COMUNE DI GENOVA

UNIONE EUROPEA
Fondo Sociale Europeo
Fondo Europeo di Sviluppo Regionale

Agenzia per la Coesione Territoriale

PON GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020

# PROGETTO SIBIT

# STANDARD ITALIANO BIGLIETTAZIONE TRASPORTI

## 4.7 EVOLUZIONE della BUONA PRATICA

TECNOLOGIE TELEMATICHE TRASPORTI TRAFFICO TORINO

5T S.R.L.
Via Bertola 34 — 10122 Torino (IT)
T +39 011 227 4101 / F +39 011 227 4201
info@5t.torino.it / direzione5t@legalmail.it
www.5t.torino.it
C.F. - P.IVA 06360270018
C.C.I.A.A. TORINO 2825/1992
CAP. SOCIALE € 100.000,00 i.v.

Liguria Digitale

Sede Legale:
Via E. Melen 77 - 16152 GENOVA
Tel. +39-01065451
info@liguriadigitale.it

# Sommario



In questo documento vengono descritte le evoluzioni per il sistema BIP Piemonte realizzate da Regione Piemonte e progettate da Regione Liguria.

# 1. Definizione di un CARD DATA MODEL localizzato sul contesto territoriale e interoperabile col gestore ferroviario.

**Card Data Model Trenitalia Liguria, principali differenze e aggiornamenti rispetto al formato BIP**

Il Card Data Model Trenitalia per il sistema Ligure ed il Card data model sono derivazioni diretta del card data Model BIP.
La principale differenza tra le carte BIP e le carte progettate per il sistema ligure risiede nella gestione delle fotografie associate alle Smart Card che non erano presenti nella Smart card BIP.
All'interno del tracciato della Smart Card si rende quindi necessario inserire uno spazio destinato alle fotografie digitali.

La massiccia diffusione degli smartphone NFC e – contemporaneamente al lancio di applicazione di carte *e-ticketing contactless* dedicate al trasporto pubblico - ha reso evidente la necessità di utilizzare immagini digitali (*ID Photo Files*) tali da rendere possibile da parte di un controllore l'identificazione del legittimo titolare del PO, laddove l'applicazione di *ticketing* contenga contratti non-trasferibili ad altri soggetti. (carte personali)

La gestione dell'ID Photo File del titolare del Portable Object (PO) presenta almeno 3 aspetti critici:

- Storage dell'immagine (dimensioni, formato);
- Prestazioni (nel contesto della transazione);
- Privacy: poiché la fotografia identificativa è considerata un dato personale, la questione della protezione del dato deve essere gestita in modo rigoroso.

La struttura degli ID Photo Files può essere inserita nel PO a 2 possibili livelli:

- In una applicazione a sé stante;
- All'interno di una applicazione esistente.

Un ID Photo è definita da 2 files:

- Un file contenente l'immagine (EF Picture Data), codificata secondo un formato standard (es. JPG o JPEG2000), protetta contro letture non autorizzate (opzionale);
- Un file (EF Picture Attributes) contenente le informazioni necessarie per utilizzare l'immagine (sistema di codifica, tipi di accesso consentiti, firma digitale…).

**Condivisione dei file**
Un'applicazione con ID Photo Files può essere installata in un PO:

- Standalone, oppure
- Assieme ad altre applicazioni di e-ticketing.

Nel secondo caso è possibile condividere gli ID Photo Files con le altre applicazioni, onde evitare duplicazioni.

Poiché le altre applicazioni devono esclusivamente leggere la fotografia, si raccomanda di utilizzare le regole di accesso illustrate nella tabella seguente, in modo che tutte le applicazioni abbiano le medesime condizioni di accesso (Calypso rev. 3.1).

| MF/DF/EF | Type | SFI | Rec Num | Rec Size | Group 0 Read Rehabilitate | Group 1 Update Invalidate | Group 2 Write Decrease | Group 3 Append Increase |
|---|---|---|---|---|---|---|---|---|
| DF: PICTURE (DF3) | **DF** | **-** | **-** | **-** | **N/A** | **N/A** | **N/A** | **N/A** |
| EF Picture Data | **Binary** | **Xxh** | **1** | **Var** | **Always** | **Never** | **Never** | **N/A** |
| EF Picture Attributes | **Linear** | **yyh** | **1** | **64** | **Always** | **Never** | **Never** | **N/A** |

**Tabella 1 - ID Photo Files (file structure – shared version, Calypso 3.1)**

**Gestione dell'accesso ai file**
Un'applicazione Calypso rende possibile 2 modalità di accesso sicuro alla fotografia:

- Cifratura e decifratura da parte del terminale
  - In questo caso i diritti di accesso a EF Picture Data permettono di leggere e scrivere SENZA cifratura: la confidenzialità è assicurata dal terminale, che cifra e decifra l'immagine usando l'algoritmo di crittografia simmetrica indicato in EF Picture Attributes e una chiave privata;
- Cifratura e decifratura da parte dell'applicazione
  - Questa opzione è disponibile solamente per le applicazioni Calypso 3.2.

# 2. Definizione di un modello architetturale adeguato ai diversi contesti territoriali

**Architettura logica di Smart Ticket Liguria**

Il modello architetturale scelto per la realtà del territorio ligure prende le mosse dalla esperienza piemontese cercando di calare il modello su un contesto territoriale più semplice (un numero inferiore di aziende) e su un canale di finanziamento esclusivamente regionale al 100%.

