Allegato 02 alla Delibera G.C. n. _____ del

RA COMPUTER
SIA Group

TesoWebSign

Servizio per la gestione degli ordinativi informatici locali
OIL

Allegato Tecnico

SISTEMA DI GESTIONE PER LA QUALITÀ CERTIFICATO UNI EN ISO 9001:2008
SINCERT DNV

REDAZIONE

Revisione	Redatto da	Funzione	Data	Approvato da	Funzione	Data
00	*M.Melegari*	*Web Developer*	*05/09/11*	*A.Speranza*	*PM Web*	*07/09/11*
01	*A.Speranza*	*PM Web*	*15/09/2011*			

REVISIONI

Revisione	Descrizione
01	*Aggiornamento per circolare Abi n.30 del 05/08/2011*

INDICE

1 INTRODUZIONE

1.1 Oggetto

Il presente documento contiene l'Analisi Tecnica relativa ad una particolare applicazione da sviluppare nel progetto Ordinativo Informatico per la Banca Tesoriera. Con il termine mandato informatico o Ordinativo Informatico Locale (OIL) si intende l'insieme delle risorse informatiche ed organizzative necessarie per l' automazione dell'iter amministrativo adottato dagli Enti Locali per l'ordinazione delle entrate e delle spese all'Istituto Tesoriere. L'OIL rappresenta il modello di collaborazione e di coordinamento tra Stato Centrale ed autonomie locali.
La soluzione proposta dalla Banca, denominata "*TesoWebSign*", risolve a pieno tutte le tematiche precedentemente descritte, nel rispetto della circolare ABI numero 80 del 29/12/2003 e successivi aggiornamento circolare ABI numero 35 del 8/2008 e circolare ABI numero 30 del 05/08/2011.

1.2 Definizioni

Acronimo/Termine	Testo esplicativo della definizione
ASP	Application Service Provisioning
API	Application Programming Interface
CA	Certification Authority
CRL	Certificate Revocation List
Ente	Ente Locale e/o Pubblica Amministrazione Locale
Ordinativo informatico	Mandati di pagamento e reversali di incasso informatici

2 DESCRIZIONE GENERALE

1.1 Identificazione e scopo del servizio/prodotto

Il servizio è realizzato dalla Banca Tesoriera con le componenti applicative periferiche e quelle erogate centralmente presso un'apposita Server Farm.

Il servizio erogato in modalità ASP ed accessibile tramite un portale internet, permette di gestire l'Ordinativo Informatico snellendo l'iter amministrativo, elevando i livelli di sicurezza, efficacia ed efficienza, minimizzando l'impatto presso gli enti e mantenendo la massima interoperabilità con le applicazioni di Tesoreria esistenti.

La soluzione di seguito illustrata si basa su un'architettura che prevede l'Invio e la Ricezione dei flussi verso e dalla Banca Tesoriera tramite un protocollo di comunicazione condiviso tra Ente e Banca Tesoreria.

3 Caratteristiche del Servizio

1.2 Il contesto di riferimento

Il servizio per la Gestione degli ordinativi informatici degli Enti Pubblici (nel seguito "Servizio") è nato dalla necessità di realizzare una soluzione per l'Ordinativo Informatico di Incasso e Pagamento, con la finalità di soddisfare le crescenti esigenze di soluzioni innovative da parte delle Pubbliche Amministrazioni e delle relative Banche Tesoriere.

La gestione dell'Ordinativo Informatico, in particolare, raggiunge i seguenti obiettivi:

- Certezza delle informazioni
- Efficacia dei controlli
- Rapidità dei pagamenti
- Dematerializzazione dei titoli di spesa.

1.3 Il servizio di Gestione dell'Ordinativo Informatico

Il servizio costituisce per le Banche Tesoriere e gli Enti Pubblici Locali una **soluzione completa** per la gestione degli ordinativi informatici intesi come mandati di pagamento e reversali di incasso.

Grazie all'informatizzazione delle procedure, IL SERVIZIO PER LA GESTIONE DEGLI ORDINATIVI INFORMATICI fornisce a Enti Pubblici e Banche Tesoriere l'opportunità di snellire l'iter amministrativo nel pieno rispetto dei loro processi organizzativi, elevando il livello di **sicurezza**, **efficacia** ed **efficienza**.

Il servizio di gestione dell'ordinativo informatico erogato in modalità ASP permette di conseguire **obiettivi strategici**, quali:

- riduzione di risorse per la gestione amministrativa dei servizi di tesoreria/cassa;
- un servizio innovativo e tecnologicamente avanzato;
- l'eliminazione del rischio di errore umano;

con **benefici immediati**:

- limitati investimenti iniziali;
- tecnologia e know-how sempre aggiornati;
- riduzione dei tempi di attivazione e implementazione;
- costi variabili;
- massima affidabilità e sicurezza;

1.4 Le funzionalità

In particolare sono rese disponibili le seguenti macro-funzionalità:

a) lato Ente

- Automazione e gestione del processo di workflow di generazione dell'ordinativo informatico, di apposizione delle firme (gestione integrata della sequenza dei firmatari, del grado di urgenza, eventuali annotazioni, etc.)
- Gestione informatica dei documenti;
- Integrazione con firma digitale qualificata;
- Gestione dell'invio sicuro dell'ordinativo informatico presso la Banca Tesoriera;

b) lato Banca

- Gestione automatica della verifica della firma digitale degli ordinativi informatici;
- Gestione dei poteri di firma con le casistiche tradizionalmente previste: firma congiunta, firma disgiunta, combinazioni di firma, importo massimo di spesa per combinazioni di firma;
- Gestione dell'invio da parte della Banca Tesoriera degli esiti applicativi;
- Monitoraggio stato dei flussi ricevuti

Il servizio presenta inoltre le seguenti caratteristiche:

- Minimo impatto verso il sistema di contabilità dell'Ente Locale e della Banca Tesoriera. La soluzione è pensata per utilizzare aree dati (o tabelle) di interfacciamento.
- Permette la gestione dell'ordinativo informatico secondo il workflow approvativo utilizzato dall'Ente Locale
- Utilizzo della firma digitale qualificata, a supporto dell'intero workflow approvativo, per rendere intrinsecamente sicuri i documenti firmati.
- Fruizione delle funzionalità da parte dell'utente in modalità web con l'utilizzo dei massimi livelli di sicurezza disponibili, grazie al protocollo SSL a 128bit.

2 Descrizione delle Funzionalità

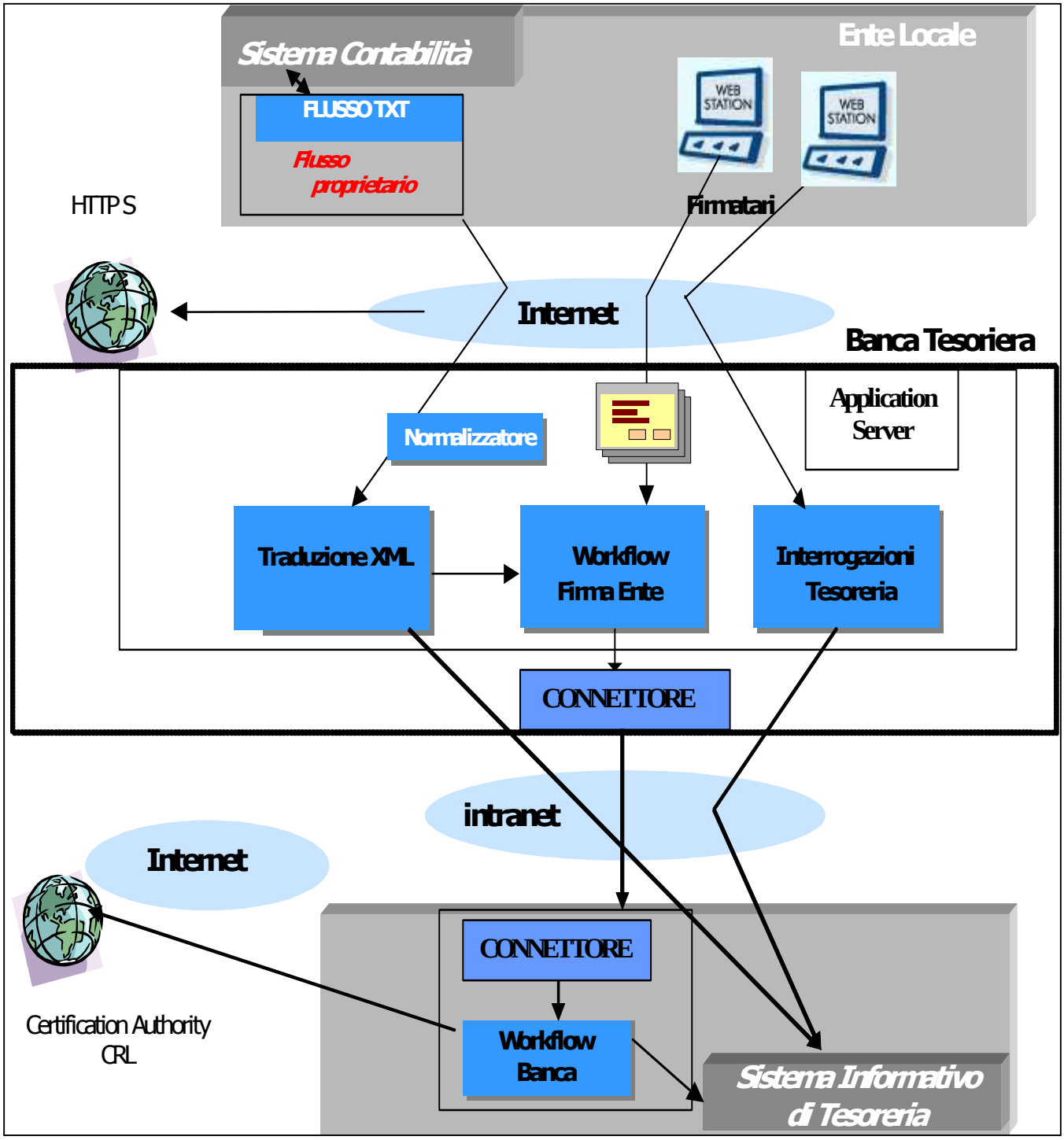


Figura 1 - Componenti logiche del Servizio

2.1 Servizi disponibili

2.1.1 Acquisizione del documento dalla contabilità dell'ente

Per poter ricevere ordinativi dall'Ente, la modalità di acquisizione dei flussi, che deve essere condivisa prima delle spedizioni dei documenti tra Ente e Banca, è costituita dalla funzionalità di "**Upload"**, sempre via HTTPS ma in modalità sicura, nella quale l'utente autorizzato, tramite il proprio browser, invia all'Application Server un file degli ordinativi dal proprio PC. Questa modalità prevede che vengano condivise tutte le specifiche di comunicazione (formato flusso ed accesso) tra Ente e Banca.

I requisiti sono:

1. Accesso ad Internet dalla propria postazione di lavoro;
2. Disponibilità sulla propria postazione di lavoro del file dei documenti da inviare all'Application Server della Banca mediante browser ed utilizzando la funzione di upload appositamente predisposta. Il file deve essere realizzato secondo un tracciato concordato.

2.1.2 WorkFlow lato Ente

La funzione di apposizione della Firma digitale nell'iter di approvazione dell'Ordinativo Informatico, prevede che le postazioni dell'Ente coinvolte siano dotate, oltre che di browser di ultima generazione e di un collegamento standard alla rete internet, anche di apposito Kit di Firma abilitato all'apposizione della Firma Digitale Qualificata secondo norme DigiPA (ex-CNIPA).

