

Club Italia: Le innovazioni tecnologiche nella bigliettazione
Torino, 5 Ottobre 2006

**“La bigliettazione elettronica di un sistema
metropolitano (Torino): la sicurezza delle
transazioni”**



Gruppo Torinese Trasporti



- ✓ 190 milioni di passeggeri per anno
- ✓ Fatturato 365 milioni di Euro
- ✓ 5.240 dipendenti
- ✓ 66 milioni km anno offerti
- ✓ 100 linee Urbane e suburbane di superficie di cui 8 tramviarie
- ✓ 1 linea Metropolitana
- ✓ 73 linee extraurbane
- ✓ 2 linee ferroviarie in concessione

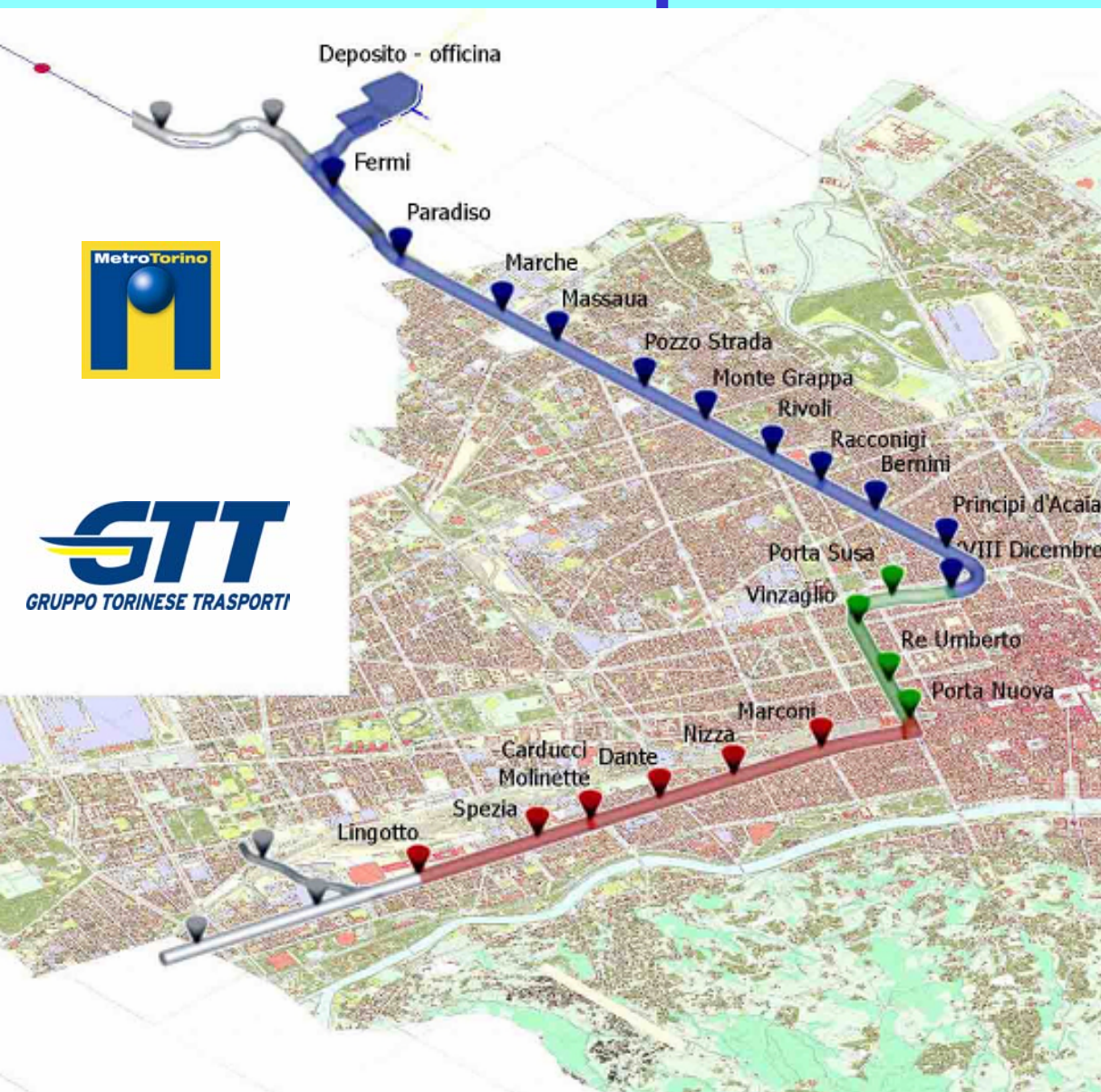


Febbraio 2006 : entra in esercizio la linea 1 della Metropolitana di Torino

Avvio del sistema di bigliettazione contactless



La Metropolitana di Torino

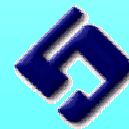


- Lunghezza della linea:
14.100 m

- Numero di passeggeri trasportati, all'ora per direzione:
15.000

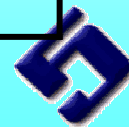
- Massima frequenza passaggi convogli:
1' e 10"