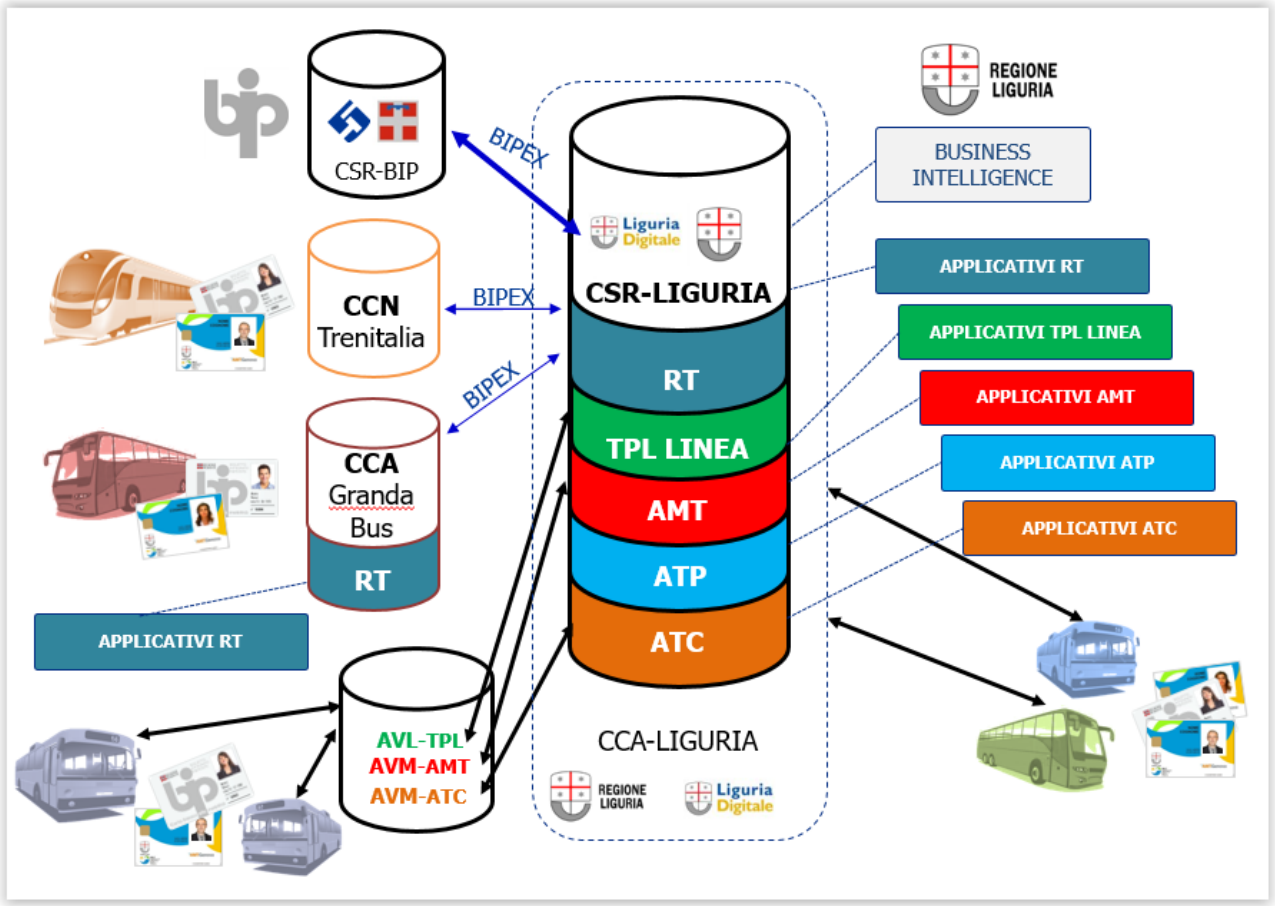
L'architettura prescelta per il progetto regionale ligure (denominato Smart Ticket Liguria) prevede la presenza di un unico Centro Servizi Regionale (CSR) a livello di territorio regionale e da più Centri di Controllo Aziendali (CCA) espressione delle Aziende TPL aderenti al progetto.

Il CSR ha il compito di gestire le funzionalità necessarie al corretto funzionamento di Smart Ticket Liguria e ha il ruolo di coordinatore dei processi regionali relativi al TPL della Liguria.
Il CSR deve essere in grado di garantire la coerenza e l'allineamento delle informazioni, provenienti dai CCA.
Ai CCA deve essere assicurata indipendenza operativa, anche nel caso di mancata e/o parziale attività da parte del CSR.
I CCA presiedono e gestiscono, in maniera integrata e organica e tra loro coordinata, le componenti progettuali operative in ogni singola Azienda e dei servizi di TPL e SBE ad essa associati.

Regione Liguria ha scelto di implementare il sistema Smart Ticket Liguria con un'architettura tale da garantire:

- Il ruolo e le funzioni degli enti pubblici locali;
- Il possesso dei dati;
- La supervisione dei sistemi;
- L'interoperabilità all'interno della Regione Liguria e di questa con le regioni limitrofe.

L'architettura è inoltre compatibile rispetto all'esigenza di realizzare un'integrazione gomma-ferro e conseguentemente garantire la partecipazione degli operatori ferroviari al sistema di bigliettazione elettronica regionale.
Abbiamo definito tale architettura un' "architettura centralizzata" in cui i sistemi centrali e la periferia risiedono nello stesso server rack.




La scelta dell'architettura centralizzata:

- Consente una più rapida ed efficace centralizzazione dei dati, soprattutto per quanto concerne l'azione di coordinamento e controllo degli Enti Regolatori;
- Assicura un ruolo centrale dei soggetti pubblici e il possesso di dati e sistemi da parte dell'Amministrazione regionale;
- Consente la realizzazione di un sistema facilmente scalabile per ospitare un'eventuale nuova azienda;
- Consente di contenere i costi connessi ad acquisti multipli di Sistemi, realizzando un solo sistema centrale.

Si elimina il passaggio dei dati tra i sistemi periferici dei singoli CCA istanziati presso le singole aziende TPL e i sistemi centrali che è probabilmente un punto di debolezza dei sistemi distribuiti, quale il sistema BIP Piemonte.

Tali CCA vengono superati dalla realizzazione di un singolo CCA a multi-partizione (*CCA-Liguria*), in grado di ospitare i dati e le funzionalità di ciascuna azienda TPL afferente al sistema.

Tale scelta architetturale è basata su una centralizzazione dei sistemi (CSR-Liguria e CCA-Liguria) presso il Data Center di Liguria Digitale, a garanzia:

- Del controllo dei sistemi da parte dei soggetti pubblici locali;
- Della continuità dei servizi pubblici erogati;
- Dell'interoperabilità dei PO sull'intero territorio regionale.

L'allineamento delle anagrafiche, delle *list* e delle altre funzionalità legate all'interoperabilità dei PO all'interno del sistema regionale sarà inoltre garantito dall' allineamento tra CSR-Liguria e le partizioni del CCA-Liguria.

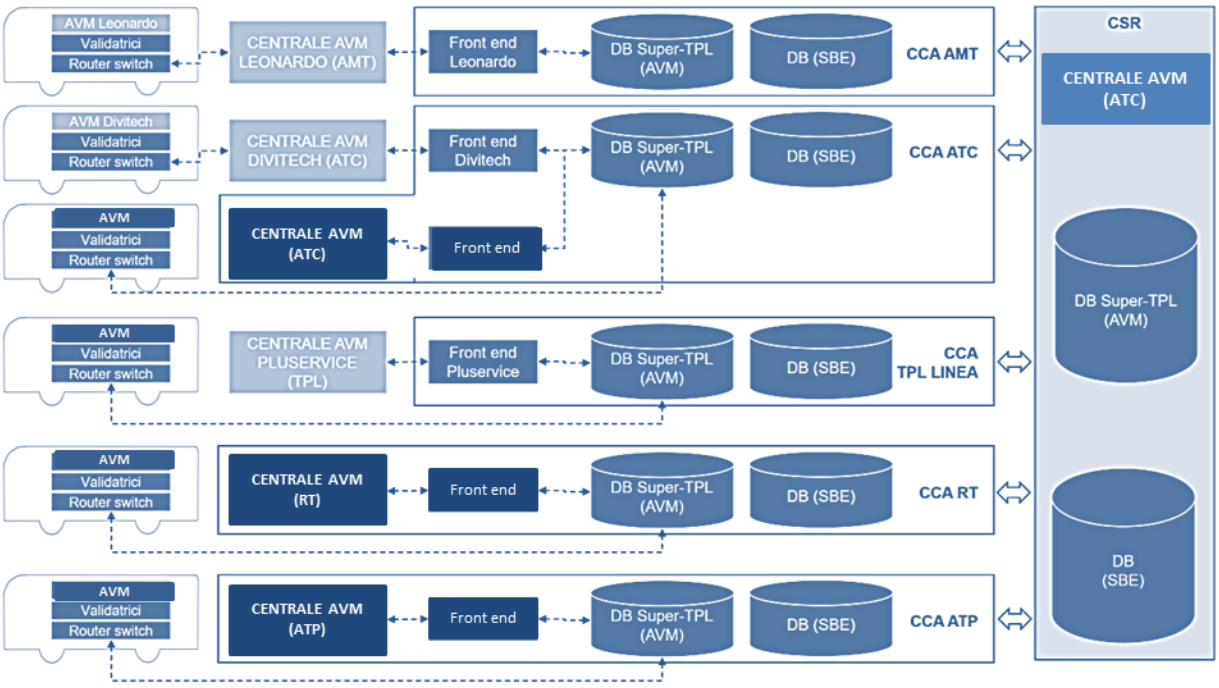
Nell'idea progettuale al CSR-Liguria spetteranno inoltre:

- L'interfacciamento (import-export di dati tramite protocollo BIPEx) da e verso il CCA di GrandaBus ed il CCN di Trenitalia – sistemi già in esercizio);
- Lo scambio dati e gli allineamenti con il sistema BIP tramite il CSR-BIP gestito da 5T per conto di Regione Piemonte;
- L'eventuale interfacciamento con il CSR di Regione Lombardia, il CSR della Toscana e del sistema *MI MUOVO* di Emilia Romagna.

