



Le linee guida tecnologiche per i progetti di e-government delle Regioni e degli Enti Locali

Potenza 13 marzo 2002

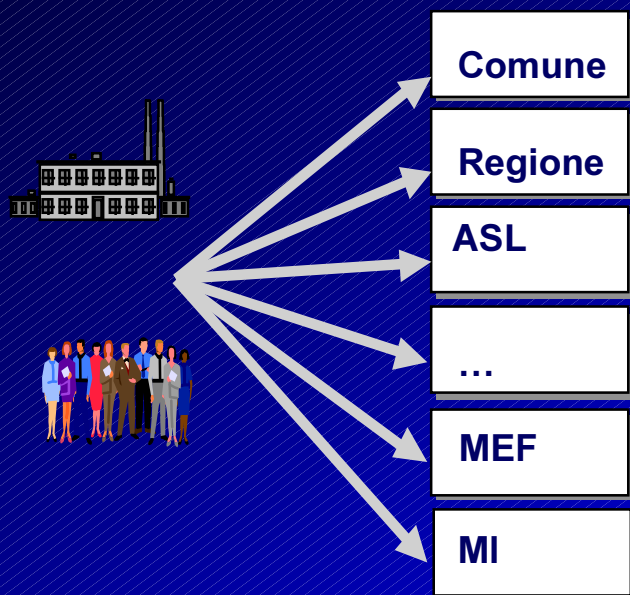
*Intervento di Elena Tabet
Dipartimento per l'innovazione e le tecnologie*



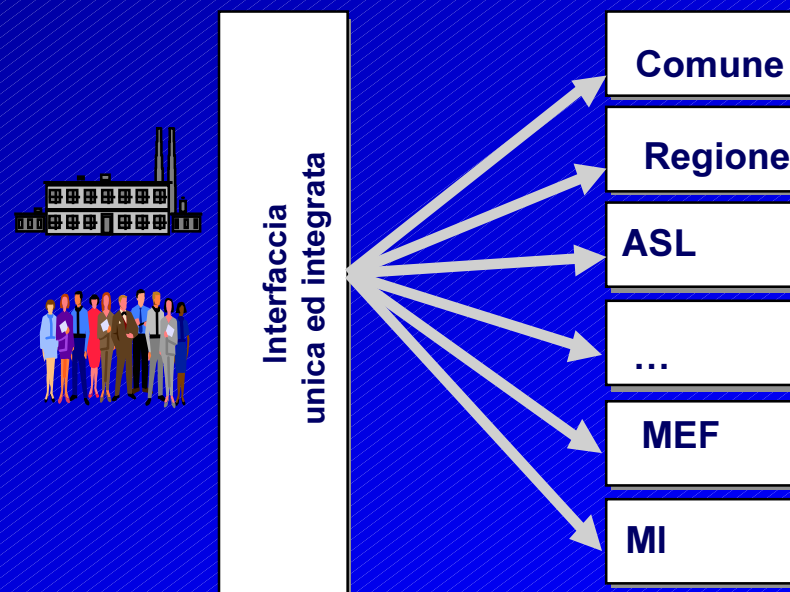


Perché delle linee guida e dei documenti di riferimento?

Lo stato attuale dell'interazione fra cittadini/imprese e la P.A.

