



*Autorità per l'informatica nella pubblica amministrazione*

# *Outsourcing e Sicurezza nella Pubblica Amministrazione Italiana*

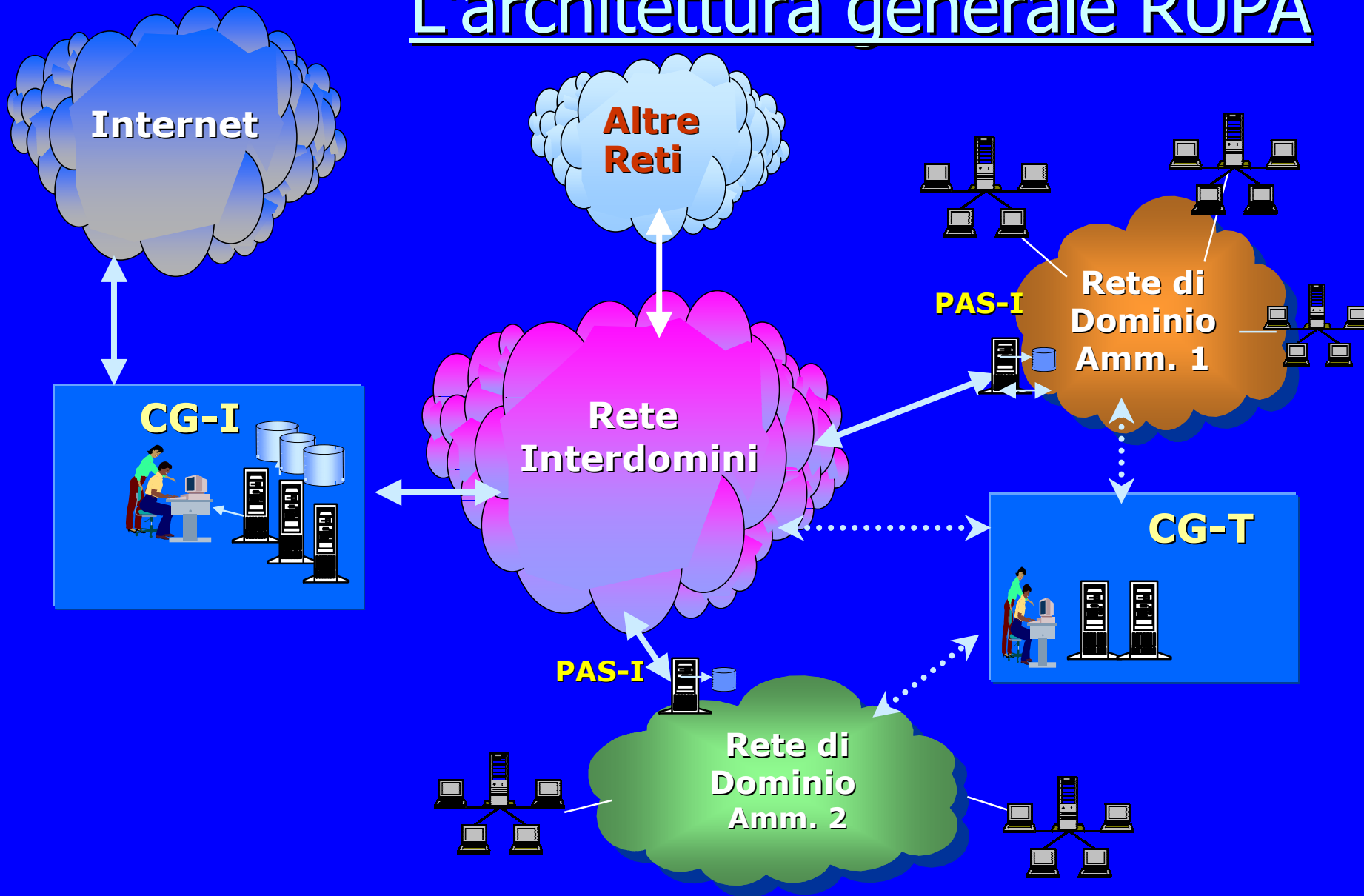
*Infosecurity - Milano, 23 gennaio 2002*

ing. Giovanni Manca  
manca@aipa.it

# Agenda

- La Certificazione della firma digitale
- La Rete Unitaria della P.A.
- La Rete Nazionale
- La sicurezza dei servizi di rete

# L'architettura generale RUPA



# Struttura di sicurezza

- Tre livelli distinti:
  - Trasporto, Interoperabilità e Cooperazione
- Strutture organizzative per la sicurezza in ciascun livello
- Controllo e supervisione esercitata dalla struttura per la sicurezza del Centro Tecnico attraverso:
  - Revisione dei Piani per la sicurezza
  - Audit
  - Test

# Cooperazione

- Complessa da realizzare ma indispensabile per disporre di un unico modello di interazione A2A e C2A.
- Si sviluppa nell'ambito della Rete Nazionale
- Trae beneficio dai modelli di interoperabilità garantiti da XML
- Integra l'autenticazione e la firma digitale con la logica delle applicazioni

# Sicurezza Trasporto

- **Trasparenza del CG-T rispetto ai flussi dei dati**
  - il CG-T ha solo funzioni di controllo e gestione della rete di trasporto
  - i dati non attraversano il CG-T
- **Protezioni fisiche e logiche del CG-T**
  - Autenticazione mediante "one-time-password" per l'accesso ai sistemi del CG-T da parte degli operatori
  - Segmentazione e protezione della LAN del CG-T mediante firewall
  - Sistemi di rilevamento degli attacchi in tempo reale
  - Sistemi antivirus
  - Sistemi di controllo dell'integrità dei file (log)
- **Protezioni fisiche e logiche degli apparati di rete**
- **Servizi di comunicazione protetta (IPSec)**

# Sicurezza Interoperabilità

Durante l'erogazione dei servizi alle Amministrazioni, il CG-I persegue i seguenti obiettivi fondamentali di sicurezza:

- Garantire riservatezza ed integrità delle informazioni gestite ed in transito
- Impedire a terzi di accedere o modificare dati e risorse di pertinenza delle Amministrazioni
- Impedire a personale interno e delle Amministrazioni di accedere o modificare dati e risorse senza averne autorizzazione
- Indirizzare al corretto destinatario le informazioni gestite

# Analisi del rischio

## ■ Esecuzione dell'analisi del rischio:

- In fase di progettazione
- Su base annua
- In seguito a gravi incidenti di sicurezza

## ■ Tre metodi di calcolo:

- Riduzione del rischio su parametri BS-7799
- Riduzione del rischio su parametri tecnologici
- Efficacia delle barriere su modello topologico

## ■ Risultati all'avvio del progetto:

- Riduzione globale del rischio superiore al 92%
- Livello di certificazione delle barriere sovraprogettato

# Sicurezza fisica

- **Controllo accessi con tre fattori di autenticazione:**
  - Smart card individuale
  - PIN
  - Elementi biometrici
  
- **Sorveglianza del perimetro e dei varchi tramite sistema di videocontrollo con registrazione continua**
  
- **Allarme perimetrale con sistema combinato motion detector, barriera microonde, infrarosso attivo/passivo, antisfondamento**
  
- **Sistema di allarme connesso al presidio di sicurezza antiterrorismo**

# Intrusion detection

- Sistema distribuito di **analisi del traffico** in real-time su tutti i segmenti di rete del CG-I:
  - Identificazione delle connessioni su porte "proibite"
  - Riconoscimento di "pattern" di attacco
  - Centralizzazione degli allarmi con visualizzazione sinottica e di dettaglio
- **Analisi continua** degli eventi sui **firewall** di perimetro ed interni per l'individuazione di condizioni anomale
- **Analisi off-line dei log** dei sistemi di sicurezza per l'evidenziazione di potenziali tentativi di attacco

# Antivirus

- Controllo antivirus sui messaggi di posta elettronica in transito all'interno del CG-I da/verso Internet e le Amministrazioni
- Controllo antivirus sui flussi FTP verso le amministrazioni
- Distribuzione ed aggiornamento centralizzato dei virus pattern sui server e sulle stazioni di lavoro

# Test di impenetrabilità

- Esecuzione periodica di test di impenetrabilità per garantire la costante sicurezza del sistema e delle Amministrazioni:
  - Sul sistema nel suo complesso da:
    - Internet
    - Domini delle amministrazioni
  - Sulle singole macchine dalla stessa subnet
- Impiego di strumenti commerciali e public domain per analisi della sicurezza globale e delle singole applicazioni
- Possibilità per le Amministrazioni di eseguire autonomamente test di impenetrabilità sui sistemi del CG-I

## LA CERTIFICAZIONE DELLA FIRMA DIGITALE

- Outsourcing con contratto di quattro anni con POSTECOM sottoscritto il 10/10/2000
- Inizio delle attività a regime a marzo 2001
- Infrastruttura di certificazione
  - 30.000 dispositivi di firma
  - 60.000 certificati
  - 60.000 smart card
  - 10.000 marche temporali
- Le Amministrazioni devono adeguare i procedimenti amministrativi al fine di consentire l'uso efficiente della firma digitale

# Aspetti chiave della sicurezza

- Architettura segmentata e protetta del CG-I
- Isolamento dei domini
- Sistemi avanzati di protezione dagli attacchi esterni ed interni
- Autenticazione forte degli operatori
- Aggiornamento continuo del sistema per la sicurezza

# La rete nazionale

- Luogo virtuale dove si acquistano e si vendono i servizi che le pubbliche amministrazioni richiedono per l'attuazione delle politiche di e-government...
- ...al fine di disporre di un'offerta standard...
- ...usufruendo di regole tecniche per la sicurezza, il monitoraggio e la qualità del servizio.
- Per maggiori dettagli [www.pianoegov.it](http://www.pianoegov.it)

# Sicurezza dei servizi di rete (1)

- Cosa possono fare le PAL e le PAC
- Il piano di e-government richiede l'incremento della sicurezza ICT
- Applicazione di un modello richiesta-risposta
- Descrizione degli aspetti generali della sicurezza (architetture e tipologie di prodotti)

## Sicurezza dei servizi di rete (2)

- Documento disponibile sul sito AIPA
- Documento che stimola all'applicazione dei Piani Programmatici della sicurezza ICT
- Saranno sviluppate delle "Linee Guida" operative
- Seguiranno progetti specifici

# I livelli di servizio ICT

- Altro Documento disponibile sul sito AIPA
- “Manuale dei livelli di servizio nel settore ICT”
- Tramite il manuale si ha un modello di riferimento
- Vengono descritti 12 casi tipo del mondo ICT
- Le problematiche di sicurezza non sono trattate esplicitamente, (salvo la firma digitale) ma non è complicato utilizzare il manuale per sviluppare un modello utile in tal senso

Grazie per l'attenzione

Domande ?

