Applicazioni reali di RSA ed altri sistemi

Renato Sabbatini

Seminario – Crittografia a chiave pubblica: oltre RSA

Università degli Studi di Torino – Dipartimento di Matematica

13 maggio 2011

INTRODUZIONE

Introduzione

- L'esposizione sarà incentrata sull'impiego dell'algoritmo RSA, con accenni agli ambiti dove sono già al momento presenti usi (o ipotesi d'uso) degli altri algoritmi a chiave asimmetrica
- Tratterò in modo più esteso le applicazioni che coinvolgono il mondo dei pagamenti, che è quello da cui provengo
- L'adozione degli algoritmi a chiave asimmetrica è stata motivata dalla necessità di superare la limitazione della condivisione di una chiave per tratta in caso di relazioni multiple, limitazione associata agli algoritmi a chiave simmetrica
- Quindi permettere la creazione di relazioni estemporanee ma in ogni caso "trusted"
- Il processo di key management, che si poteva immaginare come più semplice, è in realtà egualmente, se non maggiormente, complicato
- Il problema fondamentale è l'associazione certa fra componente pubblica di una chiave e relativo "owner", associazione che, ad es. con RSA, non è assicurata tramite regole dell'algoritmo
- Si è adottata quindi un'infrastruttura identificata con l'acronimo PKI e basata su certificati, che trasferiscono la "fiducia" da una relazione "affidabile" ad una "occasionale"
- La relazione fra componente pubblica e "owner" è certificata (da cui il nome del dato) da un'altra entità di cui ci fidiamo (o da una serie di entità che portano ad una di cui ci fidiamo)
- E' chiaro quindi come tutto l'ecosistema determinato da una PKI sia fortemente legato al concetto di fiducia (attacco a Comodo)

Introduzione

- I certificati comunemente usati sono di due tipi:
  - Quelli basati sul concetto di “signature with recovery”
  - Quelli basati sul concetto di “signature without recovery”
- “Signature with recovery” significa che la firma del certificato contiene parte della chiave pubblica che è oggetto di certificazione. Tali certificati sono tipicamente basati sugli standard:
  - ISO 9796-2 Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms
  - PKCS
- I certificati di tipo “without recovery” sono invece tipicamente basati sugli standard:
  - ITU-T X.509 – RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
  - ISO 8824 Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation
  - ISO 8825 Information technology -- ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
  - PKCS
- L’applicazione dell’algoritmo RSA, che di fatto si concretizza in una sola funzione matematica, a seconda della componente utilizzata (pubblica o segreta) e dell’input (plaintext o meno) assume quattro differenti scopi e relative denominazioni (il mancato uso del termine “cifrato” è voluto, poiché a volte inappropriato):
  - Cifratura (pubblica, plaintext)
  - Decifratura (segreta, non plaintext)
  - Firma (segreta, plaintext)
  - Verifica (pubblica, non plaintext)
- Poiché gli apparati crittografici (HSM) dispongono a volte di API limitate, avviene che si decifri utilizzando una funzionalità di firma, o che si cifri utilizzando quella di verifica (aspetto tipicamente incomprensibile per gli sviluppatori di applicazioni!!)

