

Requisiti tecnici ed operativi per l'allestimento del sito pilota

Survey

Nel presente documento si riassumono i contenuti del deliverable "**D5.1_1 Requisiti tecnici ed operativi per l'allestimento del sito pilota**" relativo all'attività *SP 5.1 Requisiti tecnici ed operativi per l'allestimento del sito pilota*, compiuta nell'ambito del quinto Obiettivo Realizzativo (OR 5) "Sperimentazione e valutazione dell'impatto della ricerca".

L'attività SP 5.1 è dedicata alla specifica delle tecnologie da utilizzare, dei dispositivi hardware e software impiegati per l'allestimento del sito pilota all'interno del quale verrà effettuata la sperimentazione dei servizi offerti dalla piattaforma SAPI.

Il documento inizia con la spiegazione dettagliata delle caratteristiche hardware dei tre dispositivi utilizzati come device lato client (chiosco, palmare e PC desktop) e dei due server (Web Server ed Application&Integration Server) impiegati per l'erogazione dei servizi.

Come mostrato in Figura 1, per la configurazione dell'architettura di rete sono state usate due reti Local Area Network, indicate genericamente come LAN A e LAN B, dove sono allocate rispettivamente le risorse hardware lato client e server.

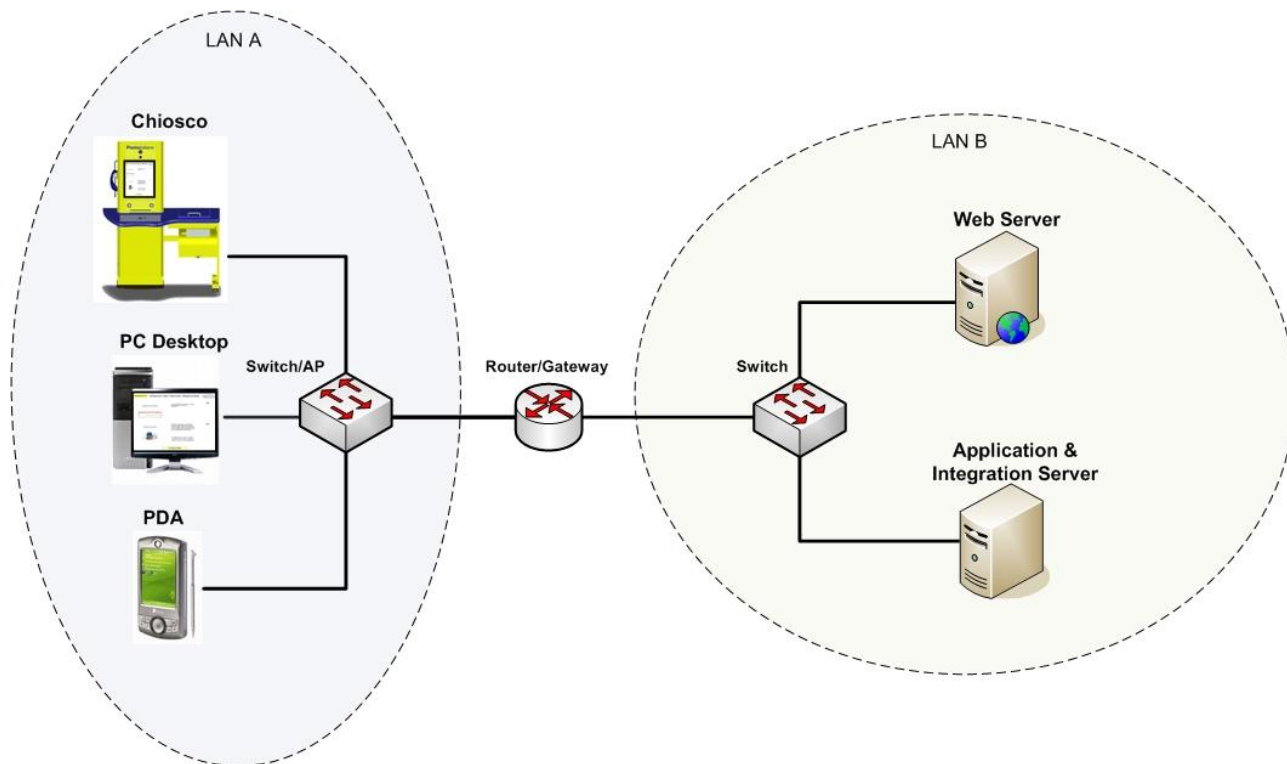


Figura 1: Diagramma di rete SAPI.

