**Progetto E.T.Na. (Elenco Telefonico Nazionale)**

Ciascun Gestore di servizi di telecomunicazioni dovrà rendere disponibile al Centro elaborazione dati del Ministero dell’Interno tutti i dati in suo possesso, riguardanti i servizi di telefonia fissa e mobile.

1. ***Caratteristiche generali***

Nell’architettura di riferimento generale del progetto E.T.Na. (**Figura 1**) sono presenti le seguenti componenti applicative:

* Portale S.I.I. (Centro elaborazione dati del Ministero dell’Interno);
* Sistema E.T.Na. (Centro elaborazione dati del Ministero dell’Interno);
* ***applicazione*** dei Gestori di servizi di telecomunicazioni.

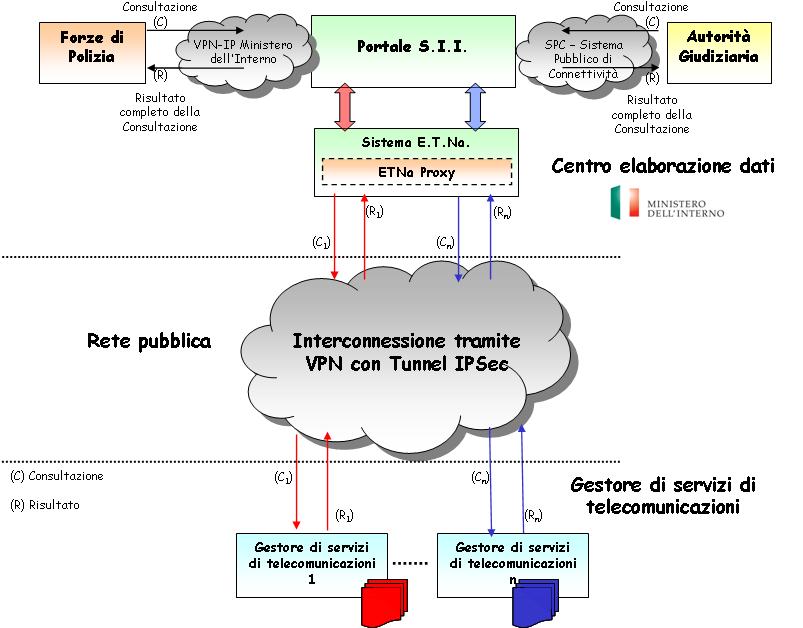


Figura 1 - Architettura di riferimento generale del progetto E.T.Na.

## Componenti applicative

*Portale S.I.I. (Centro elaborazione dati del Ministero dell’Interno)*

Il Portale S.I.I. è il portale Web del Servizio Informativo Interforze, attraverso il quale gli utenti abilitati (“utenti SDI”) accedono alle applicazioni e ai servizi offerti dal Centro elaborazione dati del Ministero dell’Interno. Tale portale è integrato con il sistema di sicurezza del citato CED, al fine di garantire esattamente l’identificazione e l’autenticazione degli utenti che accedono alle applicazioni e ai servizi offerti.

*Sistema E.T.Na. (Centro elaborazione dati del Ministero dell’Interno)*

Il sistema E.T.Na. (**E**lenco **T**elefonico **Na**zionale) è una applicazione che sarà resa disponibile (come Banca dati esterna) fruibile attraverso il citato Portale.

Nello specifico, il sistema E.T.Na. permetterà agli utenti abilitati (“utenti investigativi dello SDI”) delle Forze di Polizia e dell’Autorità Giudiziaria, la consultazione per via telematica, delle informazioni riguardanti i servizi di telefonia fissa e mobile ed i corrispondenti abbonati di tali servizi, nonché degli acquirenti del traffico prepagato della telefonia mobile, in possesso di ciascun Gestore di servizi di telecomunicazioni.

*Sistemi informatici dei Gestori di servizi di telecomunicazioni*

I sistemi informatici dei Gestori di servizi di telecomunicazioni potranno essere realizzati nelle seguenti modalità: con un “portale web dedicato” (al momento già disponibile e fruibile per fini istituzionali da parte delle Forze di Polizia e dell’Autorità Giudiziaria) o con una interfaccia “ad hoc” basata su standard Web Services.

***Misure di sicurezza***

Al fine di garantire un canale sicuro per la comunicazione, è previsto l’utilizzo della rete Internet per l’invio delle richieste di consultazione. La ricezione delle corrispondenti risposte sul sistema E.T.Na., provenienti dai sistemi informatici dei diversi Gestori di servizi si telecomunicazioni, impone l’adozione di elevati standard di “sicurezza”. Il termine “sicurezza”, nel suo complesso, comprende diversi aspetti, quali l’autenticazione, la riservatezza (confidenzialità), l’integrità e il non ripudio. I diversi aspetti che caratterizzano la sicurezza sono i seguenti:

* **L’autenticazione** - garantisce l’identità del mittente e del destinatario della comunicazione.
* **La riservatezza** - garantisce la riservatezza del contenuto della comunicazione (segretezza del messaggio) tra il mittente e il destinatario.
* **L’integrità** - garantisce l’integrità del contenuto della comunicazione (non modificabilità del messaggio) tra il mittente e il destinatario.
* **Il non ripudio** - garantisce l’impossibilità per il mittente (o per il destinatario) di negare di avere inviato (o ricevuto) il messaggio.