Le funzionalità dell'applicazione permettono agli utenti di svolgere diversi ruoli, cui sono demandati i relativi compiti ed autorizzazioni:

- Responsabile dei documenti:
  1) definisce il workflow di approvazione e firma dei documenti (in modo manuale per ogni documento)
  2) può completare i documenti con dati ausiliari (esclusivamente aggiunta di note)
  3) invia i documenti "alla firma", ovvero attiva il workflow per la sottomissione ai firmatari
  4) può monitorare lo stato di avanzamento dei documenti in workflow (in evidenza le scadenze urgenti e le firme in ritardo)

5) può monitorare lo stato dei documenti inviati alla banca (stati di trasmissione, accettazione e pagamento)
6) gestisce eventuali anomalie di percorso (re-importazione di documenti sbagliati, documenti rifiutati da Firmatario, documenti non accettati dalla Banca)

- Firmatario
  1) visualizza la lista dei documenti da firmare
  2) può controllare singolarmente il contenuto di ogni documento
  3) può rifiutare la firma in caso di difformità rilevate (in questo caso vengono automaticamente avvisati il Responsabile ed altri Firmatari precedenti)
  4) firma ogni singolo documento (per mezzo di una selezione multipla l'utente attiva la funzione in modo cumulativo, ma le firme digitali sono automaticamente apposte ad ogni documento)
  5) in modo implicito, quando firma, passa il documento allo stato di workflow successivo, con ciò abilitando altri Firmatari o completando il documento (l'operazione potrebbe eventualmente "scaricare" Firmatari paralleli che avevano pari diritti di firma)

La gestione dei documenti e la loro presentazione via web è basata su XML, permettendo una totale indipendenza dell'applicativo dal "tracciato" specifico definito tra banca ed ente.

2.1.3 Application Server Centrale

Il Servizio Gestione degli ordinativi informatici sarà erogato centralmente in modalità ASP, dalla Banca Tesoriera.

L'Application Server gestisce il dialogo verso tre fronti:

1. **Lato PA-Ente Locale**:
   con una connessione IP HTTPS viene utilizzata dai singoli utenti per importare i documenti che verranno convertiti in ordinativi XML Abi compliant.
2. **Lato WEB**:
   Il sistema è un'applicazione WEB ultra-thin-client. Tutti gli utenti si collegano attraverso pagine dinamiche e interagiscono con il sistema per mezzo di un normale browser. In particolare gli utenti firmano digitalmente via WEB i documenti elettronici generati nel sistema.

Sono attualmente disponibili tutte le principali funzionalità di Inquiry relative allo stato dei documenti emessi, i vari step del workflow approvativo e lo stato delle ricevute di servizio o applicative (Situazione Bancaria).

Il server applicativo ha quindi un fronte esposto su Internet.

3. **Lato Banca**:

   Il sistema trasmette alle banche gli ordinativi informatici con firma digitale e riceve esiti applicativi di riscontro firmati digitalmente.

2.1.4 Erogazione via WEB del Servizio e modalità di accesso

Il Servizio è fruibile via Internet accedendo al sito https://www.bpmbanking.it.

La fruizione del Servizio avviene unicamente in modalità HTTPS con SSL v.3 a 128bit.

L'accesso è consentito ai soli utenti registrati ed autorizzati, con l'autenticazione di tipo basic auth (username/password). In questa fase vengono realizzati dei progetti specifici di Single Sign On con i sistemi di autenticazione e sicurezza della Banca.

2.1.5 Workflow lato Banca: Componente Firma Remota

La componente WorkFlow Banca richiede il vincolo, della predisposizione lato Banca, di una componente di "*Firma Remota*". La gestione della "*Firma Remota*", permette di abbandonare le soluzioni di firma basate sui dispositivi personali (smartcard e token USB) a favore di architetture centralizzate in apparati di Hardware Security Module (HSM), i quali possono ospitare le credenziali di un'intera comunità di utenti. La gestione centralizzata permette di ottimizzare i costi e di minimizzare le problematiche di supporto e assistenza, in quanto tutte le operazioni critiche (es. scadenza, rinnovo, emissione etc.) possono essere svolte in un ambiente noto e ben configurato.

La normativa Italiana sulla firma digitale permette l'uso di soluzioni di firma qualificata a valenza legale che prevedano l'uso di chiavi crittografiche generate e a bordo di un dispositivo HSM (certificato Common Criteria EAL4+). L'HSM può essere installato remotamente e sostituisce a pieno titolo il dispositivo personale direttamente gestito dall'utente (smartcard o token).

Il WorkFlow Banca permette di effettuare le operazioni di firma automatica (massiva) di tutte le ricevute previste dalla circolare ABI (il formato è descritto nei paragrafi successivi di questo documento), utilizzando lo strato software di interfaccia applicativa predisposto dai diversi vendor

presenti sul mercato, e che permettono l'utilizzo del/i certificati digitali presenti nel HSM dei soggetti delegati dalla Banca Tesoriera ad effettuare tale operazione.

Il WorkFlow Banca, alla data di stesura del presente documento, è stato implementato per integrarsi con lo strato software applicativo dei seguenti fornitori presenti sul mercato:

- PKBOX Intesi Group (.net e Java);
- ACTALIS ELLIPSE 1, 2, X;
- ACTALIS BBF;
- INFOCAMERE (IC 1.x);
- TELECOM FSM.

Le soluzioni, dei vari vendor, mettono a disposizione diverse operazioni applicative, tra cui:

- Apposizione firma digitale e firma digitale qualificata (firma con imbustamento PKCS#7 attached)
- Apposizione firma digitale e firma digitale qualificata (firma con imbustamento PKCS#7 detached)
- Verifica firma digitale e verifica firma digitale qualificata (verifica della CRL, verifica via Online Certificate Status Protocol)
- Richiesta apposizione marca temporale
- Verifica marca temporale
- Verifica marca temporale sul documento marcato
- Crittografia e decrittografia
- Conversione buste PKCS#7 attached < -- > buste PKCS#7 detached

Inoltre, ciascuna di esse mette a disposizione delle interfacce applicative, in diversi canali di integrazione, per l'interfacciamento alle funzioni offerte, principalmente tramite:

- Canale HTTP/S
- Canale MQ
- Web Service

Tutte le operazioni di richiesta dei certificati digitali, emissione, gestione (scadenza, rinnovo) ecc., sono specifiche dei diversi vendor di soluzione integrate HSM e delle relative CA emittenti.

Pertanto, gli applicativi RA non hanno alcun coinvolgimento o impatto su tali processi gestionali e tecnologici.

2.1.6 Workflow lato Banca: Moduli

Il Workflow Banca è costituito, dal punto di vista logico, da vari moduli SW che svolgono le seguenti funzioni:

a) Modulo Connettore :
   - ricezione via protocollo condiviso del file degli ordinativi firmati.
   - invio all'Application Server delle ricevute di servizio ed applicative

b) Modulo AUTHENTICATION per la verifica della correttezza ed autenticità della firma. In particolare viene eseguito un controllo sintattico dell'XML ricevuto, viene verificata l'integrità del documento firmato, viene identificato il firmatario e viene verificato che il relativo certificato non sia presente nella CRL della CA. Prerequisito di quest'ultima attività e' la possibilità di accesso alla CRL pubblicata dalla relativa Certification Authority.

c) Modulo AUTHORIZATION per la verifica che l'identità di chi ha firmato l'ordinativo corrisponda a chi ha effettivamente i poteri di firma per quell'Ente (Specimen).
   Deve essere adibita allo scopo una base dati su HOST. Il Tesoriere della Banca dovrà, su richiesta scritta dell'Ente, censire nella procedura di Tesoreria i certificati emessi dalla Certification Authorithy validi per la firma degli Ordinativi Informatici, relativi alle persone autorizzate e, successivamente, dovrà censire i "poteri di firma" combinando opportunamente i certificati, fino ad un massimo di 4 firme congiunte, ed i limiti di spesa.

d) Modulo di Denormalizzazione flusso: al termine delle verifiche, deposita gli ordinativi informatici nel repository secondo un tracciato record prestabilito. Una componente progettuale di personalizzazione prevede una fase di conversione dal tracciato XML al tracciato proprietario di tesoreria, e una fase di integrazione dati secondo le regole procedurali della banca tesoriera.

e) Modulo per la firma lato Banca delle ricevute applicative generate dall'Applicazione di Tesoreria: esito al carico ed esito all'esecuzione contabile (pagamenti e riscossioni).

f) Funzione di interrogazioni sullo stato dei flussi ricevuti.

2.2 Produzione di ricevute di servizio/ esito applicativo

Il Sistema è predisposto per produrre le seguenti ricevute:

- una ricevuta di servizio per pacchetto (gruppo di ordinativi presenti nel flusso non necessariamente collegati), prodotta dalla componente WFBanca. La ricevuta di servizio contiene l'esito positivo nel caso di superamento di tutte le verifiche eseguite dall' WFBanca, od eventualmente le segnalazioni degli errori nel caso contrario.

- Ricevuta applicativa di esito al carico : viene prodotta una ricevuta sia per i documenti caricati correttamente nella procedura di Tesoreria della Banca sia per quelli scartati per errori nei controlli di merito.
- Ricevuta applicativa di esito all'esecuzione contabile : viene prodotta una ricevuta applicativa di quietanza per ogni sub processato.

L'apposizione della firma automatica sulle ricevute da parte del Tesoriere è configurabile, eventualmente rispecchiando gli accordi stipulati nella convenzione tra Banca ed Ente.

3 FUNZIONALITA' GESTITE

Le funzionalità gestite sono:

- l'inserimento
- l'annullo
- la variazione
- la sostituzione
- il reinvio

Ogni singola operazione è individuata da codice ente, numero del mandato o della reversale, progressivo, esercizio, data di emissione da parte dell'Ente e funzione richiesta.

Qualunque sia la funzionalità che si richiede, ogni operazione deve essere completa di tutti i dati, sia quelli previsti dalla legge che quelli necessari a eseguire l'ordinativo.

Nel tracciato allegato, da utilizzare per ogni tipo di richiesta, ogni dato riporta l'informazione di facoltativo o obbligatorio, oltre ad una breve spiegazione del contenuto.

3.1 Inserimento

L'ente esprime la richiesta di pagamento di un mandato o di incasso di una reversale indicando che si tratta di inserimento.

La modalità dell'operazione è fornita tramite un codice ed una specifica descrizione cui devono corrispondere i dati necessari ad espletare l'operazione di pagamento o riscossione.

Gli ordinativi sono sottoposti a controlli di congruenza. Se risultano errati, vengono scartati dal tesoriere.

Per ogni ordinativo l'Ente può indicare la data nella quale lo stesso deve essere messo in pagamento o riscossione, sempre previo accordo col Tesoriere.

Per ogni richiesta di inserimento è prodotta una ricevuta applicativa che riporta i dati identificativi dell'ordinativo, un codice che esprime l'esito dell'operazione e, nel caso di esito negativo un codice di errore condiviso oltre alle descrizioni delle segnalazioni di errore.

3.2 Annullo

L'ente può richiedere di annullare un mandato non ancora pagato o una reversale non ancora riscossa. I dati inviati devono essere completi e uguali a quelli dell'ordinativo già emesso che si vuole annullare.

Questa operazione deve sempre seguire un'operazione di inserimento o di esecuzione per la quale il Tesoriere abbia rilasciato una ricevuta applicativa con esito negativo.

Al messaggio di annullo segue una ricevuta applicativa che riporta l'esito dell'operazione, analogamente a quanto previsto per l'inserimento.

