

Analisi e specifiche per il supporto di VPN User Communication Identifier

Survey

Nel presente documento si riassumono i contenuti del deliverable **"D4.2_1 Analisi e specifiche per il supporto di VPN User Communication Identifier"** relativo all'attività *RI 4.2 Analisi e specifiche per il supporto di VPN User Communication Identifier*, nell'ambito del quarto Obiettivo Realizzativo (OR 4) "Studio di interfacce multimodali avanzate e dispositivi speciali per i disabili". L'architettura SAPI prevede per la strutturazione del Profiler un Profile Identifier. Questo blocco, le cui funzionalità sono l'identificazione utente e l'associazione dell'identificativo ad uno stereotipo d'utente, è nato con l'obiettivo di utilizzare per la parte di identificazione utente il modello UCI introdotto dall'ETSI. Tuttavia, il modello UCI è ancora lontano dall'essere standardizzato ed è tuttora "fermo" allo stato di proposta. In SAPI le indicazioni dell'ETSI su come implementare l'UCI sono state adattate all'architettura funzionale del framework (Figura 1) sia prevedendo le varie componenti funzionali necessarie al modello, sia adottando per la descrizione del profilo utente la struttura suggerita dall'ETSI.

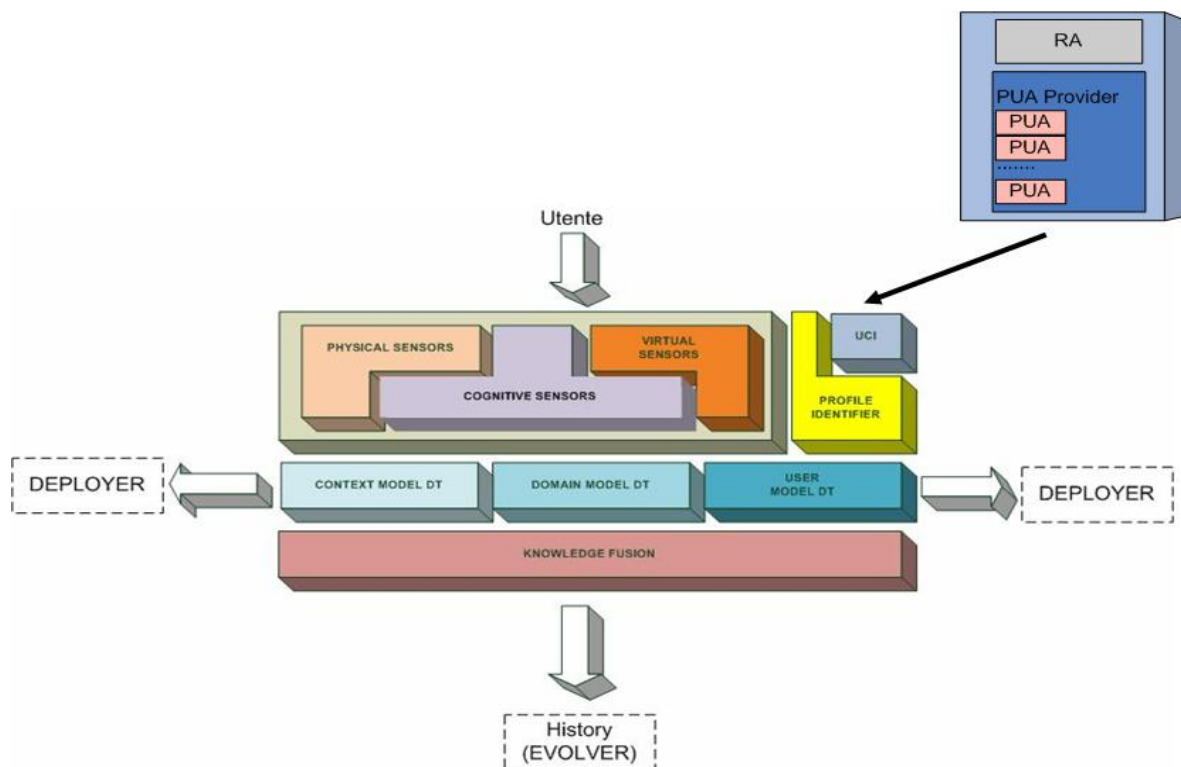


Figura 1: Architettura.