La sicurezza della comunicazione sarà garantita tramite l’adozione di protocolli IPSec (Internet Protocol Security)[[1]](#footnote-1). L’IPSec potrà essere identificato come una sorta di framework in grado di assicurare autenticità, riservatezza e integrità delle comunicazioni effettuate in una rete che utilizza il protocollo IP (ad esempio la rete Internet).



**Centro elaborazione dati del Ministero dell’Interno (ETNa)**

**Sito del generico Gestore di servizi di telecomunicazioni**

**Rete pubblica**

**VPN con Tunnel IPSec. Dati crittografati.**

**Gateway VPN con indirizzo IP pubblico statico**

@!”£$%&

@#[K”!£

**Gateway VPN con indirizzo IP pubblico statico**

Lan locale

Lan locale

**2**

**1**

Client

Server

HTTPS

HTTPS

Figura 2 - Architettura di rete con VPN e Tunnel IPSec

Quindi, con il framework IPSec (Figura 2) saranno garantiti elevati standard di sicurezza per il livello di rete (layer 3); mentre, per il livello applicativo (layer 7), gli standard di sicurezza saranno assicurati mediante l’adozione del protocollo HTTPS (HTTP con protocollo sicuro SSL v3). L’adozione del framework IPSec, che permette una facile integrazione tra le applicazioni, è completamente trasparente a livello applicativo. La soluzione completa quindi,per garantire un canale “sicuro” di comunicazione, utilizzerà SSL sopra IPSec. In particolare, l’IPSec garantirà la sicurezza della comunicazione tra i punti terminali del “Tunnel IPSec” (a livello IP), mentre, al di sopra, sarà utilizzato il protocollo SSL per garantire la sicurezza a livello di applicazione.

Nell’architettura di rete, relativa all’interconnessione tra il Centro elaborazione dati del Ministero dell’Interno ed il sito di accesso di ciascun Gestore di servizi di telecomunicazioni, sarà implementata una apposita VPN (Virtual Private Network) da parte di ciascun Operatore di Telefonia. Ogni VPN permetterà di stabilire un canale di comunicazione “sicuro” attraverso la rete Internet, creando un “tunnel IPSec” [[2]](#footnote-2) tra le due postazioni VPN Gateway.

Per il livello applicativo, oltre a quelli già previsti dal canale di comunicazione “sicuro”, saranno adottati ulteriori sistemi di sicurezza basati su certificati digitali al fine di permettere un’identificazione precisa e reciproca del mittente e del destinatario.

In particolare, i suddetti certificati digitali, saranno utilizzati per l’autenticazione a livello di applicazione. Al completamento della fase di autenticazione, è prevista una fase ulteriore di autorizzazione tramite “username” e “password”;

Nel caso di adozione, da parte del generico Gestore di servizi di telecomunicazioni, di una soluzione tecnologica per la cooperazione applicativa, basata su standard Web Services, l’ente di certificazione preposto al rilascio dei suddetti certificati digitali sarà il Centro elaborazione dati del Ministero dell’Interno.

1. ***Panoramica applicativa***

***Utenti del sistema***

L’utente del sistema E.T.Na. è sostanzialmente un “utente investigativo”, sia nel caso di appartenenza alle Forze di polizia, sia dell’Autorità Giudiziaria. Tale utente effettuerà l’autenticazione sul Portale S.I.I., quindi, se in possesso della prevista abilitazione (c.d. “profilatura applicativa”) per l’utilizzo del sistema E.T.Na., potrà accedere alle funzionalità di consultazione dell’Elenco Telefonico Nazionale. Gli utenti delle Forze di polizia che potranno utilizzare il sistema E.T.Na. per fini istituzionali, sono gli ufficiali e gli Agenti di P.G. degli Uffici Investigativi delle Forze di polizia (Arma dei Carabinieri, Polizia di Stato, Guardia di Finanza, Polizia Penitenziaria e Corpo Forestale dello Stato) opportunamente autorizzati dal rispettivo Capo Ufficio/Comandante di Reparto ai fini dell’assolvimento di indagini di P.G.

***Controllo degli accessi e garanzia della sicurezza applicativa***

Il controllo degli accessi al sistema E.T.Na. sarà garantito tramite la stessa soluzione di Autenticazione e Autorizzazione già in uso al Centro Elaborazione Dati del Ministero dell’Interno sia per il Portale del Servizio S.I.I., sia per il Sistema Di Indagine (SDI). Tale livello di autenticazione ed autorizzazione rispetterà, quindi, tutti i requisiti di sicurezza già in essere richiesti dal Garante per la protezione dei dati personali nell’ambito del trattamento dei dati da parte del Ced Interforze.