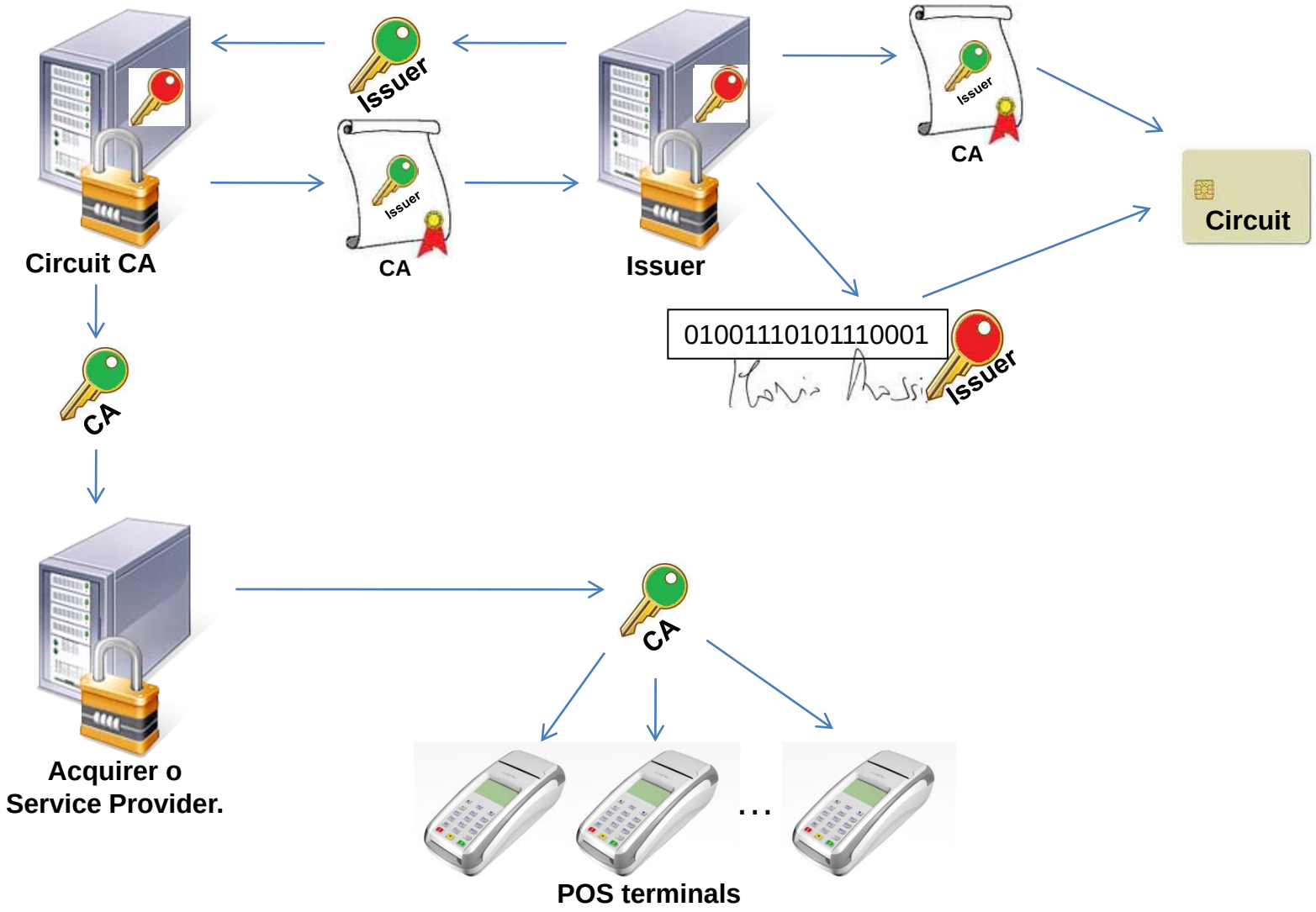
AUTENTICAZIONE

Autenticazione “on-fly” – Smart card

- L’introduzione delle carte dotate di microprocessore nasce dalla necessità di abbandonare la banda magnetica, ritenuta una tecnologia ormai troppo aperta alle frodi
- Al tempo della definizione delle specifiche un altro “driver” importante era la possibilità di operare off-line, sfruttando “l’intelligenza” della carta, poiché i tempi di connessione ai centri autorizzativi erano significativi all’interno del tempo totale di transazione (ora non è più così, e quasi tutti gli apparati operano on-line)
- Il consorzio EMV nasce da Europay, Mastercard e Visa per la definizione di specifiche che assicurassero l’interoperabilità fra carte e terminali, in ogni parte del mondo ed in modo indipendente dai “vendor”
- Il problema fondamentale era far si che fra due apparati che non erano mai stati posti in relazione in precedenza (carta e terminale), si potesse creare una relazione “trusted”
- In realtà, il problema di autenticazione si limita alla necessità, per il terminale, di riconoscere la carta come autentica (e il portatore di carta come il possessore legittimo)
- Venne scelto l’algoritmo RSA, all’interno di una PKI infrastrutturale, con certificati ISO
- Il primo metodo adottato per il riconoscimento della carta, la Static Data Authentication, scelto per mantenere il costo delle carte accettabile e così pure la durata di una transazione di pagamento, si rivelò presto come un ben misero incremento di sicurezza, proprio nel caso di off-line, che era la modalità “desiderata” agli inizi
- Si è quindi definito un nuovo metodo, la Dinamic Data Authentication, che utilizza il principio del “challenge”

