

Specifiche tecniche

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

Dati e relativo trattamento

Ordinanza n. 2 del 9/2/2021

INDICE

1.	VERSIONI DEL DOCUMENTO	4
2.	INTRODUZIONE	5
3.	CATEGORIE DI ELEGGIBILI	6
4.	SERVIZIO PER L'ACQUISIZIONE DEI DATI PER LA PREDISPOSIZIONE DEGLI ELENCHI DEGLI APPARTENENTI ALLE CATEGORIE DI ASSISTITI ELEGGIBILI	7
4.1	DESCRIZIONE DEL SERVIZIO	7
5.	FLUSSI DATI DAL SISTEMA TS VERSO LE REGIONI/PA	10
5.1	DESCRIZIONE DEI FLUSSI	10
5.2	TRASMISSIONE DEGLI ELENCHI DEGLI ELEGGIBILI	10
5.2.1	MODALITÀ DI FRUIZIONE	10
5.2.2	ACCESSO AI SERVIZI	10
5.2.3	TRACCIATO ELENCO DEGLI ELEGGIBILI PER FASCIA DI ETÀ	11
5.2.4	TRACCIATO ELENCO DEGLI ELEGGIBILI PER CATEGORIE PARTICOLARI	13
5.2.5	REGISTRAZIONE DELLE TRASMISSIONI E TEMPI DI CONSERVAZIONE	15
5.3	SERVIZIO DI INTERROGAZIONE DELL'ASSISTITO FUORI REGIONE DI ASSISTENZA/SERVIZIO	16
6.	MISURE DI SICUREZZA	17
6.1	INFRASTRUTTURA FISICA	17
6.2	REGISTRAZIONE DEGLI UTENTI ED ASSEGNAZIONE DEGLI STRUMENTI DI SICUREZZA	17
6.3	CANALI DI COMUNICAZIONE	17
6.4	SISTEMA DI MONITORAGGIO DEL SERVIZIO	18

6.5	PROTEZIONE DA ATTACCHI INFORMATICI	18
6.6	SISTEMI E SERVIZI DI BACKUP E DISASTER RECOVERY	18
6.7	SISTEMA DI LOG ANALYSIS APPLICATIVO	19
6.8	ACCESSO AI SISTEMI	19

1. VERSIONI DEL DOCUMENTO

Versione	Data modifica	Descrizione
1.0	01/03/2021	Prima versione del documento.

2. INTRODUZIONE

Il presente documento descrive le modalità tecniche per:

- l’acquisizione, da parte del Sistema TS, dalle amministrazioni e dagli enti interessati, statali e regionali, dei dati necessari per predisporre gli elenchi degli appartenenti alle categorie degli assistiti eleggibili per le vaccinazioni per la prevenzione delle infezioni da SARS-CoV-2 (art. 1, lettera a) della presente Ordinanza)
- i flussi dei dati da Sistema TS verso le regioni/PA (art. 1, lettera b) della presente Ordinanza):
 - elaborazione da parte del Sistema TS degli elenchi degli eleggibili per le vaccinazioni per la prevenzione delle infezioni da SARS-CoV-2, e loro successiva trasmissione verso le regioni/PA
 - servizio di interrogazione dell’assistito fuori regione di assistenza, offerto dal Sistema TS alle regioni/PA

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

3. CATEGORIE DI ELEGGIBILI

Si fa riferimento alle categorie del Piano vaccinale del Ministero della Salute:

<http://www.salute.gov.it/portale/nuovocoronavirus/dettaglioNotizieNuovoCoronavirus.jsp?lingua=italiano&menu=notizie&p=dalministero&id=5319>

4. SERVIZIO PER L'ACQUISIZIONE DEI DATI PER LA PREDISPOSIZIONE DEGLI ELENCHI DEGLI APPARTENENTI ALLE CATEGORIE DI ASSISTITI ELEGGIBILI

4.1 DESCRIZIONE DEL SERVIZIO

Si descrive di seguito il servizio di acquisizione e elaborazione dei dati forniti dalle amministrazioni e dagli enti interessati, statali e regionali, per predisporre gli elenchi degli appartenenti alle categorie degli assistiti eleggibili per le vaccinazioni per la prevenzione delle infezioni da SARS-CoV-2.

Le categorie saranno individuate in base a vari fattori, per esempio l'andamento dell'epidemia COVID-19 e la disponibilità dei vaccini, e le amministrazioni ed enti interessati forniranno i dati utili alla predisposizione degli elenchi di assistiti eleggibili.