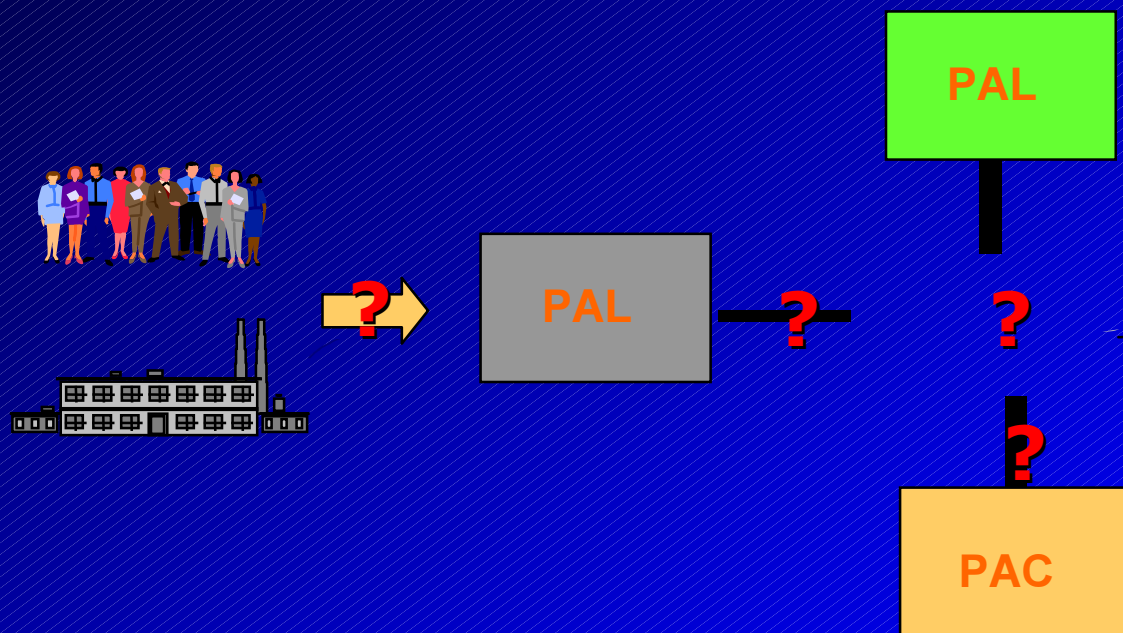


Con l'attuazione del programma di e-government:





E' necessario ri-pensare il modello di interazione fra i cittadini/imprese e la PA e fra le diverse PPAA





Perché delle linee guida e dei documenti di riferimento?

- All'avviso per la selezione di progetti per l'e-government sono allegati dei documenti tecnici di riferimento
- Scopo:
 - indirizzare i progetti verso determinati standard tecnici ed organizzativi
 - realizzare l'infrastruttura dell'e-government in maniera coerente, consistente ed integrata
- Ovvero: far convergere la trasformazione della PA verso un modello comune

