CNIPA
Centro Nazionale per l'Informatica nella Pubblica Amministrazione

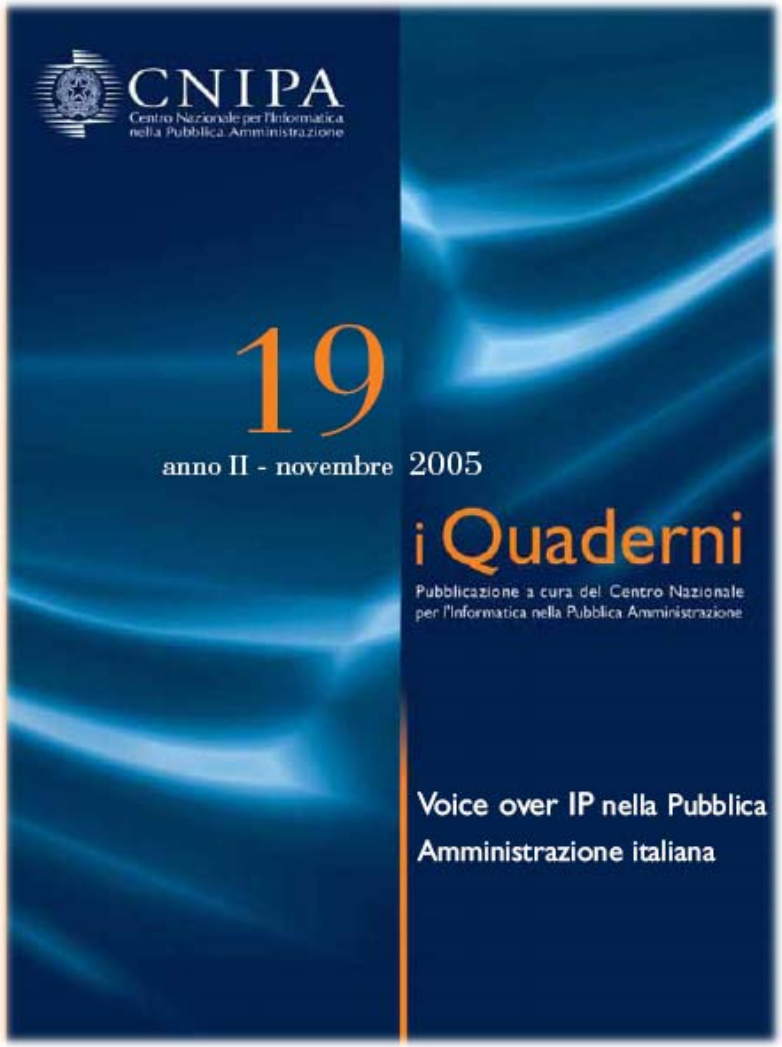
Nuove tecnologie per la PA: quale sicurezza?

Mario Terranova
Responsabile Ufficio Servizi sicurezza, certificazione e integrazione VoIP e immagini
Area Infrastrutture Nazionali Condivise
Centro nazionale per l'informatica nella Pubblica Amministrazione
terranova@cnipa.it