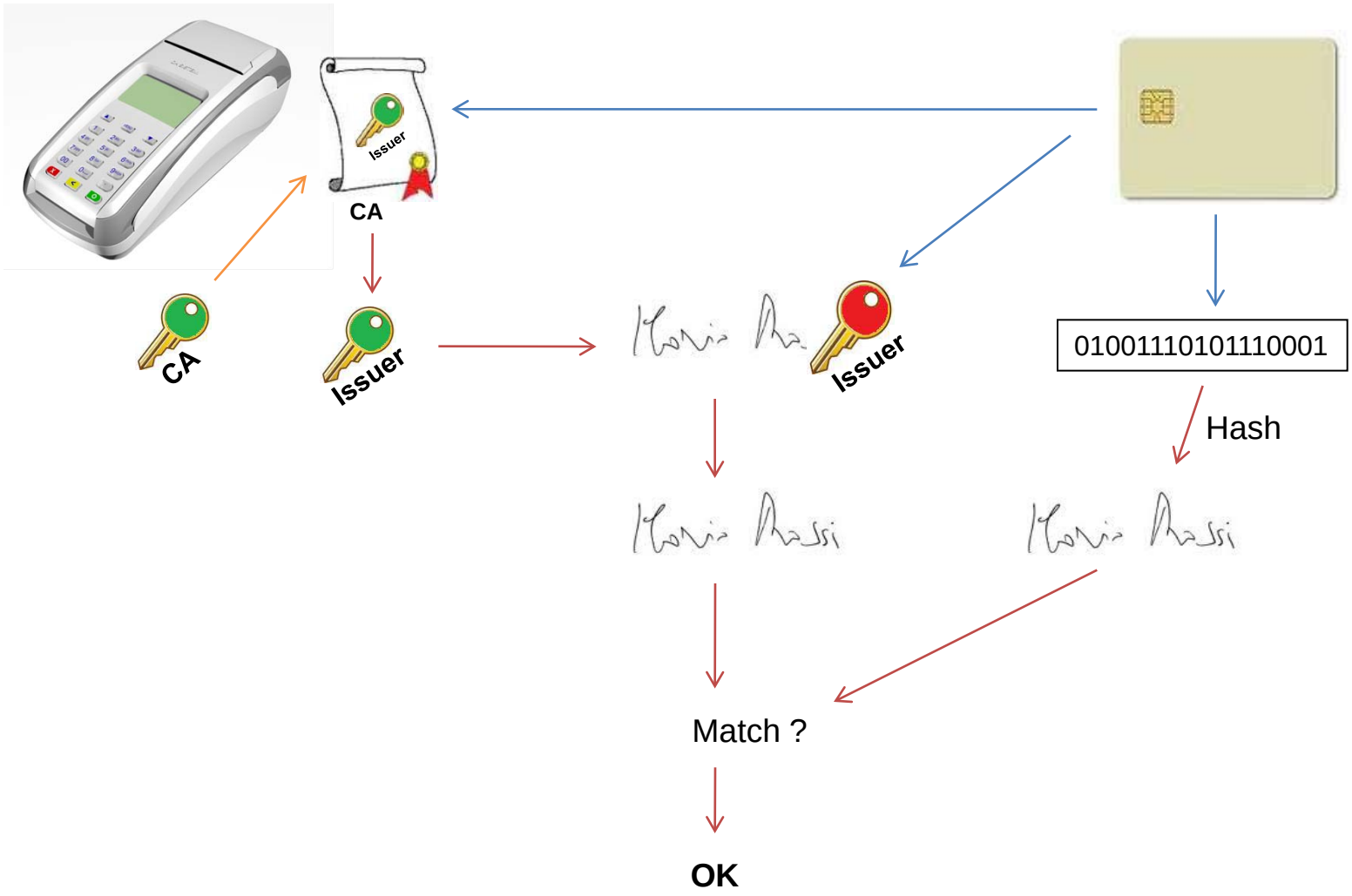
Autenticazione “on-fly” – Smart Card

Static Data Authentication - SDA



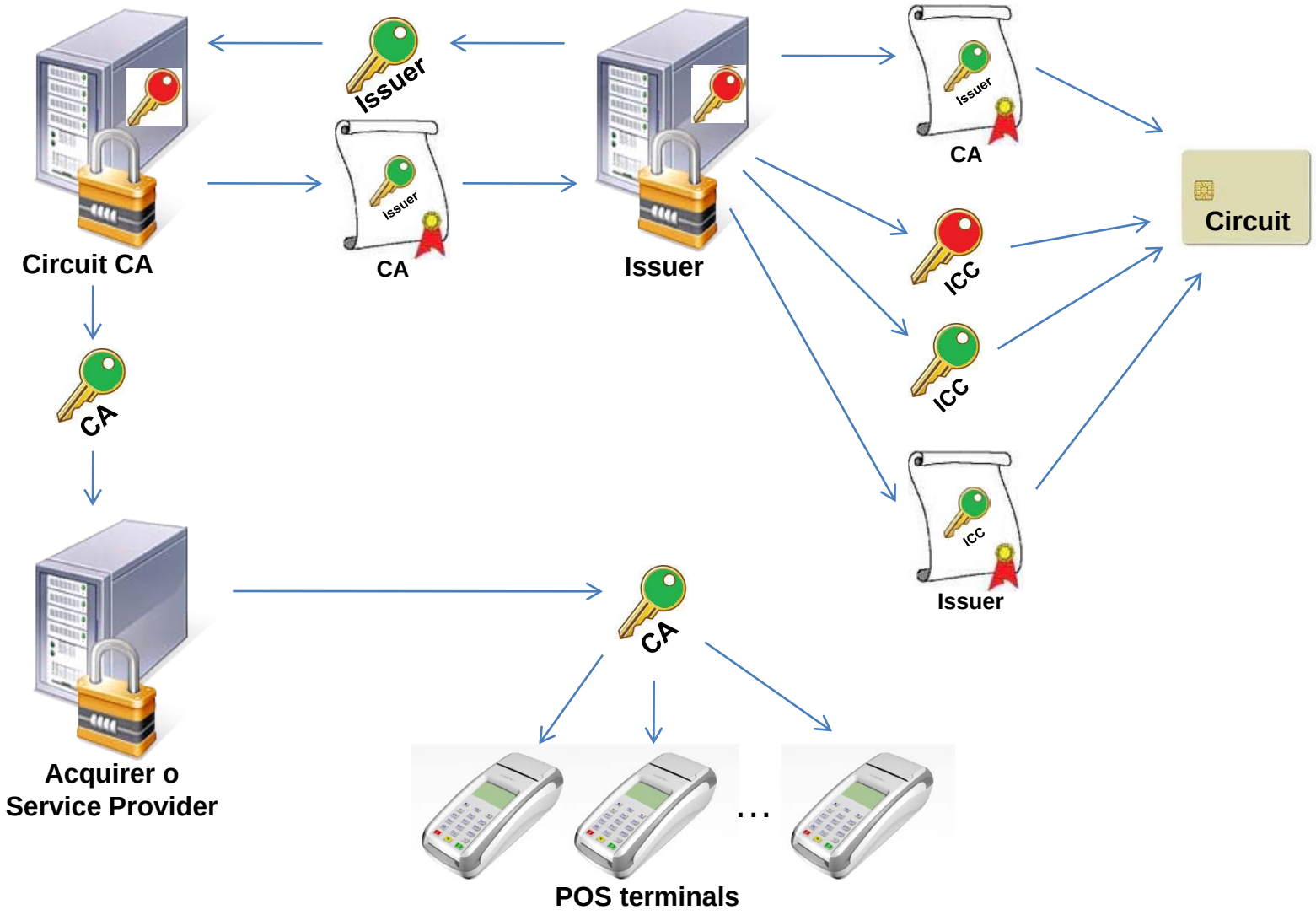
Autenticazione “on-fly” – Smart Card

Static Data Authentication - SDA



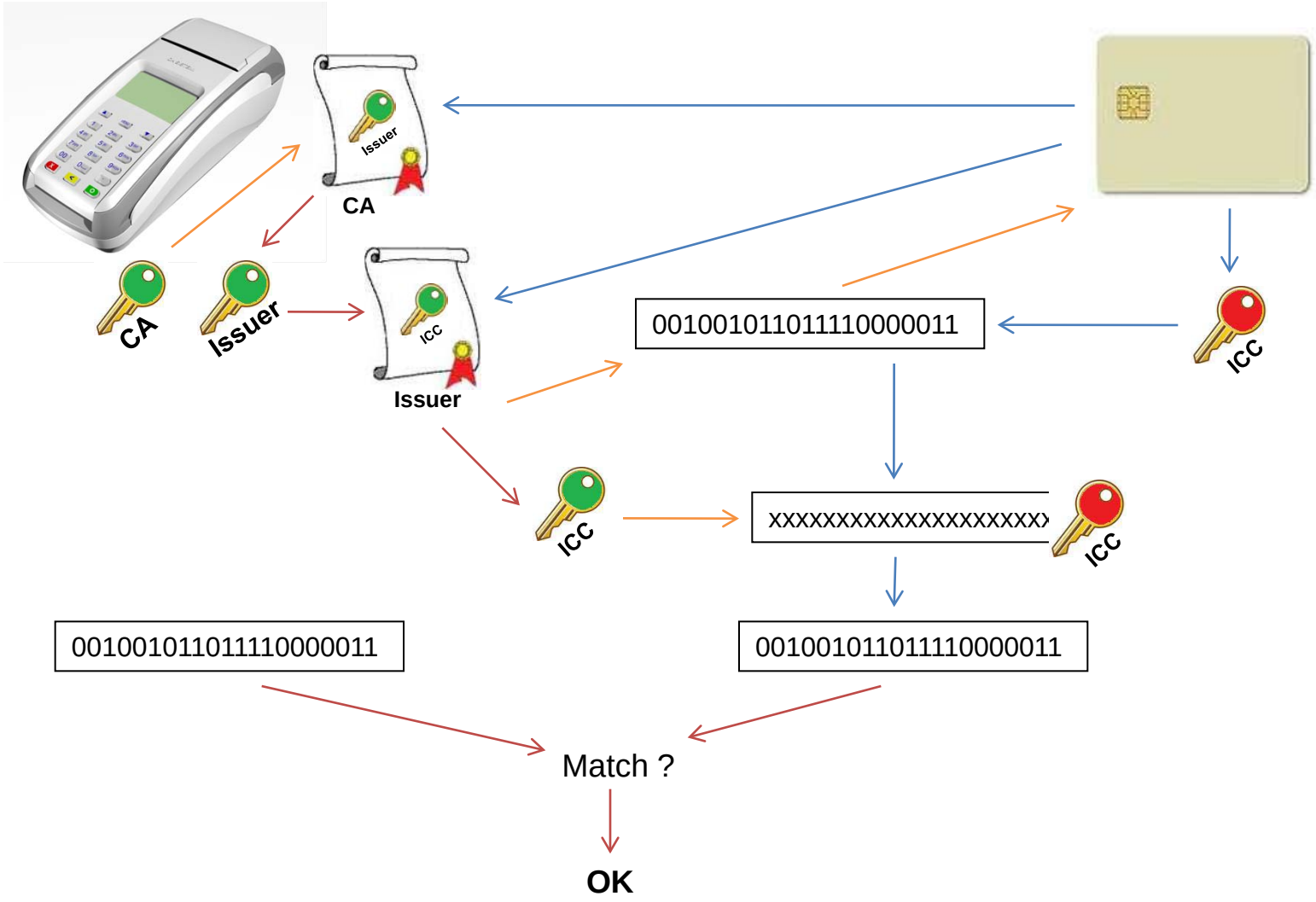
Autenticazione “on-fly” – Smart Card

Dinamic Data Authentication - DDA



Autenticazione “on-fly” – Smart Card

Dinamic Data Authentication - DDA



Autenticazione “on-fly” – Smart card

- Autenticazione monodirezionale
- Non vengono trasferite chiavi, quindi non viene costituito un canale protetto
- L’autenticazione deve rispondere anche alla necessità di integrità
- Quindi
  - In caso di SDA la stringa firmata è ottenuta tramite il concatenamento dei dati che debbono essere integri
  - In caso di DDA, la stringa dei dati di cui si vuole assicurare l’integrità è inserita nel calcolo della firma del certificato della PK ICC
- Attualmente un vincolo tecnico, legato al colloquio fra carta e terminale, limita la dimensione delle chiavi RSA a 1984 bit di modulo
- Inoltre, l’incremento del tempo di elaborazione dovuto all’aumento della dimensioni delle chiavi RSA non è compatibile con la durata di un’operazione di pagamento
- All’interno di EMVCo è quindi in corso la discussione sulle possibili alternative tecniche per risolvere tali problemi
- La questione è particolarmente complessa, poiché ha impatto su tutta la base installata di apparati, base che a tutt’oggi non è nemmeno completamente migrata alla gestione del chip
- Oltre all’estensione della dimensione delle chiavi RSA tramite segmentazione, una delle ipotesi è il cambio di algoritmo a favore delle curve ellittiche
- Il problema di una scelta del genere è che, mentre è possibile che i processori presenti negli apparati siano in grado di trattare chiavi RSA di dimensione maggiore, sicuramente non tutti dispongono delle funzionalità per la gestione delle curve ellittiche

Autenticazione “on-fly” – SSL

- In questo caso il problema da risolvere era il trasferimento in modo protetto (integrità/riservatezza) di informazioni su reti aperte, a fronte di connessioni fra entità che non avessero avuto contatti in precedenza
- SSL (Secure Socket Layer) e la sua versione più aggiornata, TLS (Transport Layer Security) sono protocolli utilizzati per la creazione di un canale protetto su reti TCP/IP
- TLS è un protocollo standard IETF che, nella sua ultima versione, è definito dalla norma RFC 5246
- Diverse versioni del protocollo sono utilizzate in applicazioni come i browser, l‘e-mail, la messaggistica istantanea e il voice-over-IP
- La creazione di un canale protetto è solo una parte del problema, poiché l’invio di informazioni all’interno di tale canale verso un destinatario sconosciuto è ugualmente pericoloso, ed è quindi necessaria un’autenticazione delle parti
- Anche se il protocollo permette una mutua autenticazione, generalmente, nelle relazioni browser client -> server, l’unico ad autenticarsi è il server
- Il server fornisce un certificato di tipo X.509
- All’interno del browser del client è “annegata” una lista di CA “affidabili” con associate le componenti pubbliche delle loro chiavi
- Questa lista è un elemento debole del sistema, in caso di una compromissione del client tramite installazione di un malware
- Le due controparti, nel momento in cui viene instaurata la connessione, si accordano su una cipher suite, che costituisce l’insieme degli algoritmi di autenticazione, di scambio chiavi, di cifratura e di calcolo MAC

Autenticazione “on-fly” – SSL

Cipher Suite	Key Exchange	Cipher	Mac
TLS_NULL_WITH_NULL_NULL	NULL	NULL	NULL
TLS_RSA_WITH_NULL_MD5	RSA	NULL	MD5
TLS_RSA_WITH_NULL_SHA	RSA	NULL	SHA
TLS_RSA_WITH_NULL_SHA256	RSA	NULL	SHA256