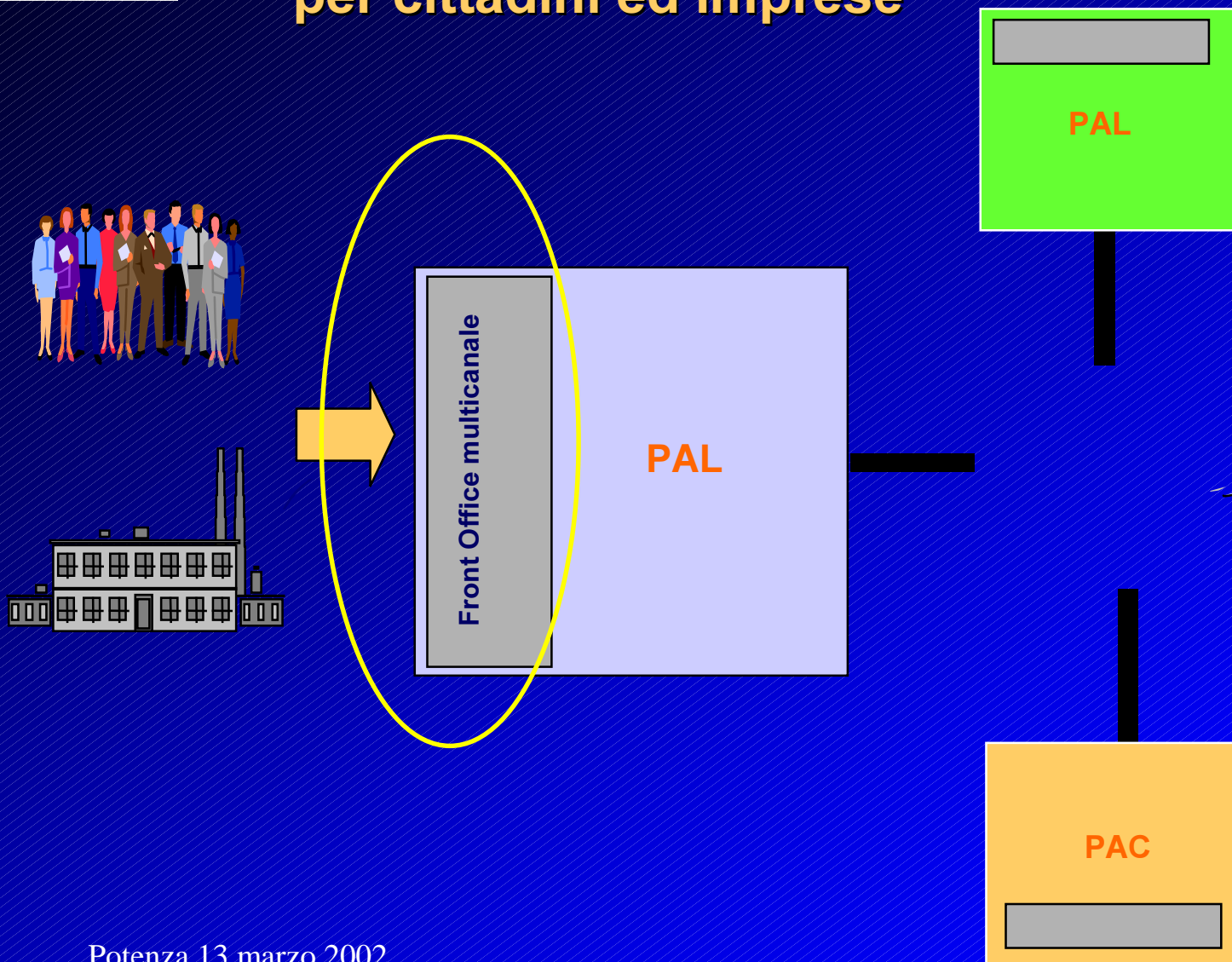


Allegati tecnici all'avviso

- Front office e servizi di e-government per cittadini ed imprese
- Rete Nazionale: caratteristiche e principi di cooperazione applicativa
- Interoperabilità dei sistemi di protocollo e la posta certificata
- Accesso ai servizi con la CIE e la CNS
- Tutela della privacy



Allegato 1 - Front office e servizi di e-government per cittadini ed imprese

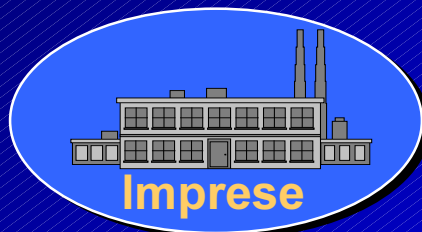




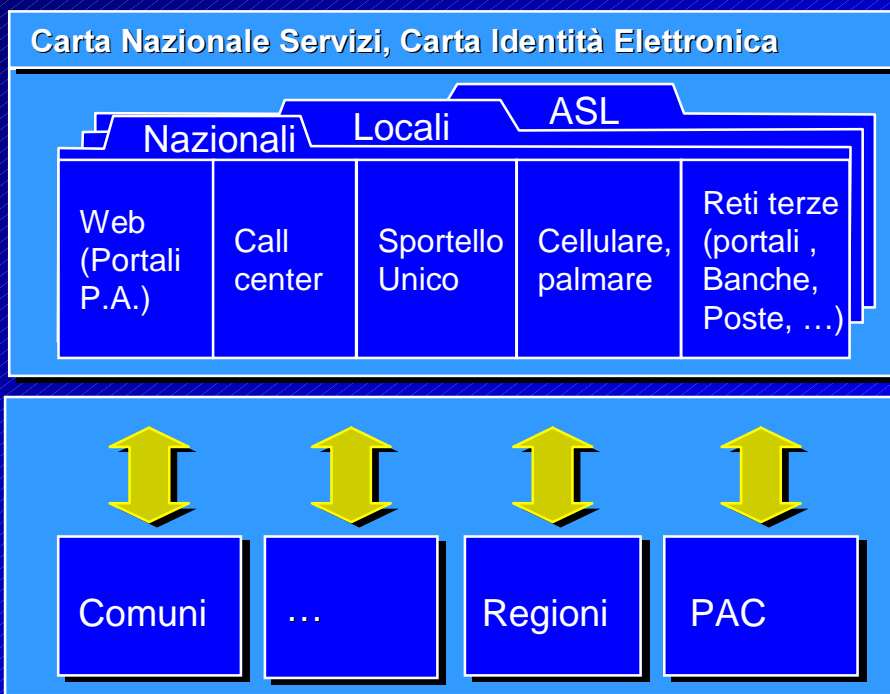
Front-end unico di accesso ai servizi della Pubblica Amministrazione – Allegato 1



