STRUMENTI A SUPPORTO DELLA CREAZIONE DI FRAMEWORK DI SCAMBIO DATI XML: L'ESPERIENZA DI MODA-ML

Alberto BUCCIERO[1], Luca MAINETTI[2], Massimo MARZOCCHI[3], Thomas IMOLESI[3], Aurelio MUZZARELLI[3]

[1] *SET-Lab, Università degli Studi di Lecce, Via Per Arnesano, 73100 Lecce - Italy*
[2] *Dip. Elettronica e Informazione, Politecnico di Milano, Via Ponzio 34/5, 20133 Milano - Italy*
[3] *Laboratorio XML, ENEA- FTI (Forum Tecnologia dell'Informazione), via Don Fiammelli 2, 40129 Bologna - Italy*

SOMMARIO

Il progetto MODA-ML (www.moda-ml.org) si occupa, in estrema sintesi, di interoperabilità tra sistemi eterogenei. Uno dei maggiori ostacoli all'affermazione del commercio elettronico Business-to-Business è stato finora l'eterogeneità degli approcci e degli strumenti scelti dalle aziende. Questo ha portato a sviluppare nuovi vocabolari e nuovi modelli tecnologici ed organizzativi che hanno contribuito a rendere più complessa e confusa la situazione. Fino ad oggi nessuna delle soluzioni proposte si è imposta come standard. E' evidente, dunque, la necessità di giungere ad una visione comune del modo di scambiare dati fra imprese nella nuova "economia digitale" e garantire così elevati livelli di interoperabilità.

1. IL PROGETTO MODA-ML

Nel progetto MODA-ML il problema dell'interoperabilità viene affrontato proponendo la costruzione di un framework verticale basato sulle tecnologie XML, applicato e sperimentato nelle aziende della filiera del Tessile Abbigliamento. Il progetto ha lo scopo di definire formati e protocolli di scambio e di rendere pubblico anche il software dimostrativo che implementa lo scambio di documenti XML basandosi sulle specifiche di trasporto ebXML. Le peculiarità del sistema Tessile/Abbigliamento italiano (estrema varietà dei soggetti industriali coinvolti, fortissima presenza di piccole e piccolissime imprese, una filiera molto lunga ma sensibilissima al fattore stagionale e moda, importanza della riservatezza delle informazioni sul prodotto) ha imposto dei vincoli molto stringenti in termini di flessibilità dell'architettura, abbassamento della soglia tecnologica minima per non essere esclusi dal flusso dei dati, critica dei modelli di scambio basati su servizi di terze parti (per esempio, i MarketPlace). Il risultato è un'architettura pensata per abbattere il nascente digital-divide tra le piccole e medie imprese a bassa capacità tecnologica ed i grandi gruppi in grado di investire in modo consistente in tecnologie dell'informazione.

La realizzazione del progetto MODA-ML ha costretto a far evolvere i modelli di scambio di documenti elettronici dai vecchi schemi EDIFACT, molto complessi, rigidi

e costosi, verso modelli più flessibili e maneggevoli, ma non per questo necessariamente più semplici da manutenere.

Oggetto di questo contributo sono quindi l'individuazione e la realizzazione degli strumenti a supporto della creazione di framework di scambio documenti elettronici basato su XML.

MODA-ML è un progetto finanziato dalla Commissione Europea nell'ambito del cluster di progetti su Middleware e Tecnologie ad Agenti denominato Eutist Ami (www.eutist-ami.org, Take-Up Actions del programma IST, Action Line IV.2.5 "Computing, communications and networks take-up measures") del V Programma Quadro della Unione Europea. Partner industriali del progetto sono i lanifici Successori Reda, Piacenza, Loro Piana, Vitale Barberis Canonico e l'industria di confezione Fratelli Corneliani; partner tecnologici sono Enea, Politecnico di Milano, Progema – Gruppo SOI e Domina srl.

2. ANALISI DEI FRAMEWORK PER IL COMMERCIO ELETTRONICO

E' noto e ormai largamente condiviso che la crescita del settore del commercio elettronico dipende in buona parte dallo sviluppo delle tecnologie dell'informazione e della comunicazione (*ICT*). Ciò evidentemente, sia pur considerando il solo punto di vista tecnico, è una condizione necessaria ma non sufficiente per garantire un efficace funzionamento ed una larga diffusione delle transazioni di commercio elettronico. Occorre infatti, come è accaduto per Internet, che i soggetti coinvolti in operazioni di "*e-commerce*" stabiliscano una piattaforma comune su cui basare i relativi processi commerciali ed i conseguenti scambi di informazioni (*messaggi*). In altre parole è necessaria un'attività di standardizzazione internazionale che permetta di giungere ad una visione comune del modo di scambiare dati fra imprese nella nuova "economia digitale" e garantire così elevati livelli d'interoperabilità.

Si presenta pertanto in questo paragrafo in modo sintetico lo stato di avanzamento delle maggiori iniziative sulle attività di standardizzazione in atto nel settore dell'"*E-Commerce*" che si basano su XML (eXtensible Markup Language), ormai riconosciuto come componente fondamentale di rappresentazione e di scambio di dati in qualunque contesto. L'importanza di tali iniziative risiede nell'utilità che esse possono rivestire per la crescita del settore del commercio elettronico. Conseguentemente, è spiegabile non solo l'interesse degli enti ufficiali di standardizzazione, ma anche di consorzi industriali e settoriali per la definizione di modelli ed architetture per l'*E-Commerce* e l'*E-business*, basate sull'uso di XML.

Pur nell'estrema dinamicità della situazione, non è facile assegnare un diverso peso, soprattutto in termini di capacità di generazione del consenso e di probabile affermazione, alle iniziative in corso che hanno dato luogo alla realizzazione di *framework*, ossia di vere e proprie architetture di riferimento in cui considerare il modello di processo di *e-business*, la generazione di documenti commerciali ed il relativo processo di scambio (comprese le modalità di trasporto in rete Internet). In questo senso, tra le varie iniziative, le più importanti per il lavoro già svolto e per le loro prospettive appaiono quelle di definizione dei modelli di cooperazione fra imprese basati su XML come **ebXML** (*electronic business XML* promossa da *UN-CEFACT* (*United Nations Centre for Trade Facilitation and Electronic Business*) e dal Consorzio *OASIS* (*Organization for the Advancement of Structured Information Standards*) che sta raccogliendo notevole consenso a livello internazionale), **BizTalk** (sponsorizzata da

Microsoft e di cui è già stata pubblicata la Versione 2 delle specifiche), **RosettaNet** (iniziativa del settore "*computer industry*" in USA, **EAN.UCC** (*European Article Numbering. Uniform Code Council*) Versione 1.0 nata dalla precedente iniziativa *EANCOM®* che definiva le linee guida dettagliate di messaggi standard secondo le specifiche *UN/EDIFACT* per lo scambio di documenti di commercio elettronico ed infine **UBL** (*Universal Business Language*) da poco avviata per volontà dello stesso Consorzio *OASIS* (prendendo come base la precedente *xCBL – XML Common Business Library*) al fine di far chiarezza tra le iniziative già in atto.

