ALLEGATO *A*

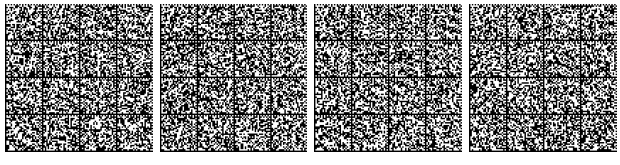
Disciplinare tecnico

Sistema TS: servizi telematici relativi al Piano strategico dei vaccini per la prevenzione delle infezioni da SARS-CoV-2

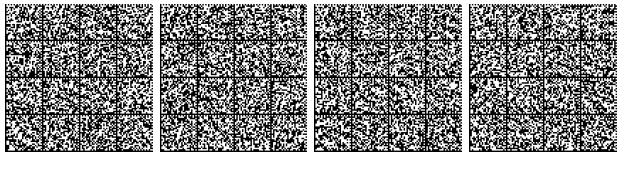
Dati e relativo trattamento

versione 1.2 del 07/04/2021

Art. 20 comma 12 DECRETO-LEGGE 22 marzo 2021, n. 41 (DL Sostegni)



INDICE



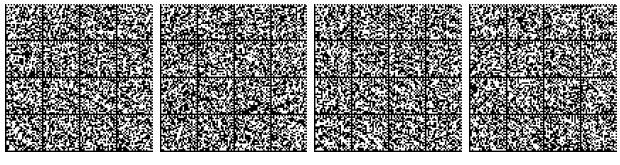
7.4 SISTEMA DI MONITORAGGIO DEL SERVIZIO

7.5 PROTEZIONE DA ATTACCHI INFORMATICI

7.6 SISTEMI E SERVIZI DI BACKUP E DISASTER RECOVERY

7.7 SISTEMA DI LOG ANALYSIS APPLICATIVO

7.8 ACCESSO AI SISTEMI



1. INTRODUZIONE

I soggetti coinvolti nei trattamenti sono le regioni, che si avvalgono dei propri sistemi informatici regionali, oppure della Piattaforma Nazionale (art. 3 DECRETO-LEGGE 14 gennaio 2021, n. 2), se la regione ha chiesto la sussidiarietà.

Il presente documento descrive le modalità tecniche per:

- collegamento degli operatori sanitari a Piattaforme regionali e Piattaforma Nazionale Vaccini mediante l'utilizzo delle credenziali di accesso al Sistema TS. La titolarità dei trattamenti è del MEF in quanto è previsto l'uso del sistema di Identity & Access Management del Sistema TS;
- servizio di interrogazione dell'assistito fuori regione di assistenza, offerto dal Sistema TS verso le Regioni, Province autonome e Piattaforma Nazionale Vaccini. Il MEF è titolare del trattamento ai sensi dell'art. 3, d.l. n. 2/21 e nel rispetto dell'art. 17-bis, comma 2, del D.L. 18/2020;
- flussi da AVN - Anagrafe Nazionale Vaccini verso Sistema TS:
    - trasmissione delle prenotazioni da AVN - Anagrafe Nazionale Vaccini verso Sistema TS
    - trasmissione delle somministrazioni da AVN - Anagrafe Nazionale Vaccini verso Sistema TS
- notifica delle prenotazioni multiple, offerto dal Sistema TS verso le Regioni, Province autonome diverse da quella di assistenza
- servizio di verifica delle somministrazioni, offerto dal Sistema TS verso le Regioni, Province autonome e Piattaforma Nazionale Vaccini

Con riferimento agli ultimi tre servizi il titolare del trattamento è il Ministero della salute che si avvale del MEF in qualità di responsabile del trattamento, ai sensi dell'art. 20, comma 12, del DECRETO-LEGGE 22 marzo 2021, n. 41 (DL Sostegni) e dell'art. 28 del Regolamento (UE) 2016/279.

Le specifiche tecniche dei servizi e le informazioni a supporto dello sviluppo degli stessi saranno pubblicati sul portale del sistema TS www.sistemats.it

2. SERVIZI DI IDENTIFICAZIONE E AUTENTICAZIONE INFORMATICA DEGLI OPERATORI SANITARI

2.1 DESCRIZIONE DEI SERVIZI

Si descrivono di seguito le caratteristiche dei servizi atti ad assicurare l'identificazione e l'autenticazione informatica degli operatori sanitari di cui all'art. 20 comma 2, lettere c) e h) del DL Sostegni, con: piattaforma delle Regioni, piattaforma delle Province autonome e piattaforma Nazionale, mediante l'utilizzo delle credenziali di accesso al medesimo Sistema Tessera Sanitaria, ai fini delle vaccinazioni per la prevenzione delle infezioni da SARS-CoV-2.