Cittadini



Imprese

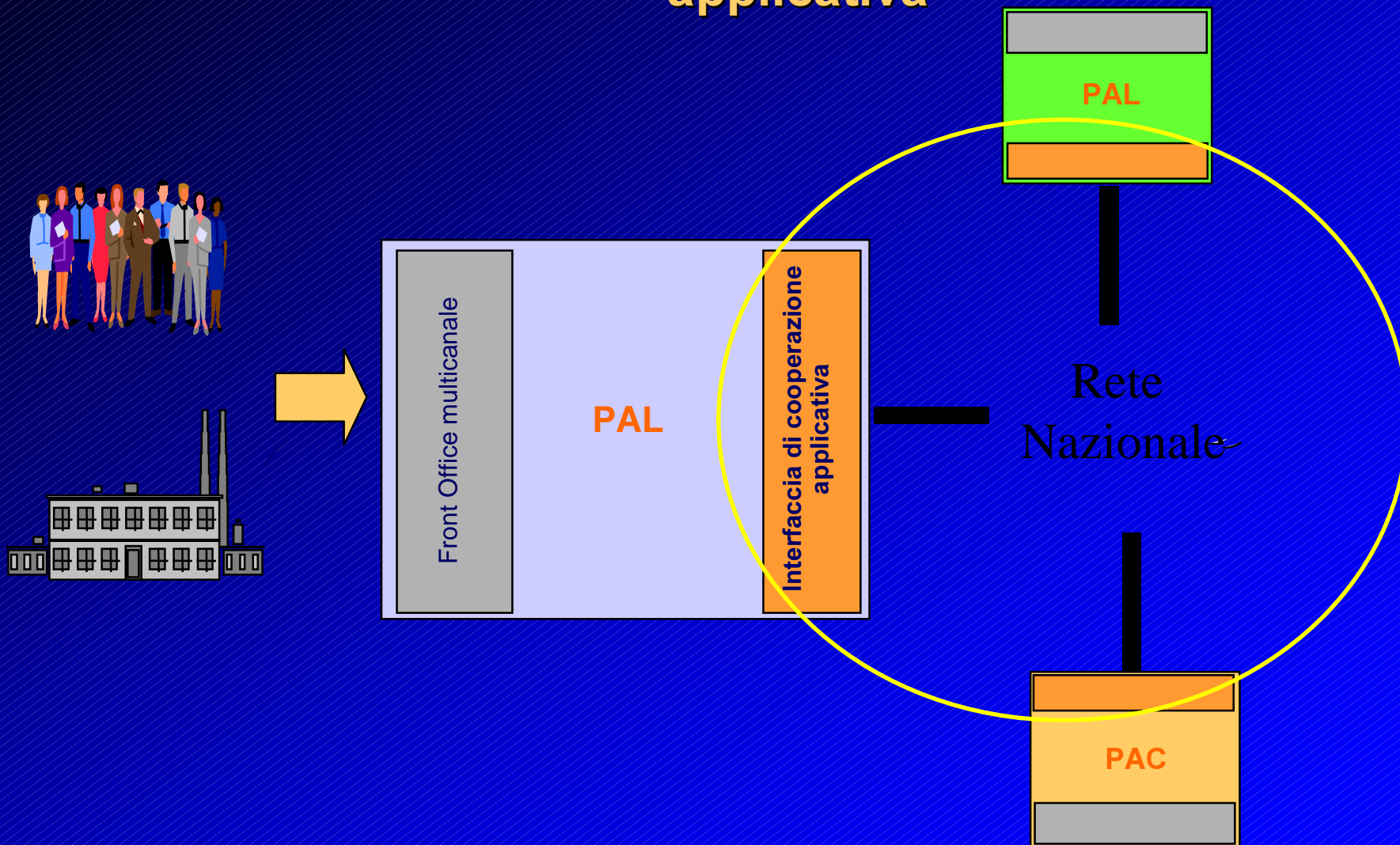


Azioni di indirizzo del Dipartimento

- Metafora di comunicazione
- Multicanalità dell'accesso
- Livelli di autenticazione utente
- Servizi prioritari
- Livello di servizi erogati



