TITOLO DOCUMENTO:	**Descrizione Servizio di MObileSTrong Authentication – MOST**
TIPO DOCUMENTO:	**Descrizione del Servizio**
EMESSO DA:	**TI Trust Technologies S.r.l.**
DATA EMISSIONE:	**03/01/2014**
N. ALLEGATI:	**0**
STATO:	**Rilasciato**

REDATTO:	**E. Grechi, G. Tovo**	**TI.TT**
VERIFICATO:	**G. Allegrezza, E. Cavallo, M. Donatone**	**TI.TT**
APPROVATO:	**C. Villani**	**TI.TT**
LISTA DI DISTRIBUZIONE:	**TI Trust Technologies srl, Telecom Italia**	**TI.TT**

REGISTRO DELLE MODIFICHE		
REVISIONE	**DESCRIZIONE**	**EMISSIONE**
00	Redazione	19/01/2010
01	Spostata scheda d'attivazione come allegato esterno	19/10/2010
02	Aggiornamento generale	25/10/2011
03	Revisione elementi di servizio	30/01/2012
04	Aggiunto paragrafo Architettura Logica e capitolo Sicurezza Fisica Centro Servizi Certification Authority	12/09/2012
05	Cambio denominazione sociale	03/01/2014

Sommario

1 Scopo del documento

Questo documento descrive le caratteristiche del servizo di *MObile STrong authentication* o **MOST**.

Sono descritte anche le caratteristiche dei servizi accessori di **Mobile SMS** e **Mobile INFO** nonché le possibili estensioni di servizio che possono essere attivati a complemento delle procedure definite dal cliente e nei servizi custom.

Tali servizi vengono erogati utilizzando la piattaforma di servizio gestita da Telecom Italia Trust Technologies (TI.TT).

2 Definizioni

Nell'ambito del documento saranno utilizzati gli acronimi e le definizioni riportate nel seguito.

CA	Autorità di Certificazione: prestatore di servizi di certificazione, la società TI.TT
CED	Centro di Elaborazione Dati
MOST	MObile STrong authentication
OPT	One Time Password
PIN	Codice personale di accesso alle chiavi custodite su HSM dispositivi sicuri di firma
PRI	Il *Primary Rate Interface*, l'interfaccia standard di telecomunicazioni per veicolare trasmissioni multiple DS0 in voce e dati tra la rete e un utilizzatore.
PSTN	*Public Switched Telephone Network*. Rete telefonica analogica. La normale rete telefonica per le trasmissioni vocali. Può essere utilizzata per l'invio di dati tramite router (o modem). Talvolta è chiamata anche POTS.
SIM	Subscriber Identity Module
SLA	Service Level Agreement
TI	Telecom Italia S.p.A.
TI.TT	TI Trust Technologies S.r.l.
TTS	Sistemi di sintesi vocale sono noti anche come sistemi Text-To-Speech
VPN	Virtual Private Network

3 Riferimenti

[1] 2006-00161 – Accesso ai Data Center Telecom Italia

[2] SOPPO06002-A – Accesso ai siti Telecom Italia S.p.A.

4 Introduzione

L'utilizzo di metodi di autenticazione tradizionale basati su "nome utente e password" nell'ambito dei servizi on-line, se utilizzati tanto in fase di "accesso al portale" che in fase di "conferma dispositiva" oggi non è più in grado di fornire sufficienti requisiti di sicurezza.

E' nata quindi negli ultimi anni l'esigenza di sviluppare sistemi tanto di "certificazione dell'identità" dell'utente del servizio che di "certificazione della volontà di effettuare un'operazione dispositiva" in grado di elevare il profilo di sicurezza. Questi sistemi sono definiti metodi di *Strong Authentication*, che aumentano la resistenza verso i più diffusi attacchi informatici e il furto di identità.

In particolare, tra le tecniche di Strong Authentication emerge quella a "canale complementare", nella quale l'utente agisce sfruttando un *canale di comunicazione differente* rispetto a quello di originale fruizione del servizio.

La rete telefonica mobile si presta a essere utilizzata in questo ambito, poiché in essa i parametri di sicurezza e il metodo di autenticazione dell'utente sono particolari.

TI.TT implementa la Strong Authentication del servizio MOST sul canale complementare di telefonia mobile.

La soluzione proposta garantisce i seguenti vantaggi:

- non è necessario dotare gli utenti di smart card, token o dispositivi hardware aggiuntivi oltre al cellulare del quale già dispongono. Ne consegue, per il cliente, un notevole vantaggio in termini riduzione del costo e del tempo necessari per lo sviluppo e diffusione del servizio.
- l'utente, nella fase di conferma dispositiva, non deve sostenere alcun costo telefonico.
- non c'è nessun limite imposto dalla tecnologia, visto che *praticamente tutti i potenziali utenti già dispongono di almeno un telefono cellulare*.

E' importante precisare che vengono autorizzate dalla Rete Telecom Italia solo chiamate originate nelle Reti degli Operatori Mobili nazionali dai numeri telefonici che iniziano con "+393".

5 Descrizione dei Servizi

Di seguito si forniscono dettagli sui tre servizi MOST, Mobile SMS e Mobile INFO.

5.1 Servizio MOST

La piattaforma applicativa utilizzata da TI.TT consente di implementare un sistema di strong authentication su canale secondario (la rete telefonica mobile) e dove il meccanismo di sicurezza è il *riconoscimento del numero chiamante dell'utente*.

In questo modo non è richiesto nessun token o dispositivo generatore di chiavi addizionale: l'utente può usare direttamente il proprio cellulare e senza necessità di installare in esso alcuna applicazione.

Per utilizzare il servizio MOST il cliente deve integrare il proprio servizio applicativo (es. portale web) con la piattaforma di erogazione di TI.TT tramite l'apposita interfaccia applicativa basata su tecnologia Web Service.

Il servizio MOST funziona come qui descritto (lo schema seguente ne illustra il meccanismo):

L'utente in genere compie una prima autenticazione al servizio che sta utilizzando mediante la classica coppia di dati Username e Password. Al momento di eseguire la strong authentication, il sistema del cliente esegue una richiesta al servizio MOST che restituisce un codice OTP numerico.

