Cagliari - 11 Novembre 2015

I sistemi di pagamento nella mobilità

con il patrocinio di

Seminario di approfondimento sull'uso delle carte bancarie contactless nella mobilità

Roberto Andreoli

ATM Milano

Contesto

La Digitalizzazione e la quasi permanente connessione delle persone durante il viaggio sta cambiando la relazione con passeggero rendendo necessario in molti casi, un ripensamento dei servizi di mobilità verso l'utenza.

Un ecosistema SMART

Crescente disponibilità
di piattaforme informatiche,
di dati e informazioni

↓

Necessità di integrazione

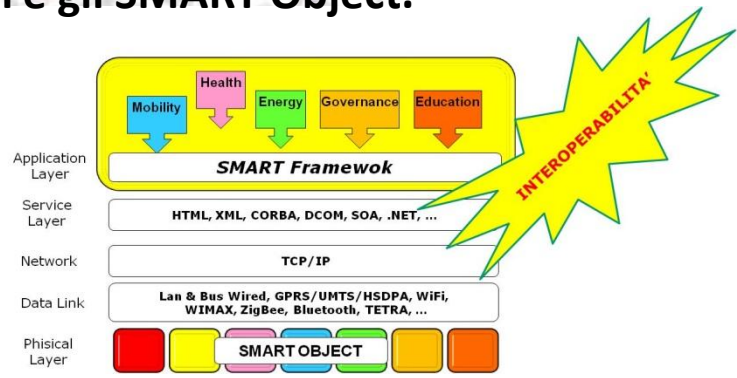
↓

Necessità di standard
al livello APPLICATIVO

↓

Un Ecosistema SMART

La standardizzazione deve portare alla realizzazione di un *Framework Applicativo* su cui inserire le SMART Application e gli SMART Object.



Timeline: ATM dal 2003 – ad oggi

Virtualizzazione dei titoli di viaggio e sosta

2003

Inizia il sistema di Bigliettazione Elettronica

2005

Tutti i titoli sono elettronici

2009

ATM portal

Emissione *di nuove tessere (abbonamenti mensili/annuali)*

2011

Bancomat o portale Web

Ricarica *delle Tessere ATM (Settimanale, mensile, annuale)*

Introduzione dei TOTEM di ricarica

2012

Parcometro

Ricarica tessera ATM

La congestion Charge di Milano: Area C una piattaforma innovativa di servizi integrati

2014

NFC ticketing Abbonamento annuale

App ATM

- *WALLET*
- *Possibilità di acquisto dei singoli Ticket*

2015

Evoluzione dei tornelli

Introduzione Lettore QR code

SMS ticketing

Acquisto biglietti singoli urbani ed EXPO

APP Sosta e parcheggi

ATM
AZIENDA TRASPORTI MILANESI S.p.A.

Sistemi di Mobile Ticketing ATM

NFC

- **Ricarica la tua tessera ATM (Itinero),** mediante una app dedicata (PosteMobile NFC);
- **Convalida la tua tessera ATM**, con un semplice gesto, utilizzando il lettore NFC presente in tutti i tornelli delle linee metro e a bordo dei veicoli di superficie.

ATM app ticketing

- Scarica la app ufficiale **ATM Milano official App**;
- Crea il tuo profilo ATM;
- Acquista i tuoi biglietti utilizzando il tuo account Paypal o la carta di credito;
- Crea il tuo **Wallet personale**;
- Non ci sono costi aggiuntivi;
- Prima di salire sui mezzi convalida il tuo biglietto digitale.

SMS-ticketing

- **Acquista il tuo biglietto ATM** via SMS;
- Servizio disponibile per i principali Operatori nazionali;
- Costi aggiuntivi relativi ai servizi premium;
- Attendi il tuo **biglietto SMS**;
- Sali a bordo, sui mezzi di superficie, oppure utilizza il lettore di QR code per abilitare i tornelli in metropolitana.

La Piattaforma di Fare Logic

Replicare lo stesso modello di condivisione dei dati di infomobilità per il sistema di Ticketing.

Possibilità di integrazione con altri attori di trasporto Pubblico (ATM-Trenord-ecc.) e non solo.