- Durata totale del percorso da Fermi a Lingotto:
24'



"Bigliettazione" nelle stazioni di Metropolitana

Ubicazione	n° Emittitrici Automatiche Biglietti	n° varchi normali	n° varchi per disabili
Fermi	2	9	1
Paradiso	2	9	1
Marche	2	9	1
Massaua	2	9	1
Pozzo Strada	2	9	1
Montegrappa	2	9	1
Rivoli	2	9	1
Racconigi	2	9	1
Bernini	2	9	1
Principi D'Acaia	2	9	1
XVIII Dicembre	2	14	1
Totale	22	104	11



Controllo Accessi : Linea di Tornelli a Flap



Altezza Flap: 120 cm



Emettitrici e Info Point



Una banchina in stazione



Passeggeri trasportati 30.000 / gg - Totale mese di settembre 890.000



Bigliettazione a Torino

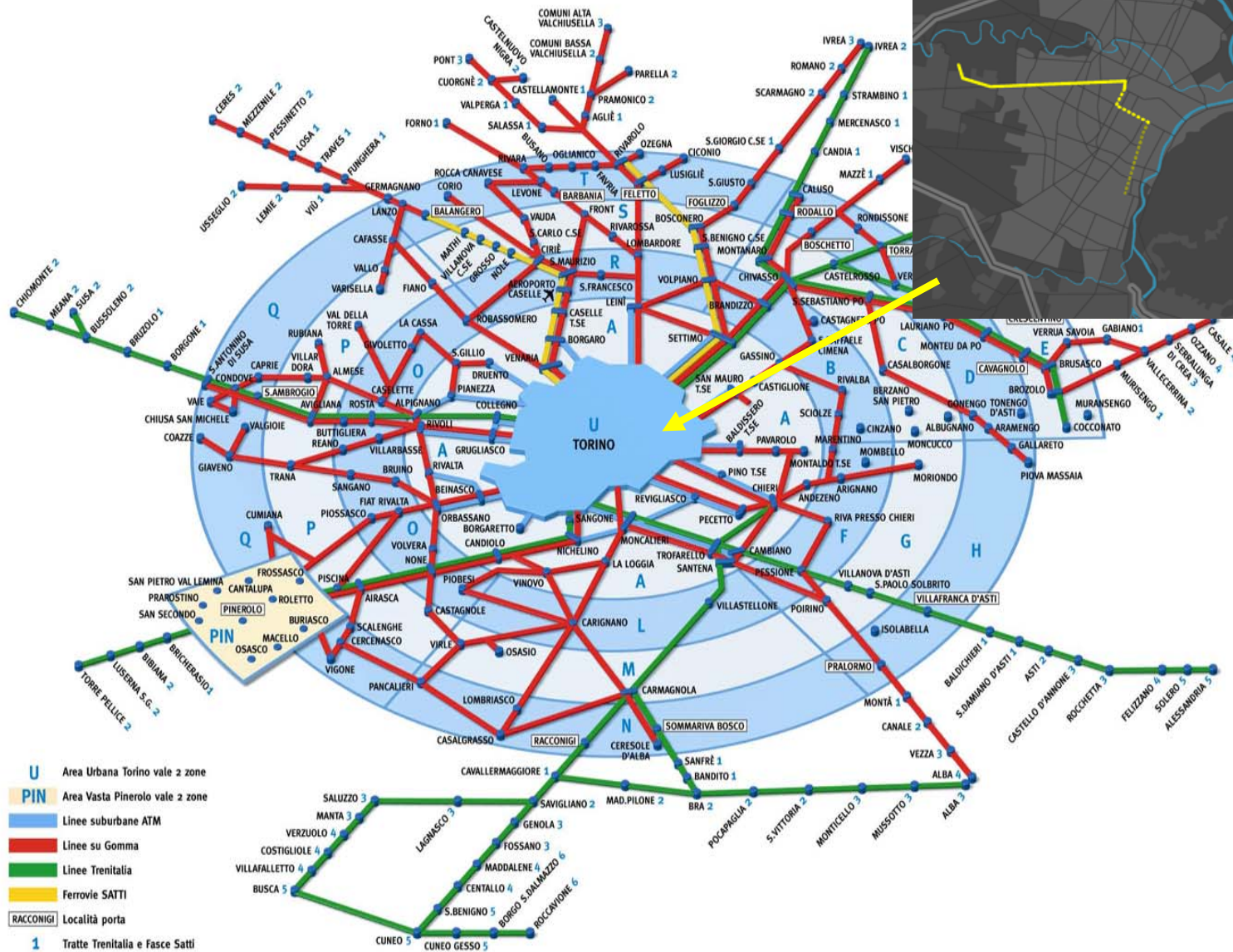
Dal 1996 vige per gli abbonamenti il sistema di integrazione tariffaria a zone denominato "FORMULA", nato dall'intesa tra Regione Piemonte, Provincia di Torino, Comune di Torino, ATM, SATTI, FS (oggi TRENITALIA). A partire dal 18 Novembre 2002 Formula è stato allargato con l'ingresso di 27 soggetti privati.