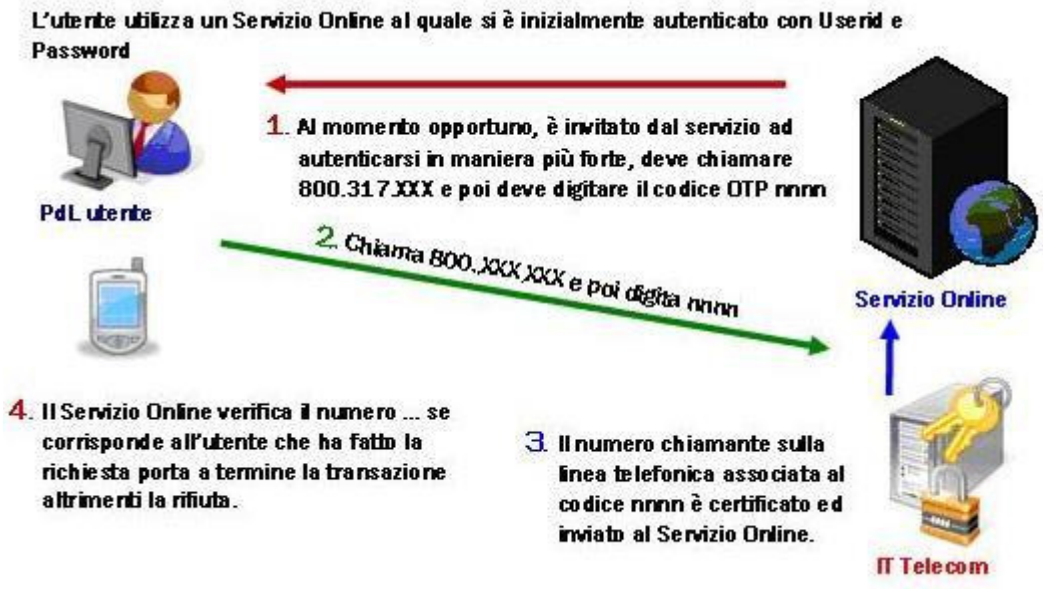
Il servizio del cliente chiede all'utente di effettuare una chiamata dal suo telefono cellulare al **numero verde** del servizio MOST e di digitare in post-selezione le **quattro** cifre numeriche del codice OTP che è stato generato per la specifica occasione.

Al codice OTP risulta associata in TI.TT una determinata linea della rete telefonica fissa alla quale sono collegati i sistemi della piattaforma del servizio MOST. Il servizio rileva il numero chiamante sulla linea e lo restituisce al servizio del cliente. TI.TT dispone di migliaia di linee telefoniche che utilizza per il servizio MOST.

Il sistema del cliente verifica la coincidenza del numero chiamante restituito dal servizio MOST con il numero del telefono cellulare memorizzato nel proprio database per l'utente che sta eseguendo l'operazione che ha richiesto l'autenticazione. In caso di esito positivo, esso concede l'autorizzazione altrimenti no.

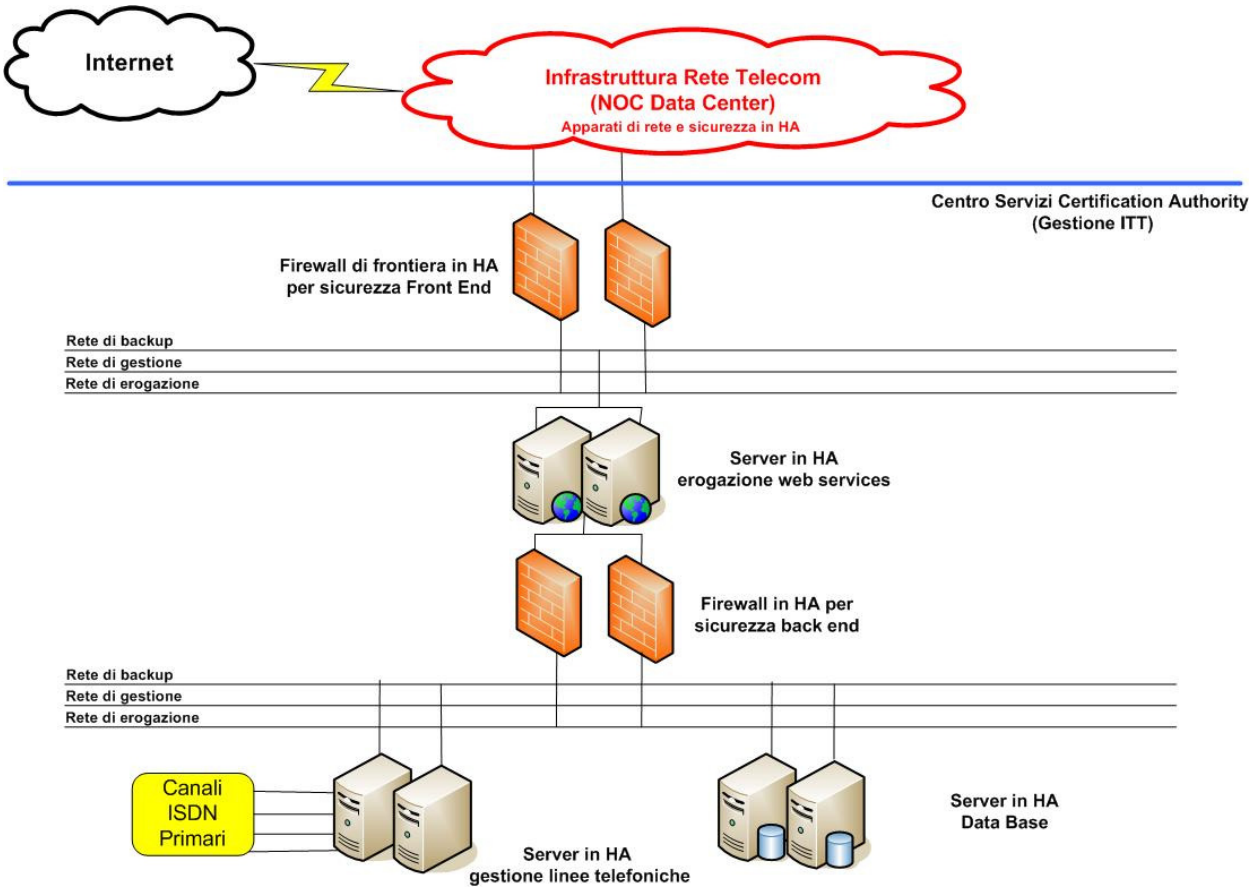
Il **numero telefonico chiamante** identifica l'utente, mentre il **codice OTP** che segue il numero verde identifica l'operazione dispositiva specifica.

Lo schema seguente descrive la chiamata con OTP.



5.2 Architettura Logica del servizio MOST

Nella figura seguente si evidenziano le componenti principali coinvolte nell'architettura del servizio MOST.



Dallo schema si evince che ogni singola componente è in configurazione di alta affidabilità oltre ad essere in costante monitoraggio sui sistemi dedicati di TI.TT.