4.2 MODALITA' DI INVIO DEI DATI AL SISTEMA TS

Le amministrazioni e gli enti interessati, statali e regionali, inviano i dati al Sistema TS con una delle seguenti modalità:

- applicazione web di Scambio File, già presente sul Sistema TS, previa autenticazione dell'utente
- web service di Scambio File, con autenticazione dell'ente con certificato client su canale TLSv1.2
- FTP su VPN end-to-end con cifratura e firma dei dati
- PEC all'indirizzo info@pec.sistemats.it
- Consegna a mano ad un incaricato del trattamento su supporto magnetico o ottico con i dati protetti da password
- Accesso con credenziali (rilasciate a incaricato del trattamento) alla piattaforma informatica dell'Amministrazione/Ente

4.3 ACCESSO AL SERVIZIO

Nel caso di applicazione web, l'utente dell'ente che trasmette i dati accede con le credenziali del Sistema TS e profilato per questo servizio. Nel caso di web service, l'accesso viene fatto dall'ente che si autentica con certificato client. Nel caso di FTP, l'ente viene preventivamente censito ed autorizzato dal Sistema TS allo scambio file.

4.4 TRACCIATO DEL SERVIZIO

Di seguito si descrive il tracciato dei dati che le Amministrazioni forniscono al Sistema TS.

4.4.1 TRACCIATO

I dati utili alla definizione di un elenco di eleggibili sono riportati nella seguente tabella.

Campo	Descrizione	Obbligatorio
Codice fiscale	Codice fiscale del soggetto eleggibile	Obbligatorio
Codice regione di servizio	Codice regione di servizio del soggetto (sede di lavoro, sede di riferimento)	Obbligatorio
Codice categoria	Amministrazione o ente di appartenenza	Obbligatorio
Numero di telefono	Numero di telefono della sede di lavoro	Obbligatorio se disponibile presso l'amministrazione/ente
email	Email della sede di lavoro	Obbligatorio se disponibile presso l'amministrazione/ente

4.4.2 ELABORAZIONE DEI DATI

Il Sistema TS acquisisce i dati e li elabora per predisporre gli elenchi degli appartenenti alle categorie degli assistiti eleggibili per le vaccinazioni per la prevenzione delle infezioni da SARS-CoV-2. In particolare, verifica la presenza dei codici fiscali in banca dati e scarta quelli non trovati. **Per i codici fiscali non trovati verrà fornito un riscontro all'Amministrazione/Ente. Anche in caso di**

dati mancanti (rispetto al tracciato) verrà fornito un riscontro all'Amministrazione/Ente.

4.5 *REGISTRAZIONE DEI DATI E TEMPI DI CONSERVAZIONE*

I dati acquisiti dal Sistema TS vengono conservati nella banca dati Sistema TS per il tempo strettamente necessario alle finalità della presente ordinanza, e comunque entro e non oltre 12 mesi.

Ne consegue che codici fiscali per cui non è stato possibile trovare un abbinamento sulla banca dati degli assistiti, sono immediatamente eliminati dalla banca dati del Sistema TS unitamente ai soggetti che risultano deceduti o emigrati in base ai dati del Sistema TS.

5. FLUSSI DATI DAL SISTEMA TS VERSO LE REGIONI/PA

5.1 DESCRIZIONE DEI FLUSSI

Si descrivono di seguito i flussi necessari alla trasmissione dei dati da parte del Sistema TS alle regioni/PA.

5.2 TRASMISSIONE DEGLI ELENCHI DEGLI ELEGGIBILI

5.2.1 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.

5.2.2 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 Regione/PA	Applicazione web	Basic authentication (ID utente e password) con pincode come fattore di autenticazione	L'operatore della Regione/PA incaricato accede all'applicazione web tramite le credenziali rilasciate dal Sistema TS.