L'area integrata comprende Torino e l'area metropolitana estesa per circa 40 chilometri di raggio, articolata in aree concentriche suddivise in 18 zone. Il sistema di bigliettazione a Torino ed in Piemonte è stato cartaceo fino a Febbraio 2006. Ora, mentre in Metro è stata avviata la bigliettazione elettronica, in superficie è ancora cartaceo ma con banda magnetica per permettere l'ingresso in Metropolitana.



Area Formula

Percorso della Metro Nel contesto Urbano



Introduzione del contactless a Torino garantendo compatibilità tra Metro e superficie

- ***Sostituzione*** dei biglietti cartacei per la corsa singola e parte degli abbonamenti (mensile, settimanale) con biglietti cartacei/magnetici mantenendo la stessa dimensione (43mm) adatta alle obliteratorici tradizionali ancora in uso su bus e tram
- ***Sostituzione degli abbonamenti cartacei con la*** carta elettronica contactless per gli abbonamenti plurimensili e annuali studenti, annuali anziani; rimangono cartacei gli altri abbonamenti annuali, abbinati ad un biglietto Chip on Paper per l'accesso alla Metropolitana
- ***Introduzione*** del Chip on Paper (43 mm) per gli abbonamenti mensili



Esempi di nuovi titoli di viaggio elettronici

- Abbonamento annuale e plurimensile studenti e anziani Urbano e Suburbano Formula: 65.000 carte
- Abbonamento annuale ordinario personale e impersonale (Formula U + Formula Integrato) 15.000 Chip on paper
- Mensile Urbano Formula Biglietto magnetico



Tecnologia adottata

- Carte a microchip:

Modello: CT-4002 Tango ISO 14443 B - Torino Mapping

Struttura : 2 GTML2 che condividono alcune aree comuni

Numero contratti : 8, gestibili in due sezioni diverse della carta 4 + 4.

Ogni sezione può essere gestita con SAM diverse

Applicazione Calypso



- Chip on Paper :

Modello: CTS - 256

- Bigletti magnetici :

Formato fisico: 43 x 95 mm in cartoncino da 235 g/mq

Banda magnetica laterale

Magnetizzazione 2750 oe con densità di 75 bpi

Ologramma antifalsificazione proprietario



Foto 1



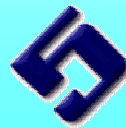
Foto 2



Come vengono ricaricate le carte contacless per gli abbonamenti plurimensili e annuali

Per la ricarica degli abbonamenti plurimensili e annuali contacless si è proceduto come segue:

- Spedizione a casa degli abbonati di istruzioni adeguate e di bollettini postali per il pagamento della ricarica presso Poste Italiane (come avveniva gli anni scorsi)
- Gestione automatica del ritorno sui pagamenti da Poste Italiane e creazione di una lista bianca da propagare presso i punti di ricarica fisica delle carte
- Creazione di punti di ricarica presso gli uffici alla clientela e tutte le TVM (emettitrici automatiche) posizionate presso le fermate del Metro. Le postazioni riconoscono automaticamente le carte per le quali è stato effettuato il pagamento e provvedono a rinnovare i periodi di validità sulla carta



La sicurezza in Metropolitana

La sicurezza è posta alla base della concezione della Metropolitana di Torino. La sicurezza sui dati è da intendersi in termini di: **riservatezza, integrità e disponibilità**.