Il principio su cui si basa l'UCI consiste nell'individuare in maniera univoca ed universale ogni utente del mondo digitale. Tale identificativo, indipendente dai servizi, dalle reti e dai service providers, potrebbe porsi in sostituzione dei tanti contatti che un generico utente potrebbe avere (indirizzo e-mail, numero cellulare, ecc). Se volessimo riassumere i vantaggi che potrebbero derivare dall'utilizzo di un identificativo univoco ed universale come l'UCI potremmo dire che:

- permette di identificare un utente (ma anche organizzazioni) in maniera significativa;
- rende pressoché inutile la necessità per un utente di avere molti identificativi;
- permette di utilizzare una label user-friendly che descrive l'autore e/o il destinatario di una comunicazione;
- permette all'autore o il destinatario di una comunicazione di esigere l'autenticità degli identificativi;
- dà la possibilità di verificare l'identità del mittente o destinatario di una comunicazione attraverso procedure aggiuntive che permettono di essere sicuri che non siano altre persone ad utilizzare il terminale del proprietario UCI;
- è in grado di fornire un ambiente comune per la gestione e per il controllo di tutte le comunicazioni personali indipendentemente dal tipo di servizio;
- può comunicare una serie di ulteriori importanti informazioni relative all'utente;
- ha un debole impatto sull'architettura dei sistemi esistenti (sistema overlay).

Tutte queste caratteristiche, con il permesso del possessore dell'UCI, possono essere rese pubbliche ad altre persone. La struttura dell'UCI è riportata in Figura 2:

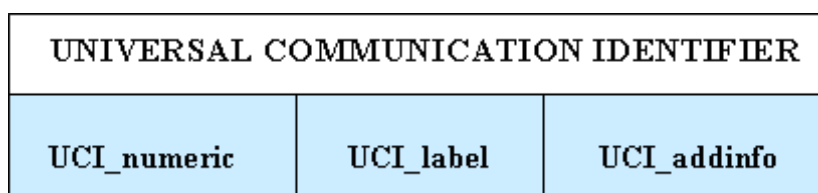


Figura 2: Struttura UCI.

- un identificativo numerico UCI_numeric che caratterizza l'univocità dell'intero UCI ed è essenziale per stabilire la comunicazione;
- una etichetta alfanumerica, non unica, UCI_label;
- un campo di informazioni aggiuntive UCI_addinfo non direttamente visibili agli utenti della comunicazione.

Di questi tre campi solo la label alfanumerica sarà direttamente visibile all'utente durante la comunicazione mentre la UCI_numeric e la UCI_addinfo saranno usate dal sistema di comunicazione sottostante. Prima di passare alle descrizioni dei singoli campi dell'UCI elenchiamo le sue principali proprietà:

- è persistente nel tempo;
- è affidabile e sicuro;
- è indipendente dalle reti di telecomunicazioni sottostanti;
- è indipendente dai servizi e dai loro provider;

- non varia con gli account utente.
- ❖ **UCI_numeric**

Il campo numerico dell'UCI è univoco e dovrebbe essere assegnato da una autorità trusted. Affinché le persone possano essere sicure che un UCI che hanno memorizzato gli permetterà sempre di contattare la persona a cui lo hanno associato c'è bisogno che tale parte numerica non cambi nel tempo (neanche in presenza di un cambiamento del service provider) rispondendo quindi al principio della "stabilità". Così, quando una persona cambia il suo nome o quando una persona cancella dei servizi di comunicazione e ne adotta di nuovi, la parte numerica dell'UCI permetterà sempre di contattarla. Infatti, attualmente, tali cambiamenti sono spesso la causa della perdita dei contatti delle persone presenti nella propria rubrica personale. Per quanto riguarda la scelta della parte numerica dell'UCI ci sono diverse politiche di scelta e si va per esempio dal riuso dell'attuale numero del cellulare ad una sequenza di numeri generata ad hoc. Ogni opzione ha molti vantaggi e svantaggi, ma la decisione sulla base della quale sarà scelto l'intervallo di valori sarà un problema più che altro commerciale e/o di natura regolamentare. A tale scopo viene considerata nell'architettura UCI la componente RA (Registration Authority).