Il servizio è rivolto agli operatori sanitari di tutte le regioni e province autonome che si autenticano mediante accesso a Sistema TS e successivamente vengono reindirizzati ai servizi delle varie Piattaforme regionali e nazionali.

2.2 MODALITÀ DI FRUIZIONE

Il servizio di identificazione e autenticazione informatica degli operatori sanitari è reso disponibile in modalità applicazione web.

2.3 ACCESSO AI SERVIZI

Le possibilità di accesso ai servizi 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.

Tabella 1 Modalità di accesso

ID	Utente	Modalità	Autenticazione	Note
1	Operatore Sanitario	Applicazione web	Basic authentication (ID utente e password) con pincode come fattore di autenticazione	L'operatore sanitario accede all'applicazione web tramite le credenziali rilasciate dal Sistema TS.

L'operatore sanitario accede ad una applicazione web resa disponibile sul portale del Sistema TS utilizzando le proprie credenziali rilasciate dal Sistema TS. L'operatore è profilato secondo un profilo dedicato alla prenotazione e somministrazione dei vaccini.

Ciascun utente è già conosciuto e al Sistema TS con la propria collocazione territoriale, per esempio un medico può essere associato ad una o più ASL nelle quali lavora.

All'utente verrà presentata la lista delle ASL nelle quali lavora e che sono associate al suo profilo, con l'aggiunta delle regioni virtuali associate alla Piattaforma Nazionale (es. 300 – Ministero della Difesa). L'utente seleziona la ASL nell'ambito dalla quale effettua il collegamento, oppure, in caso stia lavorando per un luogo lavorativo temporaneo associato all'emergenza sanitaria, seleziona la regione virtuale associata dalla Piattaforma Nazionale. Il codice regione, nell'ambito del servizio di autenticazione offerto dal Sistema TS, viene trasmesso automaticamente dalla Piattaforma Nazionale in relazione alla configurazione della relativa utenza utilizzata in fase di ingresso al servizio e serve ad indicare la regione (anche virtuale) nell'ambito della quale viene fatta la prenotazione e/o la somministrazione Successivamente le regioni e la piattaforma nazionale invieranno nei previsti flussi ad AVN il codice regione utilizzato per la prenotazione e/o la somministrazione.

Una volta instaurata la sessione applicativa, il Sistema TS effettua un reindirizzamento verso il sistema regionale, oppure verso la Piattaforma Nazionale nel caso di scelta delle regioni che utilizzano detto sistema (incluse quelle virtuali). Il reindirizzamento avviene tramite lo standard SAML (Security Assertion Markup Language).

2.4 COMUNICAZIONI DA PARTE DELLE REGIONI/PA

Ciascuna regione/PA, ed anche la piattaforma nazionale, comunica al Sistema TS la volontà di avvalersi del collegamento degli operatori sanitari, e per quali tipologie di utenti (medici, farmacisti, ecc.). Alla partenza del servizio, se la regione non ha chiesto l'accesso degli operatori tramite il Sistema TS, l'accesso sarà inibito. Se la regione richiede l'accesso per i soli medici, il Sistema TS garantirà l'accesso solo per questa tipologia di utenti. Sarà sempre possibile aggiungere o eliminare le tipologie. Per il rilascio delle credenziali si rimanda al paragrafo 7.2

2.5 REGISTRAZIONE DEGLI ACCESSI APPLICATIVI E TEMPI DI CONSERVAZIONE

Il sistema registra gli accessi all'applicazione e l'esito dell'operazione, e inserisce i dati dell'accesso in un archivio dedicato.

Per ciascuna transazione effettuata saranno registrati i seguenti dati relativi all'accesso e all'esito dell'operazione:

- Codice fiscale dell'operatore sanitario che accede al sistema
- data-ora-minuti-secondi-millisecondi dell'accesso
- operazione richiesta
- esito dell'operazione

I log degli accessi così descritti sono conservati per 12 mesi.

