Tutti i vantaggi della tecnologia Calypso

di Gianni Becattini > g.becattini@aep-italia.it

Una tecnologia aperta ed indipendente da qualsiasi monopolio industriale, nata per rispondere alle esigenze attuali e future del trasporto pubblico.

Calypso: per gli acculturati è il nome di quella ninfa che, nell'Odissea, salva ed ama Ulisse. Per i più giocondi è il nome di un ballo sudamericano. Per gli astronomi, è l'undicesimo satellite di Saturno, del diametro di 26 chilometri e in orbita a 294.660 km dal pianeta.
Ma per noi che siamo un tantino fissati per la tecnologia Calypso significa (...come viene subito fatto di pensare...) "Contact And conctaLess environment Yielding a citizen Pass integration urban Services and financial Operations" (considerando che la ninfa Calypso fece ritardare Ulisse di sette anni nel suo ritorno a casa, avrei scelto un altro nome...).
Scherzi a parte, anche se il significato della sigla è ignoto ai più (anche io me lo sono dovuto andare a cercare), la parola è ben conosciuta a tutti gli operatori della bigliettazione elettronica, sebbene non tutti abbiano al riguardo le idee chiare. Con una piccola indagine personale ho potuto raccogliere le seguenti "perle":
Calypso è un modello di smart card;
Calypso è una marca di obliteratrici;
Calypso è il nome commerciale dello standard ISO 14443B.
Spero quindi di fare una cosa utile riportando qualche informazione in merito.

Cosa è?

Diciamo subito che CALYPSO è il nome di un progetto avviato nel 1998 su finanziamento dell'Unione Europea e su coordinamento di RATP (Regie Autonome des Transport Parisiens) in collaborazione con le città di Costanza, Lisbona, Parigi e Venezia, come prosecuzione del progetto comunitario ICARE (Integration of Contactless technologies into public transport environment). Il progetto aveva come obiettivo la realizzazione di una carta multifunzionale che offrisse al cittadino la possibilità di compiere una serie di possibili operazioni di accesso e/o pagamento di beni e servizi. Tra i risultati di questi sforzi, lo sviluppo della famiglia di carte CD-97 e la definizione dello standard ISO 14443 B, oltre a sostanziali evoluzioni della normativa ENV 1545.
Oggi Calypso è il nome dello standard per la bigliettazione elettronica contactless che definisce un dialogo sicuro tra la carta ed il terminale, basato su circa dieci anni di studi e sperimentazioni.
Calypso è stato progettato da operatori del trasporto pubblico ed è quindi ragionevole pensare che esso risponda perfettamente alle esigenze specifiche del settore. E' stato anche ampiamente collaudato, essendo stato adottato da numerose città italiane ed europee (vedi la figura qui sopra).

Promesse

Calypso si presenta come una tecnologia aperta ed indipendente da qualsiasi monopolio industriale, nata per rispondere alle esigenze attuali e future dei protagonisti mondiali del trasporto pubblico. La tecnologia Calypso cerca, cioè, di definire un sistema che permetta ad ogni operatore del trasporto di trovare la propria soluzione e di modularne lo sviluppo a seconda delle proprie esigenze.

Questi alcuni dei vantaggi ipotizzati:
- multisorgente
- sicurezza
- aderenza agli standard
- ampio spettro di soluzioni
- affidabilità
- apertura
- rispetto della privacy

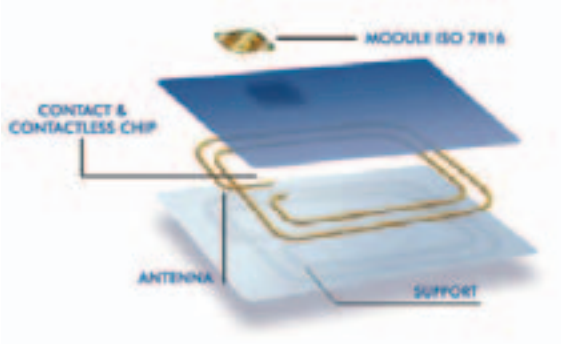
La Calypso Network Association

Per assicurare una costante evoluzione del progetto Calypso, i fondatori e gli utenti di Calypso hanno creato una organizzazione non-profit denominata Calypso Networks Association, i cui scopi sono i seguenti:
- soddisfare le esigenze degli operatori del trasporto e garantire la perennità dei loro investimenti;
- stabilire durevoli relazioni con tutti i partner che utilizzano le specifiche Calypso;
- definire ed evolvere le specifiche tecniche;
- implementare una politica di certificazione per garantire la compatibilità di tutti i prodotti attuali e futuri;
- stabilire una marcatura Calypso rilasciata da una organizzazione indipendente;
- promuovere la tecnologia Calypso presso gli operatori del settore, ossia le Compagnie di trasporto, e presso i Costruttori di

apparati e di carte;
- contribuire ai processi internazionali di standardizzazione;
- facilitare e armonizzare le esigenze e le esperienze dei membri;
- incoraggiare le azioni di mutua assistenza nella implementazione di sistemi di bigliettazione elettronica basati su Calypso.