2.1 INQUADRAMENTO DELLE INIZIATIVE E PRINCIPALI CARATTERISTICHE

Da quanto detto appare subito evidente che il processo di standardizzazione del settore *e-commerce/e-business* è paradossalmente frammentato e vario. Per avere quindi una visione più chiara delle varie iniziative in corso, sembra opportuno far riferimento ad uno schema (Fig. 2.1) abbastanza intuitivo tratto dal **CWA** (*CEN/ISSS Workshop Agreement*, vedi [CENEC01]) del giugno 2001. Tale struttura di riferimento ha lo scopo di classificare, in relazione agli obiettivi ed alle attività di standardizzazione effettivamente svolte, i gruppi che propongono *framework*, architetture e modelli nell'ambito dell'*e-commerce*. Lo schema riportato in figura non rappresenta un'architettura di sistema di commercio elettronico in senso stretto, quanto una struttura a blocchi in cui è possibile inquadrare contenuti e specifiche tecniche di coloro che partecipano alla realizzazione di sistemi di commercio elettronico. I blocchi orizzontali rappresentano le "componenti" infrastrutturali (tecnologiche, di rete, ecc.) di cui necessita il commercio elettronico, mentre i blocchi verticali rappresentano concettualmente l'insieme delle procedure e dei processi che formano il collante dei "componenti" dell'intero "edificio" del commercio elettronico.

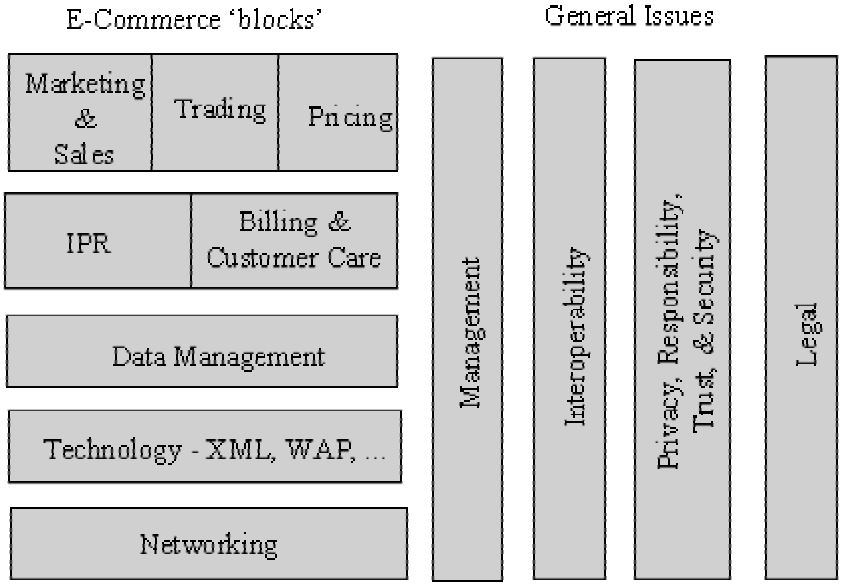


Figura 2.1: Struttura di riferimento per i framework di *eCommerce* tratta dal CWA del CEN/ISSS Electronic Commerce Workshop

Se quindi si considera come valida l'ipotesi di quanto proposto dal CEN/ISSS si può senza dubbio ritenere che **ebXML** sia il *framework* più completo finora proposto. Infatti la struttura (*framework*) ebXML deriva da una visione di commercio elettronico dove le imprese si incontrano in un mercato virtuale e svolgono le seguenti operazioni:

- ricerca elettronica (via rete) del partner con cui realizzare una transazione;
- definizione del processo di business attraverso lo scambio di messaggi XML;
  - accordo su una sequenza standard del processo di business;
  - realizzazione di messaggi XML per lo scambio di documenti di business;
  - definizione di una chiara semantica di business;
  - accordo per stabilire regole mutue o standard di protocollo di commercio tra partner;
  - uso di programmi applicativi a basso costo già pronti.

Tale visione si traduce operativamente nel lavoro di due gruppi distinti che si occupano di semantica e infrastruttura.

UN/CEFACT ha il compito di definire un "*Semantic Framework*" che consiste in un meta-modello del processo di business e nell'individuazione di un insieme di componenti che costituiscono il nucleo (*core component*) comune dei termini (cui viene attribuito un significato univoco ed accettato da tutti i partner) usati nel processo di business.

OASIS invece ha il compito di definire una "i*nfrastruttura*" che consenta il trasporto, l'indirizzamento e la "confezione" (*packaging*) dei messaggi, un'interfaccia che agevoli l'attività di business, un profilo/accordo di protocollo di collaborazione e una rete di depositi di informazioni (*repository*) condivisi in cui collocare o trovare dati sui profili delle imprese, modelli di processo di business e relative strutture di messaggi.

Il *framework ebXML* quindi tenta di concretizzare la visione di commercio elettronico citata sopra attraverso una serie di strumenti e specifiche tecniche standard (sistematizzati in una serie di documenti pubblici) perché le imprese possano interoperare in modo quanto più automatico possibile attraverso lo scambio di documenti in formato elettronico.

Tali specifiche tecniche definiscono i seguenti macro-componenti del framework: Core Component, Registry and Repository, Collaborative Protocol Profiles (CPPs), Collaboration Protocol Agreements (CPAs) e Message Service. Questi componenti, le relazioni esistenti tra di essi e le fasi attuative (progetto e attività a regime) in cui esse sono utilizzate sono schematizzate nella Fig. 2.2.

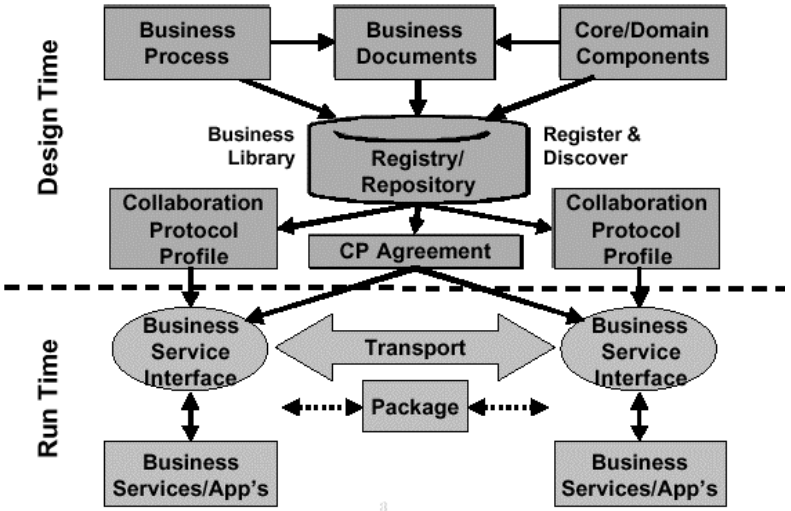


Figura 2.2: Schema a blocchi del framework ebXML

Tuttavia considerando la scarsità di effettive implementazioni di ebXML ad oggi, non si può dire che l'iniziativa abbia ancora assunto un carattere definitivo.

