

**gestione della blacklist regionale delle smart card e dei MODULI sam bip**

Specifiche e processi

*Documento confidenziale*

Versione 1.0

Sommario

[1 Introduzione 3](#_Toc488140661)

[Definizioni ed Acronimi 4](#_Toc488140662)

[Riferimenti 4](#_Toc488140663)

[2 Contesto e architettura logica del sistema 5](#_Toc488140664)

[3 Principi generali 6](#_Toc488140665)

[4 La blacklist delle smart card BIP 8](#_Toc488140666)

[4.1 Blacklist e “greylist” 8](#_Toc488140667)

[4.2 Struttura della blacklist: serial number, data di inserimento e causale 9](#_Toc488140668)

[4.3 Trasmissione della blacklist: protocollo, modalità e frequenza di trasmissione 10](#_Toc488140669)

[4.4 Gestione del pregresso 11](#_Toc488140670)

[5 La blacklist dei moduli SAM 13](#_Toc488140671)

[5.1 Struttura della blacklist: numero di serie, contatore, data di inserimento e causale 14](#_Toc488140672)

[5.2 Trasmissione della blacklist: protocollo, modalità e frequenza di trasmissione 15](#_Toc488140673)

[5.3 Gestione del pregresso 16](#_Toc488140674)

[6 Sistema antifrode e contenimento delle blacklist 17](#_Toc488140675)

[6.1 Il sistema antifrode regionale 17](#_Toc488140676)

[6.2 Contenimento dimensionale delle blacklist 18](#_Toc488140677)

[7 Comportamento degli apparati periferici 19](#_Toc488140678)

[8 Esempio di codifica BIPEx di una blacklist 20](#_Toc488140679)

1. Introduzione

La presente specifica descrive le caratteristiche e le modalità della gestione delle blacklist delle smart card e dei moduli SAM in uso nel sistema BIP.

È previsto che le aziende BIP esprimano a 5T/Regione Piemonte, i fabbisogni di smart card BIP che intendono emettere a favore dei propri clienti. Raccolte le richieste di fabbisogno, 5T procede con le gare di fornitura (ad eccezione delle smart card multi-profilo di Trenitalia, che vengono testate da 5T ma approvvigionate da Trenitalia). 5T acquisisce le smart card BIP richieste e, dopo averle testate, le rilascia a lotti alle aziende BIP. Contestualmente memorizza sui sistemi della Centrale Regionale BIP e del CSR-BIP l’associazione tra ogni smart card e l’azienda BIP a cui è stata consegnata. Da quel momento in poi e fino a prova contraria, per il CSR-BIP le smart card consegnate alle aziende BIP sono valide a tutti gli effetti.

Qualora vengano meno i requisiti di validità di una smart card BIP – siano essi dovuti a smarrimento, furto, tentativi di frode, ecc. – è responsabilità dei CCA segnalare questa problematica al CSR-BIP, che a sua volta si farà carico di condividere l’informazione con gli altri CCA.

L’elenco delle smart card BIP non più valide è denominato “Blacklist delle smart card BIP”.

Analogo trattamento deve essere riservato ai moduli SAM che ritenuti non più idonei all’operatività, ad esempio a causa di furto o danneggiamento. La particolarità della “Blacklist dei moduli SAM BIP” è che le operazioni svolte dai moduli successivamente alla data del loro inserimento nella blacklist sono da considerarsi non valide.

Il presente documento si propone di definire le modalità tecniche e operative per la condivisone delle informazioni sulle blacklist tra i CCA e il CSR-BIP e di indicare le linee guida BIP circa il comportamento delle periferiche rispetto a tessere non valide, perché inserite in Blacklist delle smart card BIP o perché oggetto di operazioni da parte di SAM già entrate in blacklist.

## Definizioni ed Acronimi

| Acronimo | Definizione |
| --- | --- |
| BIP | Biglietto Integrato Piemonte |
| SAM | Secure Access Module |
| TLC-D | Tessere di Libera Circolazione per Disabili |
| BL | Blacklist (generico) |
| BLSC | Blacklist delle smart card BIP |
| BLSAM | Blacklist dei moduli SAM BIP |
| CSR-BIP | Centro Servizi Regionale del BIP |
| CCA | Centro di Controllo Aziendale del BIP |
| CT | Credito Trasporti |
| CDM-BIP | Card Data Model BIP |
| BIPEx | BIP Exchange, protocollo di trasmissione dati tra CCA e CSR |

## Riferimenti

| Riferimento | Descrizione |
| --- | --- |
| 1. *Requisiti tecnici delle smartcard BIP (Card Data Model)* | |

1. Contesto e architettura logica del sistema

La Figura 1 seguente rappresenta schematicamente la porzione dell’architettura BIP coinvolta nella gestione delle blacklist.

