

*Documento tecnico*

*Sistema TS: servizi telematici*

*Dati e relativo trattamento*

## INDICE

<b>1.</b>	<b>INTRODUZIONE</b>	<b>5</b>
<b>2.</b>	<b>SERVIZI PER LA COMUNICAZIONE DEI ESITI DEI TAMPONI ESEGUITI DA PARTE DELLE REGIONI O DELLE STRUTTURE</b>	<b>6</b>
2.1	DESCRIZIONE DEI SERVIZI	6
2.2	MODALITÀ DI FRUIZIONE	6
2.3	ACCESSO AI SERVIZI	6
2.4	TRACCIATI DEI SERVIZI	8
2.4.1	SERVIZIO DI INVIO ESECUZIONE TEST	8
2.4.2	SERVIZIO DI ANNULLAMENTO ESECUZIONE TEST	10
2.4.3	SERVIZIO DI ELENCO TEST EFFETTUATI	11
2.5	REGISTRAZIONE DEGLI ACCESSI APPLICATIVI E TEMPI DI CONSERVAZIONE	13
<b>3.</b>	<b>SERVIZI PER IL CALL CENTER</b>	<b>15</b>
3.1	DESCRIZIONE DEI SERVIZI	15
3.2	MODALITÀ DI FRUIZIONE	15
3.3	ACCESSO AI SERVIZI	15
3.3.1	SERVIZIO VERIFICA POSITIVITÀ	16
3.3.2	SERVIZIO DI SBLOCCO CODICE IMMUNI	17
3.3.3	SERVIZIO DI CONFERMA SBLOCCO IMMUNI	18
3.4	REGISTRAZIONE DEGLI ACCESSI WEB SERVICES E TEMPI DI CONSERVAZIONE	19
<b>4.</b>	<b>MODALITÀ DI AUTENTICAZIONE DEGLI OPERATORI DEL CALL CENTER</b>	<b>22</b>

4.1	TRACCIATO DEL SERVIZIO	23
4.2	REGISTRAZIONE DEGLI ACCESSI APPLICATIVI E TEMPI DI CONSERVAZIONE	25
4.3	MISURE DI SICUREZZA	25
4.3.1	INFRASTRUTTURA FISICA	25
4.3.2	REGISTRAZIONE DEGLI UTENTI ED ASSEGNAZIONE DEGLI STRUMENTI DI SICUREZZA	26
4.3.3	CANALI DI COMUNICAZIONE	26
4.3.4	SISTEMA DI MONITORAGGIO DEL SERVIZIO	26
4.3.5	PROTEZIONE DA ATTACCHI INFORMATICI	27
4.3.6	SISTEMI E SERVIZI DI BACKUP E DISASTER RECOVERY	27
4.3.7	SISTEMA DI LOG ANALYSIS APPLICATIVO	27
4.3.8	ACCESSO AI SISTEMI	27
<b>5.</b>	<b>MODIFICHE PER IL SERVIZIO INVIO CODICE OTP DA PARTE DELLA ASL</b>	<b>29</b>
5.1	TRACCIATO DEL SERVIZIO	29
5.2	REGISTRAZIONE DEGLI ACCESSI APPLICATIVI E TEMPI DI CONSERVAZIONE	30
<b>6.</b>	<b>MISURE DI SICUREZZA</b>	<b>31</b>
6.1	INFRASTRUTTURA FISICA	31
6.2	REGISTRAZIONE DEGLI UTENTI ED ASSEGNAZIONE DEGLI STRUMENTI DI SICUREZZA	31
6.3	CANALI DI COMUNICAZIONE	31
6.4	SISTEMA DI MONITORAGGIO DEL SERVIZIO	32
6.5	PROTEZIONE DA ATTACCHI INFORMATICI	32
6.6	SISTEMI E SERVIZI DI BACKUP E DISASTER RECOVERY	32
6.7	SISTEMA DI LOG ANALYSIS APPLICATIVO	33



## **1. INTRODUZIONE**

Il presente documento descrive le modalità tecniche per:

- La trasmissione al Sistema TS, da parte delle strutture sanitarie dei dati relativi all'esecuzione dei tamponi per i cittadini. Le specifiche tecniche dei servizi e le informazioni a supporto dello sviluppo degli stessi saranno pubblicati sul portale del sistema TS [www.sistemats.it](http://www.sistemats.it)
- Le modalità di verifica e sblocco OTP, rese disponibili dal Sistema TS agli operatori del call center Immuni, per i soli esiti positivi rispetto ai tamponi
- Le modalità di autenticazione e di autorizzazione degli operatori del call center Immuni

## **2. SERVIZI PER LA COMUNICAZIONE DEI ESITI DEI TAMPONI ESEGUITI DA PARTE DELLE REGIONI O DELLE STRUTTURE**

### **2.1 DESCRIZIONE DEI SERVIZI**

Si descrivono di seguito le funzionalità necessarie alla trasmissione al Sistema TS dei dati relativi ai tamponi somministrati da parte delle strutture sanitarie. Per le regioni che sono dotate di una piattaforma regionale che raccoglie i dati inviati dalle strutture, è prevista l'autenticazione in modalità SAR (vedi paragrafo 2.3)

### **2.2 MODALITÀ DI FRUIZIONE**

I servizi descritti di seguito sono resi disponibili in modalità cooperativa tramite web service.

### **2.3 ACCESSO AI SERVIZI**

Le possibilità di accesso ai servizi da parte delle regioni o delle strutture sanitarie sono riassunte nella seguente tabella:

Tabella 1 Modalità di accesso ai servizi di comunicazione test per la struttura

ID	Utente	Modalità	Autenticazione	Note
1	Regione	Web service	Mutua autenticazione con certificato client	<p>L'operatore si connette al sistema regionale che a sua volta invoca il servizio tramite client applicativo. In alternativa la piattaforma regionale fa da raccogliitore dei dati per conto delle strutture e invia i dati al Sistema TS.</p> <p>Certificato di autenticazione rilasciato dal Sistema TS.</p> <p>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.</p>
2	Operatore della struttura	Web service	basic authentication (ID utente e password) con pincode come fattore di autenticazione	<p>L'operatore della struttura invoca il servizio tramite software gestionale.</p> <p>Credenziali di autenticazione rilasciate dal Sistema TS.</p>

La modalità 1 si rivolge alle regioni e alle province autonome di Trento e Bolzano, che sono gli intermediari che colloquiano con il Sistema TS e che permettono la comunicazione dei dati da parte delle strutture sanitarie. L'operatore sanitario della struttura (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 documento. Il sistema regionale deve garantire i requisiti minimi di sicurezza adottati dal Sistema TS in termini di autenticazione forte.

La modalità 2 si rivolge alla struttura che tramite un software gestionale sviluppato ad hoc si connette al servizio utilizzando le proprie credenziali rilasciate dal Sistema TS.

## 2.4 TRACCIATI DEI SERVIZI

Di seguito si descrivono i messaggi di richiesta e di risposta dei servizi, validi per la modalità web service.

### 2.4.1 SERVIZIO DI INVIO ESECUZIONE TEST

Con questo servizio la piattaforma regionale ovvero la singola struttura sanitaria comunica al Sistema TS l'esito relativo alla somministrazione del tampone. Il Sistema TS restituisce in risposta il codice univoco nazionale (CUN) associato all'esito.

Tabella 2 Servizio di invio esecuzione test - messaggio di richiesta

Campo	Descrizione	Obbligatorio
<b>Identificativo struttura Sistema TS</b>	Identificativo della struttura che ha eseguito il tampone secondo la codifica di Sistema TS ovvero codice regione-codice asl-codice struttura.	NO <ul style="list-style-type: none"><li>- Nel caso di invio diretto dalla struttura, il campo è obbligatorio</li><li>- Nel caso di invio da una piattaforma regionale, il campo è in alternativa con il campo "Descrizione struttura"</li></ul>
<b>Descrizione struttura</b>	Nel caso di invio dei dati dalla piattaforme regionali che non hanno un sistema di codifica delle strutture integrato con Sistema TS oppure nel caso di strutture non censite nel Sistema TS, in questo campo si può specificare una descrizione testuale della struttura (massima lunghezza 256)	NO <ul style="list-style-type: none"><li>- Nel caso di invio diretto dalla struttura, il campo non va valorizzato</li><li>- Nel caso di invio da una piattaforma regionale, il campo è in alternativa con il campo "Identificativo struttura Sistema TS"</li></ul>
<b>Codice fiscale assistito</b>	Il codice fiscale dell'assistito	SI