La Metropolitana opera in ambienti chiusi dove incidenti e molestie possono assumere maggior gravità, rendendo più critica la sicurezza dei dati che servono a prevenirli e gestirli.

Due gruppi di dati: sistema e videosorveglianza.

Nel primo caso ci si riferisce ai dati di *controllo dell'esercizio* e nel secondo alle *immagini* riprese in stazione, a bordo, in galleria, in comprensorio tecnico e volte alla tutela contro incidenti e molestie. *L'architettura* informativa prevede zone logiche distinte di trattamento dati, ridondanze hardware, meccanismi di autenticazione (per es. le immagini TV dai treni su rete Wi-Fi sono cifrate e firmate) presenza di firewall

Metropolitana: Sala PCC Posto di Comando e Controllo



fotografia di Michele D'Ottavio

Metropolitana: Sala Security



Metropolitana: sicurezza dei passeggeri

- In caso di necessità l'operatore della Sala Security/PCC prende il controllo e gestisce le situazioni da remoto. Il sistema di videosorveglianza permette all'operatore di rendere più efficace e preciso il proprio intervento.
- La presenza di un sistema video sui treni aumenta la percezione di sicurezza nei passeggeri.
- La trasmissione delle immagini dalle vetture in movimento alla Sala Security avviene con un innovativo sistema radio basato su tecnologia wi-fi.
- Si tratta di una delle prime realizzazioni in Europa e nel mondo



Monitoraggio delle stazioni e dei treni



Condizioni per garantire una buona sicurezza del sistema di bigliettazione

- Alla convalida, bisogna garantire che il titolo di trasporto presentato dal viaggiatore sia *autentico*.
- I sistemi di ricarica devono essere tenuti sotto *controllo*, bisogna cioè impedire che si possa creare un titolo di trasporto autentico in una carta, senza che l'operatore riceva la controparte finanziaria.
- In caso di problema, bisogna disporre di mezzi di *individuazione e di correzione della frode*.

Politica di sicurezza nella bigliettazione: cifratura e moduli 'SAM'

Necessità di autorizzare l'accesso alla rete esclusivamente ai titoli *autentici*:

→ GTT utilizza chiavi di cifratura memorizzate in una zona della memoria inaccessibile dall'esterno. Le chiavi risiedono nella smartcard e nel modulo di sicurezza (SAM). La loro implementazione è conforme a quanto previsto dalla tecnologia *Calyspo*

Necessità di *gestire* correttamente *le chiavi* segrete dei moduli SAM per tutelare la sicurezza del sistema garantendone la corretta disponibilità

→ sorveglianza a posteriori delle ricariche, confrontando i titoli venduti ed i titoli visti dai terminali di convalida : *al momento alcune verifiche sono effettuate dal varco di accesso e altre manualmente*

→ far aggiungere da ogni modulo di sicurezza il proprio codice ai titoli che ricarica. Ciò permette di ritrovare sempre l'origine della vendita di un titolo e anche di impedire l'utilizzo di titoli di trasporto ricaricati tramite un modulo rubato: *tale implementazione sarà sviluppata nella fase di estensione del sistema all'interoperabilità regionale*

→ protezione software dei moduli SAM: GTT attua un controllo software di sessione, che prevede ogni volta la lettura di un codice di personalizzazione a sua volta cifrato

→ protezione fisica dei moduli SAM all'interno degli apparati: *attualmente in GTT i SAM di ricarica sono presenti solo in apparati presidiati o adeguatamente protetti.*