Necessità di standardizzazione

Se qualcuno ha avuto la pazienza di leggere uno dei miei precedenti articoli su Mobility-Lab, ricorderà quella che ho giocosamente denominato "prima legge di Becattini": "**dati due apparati, la probabilità che possano parlare tra loro è pressoché nulla**", sia



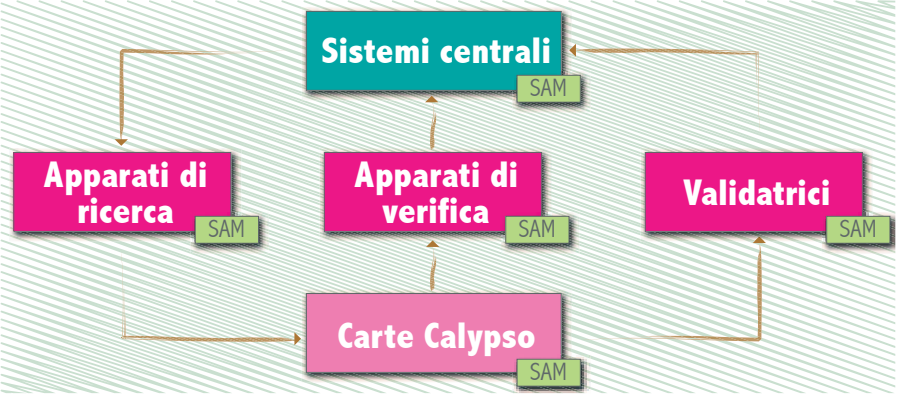
per la naturale tendenza al caos di qualunque sistema informatico, sia per la volontà dei Costruttori, espressa o meno, di rendere i propri sistemi inaccessibili alla concorrenza. Smart card ed i relativi terminali non fanno eccezione a questa legge e quindi standardizzazione ed interoperabilità sono, anche in questo caso, tanto indispensabili quanto difficili da conseguire.
Immaginiamo di dover reinventare un sistema smart card/terminale.
Quali problemi ci troveremmo ad affrontare?
Proviamo a buttar giù un elenco di punti:
- in primo luogo saremmo curiosi di capire se fosse possibile trasferire energia per via radio dal terminale alla carta;
- poi vorremmo scambiare qualche byte con la stessa;
- poi potremmo voler creare un "protocollo" per stabilire regole certe nella comunicazione dei dati ed un set di comandi per interagire con la carta.
Già questo sarebbe un bell'inizio, ma non sarebbe sufficiente: mancano ancora, come minimo, dei meccanismi per gestire la sicurezza, degli accorgimenti per assicurare un funzionamento affidabile anche quando la carta venisse rimossa troppo rapidamente dal campo, la protezione contro la presentazione simultanea di più carte (*detta collisione)*, la definizione dei formati di memorizzazione e così via. Un bel compito davvero!

Gli standard internazionali

Per fortuna qualcuno è arrivato prima di noi e ha già svolto una gran parte di questo lavoro. Facciamo un rapido riepilogo degli standard internazionali. I più importanti sono:
- ISO 7816 per le carte a contatti;
- ISO 14443 per le carte contactless; alla costruzione di questi standard, il progetto Calypso ha apportato un contributo molto significativo;
- ENV 1545 per le strutture dati.
Questi standard sono suddivisi in parti; descriviamole rapidamente:
- ISO 7816 parte prima: caratteristiche fisiche delle carte a contatti, resistenza a fenomeni fisici quali raggi UV e raggi X, campi elettromagnetici, elettrostatici ecc. Definisce inoltre le caratteristiche meccaniche e di resistenza allo stress.
- ISO 7816 parte seconda: definisce la posizione e la dimensione dei contatti;
- ISO 7816 parte terza: definisce segnali e protocolli di comunicazione;
- ISO 7816 parte quarta: contenuto dei messaggi, comandi e risposte trasmessi dal terminale alle carte e viceversa; struttura dati e file; modo di accesso ai dati ed ai file e altra simile mercanzia.
- ISO 7816 parte quinta: sistema di numerazione e procedure di registrazione per gli identificatori delle applicazioni;
- ISO 7816 parte sesta: interindustry data elements;
- ISO 14443 parte prima: dimensione delle carte contactless, qualità superficiale per la stampa, resistenza meccanica, resistenza agli UV ed ai raggi X, sensibilità ai campi elettromagnetici. Equivale, per le carte contactless, alla ISO 7816-1 delle carte a contatti;
ISO 14443 parte seconda: descrive le caratteristiche del trasferimento di potenza, basato su accoppiamento induttivo, e la comunicazione tra terminale e carta;
ISO 14443 parte terza: descrive i meccanismi di inizializzazione e di anticollisione;
ISO 14443 parte quarta: protocolli di trasmissione.
- ENV 1545: definisce la codifica delle strutture dati usate per il trasporto pubblico (es. data, ora, evento di validazione, contratto di trasporto ecc.).

Arriva Calypso

Le norme sopra citate non sono sufficienti ad implementare una effettiva interoperabilità. Ad esempio, la ENV 1545 definisce le strutture dati utilizzabili ma non la composizione delle stesse, che resta sempre demandata alle singole applicazioni. Quindi si possono avere n sistemi diversi che, pur applicando le stesse norme, non risultano assolutamente compatibili tra di loro.
Un bel pezzo che manca agli standard internazionali è quello che definisce i meccanismi di sicurezza, in particolare per quanto riguarda la cosiddetta sessione sicura. Scopi della sessione sicura sono i seguenti:
- provare l'autenticità del terminale alla carta (autenticazione del terminale);
- provare l'autenticità della carta al terminale (autenticazione della carta);
- certificare l'autenticità di tutti i dati scambiati durante la sessione;
- garantire che tutte le modifiche alla carta sono state compiute correttamente e che, pertanto, la carta non sia rimasta in qualche meta-stato per essere stata, ad esempio, ritirata anzi tempo dal campo del terminale.
Ecco che Calypso interviene a questo punto proponendo una serie di meccanismi tesi a risolvere tra altri, anche questo problema.
La sicurezza Calypso è basata sui moduli SAM, su cui ci siamo soffermati in passato in queste pagine, come schematizzato nella figura seguente:



Calypso definisce esattamente i colloqui terminale/carta e terminale/modulo SAM, nonché le varie operazioni di crittografia necessarie per conseguire gli scopi sopra elencati.
Per una reale interoperabilità, che è poi in fondo uno degli obiettivi principali del progetto Calypso, sarebbe necessario implementare i 7 livelli riportati nella tabella seguente:

	Layer	Standard	Calypso Status
7	*Security Management and Architecture*		*Calypso Security Architecture*
6	*Terminal Applicative Software*		*Calypso API*
5	*Data Model*		*Calypso Data Model*
4	*Card and SAM Security Mechanisms*		*Calypso card application*
3	*Card Data structure*	*CEN ENV 1545*	
2	*Card OS and Files structure & Commands*	*ISO 7816-4*	
1	*Contact and Contactless Communication Interface*	*ISO 7816 1-3 ISO 14443 B 1-4*	

I livelli 1, 2 e 3 sono definiti da standard internazionali; il livello 4 è risolto - e direi in maniera ottimale - da Calypso, mentre i livelli 5, 6 e 7 sono ancora in fase di implementazione.

Il costo di Calypso

La tecnologia Calypso è gratuita per gli operatori del trasporto pubblico; i costruttori di carte e di apparati, invece, pagano royalty alla società francese Innovatron. Le somme versate, si dichiara, sono utilizzate per migliorare ed estendere lo standard. Poiché non conosco costruttori filantropi, immagino che ognuno di essi giri i costi ai propri clienti, quindi in realtà la tecnologia Calypso non è di fatto gratuita, anche se il suo costo, nel bilancio di un Sistema di Bigliettazione Elettronica è di fatto del tutto trascurabile (probabilmente, nel complesso, non raggiunge lo 0,5%). Ritengo che la tecnologia abbia sempre e comunque un costo: nel caso di Calypso, credo che ciò che si ottiene meriti la spesa. “Inventarsi” una tecnologia equivalente avrebbe un costo certamente assai superiore.

Calypso in Italia

Per motivi sconosciuti, in Italia è d’uso non pronunciare mai il nome Calypso. Anche quelle Compagnie che desiderano adottare questa tecnologia, sono solite indicare, oltre alle solite norme ISO 14443 B, il modello e, implicitamente, la marca della carta. Questa vorrebbe apparire come una posizione super partes; in realtà è esattamente il contrario, in quanto la tecnologia Calypso, pur non gratuita, è aperta, mentre i modelli di carte, come la GTML, sono proprietari. La tabella successiva riporta una concisa sintesi delle scelte operate nelle maggiori realtà italiane. Come si vede, Calypso la fa da padrone, anche se spesso in parallelo con le carte MIFARE, uno standard proprietario di Philips di cui ci occuperemo in altra occasione.

Città	Ente	Tipo carta	Standard	Note
Milano	*ATM – FNM -Trenitalia*	*GTML ed altre*	*Calypso, MIFARE*	
Roma	*ATAC Trambus Metro*	*MV4000*	*ISO 14443B*	
Campania	*Unico Campania*	*GTML*	*Calypso*	
Umbria	*Titolo Regionale*	*GTML*	*Calypso*	
Venezia	*ACTV*	*GTML ed altre*	*Calypso, MIFARE*	
Padova	*APS*	*GTML ed altre*	*Calypso, MIFARE*	
Treviso	*ATTV*	*GTML*	*Calypso*	
Firenze	*ATAF*	*CTS-256 e altre*	*Calypso*	
Prato	*CAP*	*COS8*	*Proprietario*	*a contatti*
Vicenza	*FTV*	*GTML ed altre*	*Calypso, MIFARE*	
Emilia R.	*Titolo Regionale*	*GTML ed altre*	*Calypso, MIFARE*	
Trento	*Trentino T. Trenitalia*	*MIT (TSF)*	*ISO 14443B*	

Le carte Calypso

La tabella seguente dà una panoramica delle carte Calypso attuali e future.

Calypso 1				
Carta	***Chip***	***Algoritmi***	***Contatori/file***	***Note***
CD-97	*ST16RF52*	*DES*	*4F/4C*	*3*
GTML	*ST16R820*	*DES*	*1F/9C*	*3*
CT-2000	*ST16RF58*	*DES-DESX-3DES*	*1F/9C*	*3,5*
Calypso 2				
Carta	***Chip***	***Algoritmi***	***Contatori/file***	***Note***
GTML2	*ST16R820*	*DES-DESX*	*1F/9C*	*1,3*
CD-light	*ST16R820*	*DESX*	*1F/9C*	*2,3*
CD-97BX	*ST16RF52*	*DES-DESX*	*1F/9C*	*2,3,4*
BMS2	*ST19XR8*	*DES-DESX*	*1F/9C*	*2*
Tango	*ATMEL*	*DES-DESX-(3DES)*	*1F/9C*	*2*
CD-21	*ST19RWR02*	*DES-DESX-(3DES)*	*1F/9C*	*2,4*
Nota 1 - protocollo RF da decidere in fase di inizializzazione				
Nota 2 - protocollo RF selezionabile dinamicamente				
Nota 3 - chip non più in produzione				
Nota 4 - può emulare completamente la CD-97				
Nota 5 - dichiarata Calypso ma non testata da Calypso				

Come indicato nella tabella, il chip ST-16 non è più in produzione; quindi la carta GTML non sarà più producibile. Nuove carte stanno però per sostituirla, come ad esempio la CD-21 e le carte Tango di ASK, con completa emulazione della stessa. Si ritiene, nel frattempo, ancora conveniente utilizzare carte GTML “originali”, anche nell’attesa che i nuovi prodotti vengano perfettamente stabilizzati.
Tra i costruttori di carte Calypso, desidero citare
ASK (www.ask.fr)
AXALTO (www.axalto.com)
GEMPLUS (www.gemplus.com)
ITS MAGNADATA (www.magnadata.co.uk)
OBERTHUR CARD SYSTEMS (www.oberthurcs.com).

Apparati Calypso

Realizzare un terminale Calypso non è affatto facile e richiede investimenti cospicui: con il pagamento della licenza si ottengono le specifiche ma non certo schemi o programmi che devono essere sviluppati da parte del licenziatario.
In Italia, l’unica licenziataria di Calypso è AEP (www.aep-italia.it), anche se ci sono altre aziende che, non avendo sviluppato apparati propri, incorporano moduli elettronici di terze parti. Tra le aziende estere, tutte le grandi, come Ascom (www.ascom.com), ERG (www.erggroup.com) e Thales (www.thalesgroup.com).

Conclusione

Calypso è una pietra angolare dei Sistemi di Bigliettazione Elettronica; il suo costo appare largamente compensato dai benefici che offre. Tutti i principali costruttori di carte e di apparati offrono oggi soluzioni Calypso e le principali città italiane hanno adottato questa tecnologia. Chi lo desidera può contattarmi direttamente per comunicarmi le proprie osservazioni (g.becattini@aep-italia.it).

Autore

***Gianni Becattini** è uno dei pionieri dell’informatica italiana. Nel 1975 progetta uno dei primi personal computer italiani e fonda la General Processor, i cui prodotti sono oggi esposti al Museo dell’Informatica di Pisa. Dal 1999 dirige AEP, di cui oggi è Amministratore Delegato (www.aep-italia.it).*