Allegato 2 - Rete Nazionale e cooperazione applicativa





La Rete Nazionale

- Basata su di un modello che consente l'interconnessione di tutte le PPAA, centrali e locali tramite:
 - RUPA, RUPAR, reti regionali
 - Reti territoriali, community network
 - Fornitori privati dei servizi di accesso: Service Provider
- Garantisce livelli di servizio e di sicurezza standard, controllando il servizio fornito dai SP tramite i Neutral Access Point o, in futuro, tramite gli EPO



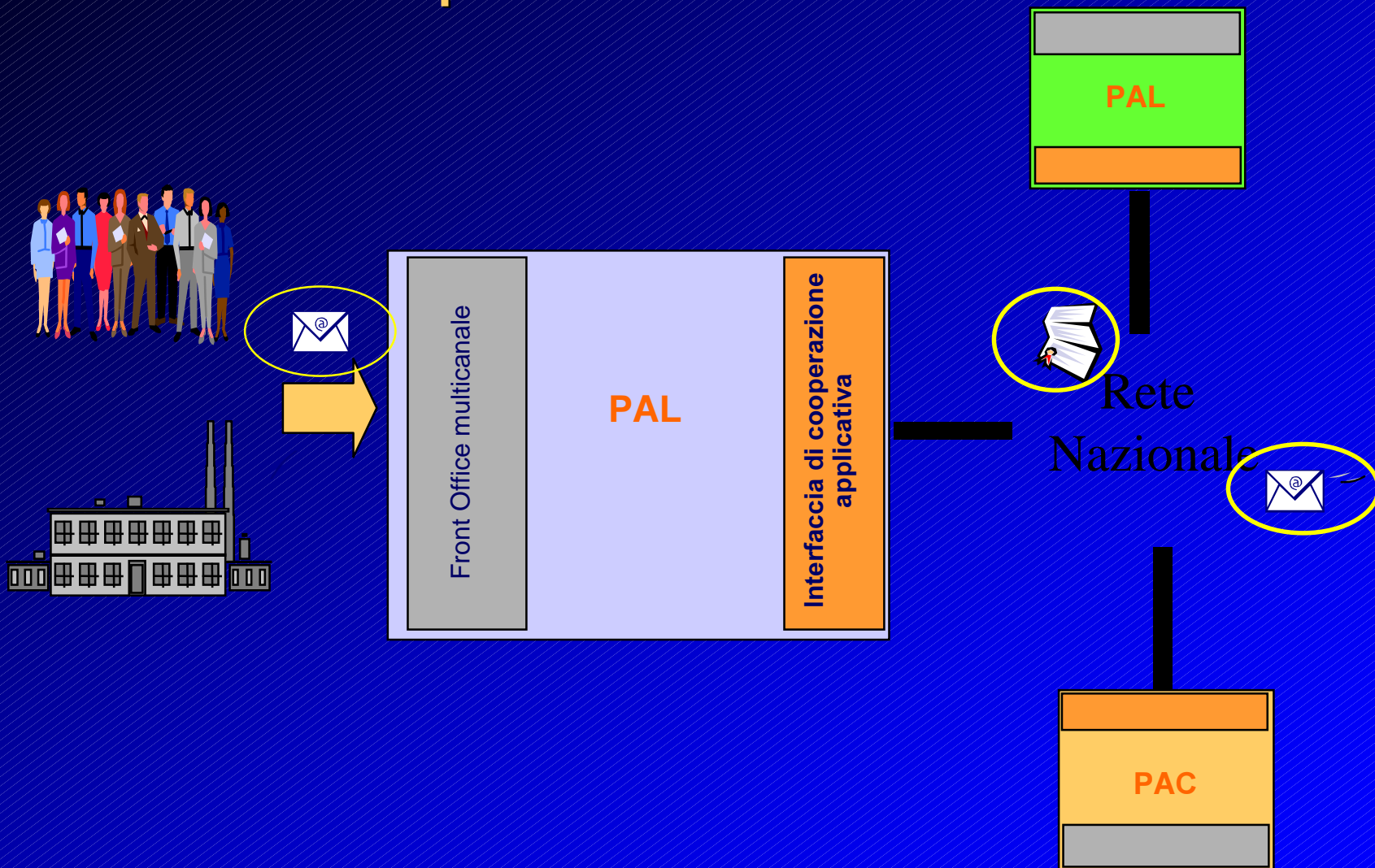
Erogare servizi in rete: la cooperazione applicativa

