COMUNE DI PAVIA

Allegato F1: gestione telematica ordinativi Unimoney

Le seguenti specifiche tecniche sono state fornite dalla ditta Unimatica spa, attuale fornitrice del software per la gestione telematica degli ordinativi.

UniMoney

Specifiche Tecniche

Verificato da
Arnaldo Ianieri

Approvato da
Ezio Rimondi

UniDistinte:

Dati identificativi del documento :

1 Versione del documento	1
Autore	Arnaldo Ianieri
Data di pubblicazione	04/05/2011
Scopo del documento	Descrive le funzionalità principali del prodotto UniMoney
Rivolto a	Utenti della ragioneria e dei servizi
Nome e versione del software	UniMoney
Organizzazione	Unimatica S.p.A.

Restrizioni all'utilizzo del documento :

2 Hardware	
Comunicazioni	
Sistemi Operativi	

Revisione	Data	Motivo Revisione	Emesso da	Approvato da

Indice

1 Introduzione

UniMoney permette una gestione automatizzata dell'ordinativo informatico, in modalità ASP, per gli Enti di diverse dimensioni sia per il servizio di cassa che di tesoreria.
Tutti i flussi prodotti dall'Ente vengono visualizzati in formato xml sia preventivamente che successivamente l'apposizione della firma digitale; apposta la firma digitale agli ordinativi, il sistema invia gli stessi alla banca e si predispone per l'acquisizione delle ricevute.

2 Modalità di comunicazione

Tutte le comunicazioni tra il sistema di contabilità dell'Ente ed UniMoney avvengono in https e tramite l'utilizzo di web service.
Sia i documenti prodotti dal sistema di contabilità sia quelli provenienti dal Tesoriere sono criptati.
L'Ente può decidere di produrre e ricevere i files sia in formato testo che in formato xml. Nel caso sia prodotto un tracciato testo compatibile con il tracciato della propria banca tesoriera UniMoney si occupa della relativa conversione in formato xml.
Se il sistema di contabilità dell'ente è predisposto per aggiornare i propri archivi con files in formato testo, UniMoney si attiva per eliminare la firma dalle ricevute prodotte dalla banca e per convertirle in formato testo.

3 Documenti scambiati

UniMoney comunica con il sistema di contabilità dell'ente mediante flussi o tabelle di database, preparate appositamente per la comunicazione.
In entrambi i casi i documenti scambiati sono:

- mandati
- reversali
- ricevute di servizio
- ricevute di carico
- ricevute di esecuzione

I mandati e le reversali si trasferiscono dal sistema di contabilità dell'Ente verso Unimoney.
Le ricevute vengono rese disponibili all'Ente per consentire l'eventuale aggiornamento dello stato dei propri ordinativi.

4 Modalità di funzionamento

Gli ordinativi esportati dalla contabilità vengono automaticamente intercettati dalla sonda ed inviati ad Unimoney. Gli utenti possono visualizzare i documenti in formato html, xml (obbligatorio per i firmatari) e pdf (eventualmente personalizzabile in modo da riprodurre la stesso layout dei documenti cartacei).
UniMoney è un sistema documentocentrico, quindi anche se il file prodotto dalla contabilità contiene centinaia di ordinativi, UniMoney consente di gestirli singolarmente.
E' possibile esaminare, inviare alla firma, confermare e firmare singolarmente ogni ordinativo. Per quanto riguarda l'apposizione della firma digitale è sufficiente inserire il pin una sola volta per firmare tutti i documenti selezionati singolarmente (quindi *non firma del flusso, ma firma dei documenti*).
Unimoney, quindi, riproduce in modalità digitale la normale operatività manuale che gli Enti attivano per gli ordinativi cartacei.

Infatti è possibile:

- verificare (sia automaticamente che manualmente) i documenti
- inviare i documenti alla firma (equivale a spostarli sulla scrivania del firmatario)
- retrocedere un documento erroneamente inviato alla firma
- firmare digitalmente i documenti, inserendo una sola volta il pin. UniMoney firma singolarmente tutti gli ordinativi selezionati tra quelli pronti per la firma
- rifiutare un documento alla firma indicandone la motivazione. Visualizzata la motivazione dall'operatore che aveva trasmesso il documento, è possibile procedere ad eventuali rettifiche o annullamenti
- effettuare una o più fasi di conferma, eventualmente con firma digitale (tale firma non sarà portata a conoscenza della banca: in pratica questo processo equivale al classico visto sul documento cartaceo)
- visualizzare lo stato dei documenti
- ricercare documenti in base ai parametri richiesti
- produrre insiemi di ordinativi e di ricevute per esempio a fini di rendicontazione nei formati p7m, pdf o entrambi
- visualizzare la storia dei documenti con i collegamenti a tutte le ricevute
- selezionare una molteplicità di documenti al fine di visualizzarli singolarmente prima della firma