La Componente di Back End è inserita nella zona più protetta della rete del Certificatore TI Trust Technologies e non viene esposta all'esterno (ossia non è per nessuna ragione raggiungibile direttamente da Internet o comunque da connessioni esterne all'infrastruttura del Certificatore), fornisce le funzionalità fondamentali della PKI e dei servizi del Certificatore. La componente di Back End è protetta da un FW (FW BE).

La Componente di Front End è l'unica componente preposta all'esposizione dei servizi e relativi dati verso Internet/Intranet. A tal fine è autorizzata a colloquiare, con opportuni sistemi di sicurezza e controllo, con la componente di Back-End. La componente di Front End è protetta da un FW (FW FE).

La Rete di Management permette agli operatori di raggiungere i sistemi posti sulle reti di Front End e Back End per le attività di conduzione sistemi. Tale rete è posta all'interno della Sala Sistemi del Centro Servizi del Certificatore e non è raggiungibile dall'esterno.

La Rete di backup garantisce il corretto servizio di salvataggio ed archiviazione dei dati. A tale rete è attestato il **sistema di Archiviazione Dati** in cui sono conservati i log di accesso a tutti i sistemi attestati sia alla rete di front end che a quella di back end.

Completano l'architettura sistemi di **IDS** (Intrusion Detection System) che identificano accessi non autorizzati ai computer o alle reti locali e sistemi di monitoraggio a vari livelli.

5.3 Varianti di Servizio

Il servizio MOST, nella sua versione **standard**, prevede il metodo di autenticazione descritto in precedenza.

Nella realizzazione di servizi personalizzati in progetti custom la piattaforma gestita da TI.TT offre diverse varianti del servizio con *opzioni di autenticazione forte* che possono essere adottate singolarmente oppure congiuntamente, a seconda delle esigenze dei singoli utenti, fra queste si citano almeno le seguenti:

Call con OTP + PIN — Alla risposta, viene richiesto l'inserimento del codice OTP, e dopo viene emesso messaggio vocale (registrato o comunicato attraverso un meccanismo di TTS) che richiede la digitazione di un codice personale PIN.

Call con Callback + PIN — Alla risposta, eseguita la rilevazione del numero chiamante, la telefonata viene abbattuta e il servizio richiama automaticamente il numero di telefono cellulare rilevato. Un messaggio registrato o comunicato attraverso un meccanismo di TTS (statico o dinamico) richiede all'utente la digitazione di un codice personale PIN.

OutgoingCall + PIN — La piattaforma, invece di attendere una chiamata dell'utente, effettua direttamente la chiamata al suo numero di telefono cellulare. Un messaggio registrato o comunicato attraverso un meccanismo di TTS (statico o dinamico) richiede la successiva digitazione di un codice personale PIN.

La configurazione della piattaforma viene realizzata in funzione della tipologia di servizio richiesto dal cliente. E' da notare che alcune modalità comportano un costo aggiuntivo come nel caso della OutgoingCall dove è necessario fatturare al cliente il costo delle chiamate effettuate.
Sempre in opzione, il sistema può inviare all'utente un SMS informativo con i dati riassuntivi dell'operazione appena autorizzata, mediante i servizi aggiuntivi di messaggistica descritti nel seguito.

5.4 Servizio INFO

La piattaforma applicativa gestita da TI.TT è collegata ai servizi di messaggistica SMS di Telecom Italia e può essere utilizzata anche per fornire informazioni personalizzate a un utente che ha chiamato il sistema con il proprio cellulare.

Si può configurare la piattaforma per rispondere alle richieste dell'utente sia mandandogli direttamente un SMS (modalità PULL), sia riproducendo dei messaggi vocali utilizzando la funzionalità TTS.
La tipologia di risposta può essere determinata dalla configurazione effettuata sul numero telefonico chiamante e/o dalla sequenza di tasti digitati dopo che è stata instaurata la connessione in base.

È possibile programmare l'azione del sistema **a seconda del numero telefonico chiamato**, ad es.: chiamare il numero 8001001 potrebbe significare "Voglio sapere lo stato del mio account" mentre chiamare il numero 8001002 potrebbe significare "Ho bisogno di un nuovo PIN temporaneo per la mia scheda", e così via.

Ancora, l'azione può essere diversificata **a seconda dalla sequenza di tasti digitati dopo che è stata instaurata la connessione**, ad es.: 100# potrebbe significare "Richiesta stato Account"; 200# potrebbe significare "Richiesta Password temporanea"; ecc.

I contenuti dei messaggi da trasmettere devono essere forniti dal cliente in modalità gestibili dalla piattaforma (ad esempio in forma di pagina HTML oppure mediante URL che effettuino interrogazioni sul sistema del cliente).

Il servizio Mobile INFO con SMS in genere prevede che il cliente acquisti un proprio canale invio di SMS di Telecom Italia: **InfoTim**.

5.5 Servizio SMS

Il modulo per la gestione degli SMS fornisce alle applicazioni del cliente la capacità di inviare e/o ricevere SMS verso i telefoni mobili tramite una connessione IP senza doversi dotare di apparati proprietari o sistemi hardware particolari (es. apparati GSM, schede SIM e altri sistemi di invio e gestione).

Si tratta di un servizio di invio SMS in modalità PUSH.

Più in dettaglio, il servizio può ricevere il testo che deve essere inviato in numerosi modi differenti, quali:

- invocando appositi Web Service;
- fornendo un URL a una pagina http/https contenente il testo inserito fra speciali 'tag';
- fornendo connessioni a Database dedicati (ADO, JDBC);
- leggendo file testuali inviati via FTP;
- inviando e-mail a un server mail dedicato (SMTP).

6 Collaudo, Attivazione e Gestione

6.1 Attivazione del Servizio

La piattaforma gestita da TI.TT dispone di un **Ambiente di Collaudo** utilizzabile dai clienti nella fase di integrazione del servizio con le proprie applicazioni.

Le attività di sviluppo e integrazione delle applicazioni del cliente col servizio sono in genere di competenza del cliente stesso. Per la configurazione delle applicazioni del cliente all'utilizzo del servizio MOST è disponibile della documentazione tecnica (manuali di riferimento del servizio) ed eventualmente è possibile la fornitura del supporto tecnico di personale specializzato.

Terminata la fase di integrazione, il servizio per il cliente viene configurato in **Ambiente di Produzione** e viene effettuato un collaudo congiunto del servizio. Con il collaudo, il servizio si considera attivato a tutti gli effetti.

6.2 Assistenza Tecnica Telefonica

I servizi di TI.TT dispongono di un Help Desk telefonico specializzato, in grado di rispondere sia a quesiti relativi ai servizi erogati che di risolvere problematiche di tipo tecnico nell'utilizzo degli stessi.

