Regole d'uso della rete InterSST

Rev.	Data	Descrizione	Redatto	Verificato	Approvato
6.3	2016-03-03	Prima versione pubblica	Alessandro Cardia Francesco Garosi Fabio Maria Teti Alessandro Picchi	Alessandro Picchi	Alessandro Picchi

Sommario

Introduzione

InterSST, come fase transitoria per il piu' ampio progetto di realizzazione della rete unitaria della Sanità Toscana, è una rete WAN MPLS sulla quale possono essere esposti servizi, raggiungibili e fruibili da parte di tutti gli Enti e Aziende del Servizio Sanitario della Toscana (SST), ma allo stesso tempo riservati in quanto non accessibili da Internet.

Gli Enti e Aziende del SST che si affacciano sulla rete InterSST sono 21; ad ognuno di questi soggetti sono state assegnate delle subnet /26 o /27 di indirizzi IP pubblici. Gli indirizzi IP InterSST utili per esporre servizi sulla rete, sono ovviamente limitati: al netto degli indirizzi necessari alla configurazione dei routers e dei firewall, la disponibilità effettiva per i soggetti è la seguente:

Indirizzi Disponibili	Subnet	Nr. Soggetti	Soggetti
56	/26	15	12 ex-ASL, 3 ex-ESTAV
24	/27	6	4 AOU, ISPO, Fondazione Monasterio

La rete InterSST, a livello di firewall periferici Telecom, è chiusa da e verso Internet, ed è aperta da e verso RTRT3. Le 21 sottoreti InterSST devono essere chiuse da e verso RTRT3 tramite regole dei singoli firewall aziendali, lasciandole aperte alla sola InterSST.
In questo modo si realizza una porzione di Extranet "riservata" ai soggetti del SST: infatti, come già delineato, tutto ciò che viene esposto sulla rete InterSST sarà ***invisibile e irraggiungibile*** da Internet.

Le modalità di esposizione/erogazione dei servizi sulla InterSST sono tecnologicamente del tutto analoghe alle modalità di esposizione/erogazione di qualsiasi servizio in Internet. In questo senso, se un qualsiasi servizio non è esponibile in Internet (per esempio applicazioni Client/Server, o pagine web che contengano riferimenti ad URL con indirizzi IP privati), non lo sarà neanche in InterSST.

InterSST è stata costituita principalmente per dare modo alle 12 ex-ASL toscane di condividere le applicazioni amministrative indispensabili alla fusione verso le sole 3 ASL previste dall'ultima legge regionale di riordino del SST.
Non si è previsto di utilizzare InterSST per esporre servizi Sanitari, e non si è previsto che sulla InterSST possano essere scambiati dati sanitari, sensibili e riservati.

In questo documento si fissano le regole fondamentali tramite cui i soggetti interessati e titolati potranno usufruire dei servizi erogati dalla rete InterSST.

Caratterizzazione dei servizi erogati

Prevedendo le future esigenze di erogazione di servizi sulla rete, il gruppo di progetto della rete InterSST ha proposto una caratterizzazione degli stessi, individuando gruppi di indirizzi all'interno delle subnet assegnate ai soggetti InterSST, da riservare a precisi ambiti di attività.

Indirizzi	**%**	**Servizi**
Riservati	32 %	Apparecchiature di gestione ed indirizzamento (routers, firewall, ...)
Servizi di Base	3 %	Servizi di gestione della rete (monitoraggi, DHCP, DNS, ...)
Progetti Regionali	18 %	Servizi per progetti a carattere regionale
Servizi Azienda Sanitaria di AV	36 %	Servizi per nuova Azienda Sanitaria a fattor comune per le ex-Aziende
Progetti condivisi Area Vasta	11 %	Progetti condivisi di Area Vasta

È disponibile una tabella, per ogni Ente, in cui è specificata la caratterizzazione di ciascun indirizzo IP ad esso assegnato su InterSST, in modo che l'utilizzo possa risultare il più possibile omogeneo "per costruzione"; non sarà possibile derogare a tale disposizione, se non per esigenze di evidenza strategica e con soluzioni concordate.

Va comunque osservato che esistono metodi per far erogare, sotto determinate ipotesi, più di un servizio attraverso lo stesso indirizzo IP – ad esempio con la gestione puntuale delle porte IP di erogazione o, come accennato nel seguito, con l'uso di reverse proxy – e pertanto sarà cura del personale ICT ESTAR incaricato della gestione di InterSST proporre e realizzare il raggruppamento di servizi multipli, secondo criteri di omogeneità e ottimizzazione delle risorse, sotto un unico indirizzo IP.