SOMMARIO

- VoIP
- Wireless
- Sicurezza delle applicazioni

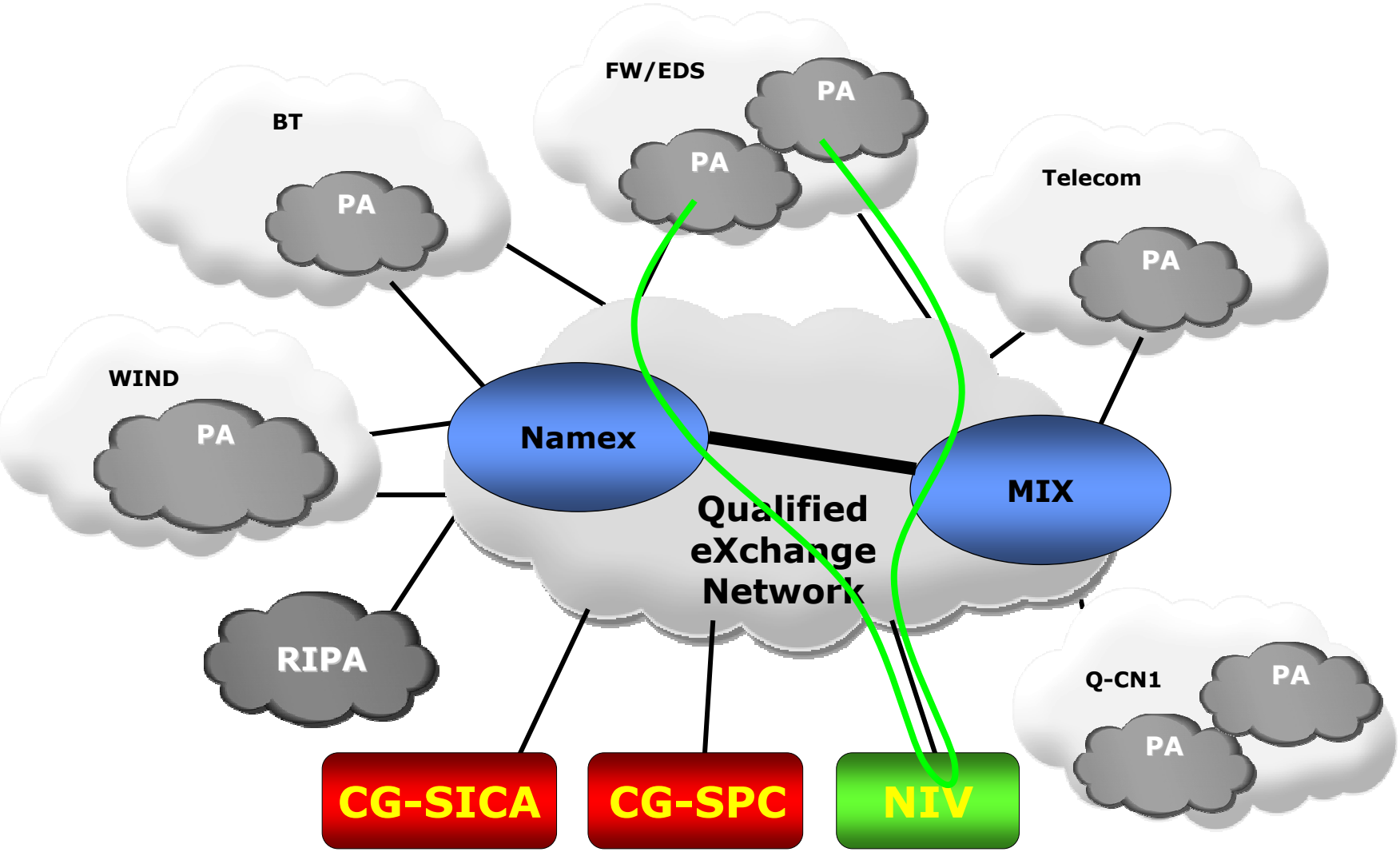
I Quaderno CNIPA



Una rete integrata per servizi convergenti

La convergenza dei servizi consente la piena valorizzazione degli investimenti della PA, abilitandone l'erogazione ubiquitaria verso utenti e cittadini

L’infrastruttura SPC



SOMMARIO

- VoIP
- Wireless
- Sicurezza delle applicazioni

Vantaggi del VoIP

- Collegamento telefonico senza costi aggiuntivi rispetto alla connessione dati.
- Convergenza dell'infrastruttura di rete.
- Outsourcing della gestione (IP Centrex).
- Implementabilità software.
- Integrazione delle applicazioni.
- Servizi avanzati.
- Flessibilità (nomadismo e mobilità).

Riservatezza

- Intercettazione
  - Sniffer
  - Analizzatori di traffico
- Redirezione del traffico
  - ARP cache poisoning
  - Switch misconfiguration
  - Phone misconfiguration

Crittografia

Autenticazione & Autorizzazione

- Default password
- DHCP Server Insertion Attack
- TFTP Insertion Attack
- Impersonificazione

Autenticazione forte

Configurazione protetta

Disponibilità

- Guasto dei componenti
- Vulnerabilità software
- Virus
- Blocco utenti (DoS)

