

ALLEGATO 2

(le specifiche tecniche qui riportate costituiscono indicazione non esaustiva da completarsi in sede di sottoscrizione definitiva del contratto)

PROTOCOLLO PER LA TRASMISSIONE TELEMATICA PER GLI ORDINATIVI INFORMATICI DI INCASSO E DI PAGAMENTO TRA IL COMUNE DI URBINO E IL TESORIERE.

Richiamate le seguenti disposizioni normative

- che, ai sensi dell'art. 15, comma 2, della Legge 15.3.1997, n. 59, gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione, e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge;
- che con D.P.R. 10.11.1997, n. 513 (abrogato), è stato approvato il regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'art. 15, comma 2, della Legge n. 59/1997;
- che con decreto 8.2.1999 del Presidente del Consiglio dei Ministri sono state dettate le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'art. 3, comma 1, del D.P.R. n. 513/1997 e, come precisato all'art. 2 dello stesso Decreto Presidenziale:
 - regole tecniche di base;
 - regole tecniche per la certificazione delle chiavi;
 - regole tecniche sulla validazione temporale;
 - regole tecniche per la protezione dei documenti informatici;
 - regole tecniche per le pubbliche amministrazioni;
- che il comma 2 dell'art. 1 del D.P.R. 20.4.1994, n. 367, stabilisce che i pagamenti dello Stato sono effettuati, di regola, con titoli informatici;
- che, ai sensi dell'art. 2 del succitato D.P.R. n. 367/1994, gli atti e documenti previsti dalla legge e dal regolamento sull'amministrazione del patrimonio e sulla contabilità generale dello Stato possono essere sostituiti a tutti gli effetti anche ai fini della resa dei conti amministrativi o giudiziari, da evidenze informatiche o da analoghi strumenti di rappresentazione e di trasmissione;
- che con deliberazione in data 9.11.1995 dell'ex Autorità per l'Informatica (AIPA), adesso Centro nazionale per l'informatica nella Pubblica Amministrazione (CNIPA) ha provveduto alla definizione delle regole tecniche per il mandato informatico;
- che con D.P.R. 28.7.1999, n. 318, è stato emanato il regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'art. 15, comma 2, della legge 31.12.1996, n. 675;
- che con D.P.R. 28.12.2000, n. 445, è stato approvato il testo unico delle disposizioni

- legislative e regolamentari in materia di documentazione amministrativa;
- che con D.Lgs. 23.01.2002, n. 10, sono state emanate le disposizioni legislative per il recepimento della direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13.12.1999, relativo ad un quadro comunitario per le firme elettroniche;
 - che con D.P.R. 7.4.2003 n. 137 è stato emanato il regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'art. 13 del D.Lgs. 23.01.2002, n. 10;
 - che, ai sensi dell'art. 2 del succitato D.Lgs. n. 10/2002, si intende per firma elettronica avanzata (firma digitale) "la firma elettronica ottenuta attraverso una procedura informatica che garantisca la connessione univoca al firmatario e la sua identificazione, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati";
 - che, ai sensi dell'art. 6 del succitato D.Lgs. n. 10/2002 che ha sostituito il disposto dell'art. 10 del D.P.R. n. 445/2000, "il documento informatico quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa (inoltre) piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto";
 - che, ai sensi del già citato art. 2 del D.Lgs. n. 10/2002, i certificati qualificati (ossia gli attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi) sono i certificati elettronici conformi ai requisiti di cui alla direttiva 1999/93/CE rilasciati da certificatori iscritti nell'elenco pubblico tenuto dall'Autorità per l'Informatica nella Pubblica Amministrazione ai sensi dell'art. 27, comma 3, del D.P.R. n. 445/2000.
- a) la Circolare ABI numero 80 del 29/12/2003 e relativo allegato tecnico;
 - b) la Deliberazione CNIPA n.4 del 17/02/2005 "Regole per il riconoscimento e la verifica del documento informatico"
 - c) le Linee Guida per l'utilizzo della Firma Digitale con data maggio 2004;
- che con D.Lgs. 7.03.2005 n. 82, è stato approvato il codice dell'amministrazione digitale.