Esigenza di regolamentazione della InterSST

L'esigenza di regolamentare l'utilizzo della rete InterSST deriva da considerazioni di natura diversa:

- **spazio di indirizzamento**: gli indirizzi disponibili per esporre servizi sulla rete sono limitati, pertanto devono essere utilizzate strategie atte ad ottimizzarne l'uso;
- **riservatezza dei dati**: la rete non e' proprietaria, ma si appoggia su apparati pubblici di Telecom, quindi la protezione dei dati che vi transitano e' a carico di ESTAR;
- **attivazione di un nuovo servizio**: è necessario individuare chi può richiedere che un determinato servizio sia esposto sulla InterSST;
- **valutazione della liceità di un servizio**: è necessario che qualcuno sia titolato a decidere quali servizi possano essere esposti sulla InterSST;
- **verifiche tecniche**: è necessario che qualcuno verifichi che le caratteristiche tecniche di ogni applicazione, candidata ad essere esposta, rispondano a criteri di scelte tecnologiche e implementative tali da garantirne il buon funzionamento.

Iter della richiesta di esposizione di un servizio

Pur tenendo conto delle varie esigenze di condivisione dei soggetti SST, delle esigenze di sicurezza e riservatezza, della concorrenza delle responsabilità, delle caratteristiche tecniche della rete, si ritiene opportuno definire un percorso che risulti il più snello possibile, ma che al tempo stesso garantisca l'efficacia della validazione sulla base delle considerazioni precedentemente indicate.

Nella individuazione dell'iter, si è tenuto conto sia di caratteristiche tecniche, che di modalità organizzative.

Richiedente

La richiesta di esposizione di un servizio deve provenire dal soggetto proprietario del servizio. Per quanto possa sembrare banale, questa affermazione vuole sottolineare la titolarità del servizio e dei dati che il servizio rende fruibile, anche in termini di responsabilità sulla funzionalità ed attendibilità degli stessi.

Rispetto ai 21 soggetti InteSST, i richiedenti saranno soltanto i 10 Enti/Aziende appartenenti al SST:

Richiedenti SST (10)	**Soggetti InterSST (21)**
USL Nordovest	ASL 1 Massa
	ASL 2 Lucca
	ASL 5 Pisa
	ASL 6 Livorno
	ASL 12 Viareggio
USL Centro	ASL 3 Pistoia
	ASL 4 Prato
	ASL 10 Firenze
	ASL 11 Empoli
USL Sudest	ASL 7 Siena
	ASL 8 Arezzo
	ASL 9 Grosseto
AOU Pisana	AOU Pisana
AOU Senese	AOU Senese
AOU Careggi	AOU Careggi
AOU Meyer	AOU Meyer
ESTAR	ESTAV-Centro
	ESTAV-Nordovest
	ESTAV-Sudest
Fondazione Monasterio	Fondazione Monasterio
ISPO	ISPO

E' necessario che i 10 soggetti richiedenti individuino una o più persone deputate a richiedere l'esposizione di servizi sulla InterSST, in modo che la richiesta arrivi ad ESTAR con la corretta legittimità.

Per mettere in grado ESTAR di comprendere bene la natura della esigenza e del servizio, e applicare le corrette regole sui firewall aziendali, il richiedente dovrebbe indicare:

- nome del servizio
- indirizzo IP sorgente privato
- porta/e utilizzate dal servizio
- se è possibile ricollocare il servizio su porte diverse dall'originale
- breve descrizione del servizio da esporre e dei dati da rendere fruibili
- fornitore del servizio (ditta esterna o srtuttura interna) e suoi recapiti
- eventuali restrizioni sui soggetti SST abilitati ad accedervi
- eventuali estensioni a soggetti non SST abilitati ad accedervi (cosa realizzabile se tali soggetti si affacciano su RTRT3)

Prima ricezione della richiesta

La raccolta della richiesta è a carico di ESTAR che ha la competenza tecnica informatica e istituzionale per condurla con completezza.

Dato che la richiesta di esposizione arriva a ESTAR da personale precedentemente individuato, non sarà necessario procedere ad ulteriori indagini sulla rispondenza tra richiesta e reale necessità di esposizione del servizio. Sarà invece necessario verificare se il servizio sia già fruibile in altra modalità, se ci sono indirizzi InterSST disponibili, o se l'esposizione su InterSST del servizio sia il modo corretto per renderlo fruibile. Per esempio, per le caratteristiche del servizio (nessuna implicazione di sicurezza, generalizzazione del bacino di utenza, ...), Internet potrebbe essere la modalità migliore di esposizione, o addirittura l'unica (come ad esempio per albi che devono essere consultati pubblicamente).

