Allegato A

Modalità di trasmissione dei dati

dagli operatori sanitari

per il tramite del Sistema TS

INDICE

1. INTRODUZIONE

Il presente allegato descrive le modalità tecniche di trasmissione da parte degli operatori sanitari dei dati alla componente di backend dell'app Immuni, ai sensi dell'art. 2 comma 3 del presente decreto.

2. SERVIZIO DI INVIO DEL CODICE OTP

2.1 DESCRIZIONE DEL SERVIZIO

In riferimento all'articolo 2 comma 2 del presente decreto, il servizio di invio dei dati al backend dell'App attraverso il servizio descritto nel presente allegato.

2.2 MODALITÀ DI FRUIZIONE

Il servizio di invio dei dati è reso disponibile in modalità applicazione web oppure in modalità cooperativa tramite web services.

2.3 ACCESSO AL SERVIZIO

Le possibilità di accesso al servizio da parte dell'operatore sanitario sono riassunte nella seguente tabella, che esplicita gli utenti che possono accedere al sistema attraverso sistemi software con interfacce web o web services, oppure per il tramite di sistemi regionali.

ID	Utente	Modalità	Autenticazione	Note
1	Regione	Web service	Mutua autenticazione con certificato client	L'operatore sanitario si connette al sistema regionale che a sua volta invoca il servizio tramite client applicativo. Certificato di autenticazione rilasciato dal Sistema TS. Il codice fiscale dell'operatore viene trasmesso come campo applicativo nel tracciato. Il sistema regionale deve garantire i requisiti minimi di sicurezza adottati dal Sistema TS in termini di autenticazione forte, nel tracciato viene dichiarata la tipologia di autenticazione: 2 fattori, CNS, CIE, SPID.

2	Operatore sanitario	Web service	TS-CNS oppure CNS oppure basic authentication (ID utente e password) con pincode come fattore di autenticazione	L'operatore sanitario invoca il servizio tramite software gestionale. Credenziali di autenticazione rilasciate dal Sistema TS.
3	Operatore sanitario	Applicazione web	TS-CNS oppure CNS oppure basic authentication (ID utente e password) con pincode come fattore di autenticazione	L'operatore sanitario invoca il servizio tramite interfaccia web. Credenziali di autenticazione rilasciate dal Sistema TS.

Tabella 1 – Modalità di accesso

La modalità 1 si rivolge alle regioni e alle province autonome di Trento e Bolzano, che sono gli intermediari SAR che colloquiano con il Sistema TS e che permettono l'accesso all'operatore sanitario. L'operatore sanitario (utente finale) si autentica con il sistema regionale con credenziali e modalità stabilite dalla regione; a sua volta la regione si autentica e coopera con il Sistema TS attraverso il servizio descritto nel presente allegato.

La modalità 2 si rivolge al singolo operatore sanitario che tramite un software gestionale sviluppato ad hoc si connette al servizio utilizzando la propria TS-CNS oppure le proprie credenziali rilasciate dal Sistema TS.

La modalità 3 si rivolge al singolo utente che accede ad una applicazione web resa disponibile sul portale del Sistema TS utilizzando la propria TS-CNS oppure le proprie credenziali rilasciate dal Sistema TS.

Gli operatori sanitari del Sistema TS sono quasi tutti dotati di pincode, la percentuale che non ne è dotata è di circa l'8%.

Al fine di rinforzare le misure di sicurezza adottate dal Sistema TS, di seguito si riporta una sintesi degli interventi che saranno attuati a breve termine:

- in aggiunta alle normali credenziali (ID utente e password), assegnazione del pincode come ulteriore fattore di autenticazione a tutti gli utenti che ancora non ne sono dotati;
- come ulteriore misura rafforzativa, implementazione dell'autenticazione a 2 fattori con OTP temporaneo;

- introduzione delle asserzioni SAML per i sistemi regionali per la trasmissione dell'utente finale al Sistema TS.

2.4 TRACCIATO DEL SERVIZIO

Di seguito si descrivono i messaggi di richiesta e di risposta del servizio, validi sia per la modalità web che per la modalità web service.

Messaggio di richiesta

Campo	Descrizione	Obbligatorio
Codice OTP	Codice One Time Password	SI
Data inizio sintomi	Data di inizio dei sintomi	SI

Messaggio di risposta

Campo	Descrizione	Fonte
Identificativo transazione	Identificativo alfanumerico della transazione, generato dal sistema	Sistema TS
Data-ora	Data-ora-minuti-secondi-millisecondi in cui si è conclusa la transazione	Sistema TS
Esito	Esito della transazione	Backend App Immuni

2.5 REGISTRAZIONE DEGLI ACCESSI APPLICATIVI E TEMPI DI CONSERVAZIONE

Il servizio non costituisce né alimenta alcuna banca dati contenuta nel Sistema TS, in quanto la sua finalità è la trasmissione dei dati al backend dall'App .