❖ **UCI_label**

Uno dei principali vantaggi del modello UCI è l'etichetta alfanumerica. Infatti, in ogni comunicazione UCI-based, un utente ha la possibilità di vedere l'etichetta alfanumerica UCI del suo interlocutore. Queste etichette non dovranno essere univoche dato che l'unicità è gestita dalla parte numerica. Per questo motivo, non c'è alcun vincolo sulla tipologia del nome che può essere visualizzata nell'etichetta. Il campo UCI_label può contenere il nome di una persona o qualsiasi altro nome (di una società, un'azienda, ecc). Comunque, distinguiamo tre diverse varianti:

1. "*nome autentico*": questo è uno dei più potenti vantaggi di UCI dato che assicura che l'altra persona veda il tuo nome vero. Il nome autentico è associato a un certificato, emesso da un'autorità trusted, che certifica che il nome utilizzato è di una persona che ha diritto ad usarlo.
2. "*alias*": un nome qualunque appare nel campo etichetta che non ha legami (almeno apparentemente) con il "nome autentico". L'alias permette alle persone di utilizzare soprannomi amichevoli invece del loro nome autentico, più formale.
3. "*anonimo*": il campo di etichetta in questo caso è vuoto. E' improbabile che questa variante sia utilizzata molto frequentemente e viene fornita solo per permettere comunicazioni anonime, che è qualcosa che attualmente è possibile.

Decidere quale versione del campo etichetta utilizzare è di grande importanza nella comunicazione in un sistema UCI, a partire dalla attendibilità degli interlocutori di una comunicazione.

❖ **UCI_addinfo**

Il campo UCI_addinfo ovvero quello delle informazioni aggiuntive è l'elemento meno definito dell'UCI. Questo è il campo che può essere migliorato ed esteso nel tempo per permettere di

personalizzare una comunicazione UCI alle varie esigenze. Le informazioni che potrebbero essere contenute in questo campo sono le seguenti:

1. Dati anagrafici
2. Modalità preferita di comunicazione
3. Lingua preferita
4. Disabilità
5. Abilità
6. Settori di interesse
7. Appartenenza dell'UCI: Privato o Corporate (azienda)
8. Ordine lettura label (per conferire una semantica all'etichetta; ad esempio se l'etichetta fosse del tipo "Mario Rossi Posteitaliane" allora l'ordine sarebbe nome-cognome-azienda)
9. Registration authority (autorità trusted che ha rilasciato l'UCI al titolare)
10. Disponibilità certificato digitale (indica se è disponibile un certificato digitale per la label autentica e l'eventuale autorità certificatrice)
11. Autenticità della label (per capire se con chi si comunica è trusted): Autentica, Alias o Anonima

I dati contenuti in questo campo possono essere anche codificati visto che non è che devono essere presentati direttamente agli utenti. In Figura 3 è riportato un generico esempio di UCI dove i dati contenuti in UCI_addinfo sono opportunamente codificati:

UNIVERSAL COMMUNICATION IDENTIFIER		
123456789	Mario Rossi	b7;g4;k12;r24

Figura 3: Esempio di UCI.

Per poter garantire un corretto utilizzo del modello UCI è necessario che esista un ambiente progettato ad hoc che consenta agli utenti di poter stabilire una comunicazione gestendo eventuali preferenze di comunicazione, abilità, disabilità ecc. In quest'ottica un "environment UCI" (Figura 4), racchiude le seguenti entità funzionali: Personal User Agent (PUA) e Service Agent (SA).

Per esse è riportata una breve descrizione così come da proposta architettonica ETSI-UCI:

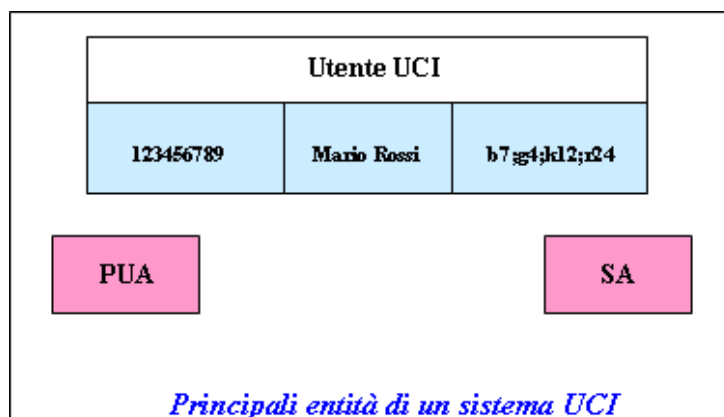


Figura 4: Principali entità di un sistema UCI.