Per quanto riguarda l'iniziativa europea *EAN.UCC*, questa ha soprattutto il merito di essere nata dal patrimonio di conoscenze accumulato con le precedenti esperienze di *EANCOM* su *EDI* (*Electronic Data Interchange*). Il modello di processo e quello logico sono stati sviluppati usando il linguaggio object-oriented *UML* (*Unified Modelling Language*). Il modello di processo identifica e definisce in modo univoco gli elementi e le funzioni necessarie alle transazioni commerciali, mentre il modello logico li elabora e li caratterizza attraverso i dati che li descrivono. In tali modelli si inquadrano quindi un processo comune di business tra partner commerciali e gli standard e le soluzioni tecniche sviluppate (*XML Schema* e il *Global Data Dictionary*).

L'architettura EAN.UCC è composta da quattro parti fondamentali:

- *Building Blocks*: sono "oggetti" comuni e riusabili obbligatori ed opzionali che costituiscono un comun denominatore per costruire il modello del processo di business (es. "*date*" e "*name*")
- *Core business models*: comprendono i componenti comuni di una funzione di business che possono essere usati in più processi. Vanno usati insieme alle "*extension*" per completare processi di business specifici di contesti particolari e non possono essere modificati. Tali componenti sono descritti singolarmente secondo uno standard di messaggio di business (*Business Message Standard for ...*) e definiscono gli elementi comuni (*Complex Core Components*) usati nel processo di business.
- *Extensions*: contengono gli elementi specifici richiesti per completare un processo di business; ad esempio per concordare tra le parti i termini della transazione (allineamento dei dati tra le parti o "*data alignment*") se questi non sono stati definiti a priori in modo cosiddetto statico. Una o più *extension* possono essere applicate ad un *core business model* o alla stessa funzione di business in differenti processi.
- *Interfaces*: definisce il punto in cui una *extension* viene applicata all'interno del modello della struttura del messaggio.

A conclusione di questa breve e necessariamente sintetica analisi di alcuni tra i più significativi *framework* operanti nel settore *e-commerce* si possono trarre comunque alcune conclusioni di carattere generale:

- il ruolo centrale che XML e i Framework di standardizzazione rivestono per le attività e-commerce;
- l'estrema dinamicità della situazione (soprattutto in ambito PMI in cui non è possibile tracciare a priori linee guida definite gerarchicamente/verticalmente) rende difficile stabilire piattaforme comuni in particolar modo per ciò che riguarda gli aspetti semantici soprattutto in ambiente multilinguistico dello scambio di informazioni e le attività di processo di business;
- l'emergere della tendenza ad un progresso dei *framework* verso una piattaforma comune o comunque interoperabile, nonostante la frammentazione di iniziative dettata dalla urgente necessità di operare con e attraverso le nuove tecnologie ICT.

3. IL PROTOTIPO MODA-ML: UNO STRUMENTO PER LA TRASMISSIONE DI DOCUMENTI COMMERCIALI

L'obiettivo principale del software di trasmissione dati di MODA-ML consiste nella predisposizione di un *sistema prototipale di interscambio di documenti*, secondo lo standard promosso dal progetto. Il cuore del sistema è composto dal *modulo MSH* (Message Service Handler), che è in grado di inviare *documenti MODA-ML*[1] da un mittente ad un destinatario, utilizzando la rete Internet. L'MSH si poggia su un *protocollo di trasporto*,[2] compatibile con ebXML (vedi [ebTA01]), che prevede la posta elettronica come canale di interscambio.

In pratica l'MSH costituisce un front-end per la trasmissione documenti XML da aggiungere ai sistemi aziendali che così non debbono misurarsi con le problematiche del trasporto e possono concentrarsi sulla produzione e sul consumo dei dati ricevuti o trasmessi.

Perché un documento MODA-ML possa essere dato all'MSH per la spedizione, deve essere inserito in una *busta di posta elettronica* (busta SMTP) (vedi [ebMS01]). Affinché il documento MODA-ML possa essere processato in modo efficace da sistemi informatici fortemente eterogenei, quali i sistemi gestionali aziendali presenti nella filiera Tessile/Abbigliamento, il suo contenuto viene strutturato secondo lo *standard SOAP* (Simple Object Access Protocol) (vedi [SOAP00], [SOAPATTACH00]), che permette di codificare in XML (vedi [XML00]) varie informazioni funzionali all'interscambio (*busta SOAP*), quali l'identificativo di rete del mittente, l'identificativo di rete del destinatario, il time-to-live dei dati, la qualità del servizio di interscambio, il livello di sicurezza, ecc., e di mantenerle distinte dal reale contenuto di business del messaggio (*payload*). Ne risulta un messaggio di posta elettronica strutturato logicamente in due parti: busta SOAP e payload. Le due parti vengono gestite come allegati distinti, codificati secondo il *protocollo MIME* (Multipurpose Internet Mail Extensions) (vedi [MIME96], [MIME98]). Tale soluzione è efficiente e flessibile e permette di trasportare più documenti MODA-ML in una singola busta di trasmissione dati. Permette cioè che la busta MIME contenga due o più allegati: il primo per la busta SOAP del documento MODA-ML; il secondo, e gli eventuali successivi, per i documenti MODA-ML (payloads) trasportati.

[1] Un documento MODA-ML è una istanza, codificata in XML, di uno dei tipi di documenti definiti dal progetto e descritti da specifiche guide implementative.

[2] Si parla di protocollo di trasporto per indicare che il messaggio di business (payload) è veicolato, in ultima analisi, dal protocollo SOAP di MODA-ML. Nella corretta accezione del termine, tale protocollo, riferendosi al modello TCP/IP, si pone sopra al livello di applicazione, imbustato nel pacchetto SMTP.

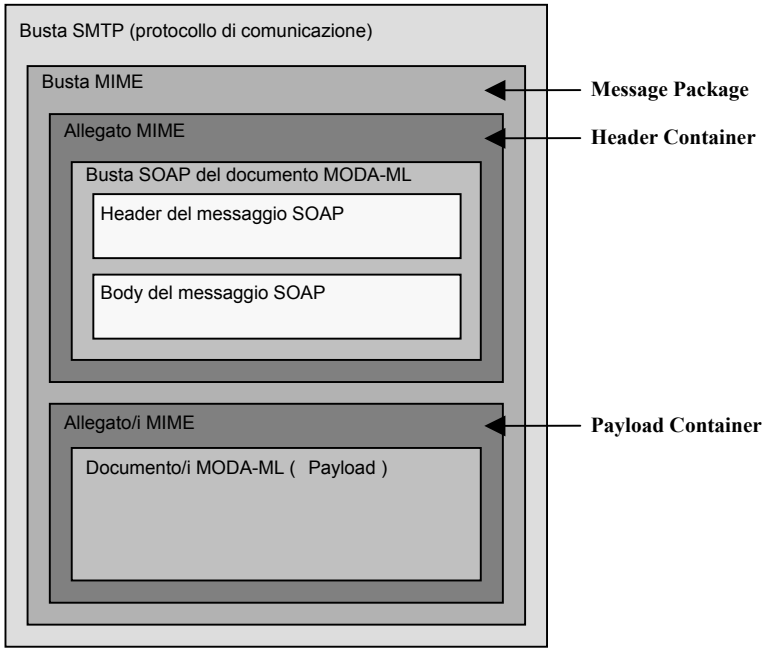


Figura 3.1: Struttura del messaggio MODA-ML

Uno o più documenti MODA-ML, inseriti in una busta SMTP e codificati secondo la struttura SOAP definita dal protocollo di trasporto di MODA-ML, prendono il nome di *messaggio MODA-ML* (Figura 3.1).