Subito dopo è descritta, come mostrato nel deployment diagram in Figura 2, la ripartizione delle componenti funzionali del framework SAPI all'interno dei nodi fisici che compongono l'ambiente di sperimentazione. Per ogni nodo individuato nel deployment diagram sono riportati gli applicativi software impiegati per garantire l'erogazione di un servizio intelligente.

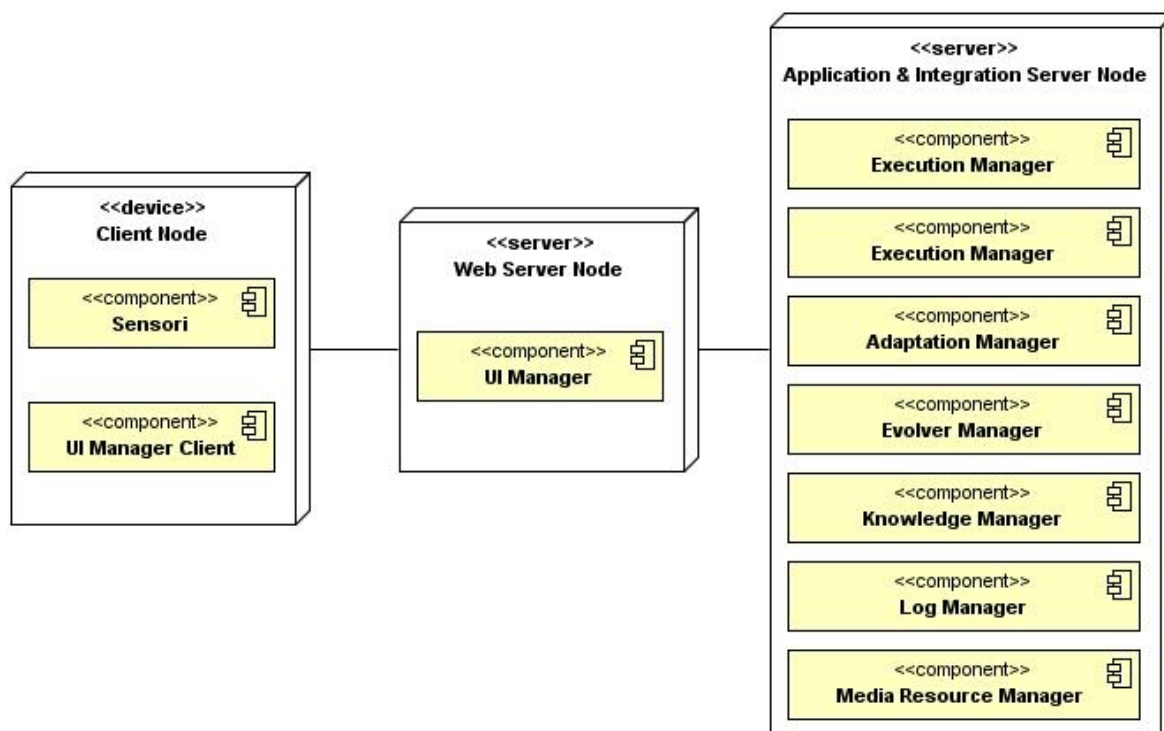


Figura 2: Deployment diagram SAPI.

Nel dettaglio l'ambiente di supporto all'esecuzione utilizzato per la fase di testing del prototipo consiste di:

- ❖ **Client Node.** Rappresenta l'hardware ed il software con cui è equipaggiato il chiosco. La configurazione di tale nodo prevede:
 - Un web browser Internet Explorer 6.0
 - JVM con Java Run-time Environment 1.6
 - Silverlight 2.0

Il software che controlla il sensore fisico in grado di rilevare la presenza dell'utente, leggere il tag RFID e avviare il browser, è un'applet Java.

- ❖ **Web Server Node.** E' un server con sistema operativo Windows Server 2003 Service Pack 2. La configurazione del server è la seguente:

- Web Server IIS 6.0
- Application Server .NET con Framework .NET 2.0 o superiore

In particolare il Web server gestirà un processo ASP.NET che comporrà la prima pagina HTML con i riferimenti ai file XAML e di conseguenza agli assembly con il code-behind, che rappresentano lo *UI Manager*. La pagina conterrà anche i riferimenti agli assembly .NET o agli applet java (ambidue con certificato associato) che implementano i *Sensori*.