Esempi di frode tecnica

<i>Tipo di frode</i>	<i>Definizione</i>	<i>Individuazione</i>	<i>Reazione</i>
Creazione di una carta	Numero di carta che non dovrebbe esistere. Può far parte di un lotto rubato o difettoso.	Il sistema centrale di individuazione della frode può individuare la falsa carta confrontandola con l'elenco delle carte usate.	Iscrizione sulla lista nera. Invalidazione possibile della carta al momento della convalida.
Ricarica non autorizzata di una carta	Dei titoli di trasporto vengono caricati o modificati su delle carte in modo fraudolento.	Il sistema centrale di individuazione della frode può individuare la falsa carta confrontando i contratti venduti per questa carta e il contenuto visualizzato dal validatore.	Iscrizione sulla lista nera. Invalidazione possibile della carta al momento della convalida.
Clonazione di una carta	Copia del contenuto di una carta, comprese le chiavi segrete. I cloni possono essere creati partendo da carte rubate prima della personalizzazione o fabbricate dai frodatori. Pertanto il clone non ha obbligatoriamente la forma di una carta a microchip!	Più il numero di cloni è basso, più l'individuazione è difficile. È basata infatti sulla sorveglianza dell'attività delle carte. Una carta usata contemporaneamente in più luoghi è sospetta.	Iscrizione sulla lista nera. Se il numero riappare dopo l'invalidazione della carta, verrà di nuovo individuato e iscritto sulla lista nera.
Falsa carta con numero variabile	A partire dalla chiave principale di convalida è possibile ideare e realizzare una carta capace di cambiare numero ad ogni convalida, impedendone quindi l'iscrizione sulla lista nera.	L'individuazione dell'esistenza del problema è semplice: il sistema individuerà una carta il cui contenuto non è noto. Tuttavia sarà difficile identificare il raggio d'azione del problema e, in particolare, il numero di carte interessate. Dovrebbe invece essere possibile localizzare il luogo e il momento in cui queste carte si presentano al sistema. I portatori, infatti, hanno spesso abitudini regolari (ad esempio, ora e stazione d'ingresso).	Ad esempio, è possibile filmare le operazioni di convalida per individuare i potenziali frodatori. Una volta localizzata l'ora e il luogo della frode, occorre chiedere l'intervento di squadre di controllo e/o di polizia per effettuare un controllo sistematico delle carte o per trovare i portatori identificati. .

Politica di sicurezza: diversificazione delle 'SAM'

GTT utilizza moduli SAM con chiavi diverse in funzione dell'apparato sul quale sono installate:

<i>Tipo di chiave</i>	<i>Azioni sottoposte alla chiave</i>	<i>Tipo di apparato</i>
Convalida	Chiave di addebito utilizzata durante la convalida per verificare l'autenticità della carta, modificare eventualmente dei contatori e registrare l'evento.	Validatori
Ricarica	Chiave di ricarica dei titoli di trasporto. Autentica il terminale di ricarica al fine di impedire una ricarica fraudolenta	Terminali di ricarica da banco, emettitrici automatiche
Emissione	Chiave che controlla la scrittura delle informazioni generali (identificatore della rete di trasporto per esempio) e delle altre chiavi dell'applicazione	Terminali di emissione e modifica carte (uffici)

Regole di gestione della sicurezza previste dal progetto a scala regionale

Le seguenti regole sono applicabili a tutte le carte interoperabili:

- Le carte e i moduli di sicurezza contengono le *chiavi* segrete di bigliettazione della regione e non le visualizzano mai in forma non cifrata
- Le *chiavi* segrete per la bigliettazione sono *diversificate* nelle carte
- Tutte le operazioni di acquisto e di convalida vengono 'verificate' crittograficamente mediante un algoritmo crittografico basato sullo standard "DES".
- Le carte devono possedere almeno *tre livelli* di chiavi: personalizzazione, ricarica, convalida. Le chiavi di *ricarica* e di *convalida* saranno *comuni a tutta la regione* Piemonte.
- I SAM che contengono le chiavi di vendita sono protetti contro il furto e il loro numero massimo di *utilizzazioni* per la vendita è limitato.
- I SAM di gestione delle carte hanno almeno le seguenti caratteristiche:

<i>SAM di</i>	<i>Limite d'uso</i>
Convalida	Non contiene le chiavi di ricarica e di personalizzazione.
Ricarica	Non contiene le chiavi di personalizzazione. La chiave di ricarica è limitata a qualche giorno d'uso o numero di operazioni.
Personalizzazione	Non può trasferire le chiavi nelle carte.
Prepersonalizzazione	Non può trasferire le chiavi principali verso altri SAM.

Regole di gestione della sicurezza previste dal progetto a scala regionale

- Gli operatori che desiderano fabbricare i propri moduli di sicurezza devono impegnarsi a rispettare la Politica di Sicurezza definita per le procedure *organizzative di gestione* e per le operazioni di *creazione* dei SAM.
- Alcuni *dati* relativi all'*emissione* delle carte interoperabili, alla *vendita* dei titoli e alla loro convalida devono essere *trasmessi ad un sistema centrale* di individuazione della frode.
- Delle chiavi e dei SAM di test dovranno essere disponibili per lo sviluppo e la manutenzione dei prodotti. Le chiavi e i SAM di test non sono quelle usate in esercizio.

*Grazie
per l'attenzione*

5T Srl:

<http://www.5t.torino.it>

GTT SpA:

<http://comune.torino.it/gtt>

agrillo.m@gtt.to.it

