

REGIONE TOSCANA



Giunta Regionale

Direzione Generale Organizzazione e Sistema Informativo
Area di Coordinamento Ingegneria dei Sistemi Informativi e della
Comunicazione

Settore ITSAE

Ambienti di sviluppo e produzione
Standard tecnologici

ottobre 2008

Versione 2.8



DOCUMENTO: Documento illustrativo – Ambienti di sviluppo e produzione- Standard Tecnologici			
EMISSIONE - VERIFICA - APPROVAZIONE			
	Funzione	Nome	firma
Emissione	Specialista Tecnico	Luca Bonuccelli	
Verifica	Specialista Tecnico	Walter Volpi	
Verifica	Specialista Tecnico	Vincenzo Martiello	
Verifica	Specialista Tecnico	Andrea Panichi	
Verifica	Specialista Tecnico	Alessandro Tarchi	
Approvazione	Responsabile	Laura Castellani	
LISTA DI DISTRIBUZIONE			
AGGIORNAMENTI			
Versione	Data	Paragrafi Modificati	Motivo Modifica
1.0	23.09.2002		Prima stesura
1.1	15.03.2004		Revisione
2.0	25.01.2005		Revisione completa
2.1	18.02.2005		Emissione
2.2	10.03.2005		Correzioni
2.3	18.08.2005		Emissione
2.4	23.11.2005		Aggiunta
2.5	09/02/2006	2, 3.1, 10	Aggiunta
2.6	30/10/2006	4, 4.1, 5, 5.3, 5.4, 6,11	Aggiunta, Modifica
2.7	03/03/2008	tutti	Aggiunta, Modifica
2.8	10/10/2008	3.1, 3.2 5,2	Aggiunta, Modifica

**SOMMARIO**

1 - PREMESSA.....	4
2 - ANALISI E PRODUZIONE DOCUMENTAZIONE.....	4
3 - PIATTAFORMA INFRASTRUTTURALE HARDWARE E NETWORKING.....	4
3.1 - ARCHITETTURA INFRASTRUTTURA MULTI-TIER REGIONALE.....	5
3.2 - AMBIENTE DI NETWORKING E REGOLE DI SICUREZZA PERIMETRALE.....	5
4 - DATABASE	6
4.1 - ACCESSO AL DATABASE.....	6
5 - SVILUPPO APPLICAZIONI.....	6
5.1 - APPLICAZIONI CON INTERFACCIA UTENTE.....	7
5.2 - WEB SERVICES.....	7
5.3 - INDICAZIONI SUL FORMATO DEGLI ARCHIVI.....	7
5.4 - SVILUPPO APPLICAZIONI SICURE.....	7
6 - DATA WAREHOUSE	8
7 - SISTEMI DI SUPPORTO ALLE DECISIONI (DSS).....	8
8 - SERVIZI DI DIRECTORY	8
9 - INFRASTRUTTURA PER LA COOPERAZIONE APPLICATIVA.....	8
10 - INFORMATION RETRIEVAL	8
11 - GLOSSARIO.....	9
12 - RIFERIMENTI.....	9



1 - Premessa

Questo documento ha lo scopo di illustrare brevemente l'ambiente tecnologico in cui sono attualmente sviluppati i servizi telematici di Regione Toscana resi disponibili all'utenza Internet e/o specificatamente riservati agli utenti interni.

Tali principi costituiscono i requisiti base a cui fornitori/collaboratori/partner si dovranno ispirare durante la progettazione e lo sviluppo di applicazioni, e/o più in generale software che debba essere messo in produzione negli ambienti gestiti direttamente od indirettamente dall'Area ISIC.

Eventuali scostamenti dalle seguenti indicazioni dovranno essere concordate ed approvate per iscritto (in forma di verbale) dal Responsabile del Settore I.T.S.A.E.

Il generale principio ispiratore delle scelte tecnologiche qui riportate è improntato a sviluppare una architettura "aperta" e conforme ai principali standard definiti da organismi internazionali ampiamente riconosciuti e affermati (si cita a puro titolo di esempio IETF, W3C, OASIS, DVB, ...), nonché definiti a livello nazionale da organismi riconosciuti quali CISIS, CNIPA, UNI, CSP, ecc.