3. SERVIZIO DI INTERROGAZIONE DELL'ASSISTITO FUORI REGIONE DI ASSISTENZA

Si descrive di seguito l'interfaccia del servizio esposto alle Regioni/PA e Piattaforma Nazionale, per l'interrogazione dell'assistito fuori regione di assistenza.

3.1 MODALITÀ DI FRUIZIONE

Il servizio descritto di seguito è reso disponibile tramite web service in modalità cooperativa.

3.2 ACCESSO AI SERVIZIO

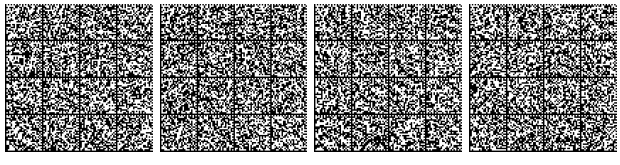
Le possibilità di accesso al servizio sono riassunte nella seguente tabella:

Tabella 2 Modalità di accesso ai servizi

ID	Utente	Modalità	Autenticazione	Note
1	Regioni e Province Autonome attraverso la Piattaforma Nazionale	Web service	Autenticazione con certificato client del sistema chiamante.	
2	Regioni e Province Autonome attraverso i propri sistemi regionali	Web service	Autenticazione con certificato client del sistema chiamante.	

La Regione/PA/Piattaforma Nazionale invoca il servizio esposto da Sistema TS in modalità cooperazione applicativa. Il servizio è esposto in modo sicuro attraverso una autenticazione tramite certificato rilasciato dal Sistema TS. E'possibile richiamare il servizio soltanto da indirizzi IP di provenienza censiti anticipatamente.

Di seguito si descrivono i messaggi di richiesta e di risposta del web service.



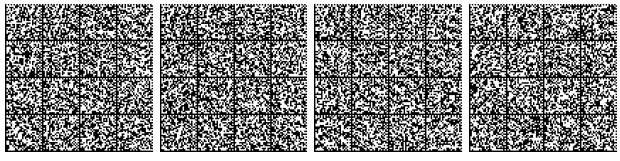
3.3 TRACCIATO DEL SERVIZIO

Il campo di input al servizio è:

Campo	Descrizione	Obbligatorio
codice Fiscale assistito	Il codice fiscale dell'assistito	SI
numero tessera sanitaria	Il numero della tessera sanitaria intestata all'assistito	NO
data scadenza tessera sanitaria	La data di scadenza della tessera sanitaria intestata all'assistito	NO
regione chiamante	Regione che invoca il servizio. Da compilare solo a carico della Piattaforma Nazionale	NO

I campi di output sono:

Campo	Descrizione	Fonte
identificativo transazione	Identificativo transazione (a scopo di controlli tecnici)	Sistema TS
esito	Esito della transazione, può assumere i seguenti valori: **00**: la verifica ha avuto esito positivo e i dati inviati in input sono validati secondo la banca dati del Sistema TS - **01**: la verifica ha avuto esito negativo, pertanto i dati inviati in input non sono coerenti secondo la banca dati del Sistema TS - **02**: la verifica non è stata effettuata. I dati inviati in input non appartengono ad un cittadino fuori regione	Sistema TS
regione di Assistenza	Regione di assistenza del cittadino nota a Sistema TS	Sistema TS
regione di Residenza	Regione di residenza del cittadino. Viene restituita solo se differente dalla regione di assistenza	Sistema TS



descrizione esito	Descrizione dell'esito della transazione	Sistema TS
Identificativo Cluster	Codice del cluster di appartenenza. Viene restituito solo se non esiste una precedente prenotazione o somministrazione.	Sistema TS concordato con gli enti competenti

3.4 ACCESSO AI SERVIZI

La regione/PA/Piattaforma Nazionale si autentica al servizio in mutua autenticazione con certificato client. La trasmissione avviene su canale sicuro TLSV1.2

3.5 REGISTRAZIONE DEGLI ACCESSI APPLICATIVI E TEMPI DI CONSERVAZIONE

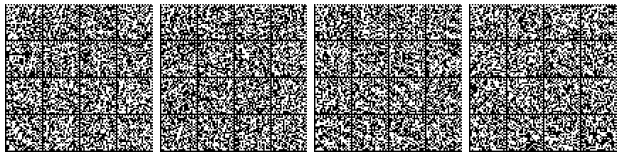
Il sistema registra gli accessi all'applicazione e l'esito dell'operazione, e inserisce i dati dell'accesso in un archivio dedicato.