- Ogni Amministrazione ha un unico punto di accesso logico alla Rete Nazionale: PORTA DI DOMINIO
- All'**interno** del proprio dominio, l'Amministrazione è autonoma nella realizzazione/gestione dei S.I.
- Lo scambio di dati e servizi verso l'**esterno** avviene sempre tramite la porta di dominio e deve rispettare **formati standard**: interoperabilità dei domini





Allegato 3 – Interoperabilità dei protocolli e posta elettronica certificata





Interoperabilità dei sistemi di protocollo e posta elettronica certificata

- **Sistemi di protocollo informatico interoperabili**
 - consentono lo scambio di **documenti in formato elettronico** fra le diverse PPAA
 - consentono di effettuare un trattamento automatico delle informazioni scambiate
 - consentono di attivare, in modo automatico, procedimenti amministrativi all'arrivo del documento
- **Sistema di posta certificata**
 - Consente di spedire/inviare documenti elettronici con le stesse garanzie della posta tradizionale



Regole per l'interoperabilità dei protocolli

- I documenti elettronici, i dati, le informazioni strutturate sono spediti tramite *posta elettronica SMTP/MIME/S-MIME*
- Ogni AOO si deve dotare di una casella di posta elettronica ufficiale *dit.user@palazzochigi.it*
- Viene istituito un indice delle caselle di posta *ufficiali* delle AOO, accessibile via LDAP
- I dati di protocollo (la *segnatura*) sono apposti dall'amministrazione mittente in formato XML (*segnatura.xml*), secondo DTD stabilite da AIPA/CT
- L'amministrazione destinataria usa il file *segnatura.xml* per protocollare il documento in ingresso