Sarà quindi possibile garantire da subito l'interoperabilità tra i sistemi regionali piemontese e ligure, consentendo agli utenti di utilizzare gli stessi PO per muoversi sul territorio di entrambe le regioni.

# 3. Modelli Ibridi: Coesistenza di Sistemi AVM Esistenti – Sistemi AVM/SBE

Smart Ticket Liguria salvaguarderà i sottosistemi di monitoraggio TPL delle aziende, alla luce dell'esistenza in talune realtà (es. AMT Genova e ATC La Spezia) di Centrali Operative dotate di sistemi AVM moderni, adeguati alle esigenze di monitoraggio e controllo.
La necessità è quella di garantire l'integrazione di centrali AVM di marche eterogenee monitorate a livello superiore in un AVM regionale e in alcuni casi integrare i sistemi esistenti con il sistema richiesto al fornitore che si aggiudicherà la gara ligure (alla data di oggi non ancora aggiudicata).




Il CCA multi-partizione espone cinque CCA, una per ciascuna delle Compagnie aderenti al progetto Smart Ticket Liguria. In conseguenza, esse sono ovviamente simili tra loro dal punto di vista del SBE, mentre presentano rilevanti asimmetrie per la parte AVM.
La soluzione progettuale dovrà prevedere quindi (vedi figura):

▪ tutti i CCA posseggano la stessa parte SBE per la bigliettazione elettronica (unico sistema regionale);
▪ sia previsto il front end per le Compagnie AMT, ATC e TPL Linea che sono già equipaggiate con una centrale AVM propria;
▪ la sola ATC venga ad essere equipaggiata con doppia centrale AVM essendo i vecchi mezzi equipaggiati con AVM Divitech e collegati alla relativa centrale, mentre altri saranno dotati di nuovi apparati e collegati ad una nuova centrale oggetto di fornitura.

# 4. Definizione di un modello di BPO (Business Process Outsourcing) applicato ad un sistema di BE

Per Business Process OutSourcing si intende il subappalto di funzioni aziendali e processi a fornitori e gestori esterni.
Quando le aziende esternalizzano i processi aziendali, delegano le mansioni ed i compiti alle aziende specializzate.
Questi processi in passato erano gestiti da uffici e risorse interne.
Quando le esigenze del mercato sono aumentate, le aziende hanno iniziato a cercare modi per aumentare la flessibilità per essere competitivi e mantenere una posizione di rilievo nel mercato.
Una di queste strategie era di delegare attività secondarie in modo che potessero concentrarsi sulle loro competenze di base.
Regione Liguria ha inteso trasferire tutte le attività di installazione, manutenzione e conduzione sistemistica al fornitore aggiudicatario in regime di full service.
Lo scopo di questa scelta è isolare il committente dalle attività fornite in modo da separare le attività proprie della P.A. (controllo, indirizzo e regolazione) da quelle del mercato (sviluppo, esecuzione, *improvement* dei prodotti e reingegnerizzazione in corso di contratto)

**Sistema di bigliettazione Regione Liguria manutenzione decennale in regime di *full service* (ESTRATTO da CAPITOLATO Liguria)**

Nella fornitura del sistema di bigliettazione ligure si ricorre ad un regime di contratto “full service” che dovrà comprendere, oltre agli apparati oggetto dell’offerta, gli apparati della rete di comunicazione, il software necessario alla completa funzionalità del sistema (comprese le licenze d’uso dei sistemi operativi e degli applicativi), tutto il materiale e tutte le prestazioni direttamente e indirettamente necessarie a rendere il sistema perfettamente funzionante in conformità a quanto stabilito negli atti di gara.
In particolare si è immaginato che la manutenzione avesse carattere decennale e vertesse sui seguenti punti:

- La manutenzione preventiva, correttiva ed evolutiva in regime di full service per periodo minimo di 10 anni dal Collaudo provvisorio del sistema;

- La disponibilità delle parti di ricambio degli apparati del sistema deve essere assicurata per almeno 15 anni;
- Il mantenimento della compatibilità, del sistema sviluppato, all'evolversi dei software di base e dei Database;
- L'installazione di tutti gli apparati e la loro messa in servizio comprensiva della soggezione ai costi relativi alla connettività per un periodo minimo di 5 anni dal Collaudo definitivo del sistema;
- La conduzione sistemistico applicativa del sistema;

# 5. Sistemi ACCOUNT BASED: descrizione, concetti di base e realizzazioni semplificate

La progettazione di un nuovo sistema di bigliettazione elettronica non può oggigiorno ignorare la tendenza sempre più marcata verso i sistemi cosiddetti *account based* resi più semplici dalla disponibilità di sistemi in *cloud* e connessioni sempre più capaci.
AMT Genova per esempio ha lanciato fin dal 2017 una carta Mifare con logica AB che sebbene non sia inserita in un sistema completo di bigliettazione può essere ricaricata on line e in remoto da applicazione mobile per Smartphone, può essere de-materializzata su Smartphone ed ha costi di gestione notevolmente inferiori ad un sistema bastato su Smart card e SAM.La carta è oggi distribuita su tutti gli abbonati annuali ed è in corso di distribuzione anche per i mensili.

L'industria della bigliettazione elettronica -come detto -si sta muovendo verso la digitalizzazione delle applicazioni e dei servizi, ovvero verso sistemi di pagamento più flessibili e meno onerosi denominati *Account Based Ticketing* (ABT) System.
Gli operatori di TPL stanno cercando di offrire sistemi di pagamento/validazione che consentano al cliente di utilizzare strumenti che già possiede, come le Carte Bancarie contactless e gli Smartphone NFC, ma anche allo stesso tempo Biglietti con tecnologia QR Code e Carte Mifare ULC (Chip on Paper).
L'approvvigionamento del biglietto non costituirà più un problema per i clienti del sistema che possiedono questi devices.

Per raggiungere questo obiettivo serve:

- Un Sistema di pagamenti che sfrutti la potenzialità:
  - Dei circuiti bancari di pagamento (Europay, MasterCARD, VISA, AmEX etc);
  - Dei sistemi di Post Payment;
  - Dei sistemi di calcolo della cosiddetta tariffa "Best Fare".