In UniMoney è, inoltre, possibile articolare la gestione dei documenti con le seguenti modalità:

- per struttura organizzativa dell’Ente
- per utente

la suddivisione per struttura è una suddivisione rigida in quanto gli utenti possono consultare solamente i documenti appartenenti alla propria struttura e non sono in grado di visualizzare i documenti prodotti da strutture diverse. La suddivisione per utente, al contrario, è più leggera: può essere disabilitata con una check box nelle pagine di documenti e ciò consente di accedere ai documenti predisposti dai colleghi della stessa struttura.

5 Glossario

Di seguito una descrizione sommaria dei termini non colloquiali per semplificare la lettura del documento.

BASE64

Standard di codifica e decodifica di stringhe binarie arbitrarie in stringhe di testo che possono essere tranquillamente spedite tramite email, usate come parti di URL o incluse come parti di richieste HTTP POST (Si veda anche RFC 3548).

Browser

Un browser è un programma che consente la navigazione nella rete internet, più precisamente nel World Wide Web. La funzione primaria di un browser è quella di interpretare il codice HTML (e più recentemente XHTML) e visualizzarlo in forma di ipertesto.

CNIPA

Il *Centro Nazionale per l'Informatica nella Pubblica Amministrazione* (CNIPA) opera presso la Presidenza del Consiglio per l'attuazione delle politiche del Ministro per l'Innovazione e le Tecnologie.
Unifica in sé due organismi preesistenti: l'*Autorità per l'Informatica nella Pubblica Amministrazione* (AIPA) ed il Centro Tecnico per la R.U.P.A.
Obiettivo primario del CNIPA è di supportare la pubblica amministrazione ad utilizzare efficacemente l'informatica per migliorare la qualità dei servizi e contenere i costi dell'azione amministrativa.

Dispositivo di firma digitale

Secondo la definizione ***CNIPA*** nel documento "Linee guida per l'utilizzodella Firma Digitale Versione 1.1 – maggio 2004" un Dispostivo di firma digitale è l'insieme di dispositivi hardware e software che consentono di sottoscrivere con firma digitale documenti informatici.

5.1.1.1.1 Documento Informatico

la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.(DPR 28 dicembre 2000 n. 445)

5.1.1.1.2 Firma digitale

La firma digitale è una tecnica crittografica che permette di legare un ***Documento informatico*** ad un firmatario in modo certificabile e sicuro. La firma sigilla il documento rivelando ogni tentativo di manomissione e permettendo di identificare univocamente il firmatario.

Forma canonica

La forma canonica di un documento ***XML*** è una sua rappresentazione fisica che risulta essere invariante rispetto alle possibili differenze sintattiche del documento stesso (ad esempio l'ordine degli attributi, la presenza di spazi bianchi, etc.).

GZip

Gzip è un formato di compressione che riduce la dimensione dei file usando la codifica di Lempel-Ziv (LZ77). Quando è possibile, ogni file è rimpiazzato da uno con l'estensione .gz, mantenendo le stesse proprietà, date d'accesso e di modifica (l'estensione predefinita è -gz per VMS, z per MSDOS, OS/2 FAT, Windows NT FAT e Atari)

Hash

Hash, nella sua accezione più comune, si riferisce ad una funzione univoca operante in un solo senso (ossia, che non può essere invertita) atta alla trasformazione di un testo in chiaro e di lunghezza arbitraria in una stringa di lunghezza relativamente limitata.
Tale stringa rappresenta una sorta di "impronta digitale" del testo in chiaro, e viene detta "*valore di hash*" o "*checksum crittografico*".
Non esiste una corrispondenza biunivoca tra l'hash e il testo. I testi possibili, con dimensione finita maggiore dell'hash, sono più degli hash possibili, quindi ad almeno un hash corrisponderanno più testi possibili.
Un hash criptograficamente sicuro non dovrebbe permettere di risalire, in un tempo congruo con la dimensione dell'hash, ad un testo che possa generarlo (che per i più resistenti è, attualmente, superiore alla durata dell'universo, applicando tutta la capacità computazionale immaginabile).
Un algoritmo di hashing comunemente utilizzato nella crittografia è SHA1 (*Secure Hash Algorithm 1*) corrispondente alla specifica RFC 3174.