Per ciascuna transazione effettuata saranno registrati i seguenti dati relativi all'accesso e all'esito dell'operazione:

- Identificativo del chiamante
- Timestamp della richiesta
- Esito della transazione
- Identificativo della transazione
- IP Client
- Codice Fiscale assistito
- Numero Tessera sanitaria (solo nel caso di esito negativo)
- Data di scadenza Tessera (se inviata in input) (solo nel caso di esito negativo)

Numero tessera e data di scadenza sono restituiti solo in caso di esito negativo della transazione, per dare supporto alle regioni in caso di richieste da parte dei cittadini su eventuali mancate prenotazioni.

I log degli accessi così descritti sono conservati per 12 mesi.



4. FLUSSI DATI DA AVN - ANAGRAFE NAZIONALE VACCINI VERSO SISTEMA TS

4.1 TRASMISSIONE DELLE PRENOTAZIONI

4.1.1 MODALITÀ DI FRUIZIONE

Il servizio descritto di seguito è reso disponibile tramite web service in modalità cooperativa, oppure tramite flusso massivo via FTP sicuro.

4.1.2 ACCESSO AI SERVIZI

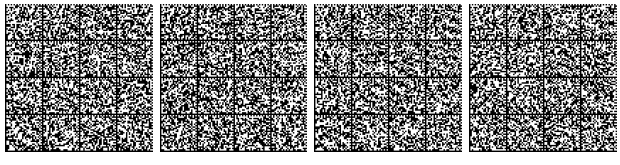
Nel caso di trasmissione dati via web services, l'Anagrafe Nazionale Vaccini si autentica al servizio in mutua autenticazione con certificato client. La trasmissione avviene su canale sicuro TLSV1.2. Nel caso di trasmissione dati via FTP, la comunicazione avviene su VPN end-to-end con cifratura e firma dei dati.

Tabella 3 Modalità di accesso

ID	Utente	Modalità	Autenticazione	Note
1	Anagrafe Nazionale dei Vaccini	Web Services	Autenticazione con certificato client del sistema chiamante.	

L'Anagrafe Nazionale Vaccini invoca il servizio esposto da Sistema TS in modalità cooperazione applicativa. Il servizio è esposto in modo sicuro attraverso una autenticazione tramite certificato rilasciato dal Sistema TS. È possibile richiamare il servizio soltanto da indirizzi IP di provenienza censiti anticipatamente.

Di seguito si descrivono i messaggi di richiesta e di risposta del web service, o dei file trasmessi via FTP.



4.1.3 TRACCIATO DEL SERVIZIO

In caso di utilizzo del web service, la trasmissione è puntuale (singolo assistito), in caso di utilizzo dell'FTP, la trasmissione è massiva (più assistiti).

Il campo di input al servizio è:

Campo	Descrizione	Obbligatorio
Tipo Operazione	Campo tecnico utilizzato per distinguere trasmissioni di informazioni nuove, modificate o eventualmente annullate	SI
Codice Regione	Individua la Regione che trasmette il dato. I valori possibili sono tutti i codici regione ed anche i codici regione virtuali (es. 300 per Ministero della Difesa, da selezionare nel caso in cui l'utente lavora per una sede temporanea di vaccinazione dedicata al Ministero della Difesa (cfr. par. 2.3)).	SI
Identificativo Assistito	Codice identificativo dell'assistito per cui è stata prenotata la somministrazione	SI
Regione di Prenotazione	Regione in cui è stata prenotata la somministrazione	SI
Codice AIC	Codice di autorizzazione immissione in commercio in Italia del vaccino rilasciato dall' AIFA (AIC)	Obbligatorio solo per seconda Dose
Data Prenotazione	Indica la data in cui verrà somministrato il vaccino	SI
Dose	Indica il numero di dose somministrata rispetto al calendario vaccinale per il singolo antigene/principio vaccinale	SI

I campi di output sono:

Campo	Descrizione	Fonte
identificativo transazione	Identificativo transazione (a scopo di controlli tecnici)	Sistema TS
esito	Esito della transazione, può assumere i seguenti valori: **00**: la transazione ha avuto esito positivo - **01**: la transazione ha avuto esito negativo	Sistema TS

4.2 TRASMISSIONE DELLE SOMMINISTRAZIONI

4.2.1 MODALITÀ DI FRUIZIONE

Il servizio descritto di seguito è reso disponibile tramite web service in modalità cooperativa.