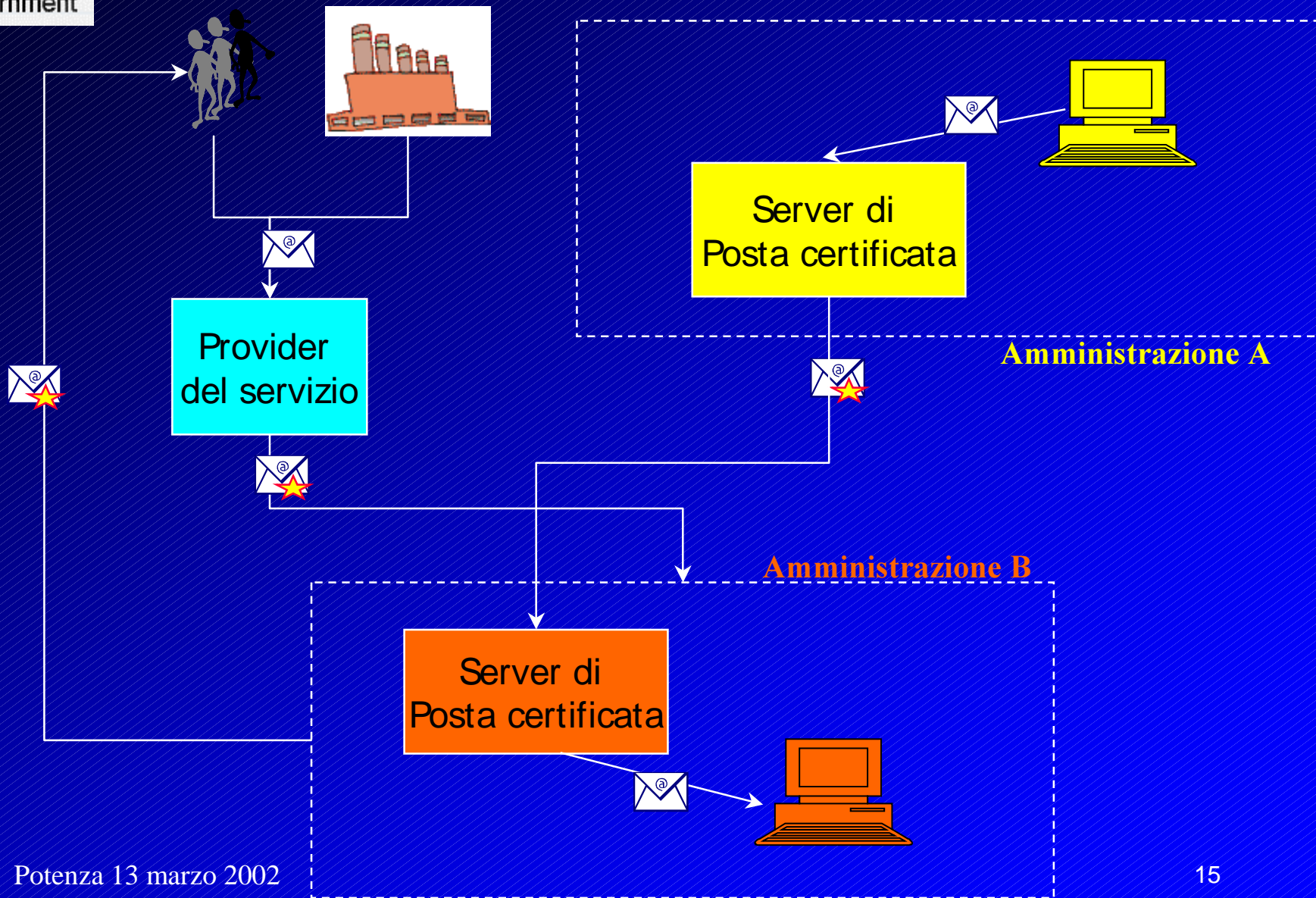


La posta elettronica certificata

- La posta elettronica è giuridicamente equivalente alla posta ordinaria se garantisce:
 - Certezza del mittente/destinatario
 - Autenticazione degli utenti
 - Certezza dell'invio e della consegna
 - Certezza della data e dell'ora di invio
 - Tracciamento degli scambi
 - Certezza della comunicazione