In particolare, ogni messaggio MODA-ML è contenuto all'interno della busta MIME (nota anche come *Message Package*) di un messaggio di posta elettronica, ed è costituito da parti distinte:

- Un primo allegato MIME, l'*Header Container* che contiene un messaggio conforme alle specifiche SOAP 1.1 (busta SOAP).
- Zero o più allegati MIME, che prendono il nome di *Payload Containers*, che trasportano le informazioni propriamente applicative.

A sua volta la busta SOAP è suddivisa in due parti :

- Un elemento *SOAP Header*, che contiene le informazioni relative all'intero messaggio riguardanti la sua identificazione, il routing, la segnalazione di eventuali errori e l'acknowledgment.
- Un elemento *SOAP Body*, che contiene informazioni relative ad ogni specifico payload, come, per esempio, lo schema di validazione.

Un messaggio MODA-ML è una sequenza di caratteri ASCII, la cui parte principale è XML (Figura 3.2).

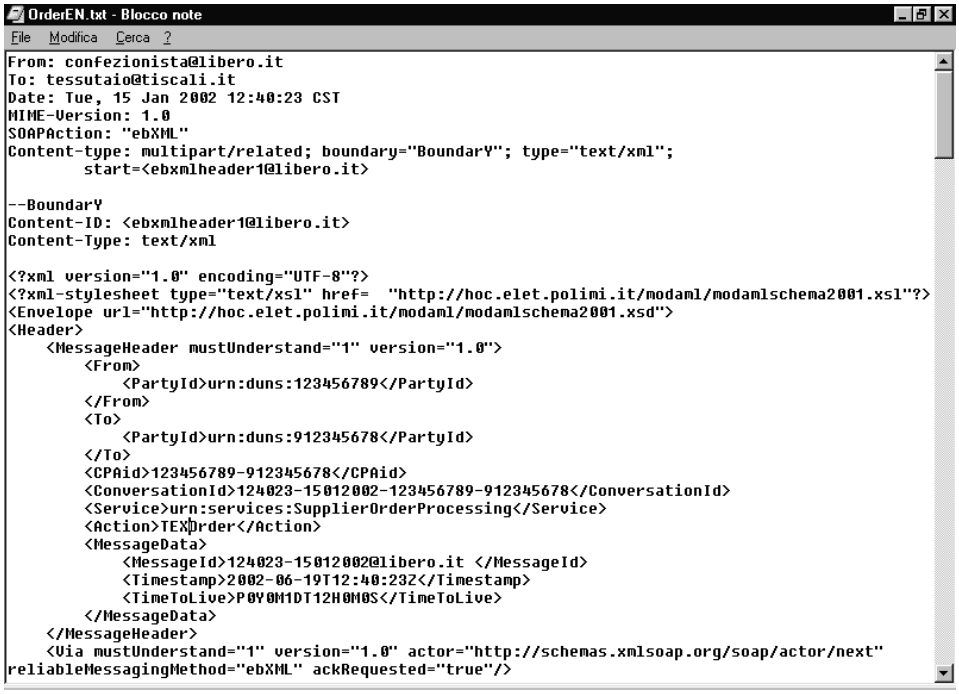


Figura 3.2: Esempio di messaggio MODA-ML

L'MSH è in grado di inviare e ricevere messaggi MODA-ML sfruttando un server SMTP (invio) ed un server POP (ricezione) standard e MIME-compliant[3]. L'MSH controlla la correttezza sintattica del messaggio prima della spedizione (e dopo la ricezione), mantiene traccia di tutte le operazioni di interscambio e dei relativi contenuti, è in grado di segnalare errori di interscambio e/o errori di codifica dei dati, è in grado di integrare standard di sicurezza a vari livelli (acknowledgment di ricezione, crittografia, firma digitale, autenticazione).

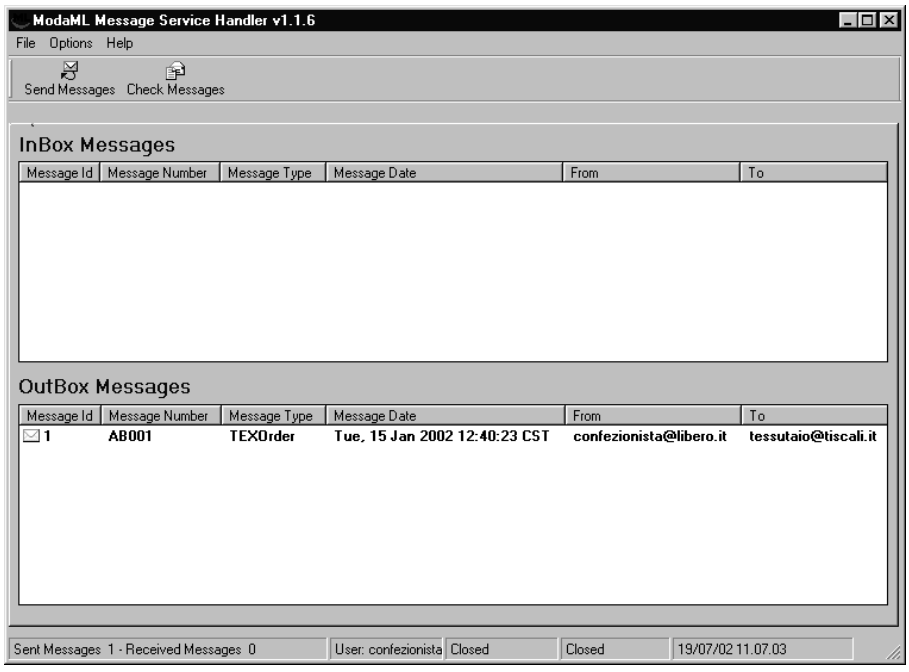


Figura 3.3: L'interfaccia utente dell'MSH di MODA-ML

[3] Nella versione attuale, l'MSH è in grado di gestire esclusivamente messaggi con payload singolo.

Le aziende più "strutturate" della filiera Tessile/Abbigliamento hanno già in forma elettronica, nei propri sistemi informatici, la maggior parte dei dati che potrebbero essere interessate ad interscambiare secondo lo standard MODA-ML. Le aziende trovano quindi più semplice poter integrare i propri sistemi informativi con l'MSH (Figura 3.4) anziché fare sviluppi ad hoc. L'attività di integrazione è facilitata da MODA-ML poiché l'interfaccia di ingresso e uscita delle informazioni (cioè, il messaggio MODA-ML) è pubblica e documentata (dizionario MODA-ML, guide implementative dei documenti MODA-ML, protocollo di trasporto MODA-ML) e poiché tecnicamente coincide con la struttura informatica più semplice e portabile: il file ASCII. Inoltre, è stato progettato da parte di una delle aziende partner del progetto, ed è in fase di implementazione, uno strumento di mapping ed interfacciamento dei documenti MODA-ML con fonti dati generiche (per struttura e tecnologia), al fine di semplificare il più possibile l'estrazione e l'inserimento dei dati trasportati dai messaggi MODA-ML nei sistemi informativi delle aziende della filiera.

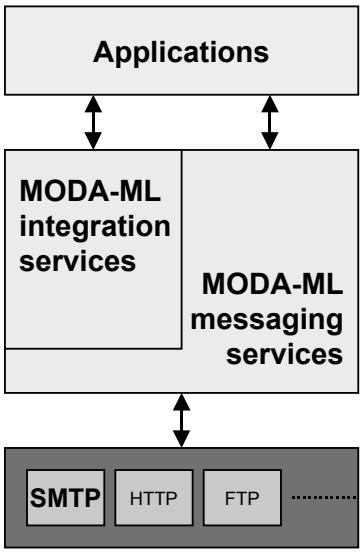


Figura 3.4: Architettura di integrazione del software di MODA-ML

Perché un'azienda possa interscambiare operativamente documenti MODA-ML, è sufficiente che installi l'MSH, che abbia un server SMTP e un server POP di transito (offerti anche dai comuni Internet Provider), che estragga i dati in forma XML dai propri sistemi informativi, che "imbusti" tali dati in messaggi MODA-ML e li renda disponibili sotto forma di file in una cartella predefinita dell'MSH. Per la ricezione di documenti MODA-ML, vale il processo inverso.

A fini dimostrativi, per poter provare il protocollo trasporto MODA-ML e l'MSH, è stato sviluppato un secondo modulo software detto *MCM* (Message Content Manager). Tale modulo ha il compito di predisporre delle interfacce utente di prova per la creazione, la modifica e la cancellazione di documenti MODA-ML limitatamente al ciclo dell'ordine[4] e per l'esportazione dei documenti MODA-ML sotto forma di messaggi XML, pronti per la spedizione con l'MSH. L'MCM simula quindi un piccolo sistema gestionale aziendale per MODA-ML e mantiene in un archivio relazionale i dati dei documenti.

[4] Documenti di ordine a tessutaio, risposta ordine, modifica ordine, avanzamento ordine.

4. SICUREZZA E MODA-ML: COME PROTEGGERE LE INFORMAZIONI SENSIBILI CONTENUTE NEI MESSAGGI

4.1 GLI OBIETTIVI DI SICUREZZA

Lo strumento scelto per effettuare la trasmissione dei dati per il progetto MODA-ML è la posta elettronica che, da una parte, è una tecnologia economica e ampiamente diffusa, ma, dall'altra, non offre le garanzie di sicurezza richieste dagli utenti finali più evoluti del prototipo. Per ovviare a questo problema, si è dedicata una specifica attività del progetto all'individuazione di specifiche per la sicurezza ed alla definizione di un modulo software in grado di realizzarle e di integrarle al meglio con l'MSH del prototipo. In particolare, questo modulo software fornisce gli strumenti per ottenere **riservatezza** (impedendo l'accesso al contenuto dei messaggi da parte di chiunque non ne sia autorizzato), **integrità** (assicurando al ricevente la possibilità di rilevare eventuali alterazioni del contenuto dei messaggi) ed **autenticazione** (garantendo al destinatario l'identità del mittente). Il **non-ripudio**, ovvero la non ripudiabilità della manifestazione di volontà espressa dal mittente con l'invio di un messaggio, viene realizzato dall'MSH mediante dei messaggi di acknowledgement. La possibilità di autenticare i messaggi, permessa dal modulo riguardante la sicurezza, consente di rafforzare questa caratteristica del prototipo e di ottenere il **non-ripudio autenticato**.

4.2 ANALISI DEI REQUISITI

Le informazioni scambiate dalle aziende destinatarie del prototipo devono essere protette utilizzando strumenti considerati validi anche da un punto di vista giuridico. A questo scopo sono state prese in esame le leggi italiane ed europee in materia di firma digitale: a partire dal 1999, infatti, la Comunità Europea considera le firme digitali ammissibili come prove nei procedimenti legali (vedi [CE99]), a patto di soddisfare alcuni requisiti di tipo tecnico (algoritmi utilizzabili per la creazione della firma di un documento, lunghezze minime per le chiavi usate per le firme, tipi di certificati) (vedi [ECAlg01]). L'Italia ha anticipato tale direttiva europea, definendo delle proprie regole tecniche per la creazione di firme digitali (vedi [DPR513] e [DCM0299]), più rigide di quelle europee e che obbligano ad utilizzare chiavi di lunghezza superiore: questo significa maggiore sicurezza, ma anche maggiori costi. Per adeguarsi alla direttiva [CE99], è stato approvato un decreto legislativo (vedi [DL0102]) che riconosce valore legale anche alle firme elettroniche eseguite secondo le indicazioni di [ECAlg01]. A livello di progetto, si sono scelti algoritmi e lunghezze delle chiavi tali da soddisfare entrambe le legislazioni, in modo da coniugare un buon livello di sicurezza all'ampia accettabilità derivante dall'aderenza alle indicazioni comunitarie.

Un altro requisito soddisfatto dal modulo riguardante la sicurezza è la sua elasticità di utilizzo, che permette di delineare alcuni casi d'uso applicabili ad utilizzatori finali caratterizzati da diverse dimensioni e cultura informatica:

- aziende prive del software MODA-ML e non interessate alla protezione dei messaggi inviati e ricevuti.
- aziende prive del software MODA-ML, ma dotate di un proprio certificato;
- aziende che intendono utilizzare il software MODA-ML e un certificato emesso da una Certification Authority riconosciuta dall'AIPA;

Le diverse tecnologie usate per rendere sicuro lo scambio dei dati sono state scelte fra quelle indicate dalle specifiche del Message Service di ebXML (vedi [ebMS01]), in modo che i messaggi spediti da un MSH MODA-ML rispettino sempre il formato previsto da questo framework, anche quando sono firmati o crittografati.