3.3 Variazione

Gli ordinativi informatici, ovvero le singole disposizioni in essi contenute non ancora eseguite, possono essere variati prima della loro estinzione.

E' consentita la variazione per la correzione di elementi non essenziali ai fini della validità e della regolarità dell'operazione di tesoreria e/o di cassa già eseguita e della quietanza.

È consentita la sostituzione per la correzione di elementi non essenziali ai fini della validità e della regolarità dell'operazione di tesoreria e/o di cassa già eseguita e della quietanza.

3.4 Sostituzione

È consentita la sostituzione per la correzione di elementi non "essenziali" ai fini della validità e della regolarità dell'operazione di tesoreria e/o di cassa già eseguita e della quietanza.

La gestione delle sostituzioni è sottoposta ai seguenti vincoli:

1. è ammessa la sostituzione di un ordinativo solo se l'ordinativo da sostituire esiste in TesoWeb Sign ed è stato completamente eseguito (altrimenti sarebbe una variazione);
2. un ordinativo completamente eseguito può essere sostituito con uno o più ordinativi dello stesso tipo (non si può sostituire un mandato con una reversale o viceversa);
3. non sono ammesse sostituzioni di tipo *da molti a molti* (ossia non possono essere sostituiti due o più ordinativi con due o più ordinativi);
4. non sono ammesse sostituzioni parziali o squadrate, ossia la somma degli importi dei documenti sostituenti deve essere congruente con l'importo del documento sostituito;
5. gli ordinativi che sostituiscono un ordinativo devono essere tutti presenti in unico file (flusso T2003 spedito dall'ente);
6. gli ordinativi che sostituiscono un ordinativo devono essere tutti inviati, dall'utente finale, attraverso un unico pacchetto (struttura contenete documenti firmati digitalmente, da passare al WFBanca);

7 se tutti gli ordinativi che sostituiscono un ordinativo saranno presenti in un unico pacchetto questi verranno tutti inviati ad host attraverso la componente di WFBanca;
8 non saranno eseguiti ulteriori controlli di validità sul documento di sostituzione al di fuori della quadratura con il sostituito;
9 un ordinativo sostituito non viene invalidato, ma subisce una variazione di stato (sostituito);
10 un ordinativo sostituito non può essere annullato o variato;
11 non sono ammesse variazioni o annulli di documenti di sostituzione (eventuali rettifiche saranno gestite con un nuovo documento di sostituzione che sostituisce il precedente documento di sostituzione)
12 le ricevute (di servizio ed applicative) di un ordinativo sostituito rimarranno collegate logicamente all'ordinativo a cui si riferiscono;
13 un ordinativo di sostituzione avrà le sue ricevute di ricezione, di acquisizione o rifiuto;
14 un ordinativo di sostituzione non avrà ricevute applicative di esecuzione.

3.5 TIPOLOGIE DI ERRORE:

L'elenco minimo delle tipologie di errore che devono essere garantite dalla procedura sono quelle di seguito riportate; la codificazione delle stesse verrà effettuata in collaborazione con l'Istituto Tesoriere

- ANNO COMPETENZA ERRATO
- DESCRIZIONE CAUSALE ASSENTE
- TIPO PAGAMENTO/INCASSO ERRATO
- BENEFICIARIO/VERSANTE ASSENTE
- C/C POSTALE ASSENTE
- INDICATIVO SPESE ERRATO
- SPESE ERRATE
- ABI ASSENTE O ERRATO
- CAB ASSENTE O ERRATO
- INDIRIZZO BENEFICIARIO ERRATO O MANCANTE
- C/C BENEFICIARIO ERRATO
- DATI RELATIVI AL TIPO PAGAMENTO/RISCOSSIONE NON PRESENTI
- ABI-CAB ERRATO O INESISTENTE
- NUMERO DOCUMENTO ASSENTE
- RECORD DOPPIO
- TIPO ESECUZIONE ERRATO
- IMPORTO NEGATIVO O NON NUMERICO
- COD. ABI NON CONGRUENTE CON TIPO ESECUZIONE
- DOCUMENTI DA ANNULLARE CON IMPORTO ERRATO
- DOCUMENTO DA VARIARE GIA PAGATO
- ORDINATIVI INFORMATICI NON PREVISTI PER ENTE
- TIPO FLUSSO ERRATO
- ORDINATIVO INESISTENTE

Si precisa in maniera univoca che tutti tracciati (pacchetto, ordinativo, ricevute ed xsd) allegati al seguente disciplinare, con i relativi vincoli di valorizzazione, sono da considerarsi soggetti a cambiamenti di carattere normativo e/o funzionale, previa condivisione ed accettazione da entrambi gli attori coinvolti nel processo (Banca Tesoriera ed Ente) di ordinativo informatico.

Nel caso di anomalie relative al flusso, il medesimo è rifiutato;
Nel caso in cui l'anomalia sia rilevata a livello di ordinativo informatico, la BT non sospende l'elaborazione degli eventuali ordinativi informatici privi di anomalie presenti nel medesimo «flusso». La comunicazione delle anomalie rilevate a livello di ordinativo informatico avviene mediante il "messaggio di esito applicativo" per il rifiuto dell'ordinativo (precisiamo che, per gli ordinativi con più versanti o beneficiari, a fronte di anomalie riscontrate su un singolo versante o beneficiario viene rifiutato l'intero ordinativo).
L'ordinativo informatico "errato", non acquisito dalla BT, potrà essere ritrasmesso dalla PA, privo di anomalie, come un nuovo ordinativo informatico, all'interno di un successivo «flusso».
La PA analizza le anomalie comunicate dalla BT e decide, nell'ambito del proprio sistema informatico e contabile, se riproporre, come un nuovo ordinativo, l'ordinativo informatico contenente anomalie ovvero annullarlo all'interno del proprio sistema.

4 Tracciati

Le colonne genere e o/f hanno i seguenti significati:
colonna genere
- s: dato struttura che può contenere altre strutture o dati
- an: dato alfanumerico
- n: dato numerico

colonna o/f
- o: dato sempre obbligatorio
- f: dato facoltativo (gli elementi facoltativi sono da intendersi obbligatori in base alla natura dell'ente ovvero alle specifiche esigenze e caratteristiche dell'operazione).

4.1 Pacchetto

Dato	genere	o/f	contenuto
Flusso_ordinativi	s	o	Aggregazione di dati che contiene tutti i dati del flusso.
Codice_ABI_BT	n	o	Codice ABI della banca destinataria del flusso trasmesso.
identificativo_flusso	An	o	Codice alfanumerico attribuito univocamente al flusso inviato da parte della PA. (es. MIUR

			[Anno in formato SSAA] [Mese in formato MM] [Progressivo distinta mensile 5 cifre] [Tipo Distinta: T/S/A (Titoli/Annullamenti/Storni)])
data_ora_creazione_flusso	An	f	Indica la data e l'ora di creazione del flusso nel formato "**SSAA-MM-GGTHH:MM:SS"** secondo il formalismo ISO 8601.
Codice_ente	An	o	Può contenere il codice istat relativo ad un ente, il codice R.G.S., il codice fiscale o la partita IVA, il codice SIA, ecc.
descrizione_ente	An	o	Contiene la denominazione della PA.
Codice_ente_BT	An	o	Codice univoco interno, attribuito dalla BT, per mezzo del quale la PA è riconosciuta dalla banca medesima.
riferimento_ente	An	f	Eventuale codice concordato tra PA e BT per particolari esigenze
Esercizio	N	o	Indica l'anno d'esercizio finanziario o contabile, nel formato "**SSAA**

4.2 Reversale

Dato	**genere**	**o/f**	**contenuto**
reversale	S	f	Aggregazione di dati che contiene i dati di una singola reversale. In presenza di più reversali la struttura può essere ripetuta più volte.
Tipo_operazione	An	o	Può assumere i seguenti valori: • "**INSERIMENTO**" • "**VARIAZIONE"** • "**ANNULLO"** • "**SOSTITUZIONE"**
numero_reversale	An	o	Indica il numero della reversale a cui fanno riferimento i dati che seguono.
data_reversale	An	o	Indica la data di emissione della reversale da parte della PA, nel formato "**SSAA-MM-GG**" secondo il formalismo ISO 8601.
Importo_reversale	N	o	Campo numerico (due cifre per la parte decimale, il separatore dei centesimi è il punto "**.**"), indicante l'importo della reversale in oggetto. Non può assumere valore negativo.
conto_evidenza	An	f	Conto evidenza concordato tra la PA e la BT
bilancio	S	f	Rappresenta un'aggregazione di dati opzionali, che può essere ripetuta più volte. È costituita dai seguenti elementi
codifica_bilancio	An	o	Identifica il codice bilancio. Obbligatorio se è prevista la gestione del bilancio.
descrizione_codifica	An	f	Descrizione del codice di bilancio in esame.

Gestione	A	o	Può assumere i valori **RESIDUO** o **COMPETENZA**
anno_residuo	n	f	Indica l'anno residuo, nel formato "**SSAA**".
numero_articolo	n	f	Indica il numero dell'articolo.
voce_economica	n	f	Indica la voce economica.
importo_bilancio	n	f	Campo numerico (due cifre per la parte decimale, il separatore dei centesimi è il punto "**.**"), indicante l'importo relativo al codice bilancio e articolo precedentemente indicati. Nel caso di gestione con multicapitolo la somma degli importi di tutti i capitoli indicati deve essere uguale all'importo della reversale. Non può assumere valore negativo.
informazioni_versante	s	o	Aggregazione di dati che contiene tutti i dati di un singolo versante, in presenza di più versanti la struttura può essere ripetuta più volte. I dati contenuti nella struttura sono dettagliati nella sezione "2.1 Informazioni versante".
dati_a_disposizione_ente_reversale	s	f	Struttura finalizzata ad accogliere informazioni utilizzate ad uso esclusivo dalla PA per rendere completo il documento informatico. Contiene strutture e informazioni definite internamente da ciascuna PA, i dati contenuti in questa struttura vengono ignorati dalla BT.