5.1.1.1.3 HDML

Handheld Device Markup Language (HDML) è un linguaggio a marcatori progettato per l'utilizzo su display di computer palmari, smartphones etc. E' simile ad HTML ma per dispositivi palmari e wireless con piccoli display come i PDA, i mobile phones e così via.

HTTP

HTTP è l'acronimo di HyperText Transfer Protocol (protocollo di trasferimento di un ipertesto). Usato come principale sistema per la trasmissione di informazioni sul web. Le specifiche del protocollo sono attualmente in carica al W3C (World Wide Web Consortium)
L'HTTP funziona su un meccanismo richiesta/risposta: il client esegue una richiesta ed il server restituisce la risposta. Nell'uso comune il client corrisponde al browser ed il server al sito web. Vi sono quindi due tipi di messaggi HTTP: messaggi richiesta e messaggi risposta.
Il messaggio richiesta può essere fatto con due diverse modalità : GET e POST.
GET è stato concepito in origine per chiedere informazioni ad un server, inviando pochi parametri tramite URL, attraverso la stringa di query. Il POST invece è stato concepito in origine per inviare al server molte informazioni, senza un limite sulla quantità di dati da trasmettere e sul tipo (cfr. File), ed in modo non visibile da URL.
Realisticamente il metodo POST sostituisce quello GET nel caso la richiesta effettuata tramite GET superi il massimo dei caratteri consentiti dal server (ad esempio 256) e le informazioni da inviare non siano solo di tipo alfanumerico (p.e. immagini, programmi, etc.), mentre il metodo GET è utile quando si desideri rendere possibile al browser registrare la chiamata in un bookmark.

HTTPS

Con il termine HTTPS ci si riferisce al protocollo ***HTTP*** (*Hyper Text Transfer Protocol*) utilizzato in combinazione con lo strato ***SSL*** (*Secure Socket Layer*).
HTTPS si utilizza in tutte quelle eventualità in cui è necessario attivare un collegamento sicuro (transazioni di pagamento nei siti di e-commerce, transazioni e/o interrogazioni di informazioni riservate, altro); in questo caso SSL garantisce la cifratura dei dati trasmessi e ricevuti su internet. Una possibilità ulteriore fornita da HTTPS è effettuare la Client Authentication, ovvero impostare il server Web in modo che questo non accetti nessun client che non abbia un certificato emesso da una CA fidata. In questo modo tutte le richieste devono avvenire attraverso connessioni SSL e devono arrivare da client che hanno certificati emessi da CA fidate, rendendo possibile l'autenticazione di client senza distribuire e gestire username e password.

Con questa opzione settata il server richiede al client un certificato quando questo si collega al sito https://.

Impronta

La definizione di impronta è riportata nell'art. 1 comma d. del DPCM 13 gennaio 2003.
" impronta di una sequenza di simboli binari (bit), la sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di ***hash***".
Nella pratica l'impronta di un file è una sequenza di numeri di lunghezza fissa che permettono di identificare univocamente il file.
Calcolata su un documento informatico, consente di identificare il documento stesso. Le due informazioni contenute in una ***marca temporale*** (impronta del documento e orario) forniscono una prova di esistenza del documento alla data riportata nella marca temporale stessa.

Login

Un sistema multiutente può essere utilizzato contemporaneamente da utenti diversi.
Ad ogni utente del sistema viene assegnato uno user name (nome utente) che lo identifica univocamente: quando si inizia una sessione di lavoro si deve "entrare" nel sistema tramite una procedura (detta *di login***)** durante la quale dovremo farci riconoscere dal sistema mediante l'introduzione del nostro user name pubblico e della nostra password (parola d'ordine) segreta

Marca Temporale

Le marche temporali sono messaggi firmati digitalmente che legano in modo sicuro e verificabile un qualsiasi documento informatico ad un riferimento affidabile di tempo, data e ora. Secondo la normativa, una marca temporale è "una evidenza informatica che consente la validazione temporale" (art. 1 comma i. del DPCM 13 gennaio 2004).
Nella marca sono contenute le seguente informazioni:

- data e ora della creazione della marca
- nome dell'emittente della
- ***impronta*** del documento cui la marca fa riferimento

La marca temporale il cui formato e modalità di richiesta sono descritte nella RFC 3161 viene detta anche Timestamp.

MIME

Il Multipurpose Internet Mail Extensions, o più brevemente MIME è un protocollo Internet che estende l'SMTP (Simple Mail Transfer Protocol) per permettere ai dati, come dati video, suoni e file binari, di essere trasmessi tramite la posta elettronica senza dover prima essere convertiti in formato ASCII; questa operazione viene compiuta mediante l'uso di vari tipi di MIME, che descrivono il contenuto di un documento. Un'applicazione compatibile MIME che invia un file, assegna un tipo di MIME al file. L'applicazione ricevente, che deve essere

anch'essa compatibile MIME, fa riferimento a un elenco standard di documenti organizzati per tipi e sottotipi di MIME al fine di interpretare il contenuto del file. Per esempio, un tipo di MIME è text che ha un certo numero di sottotipi, tra i quali plain e html. Un tipo di MIME text/html fa riferimento ad un file che contiene un testo scritto in HTML. MIME è parte di HTTP e, sia i browser web che i server HTTP lo utilizzano per interpretare i file di posta elettronica che inviano e ricevono.

Esempio di messaggio MIME:

```
From: John Doe <example@example.com>
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="XXXXboundary text"

Questo e' un messaggio MIME con piu' parti.

--XXXXboundary text
Content-Type: text/plain

Questo e' il corpo della mail

--XXXXboundary text
Content-Type: text/plain;
Content-Disposition: attachment;
        filename="test.txt"

Questo invece e' il testo allegato.

--XXXXboundary text--
```

MIME Multipart

Il tipo MIME multipart prevede la presenza di più componenti separate, con altrettante intestazioni specifiche. In questo caso si indica comunemente il confine tra una componente e l'altra attraverso una stringa particolare (di solito creata in modo da essere univoca), dichiarata con l'opzione boundary="stringa" nel campo Content-Type. Un tipo particolare di MIME Multipart è il form-data
Un messaggio "multipart/form-data" contiene una serie di parti, ciascuna rappresentante un controllo di un modulo dati. Questo formato è adatto al trasporto di grandi quantità di informazioni, file e dati binari contenenti caratteri non-ascii. Il formato “multipart/form-data” è quello normalmente prodotto dai browser web durante il submit di una form con il metodo POST.

5.1.1.1.4 Ordinativo Informatico

uno standard regolamentare e tecnico definito per consentire alle Banche tesoriere di eseguire gli ordini di incasso e pagamento degli Enti Pubblici solamente sulla base di input elettronici. (si veda a proposito (Legge Finanziaria 2005, Art. 1, comma 80)

PKCS

PKCS (*Public-Key Cryptography System*) rappresenta una serie di standard per la crittografia a chiave pubblica, sviluppate dalla RSA Data Security in accordo con un consorzio di società di informatica (Microsoft, Apple, Lotus, Sun…).
PKCS definisce lo standard per i certificati digitali, per la firma digitale e per le estensioni S/MIME di posta elettronica.

5.1.1.1.5 PIN

Persona Identification Number. E’ il numero segreto, comunicato all’utente dotato di ***firma digitale***, che gli consente di operare con la ***smart card*** ed, in particolare, di apporre la sua firma.

5.1.1.1.6 Registrazione

Una registrazione raccoglie, in base a criteri di omogeneità e di classificazione (fondo, serie, fascicolo), gruppi numericamente significativi di documenti elettronici ed è il risultato di una singola operazione di conservazione.

5.1.1.1.7 Smart card

E’ una carta elettronica delle dimensioni di una carta di credito che contiene i circuiti elettronici per effettuare le operazioni di ***firma digitale***. La smart card è un dispositivo ad alta sicurezza protetto da codice ***PIN***.