❖ **Personal User Agent (PUA)**

Il PUA è un'entità software che agisce dal lato utente per facilitare la gestione della comunicazione sia in trasmissione che in ricezione. Una volta identificato l'utente, comunica con esso. Il PUA:

- ha accesso lista dei contatti dell'utente;
- ha accesso alle informazioni sullo stato corrente dei servizi di telecomunicazioni dell'utente (ad esempio "cellulare acceso e raggiungibile", "impossibile contattare il telefono fisso", "impossibile leggere e-mail al momento", "impossibile inviare contenuto multimediale");
- ha accesso alle preferenze di comunicazione dell'utente;
- comunica con gli altri PUA al fine di realizzare reciprocamente il proprio obiettivo;
- comunica con i Server Agent dei servizi a cui l'utente UCI è registrato.

Un PUA non potrà mai comunicare a terzi informazioni personali (informazioni sensibili) del proprio utente UCI se non esplicitamente autorizzato dallo stesso.

❖ **Service Agent (SA)**

Così come il PUA, il SA è un'entità software che è legata ad un servizio o ad una rete ed è tipicamente fornito dal provider del servizio o della rete. Esso rappresenta il collegamento tra l'UCI ed i servizi o le reti di telecomunicazione. Un SA comunica con:

- i PUA;
- il proprio servizio o la propria rete;
- gli altri SA (in maniera più ristretta).

Il SA fornisce un'interfaccia verso il PUA indipendentemente dall'architettura interna della sua rete/servizio. Qualora la rete/servizio ha già proprie entità che forniscono un punto unico di controllo sulle funzionalità di rete/servizio, il SA fornisce solo un'interfaccia verso queste

funzioni di controllo. Se invece la rete/servizio non fornisce un tale punto di controllo, il SA deve anche fornire funzionalità aggiuntive che consentano di instaurare meccanismi di controllo all'interno della rete/servizio. Il SA non dovrebbe mai rilasciare informazioni personali (come identificativi) a meno che specificatamente autorizzato dal proprietario.

Un possibile scenario d'uso che dimostri la predisposizione all'integrazione di un'architettura UCI in SAPI è raffigurato in Figura 5:

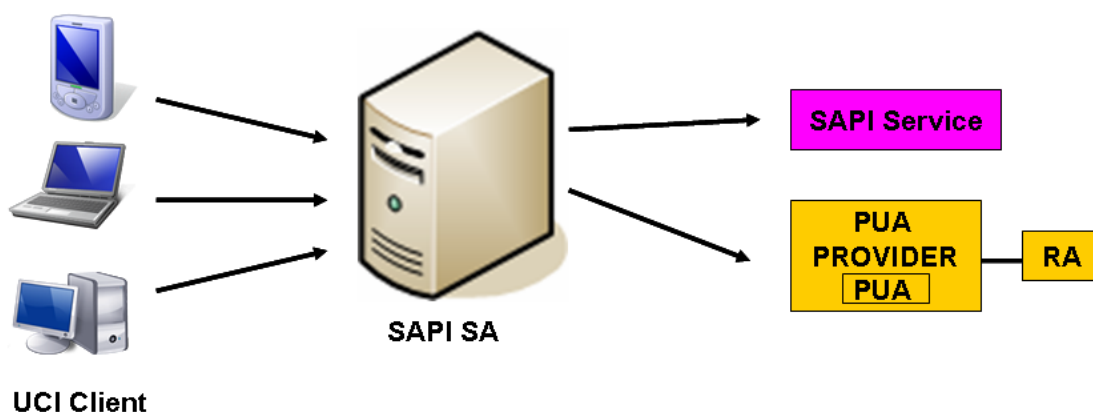


Figura 5: Scenario d'uso

Gli attori, così come mostrato, sono:

1. utente dotato di UCI (in particolare sono considerati gli utenti della piattaforma SAPI in quanto il servizio proposto nello scenario è quello SAPI) ,
2. il SA che funge da punto di accesso ai servizi SAPI,
3. i servizi di SAPI,
4. il PUA Provider,
5. il RA.