4.3 DEFINIZIONE DEI LIVELLI DI SICUREZZA APPLICABILI ALLO SCAMBIO DEI MESSAGGI MODA-ML

Per permettere la piena interoperabilità tra tutti gli utenti del progetto, sono stati definiti tre macrolivelli di sicurezza:

1. **Nessuna sicurezza**: questo livello è utilizzato per inviare messaggi a coloro che usano client di posta di elettronica che non supportano S/MIME oppure MSH MODA-ML realizzati ad hoc da parte di software house esterne al progetto che hanno preferito non sviluppare la parte riguardante la sicurezza.
2. **Base**: con questo livello è possibile proteggere i dati firmandoli e crittografandoli, ma usando chiavi relativamente brevi e algoritmi 'leggeri', in grado quindi di essere gestiti anche dai client di posta elettronica più evoluti.
3. **Avanzato**: questo livello viene usato per scambiare documenti tra aziende dotate di un MSH MODA-ML completo e, quindi, in grado di criptare e firmare i messaggi usando chiavi più lunghe e algoritmi più sicuri di quelli supportati dai client di posta elettronica. Questo livello è l'unico dei tre a soddisfare le indicazioni fornite da ebXML in fatto di algoritmi e lunghezza delle chiavi consigliate.

Le tabelle seguenti indicano quali algoritmi vengono usati per i macrolivelli Base e Avanzato e la lunghezza delle rispettive chiavi. La scelta è stata fatta tenendo conto della loro affidabilità e diffusione, oltre che delle indicazioni delle direttive nazionali e comunitarie in materia di firma elettronica.

1. Base

	Algoritmo	**Lunghezza della chiave**
Firma digitale	RSA	Almeno 512 bit
Crittografia	RC2	40 bit

2. Avanzato

	Algoritmo	**Lunghezza della chiave**
Firma digitale	RSA	Almeno 1024 bit
Crittografia	3DES	168 bit

Tabelle 4.1 e 4.2: Algoritmi e lunghezza delle chiavi consigliati per i macrolivelli di sicurezza di MODA-ML

All'interno dei macrolivelli 'Base' ed 'Avanzato è possibile individuare cinque livelli, ciascuno corrispondente all'uso (esclusivo o combinato) della firma digitale, della crittografia e del non-ripudio autenticato. Vengono così definiti 16 livelli di sicurezza, ognuno dei quali soddisfa un diverso profilo fra quelli previsti da ebXML (vedi [ebMS01]).

4.4 TECNOLOGIE DI SICUREZZA APPLICABILI A MODA-ML

I metodi per garantire riservatezza, autenticazione, integrità e non-ripudio dei messaggi conformi a MODA-ML si basano su S/MIME (vedi [SMIME99]) e sulla coppia XML Signature (vedi [XMLDS01]) e XML Encyption (vedi [XMLENC02]). S/MIME opera sulla struttura del messaggio di posta elettronica, ossia sul numero dei suoi allegati e sul tipo dei dati che essi contengono (testo XML in chiaro, crittografato oppure firmato). Ad esempio, un messaggio MODA-ML firmato con S/MIME risulta composto dal messaggio MODA-ML originale e dall'allegato che ne racchiude la firma:

Figura 4.1: Struttura del messaggio firmato con S/MIME

La Figura 4.1 mostra come l'operazione di firma con S/MIME di un messaggio comporti semplicemente l'aggiunta di un allegato al messaggio originale, il cui contenuto XML non viene modificato in alcun modo.

XML Signature e XML Encryption, viceversa, lasciano invariata la struttura del messaggio e agiscono sulla struttura delle due parti da cui è composto. Essi modificano la busta ebXML e/o il documento MODA-ML dall'interno, aggiungendo (nel caso della firma) o sostituendo (nel caso della crittografia) alcuni elementi XML in essi contenuti. Per esempio, l'effetto dell'operazione di firma eseguita utilizzando XML Signature comporta l'inserzione nella busta ebXML di un elemento XML (l'elemento *Signature*) che racchiude tutte le informazioni necessarie al destinatario per verificarne l'autenticazione e l'integrità.

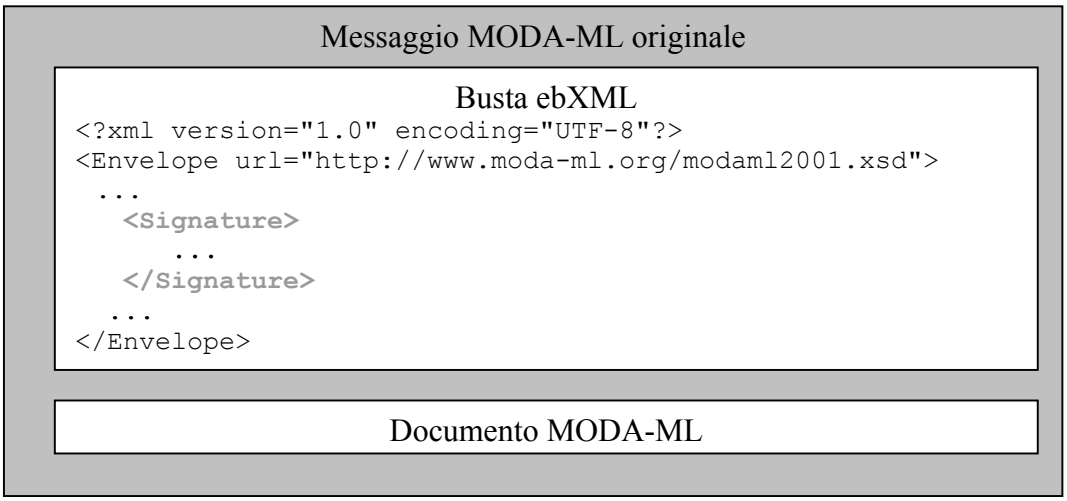


Figura 4.2: Struttura del messaggio firmato con XML Signature

4.5 VANTAGGI APPORTATI DALL'UTILIZZO DI XML SIGNATURE E XML ENCRYPTION

S/MIME è uno standard per la protezione dei messaggi di posta elettronica e, dunque, è adatto anche ai messaggi generati dal prototipo MODA-ML e ne garantisce l'interoperabilità con i client di posta elettronica usati più comunemente. Tuttavia, l'uso di XML Signature ed XML Encryption rappresenta la soluzione ottimale perché porta diversi vantaggi:

- Una maggiore elasticità di utilizzo, permettendo di proteggere solo alcuni elementi e non soltanto l'intero documento. Questo si traduce nella possibilità di modificare la politica di sicurezza senza stravolgere il lavoro di implementazione svolto nel frattempo. Utilizzando S/MIME, invece, non si ha la stessa granularità: o si firma/crittografa l'intero documento oppure non lo si protegge per nulla.
- L'indipendenza rispetto alla modalità di trasmissione dei documenti: un documento firmato con XML Signature e criptato con XML Encryption può essere spedito per posta elettronica o scaricato via HTTP o FTP, mentre S/MIME è utilizzabile soltanto con SMTP. Anche in questo caso la scelta degli standard basati su XML permette di adattare velocemente il lavoro già fatto ad eventuali scelte future di cambiamento dell'architettura del progetto. S/MIME, invece, è fortemente orientato verso la posta elettronica ed un simile mutamento costringerebbe a riscrivere interamente le funzioni che firmano e cifrano i dati in modo da supportare uno standard più adatto al protocollo utilizzato.
- La piena compatibilità con ebXML per quanto riguarda la firma digitale e quindi la maggiore interoperabilità possibile con i messaggi prodotti da altre applicazioni che ne soddisfano le specifiche.