Campo	Descrizione	Obbligatorio
<b>Data prelievo</b>	Data in cui è stato eseguito il prelievo	SI
<b>Tipologia test</b>	Tipologia del test eseguito (valorizzare a 'M' per tampone molecolare)	SI
<b>Esito test</b>	Esito del test positivo/negativo	SI
<b>Numero di cellulare</b>	Numero di cellulare dell'assistito	NO Può essere valorizzato solo uno tra i campi Numero di cellulare o Contatto Email
<b>Contatto email</b>	Email dell'assistito	NO Può essere valorizzato solo uno tra i campi Numero di cellulare o Contatto Email

Tabella 3 Servizio di invio esecuzione test - messaggio di risposta

Campo	Descrizione	Fonte
<b>Identificativo transazione</b>	Identificativo della transazione, generato dal sistema. Tale numero rappresenta il <b>CUN</b> (codice univoco nazionale) che identifica il test a livello nazionale.	Sistema TS
<b>Data-ora</b>	Data-ora-minuti-secondi-millisecondi in cui si è conclusa la transazione	Sistema TS
<b>Esito</b>	Esito della transazione	Sistema TS
<b>Descrizione esito</b>	Descrizione dell'esito della transazione	Sistema TS

#### 2.4.1.1 CUN codice univoco nazionale

Il campo CUN (codice univoco nazionale) rappresenta l'identificativo univoco a livello nazionale associato al tampone. Tale identificativo viene determinato dal Sistema TS ed è composto dal prefisso "CUN-" seguito da 10 caratteri di cui 9 selezionati casualmente, con la stessa probabilità di selezione, dal sottoinsieme di 25 caratteri dato dall'unione dell'alfabeto maiuscolo e numerico (A, E, F, H, I, J, K, L, Q, R, S, U, W, X, Y, Z, 1, 2, 3, 4, 5, 6, 7, 8, 9). Il decimo carattere viene calcolato deterministicamente sulla base dei 9 precedenti, allo scopo di disporre di un carattere di controllo, comunemente detto "check-digit", per mitigare

gli errori di dettatura o trascrizione. Per questo motivo, sono disponibili fino ad un massimo di 25<sup>9</sup> CUN distinti.

L'algoritmo è disponibile a questo indirizzo:

[https://github.com/immuni-app/immuni-backend-common/blob/master/immuni\\_common/models/marshmallow/validators.py#L184](https://github.com/immuni-app/immuni-backend-common/blob/master/immuni_common/models/marshmallow/validators.py#L184)

e si basa sull'assegnazione di un code-point ad ognuno dei nove simboli, approccio basato sull'algoritmo di Luhn mod N.

Ogni codice può essere utilizzato una sola volta per sbloccare l'applicazione Immuni ed ha una durata di 14 giorni, allo scadere della quale non è più utilizzabile per consentire il caricamento delle chiavi dell'applicazione Immuni.

#### 2.4.2 *SERVIZIO DI ANNULLAMENTO ESECUZIONE TEST*

Con questo servizio la piattaforma regionale ovvero la singola struttura sanitaria può annullare la comunicazione dell'esito relativo alla somministrazione di un tampone inviato precedentemente tramite il servizio di cui al paragrafo 2.4.1.

Tabella 4 Servizio di annullamento esecuzione test - messaggio di richiesta

Campo	Descrizione	Obbligatorio
<b>Identificativo struttura Sistema TS</b>	Identificativo della struttura che ha eseguito il tampone secondo la codifica di Sistema TS ovvero codice regione-codice asl-codice struttura.	NO <ul style="list-style-type: none"> <li>- Nel caso di invio diretto dalla struttura, il campo è obbligatorio</li> <li>- Nel caso di invio da una piattaforma regionale, il campo è in alternativa con</li> </ul>