SOAP

SOAP (inizialmente acronimo di *Simple Object Access Protocol*) è un protocollo leggero per lo scambio di messaggi tra componenti software, tipicamente nella forma di componentistica software.
La parola object manifesta che l'uso del protocollo dovrebbe effettuarsi secondo il paradigma della programmazione orientata agli oggetti.
SOAP è una struttura operativa (framework) estensibile e decentralizzata che può operare sopra vari protocol stack per reti di computers.
I richiami di procedure remote possono essere modellati come interazione di parecchi messaggi SOAP.
SOAP dunque è uno dei protocolli che abilitano i *servizi Web* (***Web Service***).
SOAP può muoversi sopra tutti i protocolli di Internet, ma HTTP è il più comunemente utilizzato e l'unico ad essere stato standardizzato dal W3C.
SOAP si basa sul metalinguaggio ***XML*** e la sua struttura segue la configurazione Head-Body, analogamente ad HTML.
Il segmento opzionale Header contiene meta-informazioni come quelle che riguardano il routing, la sicurezza e le transazioni. Il segmento Body trasporta il contenuto informativo e talora viene detto carico pagante, payload. Questo deve seguire uno schema definito dal linguaggio XML Schema.

SSL

Secure Sockets Layer (SSL) è un protocollo progettato dalla Netscape Communications Corporation per realizzare comunicazioni cifrate su Internet. Questo protocollo utilizza la crittografia per fornire sicurezza nelle comunicazioni su Internet e consente alle applicazioni client/server di comunicare in modo tale da prevenire il 'tampering' (manomissione) dei dati, la falsificazione e l'intercettazione.

5.1.1.1.8 Supporto ottico

mezzo fisico che consente la memorizzazione di documenti informatici mediante l'impiego della tecnologia laser (quali, ad esempio, dischi ottici, magneto-ottici, DVD).

Nel presente documento si utilizza il termine supporto ottico in quanto utilizzato nella normativa sull'archiviazione, tutto il software qui descritto però gestisce in maniera generica supporti anche non ottici, in quanto è possibile un'evoluzione della tecnologia nel futuro.

5.1.1.1.9 Timestamp

Si veda ***Marca Temporale***

Upload

Il termine "Upload" indica l'operazione che un utente compie quando "trasferisce" un file, tramite il web, dal suo computer verso un server. è, quindi, l'operazione inversa del download, che indica lo scaricamento di un file da un server web sul computer dell'utente. Anche il protocollo HTTP supporta l'upload. L'upload di un file via HTTP si può ottenere lato client tramite il tag HTML <input type="file" />, purchè ovviamente il server sia predisposto per la ricezione.

UML

L'UML, Unified Modeling Language, è un linguaggio grafico usato, di solito ma non necessariamente, nell'ambito della progettazione software.

L'UML è un linguaggio che definisce una sintassi e delle regole di interpretazione; non si tratta quindi di una metodologia di progettazione e per questo motivo può essere adottato con diverse metodologie o in ambiti diversi da quello informatico.
Nell'ambito della progettazione software è utilizzato per progettare e documentare un'applicazione (un programma) a diversi livelli di dettaglio e per diverse prospettive.
L'UML si basa sul disegno grafico di diagrammi; questi si possono dividere in diagrammi statici e diagrammi dinamici.
I diagrammi di tipo statico danno una visione statica e strutturale del sistema che si sta descrivendo o progettando, mentre quelli dinamici cercano di coglierne gli aspetti evolutivi.
I diagrammi di tipo statico previsti dall'UML sono gli Use Case Diagram, Class Diagram, Object Diagram, Component Diagram, Deployment Diagram.
I diagrammi di tipo dinamico previsti dall'UML sono State Chart Diagram, Activity Diagram, Sequence Diagram, Collaboration Diagram.

URI

URI (*Uniform Resource Identifier*) è un identificatore comune di risorse, metodo comune di identificazione dei servizi presenti in rete, ideato per unificare la sintassi necessaria per riferirsi a risorse di tipo diverso, comprende URL, URN, URC.

ZIP

Lo ZIP è un formato di compressione dei file molto diffuso nei computer IBM-PC con sistemi operativi Microsoft e basato su una variante dell'algoritmo LZW.

Essendo un formato senza perdita di informazioni, viene spesso utilizzato per inviare programmi o file che non possono essere modificati dal processo di compressione. Nato in ambiente DOS, ha trovato con il passare del tempo validi concorrenti in altri formati, come ARJ, RAR o ACE che offrono un rapporto di compressione maggiore; la sua grande diffusione gli permette tuttavia di essere considerato uno standard de facto per tali sistemi. Ne esistono versioni per Unix e Mac OS, in cui però sono più diffusi altri software, più performanti, come ad esempio bzip2, gzip, StuffIt e DiskImage.