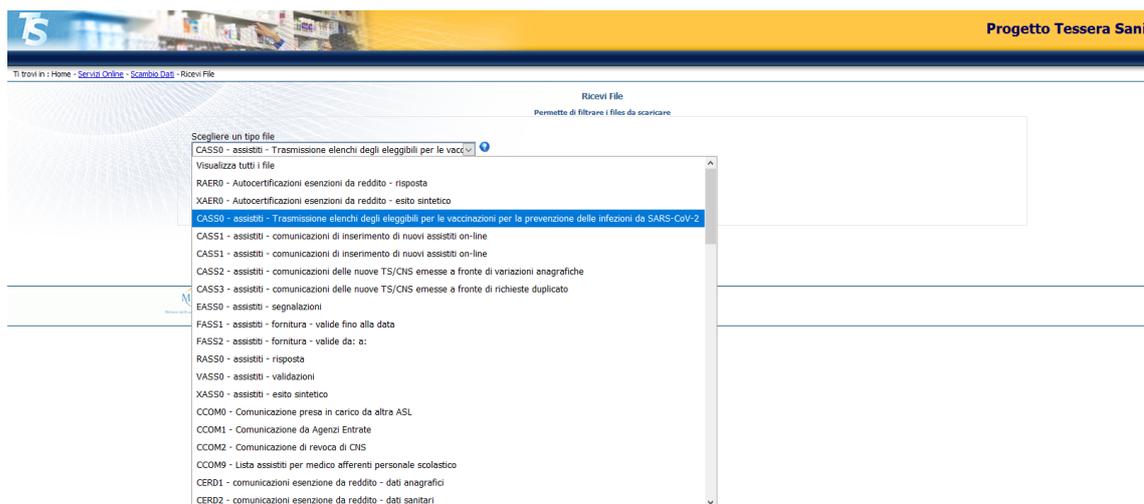
Per le Regioni/PA l'utente accede ad una applicazione web resa disponibile sul portale del Sistema TS utilizzando le proprie credenziali rilasciate dal Sistema TS. Nello specifico, le credenziali vengono rilasciate dall'amministratore di sicurezza incaricato da Regioni/PA tramite il Sistema TS.

5.2.3 TRACCIATO ELENCO DEGLI ELEGGIBILI PER FASCIA DI ETÀ

Questo tracciato viene fornito alle regioni/PA di assistenza ed è prodotto in base alle informazioni presenti nel Sistema TS.

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

Di seguito si riporta la schermata dell'applicazione:



Viene prodotto un file posizionale di tipo txt. Se un campo non è valorizzato, conterrà dei caratteri "spazio".

Il nome del file prodotto è:

`"CASS0RCCC0000000000YYYYMMDD0101--CKKKKK--00000000YYMMDDHHMISS.TXT"`

dove:

CCC = codice regione di destinazione

YYYYMMDD = data di produzione del file

KKKKK = Codice del cluster di appartenenza (es. 00001)

YYMMDDHHMISS = timestamp in questo formato

La lunghezza record dei file (uno per regione) è di **24 byte** ed il loro tracciato record è il seguente:

Progressivo campo	Posizione	Lunghezza	Descrizione del campo	Tipologia	Note
1.	1 - 16	16	Codice fiscale del cittadino	AN	Obbligatorio
2.	17 - 19	3	Codice regione di assistenza	AN	Obbligatorio
3.	20 - 24	5	Codice del cluster (categoria di eleggibili) di appartenenza	AN	Obbligatorio

La decodifica del campo 2 è la seguente:

- 001 SASN CENTRALE
- 010 Piemonte
- 020 Val d'Aosta
- 030 Lombardia
- 041 Bolzano - P. A.
- 042 Trento - P.A.
- 050 Veneto
- 060 Friuli Venezia Giulia
- 070 Liguria
- 080 Emilia Romagna
- 090 Toscana
- 100 Umbria
- 110 Marche
- 120 Lazio
- 130 Abruzzo
- 140 Molise
- 150 Campania
- 160 Puglia
- 170 Basilicata
- 180 Calabria
- 190 Sicilia