L'Help Desk è raggiungibile tramite numero verde nazionale (**800287524**) e fornisce:

1. *servizio di informazioni su servizi erogati*: dal lunedì al venerdì dalle 9.00 alle 17.00, festivi esclusi;
2. *servizio di assistenza ai clienti*: dal lunedì al venerdì dalle 9:00 alle 17.00, festivi esclusi;
3. *servizio di segnalazione malfunzionamenti*: 24 ore su 24, 7 giorni su 7, compresi i festivi.

Terminata la fase di identificazione del chiamante, i tecnici provvedono ad una prima analisi dell'anomalia segnalata (analisi di 1° livello), assegnando ad essa un determinato grado di severità e un codice di priorità. Questa fase prevede l'apertura di uno specifico "cartellino di guasto" (trouble-ticket) per il corretto tracciamento e gestione della segnalazione ricevuta.

Il sistema utilizzato consente inoltre la successiva analisi comparativa dei guasti e delle loro cause al fine di adottare azioni correttive.

Nel caso durante l'analisi di 1° livello non sia stato possibile risolvere il problema segnalato, l'anomalia verrà scalata ai tecnici specialistici di 2° livello.

Alla soluzione dell'anomalia il cliente è avvisato dagli specialisti del ripristino completo del servizio e guidato nella verifica della funzionalità al fine di chiudere il relativo "cartellino di guasto".

7 Service Level Agreement

7.1 Tempi di Attivazione del Servizio

Per l'attivazione del servizio MOST standard sono previsti circa 30 (trenta) giorni lavorativi.
Nel caso di personalizzazioni il tempo necessario per l'attivazione viene determinato caso per caso.

7.1.1 Livelli di Servizio Contrattualizzati

Servizio	SLA
Disponibilità del Servizio	99,5 % su base 4 mesi
Help Desk per segnalazione anomalie	H24 7x7

7.1.1.1 Disponibilità del servizio

Disponibilità del servizio:

Il calcolo dei valori della Disponibilità del servizio, effettuato ogni 4 mesi (base quadrimestrale), è definito secondo la formula di seguito riportata.

$$D = (1 - \frac{\sum_{i=1}^{M(\Delta t)} d_i}{365 \quad X \quad 24}) \times 100 \quad \%$$

Dove:

D: Disponibilità

di: Durata del disservizio di severità 1 (misurato in ore)

M: Numero di disservizi di severità 1

Δt: Periodo di osservazione

Non concorrono al calcolo della disponibilità i disservizi ascrivibili alle eccezioni riportate nel seguito.

Gli SLA vengono misurati sulla base delle segnalazioni degli utenti, tracciate sul sistema di trouble ticketing dell'Help Desk.

7.1.2 Tempi di risposta del servizio

Durante l'orario di copertura del servizio, il **tempo di risposta** è immediato: il numero verde messo a disposizione è sempre attivo.

7.1.3 Tempi di intervento e di ripristino

7.1.3.1 Tempo d'intervento

Per tempo d'intervento si intende il tempo intercorso da quando viene effettuata la segnalazione di disservizio da parte del cliente a quando il personale TI.TT di supporto tecnico inizia l'attività di risoluzione del guasto. Tale intervallo di tempo contiene pertanto le seguenti fasi di processo.

- Analisi preliminare
- Verifica dei tempi previsti per il ripristino del servizio
- Eventuale spostamento del personale tecnico sul luogo del guasto

Per ogni segnalazione di disservizio, il tempo d'intervento si calcola come differenza tra la data/ora in cui il personale TI.TT inizia l'attività di ripristino e la data/ora di segnalazione del disservizio stesso.

Le data/ora di risposta e di segnalazione del disservizio, saranno determinate mediante il meccanismo del trouble ticketing.

7.1.3.2 Tempo di ripristino

Per tempo di ripristino si intende il tempo intercorso da quando viene effettuata la segnalazione di disservizio da parte del Cliente a quando il personale TI.TT di supporto tecnico rimuove il guasto o anomalia segnalata.

Va segnalato che di ripristino è possibile parlare solo se si tratta di componenti HW in avaria piuttosto che di ripristino di moduli SW danneggiati o mal funzionanti.

Non essendo possibile assicurare il ripristino immediato a fronte di situazioni eccezionali che manifestino limiti di tecnologia o bug software, in tal caso IT si impegna ad elaborare un apposito progetto per la rimozione delle problematiche manifestatesi o anche a porre in essere soluzioni temporanee (bypass o workaround).

La data/ora in cui il servizio viene ripristinato e la data/ora di segnalazione del disservizio, saranno determinate mediante un meccanismo di trouble ticketing.

7.1.3.3 Severità del guasto

Si definiscono due livelli di Severità:

Severità 1 (guasto bloccante)

Appartiene alla classe di Severità 1 il fuori servizio totale della piattaforma (non è possibile erogare il servizio di MOST, SMS e/o INFO alla totalità degli utenti).

Severità 2 (guasto od anomalia)

Appartengono alla classe di Severità 2 tutti gli altri disservizi non rientranti nella classe di Severità 1.

Gli SLA relativi ai tempi di intervento e ripristino sono riassunti nella tabella seguente, salvo diversa indicazione fornita nell'elenco delle eccezioni.

Guasto	Tempo di intervento	Tempo di ripristino
Severità 1	4 ore	4 ore
Severità 2	4 ore	8 ore

Eccezioni:

- **Guasti Causa Cliente**

  Nel calcolo dei tempi intervento e ripristino non saranno conteggiati quelli per disservizi/guasti non di competenza TI.TT, per interventi di manutenzione concordati e documentati con il cliente e/o per

disservizi dovuti a "Causa Cliente" (es. eventi o situazioni determinati da atti o fatti imputabili al cliente che risultino causa scatenante del disservizio, mancata accessibilità al sito, ecc.).

- **Connettività di "back end" tra la piattaforma Cliente ed i Datacenter di Telecom**

  Gli SLA riportati in tabella non sono riferiti alle eventuali componenti di connettività di "back end" utilizzate dal cliente per la fruizione del servizio (es.: linea dedicata CDN, collegamento MPLS o VPN cifrata su Internet), in quanto questi collegamenti sono sotto il controllo "end-to-end" Telecom Italia.

- **Linee di connettività con la "Rete Telefonica Generale"**

  Ciascuna linea di connettività con la "Rete Telefonica Generale" necessaria per l'erogazione della "Mobile Strong Authentication" è un servizio gestito Telecom Italia.

- **Numeri Verdi**

  I servizi legati ai numeri Verdi seguono i parametri definiti a normativa tecnico commerciale di Telecom Italia (in conformità a quanto definito con l'Authority) [1]. A titolo di esempio, malfunzionamenti che non possono essere imputati a TI.TT e Telecom Italia sono le eventuali problematiche di non corretta configurazione sulle Rete di Operatori Telefonici diversi da Telecom Italia che non consentano il corretto routing della chiamata telefonica.