Le singole BL gestite dai CCA contribuiscono ad alimentare la BL regionale sul CSR-BIP attraverso l’invio delle informazioni relative a BLSC e BLSAM. Tale flusso informativo BIPEx, denominato (1) nello schema logico in Figura 1, avviene secondo quanto previsto dal protocollo BIPEx alla sua ultima versione (ad oggi v. 1.0.1). Le informazioni così raccolte vengono archiviate nelle banche dati regionali e organizzate per le finalità del servizio di propagazione delle BLSC e BLSAM ai CCA.

Attraverso un apposito componente del CSR-BIP denominato “Sistema di propagazione delle blacklist” i CCA sono in grado di ricevere la BL regionale tramite il flusso (2) di seguito rappresentato.

**CCA aziende TPL**

CSR-BIP

**CCA1**

**CCA2**

**CCAn**

**Figura 1** – Gestione delle blacklist e scambio dati CSR-BIP/CCA

1. Principi generali

Il presente paragrafo riassume i principi generali che sono alla base delle modalità operative e tecniche di gestione delle BL nel sistema BIP.

1. Le smart card non coincidono con i titoli di viaggio che ospitano

Per consentire di affrontare il tema delle blacklist BIP è necessario ricordare la distinzione tra la smart card BIP e i titoli di viaggio su di essa caricati. Il concetto di blacklist delle smart card (BLSC) deve infatti riferirsi unicamente alla smart card BIP (intesa come supporto portatile in grado di ospitare titoli di viaggio) e non ha pertinenza con i titoli di viaggio su essa caricati.

Ne deriva che la sospensione di un titolo di viaggio per motivi “gestionali” o di altra natura non può prevedere necessariamente l’inserimento del seriale della smart card BIP che lo ospita nella BLSC regionale. La motivazione della non-validità del titolo potrebbe infatti non essere contemplata tra le possibili motivazioni che compromettono la validità del supporto che lo ospita.

Le motivazioni che comportano l’inserimento di una smart card BIP in blacklist sono legate al supporto o ad operazioni fraudolente riscontrate su di esso e tali da interrompere l’utilizzo della smart card nel suo complesso. La non-validità della smart card deve avere effetti sulla possibilità dell’utente di utilizzare tutti i titoli di viaggio caricati su tale supporto.

1. Il CSR-BIP deve essere informato dello stato di tutte le smart card BIP circolanti

Il CSR-BIP è tenuto a conoscere lo stato di tutte le smart card BIP distribuite ai CCA, con particolare riferimento all’elenco completo dei seriali delle smart card BIP che i CCA inseriscono nelle proprie BL, con indicazione della data e della motivazione (altrimenti detta causale) di inserimento.

Non è invece interesse del CSR-BIP conoscere i numeri seriali delle smart card BIP sospese dal singolo CCA per motivi “gestionali”, non potendo tale condizione inficiare la validità della smart card negli altri bacini del sistema BIP.[[1]](#footnote-1)

1. La gestione delle blacklist a beneficio del sistema

La gestione delle BLSC BIP consente al CSR-BIP l’espletamento delle proprie funzioni rispetto ai compiti di salvaguardia della sicurezza del sistema BIP e riguardo il monitoraggio complessivo dello stato delle smart card BIP in circolazione. Permette allo stesso tempo ai CCA di essere informati sulle smart card BIP non-valide a livello regionale, in modo da impedire l’utilizzo di quest’ultime presso i propri mezzi di trasporto.

Il CSR-BIP gestisce le BL regionali di smart card e moduli SAM anche attraverso le funzionalità del Sistema Antifrode Regionale. L’utilizzo di queste funzionalità potrà consentire al CSR-BIP di realizzare un ordinamento dei seriali inseriti nella BLSC sulla base della probabilità che le smart card siano in circolazione nel sistema.

Tale soluzione potrà consentire ai CCA di elaborare, in autonomia, eventuali versioni ridotte della BLSC da utilizzare, per esempio, su tipologie di apparati in grado di gestire un quantitativo di seriali minore rispetto all’intera BLSC. L’obiettivo di questa funzionalità è quello di preservare il più possibile la sicurezza del sistema, anche nel caso in cui gli apparati dislocati sul territorio non siano in grado di gestire l’intera BL regionale.

1. La blacklist delle smart card BIP

Il venir meno dei requisiti di validità di una smart card BIP ha rilevanza per tutti gli attori operanti nel sistema BIP. A nessuna smart card BIP inserita nella BLSC deve essere consentito di validare a bordo dei mezzi, né di completare alcuna operazione di acquisto e caricamento di un nuovo titolo di viaggio.

* 1. Blacklist e “greylist”

Alcuni CCA utilizzano il termine “greylist” per indicare una lista di seriali sotto osservazione tipicamente per questioni amministrative o operative della vendita/rinnovo dei titoli di viaggio. Ogni azienda BIP esercita in autonomia la gestione delle “greylist”, secondo processi e regolamenti che non sono, per titoli aziendali non interoperabili, di pertinenza regionale.

È comunque possibile riconoscere differenze sostanziali tra le greylist e le blacklist.

Anzitutto, l’entità e la natura dell’irregolarità relativa alla smart card BIP inserita in blacklist deve essere legata al supporto e non ai titoli di viaggio in esso contenuti. La smart card è da considerarsi non più valida in caso di furto o smarrimento (in quanto il titolare non ne dispone più in prima persona), nel caso in cui sia stata ritirata dalla circolazione per motivi tecnici o gestionali oppure nel caso in cui venga bloccata per altri motivi.

Come precedentemente specificato, le irregolarità gestionali afferenti uno o più titoli di viaggio potrebbero, a discrezione del CCA o dell’azienda BIP e in base alla propria gestione della “greylist”, comportare l’inserimento dei seriali di queste smart card nelle “greylist” dei CCA, ma non l’inserimento degli stessi serial number nella blacklist che poi viene trasmessa al CSR-BIP.

Ne consegue che, ad esempio, il mancato rispetto delle scadenze di pagamento di un titolo venduto ratealmente non comporti necessariamente l’inserimento del serial number della smart card in blacklist.

***Gli inserimenti di serial number di smart card BIP nella blacklist trasmesse al CSR-BIP sono irreversibili***, mentre la gestione degli inserimenti e delle rimozioni dalla “greylist” è demandata ai CCA e non è normata a questo livello di dettaglio, lasciando ai CCA l’autonomia di deciderne le procedure di gestione.

L’irreversibilità è dovuta principalmente a due fattori:

* il primo è connesso alla complessità intrinseca delle reti di vendita e validazione delle aziende BIP e dei CCA, che in molti casi prevedono tempi di propagazione delle informazioni significativi che non consentirebbero operazioni di inserimento e rimozione di durata compatibile con le esigenze di sicurezza del sistema e di contrasto alla frode;
* il secondo fattore è legato alle attività di invalidazione del DF Trasporti, che le aziende BIP sono in grado di attuare in presenza di una smart card inserita nella BLSC.

Fatti salvi i principi appena elencati, da cui conseguono specifiche modalità di trasmissione e procedure di gestione delle blacklist tra CCA e CSR-BIP, la gestione delle greylist in seno ai singoli CCA può avvenire secondo procedure autonome e complementari a quelle di gestione delle blacklist.

* 1. Struttura della blacklist: serial number, data di inserimento e causale

Così come previsto dal protocollo BIPEx, la BLSC è costituita dall’elenco delle smart card da considerarsi non più valide, dove la smart card è identificata dal proprio serial number ed è corredata dalla causale di inserimento nella blacklist e dalla data in cui tale inserimento è stato effettuato.

Riguardo la data di inserimento è opportuno specificare che si tratta della data in cui è stato rilevato il nuovo status (smart card non più utilizzabile) nel CCA che inserisce il seriale in blacklist e non altre date come, ad esempio, la data di trasmissione al CSR-BIP.

Altra considerazione relativa alla data di inserimento in blacklist riguarda la non opportunità di retrodatare tale valore rispetto alla data di effettivo inserimento nella blacklist del CCA.

La causale costituisce un attributo fondamentale per descrivere la natura dell’inserimento di una smart card in blacklist: oltre a definire la motivazione dell’inserimento in BL, infatti, è in grado di comunicare intrinsecamente se la smart card sia ancora in circolazione o sia stata dal CCA ritirata e conservata in luogo sicuro o distrutta. Sulla base di questa informazione è quindi possibile operare strategie di contenimento dimensionale e/o ridimensionamento delle blacklist delle smart card BIP che vengono trasmesse agli apparati periferici. Tali strategie si basano sul riconoscimento del dato di fatto per cui se una smart card è stata ritirata dalla circolazione non è necessario che gli apparati periferici siano in grado di individuarla e, di conseguenza, non è necessario che ne conoscano lo status di non validità.

È facoltà dei CCA comunicare al CSR-BIP l’avvenuta distruzione delle smart card BIP ritirate. In ogni caso, qualora avvenissero furti o smarrimenti di tali smart card dai centri servizio delle aziende, i CCA sono tenuti a modificare la causale di inserimento in blacklist da “canceled” o “damaged” in “stolen” o “lost” a seconda del caso in esame. Tali seriali saranno quindi reinseriti nel flusso 2 (dal CSR al CCA) con un adeguato livello di priorità.

Nel seguito si riportano brevemente le causali già definite dal protocollo BIPEx e le caratteristiche che ciascuna di esse ha con il relativo ritiro dalla circolazione delle smart card a cui sono associate.

**Tabella 1** – Causali di inserimento nella BLSC

|  |  |  |
| --- | --- | --- |
| **Causale** | **Descrizione** | **In circolazione** |
| stolen | Smart card rubata, non più nella disponibilità del titolare | Sì |
| lost | Smart card smarrita, non più nella disponibilità del titolare | Sì |
| cloned | NON DEFINITO | - |
| damaged | Smart card danneggiata, viene ritirata dall’emettitore | No |
| canceled | Smart card cancellata per motivi tecnici o gestionali, viene ritirata dall’emettitore / Smart card il cui DF è stato invalidato dai validatori o dagli strumenti di lettura/scrittura | No |
| blocked | Smart card bloccata per motivi tecnici o gestionali, non viene ritirata dall’emettitore (in caso di ritiro avrebbe stato “canceled”) | Sì |
| duplicated | NON DEFINITO | - |
| renewed | Smart card rinnovata per motivi gestionali, viene ritirata dall’emettitore | No |

**NB**= le causali “cloned” e “duplicated” sono da considerarsi non assegnabili sebbene previste dal protocollo BIPEx.

* 1. Trasmissione della blacklist: protocollo, modalità e frequenza di trasmissione

I flussi che coinvolgono la BLSC, così come evidenziato nell’architettura logica del sistema, sono di due tipologie:

1. quello che dai CCA viene trasferito al CSR-BIP;
2. quello che dal CSR-BIP viene trasferito ai CCA.

Il flusso 1 vede il trasferimento delle informazioni sulle blacklist raccolte all’interno di ogni singolo CCA verso il CSR-BIP, al fine di completare il censimento dello stato di tutte le smart card BIP distribuite ai CCA con i dati relativi alle smart card non più valide.

Il flusso 2 permette di completare le informazioni relative alla blacklist che ciascun CCA deve poter distribuire alla propria rete, integrando i dati alimentanti la BLSC regionale provenienti dagli altri CCA con quelli che il CCA in esame già possiede.

In entrambi i casi il formato di comunicazione previsto è il protocollo BIPEx, che già include il formato di tutte le informazioni necessarie (serial number, causale, data di inserimento).

La modalità di trasmissione del flusso 1 prevede un invio quotidiano in orario notturno (che sarà concordato con ciascun CCA) in modalità “push” dal CCA al CSR-BIP, mentre per il flusso 2 è prevista una modalità “pull”, in cui sono i CCA a dover richiedere al CSR-BIP il download della blacklist che sarà aggiornata quotidianamente .

Il trasferimento delle informazioni per entrambi i flussi avviene in modalità massiva: ogni invio prevede il trasferimento complessivo di tutti gli elementi presenti nella blacklist, in modo da offrire di volta in volta una fotografia complessiva della BLSC.

Al fine di agevolare la gestione in termini dimensionali della blacklist regionale senza compromettere gli aspetti di sicurezza del sistema, è previsto che per il flusso 2 vengano adottati opportuni accorgimenti, descritti nel presente documento in un paragrafo dedicato.

* 1. Gestione del pregresso

In prossimità del momento di attivazione del sistema di gestione delle BL regionali così come descritto nel presente documento, sarà necessario per ciascun CCA adeguare le informazioni relative alle smart card in blacklist già in proprio possesso. Queste informazioni dovranno essere riorganizzate e, se possibile, integrate in modo da essere compatibili con quanto descritto dalle presenti specifiche tecniche.

Una delle prime attività da effettuare sarà la mappatura delle causali già in adozione presso il CCA, che dipenderà in gran parte dai processi di gestione delle smart card in termini, ad esempio, di ritiro e custodia delle smart card che vengono rinnovate o cancellate. È presumibile che i processi attualmente in essere presso i CCA non prevedano alcune delle causali definite o, alternativamente, prevedano causali non definite ma che devono ricondotte a quelle condivise tra le parti.

Prima di avviare il flusso 1 ciascun CCA dovrà quindi provvedere alla ridefinizione dei processi sulla base delle causali definite e alla ridefinizione degli elementi già costituenti la blacklist delle smart card, in modo da poter alimentare il CSR-BIP uniformando il pregresso a quanto verrà trasferito a regime.

Qualora non sia possibile operare sulle causali o sulle date di inserimento in blacklist a causa della mancanza di informazioni storiche sulle singole entry della blacklist pregressa, il CSR-BIP richiede di operare scelte che tutelino il più possibile la sicurezza del sistema, imponendo causali che garantiscano un livello di attenzione adeguato (es. “blocked”, che comporta che la smart card sia comunque potenzialmente circolante) o date evidentemente successive al reale inserimento in blacklist (es. la data di attivazione del flusso 1) in modo da non invalidare le politiche antifrode che saranno integrate nel CSR-BIP.

La Centrale Regionale BIP potrà supportare ciascun CCA coinvolto nella definizione di modalità operative di recupero del pregresso e di allineamento delle blacklist locali con quanto previsto dal sistema di gestione delle BL regionali.

1. La blacklist dei moduli SAM

I moduli SAM a disposizione delle aziende sono di varie tipologie:

* SAM-CPP: in uso presso i produttori di smart card per le fasi di pre-personalizzazione, o per la generazione di applet Java;
* SAM-CP: vengono usati tipicamente nelle biglietterie o nei centri di emissione smart card e consentono la personalizzazione del supporto, mediante la scrittura del file relativo all’anagrafica del cliente e all’emissione della carta;
* SAM-CL: consentono la scrittura e la firma di un TdV su smart card e la modifica del valore del borsellino elettronico (utilizzato per il CT);
* SAM-CV: solitamente installati a bordo mezzo, consentono di registrare sulla carta l‘avvenuta validazione, nonché di decrementare in valore del CT, o riaccreditare parte dell’ultimo decremento, scrivendo e firmando un record di log in tutti i casi.

Le uniche tipologie di SAM che contengono le chiavi crittografiche necessarie per la scrittura di TdV potenzialmente validi sulla rete BIP sono SAM-CP e SAM-CL (come descritto dal CDM-BIP), vanno tuttavia riportati nella BLSAM anche le informazioni relative a SAM-CPP (qualora nella disponibilità del CCA) e SAM-CV.

Ogni qual volta un TdV viene scritto su una smart card BIP, il record che lo contiene, viene firmato elettronicamente, in modo da garantirne l’autenticità. La firma elettronica è corredata dal numero di serie del modulo SAM e da un valore specifico detto “SAM counter” (nel seguito semplicemente “contatore” o “*counter*”), che indica il numero di operazioni di firma effettuate dal modulo stesso.

Contrariamente al caso del SAM-CV, per il quale il meccanismo di scrittura della firma non consente di individuare il modulo che l’ha effettivamente calcolata, i moduli SAM-CP e SAM-CL sono individuabili mediante la lettura dei record relativi ai TdV o al CT.

La presenza in blacklist di un modulo SAM-CP o SAM-CL comporta che i sistemi in uso presso tutti i CCA devono considerare come fossero in blacklist tutte le smart card sulle quali è presente almeno un TdV scritto da un modulo SAM presente nella BLSAM, ma solo nel caso in cui il valore del *counter* relativo al modulo SAM che ha firmato il TdV sia superiore a quello indicato nella BLSAM.

Il furto o lo smarrimento di un modulo SAM va immediatamente denunciato dal CCA alle autorità competenti e, subito dopo, notificato al CSR-BIP.

* 1. Struttura della blacklist: numero di serie, contatore, data di inserimento e causale

Così come previsto dal protocollo BIPEx, la blacklist dei moduli SAM BIP è costituita dall’elenco dei numeri di serie dei moduli SAM da considerarsi non più validi, dal relativo valore del contatore e dalla corrispondente causale di inserimento.

Il valore della data di inserimento può essere la stessa data in cui è stato rilevato il nuovo status, o una data precedente e deve comunque coincidere con la data più recente nella quale è stato registrato il valore più alto del contatore. Si raccomanda la massima attenzione nel reperire il dato, in quanto l’utilizzo di date scorrette (come, ad esempio, la data di trasmissione del flusso al CSR-BIP) può compromettere il corretto funzionamento dei meccanismi antifrode.

Anche nel caso dei moduli SAM, la causale costituisce un attributo fondamentale per descrivere la natura dell’inserimento in blacklist: oltre a definire la motivazione dell’inserimento in BL, infatti, è in grado di comunicare intrinsecamente se il modulo SAM sia ancora in circolazione o sia stato ritirato e conservato dal CCA in luogo sicuro, o addirittura distrutto. Sulla base di questa informazione è quindi possibile operare strategie di contenimento dimensionale e/o ridimensionamento delle blacklist dei moduli SAM che vengono trasmessi agli apparati periferici. Tali strategie si basano sull’assunto per cui se un modulo SAM è stato ritirato dalla circolazione non è necessario che gli apparati periferici siano in grado di individuarlo e, di conseguenza, non è necessario che ne conoscano lo status di non validità.

Si segnala a tal proposito che i SAM ritirati dal CCA (recanti le causali descritte alla Tabella seguente con “in circolazione” pari a “No”) devono essere inseriti in blacklist con l’apposita causale e riconsegnati al CSR-BIP.

Nel seguito si riportano brevemente le causali già definite dal protocollo BIPEx e le caratteristiche che ciascuna di esse ha con il relativo ritiro dalla circolazione dei moduli SAM a cui sono associate.

**Tabella 2** – Causali di inserimento nella BLSAM

|  |  |  |
| --- | --- | --- |
| **Causale** | **Descrizione** | **In circolazione** |
| Stolen | SAM rubato, non più nella disponibilità del titolare | Sì |
| Lost | SAM smarrito, non più nella disponibilità del titolare | Sì |
| Cloned | NON DEFINITO | - |
| damaged | SAM danneggiato, viene ritirata dall’emettitore | No |
| canceled | SAM bloccato per motivi tecnici, o non più in uso nel CCA per motivi gestionali e che comunque viene ritirata dal CCA | No |
| blocked | SAM bloccato per motivi tecnici o gestionali, che non viene ritirata dal CCA | Sì |
| duplicated | NON DEFINITO | - |
| renewed | SAM sostituito per motivi gestionali, viene ritirata dal CCA | No |

**NB** = le causali “cloned” e “duplicated” sono da considerarsi non assegnabili sebbene previste dal protocollo BIPEx.

* 1. Trasmissione della blacklist: protocollo, modalità e frequenza di trasmissione

Le modalità di trasmissione della BLSAM sono del tutto analoghe a quelle della BLSC.

Nello specifico, i flussi che coinvolgono la BLSAM, così come evidenziato nell’architettura logica del sistema, sono di due tipologie:

1. quello che dai CCA viene trasferito al CSR-BIP;
2. quello che dal CSR-BIP viene trasferito ai CCA.

Il flusso 1 vede il trasferimento delle informazioni sulle blacklist raccolte all’interno di ogni singolo CCA verso il CSR-BIP, al fine di completare il censimento dello stato di tutti i moduli SAM BIP distribuiti ai CCA con i dati relativi a quelli non più validi.

Il flusso 2 permette di completare le informazioni relative alla blacklist che ciascun CCA deve poter distribuire alla propria rete, integrando i dati alimentanti la BLSAM regionale provenienti dagli altri CCA con quelli che il CCA in esame già possiede.

In entrambi i casi il formato di comunicazione previsto è il protocollo BIPEx, che già prevede tutte le informazioni necessarie (*serial number*, *counter*, causale, data di inserimento).

La modalità di trasmissione del flusso 1 prevede un invio quotidiano in orario notturno (che sarà concordato con ciascun CCA) in modalità “push” dal CCA al CSR-BIP, mentre per il flusso 2 è prevista una modalità “pull”, in cui sono i CCA a richiedere al CSR-BIP il download della blacklist, che sarà aggiornata quotidianamente .

Il trasferimento delle informazioni per entrambi i flussi avviene in modalità massiva: ogni invio prevede il trasferimento complessivo di tutti gli elementi presenti nella blacklist, in modo da offrire di volta in volta una fotografia complessiva della BLSAM.

Al fine di agevolare la gestione in termini dimensionali della blacklist regionale senza compromettere gli aspetti di sicurezza del sistema, è previsto che per il flusso 2 vengano adottati opportuni accorgimenti, descritti nel presente documento in un paragrafo dedicato.

* 1. Gestione del pregresso

In prossimità del momento di attivazione del sistema di gestione delle BL regionali così come descritto nel presente documento, sarà necessario per ciascun CCA adeguare le informazioni relative ai moduli SAM in blacklist già in proprio possesso. Queste informazioni dovranno essere riorganizzate e, se possibile, integrate in modo da essere compatibili con quanto descritto dalle presenti specifiche tecniche.

Una delle prime attività di effettuare sarà quella di effettuare una mappatura delle causali già in adozione presso il CCA, che dipenderà in gran parte dai processi di gestione dei moduli SAM in termini, ad esempio, di ritiro e custodia dei moduli SAM.

***Contrariamente al caso della BLSC, tutti i moduli SAM inseriti in blacklist che non siano in circolazione vanno restituiti al CSR-BIP***.

È presumibile che i processi attualmente in essere presso i CCA non prevedano alcune delle causali definite o, alternativamente, prevedano causali non definite ma che devono ricondotte alle causali condivise tra le parti.

Prima di avviare il flusso 1 ciascun CCA dovrà quindi provvedere alla ridefinizione dei processi sulla base delle causali definite e alla ridefinizione degli elementi già costituenti la BLSAM, in modo da poter alimentare il CSR-BIP uniformando il pregresso a quanto verrà trasferito a regime.

