

Informazioni aggiuntive circa l'utilizzo del sistema T-serve presso gli sportelli del servizio di tesoreria (art. 9 comma 1 schema convenzione)

Al fine di rendere possibile la valutazione dei costi di quanto stabilito all'art. 9 comma 1 dello schema di convenzione per il servizio di tesoreria si precisa quanto segue:

Natura del servizio T-serve

Il servizio di pagamenti T-serve è un servizio realizzato ed erogato dal Comune di Prato mediante applicativi web accessibili dagli sportelli erogatori tramite un browser internet (explorer v. 7 o successive, mozilla firefox, Chrome).

Il servizio web, messo a disposizione del Comune, consente, all'operatore di sportello, di selezionare il debito dell'utente richiedente e di far saldare il debito riscuotendo (con i metodi di pagamento che lo stesso ente gestore dello sportello intende utilizzare) la cifra corrispondente e rilasciando una ricevuta prodotta dallo stesso sistema T-serve mediante stampa su carta comune.

Le cifre così riscosse devono affluire su di un conto corrente, le cui coordinate sono rese note a priori al Comune di Prato, da cui sono poi versate al comune con cadenza settimanale.

Il riversamento al Comune può avvenire con due meccanismi: il RID o un bonifico da parte dell'ente gestore dello sportello. Nel caso di banche il meccanismo utilizzato è quello del Bonifico.

Le cifre da riversare al Comune con ogni bonifico sono dedotte dal un sistema di contabilità di back-office, che lo stesso sistema T-serve offre all'ente gestore degli sportelli di riscossione. Tale sistema consente di totalizzare gli incassi settimanali e quindi di indicare le cifre per le quali effettuare i bonifici.

Problematiche gestionali legate al T-serve e tipiche per un ambiente bancario

Il servizio t-serve può essere erogato, dalla banca tesoriera, in ogni filiale o sportello che essa gestisce sul territorio dal momento che le cifre introitate non sono di fatto incassate dal tesoriere in prima istanza, ma versate, attraverso il procedimento indicato al punto precedente, all'ente. Sarà quest'ultimo, al ricevimento delle somme trasferite con i bonifici settimanali, ad eseguire le operazioni contabili di accertamento/incasso indicando al tesoriere, con relative reversali, di prelevare dal conto del Comune le varie cifre corrispondenti ai vari servizi per cui si è riscosso ed i capitoli di introito.

Pertanto il servizio di riscossione T-serve è, nella prima fase, quella della riscossione, del tutto indipendente dal servizio di tesoreria e serve solo a consentire al Comune di incassare degli importi. Il servizio di tesoreria, propriamente inteso, entrerà in gioco solo nella seconda fase in cui il comune reversalizzerà i singoli importi.

Va pertanto previsto che ogni sportello abilitato alla riscossione con il sistema T-serve sia abilitato a raggiungere i server del Comune da cui si eroga il servizio.

Per l'utilizzazione del servizio saranno necessarie delle credenziali di accesso per le quali valgono le considerazioni di cui al punto seguente di questo documento.

Al momento della riscossione da parte dello sportello T-Serve devono essere gestite di fatto due operazioni:

- a) La transazione T-serve per la notifica al Comune dell'avvenuta riscossione con il rilascio all'utente della ricevuta prodotta dal sistema T-serve (unica quietanza per il rapporto debitorio cittadino-Comune)
- b) La transazione bancaria con cui quest'ultima incassa effettivamente la cifra pagata e la riversa nel conto di accumulo descritto sopra. Tale incasso può avvenire con un qualunque metodo che la banca ritenga di attivare: incasso diretto, addebito su conto dell'utente, etc...

E' possibile realizzare su richiesta, un' integrazione tra T-serve e sistema della banca per la sincronizzazione delle operazioni.

Gestione delle credenziali degli operatori

Esistono due tipologie di credenziali di accesso al sistema T-serve che dovranno essere gestite:

- a) Quelle dei singoli sportellisti che gestiscono il rapporto con gli utenti paganti che devono accedere al sistema T-Serve:
 - a. Effettuano le operazioni di pagamento
 - b. Visualizzano le operazioni del giorno e eventualmente stornano le transazioni entro la giornata di effettuazione
- b) Quelle degli operatori della sede centrale della banca (nel caso di più filiali) che devono accedere al back-office del sistema T-Serve:
 - a. Monitorizzano il totale dei pagamenti e, in particolare, i rversamenti delle single filiali;
 - b. Riversano al Comune, con bonifico settimanale, le cifre introitate.
 - c. Supervisionano l'attività dei vari sportelli ed inoltrano al gestore del sistema le richieste di storno non in giornata dei vari operatori T-Serve

Per gli operatori di tipo b) è previsto il rilascio di credenziali specifiche da parte del Comune di Prato.

Per gli operatori di tipo a) (data la frequente mobilità degli stessi e la complessità per il Comune di seguire le modifiche organizzative interne alla banca) possono essere utilizzate due modalità di gestione:

- a) Rilascio da parte del Comune di credenziali come nel caso precedente (sconsigliabile per banche con un numero significativo di sportelli e per più di una filiale). In questo caso il rilascio delle credenziali è effettuato dal comune, mentre è a cura della banca lo spostamento delle persone tra filiali (qualora interessi una contabilità e quindi un controllo degli incassi per filiale)
- b) Integrazione del sistema di autenticazione della piattaforma T-serve con sistemi di single-sign-on della banca.

Per i dettagli tecnici della modalità b), che è quella consigliata per il servizio in questione, si rimanda al punto seguente.

Integrazione tra sistema di autenticazione utenti della banca e T-serve

Di seguito le specifiche per la realizzazione del single-sign-on che abbiamo implementato per altre banche.

Banche e Tserve

Per l'autenticazione degli sportellisti al sistema T-Serve viene utilizzato un sistema di autenticazione centralizzato denominato "Minosse" e gestito dal Comune di Prato. L'individuazione del singolo operatore è necessaria, oltre che per il rispetto della normativa sulla privacy e per la sicurezza del sistema stesso, anche per motivi autorizzativi alle singole tipologie di pagamento, per tracciabilità e per la corretta gestione delle commissioni.

Inoltre, nel caso di una banca, è ovvio che gli impiegati allo sportello delle banche vengono spesso spostati da una filiale all'altra e perciò è necessario assegnare dinamicamente nel tempo la 'cassa' di lavoro.

Il problema di autenticare ed individuare un utente del proprio sistema informatico è ovviamente presente anche nella stessa banca e sicuramente già risolto nell'ambito dei propri sistemi informatici. Occorre dunque individuare un modo per evitare il rilascio di credenziali aggiuntive da parte del Comune e di difficile gestione per i motivi sopra descritti.

Soluzioni già sviluppate

Per risolvere tutti questi problemi sono state sviluppate già alcune soluzioni che differiscono tra loro solo per la codifica dei token di identificazione che le banche ci possono fornire (dipende dal loro sistema di autenticazione e dalle modalità di cifratura che questi possono o vogliono utilizzare). Nel token devono essere indicati:

- cognome e nome dell'utente
- codice interno della filiale dalla quale si sta collegando
- codice ABI della banca
- identificativo univoco dell'utente bancario (tipicamente la matricola)
- data e ora della richiesta
- una firma (HASH) della stringa contenente i dati sopra citati (x controllo)

Le modalità con cui la firma è ottenuta e sulla cifratura del token possono variare ma devono essere tali da garantire l'autenticità del token (e della sua origine).

La banca deve comunicare a priori:

1. elenco delle filiali da attivare corredate di codice ABI, CAB e codice filiale con il quale identificate univocamente la filiale-sede. Ci è infatti capitato per alcune banche avessero più "filiali-sedi" con lo stesso CAB e quindi questo non era sufficiente per capire dove stava operando il cassiere. Il codice filiale è utilizzato nel token per comunicarci dove l'operatore sta lavorando in quel momento.
2. numero approssimativo dei vostri operatori che utilizzeranno il t-serve
3. indirizzi IP di provenienza

Per la realizzazione del single sign-on occorre seguire le specifiche seguenti:

esempio di Url per chiamata (ad ogni banca verrà comunicato un URL specifico):

https://as-https.ssgu.po-net.prato.it/Auth/moduli/BridgeNomeBanca.jsp?token=

dove token può passare in chiaro insieme all'hash oppure criptato e comunque deve rispettare la seguente struttura:

ffff;aaaa;mmmm;AAA-MM-GG;hh:mi:ss;nnnn;cccc;XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Il separatore è ;

Il significato dei campi è il seguente:

ffff - filiale massimo 10 caratteri (lettere o numeri)

aaaa - codice ABI della banca 5 cifre (per crsm credo sia 06300)

mmmm - matricola utente secondo codifica della banca massimo 100 caratteri (lettere o numeri)

AAA-MM-GG - data richiesta nel formato indicato

hh:mi:ss - ora richiesta (ore, minuti, secondi)

nnnn - nome utente

cccc - cognome utente

una firma (HASH) della stringa contenente i dati sopra citati (x controllo)

Tipi di implementazioni

- L'hash di controllo e di tipo MD5.
- Il token non viene cifrato ma esiste una chiave simmetrica (un segreto) che viene aggiunta al token prima di hasharlo

Il token passa in chiaro con l'HASH in formato esadecimale

es: 001;06300;MAT00AA;2010-10-13;12:54:10;Fabrizio;Isidori;ffcf64bc5475987bf2a97d7963d911df

Qualora si utilizzi un token cifrato:

- L'hash di controllo e di tipo SHA1.
- Il token viene cifrato con chiave asimmetrica (secondo un algoritmo RSA del qual ci hanno loro fornito l'implementazione).
- Il token viene formalizzato in BASE64 per poter essere trasmesso nella richiesta web

Conclusioni

Nel presente documento si sono fornite alcune indicazioni circa:

- le modalità di interazione tra la normale attività di sportello della banca e le operazioni T-serve;

- le procedure da seguire per gestire l'intero iter di incasso attraverso il T-serve;
- l'integrazione tra T-serve ed attività di tesoreria
- possibili integrazioni tra il sistema di autenticazione informatica della banca e quello del T-serve al fine di ridurre le problematiche di gestione delle credenziali per quest'ultimo

Tali informazioni tecniche sono da ritenersi puramente indicative ed esemplificative di situazioni già gestite.

Con l'Istituto che si aggiudicherà la fornitura del servizio di tesoreria saranno organizzate delle riunioni tecniche specifiche, tra il servizio sistema informativo del Comune ed i tecnici informatici della banca, per definire la migliore strategia realizzativa della integrazione dei due sistemi di autenticazione. Non vi è dunque preclusione, da parte del Comune, per soluzioni alternative a quelle indicate purché nel rispetto della normativa vigente e nella garanzia del mantenimento dei livelli di sicurezza ritenuti necessari.