La scelta di architetture "aperte" multipiattaforma permette a Regione Toscana di svincolare il livello applicativo dal livello infrastrutturale delle singole piattaforme hardware, che nel tempo possono cambiare, salvaguardando gli investimenti dello sviluppo di software.

Le indicazioni ivi contenute rappresentano una fotografia istantanea degli ambienti informatici di Regione Toscana, e sono passibili di cambiamenti relativamente alle versioni, ed ai prodotti in uso, secondo le esigenze di Regione Toscana. I cambiamenti sostanziali saranno riportati in versioni successive di questo documento.

2 - Analisi e produzione documentazione

L'ambiente di analisi scelto è un ambiente object-oriented che supporta l'UML 2.0.

La documentazione prodotta sarà consegnata in formato **Uml-XMI** per i documenti di analisi e i formati **pdf**, **rtf** e **odt** per la documentazione generica.

Potrà essere richiesto che il codice sorgente eventualmente prodotto venga fornito anche nel formato adeguato per essere importato nel sistema **CVS** in uso presso Regione Toscana.

3 - Piattaforma infrastrutturale hardware e networking

L'ambiente di produzione dei server in Regione Toscana è implementato in ambiente **Linux** per le piattaforme "industry standard"; in ambiente **Unix** per le piattaforme mini/midi proprietarie; in particolare le versioni dei sistemi operativi in uso ad oggi sono rispettivamente Linux RedHat AS/ES 32/64 bit e HP-UX 11.X. Il parco macchine della server farm regionale comprende piattaforme HP PA-Itanium, SUN Sparc, Intel Xeon/Pentium DP/MP, AMD Opteron.

L'ambiente applicativo prevede l'utilizzo misto di software sia del mondo OpenSource/Freeware che proprietario, a seconda della loro miglior rispondenza alle esigenze di Regione Toscana.



3.1 - Architettura infrastruttura multi-tier Regionale

La Regione Toscana utilizza:

- **Apache 2** come HTTP/HTTPS server. Il server Apache implementa, quando necessario, le funzioni di “name virtual hosting”, autenticazione e (in qualche caso limitato) autorizzazione
- **Tomcat** come J2EE Web Container
- **Jboss** come J2EE Application Server

HTTP server, Web Container e Application Server non risiedono di solito sulla stessa macchina, quindi non condividono la “DocumentRoot” né tendenzialmente alcuna directory dati su disco; le componenti colloquiano attraverso un *connector*: attualmente è in uso il modulo Apache *mod_jk*. In particolare per gli ambienti j2ee viene adottata la versione certificata per il sistema operativo in uso (red)

3.1.1 - Infrastrutture supportate.

Le specifiche j2ee supportate dall'infrastruttura multi-tier utilizzata da regione toscana sono:

- Servlet 2.5 / jsp 2.1 (jdk 1.6.*)
- EJB 3

nota:

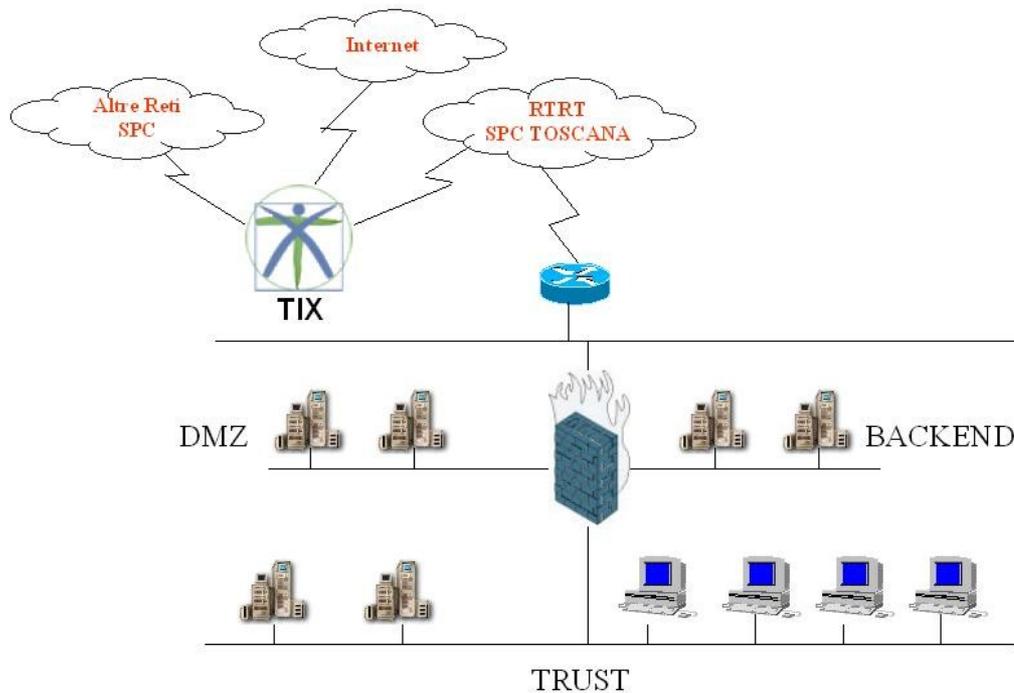
In Regione Toscana sono presenti ambienti che supportano le specifiche Servlet 2.5 / jsp 2.1 (jdk 1.5.) ma poichè la versione 1.5.* ha completato il processo di EOL (End Of Life) e non è più supportata dal distributore tali ambienti sono utilizzati per applicazioni già sviluppate e non sono oggetto di nuovi rilasci.*