- **Terminale Telefonico dell'utente finale**

  Non sono imputabili a TI.TT "non corrette configurazioni" o problematiche collegate a "bachi software" o hardware presenti sui terminali telefonici mobili dell'utente finale.

7.2 Livelli di Servizio personalizzati

Allo scopo di realizzare livelli di servizio personalizzati e particolari in termini di 'contemporaneità delle chiamate' o di disponibilità di 'numeri verdi dedicati' il cliente può acquistare ulteriori ***elementi di servizio dedicati*** erogati da Telecom Italia, come:

- un certo numero di linee telefoniche
- uno o più numeri verdi

Queste esigenze vengono gestite in appositi progetti di realizzazione di versioni custom del servizio.

[1] Telecom Italia si impegna a riparare i guasti e/o i malfunzionamenti entro il secondo giorno non festivo successivo a quello in cui è pervenuta la segnalazione. Nel caso in cui occorra un guasto specifico di Rete Intelligente (es. sconfigurazione di un'associazione codice – numero pubblico), Telecom Italia si impegna a riparare i guasti entro 4 ore lavorative con copertura oraria 8,00-18,30 dal Lunedì al Venerdì, esclusi i giorni festivi.

8 Sicurezza Fisica Centro Servizi Certification Authority

La gestione della Sicurezza Fisica del Centro Servizi di TI Trust Technologies segue le linee guida del Gruppo (Rif. [1][2]).

Di seguito vengono dettagliate le misure di sicurezza comuni e specifiche per le aree di Data Center e Sede Aziendale.

8.1 Controllo degli accessi ai siti di Pomezia e di via Oriolo Romano

Le misure di sicurezza implementate per la protezione fisica dei siti e dei locali che ospitano le piattaforme tecnologiche utilizzate per l'erogazione dei servizi di certificazione digitale si articolano su vari livelli.

8.2 Protezione del perimetro esterno

Il primo livello di protezione è finalizzato alla tutela del perimetro esterno. Il sistema di anti intrusione perimetrale è garantito da:

- una recinzione esterna con grigliato metallico, strutturata in modo da facilitarne l'ispezione visiva da parte del personale di guardiania, che delimita fisicamente il perimetro esterno e che, per altezza, spessore, materiali utilizzati, offre una elevata protezione;
- un sistema di videosorveglianza a circuito chiuso (TVCC) con video registrazione: il controllo del perimetro è effettuato con impianti a raggi infrarossi. Le telecamere sono posizionate per il controllo del perimetro dell'edificio, degli ingressi, delle porte interbloccate e di eventuali altre zone critiche;
- barriere laser-fense e a raggi infrarossi per la supervisione e il controllo del perimetro delle sedi;
- uscite di sicurezza allarmate;
- un cancello esterno, la cui apertura è a cura del personale di sorveglianza;
- un presidio di sorveglianza h24x7, presso la portineria centrale, che supervisiona i transiti, identifica i visitatori ed eventualmente autorizza l'accesso all'interno della struttura. All'interno del presidio operano gli addetti alla sorveglianza che verificano la regolarità dei transiti con badge, nonché presiedono la gestione di tutte le operazioni richieste per l'accesso degli automezzi e dei visitatori al fine di garantire, nel rispetto delle procedure di sicurezza, l'integrazione tra i vari sistemi di protezione adottati e l'attivazione degli interventi previsti dalle procedure in vigore. La portineria è realizzata con adeguate protezioni strutturali e presenta la porta di accesso posizionata verso l'interno dell'area protetta; è, inoltre, dotata di passa-documenti per lo svolgimento delle operazioni di controllo in condizioni di massima sicurezza.

8.3 Procedura di accesso ai siti

Il secondo livello di protezione implementato tutela l'accesso ai siti stessi.

Il controllo accessi riferito agli edifici che costituiscono le sedi di TI Trust Technologies, avviene, secondo quanto previsto dalla procedura *"Accesso ai siti di Telecom Italia"[2]*.

L'accesso ai siti è possibile solo attraverso un ingresso esterno regolamentato da sistemi di tornelli ad accesso singolo a lettura badge.

I dipendenti e i visitatori abituali (accessi maggiori o uguali a 90 gg) sono in possesso di un badge definitivo assegnato dopo la compilazione di un modulo di autorizzazione permanente contenente data inizio e fine validità dell'accesso ed estremi di un documento di riconoscimento della persona. Tale modulo deve essere autorizzato da un Responsabile ed inviato alla società di vigilanza. Nel caso in cui il badge venga dimenticato potrà essere richiesto alla portineria un badge visitatore dietro la consegna di un documento. I badge dei dipendenti vengono bloccati alla cessazione del rapporto di lavoro. I badge dei visitatori abituali hanno scadenza annuale e possono essere bloccati in qualsiasi momento.

I visitatori occasionali (accessi inferiori a 90 gg) utilizzano un badge provvisorio giornaliero assegnato dal personale di portineria dopo la consegna di un documento di riconoscimento e la conferma della visita da parte del Responsabile di riferimento (o suo delegato).

All'interno dei siti sono presenti zone che richiedono misure di restrizione più elevate, in tal caso, oltre al lettore di badge configurati su opportune ACL (Access Control List) redatte dai Referenti di Competenza, possono essere presenti sistemi biometrici di controllo.

Il personale con badge non autorizzato, avrà accesso alle aree protette soltanto se:

- accompagnato da una persona abilitata: in tal caso la persona abilitata accompagnatrice dovrà assicurarsi che entrino con lui solo le persone effettivamente autorizzate, identificandole opportunamente e facendo attenzione che anche persone non autorizzate possano entrare avvalendosi di una momentanea confusione;
- annunciato ad un referente interno dell'area protetta che è stato avvisato dalla reception, che provvederà all'identificazione della persona.

Nel caso di personale di ditte esterne che effettua servizi periodici (manutenzione, pulizia e simili), l'accesso è consentito solo ai nominativi che figurano in elenchi predefiniti depositati presso il servizio di Sorveglianza Aziendale; per tale personale è richiesto accompagnamento all'interno delle aree certificate.

8.4 Procedura di accesso agli Uffici del Centro Servizi TI Trust Technologies

Gli uffici del Centro Servizi TI Trust Technologies che si trovano al primo ed al secondo piano della sede di Pomezia sono protetti da un ulteriore livello di sicurezza oltre quello previsto, tramite tornelli, all'ingresso dell'edificio. L'accesso avviene, infatti, solo dopo autenticazione attraverso apparecchiature elettroniche di controllo accesso, di tipo badge con tecnologia EBR, configurate con ACL (Access Control List) conformi alla lista di autorizzazione.

La verifica della congruità delle ACL è deputata al responsabile della Certification Authority.

L'accesso ai locali della Sala Operatori al piano terra è regolato da due porte e da un sistema di controllo di tipo interbloccato che ne impedisce l'apertura contemporanea. La porta esterna è dotata di un lettore di badge, la porta interna di un ulteriore lettore di badge e di rilevatore biometrico di impronta digitale.

I visitatori o il personale con badge non autorizzato, hanno accesso alle aree protette soltanto se accompagnati da una persona abilitata. In tal caso la persona abilitata accompagnatrice dovrà assicurarsi che entrino con lui solo le persone effettivamente autorizzate, identificandole opportunamente e facendo attenzione che anche persone non autorizzate possano entrare avvalendosi di una momentanea confusione.

8.5 Procedura di accesso ai Data Center

Le misure di protezione "attive" adottate per il controllo degli accessi ai Datacenter Telecom Italia hanno l'obiettivo di:

- discriminare gli accessi garantendo l'ingresso alle aree riservate alle sole persone autorizzate;
- preservare l'integrità e la disponibilità del servizio mediante soluzioni di continuità elettrica e di rete LAN ad alta affidabilità, nonché mediante la presenza di sistemi antincendio, antiallagamento e di dissipazione termica.

L'ingresso alla Sala Sistemi del CED di via Oriolo Romano, richiede apposita autorizzazione e l'accesso è consentito solo dopo l'inserimento nel lettore di un apposito badge personale di tipo EBR [1] che comanda l'apertura del varco. Le porte sono dotate di maniglione antipanico e di sensori che fanno suonare un allarme in caso di apertura non autorizzata della porta.

I sistemi di TI Trust Technologies sono contenuti all'interno di un 'cage' dedicato. L'accesso a tale cage è protetto da un apposito lettore di badge a cui è abilitato solo personale TI Trust Technologies. La procedura di accesso a tale area riservata da parte di personale esterno e/o ospiti è regolata da un'apposita procedura concordata tra Telecom Italia ed TI Trust Technologies che prevede l'accompagnamento degli ospiti da parte del personale TI Trust Technologies.

8.6 Sicurezza Fisica Data Center

I Datacenter siti a Pomezia e in Via Oriolo Romano sono conformi alle direttive del Gruppo (Rif. [1],[2]).

Hanno pareti esterne realizzate in cemento armato, con sale apparati delimitate da tramezzi realizzati con materiale da costruzione conforme alle norme antincendio.

La Sala Sistemi di TI Trust Technologies di Pomezia, è dotata di un impianto di videocitofono utilizzato per mettere in comunicazione le persone che non fanno parte dell'organizzazione del Centro con il personale all'interno della sala stessa che è così in grado di vedere e riconoscere l'interlocutore esterno. La Sala Sistemi è inoltre collegata mediante videocitofono con la Guardiola per le eventuali comunicazioni di servizio.

In tutti i locali protetti sono installati sensori volumetrici che rilevano i tentativi di passaggio nelle zone immediatamente sottostanti il sensore stesso e/o possibili mascheramenti. Questi sensori sono attivati dal personale della guardiania nell'orario di chiusura del Centro.

La tutela delle apparecchiature viene garantita dalle misure specificate nei seguenti paragrafi.

8.7 Cablaggi

Sono applicate misure di protezione fisica delle linee di trasmissione e degli armadi di distribuzione onde evitare inserimenti, rimozioni o manomissioni accidentali e/o non autorizzati.

Le linee di trasmissione si trovano in rack chiusi e/o in cage chiusi il cui accesso è consentito solo al personale autorizzato.

8.8 Impianto elettrico

L'energia elettrica è fornita da un sistema a doppia cabina di distribuzione, che implementa un meccanismo di ridondanza per garantire la continuità. I punti di allaccio alla rete sono serviti da una doppia alimentazione con possibilità di isolamento e manutenzione di tutti i componenti. Tutti i quadri che forniscono la corrente elettrica alle apparecchiature delle piattaforme di erogazione sono alimentati da gruppi di continuità.

8.9 Ripristino dell'erogazione di energia elettrica

Tutti i sistemi utilizzati nell'erogazione dei servizi oggetto del presente piano sono protetti da mancanza di energia elettrica o da altre anomalie di carattere elettrico.

A tal fine sono state adottate le seguenti azioni:

- linee di alimentazione multiple per evitare che un singolo punto di guasto nella fornitura elettrica possa causare l'interruzione del servizio;
- sistemi di continuità statici UPS;
- generatore di back-up.

La continuità elettrica è garantita da gruppi statici di continuità, connessi in parallelo con modulo centrale di distribuzione e batterie con autonomia di molte ore. Tale impianto è asservito ad un sistema di gruppi elettrogeni di soccorso, di cui uno cabinato esterno, alimentati, all'occorrenza, tramite un deposito di combustibile costituito da serbatoi di gasolio di grande capacità.

8.10 Rivelazione fumo e sistemi antincendio

Tutti gli ambienti sono dotati di rilevatori antifumo e sistemi antincendio con attivazione degli impianti di spegnimento automatico degli incendi a saturazione di ambiente.

In caso di interventi di manutenzione, gli impianti garantiscono la disattivazione della sola zona oggetto dell'intervento. In particolare l'impianto antincendio è stato progettato nel pieno rispetto della normativa UNI 9795 che prevede la segmentazione dell'impianto e, di conseguenza, viene garantita la perdita delle sole zone oggetto di eventuale incidente o calamità naturali ed il continuo funzionamento del resto dell'impianto. Tutte le attrezzature sono in linea con quanto previsto dalle leggi e normative vigenti (D.lgs 626/1994 e D.M. 10 marzo 1998) e rispettano le prescrizioni dei VVF.

Tutte le segnalazioni dell'impianto antincendio sono tempestivamente riportate sia al presidio interno di manutenzione sia al presidio di security, in modo che il personale addetto possa avvertire in tempi contenuti i soggetti individuati nello specifico piano di sfollamento della sede.

8.11 Antiallagamento

Sono previste delle sonde di rivelazione presenza liquidi nel sottopavimento in prossimità dei raccordi, delle valvole e delle derivazioni principali dell'impianto di distribuzione dell'acqua. Eventuali fuoriuscite di acqua sono opportunamente allontanate mediante convogliamento e scarico verso l'esterno. Gli allarmi sono riportati alla struttura Data Center Services, responsabile della supervisione all'interno del Centro Servizi.