TLS_RSA_WITH_RC4_128_MD5	RSA	RC4_128	MD5
TLS_RSA_WITH_RC4_128_SHA	RSA	RC4_128	SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA	3DES_EDE_CBC	SHA
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	AES_128_CBC	SHA
TLS_RSA_WITH_AES_256_CBC_SHA	RSA	AES_256_CBC	SHA
TLS_RSA_WITH_AES_128_CBC_SHA256	RSA	AES_128_CBC	SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256	RSA	AES_256_CBC	SHA256
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA	DH_DSS	3DES_EDE_CBC	SHA
TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA	DH_RSA	3DES_EDE_CBC	SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	DHE_DSS	3DES_EDE_CBC	SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	DHE_RSA	3DES_EDE_CBC	SHA
TLS_DH_DSS_WITH_AES_128_CBC_SHA	DH_DSS	AES_128_CBC	SHA
TLS_DH_RSA_WITH_AES_128_CBC_SHA	DH_RSA	AES_128_CBC	SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	DHE_DSS	AES_128_CBC	SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE_RSA	AES_128_CBC	SHA
TLS_DH_DSS_WITH_AES_256_CBC_SHA	DH_DSS	AES_256_CBC	SHA
……			
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDH_ECDSA	3DES_EDE_CBC	SHA
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	ECDH_ECDSA	AES_128_CBC	SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE_RSA	3DES_EDE_CBC	SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE_RSA	AES_128_CBC	SHA

DEMATERIALIZZAZIONE

Dematerializzazione – Il documento in formato elettronico

- L'obbiettivo era una significativa riduzione dei costi di gestione dei documenti (ad es. nei rapporti con la Pubblica Amministrazione), mediante un trattamento automatizzato non possibile con documenti cartacei, che quindi richiedeva una loro de-materializzazione
- Era però necessario mantenere la validità legale del documento cartaceo regolarmente sottoscritto e trasmesso in modo controllato, trasferendola alla sua "versione" digitale
- La possibilità di mantenere il valore legale dipende direttamente dalla capacità di assicurare l'autenticità del documento in una specifica forma (certezza della sorgente, integrità)
- Questo ha portato allo sviluppo di tutte le varie forme di "Firma digitale", con differenti validità dal punto di vista legale, ed anche alla "Posta elettronica certificata", il sostituto digitale della classica raccomandata
- La cosa si riduce ad una funzione di hash applicata al documento digitale, e alla firma di tale hash, utilizzando algoritmi asimmetrici, sempre per superare il problema dell'assenza di un contatto precedente fra le parti
- Le "credenziali", cioè quanto necessario per apporre la "firma", vengono solitamente trasportate su smart card o token USB (Carta Nazionale dei Servizi), per permetterne l'uso in ambiti diversi
- Un aspetto interessante dell'uso di chiavi asimmetriche, nell'ambito della gestione documentale, è la "no-repudiation", non ottenibile con algoritmi a chiave simmetrica
- Poiché la componente segreta non viene mai divulgata, il firmatario non può negare di essere colui che ha apposto una firma digitale, con tutto ciò che ne consegue nella contrattualistica e, ad es., nella gestione dei referti medici (si può considerare l'equivalente digitale della perizia calligrafica)
- Altro aspetto particolare è che l'elemento tempo è fondamentale per alcuni documenti (pensiamo ai bandi di gara e al valore legale della ricevuta di ritorno di una raccomandata)
- Questo ha generato il servizio di "time-stamp", cioè la generazione di una "marca temporale", autenticata da uno specifico ente, che viene associata in modo indissolubile al documento digitale
- Il documento digitale diventa quindi un insieme di componenti differentemente autenticate, e globalmente sotto la responsabilità del firmatario finale