Le applicazioni di nuovo sviluppo saranno rilasciate su ambiente jdk1.6.

Eventuali aggiornamenti di applicazioni preesistenti saranno compilati in ambiente jdk1.6.

3.2 - Ambiente di networking e regole di sicurezza perimetrale

In generale, le LAN delle Server Farm Regionali sono protette da sistemi Firewall, in varia architettura e configurazione che suddividono l'ambiente operativo in diverse LAN a diversi livelli di sicurezza. Idealmente si possono sempre individuare la rete esterna (Internet o RTRT), una LAN di front-end (DMZ), una LAN interna dei server, la LAN delle stazioni di lavoro della Regione Toscana.



Architettura logica del networking in Regione Toscana

Indipendentemente dalla tipologia dei sistemi Firewall in uso, in fase di progettazione di una applicazione devono essere tenuti in considerazioni i seguenti principi base:

- 1.se un servizio non è ospitato, o mediato da un server in DMZ non è accessibile da Internet (o comunque dall'esterno)
- 2.se un servizio non è esplicitamente abilitato sul firewall non sarà comunque accessibile
- 3.di norma sono abilitati all'accesso dalla rete esterna alla DMZ solo applicazioni che utilizzano protocolli TCP-based (quindi utilizzanti una "porta" nota).
- 4.le stazioni di lavoro ed i server sulla LAN interna possono accedere tutti i server in DMZ e nella LAN interna tramite svariati protocolli, ma verso l'esterno possono usare tendenzialmente solo http/https e solo mediante il tramite di un http-proxy posto in DMZ
- 5.più in generale, un servizio su Internet non è accessibile dalla LAN interna se non esiste il proxy relativo in DMZ

4 - Database

Il motore RDBMS attualmente usato è DB2.

4.1 - Accesso al Database

Le applicazioni sviluppate per RT saranno indipendenti dal motore RDBMS utilizzato.



Le applicazioni che risiedono su WebContainer o Application Server si connettono al database tramite l'intermediazione del container su cui risiedono.

Tramite la API JNDI l'applicazione in esecuzione all'interno del container dovrà quindi eseguire una ricerca presso un directory service (in genere messo a disposizione dallo stesso application server) di un oggetto che implementa l'interfaccia javax.sql.DataSource e tramite questo otterrà la connessione al Database.

Tutte le operazioni di gestione della connessione, connection pool, autenticazione ed autorizzazione saranno a carico del container il quale si frappone fra il database e l'applicazione finale.

L'applicazione dovrà utilizzare uno strumento per l'object relational mapping (ORM); si consiglia l'uso di **Hibernate**.

Inclusa alla fornitura del sistema/applicazione sarà richiesta la produzione di un documento che analizzi le prestazioni delle interrogazioni effettuate verso il motore RDBMS con particolare attenzione alla normalizzazione e all'utilizzo di meccanismi di ottimizzazione. Inoltre è richiesta la consegna in opportuno formato delle principali query di ricerca e/o modifica dati.