4.3 Informazioni Versante

dato	genere	o/f	contenuto
informazioni_versante	s	o	Aggregazione di dati che contiene tutti i dati di un singolo versante, in presenza di più versanti la struttura può essere ripetuta più volte.
progressivo_versante	n	o	Indica il numero progressivo del versante all'interno dello stesso ordinativo.
Importo_versante	n	o	Campo numerico (due cifre per la parte decimale, il separatore dei centesimi è il punto "**.**"), indicante l'importo relativo al versante in oggetto. Non può assumere valore negativo.
tipo_riscossione	a	o	Può assumere i seguenti valori: • "CASSA" • "ACCREDITO BANCA D'ITALIA • "REGOLARIZZAZIONE" • "REGOLARIZZAZIONE ACCREDITO BANCA D'ITALIA" • "PRELIEVO DA CC POSTALE"

Numero_ccp		n	f	Indica il numero di conto corrente postale da utilizzare con il tipo_riscossione “PRELIEVO DA CC POSTALE”.
tipo_entrata		a	f	Può assumere i valori **FRUTTIFERO** o **INFRUTTIFERO**.
	Destinazione	a	f	Può assumere i valori **LIBERA** o **VINCOLATA**
Classificazione		s	f	L'indicazione congiunta del "codice CGE"- Unità Elementare Statistica/UES - va ripetuta tante volte fino al raggiungimento dell'importo totale per versante.
	codice_cge	n	o	Codice associato ad ogni ordinativo di incasso facente riferimento al 3° livello del Piano Unico dei Conti in uso nel Sistema di Contabilità Economica Analitica delle Amministrazioni Pubbliche.
	Importo	n	o	Campo numerico (due cifre per la parte decimale, il separatore dei centesimi è il punto “**.**”), indicante l’importo associato al codice CGE. Non può assumere valore negativo.
bilancio		s	f	Rappresenta un’aggregazione di dati opzionali, che può essere ripetuta più volte. E’ costituita dagli elementi già descritti nella sezione “reversale”.
Bollo		s	o	Aggregazione “bollo” costituita dai seguenti elementi:
	assoggettamento bollo	a	o	Può assumere i valori • “**ESENTE BOLLO**” • “**ASSOGGETTATO BOLLO A CARICO ENTE”** • **“ASSOGGETTATO BOLLO A CARICO VERSANTE”.** • **NON APPLICABILE**
	causale_esenzione_bollo	an	f	Motivazione dell’esenzione dall’imposta di bollo. Le causali sono in alternativa tra le seguenti: • Finanziamenti dallo Stato, • Finanziamenti dalla Regione, • Finanziamenti da Enti locali o da altre istituzioni pubbliche.
Versante		s	o	Aggregazione “versante” costituita dai seguenti elementi:
	anagrafica_versante	an	o	Indica il nominativo o la ragione sociale del versante.
	indirizzo_versante	an	o	Indica l’indirizzo del versante.
	cap_versante	an	o	Indica il CAP del versante (sedici caratteri).
	localita_versante	an	o	Indica la località del versante. Impostare il comune di residenza
	provincia_versante	an	o	Indica la provincia del versante.
	stato_versante	an	f	Indica lo Stato del versante. Da valorizzare con il codice paese da 2 caratteri (IT, ecc.) come

				indicato nelle specifiche SEPA.
	partita_iva_versante	n	f	Campo numerico di trentacinque caratteri contenente la partita IVA del versante.
	codice_fiscale_versante	an	o	Campo alfanumerico di trentacinque caratteri contenente il codice fiscale del versante.
causale		an	o	Rappresenta la descrizione estesa della causale dell'incasso.
sospeso		s	f	Aggregazione "sospeso", la struttura è ripetibile più volte, indicante la presenza di provvisori sospesi.
	numero_provvisorio	n	o	Indica il numero del provvisorio sospeso, oggetto di regolarizzazione.
	importo_provvisorio	n	o	Indica l'importo da regolarizzare (totale o parziale) del provvisorio sospeso, precedentemente indicato. Non può assumere valore negativo.
mandato_associato		s	f	Raggruppamento di informazioni composto da:
	numero_mandato	an	o	Eventuale numero del mandato al quale è associato il versante.
	progressivo_beneficiario	n	o	Riferimento all'eventuale beneficiario all'interno del mandato precedentemente identificato, al quale è associato il versante.
informazioni_aggiuntive		s	f	Raggruppamento di informazioni, facoltative, composto da:
	lingua	a	f	Indica la lingua utilizzata per la stampa delle ricevute (ad esempio **ITALIANO**, **TEDESCO**), per le province che adottano il bilinguismo.
	riferimento_documento_esterno	an	F	Contiene il riferimento ad un documento esterno cartaceo o informatico.
sostituzione_reversale		s	f	Raggruppamento di informazioni utilizzata per la sostituzione di un documento, struttura da valorizzare in abbinamento con il tipo_operazione "SOSTITUZIONE". E' ammessa una sola occorrenza per ciascun versante.
	numero_reversale_da_sostituire	an	O	Numero della reversale da sostituire
	progressivo_versante_da_sostituire	n	o	Numero del versante da sostituire
	esercizio_reversale_da_sostituire	n	o	Esercizio di riferimento del documento sostituito, deve essere omogeneo con l'esercizio del flusso.
dati_a_disposizione_ente_versante		s	f	Struttura finalizzata ad accogliere informazioni utilizzate ad uso esclusivo dalla PA per rendere completo il documento informatico. Contiene strutture e informazioni definite internamente da ciascuna PA, i dati contenuti in questa struttura vengono ignorati dalla BT.

4.4 Mandato

dato	genere	o/f	contenuto
mandato	s	f	Aggregazione di dati che contiene tutti i dati di un singolo mandato. In presenza di più mandati la struttura può essere ripetuta più volte.
tipo_operazione	an	o	Può assumere i seguenti valori: • "**INSERIMENTO**" • "**VARIAZIONE"** • "**ANNULLO"** • **"SOSTITUZIONE"**
numero_mandato	an	o	Indica il numero del mandato a cui fanno riferimento tutti i dati che seguono.
data_mandato	an	o	Indica la data di emissione del mandato da parte della PA, nel formato "**SSAA-MM-GG**" secondo il formalismo ISO 8601.
importo_mandato	n	o	Campo numerico (due cifre per la parte decimale, il separatore dei centesimi è il punto "**.**"), indicante l'importo del mandato in oggetto. Non può assumere valore negativo.
conto_evidenza	an	f	Conto evidenza concordato tra la PA e la BT.
estremi_provvedimento_autorizzativo	an	f	Indica la tipologia e gli eventuali estremi del provvedimento di autorizzazione della spesa.
responsabile_provvedimento	an	f	Identifica il responsabile del provvedimento.
ufficio_responsabile	an	f	Eventuale indicazione dell'ufficio emittente.
bilancio	s	f	Rappresenta un'aggregazione di dati opzionali, che può essere ripetuta più volte. è costituita dai seguenti elementi:
codifica_bilancio	an	o	Identifica il codice bilancio. Campo obbligatorio se è prevista la gestione del bilancio.
descrizione_codifica	an	f	Descrizione del codice di bilancio in esame.
gestione	a	o	Può assumere i valori **RESIDUO** o **COMPETENZA.**
anno_residuo	n	f	Indica l'anno residuo, nel formato "**SSAA**".
numero_articolo	an	f	Indica il numero dell'articolo.
voce_economica	n	f	Indica la voce economica.
importo_bilancio	n	f	Campo numerico (due cifre per la parte decimale, il separatore dei centesimi è il punto "**.**"), indicante l'importo relativo al codice bilancio e articolo precedentemente indicati. Nel caso di gestione con multicapitolo la somma degli importi di tutti i capitoli indicati deve essere uguale all'importo del mandato. Non può

			assumere valore negativo.
funzionario_delegato	s	f	Aggregazione opzionale “funzionario_delegato”.
codice_funzionario_delegato	an	o	Indica il codice fiscale o altro codice concordato tra PA e BT del funzionario delegato.
importo_funzionario_delegato	n	o	Importo attribuito al funzionario delegato. Non può assumere valore negativo.
tipologia_pagamento_funzionario_delegato	an	o	Tipologia del pagamento funzionario delegato
numero_pagamento_funzionario_ delegato	an	o	Numero del pagamento attribuito al funzionario delegato
informazioni_beneficiario	s	o	Aggregazione di dati che contiene tutti i dati di un singolo beneficiario, in presenza di più beneficiari la struttura può essere ripetuta più volte. I dati contenuti nella struttura sono dettagliati nella sezione “3.1 Informazioni beneficiario”.
dati_a_disposizione_ente_mandato	s	f	Struttura finalizzata ad accogliere informazioni utilizzate ad uso esclusivo dalla PA per rendere completo il documento informatico. Contiene strutture e informazioni definite internamente da ciascuna PA, i dati contenuti in questa struttura vengono ignorati dalla BT.

4.5 Informazioni Beneficiario

dato	genere	o/f	contenuto
informazioni_beneficiario	s	o	Aggregazione di dati che contiene tutti i dati di un singolo beneficiario, in presenza di più beneficiari la struttura può essere ripetuta più volte.
progressivo_beneficiario	n	o	Indica il numero progressivo del beneficiario all’interno dello stesso ordinativo.
importo_beneficiario	n	o	Campo numerico (due cifre per la parte decimale, il separatore dei centesimi è il punto “**.**”), indicante l’importo relativo al beneficiario in oggetto. Non può assumere valore negativo.
tipo_pagamento	a	o	Può assumere i seguenti valori: • “**CASSA**” • “**BONIFICO BANCARIO E POSTALE**” • **“SEPA CREDIT TRANSFER”** • “**ASSEGNO BANCARIO E POSTALE**” • “**ASSEGNO CIRCOLARE**” • “**ACCREDITO CONTO CORRENTE POSTALE**” • “**ACCREDITO TESORERIA PROVINCIALE STATO PER TAB A**” • “**ACCREDITO TESORERIA PROVINCIALE STATO PER TAB B**” • **“F24EP”**

			• “**VAGLIA POSTALE** “ • “**VAGLIA TESORO**” • **“REGOLARIZZAZIONE” (per la domiciliazione)** • **“REGOLARIZZAZIONE ACCREDITO TESORERIA PROVINCIALE STATO PER TAB A”** • **“REGOLARIZZAZIONE ACCREDITO TESORERIA PROVINCIALE STATO PER TAB B”** • **“ADDEBITO PREAUTORIZZATO”** • **“DISPOSIZIONE DOCUMENTO ESTERNO” (F24, RAV, MAV pagamenti diversi da bollettini, ecc.)**
impignorabili	a	f	Può assumere il solo valore **SI**. Indica pagamenti riferibili a somme non passibili di pignoramento.
frazionabile	a	f	Può assumere il solo valore **NO**. Si riferisce a pagamenti non frazionabili, in vigenza di esercizio provvisorio.
gestione_provvisoria	a	f	Può assumere il solo valore **SI** in caso di mancata approvazione del bilancio di previsione entro il termine di legge.
data_esecuzione_pagamento	n	f	Indica la data di esecuzione del pagamento; deve essere una data futura, nel formato “**SSAA-MM-GG**” secondo il formalismo ISO 8601.
data_scadenza_pagamento	n	f	E’ la data di disponibilità dei fondi sul conto corrente di destinazione, nel formato “**SSAA-MM-GG**” secondo il formalismo ISO 8601.
destinazione	a	f	Può assumere i valori **LIBERA** o **VINCOLATA**
numero_conto_banca_italia_ente_ricevente	n	f	Indica il numero di conto o contabilità speciale dell’ente beneficiario in Banca d’Italia, nel caso di operazioni di giroconto, l’informazione seguente “tipo_contabilità_ente_ricevente” indica la natura del conto Banca d’Italia di destinazione.
tipo_contabilita_ente_ricevente	a	f	Può assumere i valori **FRUTTIFERA** o **INFRUTTIFERA** e indica la natura del conto Banca d’Italia di destinazione per le operazioni di giroconto.
classificazione	s	f	l'indicazione congiunta del "codice CGU", "codice CUP", "codice CPV", "importo" - Unità Elementare Statistica/UES - va ripetuta tante volte fino al raggiungimento dell'importo totale del beneficiario.
codice_cgu	n	o	Codice associato ad ogni ordinativo di pagamento facente riferimento al 3° livello del Piano Unico dei Conti in uso nel Sistema di Contabilità Economica Analitica delle Amministrazioni Pubbliche.