8.11.1 Sistemi di controllo del livello di temperatura (HVAC - Heating Ventilation & Air Conditioning)

Gli impianti sono concepiti per poter smaltire tutta l'energia elettrica degradata in calore, al fine di garantire, sia in estate che in inverno, le seguenti condizioni ambientali:

- temperatura 18 - 24 gradi ± 1 °C;
- umidità relativa: controllata (30-70%);
- ricambi d'aria pari a 0,5 volumi/ora.

L'impianto ha le seguenti caratteristiche:

- generazione del freddo industriale attraverso 5 gruppi frigoriferi per 900.000 fr/h cadauno;
- distribuzione acqua refrigerata attraverso circuiti primario e secondario ad anello;
- 3 vasche di accumulo acqua da 10.000 litri.

Gli allarmi sono riportati alla struttura Data Center Services, responsabile della supervisione all'interno del Centro Servizi.

8.12 Dispositivi anti-intrusione

Le sale sistemi sono protette dalle seguenti misure:

- l'accesso avviene tramite porte tipo REI 120 costruite in modo da resistere ad elevate sollecitazioni meccaniche e termiche;
- su porte e finestre sono installati dei sensori (sensori magnetici, avvisatori ottici acustici e sensori RTA) collegati ad un sistema di segnalazione degli allarmi di tipo locale e remoto;
- le aree di carico e scarico merci sono fisicamente separate dagli altri punti di accesso normalmente utilizzati dal personale interno ed esterno. Inoltre, per consentire un efficace monitoraggio degli accessi fisici e delle risorse, è previsto l'utilizzo di un Registro degli Accessi Fisici conservato in modo protetto ed un inventario di tutti i sistemi e gli apparati appartenenti all'infrastruttura IT, situati all'interno dei Data Center;
- a tutela delle misure specifiche per le apparecchiature e per l'accesso fisico, è presente un presidio armato H24 7x7 con personale di vigilanza che effettua un servizio di ronda, intensificato nelle ore notturne.

8.13 Monitoring delle facility

Come anticipato nei precedenti paragrafi gli apparati di alimentazione, condizionamento/raffreddamento, antiallagamento, rilevazione temperatura ed umidità e antincendio dei Data Center sono allarmati mediante contatti a relè azionati dalle logiche interne agli apparati stessi.

Gli allarmi sono riportati alla struttura Data Center Services, responsabile della supervisione all'interno del Centro Servizi.

I criteri per l'identificazione dell'allarme, la valutazione della loro gravità e quindi l'urgenza dell'intervento sono univocamente determinati sulla base di specifiche normative interne redatte per i singoli stabili (infatti, all'interno di ogni DC, per ogni impianto vengono definiti specifici parametri di controllo. Il manutentore del sito, dopo averli concordati con la funzione impianti del DC, si occupa del loro monitoraggio).

La figura seguente riporta, a titolo di esempio, il quadro di monitoraggio disponibile per gli allarmi generati dagli impianti elettrici e di condizionamento.

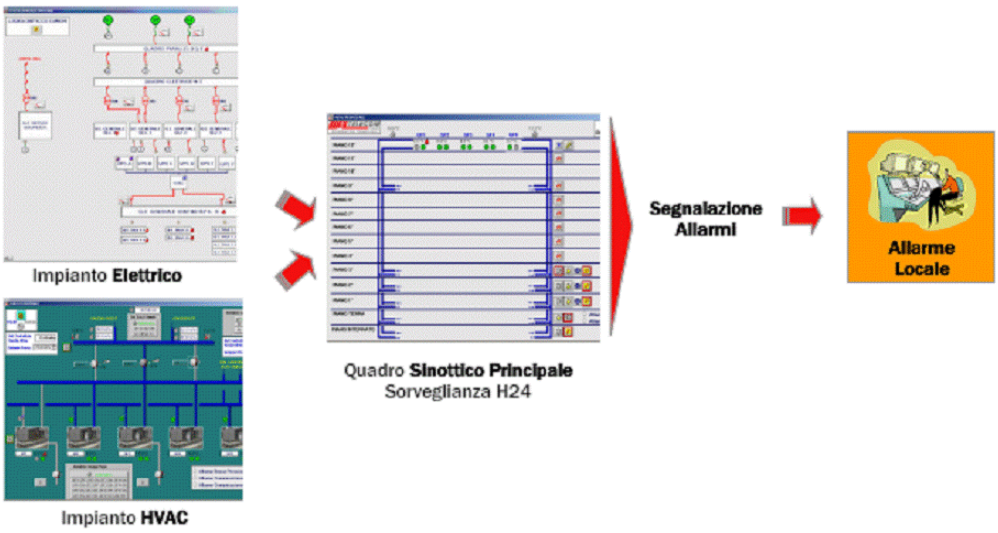


Figura 1: Schema logico Monitoraggio facility

Gli impianti antincendio, antiallagamento, di continuità elettrica, di condizionamento e di anti-intrusione sono coperti da contratti di manutenzione che prevedono livelli di servizio garantiti e controlli periodici per verificarne la perfetta efficienza.

8.14 Manutenzione degli asset tecnologici

La manutenzione ordinaria di tutti gli asset tecnologici viene effettuata secondo le raccomandazioni e le specifiche definite dai fornitori. Le attività di manutenzione sono effettuate da personale accreditato, esclusivamente on-site e nel rispetto di accordi con i fornitori.

8.15 Descrizione dei servizi di sicurezza logica implementati

I paragrafi che seguono descrivono i dispositivi e gli strumenti atti a preservare la sicurezza logica dei sistemi e delle informazioni in essi contenute.

8.15.1 Servizi di Firewall

L'infrastruttura di rete prevede una prima linea costituita da un sistema firewall, configurato in alta affidabilità, che filtra il traffico da Internet verso la componente di Front-End, ed una seconda linea costituita da un altro sistema firewall che filtra il traffico tra la componente di Front-End e quelle di Back End.

I servizi di Firewall costituiscono la prima barriera di protezione per l'accesso ai servizi erogati dal dominio di pertinenza.

8.15.2 Servizi di Intrusion Detection

Il sistema di Intrusion Detection (IDS), integrato nei sistemi di protezione perimetrale, controlla in tempo reale il traffico esplicitamente permesso ed identifica e previene una grande varietà di attività di rete considerate sospette. Tale controllo viene svolto confrontando le 'signatures' di attacchi noti e eventuali anomalie sui protocolli del traffico in transito.

Sia le signatures predefinite dell'IDS sia il motore IDS vengono costantemente aggiornati tramite la apposita rete di distribuzione del fornitore, previa autenticazione e cifratura delle comunicazioni.

La logica con la quale è costruito il sistema di IDS lo rende, di fatto, un sistema sia di alert che di prevenzione agli attacchi.