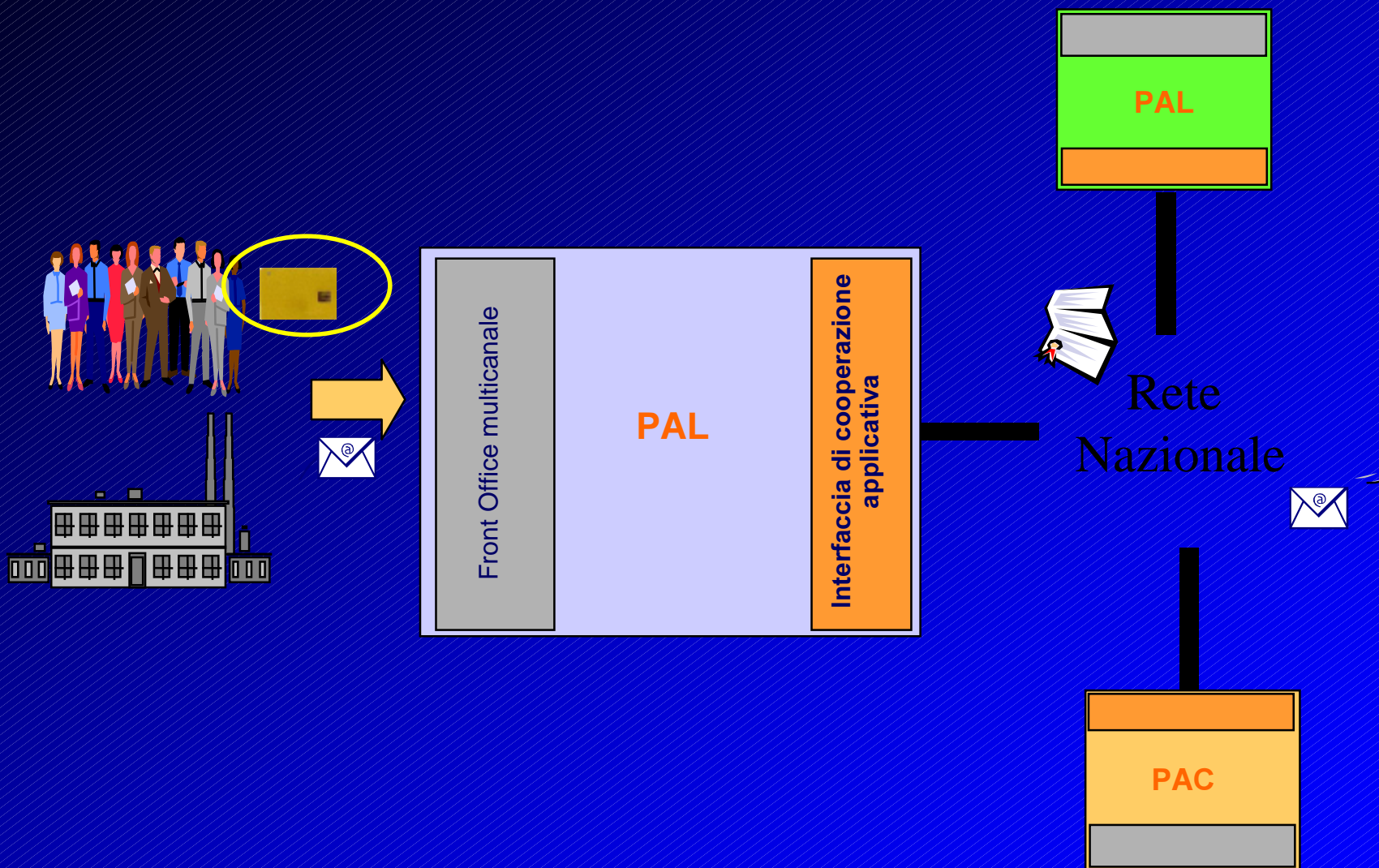


La posta elettronica certificata: uno scenario





Allegato 4 – Accesso ai servizi con la CIE e la CNS





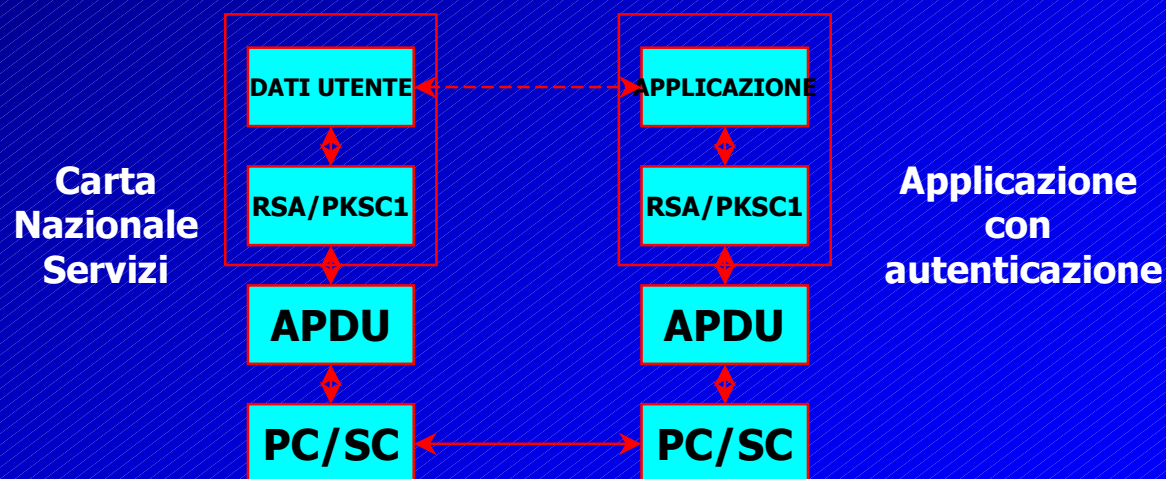
Accesso ai servizi con la CIE/CNS – Allegato 4

- Un'Amministrazione vuole erogare servizi che richiedono l'identificazione dell'utente tramite una carta elettronica
- Un cittadino, in possesso della *carta locale*, rilasciata dall'Amministrazione, accede al servizio e si identifica tramite essa
- Un cittadino in possesso della CNS può accedere anche lui al servizio, e si identifica tramite la CNS
- Il sistema software che realizza il servizio deve garantire la compatibilità con le specifiche stabilite per la CIE/CNS



Accesso ai servizi con la CIE/CNS – Allegato 4

- Le specifiche di riferimento per la CNS sono state emesse dal Ministero dell'Interno (www.cartaidentita.it) e riguardano:
 - Cryptomiddleware di cifratura – basato su RSA e PKCS#1, utilizzabile in ambiente client-server o tramite browser
 - Primitive di colloquio fra la carta ed il sistema - APDU
 - Software di interfaccia fra lettore di smart card e PC – driver aderente allo standard PC/SC





Allegato 5 – Tutela della privacy

