REGIONE TOSCANA

Giunta Regionale

TIX

Tuscany Internet eXchange

REGOLAMENTO DI UTILIZZO DEL TIX

PER GLI ISP ACCREDITATI

Tuscany Internet eXchange

1 Premesse

1.1 La Rete Telematica Regionale Toscana

La Toscana, nell'ambito del rapporto tra innovazione tecnologica e pubblica amministrazione, si caratterizza per l'esistenza di una rete di Enti Locali, la Rete Telematica Regionale Toscana (RTRT), che dal 1996, in piena autonomia, si sono aggregati e hanno dato vita a una comunità.

La Rete Telematica Regionale Toscana ha ottenuto il suo riconoscimento giuridico con la L.R. 26 Gennaio 2004 n. 1 che, con successive modifiche, costituisce la RTRT come articolazione regionale del Sistema Pubblico di Connettività (così come definito nel Decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni).

Il Sistema Pubblico di Connettività è l'insieme di strutture organizzative, infrastrutture tecnologiche e di regole tecniche, per lo sviluppo, la condivisione, l'integrazione e la circolarità del patrimonio informativo della Pubblica Amministrazione.
L'infrastruttura RTRT ed il TIX costituiscono il livello di trasporto del SPC della Toscana. L'infrastruttura di Telecomunicazione della RTRT e' articolata in:

1. Infrastruttura RTRT primaria (realizzata e gestita da un fornitore selezionato mediante procedimento di gara pubblica)
2. Infrastruttura RTRT estesa (realizzato da una pluralità di fornitori di trasporto accreditati mediante bando pubblico).
3. Tuscany Internet eXchange (TIX) nei suoi molteplici ruoli di: Internet eXchange Point tra la rete pubblica toscana e le reti degli operatori privati; Centro servizi della RTRT; Centro operativo per la sicurezza della RTRT; Centro di monitoraggio ed helpdesk della RTRT

La Rete Telematica Regionale Toscana è pertanto una infrastruttura di telecomunicazione multi-fornitore, ramificata sul territorio regionale che interconnette tra loro i soggetti aderenti (Enti locali, Università, Uffici delle Amministrazioni centrali sul territorio regionale, Aziende sanitarie, Aziende di promozione turistica e altri Enti connessi direttamente o nell'ambito delle Reti civiche), distribuendo servizi comuni quali l'accesso a banche dati regionali, al Sistema Pubblico di connettività nazionale ed ad Internet.

Ad oggi sono oltre 300 i soggetti che aderiscono al modello di governance di questa Community Network, e che usufruiscono dei servizi condivisi forniti tramite le numerose infrastrutture tecnologiche di RTRT.

1.2 Costituzione e scopo del TIX

Per sommare i benefici derivanti dal disporre di una rete della pubblica amministrazione fortemente interconnessa a quelli di una copertura territoriale totale di servizi di qualità garantita e controllata per tutta la popolazione servita da ISP accreditati, é istituito un Neutral Access Point (NAP) Toscano (il Tuscany Internet eXchange, **TIX**).
Un punto neutrale di interconnessione commuta i traffici IP degli ISP ad esso connessi, tramite opportune politiche di routing con lo scopo di migliorare l'interconnessione tra gli ISP medesimi.

Il TIX consente l'interconnessione "diretta" tra gli OPC (Operatori Pubblici di Connettività) del territorio, permettendo un'economia nel costo del traffico, e garantisce ai soggetti aderenti di poter disporre di un nodo cruciale del Sistema Pubblico di Connettività a livello regionale. Il TIX costituisce inoltre il supporto tecnico al "Centro di Competenza" chiamato a garantire il rispetto dei livelli di qualità di connettività della PA, stabiliti dalla Regione Toscana nel quadro del sistema nazionale.

La funzione del TIX é quella di punto di interconnessione fra la rete telematica regionale toscana (RTRT) e le reti di accesso ad Internet degli operatori privati (ISP) sul territorio toscano.

1.3 Definizioni

RTRT estesa: Rete Telematica Regionale Toscana estesa; l'insieme dei soggetti aderenti ad RTRT e degli enti pubblici che utilizzeranno servizi di connettivitá degli operatori privati accreditati si chiamerá nel seguito 'RTRT estesa'.

Utente finale: soggetto appartenenti alla RTRT estesa.

1.4 Soggetti afferenti

Sono ammessi al collegamento sul TIX tutti gli Internet Service Provider idonei all'accreditamento che forniscono, o vogliano fornire, servizi di connettivitá sul territorio toscano.