Alle componenti fondamentali dell'UCI precedentemente descritte si sono aggiunte altre due componenti, PUA Provider e RA. Il primo ha la funzione di gestire i PUA, le loro funzionalità, la loro attivazione, la loro configurazione, l'accesso da parte dei SA ai PUA ed inoltre ha anche la funzione di contenitore dei PUA. Per quel che concerne il RA esso è l'autorità *trusted* riconosciuta dalla comunità come l'ente di rilascio e di validazione dell'UCI. L'esistenza di almeno un RA assicura l'unicità di tale identificativo UCI.

La rappresentazione delle relazioni fisiche tra le principali entità funzionali all'interno di un sistema UCI-SAPI i è in Figura 6.

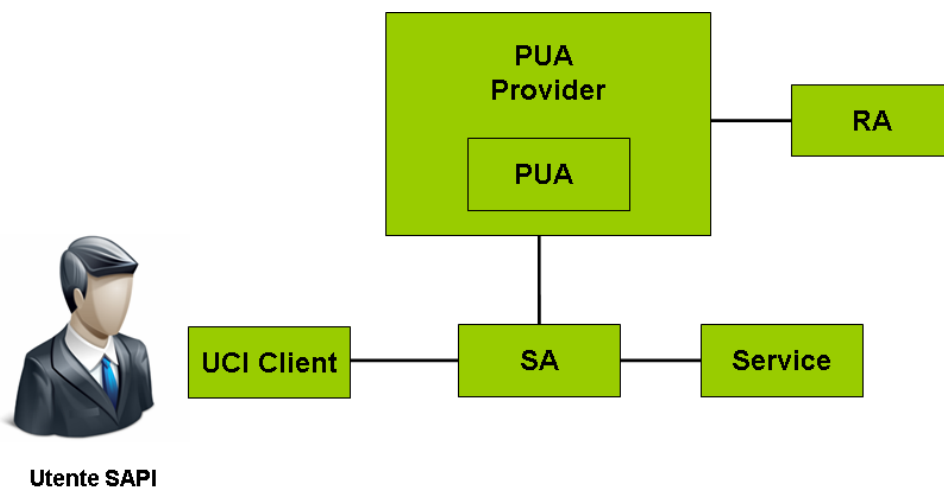


Figura 6: Relazioni tra le principali entità funzionali.

In generale l'architettura di rete ipotizzata è quella mostrata in Figura 7 dove si è tenuto conto del caso generico in cui l'utente intende usufruire di più servizi. In questa ottica si considerano N SA, uno per ogni servizio a cui potrebbe accedere l'utente, e come da proposta ETSI ad ognuno dei SA possono accedere più UCI Client. Considerando che con UCI System sono state raggruppate tutte quelle componenti coinvolte nell'architettura UCI proposta, tranne l'UCI Client, l'uso della VPN consente di considerare internamente all'UCI System una LAN. Il punto di accesso a tale LAN dall'esterno è il VPN Server dove si è scelto di far risiedere i SA. In tale LAN devono essere inclusi solo i SA, il PUA Provider ed il RA e non i servizi in quanto potrebbero essere esterni. A livello funzionale all'utente (che dispone dell'UCI Client) risulta trasparente la presenza del tunnel VPN attraverso il quale accede ai SA.