Biglietti speciali

Ticketing fare logic: TPL, Sosta, Area C

Stakeholders

Telephone carrier, Bank Acquirer, Payment Gateways….

Smart Validator

Quali nuove opportunità si aprono nel mondo del Ticketing ?

NFC – Host Card Emulation
Contacless EMV

Le normative e regole del settore bancario sono adeguate al TPL? E' possibile facilitare l'innovazione dei pagamenti EMV contactless?

Il quadro delle principali regole

PciPts 3/4
EmvCo L1 e L2
Cb2
PCI DSS

Dati di account	
I dati dei titolari di carta comprendono:	**I dati sensibili di autenticazione comprendono:**
▪ PAN (Primary Account Number) ▪ Nome titolare di carta ▪ Data di scadenza ▪ Codice di servizio	▪ Dati della traccia completa (dati della striscia magnetica o dati equivalenti in un chip) ▪ CAV2/CVC2/CVV2/CID ▪ PIN/Blocchi PIN

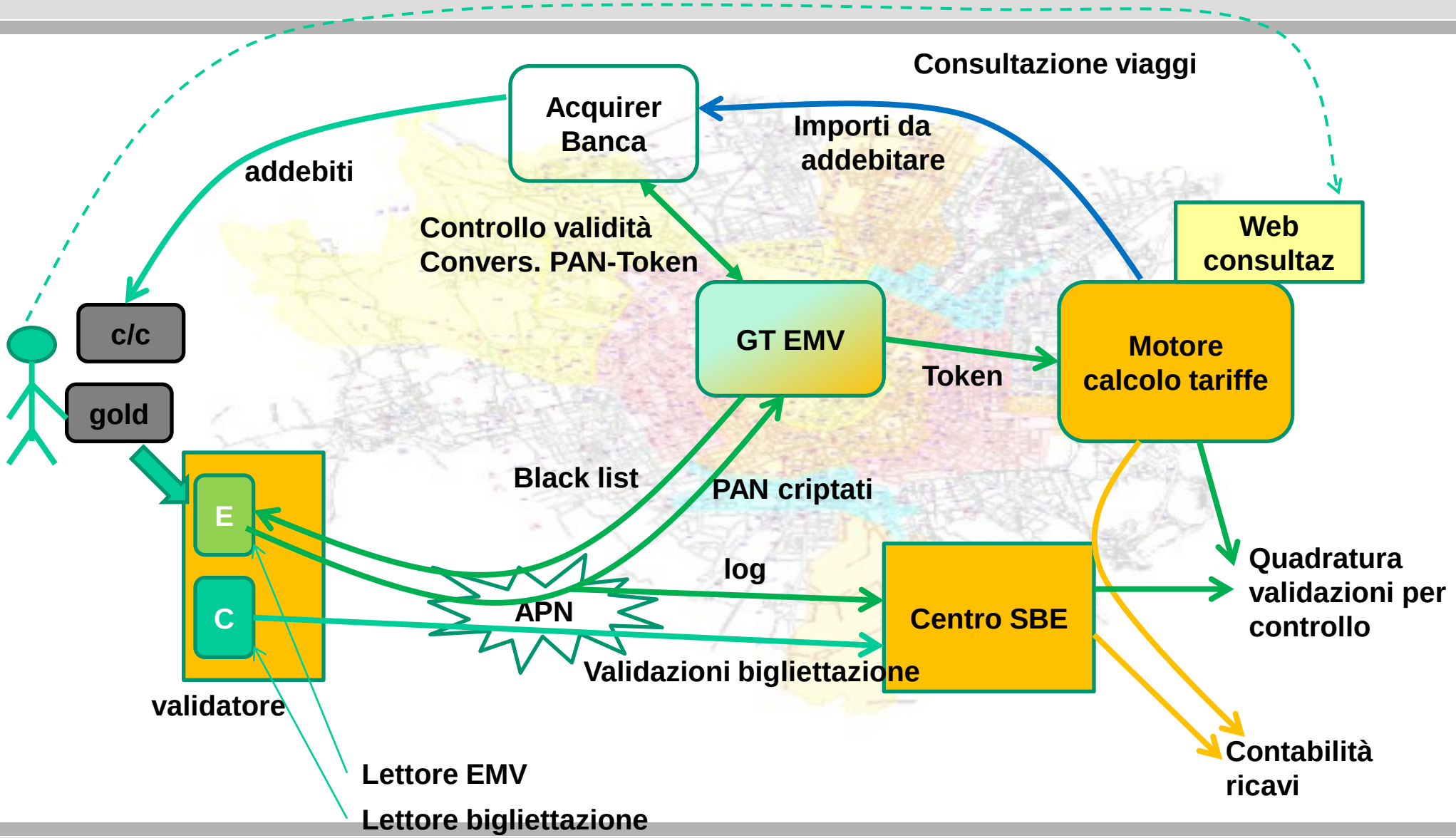
Lo standard di protezione dei dati per il settore delle carte di pagamento (PCI DSS) è stato sviluppato per favorire e migliorare la protezione dei dati dei titolari di carta nonché per semplificare l'implementazione di misure di sicurezza dei dati coerenti a livello globale. Lo standard PCI DSS mette a disposizione una base di requisiti tecnici ed operativi volti a proteggere i dati dei titolari di carta. Lo standard PCI DSS si applica a tutte le entità coinvolte nell'elaborazione di carte di pagamento, con l'inclusione di esercenti, elaboratori, acquirenti, emittenti e provider di servizi, nonché di tutte le altre entità che si occupano di memorizzare, elaborare o trasmettere dati dei titolari di carta e/o dati sensibili di autenticazione.

