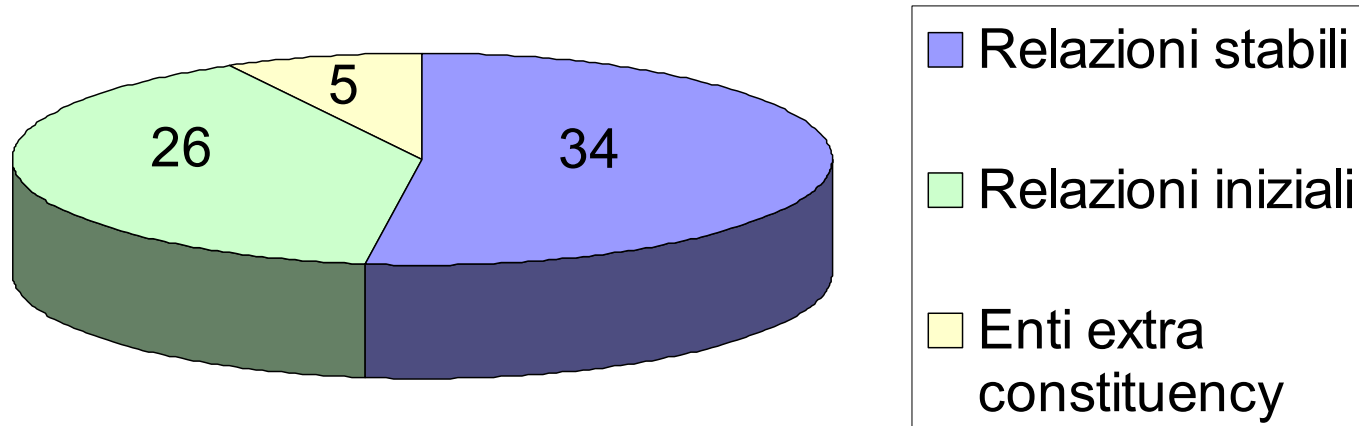
Il progetto GovCERT

- Proposto dal “Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni” ed approvato dal Consiglio dei Ministri per la Società dell’Informazione
- Attuato dal CNIPA attraverso la creazione di una “Unità di gestione degli attacchi informatici” -
- Finanziamenti resi disponibili a fine 2004
- Progetto iniziato a gennaio 2005



Constituency

Numeri attuali e distribuzione



Extra constituency: Garante protezione dati personali
CERT Regione Friuli Venezia Giulia
Agenzia del demanio
SOGEI
GARR



Servizi ed attività CERT-SPC e CG-SIC

Reattivi

Early warning

CERT

Gestione Incidenti

Analisi
Supporto alla risposta
Coordinamento della risposta

CG

Gestione Vulnerabilità

Analisi
Supporto alla risposta
Coordinamento della risposta

CG

Gestione Codici pericolosi

Analisi
Supporto alla risposta
Coordinamento della risposta

CG

Proattivi

Annunci

CERT

Verifiche

CG

Disseminazione
Informazioni

CG

Raccolta e
condivisione
informazioni

CG

Qualità e sicurezza

Analisi dei rischi

CG

Sensibilizzazione

CERT

Formazione

CG



CERT-SPC-R



È già operativo un gruppo di lavoro con le regioni per definire le modalità partecipazione al sistema di sicurezza SPC che siano:

- coerenti con le regole
- omogenee all'architettura definita per gli enti centrali
- compatibili con le specifiche realtà



Stato dell'arte

- Collaudo SOC e servizi di sicurezza in corso:
 - Completato per un Q-ISP
 - Completamento dei collaudi previsto entro fine giugno
- Collaudo QXN iniziato
- CG-Sic in corso di realizzazione
- Progetto pilota con ULS CONSIP



Per maggiori informazioni

www.cnipa.gov.it