4.2.2 ACCESSO AI SERVIZI

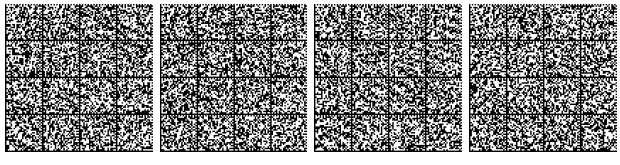
L'Anagrafe Nazionale Vaccini si autentica al servizio in mutua autenticazione con certificato client. La trasmissione avviene su canale sicuro TLSV1.2

Tabella 4 Modalità di accesso

ID	Utente	Modalità	Autenticazione	Note
1	Anagrafe Nazionale dei Vaccini	Web Services	Autenticazione con certificato client del sistema chiamante.	

L'Anagrafe Nazionale Vaccini invoca il servizio esposto da Sistema TS in modalità cooperazione applicativa. Il servizio è esposto in modo sicuro attraverso una autenticazione tramite certificato rilasciato dal Sistema TS. È possibile richiamare il servizio soltanto da indirizzi IP di provenienza censiti anticipatamente.

Di seguito si descrivono i messaggi di richiesta e di risposta del web service.



4.2.3 TRACCIATO DEL SERVIZIO

La trasmissione è puntuale (singolo assistito) in quanto si utilizza un web service.

Il campo di input al servizio è:

Campo	Descrizione	Obbligatorio
Tipo Operazione	Campo tecnico utilizzato per distinguere trasmissioni di informazioni nuove, modificate o eventualmente annullate	SI
Codice Regione	Individua la Regione che trasmette il dato. I valori possibili sono tutti i codici regione ed anche i codici regione virtuali (es. 300 per Ministero della Difesa, da selezionare nel caso in cui l'utente lavora per una sede temporanea di vaccinazione dedicata al Ministero della Difesa (cfr. par. 2.3)).	SI
Identificativo Assistito	Codice identificativo dell'assistito a cui è stato somministrato il vaccino	SI
Regione di Somministrazione	Individua la regione dove è stata effettuata la somministrazione	SI
Codice AIC	Codice di autorizzazione immissione in commercio in Italia del vaccino rilasciato dall' AIFA (AIC)	SI
Data Somministrazione	Indica la data di somministrazione del vaccino	SI
Dose	Indica il numero di dose somministrata rispetto al calendario vaccinale per il singolo antigene/principio vaccinale	SI

I campi di output sono:

Campo	Descrizione	Fonte
identificativo transazione	Identificativo transazione (a scopo di controlli tecnici)	Sistema TS
esito	Esito della transazione, può assumere i seguenti valori: **00**: la transazione ha avuto esito positivo - **01**: la transazione ha avuto esito negativo	Sistema TS

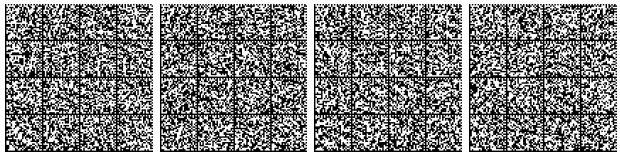
4.3 REGISTRAZIONE DEGLI ACCESSI APPLICATIVI E TEMPI DI CONSERVAZIONE

Il sistema registra gli accessi all'applicazione e l'esito dell'operazione, e inserisce i dati dell'accesso in un archivio dedicato.

Per ciascuna transazione effettuata saranno registrati i seguenti dati relativi all'accesso e all'esito dell'operazione:

- Identificativo del chiamante
- Timestamp della richiesta
- Esito della transazione
- Identificativo della transazione
- IP Client

I log degli accessi così descritti sono conservati per 12 mesi.



5. NOTIFICA DELLE PRENOTAZIONI MULTIPLE

5.1 DESCRIZIONE DEL FLUSSO

Si descrive di seguito il flusso necessario alla notifica delle prenotazioni multiple per lo stesso cittadino, offerto dal Sistema TS, verso le Regioni e Province autonome diverse da quella di assistenza

5.2 MODALITÀ DI FRUIZIONE

Il servizio di ricezione dei dati è reso disponibile in modalità applicazione web per Regioni/PA. La modalità web è erogata su canale sicuro TLSv1.2.