Art. 1 - Scopo, oggetto e limiti del protocollo

Il Comune di Urbino si avvale di strumenti informatici e telematici per la prestazione del servizio di tesoreria. Conseguentemente i documenti cartacei in uso sono sostituiti con documenti informatici: in particolare gli ordinativi di incasso (reversali) e gli ordinativi di pagamento (mandati) sono generati e trasmessi dall'ente al tesoriere in veste elettronica (ordinativi informatici) secondo le specifiche (tecniche e procedurali) descritte nell'allegato 1 alla convenzione.

L'apposizione della firma digitale ai documenti informatici e le attività di gestione, trasmissione e conservazione degli stessi dovranno rispettare la normativa vigente e conformarsi alle indicazioni tecniche emanate dal CNIPA.

I contenuti dei flussi elettronici relativi agli ordinativi di incasso (reversali) ed agli ordinativi di pagamento (mandati) sono descritti analiticamente nell'Allegato 1, denominato: "Allegato

tecnico sul formato dei flussi”, che costituisce parte integrante della convenzione.

Art. 2 - Documento informatico.

Per documento informatico si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Il documento informatico da chiunque formato, l'archiviazione su supporto informatico e la trasmissione con strumenti telematici, sono validi e rilevanti a tutti gli effetti di legge se conformi alla normativa vigente. Restano ferme le disposizioni di legge sulla tutela dei dati personali.

Il documento informatico munito dei requisiti previsti dalla normativa vigente soddisfa il requisito legale della forma scritta. Gli obblighi fiscali relativi ai documenti informatici sono assolti secondo le modalità definite con decreto del Ministro delle finanze. Il documento informatico, sottoscritto con firma digitale basata su di un certificato qualificato e generata mediante un dispositivo per la creazione di una firma sicura, fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto.

Art. 3 Documenti informatici delle pubbliche amministrazioni.

Gli atti formati con strumenti informatici, i dati e i documenti informatici delle pubbliche amministrazioni, costituiscono informazione primaria ed originale da cui è possibile effettuare, su diversi tipi di supporto, riproduzioni e copie per gli usi consentiti dalla Legge. Nelle operazioni riguardanti le attività di produzione, immissione, archiviazione, riproduzione e trasmissione di dati, documenti ed atti amministrativi con sistemi informatici e telematici, ivi compresa l'emanazione degli atti con i medesimi sistemi, devono essere indicati e resi facilmente individuabili sia i dati relativi all'amministrazione interessata sia il soggetto che ha effettuato l'operazione. Le regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni sono definite dallo CNIPA.

Art. 4 - Firma digitale.

Per firma digitale s'intende il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici. A ciascun documento informatico, o a un gruppo di documenti informatici, nonchè al duplicato o copia di essi, può essere apposta, o associata con separata evidenza informatica, una firma digitale. L'apposizione o l'associazione della firma digitale al documento informatico equivale alla sottoscrizione prevista per gli atti e documenti in forma scritta su supporto cartaceo. La firma digitale deve riferirsi in maniera univoca ad un solo soggetto ed al documento o all'insieme di documenti cui è apposta o associata. Per la generazione della firma digitale si deve utilizzare una chiave privata la cui corrispondente chiave pubblica non risulti scaduta di validità ovvero non risulti revocata o sospesa ad opera del soggetto pubblico o privato che l'ha certificata. L'uso della firma apposta o associata mediante una chiave revocata, scaduta o sospesa equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione,

non dimostri che essa era già a conoscenza di tutte le parti interessate. L'apposizione della firma digitale integra e sostituisce, ad ogni effetto previsto dalla normativa vigente, l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere. Attraverso la firma digitale devono potersi rilevare, nei modi e con le tecniche stabiliti, gli elementi identificativi del soggetto titolare della firma, del soggetto che l'ha certificata e del registro su cui essa è pubblicata per la consultazione. In tutti i documenti informatici delle pubbliche amministrazioni la firma autografa, o la sottoscrizione comunque prevista, è sostituita dalla firma digitale.

Art. 5 - Sistema di validazione.

Per sistema di validazione si intende il sistema informatico e crittografico in grado di generare ed apporre la firma digitale o di verificarne la validità.