	codice_cup	an	f	Codice Unico Progetto.
	codice_cpv	n	f	Identifica il *Common Procurement Vocabulary*.
	importo	n	o	Campo numerico (due cifre per la parte decimale, il separatore dei centesimi è il punto "**.**"), indicante l'importo associato all'Unità Elementare Statistica. Non può assumere valore negativo.
Bilancio		s	f	Rappresenta un'aggregazione di dati opzionali, che può essere ripetuta più volte. E' costituita dagli elementi già descritti nella sezione "mandato".
Bollo		s	o	Aggregazione "bollo" costituita dai seguenti elementi:
	assoggettamento_bollo	an	o	Può assumere i valori • "**ESENTE BOLLO**" • "**ASSOGGETTATO BOLLO A CARICO ENTE"** • **"ASSOGGETTATO BOLLO A CARICO BENEFICIARIO"**
	causale_esenzione_bollo	an	f	Motivazione dell'esenzione dall'imposta di bollo.
Spese		s	f	Aggregazione "spese" costituita dai seguenti elementi
	soggetto_destinatario_delle_spese	a	o	Può assumere i valori "**A CARICO ENTE",** "**A CARICO BENEFICIARIO"** o **"ESENTE".**
	natura_pagamento	an	f	Descrizione della valorizzazione del TAG precedente "**soggetto_destinatario_delle_spese**", è obbligatoria nel caso in cui il valore sia "ESENTE". Questa informazione è concordata tra la PA e la BT.
beneficiario		s	o	Aggregazione "beneficiario" costituita dai seguenti elementi (qualora il beneficiario del pagamento non coincida con il creditore effettivo quest'ultimo va riportato nell'omonima struttura creditore_effettivo) [1]
	anagrafica_beneficiario	an	o	Indica il nominativo o la ragione sociale del beneficiario.
	indirizzo_beneficiario	an	o	Indica l'indirizzo del beneficiario. L'informazione diventa obbligatoria nel caso dei tipi pagamento "ASSEGNO BANCARIO E POSTALE" e "ASSEGNO CIRCOLARE".
	cap_beneficiario	an	o	Indica il CAP del beneficiario, (sedici caratteri). L'informazione diventa obbligatoria nel caso dei

[1] Esempio: intestatario del conto corrente di accredito (beneficiario) non coincidente con l'intestatario della fattura (creditore effettivo)

				tipi pagamento “ASSEGNO BANCARIO E POSTALE” e “ASSEGNO CIRCOLARE”.
	localita_beneficiario	an	o	Indica la località del beneficiario. L’informazione diventa obbligatoria nel caso dei tipi pagamento “ASSEGNO BANCARIO E POSTALE” e “ASSEGNO CIRCOLARE”.
	provincia_beneficiario	an	o	Indica la provincia del beneficiario. L’informazione diventa obbligatoria nel caso dei tipi pagamento “ASSEGNO BANCARIO E POSTALE” e “ASSEGNO CIRCOLARE”.
	stato_beneficiario	an	f	Indica lo Stato del beneficiario. L’informazione diventa obbligatoria nel caso dei tipi pagamento “SEPA CREDIT TRANSFER”. Da valorizzare con il codice paese da 2 caratteri (IT, ecc.) come indicato dalle specifiche SEPA.
	partita_iva_beneficiario	an	f	Campo numerico di trentacinque caratteri, contenente la partita IVA del beneficiario.
	codice_fiscale_beneficiario	an	o	Campo alfanumerico di trentacinque caratteri, contenente il codice fiscale del beneficiario.
delegato		s	f	Aggregazione “delegato” costituita dai seguenti elementi
	anagrafica_delegato	an	o	Indica il nominativo del delegato.
	indirizzo_delegato	an	o	Indica l’indirizzo del delegato.
	cap_delegato	an	o	Indica il CAP del delegato (sedici caratteri).
	localita_delegato	an	o	Indica la località del delegato.
	provincia_delegato	an	o	Indica la provincia del delegato.
	stato_delegato	an	f	Indica lo Stato del delegato. Da valorizzare con il codice paese da 2 caratteri (IT, ecc.) come indicato dalle specifiche ISO 3166.
	codice_fiscale_delegato	an	o	Campo alfanumerico di dimensione pari a trentacinque caratteri, indicante il codice fiscale del delegato.
creditore_effettivo		s	f	Indica il creditore originario beneficiario ultimo della disposizione di pagamento.
	anagrafica_creditore_effettivo	an	o	Indica il nominativo o la ragione sociale del creditore effettivo
	Indirizzo_creditore_effettivo	an	f	Indica l’indirizzo del creditore effettivo.
	cap_creditore_effettivo	an	f	Indica il CAP del creditore effettivo (sedici caratteri).
	localita_creditore_effettivo	an	f	Indica la località del creditore effettivo.

provincia_creditore_effettivo	an	f	Indica la provincia del creditore effettivo.
stato_ creditore_effettivo	an	o	Indica lo stato del beneficiario. Da valorizzare con il codice paese da 2 caratteri (IT, ecc.) come indicato nelle specifiche SEPA.
partita_iva_creditore_ effettivo	an	f	Campo numerico di trentacinque caratteri, contenente la partita IVA del creditore effettivo.
codice_fiscale_creditore_effettivo	an	f	Campo alfanumerico di trentacinque caratteri, contenente il codice fiscale del creditore effettivo.
piazzatura	s	f	Aggregazione opzionale “piazzatura”, indicante le coordinate bancarie e gli estremi della banca o del conto corrente postale di accredito dell’importo
abi_beneficiario	an	o	Codice ABI della banca domiciliataria del conto corrente del beneficiario.
cab_beneficiario	an	o	Codice CAB della banca domiciliataria del conto corrente del beneficiario.
numero_conto_corrente_beneficiario	an	o	Numero di conto corrente del beneficiario presso la banca precedentemente identificata o numero del conto postale.
caratteri_controllo	an	o	Caratteri di controllo previsti dallo standard IBAN.
codice_cin	an	o	Carattere alfanumerico calcolato con speciali algoritmi, previsti dallo standard BBAN.
codice paese	an	o	Identifica univocamente il Paese, nell’ambito dell’area “euro”, in cui è situata la banca.
denominazione_banca_destinataria	an	f	Indica la denominazione delle banca, dell’agenzia e l’indirizzo dell’agenzia stessa.
sepa_credit_transfer	s	f	Strumento di pagamento per l'esecuzione di bonifici in euro fra i clienti i cui conti sono situati all’interno della SEPA
iban	an	o	Identifica l’International Bank Account Number composto da una serie di numeri e lettere che identificano, in maniera standard, il paese in cui è tenuto il conto, la banca, lo sportello e il conto corrente di ciascun cliente. È previsto inoltre il codice controllo. Lunghezza massima 34 caratteri come da standard ISO.
bic	an	f	Bank Identifier Code. BIC valido deve essere registrato nell'ISO9362, formato da 8 o 11 caratteri continui.
identificativo_end_to_end	an	f	Riferimento univoco assegnato all’ordine di pagamento che deve giungere inalterato fino al beneficiario (può anche essere valorizzato con la chiave esercizio, numero_mandato e progressivo_beneficiario)
Codice_versante	an	f	Da utilizzare con le tipologie di pagamento “BONIFICO BANCARIO E POSTALE” o

				“SEPA CREDIT TRANSFER” con coordinate IBAN individuate dalla Banca d’Italia. Indica la codifica del versante valorizzata dalla PA in ragione delle specifiche dettate dall’ente destinatario del bonifico.
causale		an	O	Rappresenta la descrizione estesa della causale del pagamento. (Corrisponde nello standard SEPA Credit Transfer all’informazione “Remittance Information - Unstructured”, in futuro è previsto l’inserimento anche delle informazioni di tipo “Structured”)
sospeso		s	F	Aggregazione “sospeso”, ripetibile più volte, indicante la presenza di provvisori.
	numero_provvisorio	n	o	Indica il numero del provvisorio oggetto di regolarizzazione.
	importo provvisorio	n	o	Indica l’importo da regolarizzare (totale o parziale) del provvisorio, precedentemente indicato. Non può assumere valore negativo.
ritenute			F	Aggregazione “ritenute” (importo da trattenere), la struttura può essere ripetuta più volte con dati omogenei. Costituita da:
	importo_ritenute	n	O	Campo numerico (due cifre per la parte decimale, il separatore dei centesimi è il punto “**.**”), indicante l’importo relativo alle ritenute in oggetto. Non può assumere valore negativo.
	numero_reversale	an	F	Eventuale numero della reversale associata alle ritenute.
	progressivo_versante	n	F	Indica il numero progressivo del versante all’interno della reversale precedentemente richiamata.
informazioni aggiuntive		an	F	Raggruppamento di informazioni facoltative, composto da:
	lingua	an	F	Indica la lingua utilizzata per la stampa delle ricevute (ad esempio **ITALIANO**, **TEDESCO**) per le province che adottano il bilinguismo.

riferimento_documento_esterno	an	f	Contiene il riferimento ad un documento esterno cartaceo o informatico.
sostituzione_mandato	s	f	Raggruppamento di informazioni utilizzata per la sostituzione di un documento, struttura da valorizzare in abbinamento con il tipo_operazione "SOSTITUZIONE". E' ammessa una sola occorrenza per ciascun beneficiario.
numero_mandato_da_sostituire	an	o	Numero del mandato da sostituire
progressivo_beneficiario_ da_sostituire	n	o	Numero del beneficiario da sostituire
esercizio_mandato_da_sostituire	n	o	Esercizio di riferimento del documento sostituito, deve essere omogeneo con l'esercizio del flusso.
dati_a_disposizione_ente_beneficiario	s	f	Struttura finalizzata ad accogliere informazioni utilizzate ad uso esclusivo dalla PA per rendere completo il documento informatico. Contiene strutture e informazioni definite internamente da ciascuna PA, i dati contenuti in questa struttura vengono ignorati dalla BT.

4.6 Struttura delle ricevute di servizio e dei messaggi di esito applicativo

4.7 Messaggio ricezione flusso

dato	genere	o/f	contenuto
codice_ABI_BT	n	o	Codice ABI della BT.
identificativo_flusso	an	f	Codice alfanumerico attribuito univocamente al flusso (degli ordinativi) inviato da parte della PA.
identificativo_flusso_BT	an	f	Codice alfanumerico generato ed attribuito univocamente al flusso da parte della BT.
data_ora_creazione_flusso	an	o	Indica la data e l'ora di creazione del flusso (messaggio) nel formato "**SSAA-MM-GGTHH:MM:SS"** secondo il formalismo ISO 8601.
codice_ente_BT	an	f	Codice univoco interno, attribuito dalla BT, per mezzo del quale la PA è riconosciuta dalla banca medesima.

4.8 Messaggio rifiuto flusso

dato	genere	o/f	contenuto
codice_ABI_BT	n	o	Codice ABI della BT.
identificativo_flusso	an	f	Codice alfanumerico attribuito univocamente al flusso (degli ordinativi) inviato da parte della

			PA.
identificativo_flusso_BT	an	f	Codice alfanumerico generato ed attribuito univocamente al flusso della BT.
data_ora_creazione_flusso	an	o	Indica la data e l'ora di creazione del presente flusso (messaggio) nel formato "**SSAA-MM-GGTHH:MM:SS"** secondo il formalismo ISO 8601.
codice_ente_BT	an	f	Codice univoco interno, attribuito dalla BT, per mezzo del quale la PA è riconosciuta dalla banca medesima.
errore		o	Aggregazione "errore", ripetibile più volte, indicante la presenza di errori nel flusso presentato dalla PA, costituita da:
codice	n	f	Eventuale codice associato all'errore.
descrizione	an	o	Descrizione dell'errore, motivo del rifiuto del flusso.