***Account Based Ticketing***

In un sistema di bigliettazione tradizionale "card centrico", i supporti tecnologici ("media") distribuiti ai clienti svolgono quattro ruoli chiave:

1. Identificare il titolare del supporto quando questo non è anonimo (es. dati del "titolare" registrati elettricamente e stampati sul supporto);
2. Proteggere le operazioni di vendita e convalida garantendo l'autenticità del supporto (utilizzo di chiavi sicure in moduli SAM);
3. Ospitare i titoli di viaggio (sono registrati sui supporti);
4. Registrare l'utilizzo di un titolo di viaggio (convalida).

Con lo sviluppo delle varie tecnologie di scambio dati (Ethernet, Wi-Fi, 3G / 4G connesso a un servizio Internet universale a banda larga), è possibile creare un sistema di ticketing in cui ogni apparecchiatura di bigliettazione ha un collegamento diretto con il sistema centrale per scambiare dati quasi in tempo reale. Questo consente di considerare lo sviluppo di sistemi di bigliettazione che implementino una modalità operativa incentrata sul server ("server centrico").
Con questa modalità operativa, i supporti di viaggio per i clienti mantengono i primi due ruoli condivisi dal sistema "card centrico":

- L'identificazione del titolare del supporto per eventuali “media” non anonimi;
- La securizzazione delle operazioni di vendita, convalida e controllo, garantendo l'autenticità dei supporti.

Al contrario, in un sistema "server centrico", i supporti di viaggio:

- Non ospitano più i titoli di viaggio, che continuano ad essere memorizzati nel sistema centrale, in un account, associato ai supporti;
- Non registrano più l'utilizzo dei titoli di viaggio (nessuna scrittura sul supporto durante la convalida).

I principali vantaggi di un sistema “server centrico” rispetto ad un sistema “card centrico” sono:

- Il superamento delle restrizioni relative al “media” (in particolare il numero e la dimensione dei dati che possono essere registrati allo scopo di descrivere un titolo di viaggio);
- La gestione e lo sviluppo dei “media” sono semplificati per gli enti organizzativi del sistema;
- Agli utenti viene fornita un'offerta di servizi più efficace, comprensiva della vendita a distanza.

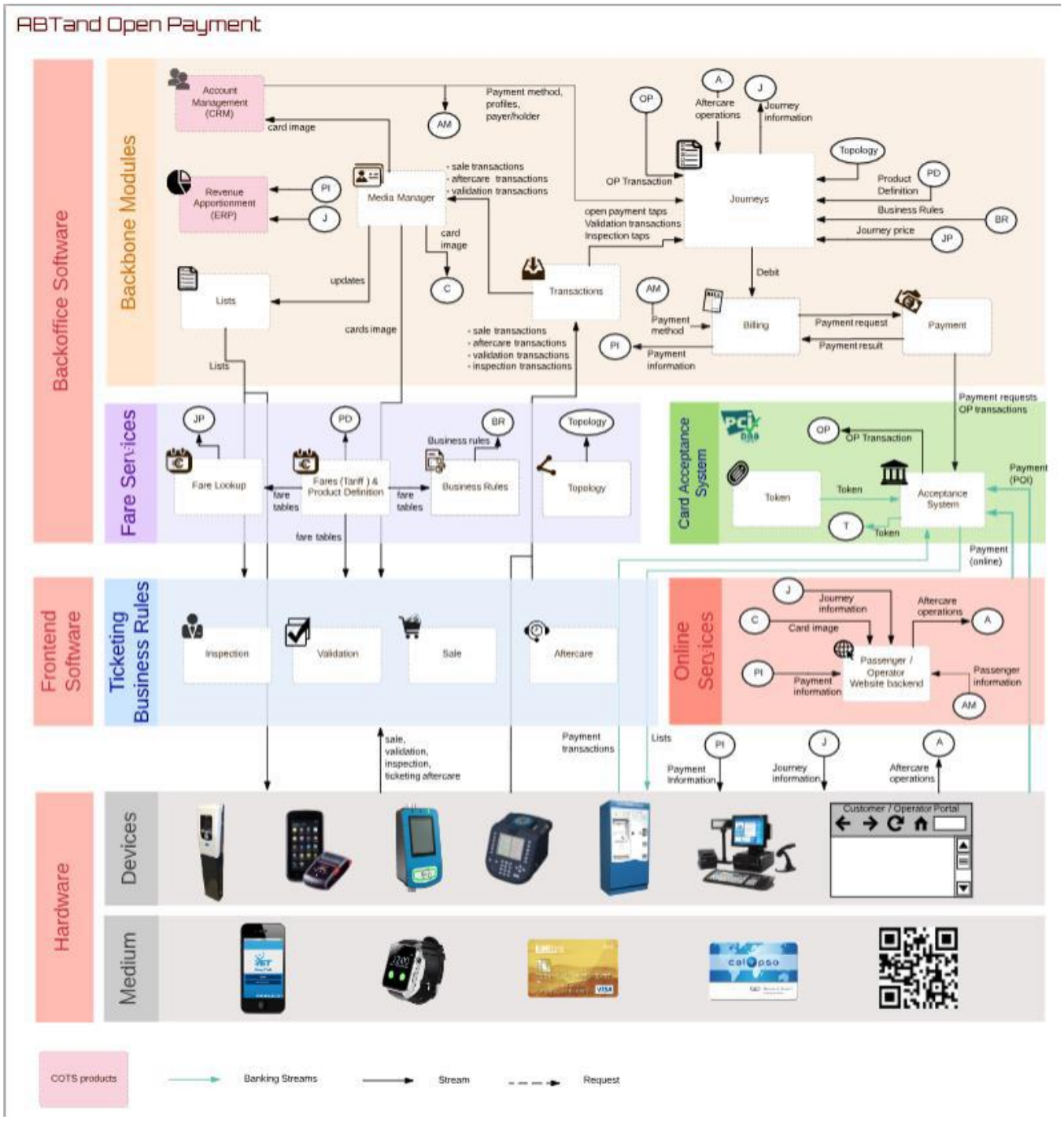
Qualsiasi utente che aggiunge credito al proprio account, può "immediatamente" ottenere un titolo di viaggio, senza dover attendere che un biglietto venga distribuito in remoto ai propri supporti.

Tuttavia, è necessario che la soluzione "server centrica" fornisca almeno lo stesso livello di servizio di un sistema "card centrico" nelle aree in cui quest'ultimo è efficace, compresa la velocità delle operazioni di vendita, convalida e controllo.

Architettura funzionale

Il sistema ABT è suddiviso in una serie di moduli funzionali, ciascuno dei quali è costituito da uno o più micro-servizi.

L'architettura funzionale del sistema è mostrata nella Figura seguente.