Campo	Descrizione	Obbligatorio
		il campo "Descrizione struttura"
<b>Descrizione struttura</b>	Nel caso di invio dei dati dalla piattaforme regionali che non hanno un sistema di codifica delle strutture integrato con Sistema TS oppure nel caso di strutture non censite nel Sistema TS, in questo campo si può specificare una descrizione testuale della struttura (massima lunghezza 256)	NO <ul style="list-style-type: none"> <li>- Nel caso di invio diretto dalla struttura, il campo non va valorizzato</li> <li>- Nel caso di invio da una piattaforma regionale, il campo è in alternativa con il campo "Identificativo struttura Sistema TS"</li> </ul>
<b>Codice fiscale assistito</b>	Il codice fiscale dell'assistito	SI
<b>Identificativo transazione</b>	Identificativo della transazione, generato dal sistema. Tale numero rappresenta il <b>CUN</b> (codice univoco nazionale) che identifica il test a livello nazionale.	SI
<b>Tipologia test</b>	Tipologia del test eseguito (valorizzare a 'M' per tampone molecolare)	SI

Tabella 5 Servizio di annullamento esecuzione test - messaggio di risposta

Campo	Descrizione	Fonte
<b>Identificativo transazione</b>	Identificativo della transazione associato all'operazione di annullamento, generato dal sistema	Sistema TS
<b>Data-ora</b>	Data-ora-minuti-secondi-millisecondi in cui si è conclusa la transazione	Sistema TS
<b>Esito</b>	Esito della transazione	Sistema TS
<b>Descrizione esito</b>	Descrizione dell'esito della transazione	Sistema TS

### 2.4.3 SERVIZIO DI ELENCO TEST EFFETTUATI

Con questo servizio la piattaforma regionale ovvero la singola struttura sanitaria può accedere all'elenco degli esiti comunicati correttamente al Sistema TS. Per questo servizio si rende necessario indicare il codice fiscale dell'operatore che sta inviando la richiesta. Tale operatore deve essere censito nella banca dati degli utenti Sistema TS attraverso le procedure di censimento previste per gli operatori

regionali/ASL e deve essere abilitato al profilo di sicurezza “Elenco Tamponi Molecolari” dall’amministratore di sicurezza Sistema TS. Il numero di operatori che possono essere abilitati a questa operazione è al massimo 3 per regione.

Tabella 6 Servizio di elenco test effettuati - messaggio di richiesta

<b>Campo</b>	<b>Descrizione</b>	<b>Obbligatorio</b>
<b>Identificativo struttura Sistema TS</b>	Identificativo della struttura che ha eseguito il tampone secondo la codifica di Sistema TS ovvero codice regione-codice asl-codice struttura.	NO <ul style="list-style-type: none"> <li>- Nel caso di invio diretto dalla struttura, il campo è obbligatorio</li> <li>- Nel caso di invio da una piattaforma regionale, il campo è in alternativa con il campo “Descrizione struttura”</li> </ul>
<b>Descrizione struttura</b>	Nel caso di invio dei dati dalla piattaforme regionali che non hanno un sistema di codifica delle strutture integrato con Sistema TS oppure nel caso di strutture non censite nel Sistema TS, in questo campo si può specificare una descrizione testuale della struttura (massima lunghezza 256)	NO <ul style="list-style-type: none"> <li>- Nel caso di invio diretto dalla struttura, il campo non va valorizzato</li> <li>- Nel caso di invio da una piattaforma regionale, il campo è in alternativa con il campo “Identificativo struttura Sistema TS”</li> </ul>
<b>Data inizio intervallo</b>	Data di inizio dell'intervallo temporale di ricerca	SI
<b>Data fine intervallo</b>	Data di fine dell'intervallo temporale di ricerca	SI
<b>Tipologia test</b>	Tipologia del test eseguito (valorizzare a 'M' per tampone molecolare)	SI
<b>Identificativo utente</b>	Il codice fiscale dell'operatore autorizzato all'utilizzo del servizio	SI