4.9 Messaggi esito applicativo

dato	**genere**	**o/f**	**contenuto**
codice_ABI_BT	n	o	Codice ABI della BT.
identificativo_flusso_BT	an	f	Codice alfanumerico generato ed attribuito univocamente al flusso della BT.
codice_ente	an	f	Può contenere il codice istat relativo ad un ente il codice R.G.S, il codice fiscale o la partita IVA, il codice SIA, ecc.
descrizione_ente	an	f	Campo alfanumerico contenente la denominazione della PA.
codice_ente_BT	n	o	Codice univoco attribuito dalla BT, per mezzo del quale la PA è riconosciuta dalla banca medesima.
esito_reversali		f	Aggregazione "esito_reversali" costituita da:
identificativo_flusso	an	f	Codice alfanumerico attribuito univocamente al flusso (degli ordinativi) inviato da parte della PA.
esercizio	n	o	Indica l'anno d'esercizio finanziario o contabile, nel formato "**SSAA**".
numero_reversale	an	o	Indica il numero della reversale a cui fanno riferimento tutti i dati che seguono.
progressivo_versante	n	f	Indica l'eventuale numero progressivo del versante all'interno dello stesso ordinativo.
data_reversale	an	f	Indica la data di emissione della reversale da parte della PA, nel formato "**SSAA-MM-GG**" secondo il formalismo ISO 8601.
importo	n	f	Campo numerico (due cifre per la parte decimale, il separatore dei centesimi è il punto "**.**"), indicante l'importo della reversale in oggetto.

				Non può assumere valore negativo.
	esito_operazione	an	o	Può assumere i valori: • “**ACQUISITO**” • “**NON ACQUISITO**” • **“VARIATO”** • **“NON VARIATO”** • **“ANNULLATO”** • **“NON ANNULLATO”** • **“SOSTITUITO”** • **“NON SOSTITUITO”** • **“RISCOSSO”** • **“REGOLARIZZATO”** • **“NON REGOLARIZZATO”** • **“STORNATO”**
	data_ora_esito_operazione	an	o	Indica la data e l’ora esito dell’operazione di tesoreria nel formato “**SSAA-MM-GGTHH:MM:SS”** secondo il formalismo ISO 8601, nel caso in cui il TAG esito sia valorizzato con “RISCOSSO”, “REGOLARIZZATO”, “STORNATO” l’ora può essere impostata a “00:00:00”.
	lista_errori		f	Aggregazione “lista errori”, presente in caso di riscontro di errori, costituita da:
	progressivo_versante	n	f	Indica l’eventuale numero progressivo del versante all’interno dello stesso ordinativo.
	codice_errore	n	f	Eventuale codice associato all’errore.
	descrizione	an	o	Descrizione dell’errore, motivo della non esecuzione dell’operazione.
	elemento	an	f	Nome dell’elemento che presenta l’errore.
esito_mandati			f	Aggregazione “esito_mandati”, costituita da:
	identificativo_flusso	an	f	Codice alfanumerico attribuito univocamente al flusso (degli ordinativi) inviato da parte della PA.
	esercizio	n	o	Indica l’anno d’esercizio finanziario, nel formato “**SSAA**”.
	numero_mandato	an	o	Indica il numero del mandato a cui fanno riferimento tutti i dati che lo seguono.
	progressivo_beneficiario	n	f	Indica l’eventuale numero progressivo del beneficiario all’interno dello stesso ordinativo.
	data_mandato	an	f	Indica la data di emissione del mandato da parte della PA, nel formato “**SSAA-MM-GG**” secondo il formalismo ISO 8601.
	importo	n	f	Campo numerico (due cifre per la parte decimale, il separatore dei centesimi è il punto “**.**”), indicante l’importo del mandato in oggetto. Non può assumere valore negativo.

esito_operazione	an	o	Può assumere i valori: • **“ACQUISITO**” • “**NON ACQUISITO**” • **“VARIATO”** • **“NON VARIATO”** • **“ANNULLATO”** • **“NON ANNULLATO”** • **“SOSTITUITO”** • **“NON SOSTITUITO”** • **“PAGATO”** • **“REGOLARIZZATO”** • **“NON REGOLARIZZATO”** • **“STORNATO”**
data_ora_esito_operazione	an	o	Indica la data e l’ora esito dell’operazione di tesoreria nel formato “**SSAA-MM-GGTHH:MM:SS”** secondo il formalismo ISO 8601, nel caso in cui il TAG esito sia valorizzato con “PAGATO”, “REGOLARIZZATO”, “STORNATO” l’ora può essere impostata a “00:00:00”.
lista_errori		f	Aggregazione “lista errori” presente in caso di riscontro di errori, costituita da:
progressivo_beneficiario	n	f	Indica l’eventuale numero progressivo del beneficiario all’interno dello stesso ordinativo.
codice_errore	n	f	Eventuale codice associato all’errore.
descrizione	an	o	Descrizione dell’errore, motivo della non esecuzione dell’operazione.
elemento	an	f	Nome dell’elemento che presenta l’errore.

5 Prerequisiti per l'adesione al servizio da parte degli enti

5.1 Accesso al Servizio e processo di firma

I requisiti sono:

1. Accesso ad Internet dalla propria postazione di lavoro
2. Il browser supportato : Internet Explorer 7.0 o successivi
3. Lettore di Smart Card connesso alla propria postazione di lavoro
4. Smart Card contenente un Certificato per la Firma Digitale qualificata rilasciato da una Certification Authority riconosciuta dal DigitPA (ex-CNIPA)

In generale qualunque carta che disponga di una libreria PKCS#11, si dovrà prevedere una opportuna fase di test di integrazione per verificare il funzionamento con l'applicazione. Non sono previste in alcun modo attività, da parte del personale tecnico della Banca, per effettuare configurazione di postazioni di lavoro per i KIT di Firma.

Si rimanda ai capitoli successivi di questo documento per maggiori informazioni.

6 Sicurezza

6.1 Messaggi Scambiati e Firma Digitale

I messaggi XML scambiati tra Ente e Tesoriere vengono imbustati secondo il formato Pkcs#7 conforme alla specifica RFC 2315 – PKCS#7 Cryptographic Message Syntax - v.1.5. Tutte le ricevute (servizio, elaborazione e applicative) vengono imbustate solo con il formato Pkcs#7.

La tabella che segue indica per ciascun messaggio previsto, quali sono i meccanismi di sicurezza che si applicano e quali sono servizi di sicurezza che si ottengono applicando questi meccanismi.

Documento XML	Meccanismi di Sicurezza	Servizi
Mandati di pagamento **Reversali di Incasso**	Firma digitale	• Autenticità dell'origine • integrità dei dati • non ripudio dell'invio
Ricevuta di servizio, elaborazione e applicativa	Firma digitale	• Autenticità dell'origine • integrità dei dati • non ripudio dell'invio della ricevuta • non ripudio della ricezione degli ordinativi a cui si riferiscono (la ricevuta di elaborazione e quella applicativa)

Tabella 1 Meccanismi di sicurezza

I servizi di autenticazione del mittente, integrità dei dati, non ripudio dell'invio e non ripudio della ricezione vengono realizzati attraverso il meccanismo di firma digitale.

Di seguito vengono riportate le indicazioni riguardanti il formato PKCS#7 da utilizzarsi per imbustare i messaggi:

PKCS#7 SignedData (per la firma del messaggio)

Il formato è conforme al tipo SignedData definito nelle specifiche RFC 2315 – PKCS#7: Cryptographic Message Syntax Versione 1.5.

Tale tipologia di firma, secondo la normativa del CNIPA sarà valida fino al 30 Giugno 2011, dal 1 Luglio 2011 invece la normativa prevede una firma CAdES-BES

CAdES-BES

La novità più consistente riguarda l'introduzione dell'uso di un nuovo algoritmo di calcolo delle impronte, lo SHA – 256, definito nella norma ISO/IEC 10118-3:2004, in luogo dell'algoritmo usato finora, lo SHA – 1.

Il certificato del firmatario è incluso nel PKCS#7 SignedData.

I dati su cui viene calcolata la firma vanno dal primo carattere del tag di apertura all'ultimo carattere del tag di chiusura del file XML.

L'algoritmo di firma digitale utilizzato è sha-1WithRSAEncryption. La lunghezza della chiave RSA è 1024 bit.

6.2 Gestione delle Chiavi

I meccanismi di sicurezza prevedono l'utilizzo di chiavi RSA, utilizzate nei processi di firma.

Chiavi RSA: l'algoritmo RSA opera su una coppia di chiavi: una privata e una pubblica. La chiave privata, in osservanza a quanto stabilito dalla normativa nazionale, deve essere custodita segreta all'interno del dispositivo di firma e non deve mai essere distribuita. Quella pubblica, invece va comunicata alla parte corrispondente dell'interscambio e inserita, a cura del certificatore, su directory di pubblico dominio. La chiave privata viene utilizzata dal mittente per sottoscrivere con firma digitale i dati da trasmettere. La chiave pubblica del mittente viene utilizzata dal destinatario per verificare l'autenticità del mittente e l'integrità dei dati ricevuti (verifica della firma elettronica). In caso di temuta compromissione della chiave o di smarrimento del dispositivo di firma, i contraenti dovranno richiedere al certificatore la revoca della validità delle chiavi RSA.

6.3 Certificazione

Le chiavi, i certificati e gli algoritmi utilizzati per il sistema di interscambio tra Ente e Tesoriere sono conformi a quanto stabilito dalla vigente normativa in materia di "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione anche temporale, dei documenti informatici".

Ogni parte procede autonomamente alla scelta dell'Autorità di Certificazione tra quelle iscritte all'Albo dei Certificatori approvati da CNIPA e all'acquisizione dei servizi messi a disposizione.

L'ente deve dotarsi dei seguenti certificati:

Un certificato di firma per ogni firmatario;

Il certificato dell'Autorità di Certificazione che ha emesso i certificati di firma.

La tesoreria deve dotarsi dei seguenti certificati:

Un certificato di firma, per apposizione firme "massive";

Il certificato dell'Autorità di Certificazione che ha emesso i certificati di firma.

6.4 Responsabilità

Le parti si impegnano a non attivare processi di firma a fronte di certificati scaduti.

Le parti rigettano, in ogni caso, pacchetti firmati il cui certificato risulti scaduto al momento della verifica, indipendentemente dal fatto che la firma sia stata apposta in condizioni di validità del certificato stesso (non scaduto).

Qualora, in sede di verifica, risulti che il certificato è stato revocato, il pacchetto verrà rifiutato indipendentemente dalla data di pubblicazione nella CRL, in quanto la compromissione reale può essere avvenuta anche antecedentemente alla data di firma o di pubblicazione nella CRL.

In caso di smarrimento del dispositivo, divulgazione PIN di accesso al dispositivo, revoca autorizzazione, o qualsiasi altro eventuale motivo, Ente e Tesoriere concordano di richiedere immediatamente al proprio Certificatore la revoca del relativo certificato.

7 TECNOLOGIE UTILIZZATE DAL SISTEMA

7.1 Tecnologie Client

Browser Web del tipo :

- Internet Explorer;
- Mozzilla;
- Opera;
- FireFox;
- Chrome.

Sicurezza Client:

- Certificato Digitale SSL.

Sistema Operativo:

- Windows (xp, vista,etc.)
- Linux

Java Runtime:

- Dalla versione 1.4 (ove il client dell'utente non la avesse già come nel caso di chi utilizza i servizi dell'agenzia delle Entrate). Eventuali versioni precedenti possono essere gestite ma non sono più mantenute da Sun Microsystem, soprattutto per i noti problemi https con proxy in cascata

Kit di Firma:

- Riportiamo di seguito un elenco di Certificati digitali di firma e relativi dispositivi

7.2 Elenco dei token supportati

Le credenziali di firma, contenute nei Token gestiti dall'Applet, devono essere rilasciate da certificatori presenti nell'elenco pubblico di quelli accreditati come previsto dall'articolo 29, comma 1 del DLGS 7 marzo 2005 nn. 82 e specificato nel DPCM 13 gennaio 2004, é mantenuto e reso disponibile dal CNIPA attraverso la rete Internet, ai sensi dell'articolo 29, comma 6 del citato decreto legislativo.