XML

XML (acronimo per Extensible Markup Language) è il formato definito dal World Wide Web Consortium (www.w3c.org) per l'interscambio di documenti e dati strutturati su Internet. Oltre all'universale affermazione come standard, l'XML presenta l'importante caratteristica di essere autoesplicativo e leggibile di per sé (senza programmi di visualizzazione particolari), il ché porta un ovvio vantaggio di durabilità e interscambio dei ***Documenti elettronici***.

5.1.1.1.10 XML Schema

XML Schema è una descrizione della struttura di un documento ***XML*** tramite un secondo documento XML (detto schema XSD).
Analogamente a quanto avviene con i DTD è possibile validare un documento rispetto al proprio schema

XML Signature

XML Signature è una tecnologia che permette di firmare digitalmente documenti ***XML*** o parti di essi, garantendone l'autenticità e l'integrità e restituendo documenti firmati che sono a loro volta documenti XML validi. Visto che la firma digitale è ovviamente molto sensibile alle variazioni del documento e quindi al fine di garantire il corretto funzionamento del meccanismo della firma digitale, la firma deve essere generato utilizzando la ***forma canonica*** del documento XML.

XSD

Si veda ***XML Schema***.

Web Service

I web service sono degli applicativi che pubblicano verso l'esterno dei metodi, richiamabili attraverso uno standard, che consentono di erogare dati verso il fruitore finale o fungere da interfaccia verso altri web service.
Consentono quindi di sviluppare una rete di punti di calcolo, ognuno specializzato in un proprio compito e con una propria business logic, pronti per l'interazione in un ambiente distribuito.
Il protocollo attraverso il quale un webservice accetta l'invocazione remota di metodi e rende disponibile i dati è il ***SOAP*** (Simple Object Access Protocol), che utilizza ***XML*** per l'encoding dei dati e HTTP o ***HTTPS*** per il trasporto.
In questo modo, qualsiasi client (eventualmente richiesto di autorizzazione) può dialogare con un dato web service, consentendo anche di utilizzare diverse piattaforme come interfaccia.
Questa tecnologia incoraggia il riutilizzo delle infrastrutture esistenti, con lo sviluppo di nuove funzionalità.
È dunque naturale disegnare ed implementare dei web service quando si tratta di interfacciare i mainframe storicamente presenti nell'architettura informatica di una grossa azienda, mantenendo la struttura di calcolo presente ma permettendone l'interazione verso le nuove applicazioni realizzate (in particolare rivolte al web).

5.1.1.1.11 WAP

WAP (acronimo di Wireless Application Protocol) Protocollo di Applicazione Senza Fili, dove per wireless si intende: telefoni cellulari, palmari, reti trasmissive senza fili e tutto quanto concerne la comunicazione mobile.
WAP è costituito da una serie di protocolli che permettono una navigazione del tutto simile a quella a cui siamo abituati, ma senza l'ausilio del personal computer e ricorrendo a specifici software per adattare il linguaggio del Web alle esigenze ed alle limitate potenzialità di un telefonino cellulare

5.1.1.1.12 WML

WML (acronimo di Wireless Markup Lenguage)è un linguaggio a marcatori, largamente basato sull'HDML, che rende accessibili ipertesti a "piattaforme alternative" ai personal computer ovvero telefoni cellulari, i PDA (Personal Digital Assistant) ovvero i palmari e i Pager (in Italia il

Teledrin)

WSDL

Lo standard WSDL (*Web Service Definition Language*) consente di descrivere un ***Web Service*** in tutti i suoi aspetti.
Un documento WSDL è un documento ***XML*** valido.
In un documento WSDL si trovano tutte le possibili chiamate che è possibile fare ad un servizio Web, le specifiche delle strutture dati di input ed output, gli URL per accedere ai servizi.
WSDL non è uno standard legato ad un livello di trasporto particolare (come ***SOAP***), ma è aperto all'utilizzo con protocolli differenti, specificando di volta in volta bindings (collegamenti) a questo o quell'altro protocollo.
Nonostante ciò, WSDL privilegia SOAP, indicando, in una sezione delle sue specifiche, le modalità di collegamento a questo standard.

Con in mano un documento WSDL, un integratore di sistemi è in grado di sapere come dialoga un determinato servizio