Tabella 7 Servizio di elenco test effettuati - messaggio di risposta

<b>Campo</b>	<b>Descrizione</b>	<b>Fonte</b>
<b>Identificativo transazione</b>	Identificativo della transazione, generato dal sistema	Sistema TS
<b>Data-ora</b>	Data-ora-minuti-secondi-millisecondi in cui si è conclusa la transazione	Sistema TS
<b>Esito</b>	Esito della transazione	Sistema TS
<b>Descrizione esito</b>	Descrizione dell'esito della transazione	Sistema TS
<b>Lista test</b>	Lista di valori contenente i campi seguenti	Sistema TS
<ul style="list-style-type: none"> <li><b>Identificativo struttura Sistema TS</b></li> </ul>	Identificativo della struttura che ha eseguito il tampone secondo la codifica di Sistema TS ovvero codice regione-codice asl-codice struttura.	Sistema TS
<ul style="list-style-type: none"> <li><b>Descrizione struttura</b></li> </ul>	Nel caso di invio dei dati dalla piattaforme regionali che non hanno un sistema di codifica delle strutture integrato con Sistema TS oppure nel caso di strutture non censite nel Sistema TS, in questo campo si può specificare una descrizione testuale della struttura (massima lunghezza 256)	Sistema TS
<ul style="list-style-type: none"> <li><b>Data prelievo</b></li> </ul>	Data in cui è stato eseguito il prelievo	Sistema TS
<ul style="list-style-type: none"> <li><b>Identificativo test</b></li> </ul>	Identificativo del test (CUN)	Sistema TS
<ul style="list-style-type: none"> <li><b>Data inserimento</b></li> </ul>	Data in cui è stato comunicato il dato al Sistema TS	Sistema TS
<ul style="list-style-type: none"> <li><b>Esito test</b></li> </ul>	Esito del test eseguito	Sistema TS
<ul style="list-style-type: none"> <li><b>Tipologia test</b></li> </ul>	Tipologia del test eseguito ('M' per tampone molecolare)	Sistema TS

## 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:

- Identificativo o descrizione della struttura che esegue l'inserimento
- Codice fiscale dell'operatore regionale (per il servizio del paragrafo 2.4.3)

- data-ora-minuti-secondi-millisecondi dell'accesso
- operazione richiesta, esito della transazione
- identificativo della transazione.

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

Il servizio alimenta una banca dati contenuta nel Sistema TS che include, in particolare:

- identificativo nazionale associato al test (CUN)
- data prelievo
- tipologia del test
- esito del test
- identificativo o descrizione della struttura che ha eseguito il test
- numero di cellulare e email dell'assistito (se presente)
- data comunicazione al Sistema TS

in un archivio separato saranno tracciati i seguenti dati al fine di consentire unicamente lo sblocco della app Immuni da parte degli operatori del call center:

- identificativo nazionale associato al test (CUN)
- codice fiscale dell'assistito a cui è stato somministrato il test.

Il codice fiscale dell'assistito sarà cancellato in modo irreversibile da tale archivio nel momento in cui avviene la conferma dello sblocco della app Immuni attraverso il servizio descritto al paragrafo 3.3.3.

### 3. SERVIZI PER IL CALL CENTER

#### 3.1 DESCRIZIONE DEI SERVIZI

Si descrivono di seguito le interfacce dei servizi esposti al Call Center per verificare la positività dell'assistito e comunicare l'OTP al servizio di Immuni.

#### 3.2 MODALITÀ DI FRUIZIONE

I servizi descritti di seguito sono resi disponibili tramite web service in modalità cooperativa.

#### 3.3 ACCESSO AI SERVIZI

Le possibilità di accesso ai servizi da parte del Call Center sono riassunte nella seguente tabella:

*Tabella 8 Modalità di accesso ai servizi per la comunicazione del codice OTP di Immuni tramite Call Center*

ID	Utente	Modalità	Autenticazione	Note
1	Operatore del Call Center	Web service	Autenticazione con certificato client del sistema chiamante.	L'operatore viene identificato e accede all'applicazione del Call Center. Quest'ultima richiama i web service, utilizzando a fini di autenticazione un certificato rilasciato da Sistema TS. Il codice fiscale dell'operatore viene trasmesso come campo applicativo nel tracciato, e deve essere stato preautorizzato.  La piattaforma del Call Center deve garantire i requisiti minimi di sicurezza adottati dal

				Sistema TS in termini di autenticazione forte, nel tracciato viene dichiarata la tipologia di autenticazione
--	--	--	--	--

L'operatore, tramite una applicazione messa a disposizione dal Call Center, potrà richiamare i servizi esposti da Sistema TS in modalità cooperazione applicativa. L'operatore, censito sul sistema dall'amministratore di sicurezza della struttura chiamante, verrà identificato e si autenticherà sul sistema informativo del Call Center e a sua volta quest'ultimo, autenticandosi tramite certificato client, richiamerà i suddetti servizi. La corretta associazione operatore/chiamata è a carico della parte client. Il sistema informatico del Call Center deve garantire i requisiti minimi di sicurezza adottati dal Sistema TS in termini di autenticazione forte. I dettagli dell'autenticazione degli operatori del Call Center vengono descritti nel capitolo 4. E' possibile richiamare con esito positivo i servizi soltanto da indirizzi IP di provenienza censiti anticipatamente.