5 - Sviluppo applicazioni

Le applicazioni sviluppate in Regione Toscana sono di tipo web, sviluppate principalmente su tecnologia jsp, servlet e J2EE in genere secondo le specifiche indicate nel paragrafo 3.1.

Gli ambienti di produzione J2EE, dovendo ospitare applicazioni sviluppate da diversi fornitori, sono configurati con politiche di sicurezza impostate anche a livello di web container e application server.

Le applicazioni sviluppate per Regione Toscana dovranno essere progettate in modo tale che:

- Possano essere eseguite in concorrenza con altre applicazioni e quindi non dovranno effettuare operazioni che potrebbero ridurre o bloccare il funzionamento di altre applicazioni e/o servizi;
- Possano essere eseguite su web container e application server configurati in cluster ed accederanno alle risorse esterne secondo il paradigma J2EE;
- Presentino una welcome page;
- Adottino una politica di rotazione e/o cancellazione dei file di log;
- Permettano di indicare, tramite l'opportuno file di configurazione, le directory utilizzate per scritture di file temporanei e/o log;
- Sia esposto un servizio per la diagnostica; il servizio potrà essere interrogato dal sistema di monitoraggio di Regione Toscana;
- In caso di non funzionamento, presentino (se applicazioni con interfaccia utente) un messaggio di errore utile all'individuazione della causa.

Le applicazioni sono suddivise nelle seguenti tipologie: con interfaccia utente e web-services.

5.1 - Applicazioni con interfaccia utente

L'applicazione in questo caso presenta all'utente, tramite un generico browser, le necessarie pagine HTML. In funzione delle caratteristiche richieste le applicazioni saranno sviluppate seguendo i principali pattern per la programmazione su tecnologia j2EE (ad esempio: Business Delegate, Data Access Object (DAO), Intercepting Filter, Model-View-Controller, Service Locator, Session Facade)



I servizi che prevedono un accesso autenticato ed autorizzato mediante meccanismi di strong authentication utilizzeranno l'infrastruttura ARPA (per maggiori dettagli sull'infrastruttura si veda la documentazione indicata nel paragrafo Riferimenti).

5.2 - Web services

L'applicazione, o parte di essa, risulta essere composta da una serie di web services per cui il client è un programma che utilizza il protocollo **SOAP**. L'implementazione di SOAP utilizzata da Regione Toscana è **Axis** fornita dall'Apache Group.

Nel caso in cui l'accesso al webservice debba essere protetto saranno adottati, in funzione del livello di riservatezza desiderato, meccanismi di sicurezza sia sul canale di comunicazione (IP Filtering, SSL), sia utilizzando implementazioni dello standard WSS.

Nel caso in cui il web service debba essere acceduto esclusivamente da applicazioni ospitate sui sistemi server allocati in lan interna di Regione Toscana, il servizio sarà pubblicato su un frontend non pubblico.

5.3 - Indicazioni sul formato degli archivi

All'interno dei file descrittori degli archivi consegnati (jar,war,ear) saranno indicati, utilizzando gli appositi tag previsti dallo standard: nome applicazione, identificativo e data della versione, referente di Regione Toscana e referente del fornitore.

5.4 - Sviluppo applicazioni sicure

Regione Toscana utilizza una PKI che fornisce i servizi di emissione certificati digitali di autenticazione e di firma con valore legale, il servizio di rilascio di marche temporali e il servizio di posta elettronica certificata.

Per le applicazioni, che necessitano di autenticazione client secondo il protocollo HTTPS in modalità di mutua autenticazione, è adottata l'infrastruttura ARPA (per maggiori dettagli sull'infrastruttura si veda la documentazione indicata nel paragrafo Riferimenti).

Per le applicazioni e/o i componenti che accedono direttamente ai dispositivi di autenticazione e firma digitale e/o che necessitano di funzioni crittografiche vengono ad oggi utilizzati:

- **la libreria IAIK PKCS#11 Wrapper**. La libreria utilizza la Java Native Interface per accedere ai moduli PKCS#11 delle smart card.
- **IAIK-JCE e Baltimore Betrustrusted KeyTools** come insieme di API e implementazioni di funzioni crittografiche e di firma digitale.