Standard di protezione dei dati PCI - Panoramica di alto livello

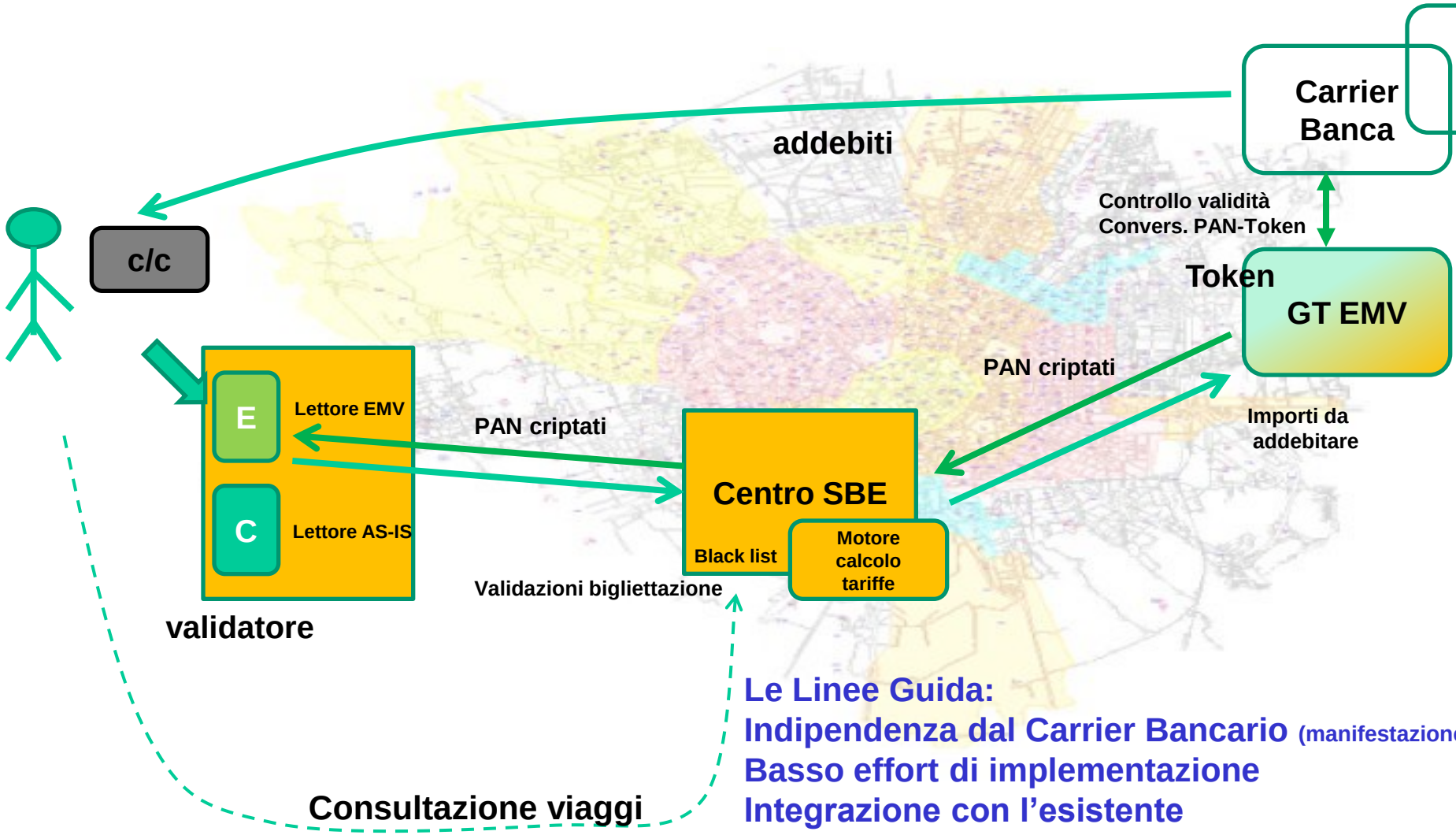
Sviluppo e gestione di sistemi e reti sicure	**1.** Installare e gestire una configurazione firewall per proteggere i dati dei titolari di carta **2.** Non utilizzare valori predefiniti del fornitore per le password di sistema e altri parametri di protezione
Protezione dei dati dei titolari di carta	**3.** Proteggere i dati dei titolari di carta memorizzati **4.** Cifrare i dati dei titolari di carta trasmessi su reti aperte e pubbliche
Utilizzare un programma per la gestione delle vulnerabilità	**5.** Utilizzare e aggiornare regolarmente il software o i programmi antivirus **6.** Sviluppare e gestire sistemi e applicazioni protette
Implementazione di rigide misure di controllo dell'accesso	**7.** Limitare l'accesso ai dati dei titolari di carta solo se effettivamente necessario **8.** Individuare e autenticare l'accesso ai componenti di sistema **9.** Limitare l'accesso fisico ai dati dei titolari di carta
Monitoraggio e test delle reti regolari	**10.** Registrare e monitorare tutti gli accessi a risorse di rete e dati dei titolari di carta **11.** Eseguire regolarmente test dei sistemi e processi di protezione.