Ridondanza

Telealimentazione

Gestione aggiornamenti

Separazione range indirizzi

QoS

Firewall & NAT

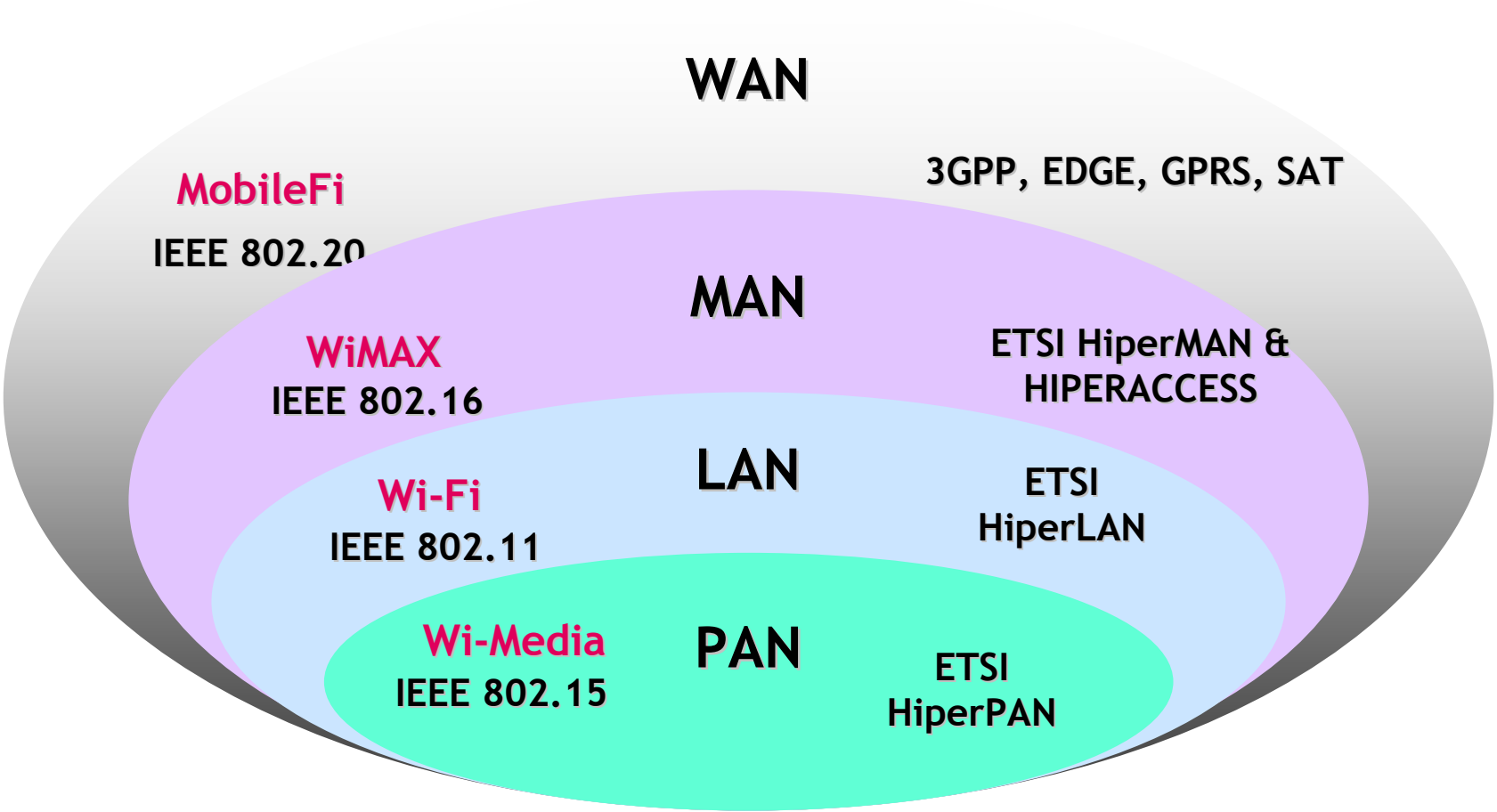
- 400 msec ritardo massimo
- Elevata dinamicità nell'utilizzo delle porte
- Informazioni rilevanti nel protocollo di segnalazione
- Uso della crittografia