1.5 Scopo di questo documento

Lo scopo del presente documento è di regolamentare gli obblighi e le responsabilità che vincolano reciprocamente il TIX e i soggetti che vi afferiscono, con particolare riferimento ai vincoli tecnici e al comportamento nella sede del TIX.

2 Gestione del TIX

2.1 Gestione tecnica

Il gestore del TIX ha il compito di amministrare i locali, di fornire un servizio di Help Desk, di sorvegliare il corretto svolgersi delle attività presso la sede del TIX.

La realizzazione del TIX e la relativa conduzione è affidata per 3 anni al Consorzio HyperTIX, costituito da *CDC S.p.A., Almaviva TFS S.p.A., TD Group S.p.A.*

2.2 Direzione

All'interno del Consorzio cui è demandata la conduzione del TIX è individuato un Responsabile del TIX che sovraintende la gestione giornaliera e le attività delle strutture operative; egli risponde direttamente a Regione Toscana della delivery dei servizi di gestione nei confronti degli utenti.

3 Obblighi dei partecipanti

I soggetti ammessi al TIX si impegnano ad attenersi ai punti seguenti.

3.1 Peering

Ciascuno dei soggetti ammessi deve fare peering in modo gratuito con l'Autonomous System AS6882 di Regione Toscana. Esso si impegna inoltre a sviluppare politiche di peering all'interno del TIX atte a favorire il migliore sviluppo possibile dell'infrastruttura del territorio toscano.

3.2 Amministrazione dei router nella rete TIX

Ciascuno dei soggetti afferenti al TIX curerà la configurazione, la manutenzione, e l'aggiornamento del router di sua proprietà garantendo che questo possa operare nella rete del TIX come descritto al punto. 4.7 del presente regolamento.

3.3 Riservatezza

Ciascuno degli soggetti ammessi si impegna a non divulgare in nessuna forma pubblica dati ed informazioni del TIX e degli altri soggetti accreditati di cui venisse a conoscenza; si impegna inoltre a non diffondere dati parziali sulle statistiche ufficiali del TIX a meno di specifici accordi con Regione Toscana.

3.4 Banda nominale

Ciascuno dei soggetti ammessi al TIX dovrà certificare, mediante apposita relazione tecnica da allegare alla domanda di accreditamento eventualmente supportata da contratti di fornitura con soggetti –anche terzi- che forniscono servizi di trasporto dati verso il TIX, la qualità e la banda nominale con cui vorrà collegarsi.

3.5 Condivisione delle risorse

L'utilizzo delle risorse del TIX da parte di ciascuno dei soggetti ammessi al TIX non può andare a scapito dell'utilizzo da parte degli altri partecipanti al TIX.

3.6 Responsabilità in caso di danno civile o penale

Ciascuno dei soggetti ammessi al TIX esplicitamente solleva la Regione Toscana da qualsiasi danno civile o penale dovuto all'utilizzo del servizio del TIX.

3.7 Assicurazione degli apparati

Gli apparati di proprietà del soggetto ammesso al TIX devono essere coperti da apposita polizza assicurativa contro furto, incendio e danni a terzi. L'installazione degli apparati sarà autorizzata solo dietro deposito di copia del contratto di copertura assicurativa presso il responsabile del TIX.

4 Obblighi del TIX

Il TIX si impegna ad attenersi alle condizioni riportate nei seguenti punti.

4.1 Pubblicazione confidenziale dei dati di traffico

Pubblicazione periodica dei dati relativi al traffico, resi accessibili ai soli soggetti direttamente interessati.

4.2 Aggiornamento delle informazioni

Mantenere aggiornate tutte le informazioni utili per gli afferenti sul sito http://www.tix.it.

4.3 Supporto ai soggetti ammessi al TIX in fase di installazione degli apparati

Supportare i soggetti ammessi nella fase di installazione degli apparati. Il supporto é garantito ai soggetti ammessi al TIX che rispettano le clausole indicate nelle note tecniche del TIX riportate nell'Art. 4.7.

4.4 Assistenza e accesso alla sala TLC

Fornire assistenza di primo livello agli ISP ammessi e accesso a richiesta degli ISP alla sala TLC del TIX in caso di guasti sui loro apparati nella seguente tempistica:

Servizio	Copertura	Tempo di intervento	Tempo di risoluzione problemi bloccanti[1]	Tempo di risoluzione problemi non bloccanti
Assistenza/Manutenzione sala TLC e NAP	24 x 7	30 minuti	1 ora	1 giorno

4.5 Sorveglianza funzionamento apparati

Mantenere nella migliore efficienza possibile le apparecchiature della LAN del TIX e sorvegliarne il funzionamento, garantendo la copertura del servizio di sorveglianza 24 ore al giorno per 7 giorni alla settimana.

