

***REGOLAMENTO DI UTILIZZO DEL TIX
PER GLI ISP ACCREDITATI -***

Tuscany Internet eXchange

1	PREMESSE.....	3
1.1	LA RETE TELEMATICA REGIONALE TOSCANA.....	3
1.2	COSTITUZIONE E SCOPO DEL TIX.....	3
1.3	DEFINIZIONI.....	3
1.4	SOGGETTI AFFERENTI.....	3
1.5	SCOPO DI QUESTO DOCUMENTO.....	3
2	GESTIONE DEL TIX	3
2.1	GESTIONE TECNICA	3
2.2	DIREZIONE.....	4
3	OBBLIGHI DEI PARTECIPANTI.....	4
3.1	PEERING.....	4
3.2	AMMINISTRAZIONE DEI ROUTER NELLA RETE TIX.....	4
3.3	RISERVATEZZA.....	4
3.4	BANDA NOMINALE.....	4
3.5	CONDIVISIONE DELLE RISORSE	4
3.6	RESPONSABILITÀ IN CASO DI DANNO CIVILE O PENALE	4
3.7	ASSICURAZIONE DEGLI APPARATI.....	4
4	OBBLIGHI DEL TIX.....	4
4.1	PUBBLICAZIONE CONFIDENZIALE DEI DATI DI TRAFFICO.....	5
4.2	AGGIORNAMENTO DELLE INFORMAZIONI	5
4.3	SUPPORTO AI SOGGETTI AMMESSI AL TIX IN FASE DI INSTALLAZIONE DEGLI APPARATI.....	5
4.4	ASSISTENZA E ACCESSO ALLA SALA DATI.....	5
4.5	SORVEGLIANZA FUNZIONAMENTO APPARATI.....	5
4.6	INTERVENTI DI MANUTENZIONE INFRASTRUTTURA TIX	5
4.7	CARATTERISTICHE TECNICO-LOGISTICHE DEL TIX.....	5
5	PROCEDURE DI GESTIONE E CONTROLLO	6
5.1	ETICETTATURA APPARATI E CABLAGGI	6
5.2	INTERVENTO SU MATERIALE DI PROPRIETÀ ALTRUI.....	6
5.3	PUBBLICAZIONE DEI LIVELLI DI SERVIZIO.....	6
5.4	TERMINAZIONI	6
5.5	REGISTRAZIONE POLITICHE DI ROUTING.....	6
5.6	PROTOCOLLO DI PEERING.....	6
5.7	RAPPRESENTANTE TECNICO E AMMINISTRATIVO.....	6
	APPENDICE A AL REGOLAMENTO DI UTILIZZO DEL T.I.X. PER ISP ACCREDITATI	7
	<u>CARATTERISTICHE DELLA VPN IPSEC E DEL CONCENTRATORE.....</u>	<u>7</u>

1 Premesse

1.1 *La Rete Telematica Regionale Toscana*

La Rete Telematica Regionale Toscana (RTRT) è una infrastruttura di telecomunicazione 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, alla Pubblica Amministrazione Centrale, ad Internet.

La Rete Telematica Regionale Toscana si basa su un modello integrato di governo e gestione che impegna pariteticamente le varie Amministrazioni, favorendo lo svolgimento dei ruoli istituzionali specifici. Tale modello è definito nel Piano di indirizzo approvato dal Consiglio regionale l. 21 maggio 1997 e dalla delibera attuativa della Giunta regionale n.376 del 20 aprile 1998. Negli anni 1998 e 1999 il modello si è venuto a realizzare compiutamente, con la attivazione degli organi (Direzione strategica, Direzione operativa, Direzione tecnica) e degli strumenti di progettazione comuni (Piano annuale delle attività della Rete).

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, è 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.

La funzione del TIX è 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 connettività degli operatori privati accreditati si chiamerà 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 vogliono fornire, servizi di connettività 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 5 anni ad un Raggruppamento Temporaneo d'Impresa, costituito da *Telecom Italia S.p.A.*, *Getronics Solutions S.p.A.*, *Brain Technology S.p.A.*

2.2 Direzione

All'interno del R.T.I. cui è demandata la conduzione del TIX è individuato un Responsabile del TIX che sovrintende 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 su un apposito WEB.