5. AMBIENTE DI SUPPORTO ALLA REALIZZAZIONE DEL FRAMEWORK MODA-ML

5.1 DIZIONARIO MODA-ML

La necessità di disporre di un repository dinamico, di un pratico supporto multilingue e di una struttura relazionale dei dati ha consigliato di implementare il dizionario MODA-ML utilizzando una base dati.

Per favorire la riusabilità prima e per affinare la generazione degli XML Schema poi, si è scelto di categorizzare le informazioni sul modello Entity-Relationship. Ciò significa che non si è usato un elenco strutturato di tag XML, ma si sono definiti tipi che verranno successivamente istanziati in tag XML. Viene, in questo modo, supportato il meccanismo dell'ereditarietà ed è quindi possibile descrivere nuovi tipi MODA-ML (e di conseguenza nuovi tag e nuovi attributi) specificando solo le differenze che li distinguono da altri già definiti.

5.2 ANALISI DEI REQUISITI

I requisiti funzionali del dizionario che hanno condizionato maggiormente la scelta della piattaforma di sviluppo sono stati di carattere operazionale: le modalità di inserimento, aggiornamento e cancellazione dei dati dovevano essere le più semplici e flessibili possibile.

Per le sua caratteristiche è stato scelto Microsoft Access come base dati idonea a contenere il dizionario: il prezzo accessibile, la capillare diffusione, la semplicità di utilizzo e la possibilità di creare una gestione integrata di relazioni, maschere e report tramite una facile programmabilità, sono le caratteristiche che hanno evidenziato questo prodotto rispetto ad altri.

5.3 ARCHITETTURA DEL DIZIONARIO

Il contenuto del dizionario definisce i macroprocessi del segmento di filiera in esame, le attività che compongono questi processi e i messaggi che vengono scambiati dagli anelli del segmento. La struttura adottata è di tipo gerarchico e permette che ad ogni messaggio venga abbinato un documento XML tramite un puntatore ad un "tipo complesso" che ha il ruolo di radice del documento.

A partire da questo tipo complesso, la struttura ad albero del documento XML è definita da una serie di puntatori ad elementi figli. Di ogni elemento (o attributo) il dizionario contiene il tipo e l'istanza: il tipo ne caratterizza gli aspetti generali quali ad esempio la lunghezza massima per una stringa o il numero di cifre decimali per un decimal, l'istanza invece rappresenta il vero oggetto XML.

Il dizionario descrive inoltre le relazioni gerarchiche fra gli oggetti per mezzo di parametri corrispondenti a quelli di XML Schema (vedi [XMLSC01]) con la possibilità di aggiungere note di aggregazione specifiche per ogni relazione.

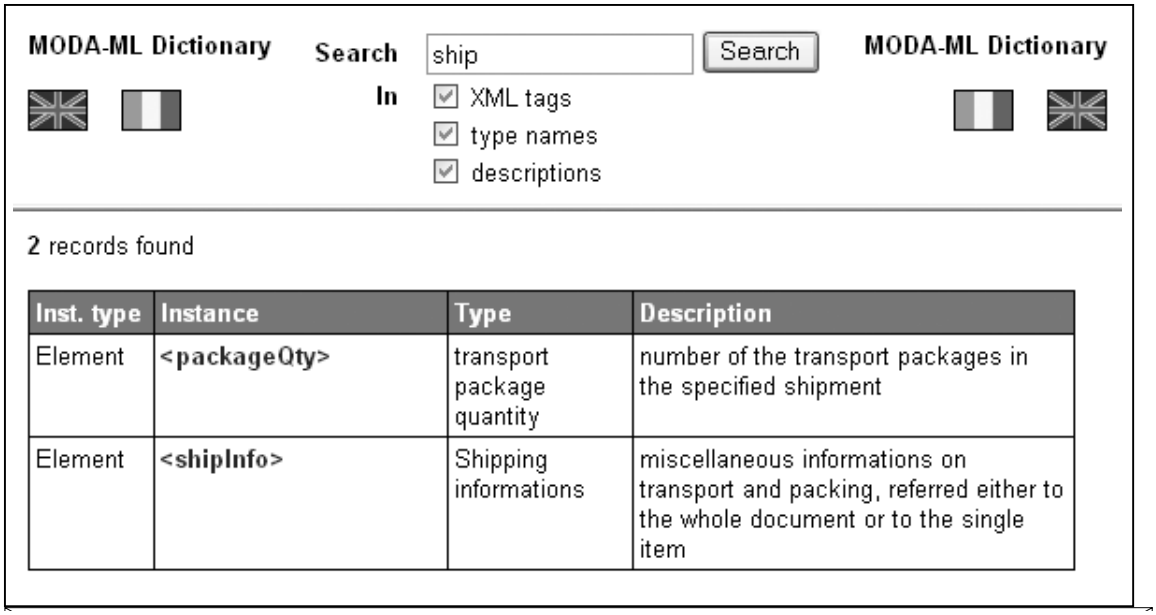
5.4 FUNZIONALITÀ IMPLEMENTATE

Nel dizionario è presente la reportistica completa su tipi, istanze e relazioni, ma gli strumenti più significativi sono stati sviluppati per darne la massima visibilità tramite il web. Sono state realizzate tre applicazioni, su web server IIS, che accedendo alla base dati descritta producono tre diversi servizi: "Guide implementative", "Generatore di XML-Schema" e "Motore di ricerca".

Le "Guide implementative" descrivono, per ogni documento XML ed in entrambe le lingue attualmente supportate (italiano ed inglese), la collocazione all'interno del segmento di filiera, lo scopo a cui è destinato, e mostrano la struttura gerarchica del documento, esponendo i dettagli di ogni elemento utilizzato.