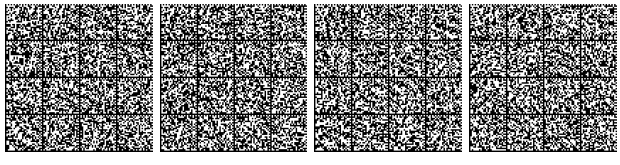
5.3 ACCESSO AI SERVIZI

Le possibilità di accesso ai servizi 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.

Tabella 5 Modalità di accesso

ID	Utente	Modalità	Autenticazione	Note
1	Operatore Regione/PA	Applicazione web	Basic authentication (ID utente e password)	L'operatore della Regione/PA incaricato accede all'applicazione web tramite le credenziali rilasciate dal Sistema TS.

Per le Regioni/PA l'utente accede ad una applicazione web resa disponibile sul portale del Sistema TS utilizzando le proprie credenziali rilasciate dal Sistema TS. Nello specifico, le credenziali vengono rilasciate dall'amministratore di sicurezza incaricato da Regioni/PA tramite il Sistema TS.



5.4 TRACCIATO ELENCO PRENOTAZIONI MULTIPLE

Di seguito si descrive il tracciato del file che l'operatore della Regione/PA può scaricare tramite la funzionalità (applicazione web) "Scambio File" già in uso nel Sistema TS.

Tabella 6 Tracciato file

Campo	Descrizione	Obbligatorio
Codice Fiscale	Codice fiscale del cittadino	Obbligatorio
Codice regione/SASN che eroga l'assistenza	Codice regione/SASN che eroga l'assistenza sanitaria	Obbligatorio
Numero prenotazioni effettuate	Numero totale di prenotazioni multiple	Obbligatorio
Elenco regioni di prenotazione diverse da quella di assistenza	Lista delle regioni dove è stata effettuata la prenotazione diverse da quella di assistenza	Obbligatorio

5.5 REGISTRAZIONE DELLE TRASMISSIONI E TEMPI DI CONSERVAZIONE

Il sistema registra l'esito, durata e data della trasmissione, e inserisce i dati dell'accesso in un archivio dedicato.

Per ciascuna trasmissione effettuata saranno registrati i seguenti dati:

- ente verso il quale è stata effettuata la trasmissione
- operatore che effettuato il download della fornitura
- data-ora-minuti-secondi-millisecondi della trasmissione
- esito della trasmissione
- durata della trasmissione

I log degli accessi così descritti sono conservati per 12 mesi.

6. SERVIZIO DI VERIFICA DELLE SOMMINISTRAZIONI

Si descrive di seguito l'interfaccia del servizio esposto alle Regioni/PA e Piattaforma Nazionale. La finalità del servizio è la verifica dell'avvenuta somministrazione per i singoli assistiti, per assicurare l'appropriatezza di una successiva somministrazione ai medesimi.

6.1 MODALITÀ DI FRUIZIONE

Il servizio descritto di seguito è reso disponibile tramite web service in modalità cooperativa.

6.2 ACCESSO AI SERVIZIO

Le possibilità di accesso al servizio sono riassunte nella seguente tabella:

Tabella 7 Modalità di accesso ai servizi

ID	Utente	Modalità	Autenticazione	Note
1	Regioni e Province Autonome attraverso la Piattaforma Nazionale	Web service	Autenticazione con certificato client del sistema chiamante.	
2	Regioni e Province Autonome attraverso i propri sistemi regionali	Web service	Autenticazione con certificato client del sistema chiamante.	

La Regione/PA/Piattaforma Nazionale invoca il servizio esposto da Sistema TS in modalità cooperazione applicativa. Il servizio è esposto in modo sicuro attraverso una autenticazione tramite certificato rilasciato dal Sistema TS. E' possibile richiamare il servizio soltanto da indirizzi IP di provenienza censiti anticipatamente.

Di seguito si descrivono i messaggi di richiesta e di risposta del web service.