4.6 Interventi di manutenzione infrastruttura TIX

Informare tutti i soggetti ammessi circa le date e le modalità degli interventi di manutenzione ordinaria e straordinaria, rispettando le seguenti tempistiche di preavviso:

- almeno 15 gg. prima l'intervento stesso, per gli interventi di manutenzione ordinaria;
- in modo immediato, per tutti per gli interventi di manutenzione straordinaria.

4.7 Caratteristiche tecnico-logistiche del TIX

Per l'installazione dei propri apparati sulla LAN del TIX, ogni ISP deve tenere in considerazione che il TIX predispone:

- Sala TLC condizionata per spazi rack di tipo standard (600x600 e 800x1000);
- Permutatori in F.O. OM3 e OS1, ed in cavo UTP Cat 6;
- Rack per uso condiviso predisposti con due PDU connesse alle due linee energia AC e raccordo UTP Cat. 6 verso il Permutatore; ad un singolo ISP può essere assegnato al massimo metà rack;

[1] Per problema bloccante si intende un malfunzionamento di sistemi/apparati/cablaggi/linee in seguito al quale gli utenti sono impossibilitati ad usufruire in toto dei servizi forniti. Es.: il malfunzionamento di una LAN presso il TIX.

- Spazio rack destinato a singolo ISP: secondo le necessità rilevabili dal progetto tecnico;
- Alimentazione 220 V AC 50Hz su due linee energia indipendenti dotate entrambe di UPS e gruppo elettrogeno;
- Alimentazione 48V DC su due stazioni energia indipendenti protette entrambe da gruppo elettrogeno;
- Due switch di NAP e due router BGP;
- Porte Ethernet 10/100/1000 Mbit/s;
- Porte GigaEthernet Fibra Ottica Multimode;
- Cablaggio in UTP Cat. 6, in Fibra Ottica OM3 e per casi specifici OS1;
- Due distinte canalizzazioni polifore di accesso per cavi in fibra ottica;
- Traliccio per collegamenti radio punto-punto verso le reti di backbone degli ISP.

Si ricorda che i router degli ISP al TIX devono poter supportare il protocollo BGP ver.4.
E' cura dell'ISP approntare quanto necessita per la connessione dal Router di peering al proprio apparato di frontiera.
Nel caso in cui l'ISP avesse necessità di installare apparecchiature che richiedano maggiori risorse di quanto predisposto, dovrà sostenere le eventuali spese accessorie (armadi, cablaggi, ecc. ...) e comunque dovrà confrontarsi tecnicamente con il gestore tecnico del TIX per collocare gli apparati a norma e secondo quanto previsto da Regione Toscana.
Si invitano gli ISP ad utilizzare l'alimentazione ridondata impiegando apparati dotati di doppia alimentazione oppure installando appositi sistemi quali STS (Static Trasfert Switch), ATS (Automatic Trasfert Switch), RPS (Reduntant Power System).
Allo stesso modo è auspicabile che si colleghino ad entrambi gli switch di NAP.

5 Procedure di gestione e controllo

Ciascun soggetto ammesso al TIX si impegna al rispetto delle seguenti procedure:

5.1 Etichettatura apparati e cablaggi

Ogni apparato/cablaggio, presente nei locali del TIX, deve essere dotato di opportuna etichetta riportante i dati del soggetto proprietario o del gestore del TIX.

5.2 Intervento su materiale di proprietà altrui

Ogni soggetto ammesso al TIX si impegna a non intervenire su apparati di proprietà altrui senza esplicito consenso scritto del proprietario.

5.3 Pubblicazione dei livelli di servizio

Ogni soggetto ammesso al TIX autorizza RT a pubblicare i livelli di servizio monitorati dalla struttura tecnica del TIX e dal soggetto terzo.

5.4 Terminazioni

Su ogni apparato ospitato in sala TLC è consentita la terminazione di collegamenti (ogni collegamento può essere composto da diversi flussi) con non più di due sedi della rete di backbone del soggetto ammesso. La terminazione dedicata o dial-in di collegamenti verso sedi di Clienti finali, direttamente sugli apparati presenti i Sala TLC è comunque vietata: ad esempio, il TIX non può essere usato dagli ISP come nodo di accesso per attestarvi i loro Clienti.