***Logging applicativo***

La scrittura del log applicativo viene effettuata dal sistema E.T.Na. ogni qualvolta viene espressa una INTENZIONE DI RICERCA da parte degli operatori autorizzati delle Forze di polizia e dell’Autorità Giudiziaria. Le principali informazioni memorizzate a seguito di una INTENZIONE DI RICERCA attivata nel sistema E.T.Na., saranno le seguenti:

* timestamp dell’INTENZIONE DI RICERCA;
* identificativo dell’utente che ha espresso la specifica INTENZIONE DI RICERCA;
* postazione di lavoro utilizzata;
* identificativo dell’ufficio di appartenenza;
* INTENZIONE DI RICERCA;
* esito della ricerca, contenente le informazioni visualizzate dall’utente.

Dal log applicativo saranno opportunamente generati dei file basati sullo standard xml i quali saranno successivamente archiviati all’interno di supporti di memorizzazione dedicati, garantiti dagli stessi standard e requisiti di sicurezza già in uso per il Portale del Servizio S.I.I. e per il Sistema Di Indagine (SDI).

***Consultazione del sistema***

La nuova progettualità del sistema E.T.Na., in ottemperanza al provvedimento del Garante per la protezione dei dati personali (**Bollettino n.72/maggio 2006**), prevede la consultazione di una banca dati “distribuita”[[3]](#footnote-3) - costituita “logicamente” dalle banche dati dei *Gestori di servizi di comunicazione*. In tale scenario, la consultazione di una banca dati “distribuita” elimina, di fatto, la duplicazione delle informazioni già presenti nelle banche dati dei diversi Gestori di servizi di telecomunicazioni.

L’architettura funzionale del sistema E.T.Na. sarà del tipo *Web-Oriented*. Quindi, a seguito dell’inserimento di una specifica INTENZIONE DI RICERCA (tramite l’utilizzo di un web browser), la funzionalità applicativa ETNa Proxy (del sistema E.T.Na.) invierà la richiesta di consultazione verso i sistemi informatici dei diversi Gestori di servizi di telecomunicazioni.

L’interazione per via telematica, tra il sistema E.T.Na. ed i sistemi informatici dei diversi Gestori di servizi di telecomunicazioni, avverrà tramite interfaccia informatica automatica. Sarà cura del Centro Elaborazione Dati del Ministero dell’Interno predisporre l’opportuna interfaccia informatica (automatica) nel sistema E.T.Na. in modo tale da interagire con le varie soluzioni adottate dai Gestori Telefonici: “portale web dedicato” o standard Web Services.

L’invio delle richieste di consultazione e la ricezione delle corrispondenti risposte, da parte del sistema E.T.Na., avviene tramite il protocollo HTTPS (HTTP con protocollo sicuro SSL v3).

Al fine di rendere fruibile un servizio efficace ed efficiente per le attività investigative delle Forze di polizia e dell’Autorità Giudiziaria, ogni Gestore di servizi di telecomunicazioni dovrà garantire almeno le seguenti tipologie di INTENZIONI DI RICERCA.

Campi di ricerca previsti nel caso della **telefonia fissa** (numerazione geografica e non):

* Numero telefonico;
* Cognome e Nome o Codice Fiscale (nel caso di persona fisica);
* Ragione Sociale o Partiva IVA (nel caso di persona giuridica).

Per la parte dati:

* IP Statico o Login Adsl.

Opzione storico dei dati.

Campi di ricerca previsti nel caso della **telefonia mobile**:

* Numero telefonico;
* Cognome e Nome o Codice Fiscale (nel caso di persona fisica);
* Ragione Sociale o Partiva IVA (nel caso di persona giuridica);
* ICCID;
* IMSI;
* Dealer (punto vendita/attivazione).

Opzione “reale utilizzatore”;

Opzione storico dei dati.

Con l’obiettivo di fornire un’alta qualità del servizio a supporto delle attività investigative delle Forze di polizia e dell’Autorità Giudiziaria, il Centro Elaborazione Dati del Ministero dell’Interno può concordare con ciascun Gestore di servizi di telecomunicazioni il numero massimo giornaliero delle richieste di consultazione (nell’eventualità, anche suddiviso per tipologia di INTENZIONE DI RICERCA) ed il numero massimo delle richieste di consultazione concorrenti (simultanee).

In allegato le tabelle dati per i servizi di telefonia fissa e mobile.



CONVENZIONE TRA IL GESTORE DI SERVIZI DI TELECOMUNICAZIONI ED IL MINISTERO DELL’INTERNO



1. IPSec non è costituito da un solo protocollo ma da un insieme di protocolli, di tecniche ed algoritmi sviluppati in ambito internazionale dall’IETF. [↑](#footnote-ref-1)
2. Tra le due postazioni VPN Gateway verrà configurato un tunnel IPSec utilizzando il protocollo ESP con Triple DES e SHA-1. Il protocollo ESP garantisce l’autenticazione, la riservatezza, l’integrità e la protezione anti-replay. [↑](#footnote-ref-2)
3. Mediante reti di comunicazione elettronica. [↑](#footnote-ref-3)