Art. 6 - Sistema di chiavi.

Per chiavi asimmetriche si intende la coppia di chiavi crittografiche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di validazione e di cifratura di documenti informatici. Per chiave privata si intende l'elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico o si decifra il documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica. Per chiave pubblica si intende l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche o si cifrano i documenti informatici da trasmettere al titolare delle predette chiavi. Per chiave biometrica si intende la sequenza di codici informatici utilizzati nell'ambito di meccanismi di sicurezza che impiegano metodi di verifica dell'identità personale basati su specifiche caratteristiche fisiche dell'utente.

Art. 7 - Certificazione.

Per certificazione si intende il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave e il termine di scadenza del relativo certificato, in ogni caso non superiore a tre anni. Le chiavi pubbliche di cifratura sono custodite per un periodo non inferiore a dieci anni a cura del certificatore e, dal momento iniziale della loro validità, sono consultabili in forma telematica. Le attività di certificazione sono effettuate da certificatori inclusi in apposito elenco pubblico, consultabile in via telematica, predisposto, tenuto e aggiornato a cura dell'autorità per l'informatica nella pubblica amministrazione.

Le chiavi, i certificati e gli algoritmi utilizzati per il sistema di interscambio tra le parti coinvolte nel processo di Firma Digitale (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 e relativo supporto fisico :

- *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 e relativo supporto fisico (es. Hardware crittografico):

- *Un certificato di firma;*
- *Il certificato dell'Autorità di Certificazione che ha emesso i certificati di firma.*

Art. 8 - Conservazione delle chiavi.

Le chiavi private sono conservate e custodite all'interno di un dispositivo di firma. E' possibile utilizzare lo stesso dispositivo per conservare più chiavi. E' vietata la duplicazione della chiave privata o dei dispositivi che la contengono. Per fini particolari di sicurezza, è consentita la suddivisione della chiave privata su più dispositivi di firma. Il titolare delle chiavi deve:

- a) conservare con la massima diligenza la chiave privata e il dispositivo che la contiene al fine di garantirne l'integrità e la massima riservatezza;
- b) conservare le informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave;
- c) richiedere immediatamente la revoca delle certificazioni relative alle chiavi contenute in dispositivi di firma di cui abbia perduto il possesso o difettosi;
- d) le parti si impegnano a non attivare processi di firma a fronte di certificati scaduti;
- e) le parti rigettano, in ogni caso, documenti firmati digitalmente il cui certificato risulti scaduto o revocato al momento della verifica, indipendentemente dal fatto che la firma sia stata apposta in condizioni di validità del certificato stesso (non scaduto o non revocato) o non esistano le condizioni minime per la verifica dei certificati digitali (es. reperimento o verifica dell'integrità della Certificate Revocation List rilasciata dalle Registration Authority);
- f) 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.

Le regole tecniche relative ai controlli formali dei flussi sono indicate nell'Allegato B, denominato "Allegato tecnico dei controlli formali", che costituisce parte integrante e sostanziale del presente disciplinare.

Art. 9 – Sicurezza

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.

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
Pacchetti di ordinativi (man/rev)	Nessuna Firma	<ul style="list-style-type: none"> • Autenticità della struttura, mediante schema xsd di condivisione • Univocità e condivisione del documento di trasporto atto a contenere i singoli ordinativi
Ordinativi (man/rev)	Firma digitale	<ul style="list-style-type: none"> • Autenticità dell'origine • integrità dei dati • non ripudio dell'invio
Ricevuta di servizio ed applicativa	Firma digitale	<ul style="list-style-type: none"> • Autenticità dell'origine • integrità dei dati • non ripudio dell'invio della ricevuta • non ripudio della ricezione degli ordinativi a cui si riferiscono (le ricevute applicative)

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:

Il 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 Version 1.5.

Il certificato del firmatario è incluso nel PKCS#7 SignedData. dati su cui viene calcolata la firma che 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.