❖ **Application Server Node.** . E' un server con sistema operativo Windows Server 2003 Service Pack 2 che espone, attraverso web services, le funzionalità necessarie per la composizione di un servizio intelligente. La configurazione del server prevede:

- Java Standard Edition Versione 5
- Apache Tomcat ver 5.5
- Apache AXIS 2
- Loquendo MRPC Server
- MySQL Server 5.0
- Framework JENA 2.5
- Jess Rule Engine

Nel deliverable sono inoltre descritte le specifiche ambientali adottate per l'allestimento dell'area nella quale verranno installate le apparecchiature. In particolare, la server farm è stata realizzata in ambiente climatizzato, protetto da accessi non autorizzati con un supporto ai dispositivi hardware costituito da colonne di rack destinati ad alloggiare i vari componenti hardware. Il locale è inoltre dotato di sistema antincendio con sensori di rilevazione fumi. La protezione verso qualsiasi tipo di perturbazione elettrica quali mancanza di tensione o variazioni di frequenza, è garantita da appositi UPS e relative batterie di accumulatori in configurazione parallela ridondata che assicurano la massima affidabilità verso i carichi critici.

Il documento si conclude con la descrizione dell'architettura del dimostratore VPN-UCI (vedi Figura 3) che ha lo scopo di evidenziare gli eventuali vantaggi ottenibili dall'utilizzo di una tunnel VPN per il collegamento delle postazioni d'utente ad un UCI-Service System che eroga i servizi Web di SAPI adottando un paradigma di individuazione dell'utente basato sul modello di identificativo univoco introdotto dall'ETSI.

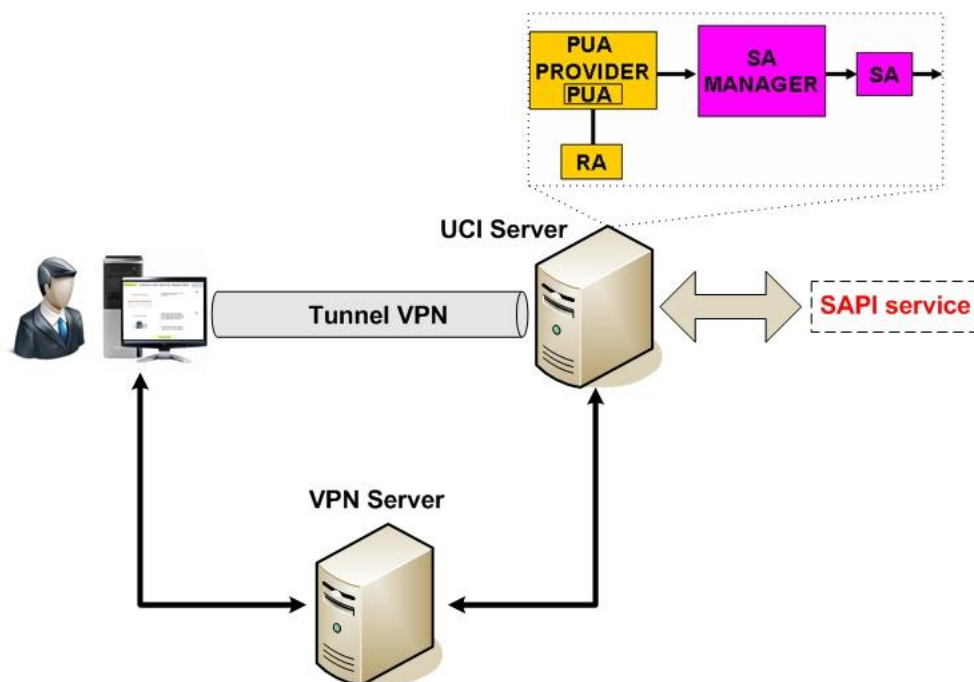


Figura 3: Architettura del dimostratore VPN-UCI.

Come mostrato nello scenario implementativo in figura, un utente che dispone di UCI può accedere mediante VPN alla piattaforma SAPI da una postazione su internet. A livello funzionale all'utente risulta trasparente la presenza del tunnel VPN attraverso il quale accede al servizio. Al servizio SAPI è associato un SA, che costituisce l'interfaccia di SAPI verso i Personal User Agent (PUA) e, quindi, verso gli utenti che vogliono accedere alla piattaforma. Le entità del framework UCI (i PUA e l'SA di SAPI) nonché la stessa piattaforma sono attestati nella intranet aziendale. Il punto di accesso alla intranet dall'esterno è il VPN Server.