Qualora non sia possibile operare sulle causali o sulle date di inserimento in blacklist a causa della mancanza di informazioni storiche sulle singole entry della blacklist pregressa, il CSR-BIP richiede di operare scelte che tutelino il più possibile la sicurezza del sistema, imponendo causali che garantiscano un livello di attenzione adeguato (es. “blocked”, che comporta che il modulo SAM sia comunque potenzialmente circolante) o date evidentemente successive al reale inserimento in blacklist (es. la data di attivazione del flusso 1) in modo da non invalidare le politiche antifrode che saranno integrate nel CSR-BIP.

La Centrale Regionale BIP potrà supportare ciascun CCA coinvolto nella definizione di modalità operative di recupero del pregresso e di allineamento delle blacklist locali con quanto previsto dal sistema di gestione delle BL regionali.

1. Sistema antifrode e contenimento delle blacklist

Nel contesto della gestione delle blacklist richiede particolare attenzione il tema delle limitazioni dimensionali di cui possono soffrire gli apparati periferici che si trovano a dover gestire le BLSC. Il presente paragrafo descrive il ruolo del sistema antifrode regionale, istanziato presso il CSR-BIP, e le strategie adottabili per contenere dimensionalmente le BLSC pur garantendo un adeguato livello di sicurezza del sistema BIP.

* 1. Il sistema antifrode regionale

Il 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, è in primo luogo in grado di segnalare alla Centrale Regionale BIP specifiche attività sospette, come ad esempio:

* l’esistenza di SAM clonate
* la firma di contratti con SAM inserite nella BLSAM
* l’esistenza di smart card clonate e/o emulate
* l’utilizzo di SAM non BIP per la firma di titoli BIP
* asimmetrie tra validazioni e titoli venduti
* l’emissione di titoli da aziende BIP non titolate alla vendita specifica
* le validazioni da Credito Trasporti per un ammontare superiore al credito venduto o che mostrano un credito superiore ad una determinata soglia
* gli errori di ricarica multipla di titoli da whitelist
* la presenza di più smart card BIP associate al medesimo codice fiscale.

Per ognuna delle tipologie di segnalazione provenienti dal sistema antifrode regionale è individuata una procedura di gestione, che può prevedere una segnalazione di rischio per il CCA coinvolto oppure innescare attività di approfondimento della problematica propedeutiche all’eliminazione del problema stesso e, se necessario, alla segnalazione di attività illecite alle autorità di pubblica sicurezza.

Tra i compiti del sistema antifrode c’è anche l’attribuzione di un coefficiente di rischio ad ogni entry della BLSC (il concetto sarà più ampiamente sviluppato nel prossimo paragrafo). Il coefficiente è calcolato da un algoritmo che tiene in considerazione alcuni aspetti quali:

* la presenza di tentativi di validazione recenti con smart card inserite in blacklist,
* la presenza di titoli spendibili su più CCA (es. Formula, Libera Circolazione o Credito Trasporti),
* la possibilità che la smart card sia stata clonata e/o emulata,
* la presenza di un Credito Trasporti considerevole.
  1. Contenimento dimensionale delle blacklist

La dimensione della BLSC regionale a regime dipende strettamente dai processi di emissione, gestione e ritiro delle smart card circolanti. In linea generale è possibile ipotizzare che un certo tipo di apparati periferici a basse prestazioni possa essere messa nelle condizioni di operare al meglio gestendo un sottoinsieme della BLSC, che convenzionalmente prende il nome di “blacklist dinamica”, rispetto alla blacklist nella sua forma integrale.

Il dimensionamento della “blacklist dinamica” non può essere definito a priori dal CSR-BIP, ma deve essere autonomamente definito da ciascun CCA sulla base delle proprie esigenze, di propri ragionamenti di opportunità e dei limiti tecnici relativi ai propri apparati.

Il CSR-BIP, sfruttando le potenzialità del proprio sistema antifrode, applica opportune strategie nella redazione della BLSC regionale.

***Tali strategie possono consentire il contenimento dimensionale della blacklist da parte di ciascun CCA***.

Il passaggio dalla BLSC integrale diffusa dal CSR-BIP a quella dinamica eventualmente implementata dal CCA è reso infatti possibile grazie all’ordinamento della blacklist in funzione del coefficiente di rischio che viene attribuito ad ogni singola smart card della BLSC dal sistema antifrode del CSR-BIP. Le smart card ad alto rischio sono riportate nella blacklist integrale con priorità alta, consentendo ai CCA di operare scelte quali il troncamento della lista dei codici seriali sulla base della dimensione tollerata dai propri apparati, massimizzando l’efficacia della blacklist dinamica in relazione al rischio di frode.