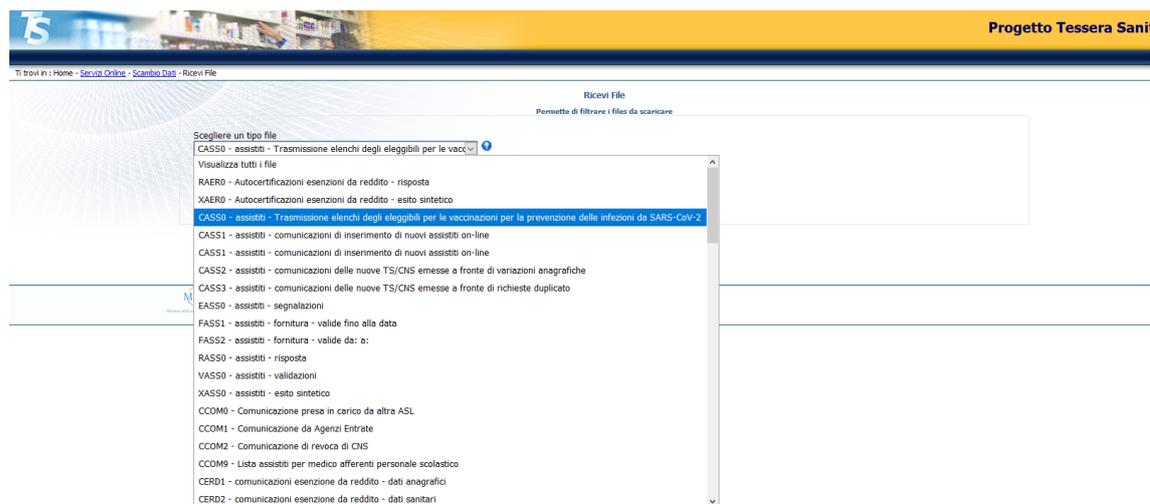
La decodifica del campo 3 è riportata in un documento tecnico a corredo di questa specifica.

5.2.4 TRACCIATO ELENCO DEGLI ELEGGIBILI PER CATEGORIE PARTICOLARI

Questo tracciato viene fornito alle regioni/PA di servizio a seguito della fornitura dei dati descritti nel par. 2, che viene utilizzata per individuare particolari categorie di eleggibili.

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

Di seguito si riporta la schermata dell'applicazione:



Viene prodotto un file posizionale di tipo txt. Se un campo non è valorizzato, conterrà dei caratteri "spazio".

Il nome del file prodotto è:

"CASS0RCCC0000000000YYYYMMDD0101--CKKKKK--00000000YYMMDDHHMISS.TXT".

dove:

CCC = codice regione di destinazione

YYYYMMDD = data di produzione del file

KKKKK = Codice del cluster di appartenenza (es. 00001)

YYMMDDHHMISS = timestamp in questo formato

La lunghezza record dei file (uno per regione) è di **77 byte** ed il loro tracciato record è il seguente:

Progressivo campo	Posizione	Lunghezza	Descrizione del campo	Tipologia	Note
1.	1 - 16	16	Codice fiscale del cittadino	AN	Obbligatorio
2.	17 - 19	3	Codice regione di assistenza	AN	Obbligatorio
3.	20 - 24	5	Codice del cluster (categoria di eleggibili) di appartenenza	AN	Obbligatorio
4.	25 - 27	3	Codice regione della sede di servizio	AN	Obbligatorio
5.	28 - 47	20	Numero di telefono della sede di servizio	AN	Obbligatorio se fornito dall'Amministrazione/Ente
6.	48 - 77	30	Email della sede di servizio	AN	Obbligatorio se fornito dall'Amministrazione/Ente

La decodifica dei campi 2 e 4 è la seguente:

001 SASN CENTRALE (solo assistenza)

010 Piemonte

020 Val d'Aosta

030 Lombardia

041 Bolzano - P. A.

042 Trento - P.A.

050 Veneto

060 Friuli Venezia Giulia

070	Liguria
080	Emilia Romagna
090	Toscana
100	Umbria
110	Marche
120	Lazio
130	Abruzzo
140	Molise
150	Campania
160	Puglia
170	Basilicata
180	Calabria
190	Sicilia
200	Sardegna

La decodifica del campo 3 è riportato in un documento tecnico a corredo di questa specifica.

5.2.5 *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
- data-ora-minuti-secondi-millisecondi della trasmissione
- esito della trasmissione
- durata della trasmissione

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

5.3 *SERVIZIO DI INTERROGAZIONE DELL'ASSISTITO FUORI REGIONE DI ASSISTENZA/SERVIZIO*

Le specifiche tecniche del servizio sono riportate in un documento a parte.

6. MISURE DI SICUREZZA

6.1 *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.

6.2 *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 le credenziali rilasciate dal Sistema TS oppure tramite certificato rilasciato alla piattaforma regionale.

6.3 *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).

6.4 *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.

6.5 *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.

6.6 *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.

E' unicamente previsto il backup dei sistemi.

6.7 *SISTEMA DI LOG ANALYSIS APPLICATIVO*

Non è previsto un sistema di log analysis applicativo in quanto non è prevista la registrazione dei dati applicativi.

6.8 *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.