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 dati

Fornire assistenza di primo livello agli ISP ammessi e accesso a richiesta degli ISP alla sala dati 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 Data Center 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 predisponde:

- Rack di tipo standard (600x800 precablati in F.O. e in cavo UTP Cat 6 verso gli Switch)
- Spazio rack destinato a singolo ISP: 6 unità rack
- Alimentazione 220 V 50Hz
- Porte Ethernet 10/100/1000 Mb
- Porte GigaEthernet Fibra Ottica Multimode
- Cablaggio UTP di tipo 6
- Cablaggi su Fibra Ottica
- UPS
- Accessibilità per impianti radio LAN.

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.

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.

Nel caso in cui l'ISP avesse necessità di installare apparecchiature che occupino più di 6 unità rack, quest'ultimo 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.

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 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 soggetti direttamente sugli apparati presenti nella sede del TIX è comunque vietata.

5.5 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.

5.6 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.

5.7 Rappresentante tecnico e amministrativo

Ogni soggetto ammesso deve comunicare i nominativi di un proprio rappresentante tecnico ed uno amministrativo. Tali rappresentanti 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.

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

Caratteristiche della VPN IPSEC e del concentratore

VPN IPSEC

- (a) La funzionalità IPsec in una prima fase sarà erogata mediante l'utilizzo di pre-shared key per poi passare alla gestione tramite certificati digitali;
- (b) Il gestore del TIX fornirà il dettaglio della modalità di configurazione, gestione e trasmissione delle pre-shared key agli ISP accreditati;
- (c) Il formato delle richieste di certificato dovrà essere conforme allo standard PKCS#10;
- (d) 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;
- (e) Dovrà essere garantito il supporto del protocollo IKE con certificati X.509v3;
- (f) Dovrà essere garantito il supporto di liste di revoca conforme allo standard CRL v2 (RFC 2459) o il supporto del protocollo OCSP;
- (g) I dispositivi utilizzati come end-point dovranno implementare la funzione anti-replay;
- (h) Deve essere garantita la compatibilità con gli standard RFC-1825, 1826, 1827, 1828, 1829 e successivi aggiornamenti;
- (i) Deve essere fornito il supporto per IPsec Tunnel Mode;
- (j) 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:
 - 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),
 - Cisco VPN 3002 Hardware Client,
 - Microsoft PPTP/MPPE/MPPC,
 - Microsoft L2TP/IPsec per Windows 2000
 - MovianVPN (Certicom) Handheld VPN Client con ECC;
- Protocolli di Tunneling supportati sono:
 - PPTP (Point-to-Point Tunneling Protocol) con crittografia;
 - L2TP (Layer 2 Tunneling Protocol);
 - Protocollo IPsec (IP Security);
 - Client-to-LAN, usando il VPN Client o altri client compatibili con il protocollo IPsec;

- 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;
- L2TP su IPsec (per la compatibilità con il client Windows 2000);
- NAT Transparent Ipsec;
- Algoritmi di cifratura supportati sono:
 - ESP (Encapsulating Security Payload),
 - IPsec con DES/3DES (56/168 bit) con MD5 o SHA,
 - MPPE con 40/128 bit RC4;
- Algoritmi di autenticazione supportati sono:
 - MD5 (Message Digest 5);
 - SHA-1 (Secure Hash Algorithm);
 - HMAC (Hashed Message Authentication Coding) con MD5;
 - 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:
 - Baltimore;
 - CyberTrust;
 - Entrust;
 - Microsoft Windows 2000;
 - RSA Keon;
- Compatibilità con terze parti:
 - iPass Ready,
 - certificato Funk Steel Belted RADIUS,
 - NTS TunnelBuilder VPN Client (Mac e Windows),
 - Microsoft Internet Explorer,
 - Netscape Communicator,
 - Entrust,
 - GTE Cybertrust,
 - Baltimore,
 - RSA Keon,
 - 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).