

REGIONE TOSCANA



Giunta Regionale

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

Settore I.I.T.R.

Ambienti di sviluppo e produzione
Standard tecnologici

Marzo 2005

Versione 2.2



Ambienti di sviluppo e produzione Standard Tecnologici

DOCUMENTO: Documento illustrativo – Ambienti di sviluppo e produzione- Standard Tecnologici			
EMISSIONE - VERIFICA - APPROVAZIONE			
	Funzione	Nome	firma
Emissione	Specialista Tecnico	Walter Volpi	
Emissione	Specialista Tecnico	Giovanni Armanino	
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



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
5	SVILUPPO APPLICAZIONI	6
5.1	APPLICAZIONI CON INTERCACCIA UTENTE	6
5.2	WEB SERVICES.....	6
5.3	INDICAZIONI SUL FORMATO DEL “WAR”	6
5.4	SVILUPPO APPLICAZIONI SICURE	6
6	DATA WAREHOUSE	7
7	SERVIZI DI DIRECTORY	7
8	INFRASTRUTTURA PER LA COOPERAZIONE APPLICATIVA	8
9	GLOSSARIO	8



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.I.T.R..

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, ecc.

La scelta di architetture "aperte" multiplatforma 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, in particolare **Rational Rose**.

Per quanto riguarda quindi la documentazione prodotta i formati supportati attualmente sono il formato **Rose 2000** per i documenti di analisi e i formati **pdf, rtf e doc** 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 3.0 32/64 bit, HP-UX 11.0 e Solaris 9. Il parco macchine della server farm regionale comprende piattaforme HP PA-RISC, 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

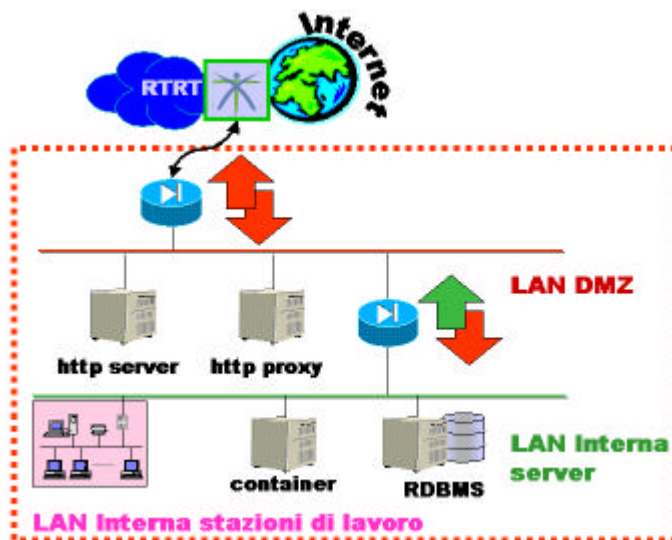
La Regione Toscana utilizza:

- **Apache 1.3.x / 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 4.1.x** come Web Container

HTTP server e Web Container non risiedono di solito sulla stessa macchina, quindi non condividono la "DocumentRoot" né tendenzialmente alcuna directory dati su disco; le due componenti colloquiano attraverso un **connector**: attualmente è in uso il modulo Apache mod_jk.

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 l'http/https e solo 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 usato è **Informix Dynamic Server**.

5 Sviluppo applicazioni

Le applicazioni sviluppate in Regione Toscana sono di tipo web e sono pubblicate tramite il JSP/servlet container **Tomcat 4.1.X**. 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. La tecnologia da utilizzare nella realizzazione è JSP2 (pattern MVC), Servlet e JDBC per la connessione al database. Se il riconoscimento dell'utente avviene tramite certificato digitale dovrà essere utilizzato il framework **SRTY**.

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.

Se il riconoscimento del client avviene tramite certificato digitale dovrà essere utilizzato un apposito filtro fornito da Regione Toscana che si interfaccia con il framework **SRTY**.

5.3 Indicazioni sul formato del "war"

Non sono ammessi scritture di file interne allo spazio in "webapps" delle singole applicazioni: eventuali directory in scrittura per file temporanei devono essere configurabili nell'opportuno file di properties ed in ogni caso esterne allo spazio dell'applicazione e del web container.

5.4 Sviluppo applicazioni sicure

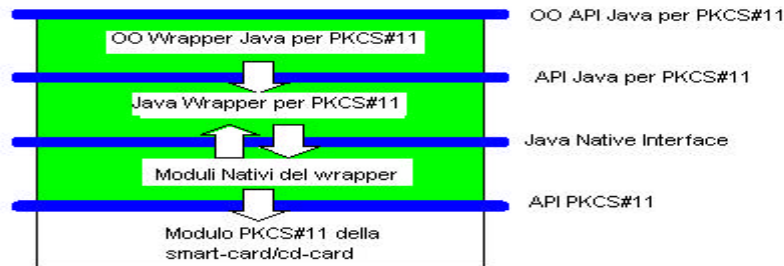
In Regione Toscana è disponibile una PKI in grado di emettere certificati digitali usati per l'autenticazione.

Per lo sviluppo di applicazioni Java con uso di autenticazione attraverso certificato digitale e di firma digitale viene usata la libreria **IAIK PKCS#11 Wrapper** per accedere ai moduli PKCS#11: questa usa la Java Native Interface per accedere ai moduli PKCS#11 delle smart cards. Nel caso di



Regione Toscana accede ai moduli PKCS#11 per le smart card e ai moduli PKCS#11 per le cd-card (usate in Regione Toscana in alternativa alle smart-card).

In figura lo schema di funzionamento del wrapper



Per lo sviluppo di applicazioni che gestiscono la firma digitale di dati viene usato il **IAIK-JCE** che è un insieme di API e implementazioni di funzioni crittografiche.

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** della Ardent come strumento ETL
- **Business Object** 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 Informix IIF2000.

7 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 e le informazioni relative ai servizi di cooperazione applicativa.

I servizi di Directory vengono implementati usando **Iplanet Directory Server**.



8 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 ulteriori approfondimenti su questa infrastruttura si rimanda al documento "CART Infrastruttura per la Cooperazione applicativa".

9 Glossario

Applet	Applicazione scritta in Java che viene scaricata dal server Web e gira sul client all'interno del browser
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
HTML	<i>HyperText Markup Language</i> Linguaggio per la pubblicazione di hypertext nel mondo Internet
J2EE	<i>Java 2 Enterprise Edition</i>
JMS	<i>Java Message Services</i> API Java per la gestione della messaggistica
JSP	<i>Java Server Page</i>
OLAP	<i>On-line Analytical Processing</i> Sistema che permette di effettuare analisi multidimensionale su dati provenienti da diverse fonti
RDBMS	<i>Relational Database Management System</i> Database relazionali
ROLAP	<i>Relational On-line Analytical Processing</i> Sistema che permette di effettuare analisi multidimensionale basato su database relazionale
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