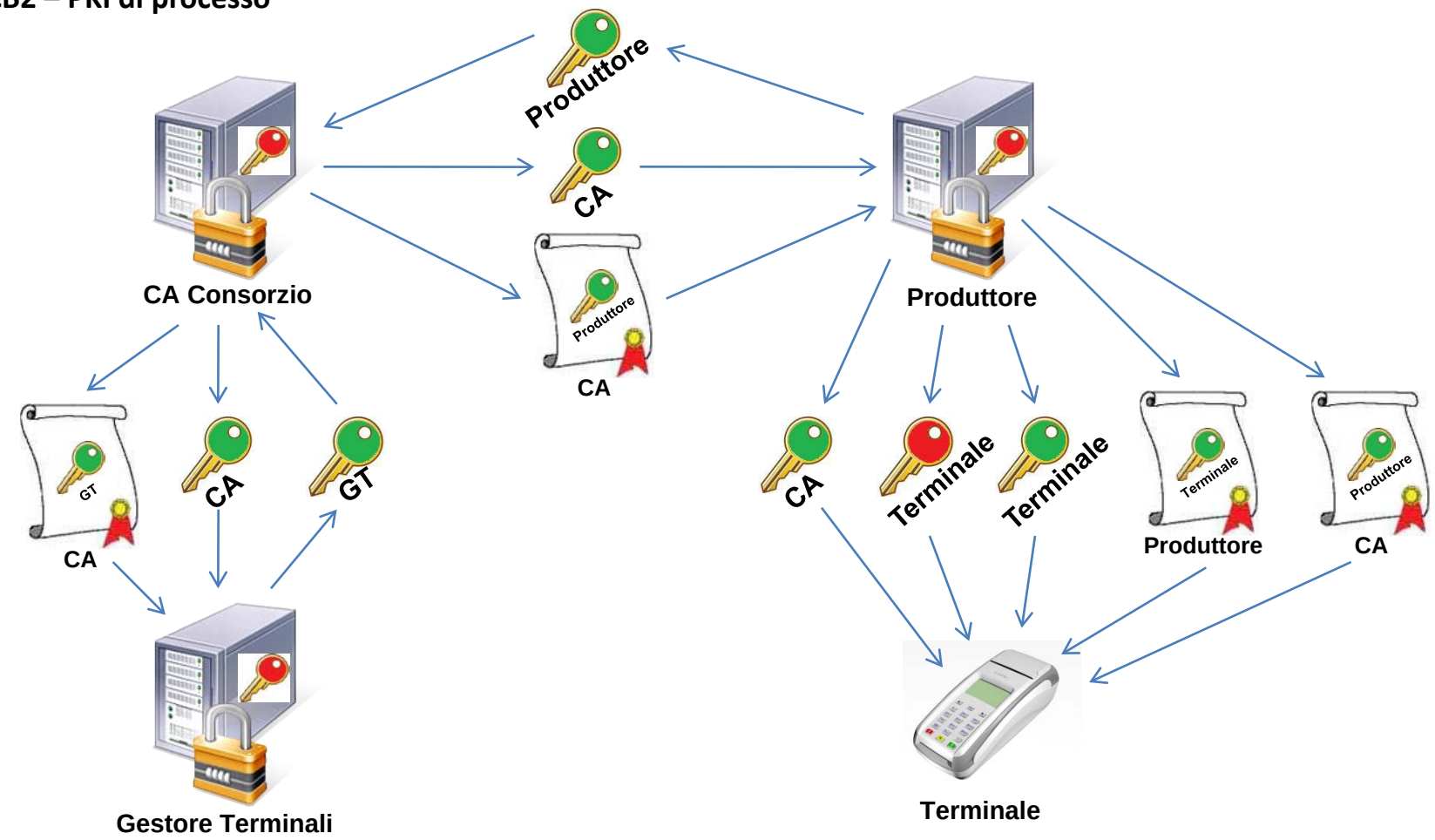
APPARTENENZA

Appartenenza – CB2

- Il Consorzio Bancomat, posseduto dalle banche italiane tramite l'ABI, controlla i brand Bancomat e Pagobancomat. E' quindi l'organo tecnico che determina le regole che si applicano alla carta di debito nazionale.
- Il suo problema era di sviluppare un metodo che permettesse la distribuzione delle chiavi operative ai terminali POS, direttamente sul campo e senza che dovessero transitare in specifici ambienti protetti in carico alle singole banche
- Il metodo doveva inoltre permettere sia che un parco terminali fosse controllato da più Gestori Terminali (i Service Provider del sistema italiano), sia il rimpiazzo di un Gestore con un altro, per mantenere la capacità contrattuale delle banche
- Per chiavi operative intendiamo le chiavi simmetriche di protezione dei dati del possessore della carta, dei dati della transazione di pagamento e del PIN (se verificato on-line)
- Analoga protezione doveva essere assicurata anche a tutti i parametri "sensibili" necessari al funzionamento del terminale (ad es. numero telefonico o indirizzo IP della controparte)
- Il protocollo specificato, comunemente conosciuto come CB2, ha definito una PKI con l'uso di certificati ISO
- La struttura della PKI ricalca in gran parte quanto già visto per le smart card, tranne che in questo caso si tratta di una mutua autenticazione
- Questo perché devono essere certe sia la sorgente che la destinazione del trasferimento di informazioni
- Inoltre, in questo caso, deve essere assicurata anche la riservatezza delle informazioni, cosa che per le smart card non è richiesta (tranne per il PIN)

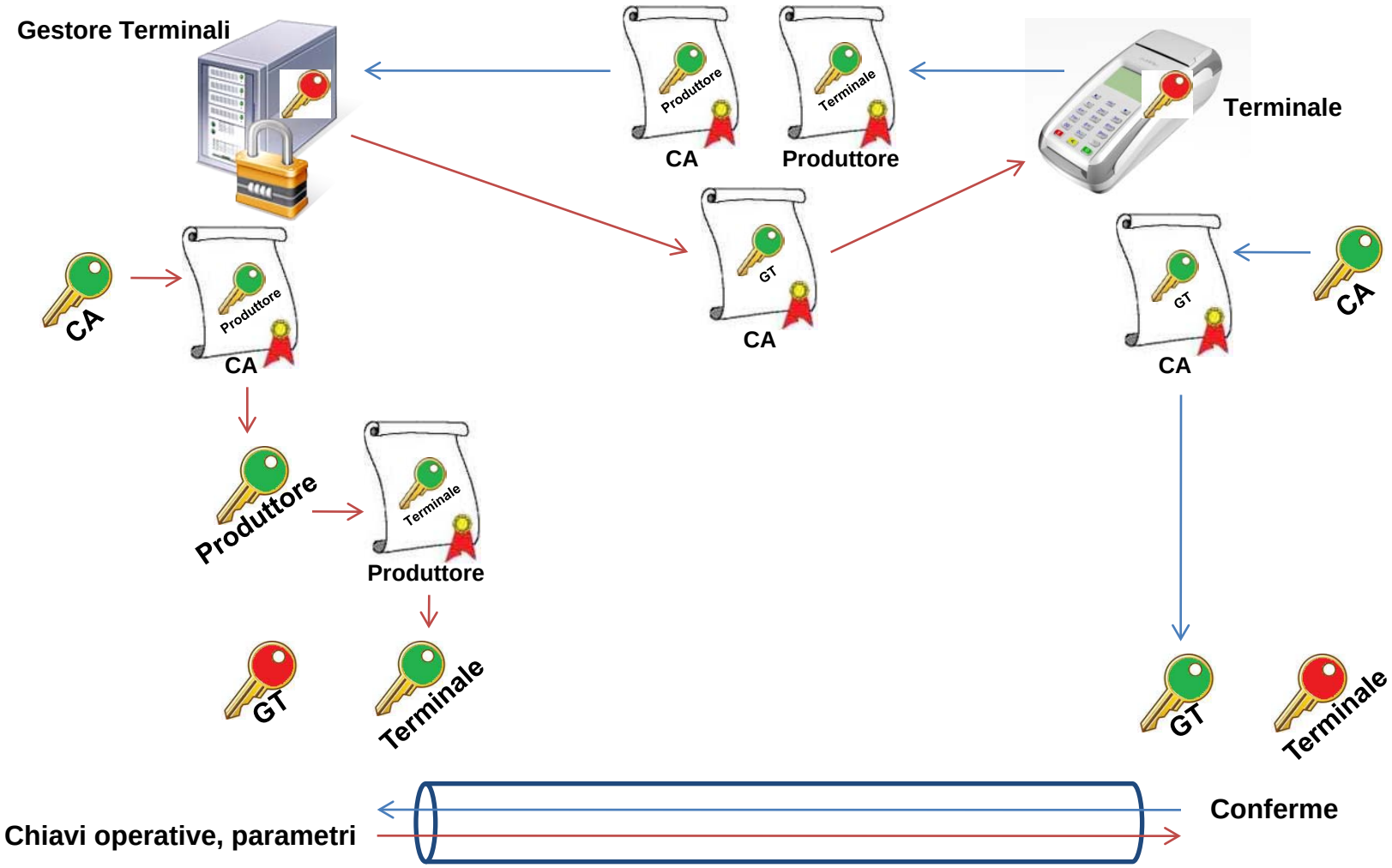
Appartenenza – CB2

CB2 – PKI di processo



Appartenenza – CB2

CB2 – Distribuzione chiavi operative e parametri



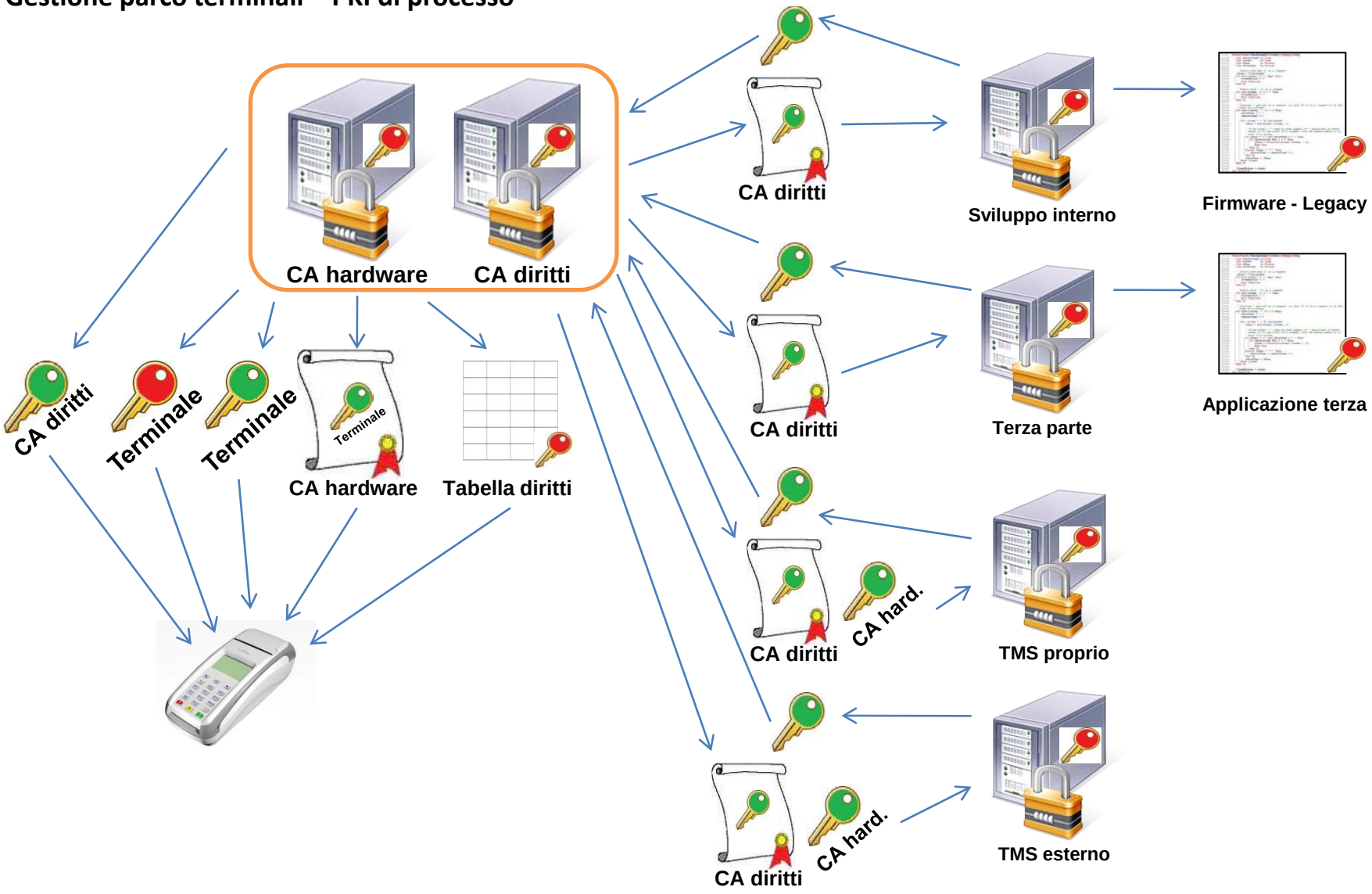
DIRITTI

Diritti – Gestione di un parco terminali

- In questo caso il problema è gestire un parco terminali, in termini di parametrizzazione, di aggiornamento firmware e software e di assistenza da remoto
- Questo in presenza di più entità che sono abilitate a fare operazioni differenti, cioè ad esercitare differenti diritti definiti a livello contrattuale
- Pensiamo all'esclusivo controllo del produttore sul sistema operativo e sulle librerie di sicurezza, mentre terze parti possono essere autorizzate alla scrittura di applicazioni
- Oppure alla possibilità di differenti Terminal Management System (TMS) di effettuare solo specifiche operazioni, come il download di file particolari o la modifica di alcuni parametri
- La struttura dei certificati (sia ISO che X.509) non permette una gestione adeguata dei diritti, nel caso questi non siano uniformi all'interno del gruppo di appartenenza
- E' stata creata quindi un'infrastruttura PKI "multipla", con differenti chiavi di "radice" e l'impiego di certificati X.509
- La scelta dei certificati X.509 è stata fatta perché permettono una maggior libertà nella creazione dell'identificativo del possessore della chiave
- E' stato anche introdotto il concetto di "Tabella dei diritti", per aggiungere quella "granularità" nell'applicazione dei diritti che non era ottenibile con i soli certificati

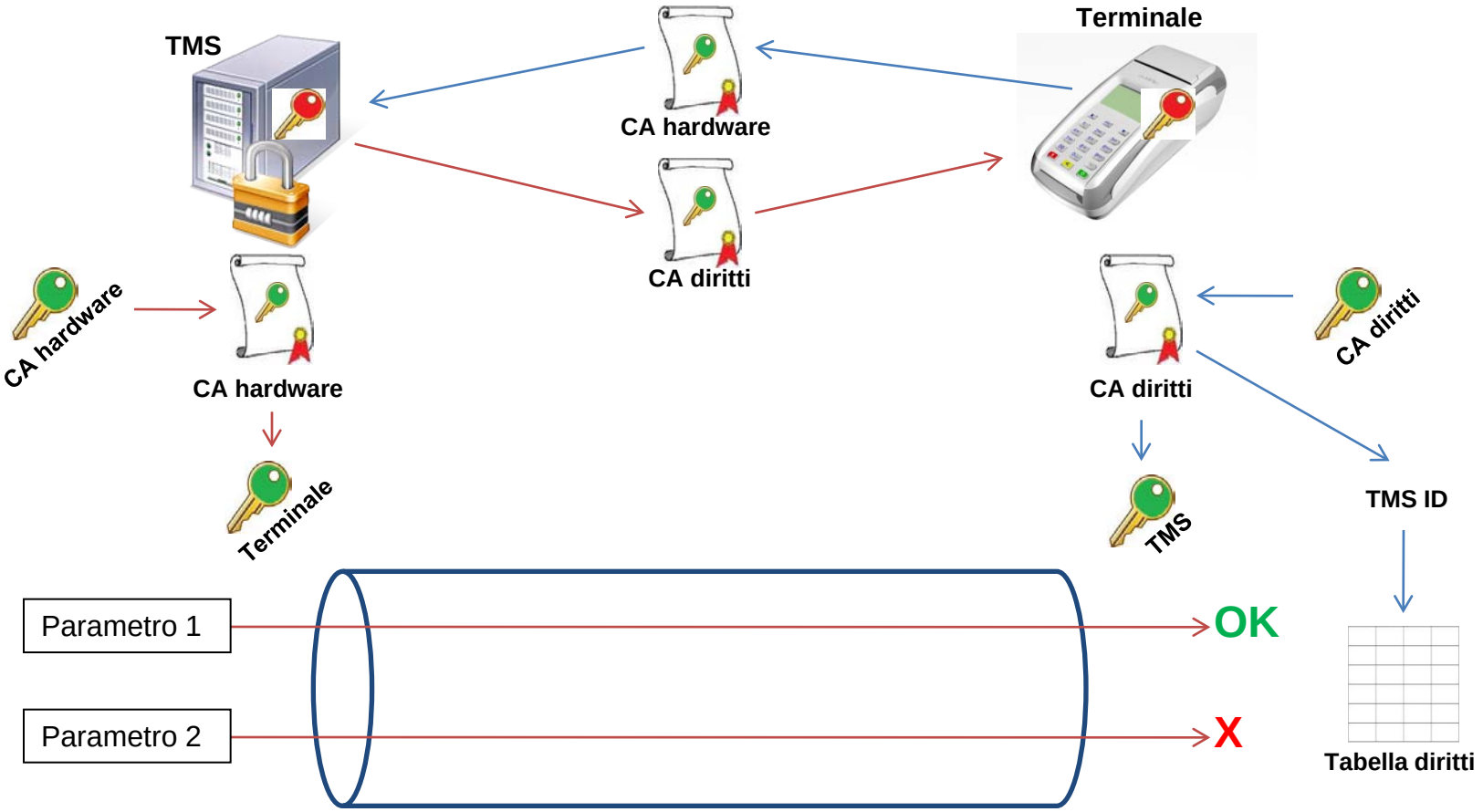
Diritti – Gestione di un parco terminali

Gestione parco terminali – PKI di processo



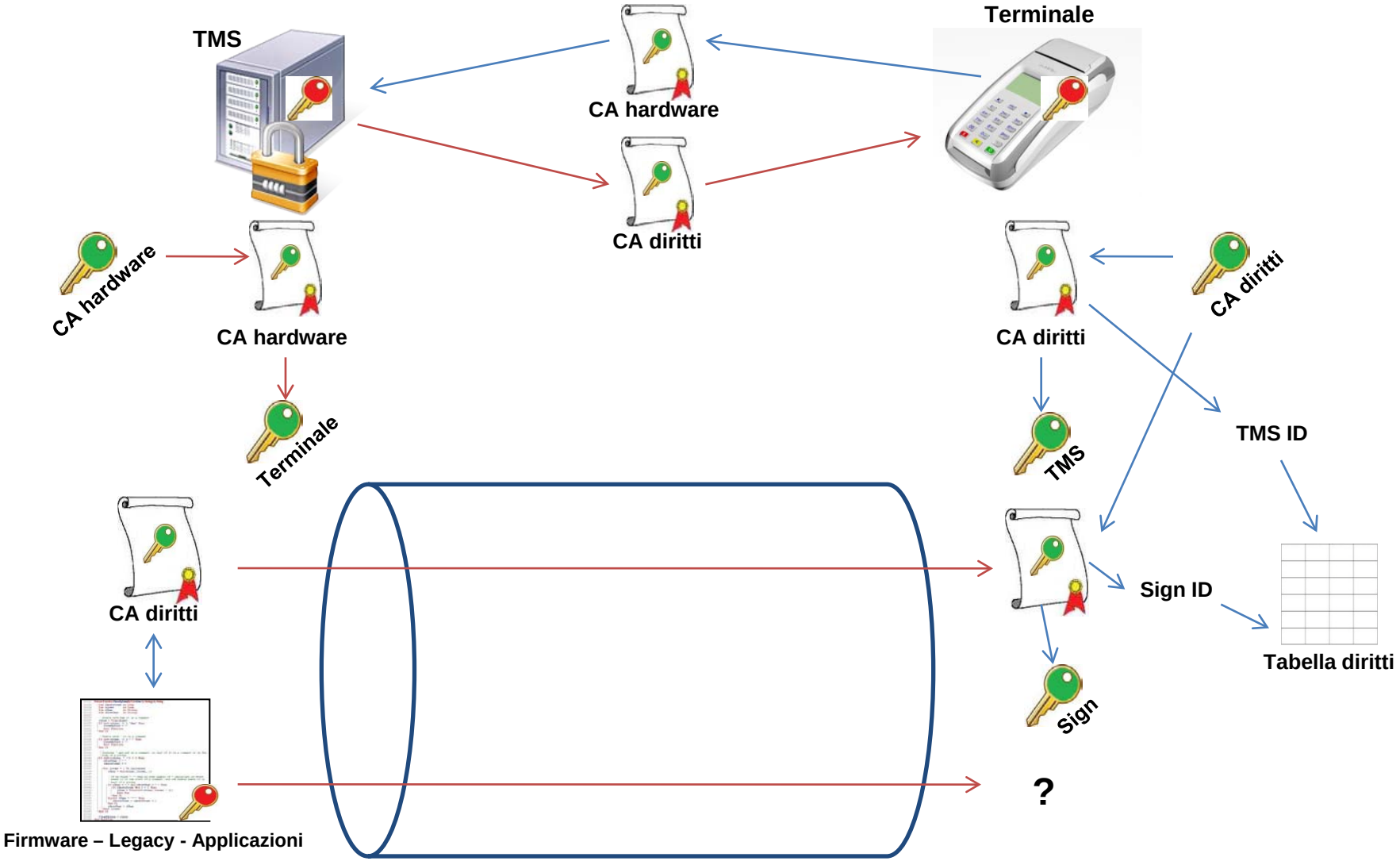
Diritti – Gestione di un parco terminali