5.5 Traffico ammesso

Il traffico di *peering* a titolo gratuito tra ISP avviene tramite gli switch di NAP. Ogni altro tipo di traffico tra ISP deve avvenire tra collegamenti diretti realizzati con patch UTP/fibra al permutatore di Sala TLC.
Gli ISP transitando tramite il permutatore di Sala TLC, possono fornire collegamenti diretti agli Enti loro Clienti ospitati nella contigua server farm del TIX.

5.6 Registrazione politiche di routing

Ogni soggetto ammesso deve registrare, in anticipo, le proprie politiche di routing e i 'route object' presso il routing registry RIPE NCC. Tali dati devono essere conformi alle direttive RIPE-181 o future raccomandazioni dell'IETF.

5.7 Protocollo di peering

Il protocollo utilizzato per il peering tra i partecipanti al TIX è il BGP versione 4. Ogni soggetto ammesso si impegna a propagare informazione di routing ottimizzate, in particolare riducendo al minimo 'route flaps' e evitando annunci specifici. A tal fine è fortemente scoraggiata la propagazione di informazioni di routing con prefissi maggiori di 24 bit.

5.8 Rappresentante tecnico e amministrativo

Ogni soggetto ammesso deve comunicare i nominativi di un proprio rappresentate tecnico ed uno amministrativo. Tali rappresentati vengono inclusi nella mail-list del TIX. Questa mail-list e, più in generale, la posta elettronica è lo strumento ufficiale di comunicazione tra i clienti e il TIX. Tali comunicazioni sono da ritenersi confidenziali e non devono essere rese note a persone fisiche o giuridiche al di fuori del TIX. In particolare l'afferente dovrà comunicare un recapito telefonico di emergenza per eventuali malfunzionamenti.

6 Specifiche tecniche per la connessione alla LAN di Peering

1. Possono installare apparati ed infrastrutture presso il TIX solo ISP accreditati.
2. Non é consentito ad ISP accreditati al TIX inserire nell'area NAP apparati che non siano propri
3. I carrier utilizzabili al TIX devono essere ISP accreditati.

6.1 Norme di Livello 2

1. Sulla LAN di peering TIX sono permesse trame Ethernet basate sullo standard Ethernet II (802.3) o 'DIX Ethernet. L'incapsulamento LLC/SNAP non è permesso

2. A livello di pacchetti Ethernet sono ammessi i seguenti Ethertypes:
   - 0x0800 IPv4
   - 0x0806 ARP
   - 0x86dd IPv6

3. Le trame indirizzate verso una porta degli switch del TIX hanno esclusivamente gli indirizzi MAC sorgenti autorizzati a transitare su quella porta.

4. Le interfacce dei router collegate agli switch del TIX non possono essere configurate all'uso del proxy ARP.

6.2 Norme di Livello 3

1. Le apparecchiature di peering non hanno protocolli IGP attivi (come OSPF, ISIS, IGRP, EIGRP, RIP) verso la LAN del TIX.

7 Traffico indesiderato sulla LAN di Peering

7.1 Spanning Tree (STP)

Non vi è alcuna ragione per cui i dispositivi direttamente connessi a TIX siano visibili dagli switch di TIX come apparati attivi di Livello 2: quindi non vi è alcuna necessità di mantenere attivi verso TIX protocolli di controllo della tipologia L2 come Spanning Tree o simili.

7.2 Protocolli di Routing Interno di Livello Tre

Il traffico generato da protocolli di routing interno quali RIP, OSPF, EIGRP, IGRP o ISIS sia unicast che multicast non ha ragione di essere veicolato sulla LAN condivisa di TIX. L'unico protocollo di routing ammissibile su TIX è EBGP.

7.3 Proxy ARP

Essendo il traffico scambiato su TIX sotto il controllo esclusivo del protocollo BGP-4 non c'è alcuna ragione per uno qualsiasi dei router connessi alla LAN di Peering TIX di rendere disponibili funzionalità di Proxy ARP sulle LAN di peering. Purtroppo queste funzionalità sono spesso abilitate di default sulle porte Ethernet da parte di molti vendor. L'abilitazione di questa funzione non ha solo impatti negativi per l'Exchange Point ma sicuramente anche direttamente sulla rete dell'afferente che lo abilita, quindi è fondamentale il controllo che per nessun motivo il proxy ARP sia attivo sulle porte di Peering.