I certificatori iscritti nell'elenco, alla data di stesura del presente documento, sono:

Certificatore	Iscrizione al Ruolo
ACTALIS S.p.A.	27-03-2002
Aruba Posta Elettronica Certificata S.p.A.	05-12-2007
Banca d'Italia	23-01-2008
Banca Monte dei Paschi di Siena S.p.A.	02-08-2004
Cedacri S.p.A. (già Cedacrinord S.p.A.)	14-11-2001
Comando C4 Difesa - Stato Maggiore della Difesa	20-09-2006
Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili	09-07-2008
Consiglio Nazionale del Notariato	11-09-2002
Consiglio Nazionale Forense	10-12-2003
I.T. Telecom S.r.l.	12-01-2005
In.Te.S.A. S.p.A.	21-03-2001
Infocert S.p.A.	18-07-2007
Intesa Sanpaolo S.p.A. (già Sanpaolo IMI S.p.A. e Banca Intesa S.p.A.)	07-04-2004
Lombardia Informatica S.p.A.	15-12-2010
Namirial S.p.A.	02-11-2010
Postecom S.p.A.	19-04-2000
SOGEI S.p.A.	25-02-2004

Di seguito riportiamo un elenco, esplicativo, dei token gestiti, alla data di stesura del presente documento, dall'Applet di Firma; qualora il token da utilizzare non fosse presente nell'elenco, tramite "getatr" riusciamo ad identificarne la struttura ed i driver di destinazione, ottenendo la libreria specifica. Questo risultato è possibile grazie a diverse collaborazioni instaurate con alcune aziende che operano nel settore dei driver digitali ed al fatto che l'applet lavora a livello di librerie pkcs#11 driver.

Sistema operativo: ***Windows***:

ATR Carta, ove presente ATR Mask e Driver

Actalis HID Key
Actalisone.dll
bit4opki.dll
bit4ipki.dll
bit4tpki.dll

BusinessKey HID
bit4opki.dll
bit4cpki.dll
bit4ipki.dll

ASECard III (Athena)
3BD6180081B1807D1F038051006111308E
asepkcs.dll
3BD6180081B1807D1F038051006110308F
asepkcs.dll

ASEToken PIV (Athena) v5.0.1.7

3BDF18008131FE7D006B1F0C0180010001434E53103180F2
FFFFFFFFFFFFFFFFFFFF0FFFFF0FF00FFFFFFFFFFFFF00 asepkcs.dll
bit4p11.dll

eToken Card M4.20 (Aladdin)
3BF2180000C10A31FE55C80600
FFFFFFFF00FFFFFFFFFFFFFF00
eTpkcs11.dll

eToken HS (Aladdin)
3B811F00CC52
eTpkcs11.dll

eToken JC NG-Flash 72k (Aladdin)
3BD5180081313A7D8073C8211030
eTpkcs11.dll

eToken pro 16K and pro 32 (Aladdin)
3BE200FFC11031FE55C8029C
eTpkcs11.dll

3BF29800FFC11031FE55C80315
eTpkcs11.dll

eToken marchiato Telecom (Aladdin)
3BF2180002C10A31FE58C80975
eTpkcs11.dll

(Siemens CryptoVision) & (Charismatics Smart Security Interface CardOS M4.01)
3BF49800FFC11031FE554D346376B4
cvp11_M4.dll

(Charismatics)
3BF2180002C10A31FE58C80975
cmP11.dll
siecap11.dll

Charismatics (Siemens CardOS V4.3B Chip SLE66CX642P) using cmP11.dll v4.7.1.1
3BF2180002C10A31FE58C80874
cmP11.dll

(Siemens)
3BFC9800FFC11031FE55C803496E666F63616D65726528
SI_PKCS11.dll
CardOS_PKCS11.dll

3BFC9800FFC11031FE55C804496E666F63616D6572652F
SI_PKCS11.dll
CardOS_PKCS11.dll

CardOS M4.01a (Siemens), Sysgillo (Incard) and EutronITSEC
3BF29800FFC11031FE55C80412
SI_PKCS11.dll
CardOS_PKCS11.dll
ipmpkilc.dll
ipmpki32.dll

CardOS M4.01 (Siemens) and EutronITSEC
3BF29800FFC11031FE55C80315
CardOS_PKCS11.dll
SI_PKCS11.dll

(Eutron)
3B25008053415201
sadaptor.dll

3B15008053415200
FFFFE0FFFFFFFFF0
sadaptor.dll

Crypto Identity ITSEC-P (Eutron)
3BB794008131FE6553504B32339000D1
aetpkss1.dll

Siemens CardOS V4.3B Crypto Identity ITSEC-I (Eutron - Green/Blue cover USB - Charismatics)
3BF4180002C10A31FE5856346376C5
cmP11.dll

AuthentIC v 203 and ID-One Bio (Cosmo v4.x) (Oberthur)
3B7F1800000031C0739E010B6452D90400829000
FF0000FFFFFFFFFFFFFFFFFFFFFFFF00FFFFFFFF O
CSCryptolib_P11.dll

AuthentIC SSB (Oberthur)
3B6F00FF905353422D504B4353233131049000
cryptoki.dll

AuthentIC Identrus (Oberthur)
3B7F1800000031C0531DE2126452D90400829000
IdentrusPkcs11.dll
AuthentIC_B2B_Pkcs11.dll

3B7F1800000031C0531DE2126452D90300819000
IdentrusPkcs11.dll
AuthentIC_B2B_Pkcs11.dll

ID-One Bio (Cosmo v5.x) and OCS Cosmo 64 RSA v5.x (Oberthur)
3B7B0000000031C06400E30000829000
FFFF00FFFFFFFFFFFF00FF00FFFFFFFF
OCSCryptolib_P11.dll

CardOS M4, GemGATE – 32k, GPK16000, GPK8000 (Gemplus)
3BE200FFC11031FE55C8029C
gclib.dll

CardOS M4, GemGATE – 32k, GPK16000, GPK8000 (Gemplus) and eToken pro 16K (Aladdin)
3BFB9800FFC11031FE55006405204703318000900 0F3
gclib.dll

3BA70040108065A209010052
FFFFFFFFF3FFFFFFFFF00FF
gclib.dll

3BA70040108065A208010152
FFFFFFFFF3FFFFFFFFFFFFF
gclib.dll

Gemalto Classic TPC IS 32k, TPC IM 64k (Gemplus)
3B7D00000080318065B08300000083009000
FFFF00FFFFFFFFFFFFFFFF000000FFFFFFFF
gclib.dll

Sysgillo (Incard)
3BB794008131FE6553504B32339000D1
ipmpkilc.dll
ipmpki32.dll

3B9F94401E00671643464953451052 66FF819000
ipmpki32.dll
ipmpkilc.dll

Belgium EID
3B989440FFA503010101AD1310
Belgium Identity Card
PKCS11.dll
3B9894400AA503010101AD1310
Belgium Identity Card
PKCS11.dll

3B9813400AA503010101AD1311
Belgium Identity Card
PKCS11.dll

Rainbow USB token
3B0F524E424F2454232D0B00A067452301

CNS:PDC (Oberthur - ICM=04,ICT=05)
3BFF1800008131FE45006B0405010001210143 4E5310318059
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF00FFFFFFFF00FFFF00
bit4opki.dll

CNS:HPC (Oberthur - ICM=04,ICT=05)
3BFF1800008131FE45006B040501000112024850431031806C
bit4opki.dll

CNS (ST/Incard)
3BFF1100FF8131805500680200101049 4E43525950544F001A
Ipmpki32.dll
bit4cpki.dll
incryptoki2.dll

CNS
3BC4FF0000318000
bit4cpki.dll
incryptoki2.dll

3BF41100FF8131805500318000CE
bit4cpki.dll incryptoki2.dll

CNS:DEMO
3BFB1100FF8131805500680200101044454D4F0019
bit4cpki.dll
incryptoki2.dll

CNS:SIAE
3BFB1100FF8131805500680200101053494145 0004
bit4cpki.dll
incryptoki2.dll

CNS:PDC (ST/Incard - ICM=02, ICT=09)
3BFF1800FF8131FE55006B0209020001 1101434E531031808F
FF0F00FFFF0FFF0000FFFFFFFFFFFFFF00FFFFFFFF00FFFF00
bit4ipki.dll
bit4cpki.dll
incryptoki2.dll

DSD (ST/Incard - ICM=02, ICT=09)
3BFF1800FF8131FE55006B0209020001010144534410318092
bit4cpki.dll
incryptoki2.dll

CNS:PDC (ST/Incard - ICM=02, ICT=09) serie 7420057800421700
3BFF1800FF8131FE55006B0209030301 1101434E531131808C
FF0F00FFFFFFFF0000FFFFFFFFFFFFFF0FFFF00000F0FFFF00
bit4ipki.dll
bit4cpki.dll
incryptoki2.dll

CNS:PDC (Infineon/Siemens - ICM=05, ICT=08)
3BFF1800FFC10A31FE55006B0508C805011101434E531031800C
FF0F00FFFF0F00FF0000FFFFFFFFFFFFFF00FFFFFFFF00FFFF00
bit4ipki.dll
bit4cpki.dll
incryptoki2.dll
cnsPKCS11.dll
bit4p11.dll

CNS:HPC (Infineon/Siemens - ICM=05, ICT=08)
3BFF1800FFC10A31FE55006B0508C8050102014850430031800A
FF0F00FFFF0F00FF0000FFFFFFFFFFFFFF00FFFFFFFF00FFFF00
bit4cpki.dll
incryptoki2.dll

CNS:HPC - SISS (Infineon/Siemens - ICM=05, ICT=08)
3BFF1800FFC10A31FE55006B0508C80501020A48504300318001
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF0FF0FFFFFFFFFFFF00
sissp11.dll

CNS:PDC ContactLess (Infineon/Siemens - ICM=05, ICT=08)
3BFF1800FFC10A31FE55006B0508C80A010101434E5310318013
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF0FFFFFFFFFFFFFF0F
bit4cpki.dll
incryptoki2.dll

GXPPro with RSA512->1024 (GemSAFE)
3B7B9400008065B08301017483009000
gclib.dll

Used by GUMAR
3B7D96000080318065B0831148C883009000
gclib.dll

eToken marchiato Telecom (laddin)
3BF2180002C10A31FE58C80975"
eTpkcs11.dll

Sistema operativo: ***Linux***

ATR Carta, ove presente ATR Mask e Driver

// ASECard III (Athena)
3BD6180081B1807D1
F038051006111308E
libasepkcs.so
libASEPKCS11.so

3BD6180081B1807D1F038051006110308F
libasepkcs.so
libASEPKCS11.so

// Crypto Identity ITSEC-P (Eutron)
3BB794008131FE6553504B32339000D1
libaetpkss.so

// Belgium EID
3B989440FFA503010101AD1310
Belgium-EID-pkcs11.so

3B9894400AA503010101AD1310
Belgium-EID-pkcs11.so

3B9813400AA503010101AD1311
Belgium-EID-pkcs11.so

// CNS (ST Incard)
3BFF1100FF8131805500680200101049 4E43525950544F001A
libincryptoki2.so

3BC4FF0000318000
libincryptoki2.so

3BF41100FF8131805500318000CE
libincryptoki2.so

3BFB1100FF8131805500680200101044454D4F0019
libincryptoki2.so

3BFB1100FF81318055006802001010534941450004
libincryptoki2.so

3BFF1800FF8131FE55006B02090200011101434E531031808F
FF0F00FFFF0FFF0000FFFFFFFFFFFFFF00FFFFFFFF00FFFF00 l
ibincryptoki2.so

3BFF1800FF8131FE55006B0209020001010144534410318092
libincryptoki2.so

3BFF1800FF8131FE55006B02090303011101434E531131808C
FF0F00FFFF0FFF0000FFFFFFFFFFFFFF00FFFFFFFF00FFFF00
ibincryptoki2.so

3BFF1800FFC10A31FE55006B0508C805011101434E531031800C
FF0F00FFFF0F00FF0000FFFFFFFFFFFFFF00FFFFFFFF00FFFF00
libincryptoki2.so

3BFF1800FFC10A31FE55006B0508C8050102014850430031800A
FF0F00FFFF0F00FF0000FFFFFFFFFFFFFF00FFFFFFFF00FFFF00
libincryptoki2.so

3BFF1800FFC10A31FE55006B0508C80A010101434E5310318013
libincryptoki2.so

ASEKey CNS (Athena with bit4id token)
3BDF18008131FE7D006B1F0C0180010001434E53103180F2
libasepkcs.so
libASEPKCS11.so

3BDF18008131FE7D006B150C0181010001434E53103180F9
libasepkcs.so
libASEPKCS11.so

3BDF18008131FE7D006B150C0181011101434E53103180E8
libasepkcs.so
libASEPKCS11.so

3BDF18008131FE7D006B150C0180011101434E53103180E9
libasepkcs.so
libASEPKCS11.so

7.3 Tecnologie Server

Pur essendo sviluppato in ambiente IBM (WSAD e Rational Application Developer) il prodotto "TesoWebSign" è "**multipiattaforma"** (WINDOWS, UNIX, LINUX, etc.) e compatibile con qualunque altro "**Application Server"** (WEBSPHERE, APACHE TOMCAT, RESIN,ORACLE APPSERVER etc.) che rispetti le specifiche J2EE.

Il prodotto prevede sia per le componenti Web (Ear TesoWebsign) che per i Batch (Normalizzatore, WorkFlowBanca) meccanismi di carico bilanciato, gestiti direttamente dall'Application Server o in maniera applicativa tramite servizi interni al prodotto.

Il prodotto può operare con qualsiasi "**database**" di tipo relazionale (Oracle, Db2 Web o Host, Udb, SqlServer, etc.)

Il tutto tenendo conto delle caratteristiche di architetture applicative distribuite, in grado, quindi, di supportare grandi carichi di lavoro.

7.4 Tecnologie di Interazione

La componente Applet, descritta in precedenza, ha una dimensione di circa 2 Megabyte e viene scaricata sulle singole postazioni di lavoro (client), in maniera integrale, solo alla prima esecuzione; durante lo scarico ed installazione in locale viene distribuita tutta la parte core business del software. Può lavorare in modalità "Cache Sun" oppure "Online Working".

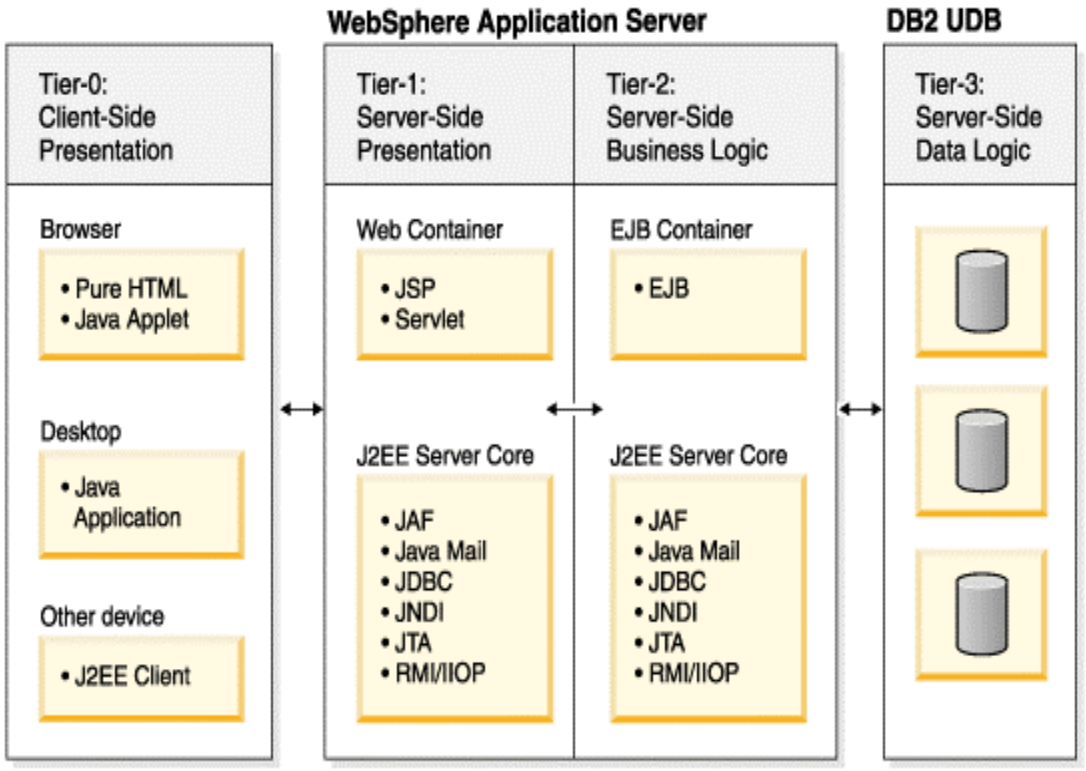
I file che vengono firmati digitalmente, contenenti i dati del Challenge (descritto in precedenza), hanno una dimensione valutabile in kbyte.

Il software è stato sviluppato nel contesto dell' Ordinativo Informatico Locale a Norma DigitPA (ex-Cnipa *circ. 80 del 2003 e circ. 35 del 2008*), i cui utilizzatori finali del servizio sono Enti Pubblici, che utilizzano spesso connessioni di rete a velocità molto ridotte (es. modem a 56kb) e devono operare regolarmente senza alcun disservizio.

8 ARCHITETTURA DEL SISTEMA

8.1 Modello logico di riferimento

Il modello di applicazioni di tipo J2EE può essere così schematizzato :



Per poter più facilmente gestire la manutenzione dell' applicazione, è conveniente che questa abbia una natura modulare e basata sulle responsabilità, al fine di ottenere un prodotto component - based. A tal fine, il prodotto è stato sviluppato seguendo la logica della programmazione ad "oggetti" riutilizzabili (Object Oriented Programming), in relazione alla metodologia di progettazione in linguaggio JAVA.

Tale metodologia garantisce:

1 ***Portabilità*** del software su piattaforme fisiche differenti

2 ***Indipendenza*** dalla piattaforma

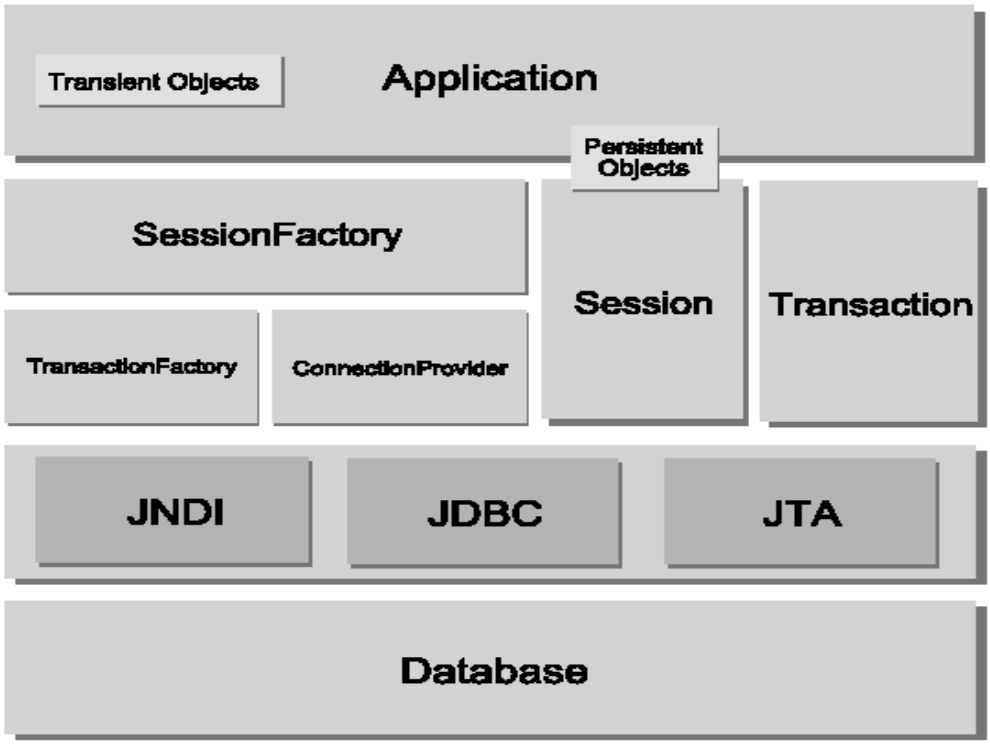
3 ***Scalabilità*** del software come estendibilità delle proprie funzioni: una volta definite classi e relazioni, sarà possibile, mediante il linguaggio, implementare applicazioni in termini di

classi generiche; questo significa che una applicazione sarà in grado di utilizzare ogni oggetto specifico senza essere necessariamente riscritta, ma limitando le modifiche alle funzionalità fornite dall'oggetto per manipolare le sue proprietà.

Appare quindi chiaro il bisogno di un'architettura che permetta la separazione netta tra i componenti software che gestiscono il modo di presentare i dati, e i componenti che gestiscono i dati stessi.

Per la gestione relazionale dei dati è stato utilizzato Hibernate, un framework, che si occupa non solo della relazione tra le classi Java alle tabelle della base di dati (e dai tipi di dato Java a quelli SQL), ma fornisce anche funzionalità di interrogazione e recupero dei dati (query), e può ridurre significativamente i tempi di sviluppo altrimenti impiegati in attività manuali di gestione dei dati in SQL e JDBC.

Lo schema relativo all'architettura Hibernate è il seguente:



9 STANDARD APPLICATI AL SISTEMA

9.1 Standard Implementativi

Tutti i prodotti software realizzati nel progetto “TesoWebSign” rispettano gli standard delle applicazioni Java Sun Microsystem cioè: J2EE specifiche alla versione 1.4, con Java Virtual Machine alla versione 1.5.
Inoltre, sono stati rispettati tutti gli standard dei prodotti del gruppo nuove tecnologie e disegno architetture di SIASSB.

9.2 Standard Strumenti

Per realizzare alcune funzioni generalizzate sono stati utilizzati oggetti di libreria SIASSB (LIBRA alla versione 4.0 ed Hopera v.1.2)

9.2.1 Strumenti di Analisi

- Microsoft Project
- ABC Web
- Uml

9.2.2 Strumenti di Sviluppo Software

Per gli strumenti di sviluppo sono stati utilizzati :

1 Ibm Websphere versione 5.5 o Ibm Rational Application Developer v.7.0.7;

2 Database Relazionale (es. Ibm Db2, SQLServer, Mysql etc.);

Per l’installazione in ambiente di test sono stati utilizzati :

3 IBM WebSphere Application Server 5 o superiore

4 Application Server di tipo J2EE

9.2.3 Strumenti di Management

Monitoraggio Progetti SIASSB
Manage project SIASSB
Microsoft Project