Le configurazioni previste per l'IDS sono create in maniera da rilevare e fermare le minacce principali ma non inficiare la funzionalità della rete. Le porte di 'sniffing' saranno configurate in modalità stealth, ossia non sarà effettuato il binding di uno stack TCP/IP

8.15.3 Servizio di Antivirus

Tutti i sistemi operativi ed i software utilizzati sono costantemente aggiornati allo stato dell'arte e sui sistemi vulnerabili sono installati antivirus.

Un sistema centralizzato permette di aggiornare in modo automatico tutti i server windows.

8.15.4 Controllo della vulnerabilità

Tutti i sistemi utilizzati in rete sono periodicamente controllati tramite scansioni a livello rete da un sistema centralizzato che fornisce report dettagliati sullo stato di vulnerabilità dei sistemi *(vulnerability assessment).*

8.15.5 Ridondanza degli apparati

Tutti i componenti critici della piattaforma di erogazione sono configurati per operare in modalità ridondata. Se uno dei componenti si guasta la sua funzione può essere mantenuta da un componente di riserva senza interventi da parte degli operatori. Queste funzionalità sono garantite dalle caratteristiche HW e SW dei sistemi utilizzati:

- I firewall posizionati a difesa della rete di front-end sono configurati in High Availability e in load sharing, tali prodotti garantiscono la continuità del servizio anche a fronte di fault di uno dei due sistemi.
- I firewall posizionati a difesa della rete di back-end sono configurati in High Availability tramite l'utilizzo di una soluzione architetturale che consente l'utilizzo di un indirizzo IP virtuale a cui corrisponde una coppia di appliance Firewall.

- La gestione dei dati avviene attraverso l'utilizzo di DataBase configurati in High Availability (ad esempio RDBMS Oracle..). I sistemi di storage dei Database garantiscono la corretta gestione dei dischi in modalità mirroring per soddisfare requisiti di alta affidabilità.

8.15.6 Sicurezza degli elaboratori

La piattaforma di gestione delle attività di certificazione è stata progettata in modo da garantire nel tempo la capacità di incrementare gradualmente la performance e la capacità di produzione attraverso l'espansione dello spazio disco utilizzabile e l'aggiunta di ulteriori sistemi. Pertanto l'infrastruttura di erogazione si caratterizza per la sua flessibilità e garantisce l'adeguamento fino al livello massimo di produzione.

La piattaforma di erogazione adotta soluzioni hardware e software leader di mercato per interoperabilità, affidabilità e sicurezza..

I sistemi operativi dei sistemi di elaborazione utilizzati nelle attività di certificazione, nella generazione dei certificati e nella gestione del registro dei certificati sono configurati in modo tale da ridurre al minimo il rischio di alterazione delle configurazioni. Sono quindi previsti, nel normale uso dei sistemi stessi, dei profili con diritti di accesso non assimilabili a quelli amministrativi.

8.15.7 Protocolli Sicuri di comunicazione

I funzionari delle sedi di riferimento comunicano dalle loro postazioni con il sistema informatico del Centro Servizi mediante un canale di comunicazione costituito da una connessione Internet opportunamente protetta mediante sistemi firewall e proxy. La connessione è soggetta ad autenticazione. Tale autenticazione avviene, a seconda dei servizi, mediante inserimento di userid e password oppure mediante certificato digitale di autenticazione emesso dal Certificatore.

Gli Addetti IT alle risorse del Centro Servizi per la parte di conduzione sistemi sono effettuati in modalità SSH con accesso controllato da FIREWALL e autenticazione centralizzata LDAP attraverso l'utilizzo di apposite postazioni allocate all'interno del centro servizi stesso. Pertanto non è possibile in alcun modo accedere ai sistemi via rete al di fuori della LAN locale.

8.15.8 Procedura per la gestione dell'accesso ai sistemi della CA

La politica di gestione delle credenziali e dei diritti di accesso del personale del Gruppo si basa sui seguenti tre principi cardine:

- la corretta identificazione e autenticazione di tutte le persone che accedono ai sistemi;
- l'assegnazione a ciascuna risorsa dei giusti privilegi di accesso;
- il controllo del corretto mantenimento dei privilegi.

La politica prevede misure specifiche per le regole e le modalità di accesso ai sistemi ed è formalizzata in accordo a:

- il provvedimento del Garante Privacy del 01-06-2006 per gli aspetti riguardanti la corretta gestione dei profili di accesso di tipo amministrativo e la separazione organizzativa tra le funzioni deputate all'assegnazione delle credenziali e dei diritti di accesso rispetto a quelle di gestione tecnica dei sistemi;
- gli obblighi di legge previsti dal Testo Unico in materia di privacy – D.Lgs. 196/03;

gli standard internazionali di sicurezza e le best practices richiamate anche dall'ISO27001, in materia di User Access Management;

8.16 Back-Up e Restore

I dati contenuti nei sistemi del Certificatore sono soggetti a precise politiche di back up, tali politiche si differenziano in funzione della tipologia dei dati e della loro riservatezza. Le copie di back up dei dati della Piattaforma sono effettuate utilizzando un sistema di back up e recovery centralizzato situato all'interno del Centro Servizi del Certificatore, fra le principali caratteristiche della soluzione scelta si annoverano le seguenti:

- Funzionamento automatico
- Controllo centralizzato
- Integrazione con tutti i sistemi presenti all'interno di TI Trust Technologies
- Facilità di gestione
- Scalabilità su nuovi sistemi
- Riservatezza dei dati archiviati

Il prodotto software selezionato per il salvataggio periodico dei dati permette, tramite i suoi processi automatici di backup, archiviazione e indicizzazione dei dati presenti in ogni client; garantisce, il ripristino dei singoli dati o di tutto il contenuto di uno o più dischi/nastri di backup del client stesso assieme alle librerie dotate di tutte le caratteristiche di sicurezza necessarie per l'adeguata conservazione dei supporti magnetici, su cui vengono salvati i dati.

La Certification Autorithy prevede, a meno di indicazioni specifiche, le seguenti Politiche di Back Up:

- *Back Up incrementale giornaliero*
- *Back Up full settimanale*
- *Retention dei dati di 1 mese*

L'attività di ripristino totale o parziale di dati utilizza le componenti software ed infrastrutturali del sistema di back-up; tale attività si articola nei seguenti passi:

- *identificazione del perimetro d'intervento, ovvero individuazione dei server sui quali deve essere eseguita l'attività di ripristino per rendere consistenti i dati;*
- *selezione dei dati di back-up in base all'identificativo temporale (giorno e ora);*

esecuzione del restore dei dati e verifica dell'esito positivo; nel caso in cui il restore non abbia esito positivo, viene effettuata un'operazione di roll-back