L'accesso alle funzioni esposte dalle librerie sopra elencate avviene mediato da uno strato di software che permetterà di poter cambiare provider in futuro.

Regione Toscana mette a disposizione una implementazione di tale strato software.

6 - Data warehouse

In Regione Toscana è presente un'architettura per la costruzione di data warehouse a partire da dati gestionali.

L'ambiente scelto per la costituzione di data mart e data warehouse è composto da:

- **Data Stage (7.5.x)** IBM come strumento ETL
- **Business Object (XIR2)** come ambiente di analisi OLAP e produzione reportistica interattiva anche via Web (**Web Intelligence**)



L'architettura di riferimento è basata su metodologia di ROLAP e modello a *star schema* o *snowflake schema* ; il DBMS relazionale su cui poggia l'architettura è IBM DB2.

7 - Sistemi di Supporto alle Decisioni (DSS)

In Regione Toscana è presente lo strumento SAS 9 su piattaforma Unix/Linux per lo sviluppo di sistemi orientati al supporto alle decisioni.

8 - Servizi di Directory

In Regione Toscana è presente un servizio di Directory accessibile attraverso il protocollo LDAP dove sono memorizzate informazioni relative ai dipendenti regionali.

Regione Toscana sta attualmente migrando i servizi di Directory dall'attuale ambiente Iplanet Directory Server a Identity Management di Novell.

I servizi di Directory verranno implementati usando Novell Identity Manager.

9 - Infrastruttura per la cooperazione applicativa

Per garantire l'interoperabilità tra diverse applicazioni è stata realizzata una infrastruttura di cooperazione applicativa che supporta le due modalità principali della cooperazione:

- Invocazione sincrona di servizi
- Scambio asincrono di messaggi

Per maggiori dettagli sull'infrastruttura si veda la documentazione indicata nel paragrafo Riferimenti.

10 - Information Retrieval

In Regione Toscana è presente un'architettura di Information Retrieval.

Per maggiori dettagli sull'infrastruttura si veda la documentazione indicata nel paragrafo Riferimenti.



11 - Glossario

Applet	Applicazione scritta in Java che viene scaricata dal server Web e gira sul client all'interno del browser
Cluster	Pool comune di server che consentono di continuare a fornire il servizio a pieno regime, anche qualora alcuni dei macchinari stessi subiscano interruzioni nel funzionamento
DMZ	<i>DeMilitariZed network</i> rRete demilitarizzata, quindi ad un livello di sicurezza più basso di una rete <i>militarizzata</i> . Si indicano con questo termine le reti dove risiedono i server pubblici accessibili da Internet
J2EE	Java 2 Enterprise Edition
JNDI	Java Naming Directory Interface
JMS	Java Message Services <i>API Java per la gestione della messaggistica</i>
JSP	<i>Java Server Page</i>
OLAP	On-line Analytical Processing <i>Sistema che permette di effettuare analisi multidimensionale su dati provenienti da diverse fonti</i>
RDBMS	<i>Relational Database Management System</i> Database relazionali
ROLAP	Relational On-line Analytical Processing <i>Sistema che permette di effettuare analisi multidimensionale basato su database relazionale</i>
SOAP	<i>Simple Object Access Protocol</i> Protocollo basato su XML/HTTP per accedere a servizi, oggetti e server indipendenti dalla piattaforma
SQL	<i>Structured Query Language</i> Linguaggio di interrogazione database
UDDI	<i>Universal Description, Discovery and Integration</i> Servizio per la localizzazione degli Web Services
WDSL	<i>Web Service Definition Language</i> Linguaggio per la definizione di web services

12 - Riferimenti:

•CART: <http://www.cart.rete.toscana.it>

•ARPA: <http://www.e.toscana.it>

link : "linea 1", "2007010 Progetto ARPA- Infrastruttura per l'autenticazione, autorizzazione ed accesso ai servizi on-line"

•INFORMATION RETRIEVAL: <http://www.e.toscana.it>

link : "linea 1", D2 Sportello informativo per il cittadino: Rete degli URP della Toscana"

Il presente documento e le versioni precedenti sono reperibili all'indirizzo:

<http://www.e.toscana.it/enteRT/standard>