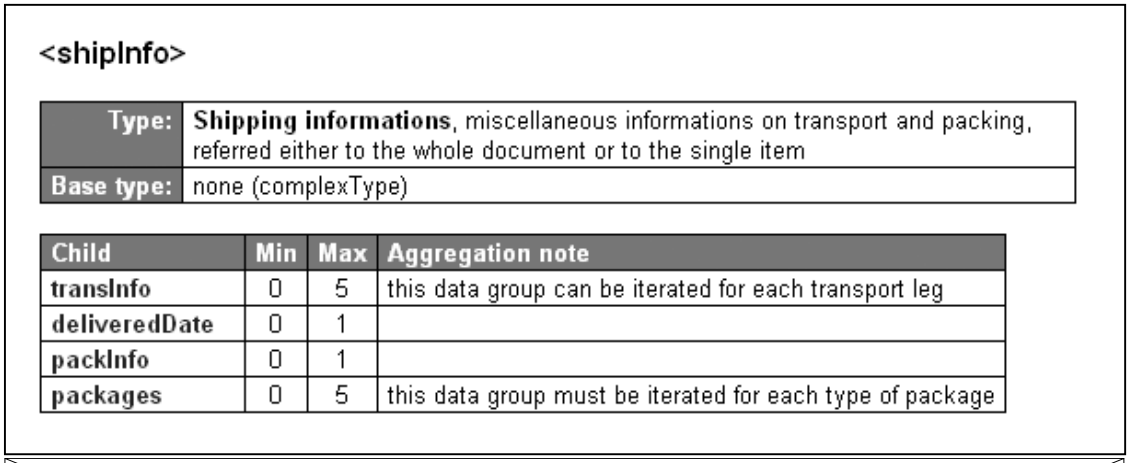
Il "Generatore di XML-Schema" fa uso intensivo delle relazioni definite nel dizionario MODA-ML e genera gli schemi validanti dei documenti XML secondo il metodo di design denominato "Venetian Blind" (vedi [VENBL02]) che ben si adatta alla tipizzazione dei dati assunta nel dizionario.

Il "Motore di ricerca" recupera gli oggetti definiti nel dizionario secondo determinate chiavi di ricerca (fig. 5.1). Selezionando uno degli elementi trovati vengono mostrati i suoi dettagli implementativi tra cui eventuali figli e attributi (fig. 5.2).



Inst. type	Instance	Type	Description
Element	<packageQty>	transport package quantity	number of the transport packages in the specified shipment
Element	<shipInfo>	Shipping informations	miscellaneous informations on transport and packing, referred either to the whole document or to the single item

Figura 5.1: Risultato di una ricerca



Child	Min	Max	Aggregation note
transInfo	0	5	this data group can be iterated for each transport leg
deliveredDate	0	1	
packInfo	0	1	
packages	0	5	this data group must be iterated for each type of package

Figura 5.2: Dettagli di un elemento

6. CONCLUSIONI

MODA-ML si basa su una descrizione completa e moderna dei business process più comuni della supply chain del settore Tessile/Abbigliamento, derivata da un'attenta analisi di ciò che è stato realizzato in materia di EDI e dei più promettenti framework per il commercio elettronico.

La scelta di utilizzare XML e le tecnologie ad esso correlate permette di abbassare la soglia tecnologica richiesta alle PMI e rende più semplice l'interoperabilità con i sistemi informativi aziendali più complessi. Questa semplicità nell'operare su documenti XML si traduce, inoltre, nella possibilità di creare strumenti efficaci e sicuri sia per gli utilizzatori finali (Message Service Handler, Message Content Manager, Integration Services, supporto a crittografia e firme digitali) che per il team di sviluppo del progetto (dizionario, generatore di XML Schema e guide implementative).

Il risultato è, dunque, la definizione e la realizzazione di una piattaforma comune per la comunicazione di informazioni gestionali e di servizio, che permetterà alle

aziende della filiera di interoperare senza modificare in modo sensibile i propri sistemi informativi.

7. RIFERIMENTI

[CE99] "Direttiva 1999/93/CE del Parlamento Europeo e del Consiglio, del 13/12/1999", in: *Gazzetta ufficiale n. L 013 del 19/01/2000*, 2000, http://europa.eu.int/eur-lex/it/archive/2000/l_01320000119it.html

[CENEC01] CEN/ISSS Electronic Commerce Workshop, "CWA 14228 - Summaries of some Frameworks, Architectures and Models for Electronic Commerce", 2001, http://www.cenorm.be/isss/cwa_download_area/cwa14228.pdf

[DCM0299] "Decreto del Consiglio dei Ministri 8 Febbraio 1999", in: *Gazzetta Ufficiale n.87 del 15/04/1999*, 1999, http://www.aipa.it/servizi[3/normativa[4/ leggi[1/regfin.asp

[DL0102] "Decreto Legislativo 23 Gennaio 2002, n.10", in: *Gazzetta Ufficiale n.39 del 15/02/2002*, 2002, http://www.gazzettaufficiale.it/index.jsp

[DPR513] "Decreto del Presidente della Repubblica 10 novembre 1997, n.513", in: *Gazzetta Ufficiale n.60 del 13/03/1998*, 1998, http://www.aipa.it/servizi[3/normativa[4/ leggi[1/dpr513_97.asp

[ebMS01] ebXML Transport, Routing and Packaging Team, "ebXML Message Service specification v1.0", 2001, http://www.ebxml.org/specs/ebMS.pdf

[ebTA01] Technical Architecture Team, "ebXML Technical Architecture Specification v1.04", 2001, http://www.ebxml.org/specs/ebTA.doc

[ECAlg01] Gruppo ALGO dell'EESSI-SG, "Algorithms and Parameters for Secure Electronic Signatures", 2001, http://www.ict.etsi.org/EESSI/Documents/20011019_Algorithm_Proposal_V2.11.doc

[MIME96] Freed, N., Borenstein, N., "RFC 2045 - Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", 1996, http://www.ietf.org/rfc/rfc2045.txt

[MIME98] E. Levinson, "RFC 2387 -The MIME Multipart/Related Content-type", 1998, http://www.ietf.org/rfc/rfc2387.txt

[SOAP00] Box, D., Ehnebuske, D., Kakivaya, G., Layman, A., Frystyk Nielsen, H., Thatte, S., Mendelsohn, N., Winer, D., "W3C Note Simple Object Access Protocol (SOAP) v1.1", 2000, http://www.w3.org/TR/SOAP

[SOAPAtt00] Barton, J. J., Frystyk Nielsen, H., Thatte, S., "W3C Note SOAP Messages with Attachments", 2000, http://www.w3.org/ TR/SOAP-attachments

[SMIME99] Ramsdell, B., "RFC2311 - S/MIME Version 3 Message Specification", 1999, http://www.ietf.org/rfc/rfc2633.txt

[VENBL02] Mitre Corp., "XML Schemas: Best Practice - Homepage", 2002, http://www.xfront.com/GlobalVersusLocal.html#ThirdDesign

[XML00] Bray, T., Paoli, J., Sperberg-McQueen, C. M., Maler, E., "W3C Recommendation: Extensible Markup Language (XML) 1.0 (Second Edition)", 2000, http://www.w3.org/TR/2000/REC-xml-20001006

[XMLDS01] Eastlake, D., Reagle, J., Solo, D., "W3C Proposed Recommendation XML-Signature Syntax and Processing", 2001, http://www.w3.org/TR/2001/PR-xmldsig-core-20010820/

[XMLENC02] Eastlake, D., Reagle, J., "W3C Candidate Recommendation XML Encryption Syntax and Processing", 2002, http://www.w3.org/TR/2002/CR-xmlenc-core-20020304/

[XMLSC01] Thompson, H. S., Beech, D., Maloney, M., Mendelsohn, N., "W3C Recommendation XML Schema Part 1: Structures", 2001, http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/