Gestione parco terminali – Parametrizzazione



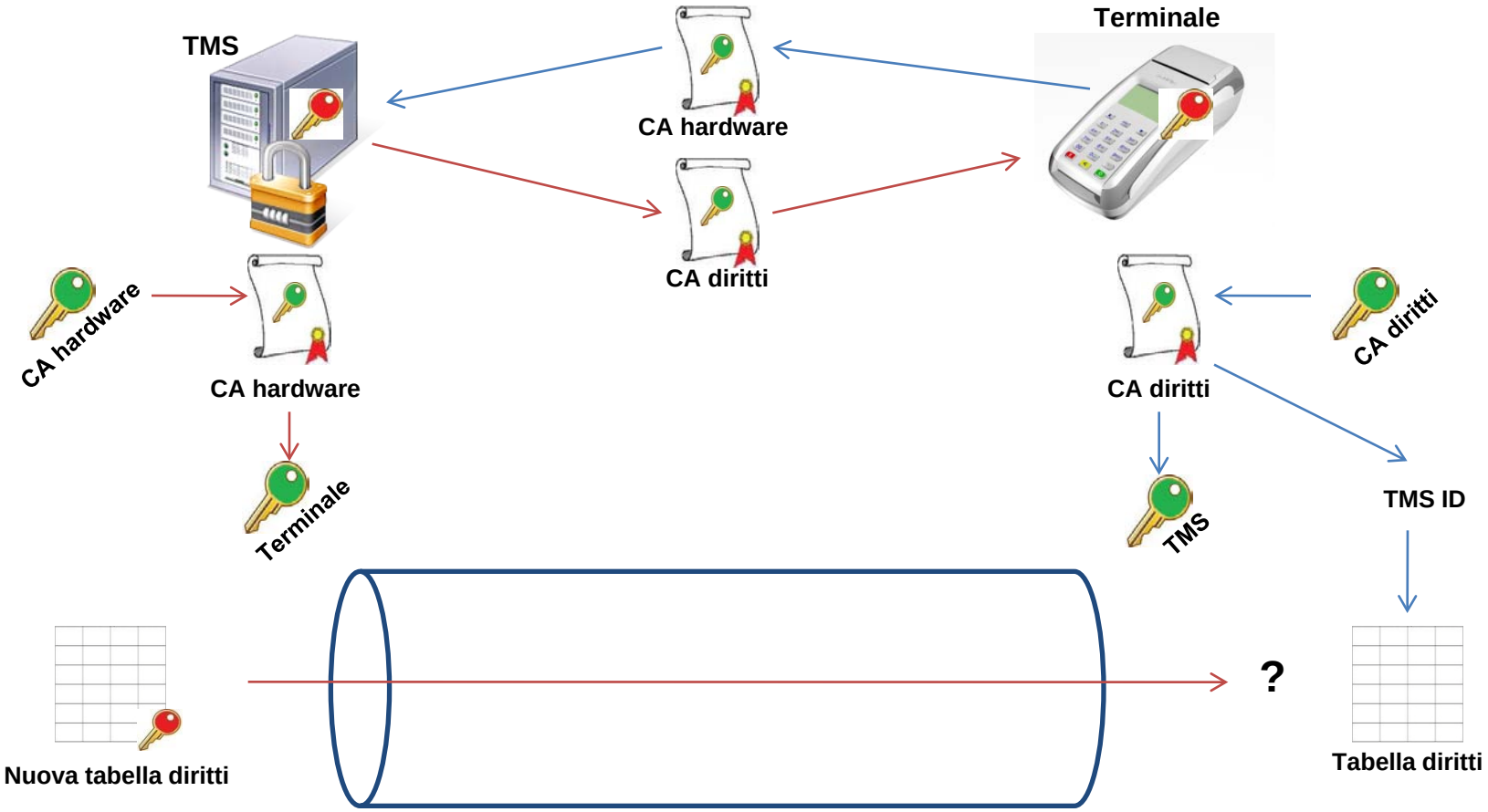
Diritti – Gestione di un parco terminali

Gestione parco terminali – Download firmware-software



Diritti – Gestione di un parco terminali

Gestione parco terminali – Cambio diritti



CONCLUSIONI

Conclusioni

- La sostituzione di un algoritmo con un altro deve essere motivata da, ad es.:
  - L'introduzione di nuove funzionalità prima non ottenibili ed economicamente interessanti
  - Un significativo miglioramento delle performance in una o più delle funzionalità già disponibili, o il superamento di un limite non più accettabile, o la riduzione di un costo
  - Un incremento significativo del rischio nel caso venisse mantenuto l'algoritmo correntemente utilizzato
- Il nuovo algoritmo deve essere verificato con attenzione, tenendo in debito conto l'impatto che avrà nell' "eco-sistema" a cui è destinato
- La sostituzione deve essere accettabile per il mercato in termini di costi e tempi di messa in servizio della nuova infrastruttura
- Deve esistere la possibilità di un periodo di "interregno" in cui entrambi gli algoritmi devono convivere "in campo", poiché, in base alla distribuzione degli apparati che li impiegano, il tempo di aggiornamento può essere più o meno lungo
- Per tutto quanto sopra indicato, non si può pensare che le sostituzioni avvengano frequentemente, indipendentemente
  - da quanto siano mirabolanti i risultati della ricerca o anche, purtroppo,
  - da quale sia il rischio a continuare ad utilizzare qualcosa di "obsoleto"

Grazie dell'attenzione!

http://it.linkedin.com/in/rsabbatini

info@alphaorionis.eu alpha orionis