***Account***

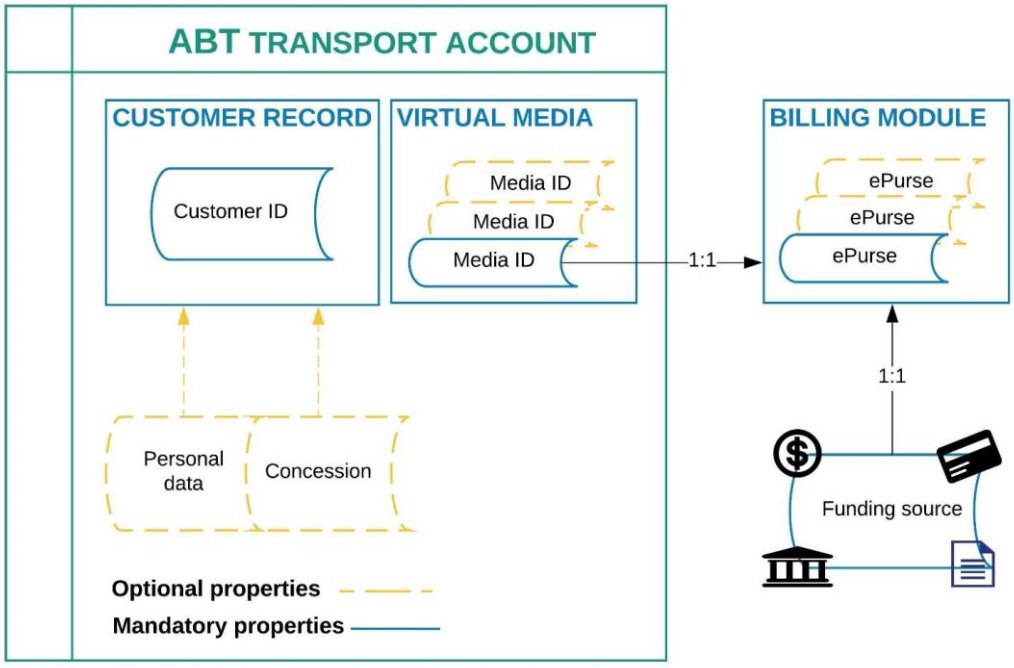
Ogni cliente crea un account sul sistema ABT quando utilizza per la prima volta il sistema oppure eseguendo manualmente la procedura online o in un punto vendita abilitato.

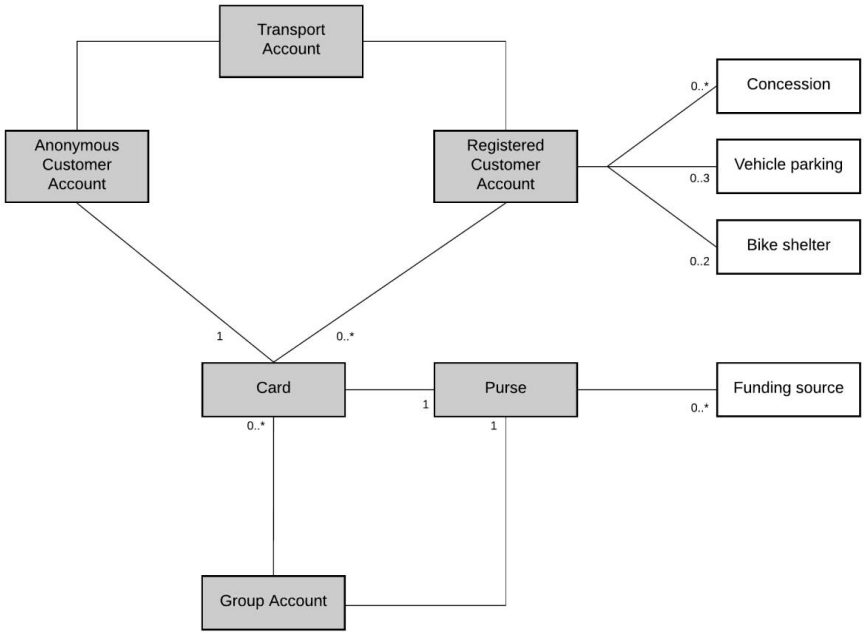
I comuni denominatori per tutti i supporti tecnologici basati su sistemi account based sono:

- ID cliente - Un ID cliente assegnato in modo casuale viene creato nel database e associato al supporto tecnologico quando questo viene registrato nel sistema per la prima volta.

L'operazione può avvenire ad esempio in un punto vendita autorizzato o in un dispositivo che distribuisce le carte.

- Media ID - Questo è l'ID univoco preso dal supporto quando la carta viene "letta" per la prima volta da un dispositivo non presidiato come un ETM, TVM o in un punto vendita utilizzando un POS.
- Media Manager - Memorizza i supporti associati all'account.
- ePurse - Fornisce il meccanismo attraverso il quale vengono pagati i titoli di viaggio. Da un punto di vista tecnico, il borsellino elettronico (ePurse) è direttamente associato al supporto tecnologico assegnato a un determinato account. L'ePurse deve disporre di un meccanismo di finanziamento associato.






**Esistono due tipi principali di account ABT che possono essere creati:**

- Anonimo: Un cliente non ha bisogno di registrarsi per viaggiare con una smart card appena acquisita. A condizione che il "media" sia stato reciprocamente autenticato dal dispositivo come valido per il sistema di trasporto e l'account associato ad esso sia precaricato con credito sufficiente.
  Il cliente può utilizzarlo per effettuare il check in/check out sul veicolo e il suo titolo di viaggio verrà aggiunto a un account associato al token di viaggio.
  In un account anonimo nessun dato personale è conservato sui supporti o nel back office. L'account viene creato nel back office con un ID casuale e l'ID smart media viene associato all'account. Il cliente può ricaricare l'account senza dover registrare i propri dati personali.

- Registrato: Gli utenti registrati sono quelli che hanno inserito i propri dati personali attraverso il portale clienti. Registrandosi vengono garantite funzionalità avanzate, come ad esempio maggiori informazioni sui dettagli di viaggio, notifiche e possibilità di registrare i familiari a carico.
  In questa modalità il "media" può essere anonimo o personalizzato a seconda di chi lo ha emesso. Ad esempio, le carte emesse e personalizzate da terze parti possono essere accettate dal sistema e utilizzate per i viaggi, ma il cliente rimarrà anonimo al sistema fino a quando non creerà un account registrato. Inoltre, un "media" registrato può essere utilizzato solo dal suo proprietario. A questo tipo di account possono essere associati più supporti, ma una carta può essere associata a un solo account registrato alla volta.

***Supporti tecnologici***

Smart media: è un token fisico di proprietà del cliente che è per lui univoco e che contiene un ID univoco che non cambia ogni volta che esso viene utilizzato. In genere si tratta di una smart card, ma è possibile utilizzare altri dispositivi smart.
**Smart Device**: con il sistema di bigliettazione account based viene generato un singolo "Token" univoco dai “media”, da collegare con l'account nel back office. Il meccanismo di convalida controlla la presenza del "token" in una "lista di azioni" per verificare se il dispositivo è vietato o autorizzato per il viaggio successivo. Tutte le altre funzioni vengono eseguite all'interno del server Cloud in back office.

Dispositivo mobile: A causa del fatto che la maggior parte dei dispositivi mobili cambia l'ID (token) ogni volta che vengono utilizzati (tipicamente NFC), essi devono essere impiegati con le app per i pagamenti di GooglePay ,SamsungPay, ApplePay, etc.

## Rinnovo supporti

Il portale clienti crea un avviso prima che venga raggiunta la data di scadenza della carta in modo che il cliente possa richiederne una sostituzione. Quando una carta scade, viene automaticamente aggiunta alla lista negativa. Il cliente acquista una nuova carta da un TVM e la registra su un account web esistente o direttamente in un punto vendita aziendale. La nuova carta dà accesso ai diritti di viaggio esistenti, che sono memorizzati per ogni account nel “Media Manager”, per cui avviene un trasferimento di valore dalla carta in scadenza a quella nuova.