6.3 TRACCIATO DEL SERVIZIO

Il campo di input al servizio è:

Campo	Descrizione	Obbligatorio
codice Fiscale assistito	Il codice fiscale dell'assistito	SI
numero Tessera Sanitaria assistito	Il numero di tessera sanitaria dell'assistito	Dipende dal contesto organizzativo regionale: **NO**, solo durante fasi elaborative automatiche in cui la regione non disporrebbe ditale dato perché non presente nelle anagrafiche regionali. **SI**, il numero identificativo dellaTessera Sanitaria dell'assistito deve ritenersi obbligatorio nei casi in cui il predetto serviziosia utilizzato nell'ambito di transazioni che prevedano il coinvolgimento di una personafisica (assistito/operatore).

I campi di output sono:

Campo	Descrizione	Fonte
identificativo transazione	Identificativo transazione (a scopo di controlli tecnici)	Sistema TS
esito	Esito della transazione, può assumere i seguenti valori: **00**: la verifica ha avuto esito positivo e i dati inviati in input sono validati secondo la banca dati del Sistema TS - **01**: la verifica ha avuto esito negativo, pertanto i dati inviati in input non sono coerenti secondo la banca dati del Sistema TS	Sistema TS

Data Somministrazione*	Data della somministrazione	AVN
Numero Dose*	Progressivo della dose	AVN
Codice AIC*	Codice AIC della somministrazione	AVN
Regione di Somministrazione*	Regione dove è stata effettuata la somministrazione	AVN

(*) i campi si ripetono, si tratta di una lista

6.4 ACCESSO AI SERVIZI

La regione/PA/Piattaforma Nazionale si autentica al servizio in mutua autenticazione con certificato client. La trasmissione avviene su canale sicuro TLSV1.2

6.5 REGISTRAZIONE DEGLI ACCESSI APPLICATIVI E TEMPI DI CONSERVAZIONE

Il sistema registra gli accessi all'applicazione e l'esito dell'operazione, e inserisce i dati dell'accesso in un archivio dedicato.

Per ciascuna transazione effettuata saranno registrati i seguenti dati relativi all'accesso e all'esito dell'operazione:

- Identificativo del chiamante
- Timestamp della richiesta
- Esito della transazione (solo se l'esito è negativo, al fine di poter verificare il motivo di errore di una transazione)
- Identificativo della transazione
- IP Client
- Codice Fiscale assistito

I log degli accessi così descritti sono conservati per 12 mesi.

7. MISURE DI SICUREZZA

7.1 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 dall'ordinanza di cui al titolo del presente documento.

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.

7.2 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 degli operatori sanitari avviene con le credenziali rilasciate dal Sistema TS oppure tramite certificato rilasciato alla piattaforma regionale.

7.3 CANALI DI COMUNICAZIONE

Le comunicazioni sono scambiate in modalità sicura su rete 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).

7.4 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 per il corretto funzionamento del Sistema. Il sistema offre funzioni per visualizzare i dati aggregati come il numero di prenotazioni e di vaccini trasmessi al Sistema TS, ed anche il numero di interrogazioni fatte verso il Sistema TS. L'aggregazione può essere fatta per regione di prenotazione o di somministrazione, o di interrogazione, ed anche in un intervallo temporale. La finalità è fornire il monitoraggio dell'utilizzo del sistema, ed anche eventuali usi impropri dello stesso, per esempio è possibile monitorare il numero di chiamate giornaliere o settimanali al servizio, che deve essere proporzionato al numero di assistiti presenti nella regione chiamante, Il controllo può essere effettuato sia sulla regione chiamante, che sull'indirizzo IP di provenienza.

7.5 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 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.

7.6 SISTEMI E SERVIZI DI BACKUP E DISASTER RECOVERY

E' previsto il backup dei log di sistema, e il disaster recovery dei log di accesso, ed anche il disaster recovery della base dati.

7.7 SISTEMA DI LOG ANALYSIS APPLICATIVO

Non è previsto un sistema di log analysis applicativo in quanto l'alimentazione della banca dati avviene da un unico canale (AVN del Ministero della Salute) ed è quindi facilmente controllabile. Invece, per quanto riguarda gli accessi da parte delle regioni, le interrogazioni sono tracciate come accessi al sistema, ed il controllo si effettua in fase di monitoraggio sull'utilizzo dei servizi (par. 7.4). Il monitoraggio assolve quindi anche alla funzione di analisi di eventuali usi impropri del sistema.

7.8 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.

21A03613