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

### 3.3.1 *SERVIZIO VERIFICA POSITIVITÀ*

Il servizio di verifica positività permette agli operatori del Call Center di accertarsi che il CUN comunicato telefonicamente dall'assistito sia legato a un tampone positivo e debba effettivamente dare luogo a una successiva comunicazione di OTP verso Immuni.

*Tabella 9 Servizio di verifica positività - messaggio di richiesta*

<b>Campo</b>	<b>Descrizione</b>	<b>Obbligatorio</b>
<b>Codice Fiscale Operatore</b>	Il codice fiscale dell'operatore che richiede la verifica. L'ID Transazione in risposta è utilizzabile soltanto da quest'ultimo in ambito di comunicazione verso Immuni	SI



<b>Numero tessera sanitaria</b>	Ultime 8 cifre del numero di tessera sanitaria (TEAM)	SI
<b>CUN</b>	Codice univoco nazionale associato al tampone.	SI

Tabella 10 Servizio di verifica positività - messaggio di risposta

<b>Campo</b>	<b>Descrizione</b>	<b>Fonte</b>
<b>Identificativo transazione</b>	Identificativo transazione (a scopo di controlli tecnici)	Sistema TS
<b>Esito</b>	Esito della transazione	Sistema TS
<b>Descrizione esito</b>	Descrizione dell'esito della transazione	Sistema TS
<b>ID Verifica Tampone</b>	ID da comunicare al servizio di caricamento OTP Immuni	Sistema TS
<b>Data prelievo</b>	Data in cui è stato eseguito il prelievo relativo al tampone	Sistema TS

### 3.3.2 SERVIZIO DI SBLOCCO CODICE IMMUNI

Il servizio di sblocco codice immuni permette agli operatori del Call Center di inviare al sistema centrale il codice OTP generato dall'App Immuni per il tracciamento della positività dell'assistito in maniera anonima. Il Sistema TS non memorizza in alcun archivio persistente l'informazione del codice OTP ricevuto ma si limita a rendere disponibile tale informazione al backend di Immuni unitamente alla data inizio sintomi.

Tabella 11 Servizio di sblocco codice immuni - messaggio di richiesta

<b>Campo</b>	<b>Descrizione</b>	<b>Obbligatorio</b>
<b>Codice OTP</b>	Codice OTP generato dall'App Immuni dell'assistito	SI
<b>Data inizio sintomi</b>	Nel caso l'assistito sia sintomatico inserire la data in cui si sono manifestati i primi sintomi. In caso di assistito asintomatico inserire la data del prelievo restituita dal servizio di verifica positività.	SI
<b>Codice Fiscale Operatore</b>	Il codice fiscale dell'operatore che effettua la chiamata	SI

<b>ID Verifica Tampone</b>	ID Ottenuto dal servizio di verifica della positività dallo stesso operatore che sta richiedendo il servizio 3.3.1	SI
----------------------------	--	----

Tabella 12 Servizio di sblocco codice immuni - messaggio di risposta

<b>Campo</b>	<b>Descrizione</b>	<b>Fonte</b>
<b>Identificativo transazione</b>	Identificativo transazione (a scopo di controlli tecnici)	Sistema TS
<b>Esito</b>	Esito della transazione	Sistema TS
<b>Descrizione esito</b>	Descrizione dell'esito della transazione	Sistema TS
<b>Data-ora</b>	Data-ora-minuti-secondi-millisecondi in cui si è conclusa la transazione	Sistema TS

### 3.3.3 SERVIZIO DI CONFERMA SBLOCCO IMMUNI

Il servizio permette al sistema client di comunicare a Sistema TS l'avvenuto upload del codice Immuni da parte dell'assistito. Tale servizio cancella in modo irreversibile nella banca dati del Sistema TS l'informazione del codice fiscale assistito collegato al CUN e l>ID verifica tampone.