Il processo di rinnovo di un supporto associato a un account anonimo può avvenire anche in presenza del cliente con il proprio “media”:

- L'operatore del terminale POS legge il “media” da rinnovare per recuperare l'ID Media e richiede quindi il rinnovo del supporto;
- Se non è ancora scaduto, il supporto da rinnovare viene aggiunto alla lista negativa dei “media”;
- L'operatore registra un nuovo supporto sull'account e lo consegna al titolare.

## Borsellino elettronico e opzioni di pagamento

Il sistema offre al cliente vari modi per finanziare il borsellino elettronico (ePurse) associato alla sua smart card / supporto.
Un ePurse conserva una quantità finanziaria di titoli di viaggio per un titolare di account. L'ePurse è conservato nel back office per conto di una specifica carta e viene utilizzato per fornire finanziamenti per i viaggi da una determinata fonte di finanziamento. Il cliente aggiunge valore all’ePurse per il pagamento del biglietto, prima del viaggio. Nella modalità prepagata, le tariffe vengono aggregate e addebitate da ePurse durante il viaggio del cliente. Le regole aziendali vengono applicate dinamicamente durante la giornata, al fine di ottenere la tariffa più conveniente.

Il sistema consente inoltre a un operatore del sistema, in possesso dell'autorizzazione appropriata, di regolare un saldo ePurse (ovvero, accreditare o addebitare manualmente un borsellino). Questa funzione è basata sulle attestazioni di autorizzazione.
In uno scenario di pagamento posticipato, il cliente registra un metodo di pagamento, ad esempio carta di credito/debito o addebito diretto (SEPA) sul proprio conto corrente. Il pagamento non avviene alla data di effettuazione del viaggio e l'operatore di trasporto può definire quando il pagamento verrà effettuato, ad esempio mensilmente tramite addebito diretto oppure generare una fattura per un account aziendale.
Un addebito diretto può essere associato solo a un account di trasporto registrato. In questo scenario il cliente utilizza una smart card (o un altro smart token) per viaggiare, ma garantisce il pagamento impostando sul suo account l'addebito diretto. Il valore addebitato alla fine del mese risulta dal calcolo dei viaggi effettuati durante il periodo, a seguito dell'applicazione delle regole aziendali con l'obiettivo di applicare sempre la tariffa migliore.

Il recupero automatico del debito non può essere effettuato con le smart card ABT allo stesso modo di come avviene per gli Open Payments. Un metodo di addebito diretto tende ad essere migliore, in quanto riduce il rischio. Se una successiva richiesta di pagamento viene rifiutata più del numero di tentativi configurato o non viene effettuato il pagamento entro il periodo di tempo configurabile, qualsiasi smart media associato all'account viene aggiunto alla lista negativa, per impedire ulteriori viaggi. L'operatore deve contattare il cliente per recuperare il debito tramite altri metodi di pagamento.

l cliente può scegliere di caricare automaticamente ePurse per assicurarsi che non si esaurisca il credito. Solo gli account registrati beneficiano del credito e della funzionalità di caricamento automatico. Il cliente seleziona un livello al quale attivare una ricarica e l'importo della ricarica stessa. Quando il saldo dell'account raggiunge questo livello, viene effettuata una richiesta di pagamento utilizzando il metodo di pagamento scelto ed il saldo del borsellino viene aggiornato.

I caricamenti automatici per essere configurati e abilitati richiedono una carta bancaria o un altro metodo di pagamento automatico (es. Paypal). Il credito non viene aggiunto a ePurse finché il pagamento non è stato approvato. Il cliente o l'amministratore dell'account di gruppo possono anche aggiungere, rimuovere, modificare le fonti di finanziamento associate alla funzionalità di caricamento automatico; sospendere e riattivare i pagamenti come richiesto.

Nel caso in cui la richiesta di pagamento venga rifiutata, il sistema:

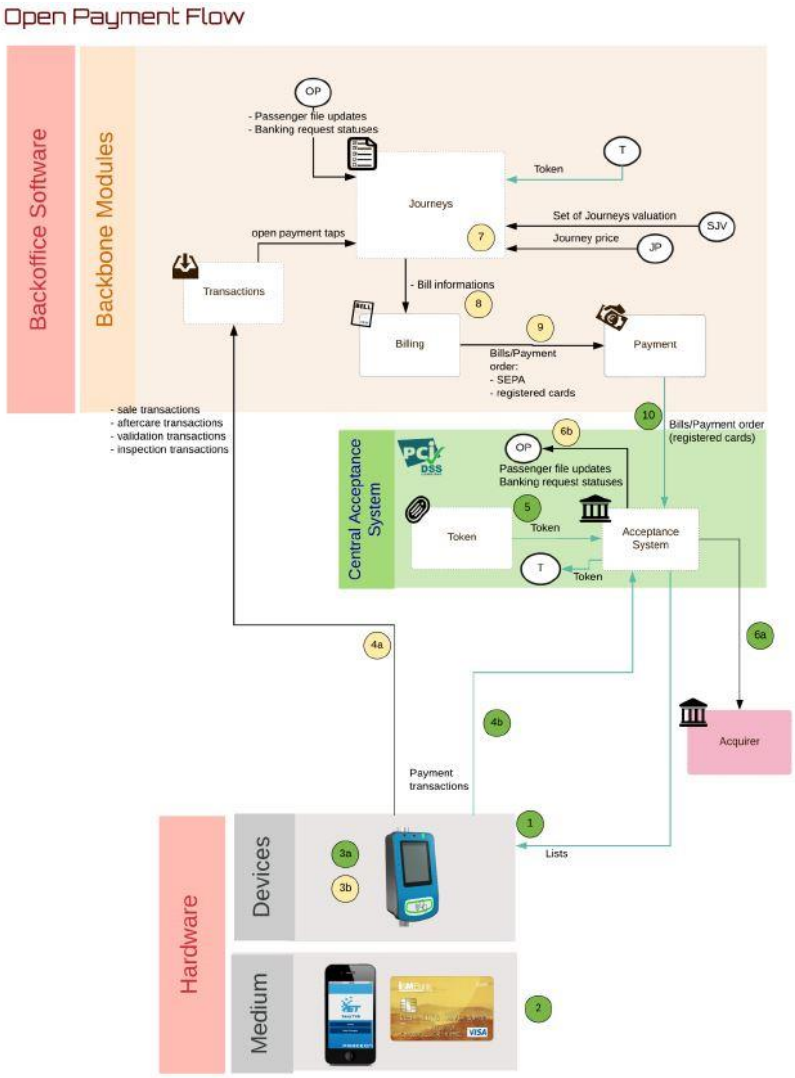
- Aggiunge lo smart media alla lista negativa;
- Invia una notifica al cliente registrato per informarlo che la sua funzione di caricamento automatico è stata annullata;