Gestione di una politica di sicurezza delle informazioni	**12.** . Gestire una politica che garantisca la sicurezza delle informazioni per tutto il personale.

		Elemento di dati	*Memorizzazione consentita*	*Rendere i dati memorizzati illeggibili in base al Requisito 3.4*
Dati di account	*Dati dei titolari di carta*	*PAN (Primary Account Number)*	*Sì*	*Sì*
		Nome titolare di carta	*Sì*	*No*
		Codice di servizio	*Sì*	*No*
		Data di scadenza	*Sì*	*No*
	Dati sensibili di autenticazione[2]	*Dati della traccia completa*[3]	*No*	*Impossibile memorizzare in base al Requisito 3.2*
		CAV2/CVC2/CVV2/CID[4]	*No*	*Impossibile memorizzare in base al Requisito 3.2*
		PIN/Blocco PIN[5]	*No*	*Impossibile memorizzare in base al Requisito 3.2*

Il modello proposto dal «sistema»



Il modello 2.0 e linee guida



Le Linee Guida:
Indipendenza dal Carrier Bancario (manifestazione di interesse)
Basso effort di implementazione
Integrazione con l'esistente

La conformità alle regole

Secondo le regole, in conformità ai requisiti PCI e gestione dei dati sensibili :

- ATM non potrà essere soggetta a certificazione PCI DSS.
- ATM non potrà avere visibilità di alcun dato sensibile della carta.
- Il numero di Carta (PAN) essendo dato sensibile dovrà essere cifrato.

I Dati delle Carte dovranno essere gestiti rispettando le regole EMV e PCI DSS mediante l'utilizzo di:
Lato Campo:
CNV (validatori) con
-NFC reader in possesso di certificato L1
-Software on-board EMV certificato L2 e PCI DSS

Lato centro :
- Un PG in possesso dei certificati PCI DSS con software conforme alle regole CB2 sull'utilizzo delle Carte Contacless per il mondo trasporti che possibilmente acconsenta al transito del dato (criptato) attraverso il sistema BME di ATM .

I dati possono essere decriptati e ri-criptati anche ad ogni step del processo introducendo però nuove e sfidanti approvazioni.
Il Merchant può effettuare il passaggio dei dati ma senza trattarli
(PCI Security standard scouncil)

Una ipotesi di flusso

La convalidatrice (Modulo POS che cattura la lettura carta installato al suo interno) invia il PAN cifrato al sistema BME ATM che lo inoltra al PG (o direttamente al PG), assieme ad un subset di informazioni contenute nel flusso volte ad identificare l'ammontare da addebitare (al check out).

Il PG riceve questo dato e lo passa all'acquirer scelto da ATM con una frequenza di invio che è funzione delle caratteristiche del sistema di accettazione ATM.

L'acquirer si fa carico di verificare l'integrità del PAN inviato e apre, se necessario, una preautorizzazione al pagamento.

Il PG restituisce un flusso di feedback ad ATM.

Se la carta è buona, con frequenza da stabilire (ad esempio a fine giornata), ATM invia i flussi di addebito della carta al PG che provvede ad inoltrare ai circuiti.

Il rischio esercente rimane totalmente a carico dell'issuer se la carta risulta rubata/non conforme ed è la prima volta che la carta viene trasmessa all'issuer da ATM (ATM non l'ha mai vista pertanto non può esserne responsabile);

Non appena il PG restituisce il flusso di feedback ad ATM, ATM deve provvedere quanto prima ad alimentare le proprie black-list per evitare un nuovo transito della carta marcata come non valida;

Quanto più è rapido il flusso di andata e ritorno, tanto minore è il rischio di far viaggiare "gratis" una carta "rifiutata" il rischio esercente in questo caso è in carico ad ATM (a meno di negoziazione con l'acquirer)

L'infrastruttura

L'utilizzo della carta contactless :

a. Viaggio in metro (check in e check out su tutta la rete)
b. Viaggio in superficie anche sulla rete interurbana
b1. Tariffa differenziata (check in e check out)
b2. Tariffa unica forfait (solo check in, come a Londra)

Componenti necessarie:

Metropolitana:

Equipaggiamento dei tornelli (TUTTI)

Superficie:

Lettore EMV connesso al centro via rete GSM e all' AVM.
Ipotesi b2 : 1 lettori per Veicolo, solo davanti
Ipotesi b1 : equipaggiamento tutti i lettori sulla flotta

Controllori:

Rivedere l'attuale dispositivo sulla base delle regole EMV

- **Variazione significativa al sistema tariffario**
- **Obbligo di convalida anche sul cambio mezzi**
- **Penalizzazione verso chi non convalida.**
- **Nel caso b2. ingresso solo davanti**

- **Variazione significativa sulle regole di controllo e sanzionamento**
- **Sanzionamento a posteriori**
- **Il Cliente non conosce l'importo al momento del pagamento**
- **Il cliente non ha alcuna ricevuta**

L’infrastruttura, i costi e i vincoli

Quali sarebbero i costi totali da sostenere per ATM ?