Il sistema registra unicamente gli accessi all'applicazione e l'esito dell'operazione, e inserisce i dati dell'accesso in un archivio dedicato. In nessun caso sono tracciati i dati applicativi (OTP, data inizio sintomi), né su banca dati né su file di log, né su altro mezzo.

Per ciascuna transazione effettuata saranno registrati i seguenti dati relativi all'accesso e all'esito dell'operazione. Nel caso di utente regione: identificativo della regione che si autentica, codice fiscale dell'operatore

sanitario, data-ora-minuti-secondi-millisecondi dell'accesso, operazione richiesta, esito della transazione, identificativo della transazione. Nel caso di utente operatore sanitario: codice fiscale dell'operatore sanitario, data-ora-minuti-secondi-millisecondi dell'accesso, operazione richiesta, esito della transazione, identificativo della transazione.

I log degli accessi così descritti sono conservati per dodici mesi.

3. MISURE DI SICUREZZA

3.1 INFRASTRUTTURA FISICA

L'infrastruttura fisica è realizzata dal Ministero dell'economia e delle finanze attraverso l'utilizzo dell'infrastruttura del Sistema Tessera sanitaria in attuazione di quanto disposto dal presente decreto.

I locali sono sottoposti a videosorveglianza continua e sono protetti da qualsiasi intervento di personale esterno, ad esclusione degli accessi di personale preventivamente autorizzato necessari alle attività di manutenzione e gestione tecnica dei sistemi e degli apparati.

L'accesso ai locali avviene secondo una documentata procedura, prestabilita dal Titolare del trattamento, che prevede l'identificazione delle persone che accedono e la registrazione degli orari di ingresso ed uscita di tali persone.

3.2 REGISTRAZIONE DEGLI UTENTI ED ASSEGNAZIONE DEGLI STRUMENTI DI SICUREZZA

E' presente una infrastruttura di Identity e Access Management che censisce direttamente le utenze, accogliendo flussi di autenticazione e di autorizzazione, per l'assegnazione dei certificati client di autenticazione, delle credenziali di autenticazione e delle risorse autorizzative.

L'autenticazione delle regioni verso il sistema avviene attraverso certificato client con mutua autenticazione. Il certificato viene emesso con un sistema di crittografia asimmetrica a chiave pubblica/privata.

Il sistema effettua la gestione completa del certificato di autenticazione: assegnazione, riemissione alla scadenza, revoca.

La gestione e la conservazione del certificato client è di esclusiva responsabilità del soggetto cui è stato assegnato.

L'autenticazione degli operatori sanitari avviene tramite TS-CNS oppure CNS oppure credenziali e pincode.

La TS-CNS è prodotta e consegnata dal Sistema TS a tutti gli assistiti del SSN. La tessera è dotata di chip che contiene il certificato di autenticazione

personale. Prima del primo utilizzo come dispositivo di autenticazione, la tessera deve essere attivata presso il Card Management System della regione di riferimento.

Per l'autenticazione è possibile anche utilizzare una CNS distribuita dai sistemi regionali.

Un ulteriore metodo di autenticazione per gli operatori sanitari è costituito dalle credenziali dotate di pincode. L'assegnazione delle credenziali agli utenti del Sistema TS è effettuata dagli Amministratori di sicurezza presenti in ciascuna ASL. La registrazione degli operatori sanitari si effettua presso la ASL di riferimento che consegna le credenziali e la prima parte del pincode. La seconda parte del pincode si ottiene direttamente sul portale del Sistema TS dopo la prima autenticazione.

La gestione dei profili di autorizzazione è effettuata sempre dagli amministratori di sicurezza delle ASL. A tutti gli operatori sanitari che devono essere autorizzati viene assegnata una risorsa di autorizzazione creata e dedicata appositamente al servizio descritto dal presente decreto.

Gli amministratori di sicurezza si autenticano con le credenziali in basic authentication. A breve termine saranno dotati di strumenti di autenticazione forte.

La gestione degli amministratori di sicurezza delle ASL è effettuata dall'Amministratore centrale della sicurezza. L'Amministratore centrale della sicurezza è nominato tra gli incaricati del trattamento.

3.3 CANALI DI COMUNICAZIONE

Le comunicazioni sono scambiate in modalità sicura su rete SPC per le regioni ovvero tramite Internet, mediante protocollo TLS in versione minima 1.2, al fine di garantire la riservatezza dei dati. I protocolli di comunicazione TLS, gli algoritmi e gli altri elementi che determinano la sicurezza del canale di trasmissione protetto sono continuamente adeguati in relazione allo stato dell'arte dell'evoluzione tecnologica, in particolare per il TLS non sono negoziati gli algoritmi crittografici più datati (es. MD5).

3.4 SISTEMA DI MONITORAGGIO DEL SERVIZIO

Per il monitoraggio dei servizi, il Ministero dell'economia e delle finanze si avvale di uno specifico sistema di reportistica.

3.5 PROTEZIONE DA ATTACCHI INFORMATICI

Per proteggere i sistemi dagli attacchi informatici al fine di eliminare le vulnerabilità, si utilizzano le seguenti tecnologie o procedure.

a) Aggiornamenti periodici dei sistemi operativi e dei software di sistema, hardening delle macchine.
b) Adozione di una infrastruttura di sistemi firewall e sistemi IPS (Intrusion Prevention System) che consentono la rilevazione dell'esecuzione di codice non previsto e l'esecuzione di azioni in tempo reale quali il blocco del traffico proveniente da un indirizzo IP attaccante.
c) Esecuzione di WAPT (Web Application Penetration Test), per la verifica della presenza di eventuali vulnerabilità sul codice sorgente.
d) Adozione del captcha sull'applicazione web e di sistemi di rate-limit sui web services che limitano il numero di transazioni nell'unità di tempo, al fine di mitigare il rischio di accesso automatizzato alle applicazioni che genererebbe un traffico finalizzato alla saturazione dei sistemi e quindi al successivo blocco del servizio.

3.6 SISTEMI E SERVIZI DI BACKUP E DISASTER RECOVERY

Non sono previsti sistemi e servizi di backup e disaster recovery per i log di accesso in quanto non necessari per le finalità di trattamento dei dati del servizio. Tali sistemi non sono previsti nemmeno per i dati, in quanto come già indicato nel par. 2.5 il sistema non registra nessun dato. Infatti, poiché il sistema non prevede una banca dati e registra unicamente gli accessi al servizio, la perdita delle informazioni registrate non pregiudica né l'utilizzo né l'efficienza del servizio, in quanto il codice OTP ha durata limitata, non è in alcun modo riconducibile all'interessato, e comunque può essere rigenerato

in qualunque momento dal dispositivo “mobile” per poi essere trasmesso attraverso il servizio.

E’ unicamente previsto il backup dei sistemi.

3.7 SISTEMA DI LOG ANALYSIS APPLICATIVO

Non è previsto un sistema di log analysis applicativo in quanto come indicato nel par. 3.6 non è prevista la registrazione dei dati applicativi.

3.8 ACCESSO AI SISTEMI

L’infrastruttura dispone di sistemi di tracciamento degli accessi ai sistemi informatici di supporto come base dati, server web e infrastrutture a supporto del servizio.

L’accesso alla base dati avviene tramite utenze nominali o riconducibili ad una persona fisica (escluse le utenze di servizio). Il sistema di tracciamento registra (su appositi log) le seguenti informazioni: identificativo univoco dell’utenza che accede, data e ora di login, logout e login falliti, postazione di lavoro utilizzata per l’accesso (IP client), tipo di operazione eseguita sui dati (ad esclusione delle risposte alle query).

Per ogni accesso ai sistemi operativi, ai sistemi di rete, al software di base e ai sistemi complessi, il sistema di tracciamento registra (su appositi log) le seguenti informazioni: identificativo univoco dell’utenza che accede, data e ora di login, logout e login falliti, postazione di lavoro utilizzata per l’accesso (IP client).

I log prodotti dai sistemi di tracciamento infrastrutturali sono soggetti a monitoraggio costante allo scopo di individuare eventuali anomalie inerenti alla sicurezza (accessi anomali, operazioni anomale, ecc.) e di valutare l’efficacia delle misure implementate.

I log di accesso degli Amministratori di sistema e degli incaricati sono protetti da eventuali tentativi di alterazione e dispongono di un sistema di verifica della loro integrità.

I log relativi agli accessi e alle operazioni effettuate sui sistemi operativi, sulla rete, sul software di base e sui sistemi complessi sono conservati per dodici mesi.