***Open payments***

Per Open Payment si intende la possibilità per un cliente del servizio di Trasporto Pubblico di utiizzare la propria carta di credito contactless.
I clienti possono utilizzare carte contactless EMV Visa, MasterCard, American Express, Diners Club (inclusi portafogli mobili o altri metodi abilitati conformi a EMV quali carte loyalty o fidelity) per i viaggi. In questo caso, il cliente non deve necessariamente registrarsi nel sistema, sebbene la registrazione fornisca ulteriori rapporti e notifiche.
Il cliente arriva al punto di partenza del viaggio e presenta la carta EMV C-less (passandola sul validatore).
Il meccanismo di convalida controlla se la carta è valida, eseguendo un controllo locale della carta (Offline Data Authentication - ODA e controllo del numero BIN) seguito da una verifica della data di scadenza e delle liste di blocco (Deny list + Hotlist).
Nel caso la carta fosse presente nelle liste di blocco, viene impedito al cliente di salire a bordo del mezzo. La Deny list identifica che se carta è stata precedentemente rifiutata durante l'esecuzione di un'autorizzazione o durante il tentativo di prelevare un pagamento da essa (ad esempio fondi insufficienti).
La Hotlist fornita dall'Acquirer (se disponibile) identifica se la carta è bloccata dall'emittente (rubata, smarrita, fraudolenta), in questi casi al cliente viene impedito di viaggiare a meno che egli non paghi con altri mezzi o rimuova sé stesso dalla lista negativa, ottenendo un'autorizzazione positiva.
La stessa carta o dispositivo deve essere utilizzata per tutti i viaggi al fine di garantire l'applicazione dei limiti della tariffa massima attuabile. Questo perché i viaggi sono collegati a uno specifico "token" che è legato a un account.
Il token varia tra carte e dispositivi mobili con app di pagamento come Apple Pay, Google Pay o Samsung Pay, quindi ci sarebbe un account per una carta bancaria (PAN) e un account per un dispositivo mobile (dPAN).
Se la carta sta per scadere ed è stata già emessa una nuova carta, la carta sostitutiva non può essere utilizzata fino all'inizio del nuovo periodo di calcolo della tariffa, al fine di mantenere i vantaggi maturati fino a quel momento.
Questo vale sia per gli account anonimi che per quelli registrati. Negli Open Payments ogni tipo di token (es. carta fisica - fPAN o portafoglio mobile - dPAN) creerà un account anonimo univoco. Questo perché i token generati per i diversi dispositivi sono differenti.
Dove non è presente un validatore all'uscita sul veicolo, viene inviata dal lettore di pagamento al back office una tariffa fissa o una tariffa avviata dal conducente. Questa tariffa viene inviata solo come parte del messaggio di "tap", ma non viene eseguita alcuna transazione finanziaria con la carta.
Supponendo che la carta sia accettata dal sistema in ingresso, se è presente il validatore anche all'uscita del mezzo, il cliente provvede a passare sul lettore nuovamente la sua carta

cEMV. Il sistema calcola la tariffa in base ai "tap" del viaggio applicando le regole aziendali e addebitando a fine giornata la tariffa migliore.

**Flusso transazioni Open Payment**




<u>Quando un cliente utilizza una carta Open Payments, il processo è il seguente:</u>

1. Il validatore scarica regolarmente l'aggiornamento con le modifiche della "Deny list" dal sistema di accettazione della carta, generalmente ogni 15 minuti.
2. Il cliente presenta (effettua il "tap") la sua carta Open Payment.
3. Il validatore elabora la transazione e:
   a) Legge attraverso il lettore contactless i dati bancari della carta, eseguendo un ODA;
   b) Autentica il "media" contactless (verifica che non sia contraffatto);

c) Verifica se il Token PAN appartiene alla Deny list. Il dispositivo di validazione genera un ID univoco di transazione per questo livello. Tale ID viene inviato a entrambi i sistemi (bigliettazione e accettazione della carta).
d) Genera una transazione “tap di viaggio” univoca come transazione ID (come per il punto 4a).

4. Vengono registrate due transazioni: l'interazione sicura (o transazione bancaria generata dall'applicazione bancaria) e la transazione di ticketing (generata dall'applicazione di bigliettazione). L'ID univoco di transazione è comune a entrambi i “tap” e viene utilizzato per collegarli al back office.
   a) Il “tap” del viaggio viene inviato al processore della transazione (ID transazione univoco, dati / ora, dettagli del viaggio, ecc.);
   b) La transazione di pagamento sicura al sistema di accettazione della carta (ID transazione univoco, data / ora, dati protetti EMV).
5. Sul sistema di accettazione della carta o il PAN è tokenizzato oppure viene utilizzato il token fornito nel messaggio. Ciò assicura che il sistema utilizzi il token e non il PAN, che è così garantito come da conformità PCI.
6. Il sistema di accettazione della carta esegue quindi una richiesta di autorizzazione (o informazione) con un importo definito dalle regole dello schema. Il risultato dell'autorizzazione (o delle informazioni) viene poi inviato al Modulo di viaggio. Se la richiesta di autorizzazione (o informazione) viene rifiutata, la Deny list viene aggiornata sul sistema di accettazione delle carte e il record corrispondente al cliente sul sistema di bigliettazione viene conseguentemente contrassegnato. Se la richiesta di autorizzazione (o informazione) viene accettata, il token associato viene inviato anche al server del sistema di bigliettazione per associarlo alla transazione di ticketing.
7. I viaggi effettuati dal cliente vengono aggregati nell'arco della giornata e viene applicato il limite tariffario massimo fissato dell’operatore di trasporto.
8. Alla fine del periodo viene generata una fattura e la richiesta di pagamento viene effettuata al modulo di pagamento.
9. Il modulo di pagamento genera quindi la richiesta di rimunerazione pertinente al sistema di pagamento.
10. Il sistema di accettazione della carta genera quindi una richiesta di pagamento al sistema di accettazione della carta utilizzando il token generato nel punto 5.

**Rischio di prima corsa (First ride risk):**

Uno dei principi del cEMV Open Payment è la natura differita delle autorizzazioni di accesso al sistema. Esiste infatti il rischio che il cliente possa viaggiare durante una giornata ed il relativo pagamento possa essere rifiutato, con conseguente potenziale perdita di entrate per l'operatore di trasporto. Nel Regno Unito questo rischio è mitigato dalla protezione della responsabilità dell'emittente fino a dieci sterline (limite attuale). Per gli importi di tariffa che vengono rifiutati, superiori a questo limite, l'operatore di trasporto si occuperà del recupero del debito e inserirà i dettagli della carta nella Deny list.

# 6. Sistema Antifrode e gestione Blacklist

Un sistema antifrode regionale è costituito da un insieme di funzionalità software che, integrando i dati raccolti dal CSR-BIP e relativi alle blacklist, alle validazioni e ai dati di vendita provenienti dai CCA, segnala alla Centrale Regionale BIP specifiche attività sospette, come ad esempio la firma di contratti con SAM inserite nella blacklist dei SAM, l'esistenza di smart card clonate e/o emulate, asimmetrie tra validazioni e titoli venduti, validazioni da Credito Trasporti per un ammontare superiore al credito venduto, etc.

Per ognuna delle tipologie di segnalazione provenienti dal sistema antifrode regionale è individuata una procedura di gestione, che prevede una segnalazione di rischio per il CCA coinvolto oppure innesca attività di approfondimento della problematica propedeutiche all'eliminazione del problema. Tra i compiti del sistema antifrode è prevista anche l'attribuzione di un coefficiente di rischio ad ogni entry della blacklist delle carte BIP che consentirà la trasmissione di una blacklist ordinata per ciascun CCA.