Necessità di adeguamento dei firewall e NAT

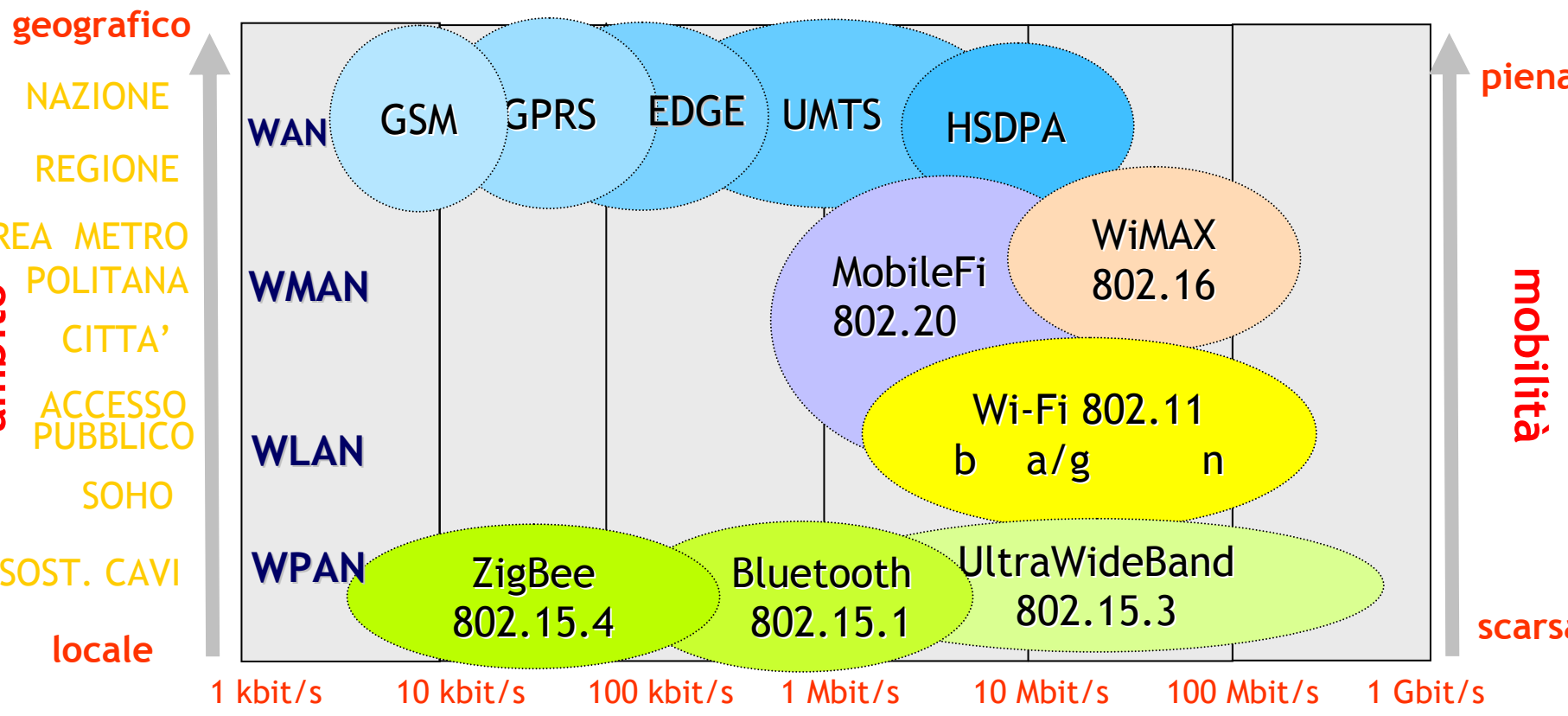
SOMMARIO

- VoIP
- Wireless
- Sicurezza delle applicazioni

Le reti dati wireless



Sintesi delle caratteristiche



Problematiche di sicurezza

- Controllo accesso
  - Consentire l'uso delle risorse solo agli autorizzati
- Riservatezza
  - Impedire a terzi l'acquisizione delle informazioni scambiate.
- Disponibilità
  - Garantire l'accesso alle risorse agli autorizzati nei periodi previsti

Evoluzione sicurezza Wi-Fi

- WEP (Wired Equivalent Privacy)
  - Solo crittografia debole (RC4-56)
  - Autenticazione basata su chiave condivisa
- WPA (Wi-Fi Protected Access)
  - Subset di 802.11i HW compatibile con WEP
  - Autenticazione forte (802.1x/EAP) con PSK
  - RC4-128 con TKIP
- 802.11i (WPA2) [2004]
  - Sostituzione RC4 con AES
  - Key caching e pre-authentication (roaming)
- 802.11w
  - WG istituito nel 2005 per ulteriori estensioni

Problemi di disponibilità

- Condivisione della banda
  - Disponibilità canali limitata
- Interferenza
  - Banda 2,4 GHz non licenziata ed affollata
  - Interferenza tra AP
- Progetto accurato
  - Rapido degrado NLOS
  - Assegnazione dei canali
- Strumenti di simulazione

Connessioni satellitari

- Vasta area coperta
- Facilità di intercetta-zione

- Autenticazione delle stazioni
- Prevalenza uplink
- Crittografia di canale

SOMMARIO

- VoIP
- Wireless
- Sicurezza delle applicazioni

La sicurezza applicativa

- Accesso in scrittura
- Vulnerabilità del sw
- Problemi di progetta-zione
- Problemi di configura-zione

- Autenticazione
- Diagnostica
- Vulnerability scan

Per maggiori informazioni

www.cnipa.gov.it