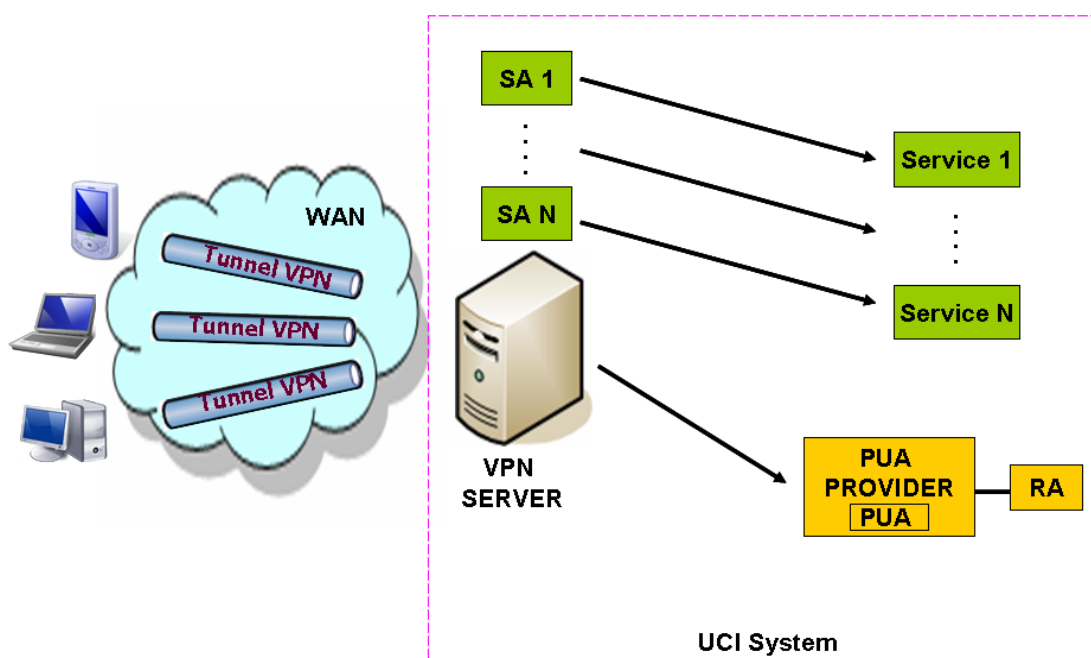


Figura 7: Architettura di rete generica

Nel caso del dimostratore UCI-VPN, il sistema SAPI è stato preso in considerazione come servizio a cui associare un SA. L'utente è quindi un utente SAPI. L'architettura di rete del dimostratore è quella mostrata in Figura 8.

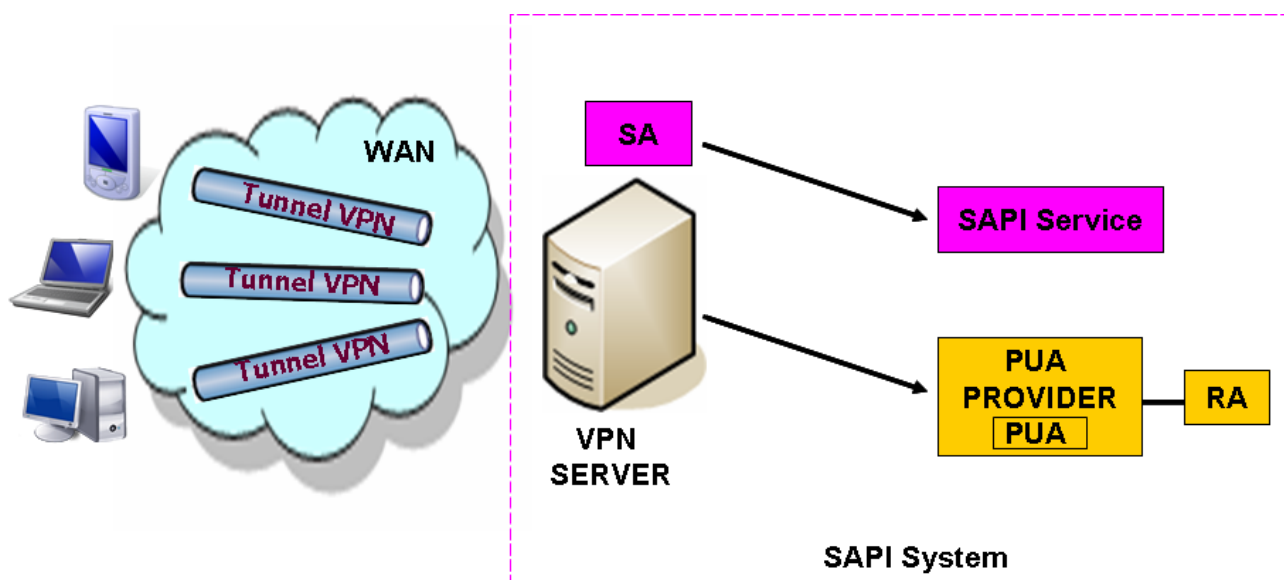


Figura 8: Architettura di rete del dimostratore SAPI

Ulteriore integrazione con SAPI di questa architettura UCI proposta è il fatto che il PUA Provider ed il RA siano parti integranti della componente Profiler all'interno del sistema SAPI. Per tale motivo il SAPI Service sarà localizzato nella LAN in cui, come detto, sono presenti PUA Provider, SA e RA.