7.4 IPv6 ND-RA

I router advertisement IPv6 non sono permessi sulle LAN di peering: essi generano molto traffico non necessario in quanto in sostanza non esiste un default router IPv6 sulla LAN di TIX

Appendice A al Regolamento di utilizzo del T.I.X. per ISP accreditati

Caratteristiche della VPN IPSEC e del concentratore

VPN IPSEC

- La funzionalità IPSec in una prima fase sarà erogata mediate l'utilizzo di pre-shared key per poi passare alla gestione tramite certificati digitali;
- Il gestore del TIX fornirà il dettaglio della modalità di configurazione, gestione e trasmissione delle pre-shared key agli ISP accreditati;
- Il formato delle richieste di certificato dovrà essere conforme allo standard PKCS#10;
- I dispositivi utilizzati come end-point dovranno garantire il supporto del protocollo ESP con algoritmo di cifratura 3DES ed il supporto del protocollo AH con algoritmo SHA-1;
- Dovrà essere garantito il supporto del protocollo IKE con certificati X.509v3;
- Dovrà essere garantito il supporto di liste di revoca conforme allo standard CRL v2 (RFC 2459) o il supporto del protocollo OCSP;
- I dispositivi utilizzati come end-point dovranno implementare la funzione anty-replay;
- Deve essere garantita la compatibilità con gli standard RFC-1825, 1826, 1827, 1828, 1829 e successivi aggiornamenti;
- Deve essere fornito il supporto per IPSec Tunnel Mode;
- I dispositivi utilizzati dovranno garantire di trattare traffico cifrato senza apportare un degrado significativo delle prestazioni complessive.

CONCENTRATORE

Presso il TIX è installata una coppia di concentratori Cisco System modello 3030 in VRRP; di seguito vengono riportate alcune delle caratteristiche dell'apparato relative alle varie modalità di connessione:

- Compatibilità software client:
    14. Cisco VPN Client (IPsec) per Windows 95, 98, ME, NT 4.0 e Windows 2000 (incluso il controllo centralizzato di tunneling suddiviso e la compressione dati),
    15. Cisco VPN 3002 Hardware Client,
    16. Microsoft PPTP/MPPE/MPPC,
    17. Microsoft L2TP/IPsec per Windows 2000
    18. MovianVPN (Certicom) Handheld VPN Client con ECC;

- Protocolli di Tunneling supportati sono:
    20. PPTP (Point-to-Point Tunneling Protocol) con crittografia;
    21. L2TP (Layer 2 Tunneling Protocol);
    22. Protocollo IPSec (IP Security);
    23. Client-to-LAN, usando il VPN Client o altri client compatibili con il protocollo IPSec;

24. LAN-to-LAN, tra pari VPN Concentrators o tra un VPN Concentrator ed un altro gateway sicuro, compatibile con il protocollo IPSec, ivi compresi router Cisco System equipaggiati con IPSec;
25. L2TP su IPSec (per la compatibilità con il client Windows 2000);
26. NAT Transparent Ipsec;

- Algoritmi di cifratura supportati sono:
    28. ESP (Encapsulating Security Payload),
    29. IPsec con DES/3DES (56/168 bit) con MD5 o SHA,
    30. MPPE con 40/128 bit RC4;

- Algoritmi di autenticazione supportati sono:
    32. MD5 (Message Digest 5);
    33. SHA-1 (Secure Hash Algorithm);
    34. HMAC (Hashed Message Authentication Coding) con MD5;
    35. HMAC con SHA-1;

- Key Management supportate sono le Internet Key Exchange (IKE), formalmente chiamate ISAKMP/Oakley, con la tecnica di chiave Diffie-Hellman;

- Certificate Authorities Supportati sono:
    38. Baltimore;
    39. CyberTrust;
    40. Entrust;
    41. Microsoft Windows 2000;
    42. RSA Keon;

- Compatibilità con terze parti:
    44. iPass Ready,
    45. certificato Funk Steel Belted RADIUS,
    46. NTS TunnelBuilder VPN Client (Mac e Windows),
    47. Microsoft Internet Explorer,
    48. Netscape Communicator,
    49. Entrust,
    50. GTE Cybertrust,
    51. Baltimore,
    52. RSA Keon,
    53. Network Associates PGP VPN.

Si ricorda inoltre che è possibile la creazione di tunnel IPSec anche utilizzando come end-point un router con indirizzo IP pubblico assegnato dinamicamente (tipicamente, una connessione dialup verso un ISP).