Art. 10 – Requisiti postazione di lavoro dell'Ente

Vengono riportati di seguito i requisiti minimi per poter utilizzare il servizio ... :

- ✓ Occorre disporre di un computer equipaggiato con sistemi operativi: Microsoft Windows (98/NT/2000/2003/XP/VISTA) oppure Linux (redhat, etc.);
- ✓ Occorre che il pc sia dotato di una connessione ad internet;
- ✓ E' consigliabile utilizzare una versione recente dei browser diffusi sul mercato: Internet Explorer 5.5 o superiore, Mozilla Firefox, Netscape 7.0 o superiore;
- ✓ E' necessario che gli utenti, coinvolti nelle sole operazioni di firma digitale, siano "amministratori di macchina", o che abbiano le abilitazioni (grant) necessarie ad eseguire ed installare programmi Web;
- ✓ Occorre disporre di un lettore di smart-card, collegato al pc e con gli appositi driver correttamente installati sul computer, oltre alle librerie pkcs#11. Queste vengono

- installate unitamente ai driver di firma delle singole smart-card.
- ✓ E' necessario configurare il browser affinché consenta l'esecuzione di script e di applicazioni di programmi Web (Applet Java), in modalità sicura (ponendo, ove previsto dal Browser, le Autorizzazioni Java in Protezione Alta).
 - ✓ E' necessario avere installato, sulla postazione di lavoro, l'ambiente Java Runtime Plugin, in molti casi questa componente è già presente sui pc perché facente parte del sistema operativo. Per verificarne la presenza controllare la lista dei software installati sul sistema (es. in windows installazione/applicazioni nome programma J2SE Runtime Environment 5.0). Qualora questo programma non fosse presente sul sistema l'Applet ne richiede l'installazione in maniera automatica. Quindi, alla richiesta del software confermare lo scarico del java runtime. Si consiglia di utilizzare una versione dalla 1.4.x in poi.

Art. 11 – Accesso al sistema

Il Comune, ai sensi del vigente Regolamento di Contabilità, autorizza il responsabile del servizio finanziario e le persone comunque ed in ogni caso designate allo svolgimento delle attività di formazione, trasmissione e sottoscrizione degli ordinativi elettronici con firma digitale, a compiere tutte le operazioni e gli interventi necessari ai fini della trasmissione per via telematica al Tesoriere degli ordinativi di riscossione (reversali) e degli ordinativi di pagamento (mandati) in veste elettronica e di ogni altro documento nella stessa veste, inerente alla gestione del servizio di tesoreria e ad apporre o associare agli stessi la propria rispettiva firma digitale.

Si dà atto, in particolare, che la sottoscrizione avverrà sempre in maniera disgiunta tra due incaricati del Comune e che i nominativi facoltizzati alla sottoscrizione ed i relativi poteri, saranno di volta in volta comunicati al Tesoriere per il necessario inserimento nella procedura applicativa di gestione che la Banca utilizza per acquisire i dati dei firmatari designati dall'Ente.

Art. 12 - Codici di accesso.

Ai fini del riconoscimento del soggetto (Ente) durante l'utilizzo del servizio e della firma digitale, per garantire e verificare l'integrità, la riservatezza, la legittimità e la non ripudiabilità dei documenti trasmessi in veste elettronica, si renderà necessaria l'implementazione di un sistema di codici di accesso.

Detti codici sono strettamente personali e non devono essere divulgati o comunicati ad alcuno. L'utente è l'unico responsabile della custodia dei codici e del loro regolare e legittimo utilizzo nei confronti dell'Ente al quale soltanto - e non al tesoriere - risalirà l'eventuale danno conseguente all'uso improprio dei codici suddetti. In caso di smarrimento o furto dei codici, l'utente deve darne immediata comunicazione al Tesoriere con ogni mezzo che consenta una sommaria verifica circa l'identità di chi effettua la comunicazione, e deve, altresì, far seguire a mezzo raccomandata con avviso di ricevimento l'invio di una copia della denuncia all'Autorità di Polizia.

Il Tesoriere, non appena in possesso della comunicazione dell'ente, ove per comunicazione si deve intendere anche la telefonata di un dipendente comunale purchè nota e conosciuta al Tesoriere, provvederà a disattivare i codici.

Si dà tuttavia atto che la generazione del procedimento per l'assegnazione di una nuova coppia di codici sarà effettuata dal tesoriere solo dopo l'avvenuta ricezione da parte dello stesso della denuncia presentata dall'ente all'Autorità di Polizia.

Art. 13 - Trasmissione dei documenti.

Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario se trasmesso all'indirizzo elettronico da questi dichiarato. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alle disposizioni del regolamento approvato con il D.P.R. n. 513/1997 ed alle regole tecniche di cui all'art. 3, sono opponibili ai terzi. Per indirizzo elettronico si intende l'identificazione di una risorsa fisica o logica in grado di ricevere e registrare documenti informatici. E' inteso che ogni flusso contenente disposizioni firmate digitalmente dovrà essere inviato all'indirizzo Web del portale di Tesoreria della Banca (<http://www.>).

Art. 14 - Trasmissione ordinativi dall'Ente al Tesoriere.

L'Ente provvede alla trasmissione per via telematica dell'archivio contenente gli ordinativi di incasso e di pagamento sottoscritto mediante firma digitale.

In ogni caso, la trasmissione dovrà avvenire con strumenti o con modalità che garantiscano, mediante cifratura, la riservatezza delle informazioni trasmesse (es. protocollo Internet sicuro: HTTPS SSL a 128 bit).

L'archivio, predisposto secondo le allegate specifiche tecniche fornite dal Tesoriere, deve contenere tutte le informazioni previste per i documenti della specie e comunque necessarie per dar corso alle operazioni di incasso e di pagamento.

Art. 15 - Ricezione degli ordinativi da parte del Tesoriere.

Il Tesoriere, all'atto del ricevimento dei flussi contenenti gli ordinativi di riscossione e gli ordinativi di pagamento in veste elettronica, provvede a rendere disponibile un messaggio attestante la semplice ricezione del flusso, con riserva di verificarne il contenuto. Eseguita la verifica del contenuto del flusso suddetto ed acquisiti i dati nel proprio sistema informativo, il tesoriere predispone e trasmette all'ente, per via telematica, un successivo documento informatico destinato all'Ente, sottoscritto con firma digitale, contenente il risultato dell'acquisizione, segnalando i documenti presi in carico e quelli non potuti acquisire; per questi ultimi sarà evidenziata la causa che ne ha impedito l'assunzione.

Rimane comunque inteso che il trattamento dei dati contenuti nell'archivio suddetto pervenuti alla Banca nei giorni e nelle ore di chiusura al pubblico degli sportelli bancari non potrà avere luogo prima delle ore 9 (nove) del primo giorno bancabile successivo a quello di ricevimento dell'archivio stesso.

Art. 16 –Messaggi Scambiati

I tipi di messaggi previsti sono il mandato di pagamento, la reversale di incasso, la ricevuta di servizio e la ricevuta applicativa. Ogni messaggio è costituito da una intestazione da una componente di dettaglio avente contenuto diverso in funzione del tipo di messaggio.

Messaggi contenenti mandati

L'ente raggruppa più mandati in un unico pacchetto di scambio. Il pacchetto costituisce la struttura atta a contenere i singoli ordinativi di mandati ed è costituito da singoli file di tipo XML. Ogni ordinativo, prima di essere spedito alla tesoreria, deve essere firmato digitalmente, con l'apposizione di una doppia firma digitale.

Messaggi contenenti reversali

L'ente raggruppa più reversali in un unico pacchetto di scambio. Il pacchetto costituisce la struttura atta a contenere i singoli ordinativi di reversali ed è costituito da singoli file di tipo XML. Ogni ordinativo, prima di essere spedito alla tesoreria, deve essere firmato, con l'apposizione di una firma digitale.

Ricevuta di servizio

In seguito alla ricezione di ogni pacchetto, la tesoreria emette una ricevuta di servizio nella quale riporta l'esito dei controlli di sicurezza e dei controlli sulla sintassi dell'XML ricevuto (XML valido e ben formato). Nel caso in cui tali controlli evidenzino degli errori, l'intero pacchetto viene rifiutato dalla tesoreria. Ogni ricevuta di servizio viene inviata singolarmente e viene sottoscritta con firma digitale. Dopo le fasi di controllo del pacchetto vengono analizzati i singoli ordinativi in esso contenuti, per ciascuno viene generata una ricevuta di servizio, che riporta l'esito dei controlli di sicurezza e di integrità delle informazioni trasmesse. La singola ricevuta di servizio, indistintamente dall'esito evidenziato ("OK" o "KO"), viene inviata singolarmente e viene sottoscritta con firma digitale apposta dal Tesoriere.

Ricevuta applicativa

A seguito dell'elaborazione dei singoli ordinativi (mandati di pagamento o reversali di incasso), la tesoreria emette una ricevuta applicativa nella quale riporta l'esito dell'elaborazione stessa. Ogni ricevuta applicativa viene inviata singolarmente e viene sottoscritta con firma digitale apposta dal Tesoriere.

Si precisa in maniera univoca che tutti tracciati (ordinativo e ricevute) utilizzati nella gestione dell'ordinativo informatico, 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).

Art. 17 - Esecuzione delle operazioni.

Le parti contraenti si danno reciprocamente atto che lo svolgimento del servizio di tesoreria comunale continua ad essere disciplinato, oltre che dalle leggi e dai regolamenti che disciplinano la materia, anche dalle norme, dai patti e dalle condizioni di cui alla convenzione di tesoreria in corso, non incompatibili e non derogate, neppure implicitamente e tacitamente, dalle norme, dai patti e dalle condizioni di cui al presente disciplinare e dagli allegati tecnici che ne formano parte integrante e sostanziale.

In particolare:

- gli ordinativi di incasso ed i ordinativi di pagamento saranno in veste informatica e saranno trasmessi dall'Ente al Tesoriere in ordine cronologico per via telematica;
- in luogo e in sostituzione della copia della distinta cartacea di accompagnamento degli ordinativi di incasso e dei mandati di pagamento data e firma in segno di ricevimento dei documenti in essa indicati, il Tesoriere trasmetterà all'Ente per via telematica il messaggio di avvenuta ricezione firmato anch'esso digitalmente;

- l'Ente, al fine di consentire una corretta gestione degli ordinativi di incasso e dei mandati di pagamento, trasmetterà al Tesoriere – in luogo e in vece delle firme autografe con la precisazione delle generalità e delle qualifiche delle persone autorizzate a sottoscrivere detti ordinativi e mandati di pagamento – i corrispondenti certificati pubblici di sottoscrizione di ciascun firmatario dai quali risulta la sussistenza dei poteri di rappresentanza o di altri titoli relativi alle cariche rivestite nonché l'indicazione del provvedimento di attribuzione o di conferimento della attribuzioni e dei poteri stessi, in conformità al disposto dell'art. 28, lettera c), del D.P.R. n. 445/2000;
- a comprova dei pagamenti effettuati, il Tesoriere raccoglierà, ove del caso, la quietanza del creditore su foglio separato da trattenere ai propri atti e provvederà ad annotare gli estremi del pagamento effettuato sulla pertinente documentazione meccanografica da consegnare all'Ente in allegato al proprio rendiconto;
- a fronte dell'incasso il Tesoriere rilascerà, come previsto dalla convenzione di tesoreria in corso, in luogo e vece dell'Ente, regolari bollette numerate in ordine cronologico per esercizio finanziario, esclusivamente compilate con procedure informatiche su moduli meccanizzati. Soltanto a fine esercizio, sulla base delle bollette come sopra rilasciate, il Tesoriere provvederà all'elaborazione della documentazione meccanografica, comprensiva delle matrici di dette bollette, da consegnare all'Ente in allegato al proprio rendiconto.

Rimane inteso che:

- il Tesoriere consegnerà annualmente al Comune di Urbino, entro la scadenza del rendiconto di cui all'art.226 del TU di cui al D.Lgs 267/2000 un supporto multimediale (cd) contenente ogni ricevuta applicativa della gestione elettronica, gli ordinativi salvati in formato atto a riprodurne in chiaro il contenuto (ad es. "pdf" o "txt" o "word" o sistemi analoghi) sottoscrivendolo con firma digitale. Tale supporto sarà integrato anche con il file relativo al conto del tesoriere che continuerà ad essere redatto secondo lo schema cartaceo attualmente in uso.