Il sistema di gestione delle blacklist consente di raccogliere la lista delle carte BIP e dei moduli di sicurezza SAM che le aziende BIP o altri attori del sistema autorizzati dichiarano fuori validità a seguito di notizie di furto, smarrimento o deterioramento, a causa di un utilizzo improprio o per altre ragioni che ne impongano il ritiro dal circuito BIP.

Al momento dell'inserimento di una carta BIP in blacklist, l'azienda BIP emettitrice, utilizzando il protocollo BIPEx, trasferisce questa informazione al CSR-BIP, che memorizza i numeri seriali delle tessere revocate nella blacklist regionale. Analogamente, ogni qual volta una SAM viene messa in blacklist, grazie al sistema di firma dei titoli di viaggio BIP è possibile individuare tutti i titoli di viaggio emessi con quella SAM a partire dalla data dell'inserimento in blacklist, consentendo quindi di invalidare tutti i titoli di viaggio, e di conseguenza le smart card, emesse con quella SAM.

La blacklist regionale costituisce dunque l'elenco dei numeri seriali delle smart card e dei SAM BIP non più validi nel sistema e viene comunicata a tutti i CCA del sistema secondo protocollo BIPEx. Per comodità di utilizzo e recepimento da parte dei sistemi aziendali in uso presso i CCA, la blacklist regionale è esposta anche in formato CSV.

# 7. Post-payment

Si tratta di un nuovo e futuribile sistema di tariffazione di tipo Pay per Use, volto ad incentivare un maggiore uso del mezzo pubblico su percorsi non-abituali.

Tale incentivazione avverrà da un lato intrinsecamente, rendendo più semplice l'accesso al servizio grazie al principio del *post-payment*, dall'altro in modo estrinseco, favorendo gli utenti che viaggiano su percorsi differenziati grazie a scontistiche incrementali elaborate con appositi algortimi.

La modalità di addebito in post-payment prevede che l'utente possa utilizzare liberamente qualunque sistema di trasporto aderente, effettuando le operazioni di check-in e check-out ogni qual volta queste siano previste.
La smartcard opera – in tale contesto – come una credenziale identificativa dell'utente (in modo simile a quanto avviene per le carte di credito) ed il sistema, una volta raccolti i dati di tutte le validazioni, verifica i viaggi effettuati e calcola – indicativamente una volta al mese – l'entità della somma dovuta, applicando eventualmente algoritmi di ottimizzazione, calcolo della *best-fare*, o scontistiche dedicate.
Il titolo di viaggio deve essere caricato a bordo della smartcard BIP a seguito di una esplicita richiesta o azione dell'utente, congiuntamente alla raccolta delle informazioni necessarie ad addebiti e pagamenti.
Il titolo di viaggio post-payment dà diritto ad effettuare un numero di corse e di cambi illimitato nell'ambito territoriale, limitatamente ai servizi ed alle aziende aderenti. La modalità di funzionamento può essere riassunta in:

- **adesione esplicita da parte dell'utente a circuito post-payment:** l'utente deve aderire di sua iniziativa al circuito, recandosi presso uno sportello abilitato o direttamente tramite portale BIP, e fornire contestualmente una modalità di addebito e di pagamento valida e verificabile (carta di credito, RID ecc.);
- **caricamento del titolo sulla smartcard:** dopo l'adesione e prima di poter viaggiare, il titolo deve essere caricato sulla card per essere riconosciuto e gestito correttamente dai validatori (inizialmente il titolo verrà caricato su una smartcard con layout personalizzato pay-per-use); il titolo non ha scadenza;
- **validazione ad ogni cambio:** per poter ricostruire l'itinerario dell'utente ed addebitare correttamente e senza sovracosti quanto dovuto, è richiesta la validazione in salita ed in discesa da ogni mezzo, a meno di condizioni differenti (es: nel contesto urbano potrà essere richiesta la sola validazione in salita).

Le informazioni di ciascuna validazione, inclusi i dati relativi alla cifra decrementata in fase di check-in ed a quella riaccreditata in fase di check-out, calcolate a bordo mezzo (in maniera non dissimile a quanto avviene per il credito trasporti), vengono trasmesse al CCA aziendale e da qui al CSR per le operazioni di verifica e di clearing. In alternativa, il CCA calcolerà gli importi dovuti direttamente al centro, prima di trasmettere il BIPEx al CSR.

## 8. Servizi per CCA

Nel corso dell'implementazione e della realizzazione dell'ecosistema CSR è da sempre maturata l'esigenza dell'implementazione di una serie di servizi rivolti ai CCA ed alle Aziende TPL.
La necessità primaria nasce dal bisogno di poter accedere ad un servizio centralizzato che rendesse disponibile a tutti gli stakeholder tutte le informazioni ricevute dal CSR fornite localmente dia vari CCA.
La realizzazione di servizi integrati nei confronti delle aziende, che armonizzi e semplifichi la gestione di utenti e titoli a livello regionale, è da sempre uno degli obiettivi del progetto BIP e del suo CSR. Il termine stesso "CSR" (Centro Servizi Regionale) evoca il vero scopo di tale

componente: non solo acquisire ed aggregare dati, ma anche e soprattutto essere un riferimento centralizzato al "servizio" degli Enti, degli Operatori, e più in generale del territorio.
Lo scopo finale rimane quello di semplificare la vita dei cittadini, favorendoli nei loro spostamenti, migliorarne la mobilità trasmettendo al contempo l'immagine di un vero sistema di trasporti e servizi "integrato", moderno ed affidabile.
Allo stesso tempo, i servizi del CSR sono volti ad agevolare le imprese, in particolare quelle più piccole e meno informatizzate, semplificando gli aspetti di gestione degli utenti e la consistenza dei dati.
Le funzionalità principali, messe a disposizione del CSR verso i CCA e le Aziende TPL possono essere riassunte nel seguente modo:

- visualizzare/richiedere i dati di un utente noto, con particolare riferimento alle informazioni di contatto o ad altri dati che l'utente abbia inserito a Portale
- richiedere i dati di un utente sconosciuto, ad esempio a fini di emissione di una nuova tessera
- effettuare una ricerca per seriale tessera: questa funzionalità può esse utile nel caso di ritrovamento di una tessera smarrita o di tessera con codice fiscale errato
- visualizzare dati relativi a titoli e validazioni;
- effettuare operazioni sulla blacklist,
- richiedere la ricarica di titoli tramite la Rete di Ricarica Regionale,
- servizi evoluti per la riscrittura titoli e tessere, questi rappresentano l'evoluzione più interessante ed innovativa delle funzionalità della Rete di Ricarica, una volta completati, tali servizi permetteranno:

  - ❖ il caricamento tramite rete di ricarica di un generico titolo emesso da qualunque azienda aderente; in questa casistica rientrano eventuali titoli acquistati online e caricati su Smart Card tramite app;
  - ❖ l'emissione di tessere sostitutive da parte delle aziende, con lo spostamento (o impropriamente la "clonazione") su una nuova tessera di titoli preesistenti, anche emessi da aziende differenti , e l'inclusione automatica in blak list della tessera sostituita;
  - ❖ il servizio di emissione di tessere sostitutive da parte del CSR, che potrebbe potenzialmente includere la filiera completa: dalla richiesta online, alla stampa delle tessere alla postalizzazione delle stesse.