Le richieste saranno raccolte dal dirigente ICT Responsabile della UU.OO.SS. Reti per l'Area Vasta di pertinenza.
Le richieste potranno essere approvate o respinte.

Di seguito tabella con i riferimenti dei dirigenti ICT responsabili per InterSST per ciascuna Area Vasta.

Area Vasta	**UU.OO.SS.**	**Dirigente Responsabile**	**e-mail**
Nord Ovest	Reti Toscana Nord Ovest	Dr. Marco Battaglia	marco.battaglia@estar.toscana.it
Centro	Reti Toscana Centro	Dr. Simone Morini	simone.morini@estar.toscana.it
Sud Est	Reti Toscana Sud Est	Dr.ssa Stefania Scarnato	s.scarnato@estar.toscana.it

Tra la richiesta di esposizione di un servizio da parte dei 10 soggetti istituzionali e la ricezione della stessa da parte del dirigente ESTAR preposto, resta comunque confermato il fondamentale ruolo di mediatore dei rapporti con le Aziende del SST svolto dai KAM ICT delle tre Aree Vaste.

Esame tecnico del servizio

Una volta che la richiesta è stata vagliata e validata dai dirigenti ESTAR nella fase di prima ricezione, questa potrà essere passata alla fase di esame tecnico.
L'esame tecnico verrà svolto da personale informatico di comparto del dipartimento ICT di ESTAR, ed è teso a capire effettivamente se, per le caratteristiche tecniche e architetturali del servizio, questo possa essere esposto in InterSST.

E' possibile che per esporre in InterSST un servizio, si verifichi la necessità di apportare qualche piccola modifica al software; per questo è importante che il richiedente indichi, in richiesta, il fornitore del servizio (ditta esterna, o personale interno) e i suoi recapiti. È inoltre opportuno mettere a conoscenza il personale che gestisce InterSST dell'eventuale servizio di assistenza e manutenzione del software che realizza il servizio da esporre, al fine di poter valutare l'effettiva possibilità di riconfigurare o modificare il software in modo da rendere fruibile il servizio su InterSST.

E' certamente vero che InterSST è stata concepita e realizzata per esporre i servizi amministrativi necessari alla nascita delle nuove tre USL toscane di Area Vasta, oltre che di ESTAR stesso, ma è anche vero che, se l'accesso ai servizi esposti in InterSST avviene su socket sicuro, non esiste alcuna preclusione tecnica per l'esposizione di servizi inerenti dati sanitari.

Registrazione DNS

Una volta che l'esame tecnico è risultato positivo e il servizio richiesto è risultato tecnicamente idoneo per essere erogato sulla InterSST, lo si registra nel DNS opportuno, e poi si passa alla sua esposizione.

La registrazione del nome di un servizio InterSST, si basa su due considerazioni:

1. le risorse esponibili/erogabili provengono dai 21 soggetti InterSST
2. chi di fatto espone/eroga i servizi, sono i 10 soggetti SST esistenti dal 1° gennaio 2016, cui corrispondono altrettanti nomi di dominio

Una qualsiasi risorsa esposta/erogata sulla InterSST avra' nome nome-risorsa@unodei10domini, le entries si troveranno nei DNS autoritativi dei domini dei 10 soggetti SST, e l'indirizzo IP corrispondente farà parte della subnet assegnata ad uno dei 21 soggetti InertSST.

Il nome della risorsa InterSST sarà risolto nel mondo intero, e:

a) la risorsa sarà raggiungibile all'interno di InterSST, a meno di regole restrittive sul firewall lato esponente
b) la risorsa potra' essere raggiungibile in ambito RTRT3, in virtù di regole estensive sul firewall lato esponente
c) la risorsa non sarà mai raggiungibile al di fuori di RTRT3

Ecco lo schema generale di quanto sopraesposto:

Soggetto InterSST	**Subnet Indirizzi IP**	**Dominio Internet**	**Registrante Admin-C, Tec-c**
ASL 1 Massa	159.213.144.128/26	uslnordovest.toscana.it	Regione Toscana Angelo Marcotulli - ADM Vincenzo Martiello - TEC
ASL 2 Lucca	159.213.144.64/26		
ASL 5 Pisa	159.213.144.192/26		
ASL 6 Livorno	159.213.144.0/26		
ASL 12 Viareggio	159.213.142.192/26		
ASL 3 Pistoia	159.213.143.192/26	uslcentro.toscana.it	Regione Toscana Angelo Marcotulli - ADM Vincenzo Martiello - TEC
ASL 4 Prato	159.213.143.128/26		
ASL 10 Firenze	159.213.143.64/26		
ASL 11 Empoli	159.213.143.0/26		
ASL 7 Siena	159.213.142.128/26	uslsudest.toscana.it	Regione Toscana Angelo Marcotulli - ADM Vincenzo Martiello - TEC
ASL 8 Arezzo	159.213.142.0/26		
ASL 9 Grosseto	159.213.142.64/26		
AOU Pisana	159.213.146.128/27	ao-pisa.toscana.it	Azienda Ospedaliera Pisana Mario Vettori - ADM Fabio Maria Teti - TEC
AOU Senese	159.213.146.32/27	ao-siena.toscana.it	Azienda Ospedaliera Senese Silvano Ripaccioli - ADM Gilberto Civai - TEC

Soggetto InterSST	Subnet Indirizzi IP	Dominio Internet	Registrante Admin-C, Tec-c
AOU Careggi	159.213.146.64/27	aou.careggi.toscana.it	Azienda Ospedaliera Careggi Riccardo Sforza - ADM Barbara Cappelli - TEC
AOU Meyer	159.213.146.96/27	meyer.it	Azienda Ospedaliera Meyer Paolo Morello Marchese - ADM Massimiliano Mancini - TEC
ESTAV-Centro	159.213.145.0/26	estar.toscana.it	Regione Toscana
ESTAV-Nordovest	159.213.145.64/26		Angelo Marcotulli - ADM
ESTAV-Sudest	159.213.145.128/26		Vincenzo Martiello - TEC
Fond. Monasterio	159.213.146.160/27	ftgm.it	fondazione toscana gabriele monasterio Luigi Donato - ADM - TEC
ISPO	159.213.146.0/27	ispo.toscana.it	ISPO (Istituto per lo studio e la prevenzione oncologica) Gianni Amunni - ADM Andrea Baldini - TEC

N.B.: Mario Vettori, Silvano Ripaccioli, Gilberto Civai, Riccardo Sforza, Barbara Cappelli, Paolo Morello Marchese e Massimiliano Mancini, benché attualmente registrati come Amin-C e Tec-C, non svolgono più attività coerenti con la registrazione. (pensionamento, cambio attività, trasferimento presso altro Ente).

Convenzioni per i nomi degli Host

Al fine di evitare il diffondersi di nomi degli host che ne rendano difficile l'identificazione, è opportuno che tali nomi vengano attribuiti con criteri il più possibile omogenei. Il nome di uno host deve rispondere ad alcune caratteristiche:

- identificare con precisione l'attività primaria dello host
- identificare mnemonicamente il servizio o i servizi che lo host espone
- essere facilmente memorizzabile e semplice da trascrivere (ad esempio per URL dettate al telefono)

pertanto si raccomanda di assegnare (o far assegnare) nomi secondo le linee guida che seguono. Nella tabella si indicano alcune funzionalità comuni che possono avere degli host alle quali dovrebbero corrispondere i criteri di nomina indicati:

Tipo Servizi	***Protocolli Principali***	***Criteri Nome***
Siti Web	HTTP, HTTPS	www, www1, …, www*N*
Posta Elettronica	POP3, SMTP, IMAP	mail
Autenticazione	LDAP, TACACS, RADIUS, Kerberos	auth01, …, auth*NN*
Reverse Proxy	HTTP, HTTPS, altri	rp01, …, rp*NN*
Gateway Applicativi	RDP, VDI, altri	appgw01, …, appgw*NN*
Monitoraggio	SNMP, SSH, web service	mon01, …, mon*NN*
Infrastruttura CAST	web service	cast01, …, cast*NN*

Dove per *xxx01, …, xxxNN* si intende lo mnemonico *xxx* seguito da un intero progressivo a due cifre fisse, assegnato dal personale ESTAR secondo l'ordine di registrazione. Per quanto riguarda i servizi applicativi esposti, il nome dello host (o l'*alias* di uno degli host precedentemente nominati secondo i criteri della tabella sopra riportata, specialmente nel caso dei reverse proxy e dei gateway applicativi) dovrà avere le seguenti caratteristiche:

1. ricordare mnemonicamente in modo chiaro la natura del servizio applicativo offerto

2. essere semplice da digitare e facilmente riconoscibile, possibilmente costituito da una parola italiana a meno che un termine non italiano non sia diffuso a tal punto da risultare più indicato (ad esempio: tra *compartecipazione-alla-spesa.uslcentro.toscana.it* e *ticket.uslcentro.toscana.it* va ovviamente preferito il secondo nome)
3. non deve contenere il nome specifico dell'applicativo (a meno che non si tratti esso stesso di un nome generico), riferimenti al produttore, riferimenti a marchi registrati, brand, produttori di software applicativo o di sistema (ad esempio è da evitare il nome *logistica-win2000.estar.toscana.it*)
4. essere il più possibile corto e non generare ambiguità: si pensi a un'eventuale dettatura al telefono di un URL
5. se possibile non deve contenere numeri.

Il procedimento migliore per l'assegnazione di un nome comprenderà una fase in cui esso viene concordato con i responsabili (non ICT) del servizio applicativo offerto, che dovranno tenere conto comunque dei criteri appena stabiliti.

Si fa riferimento al paragrafo 10in merito alla necessità di aggiornare il catalogo anche specificando i nomi degli host e gli eventuali alias relativi ai servizi.

Nota: Nel caso in cui uno host tra le tipologie elencate in tabella abbia natura *transitoria* o comunque *temporanea* è opportuno che l'identificativo numerico assegnato corrisponda a un range stabilito a priori che ne individui convenzionalmente tale caratteristica: si stabilisce dunque che *gli host con identificativo numerico tra 71 e 99 sono da considerarsi transitori*.

Esposizione

A valle della positività dell'esame tecnico, e dopo che il servizio è stato registrato nel corretto dominio, si passa alla sua esposizione su InterSST.

Come regola generale, InterSST è nativamente aperta verso se stessa, cioè ogni sottorete aziendale di indirizzi InterSST non ha chiusure verso le altre sottoreti InterSST.

Deroghe a questa regola, applicabili e gestibili tramite i firewall aziendali da parte di chi eroga il servizio, possono essere:

- **Restrittive** : l'accesso ad alcuni servizi esposti su InterSST può essere limitato ad alcuni soggetti InterSST.

- **Estensive** : l'accesso ad alcuni servizi esposti su InterSST può essere esteso ad altri soggetti non InterSST. Questo è possibile solo se i soggetti esterni alla InterSST si affacciano sulla rete RTRT3. Potrebbe essere il caso di alcuni Comuni, o altri Enti pubblici che hanno necessità di accedere a servizi erogati in ambito Sanitario.

Le suddette deroghe fanno parte integrante della richiesta di esposizione del servizio, e la richiesta di deroga deve essere motivata con adeguata documentazione che ne giustifichi l'effettiva necessità per ragioni tecniche o legali: in entrambi i casi la documentazione suddetta dev'essere allegata alla richiesta e ne costituisce parte integrante.

La configurazione del servizio sarà effettuata da personale tecnico ICT di ESTAR:

direttamente: attraverso opportuna configurazione dei firewall del soggetto SST interessato

indirettamente: attraverso la richiesta alla ditta che ha in gestione i firewall del soggetto SST interessato

Catalogo

Una volta che un servizio viene esposto in InterSST, andrà ad integrare il Catalogo InterSST, che conterrà per ogni servizio le seguenti informazioni:

a) Nome del Servizio
b) Ente di provenienza (uno dei 21 soggetti InterSST)
c) Indirizzo IP sorgente e porta/e IP utilizzate
d) Indirizzo IP o URL su cui è stato esposto il servizio e porta/e IP utilizzate, indicando eventuali traslazioni e conversioni
e) nome DNS a cui fa riferimento al servizio: in caso si tratti di un alias indicare anche il nome primario a cui si riferisce
f) Ente richiedente l'esposizione (uno dei 10 soggetti SST)
g) Breve descrizione del servizio
h) Fornitore del Servizio (ditta o struttura interna)
i) Deroghe sulla accessibilità del servizio esposto.

Nessuna deroga significa che il servizio esposto è accessibile da parte di tutti e 21 i soggetti InterSST. In altro caso, si indicherà la lista dei soggetti oggetto di restrizione / estensione

Schema sintetico del flusso dell'iter

Nella figura successiva si è schematizzato l'iter della richiesta di esposizione di un servizio su InterSST: