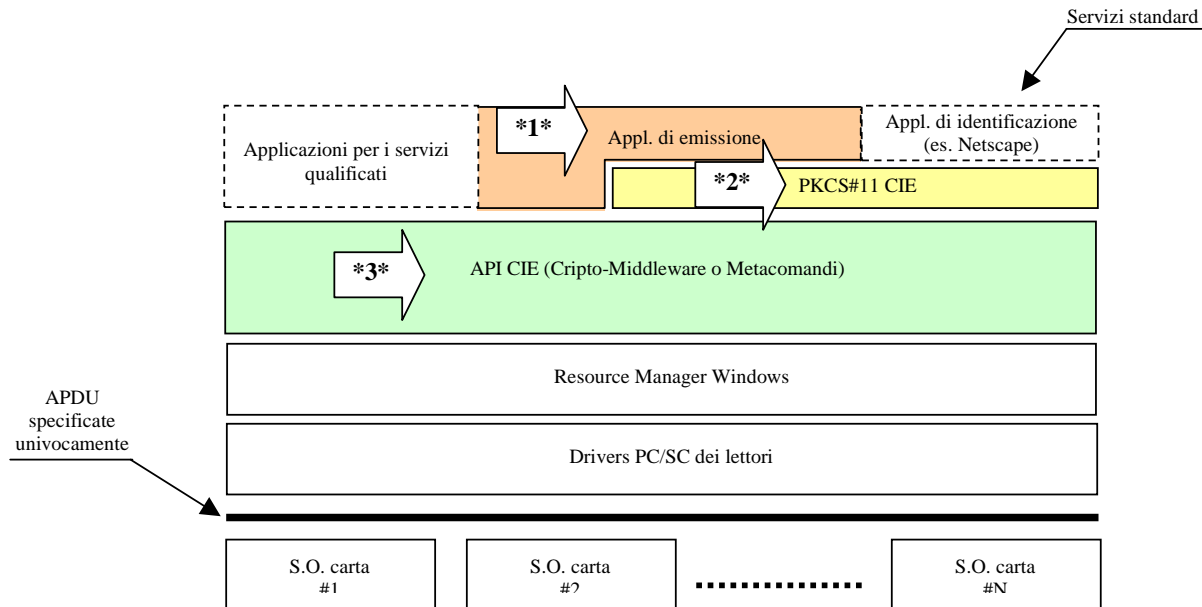


Interoperabilità tra carte e disaccoppiamento rispetto ai S.O.

Questo documento intende illustrare due delle diverse modalità attraverso le quali è possibile ottenere l'interoperabilità dei chip delle smart card utilizzate per la realizzazione della carta di identità elettronica.

Soluzione 1: definizione puntuale dei comandi APDU



In questo schema è necessario sviluppare tre oggetti:

1. il software applicativo per l'emissione della carta,
2. lo strato intermedio PKCS#11 CIE, costituito dal sottoinsieme dei comandi PKCS#11 direttamente utilizzabili dai tools PKI enabled.
3. le API CIE (ossia l'insieme dei metacomandi utilizzabili dal livello applicativo e che mascherano i comandi APDU),

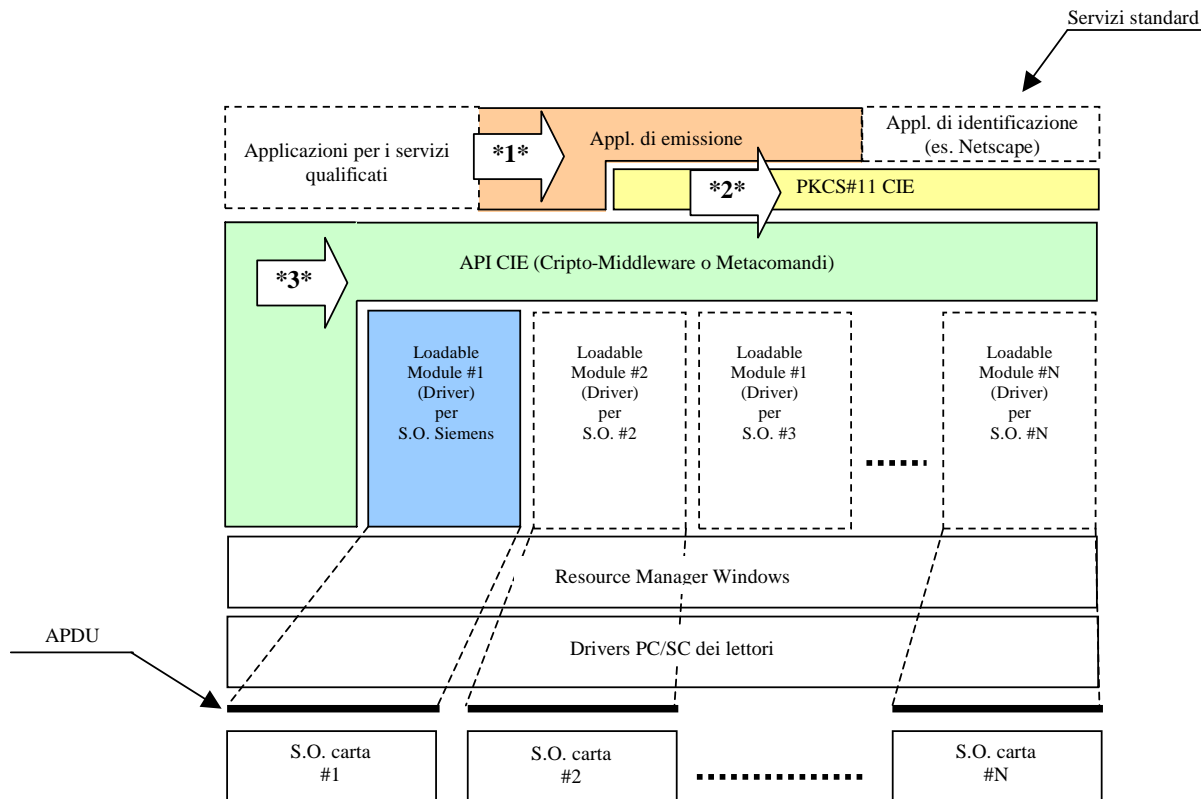
Lo strato intermedio PKCS#11 CIE può essere utilizzato anche direttamente da applicazioni commerciali come gli attuali browser per procedere all'identificazione remota del titolare attraverso i meccanismi standard previsti (SSL V3 – autenticazione client). Le applicazioni di identificazione possono comunque ricorrere anche direttamente ai metacomandi CIE quando non fanno uso dello strato PKCS#11 CIE.

Le API CIE (cioè i metacomandi) sono rese pubbliche e vengono utilizzate, ad es., dalle generiche applicazioni create dagli enti responsabili dei servizi.

Il Resource Manager di Windows consente di prescindere rispetto alle specificità dei lettori di chip, che devono essere però equipaggiati di driver PC/SC e comunque "certificati" per la stazione di emissione. Lo stesso meccanismo vale sulle stazioni client dalle quali ci si voglia identificare (ad es. per mezzo di Netscape).

Il livello di disaccoppiamento con gli altri sistemi operativi è realizzato a livello di APDU (linea nera in figura). Questo significa che il produttore di un altro sistema operativo, per poter partecipare al circuito CIE, deve rispettare il set di comandi definito appositamente per la CIE (opportunamente pubblicato), adattando le eventuali APDU non rispondenti al set CIE.

Soluzione 2: scrittura di un middleware per i comandi APDU



Analogamente alla soluzione descritta precedentemente, anche in questo schema è necessario sviluppare tre oggetti:

1. il software applicativo per l'emissione della carta,
2. lo strato intermedio PKCS#11 CIE, costituito dal sottoinsieme dei comandi PKCS#11 direttamente utilizzabili dai tools PKI enabled.
3. le API CIE (ossia l'insieme dei metacomandi utilizzabili dal livello applicativo e che mascherano i comandi APDU),

Mentre per quanto riguarda i primi due punti non esiste differenza con la soluzione precedentemente descritta, relativamente al terzo punto, va specificato che le API CIE, interfacciano anche i driver con cui i diversi sistemi operativi implementano i comandi APDU.

I driver vengono forniti a livello di loadable module e vengono distribuiti dal fornitore al Ministero dell'Interno che li pubblica sul sito per la loro distribuzione alle stazioni client.

Vantaggi e svantaggi delle due impostazioni

Senza voler affermare che una soluzione sia tecnicamente od organizzativamente migliore o peggiore dell'altra, di seguito si elencano alcuni elementi oggettivi che evidenziano vantaggi e svantaggi delle due impostazioni con cui è possibile ottenere l'interoperabilità.

Anzitutto va precisato che entrambe le soluzioni conservano il concetto di disaccoppiamento realizzato attraverso un livello di middleware, in quanto in tutti e due i casi le applicazioni non cambiano al variare del sistema operativo sottostante. La differenza tra le due impostazioni può sintetizzarsi affermando che la prima è una soluzione a middleware costante, mentre la seconda è una soluzione a middleware variabile.

	Soluzione 1: middleware statico	Soluzione2: middleware variabile
PRO	<ol style="list-style-type: none"> 1. Approccio già collaudato in progetti di interoperabilità tra smart card specialmente in nazioni ove esiste la presenza di un rilevante fornitore di chip; 2. esiste la possibilità – se necessario – di far evolvere lo strato di middleware statico alla soluzione middleware variabile; 3. ferme restando le funzionalità richieste ai comandi APDU, non esiste onere di aggiornamento del S/W per le Amministrazioni locali; 4. soluzione più veloce da implementare. 	<ol style="list-style-type: none"> 1. Indipendenza dal fornitore che fornisce i propri driver per l'implementazione dei comandi APDU che possono essere scaricati in modalità consuete agli operatori Internet; 2. apertura a nuove soluzioni di mercato; 3. non fornisce vantaggi temporali a fornitori di chip.
CONTRO	<ol style="list-style-type: none"> 1. Pesante gestione degli aggiornamenti sia di tipo evolutivo che di tipo adeguativo; 2. fornitura di un vantaggio temporale competitivo al fornitore che specifica per la prima volta i comandi APDU; 3. sottrazione di memoria al chip nel caso in cui i comandi APDU venissero implementati in EPROM. 	<ol style="list-style-type: none"> 1. Onere di aggiornamento da parte delle Amministrazioni locali e degli utenti finali nel caso in cui dovesse entrare nel circuito CIE un nuovo fornitore con un nuovo sistema operativo.