Come indicato nel paragrafo dedicato, la causale di inserimento in blacklist in alcuni casi indica che la smart card non è in circolazione e quindi il rischio di essere esibita da un utente è nullo: questo aspetto comporta l’esclusione dalla blacklist diffusa ai CCA attraverso il flusso 2. Al fine di massimizzare i risultati derivanti dall’ordinamento per fattore di rischio della BLSC, potranno inoltre essere valutati con ciascun CCA output dedicati, in modo che sia possibile attribuire un rischio inferiore a smart card che non contengono titoli di viaggio validi presso le aziende afferenti a quello specifico CCA rispetto a smart card potenzialmente utilizzabili con successo nell’area di riferimento.

Un ulteriore elemento che può consentire il contenimento della dimensione della blacklist viene dalla possibilità degli apparati periferici di invalidare le smart card BIP agendo sul record DF della carta stessa, come descritto nel paragrafo seguente.

1. Comportamento degli apparati periferici

Gli apparati periferici, siano essi validatrici, TVM o analoghi, sono in grado di invalidare il DF Trasporti (*Dedicated File: Transport application 1* – o DF1 – le cui caratteristiche sono indicate nelle Specifiche Tecniche della smart card BIP [1]), rendendo inutilizzabile la smart card.

Il comportamento degli apparati periferici nel caso di smart card in Blacklist è normato dal Card Data Model BIP al par.3.8.4 (Codice Stato Carta):

*Durante l'utilizzo da parte dell'utente la carta può essere posta nello stato di Black Listed, quindi bloccata, se essa risulta presente nella relativa lista.*

*Per portare lo stato logico della carta in Black Listed il validatore oppure lo strumento di lettura/scrittura dovrà utilizzare il comando di “Invalidate” presente nel sistema operativo. Il comando dovrà operare sulla ADF Trasporti sospendendone temporaneamente le funzionalità della carta fino allo sblocco della carta effettuabile presso le biglietterie aziendali autorizzate dotate di appositi terminali di lettura/scrittura.*

Nel caso in cui una smart card BIP presente in blacklist venga presentata al validatore oppure ad altri strumenti di lettura/scrittura, tali strumenti devono invalidarla attraverso l’operazione prima descritta.

L’invalidazione del DF Trasporti della smart card deve quindi generare una modifica nella causale di inserimento nella BLSC. Il seriale della smart card BIP invalidata viene reinserito nella blacklist da parte del CCA che ha realizzato l’operazione di invalidazione del DF Trasporti con causale “canceled” - causale corrispondente ad una smart card non circolante - a beneficio delle future elaborazioni da parte del CSR-BIP e di successiva rimozione del seriale della smart card BIP da successive versioni della BLSC regionale trasmesse ai CCA.

Al fine di verificare il funzionamento del sistema e del servizio di raccolta e diffusione delle BLSC e delle BLSAM, si rimanda ad un’apposita decisione del Gruppo di Lavoro sulle Blacklist regionali l’attivazione delle funzionalità di invalidazione del DF Trasporti da parte delle aziende TPL che attualmente non ne fanno uso.

1. Esempio di codifica BIPEx di una blacklist

Si riporta di seguito un esempio di codifica BIPEx relativo ad una blacklist fittizia contenente sia smartcard che SAM.

<?xml version="1.0"?><Siri xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" version="2.0" xsi:schemaLocation="http://bip.piemonte.it/bipex ../bipex\_report.xsd" xmlns="http://bip.piemonte.it/bipex"> <ServiceDelivery> <ResponseTimestamp>2017-07-18T06:01:01+02:00</ResponseTimestamp> <ProducerRef>CSR-Piemonte</ProducerRef> <ResponseMessageIdentifier>16</ResponseMessageIdentifier> <BlackListDelivery> <ResponseTimestamp>2017-07-18T06:01:01+02:00</ResponseTimestamp> <BlackList> <BlackListElement id="53:ble:941150020"> <InsertionDate>2017-05-03</InsertionDate> <InsertionType>lost</InsertionType> <TravelDocumentRef ref="53:td:941150020"/> </BlackListElement> <BlackListElement id="53:ble:940823334"> <InsertionDate>2017-07-18</InsertionDate> <InsertionType>damaged</InsertionType> <TravelDocumentRef ref="53:td:940823334"/> </BlackListElement> <BlackListElement id="1:ble:AE10A06D"> <InsertionDate>2017-06-01</InsertionDate> <InsertionType>stolen</InsertionType> <SAMRef ref="1:sam:AE10A06D"/> <SAMCounter>62603</SAMCounter> </BlackListElement> </BlackList> </BlackListDelivery> </ServiceDelivery></Siri>

1. Eventuali procedure per la gestione di liste di serial number di smart card BIP da bloccare per motivi gestionali legati a titoli interoperabili e/o integrati (es. titoli Formula) saranno oggetto di approfondimenti. [↑](#footnote-ref-1)