Infrastruttura:

ca. 1700 Tornelli
ca. 2200 Veicoli

Rete, connessioni integrazioni con l’esistente……

Gestione:

% per il PG
% per l’Acquirer (dipendente dall’accordo sul rischio)

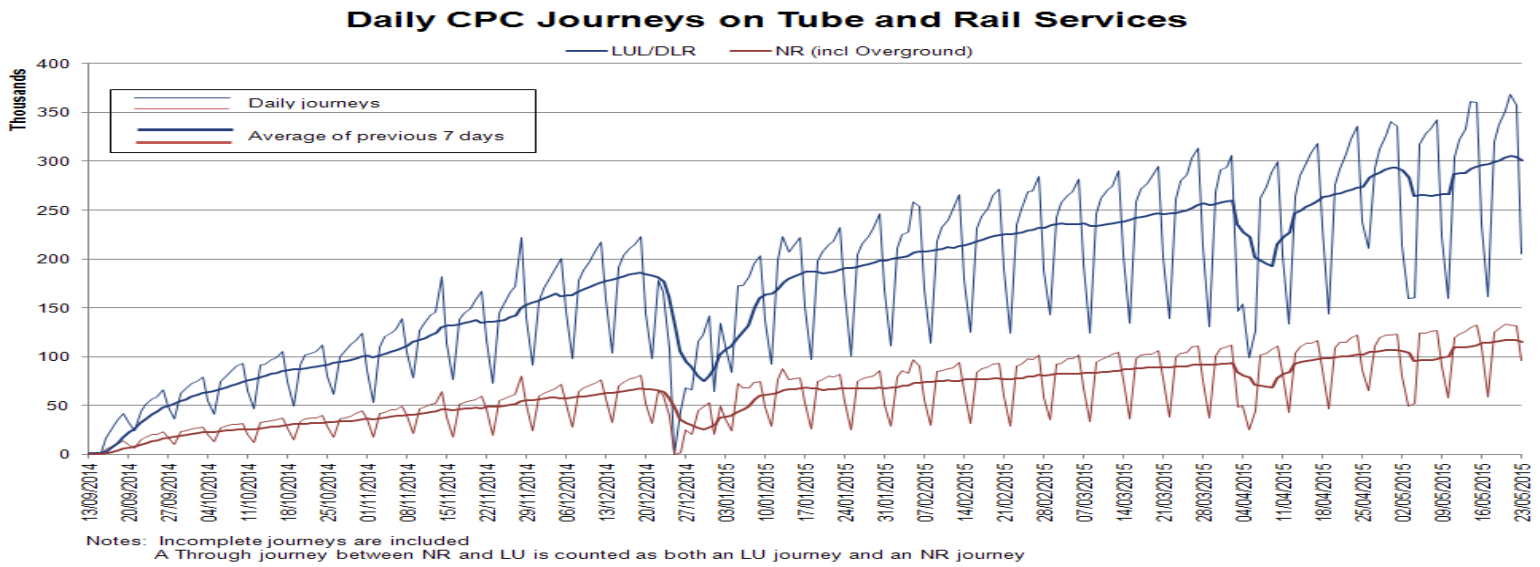
Vincoli:

- **Rientro dagli investimenti se si riducono le spese per altri canali di vendita.**
- **Delibere Regionali e Comunali; modifiche tariffarie e implementazione.**
- **Delibera Regionale sulle modalità di controllo e sanzionamento.**
- **Business model a lungo termine.**

Il Case Study, i numeri

Il Business Case:

Londra: **300.000 viaggi al giorno vengono effettuati mediante carta Contactless (su circa 14M/viaggi/Giorno)**
Il 21% degli utilizzatori delle carte PAYG è passato al contactless



In Europa mediamente (fonte UE) i pagamenti elettronici sono utilizzati nel 40% delle transazioni complessive.
In Italia mediamente i pagamenti elettronici raggiungono il 13% del totale.

Come incentivare l'utilizzo ?

Perché quindi usare un pagamento contacless? Come incentivare l'utilizzo di questo canale innovativo ?

I possibili driver importabili dall'esperienza di Londra secondo una indagine sui clienti che utilizzano la carta contactless sono:

Convenienza di utilizzo 50%	Una sola carta 16%	Facile utilizzo 15%	Ho dimenticato la mia carta. (Oyster) 9%

A Londra usare la contactless è più economico, ad esempio il costo del biglietto addebitato è di £1.35 rispetto ai £2.30 di chi paga con contanti.

Necessità di un modello sostenibile con le possibili soluzioni percorribili.

Grazie per l'attenzione