Tabella 13 Servizio di conferma sblocco Immuni - messaggio di richiesta

<b>Campo</b>	<b>Descrizione</b>	<b>Obbligatorio</b>
<b>ID Tipo Comunicazione</b>	L'identificativo del tipo di comunicazione Valorizzare a: 'C' per la conferma dello sblocco 'A' per l'annullamento della conferma dello sblocco	SI
<b>Codice Fiscale Operatore</b>	Il codice fiscale dell'operatore che richiede la verifica. L>ID Transazione in risposta è	SI

	utilizzabile soltanto da quest'ultimo in ambito di comunicazione verso Immuni	
<b>ID Verifica Tampone</b>	ID Ottenuto dal servizio di verifica della positività dallo stesso operatore che sta richiedendo il servizio 3.3.1	NO È possibile ometterlo in caso di operazione non contestuale alla chiamata dell'assistito
<b>CUN</b>	Codice univoco nazionale associato al tampone.	SI

Tabella 14 Servizio di conferma sblocco Immuni - messaggio di risposta

<b>Campo</b>	<b>Descrizione</b>	<b>Fonte</b>
<b>Identificativo transazione</b>	Identificativo transazione (a scopo di controlli tecnici)	Sistema TS
<b>Esito</b>	Esito della transazione	Sistema TS
<b>Descrizione esito</b>	Descrizione dell'esito della transazione	Sistema TS

### 3.4 **REGISTRAZIONE DEGLI ACCESSI WEB SERVICES E TEMPI DI CONSERVAZIONE**

Il sistema registra gli accessi ai servizi web e l'esito dell'operazione, e inserisce i dati dell'accesso in archivi dedicati.

Servizio verifica positività:

Per ciascuna transazione effettuata per il servizio di verifica positività saranno registrati i seguenti dati relativi all'accesso e all'esito dell'operazione:

- Codice Fiscale dell'operatore che ha richiesto la verifica
- Timestamp della richiesta
- Esito della transazione
- Identificativo della transazione
- Codice restituito all'operatore per il richiamo del servizio immuni (ID verifica tampone)
- CUN per il quale è stata richiesta la verifica

- IP Client

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

Il servizio di verifica positività alimenta una banca dati su Sistema TS con i seguenti dati:

- ID verifica tampone
- Codice Fiscale Operatore associato all'ID verifica tampone
- Regione dove è stato effettuato il tampone
- Data di inserimento del record
- Data del prelievo relativo al tampone identificato dal CUN per il quale è stata effettuata la verifica

Servizio sblocco codice immuni:

Per ciascuna transazione effettuata per il servizio di sblocco codice Immuni saranno registrati i seguenti dati relativi all'accesso e all'esito dell'operazione:

- Codice Fiscale dell'operatore che ha richiesto lo sblocco
- Tipo di autenticazione lato client
- Data inizio/fine transazione
- Esito della transazione
- Identificativo della transazione
- ID Verifica Tampone
- IP Client

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

Servizio conferma sblocco Immuni:

Per ciascuna transazione effettuata per il servizio di comunicazioni aggiuntive saranno registrati i seguenti dati:

- Codice Fiscale dell'operatore (se presente nel messaggio)
- Tipo Comunicazione

- Codice restituito all'operatore per il richiamo del servizio immuni (ID verifica tampone)
- CUN per il quale è stata richiesta la verifica
- Informazioni inviate dal client (lista coppie chiave/valore)
- Esito comunicazione
- IP Client

#### **4. MODALITÀ DI AUTENTICAZIONE DEGLI OPERATORI DEL CALL CENTER**

Per l'accesso al Sistema TS, l'operatore di Call Center deve essere stato preventivamente abilitato al Sistema TS dall'Amministratore di Sicurezza denominato all'uso nonché possedere le credenziali di accesso al CRM. Le credenziali di autenticazione vengono distribuite da un Amministratore di Sistema (Profilo Amministratore) che, tramite autenticazione di tipo forte al pannello Amministrativo del CRM, ha la possibilità di abilitare gli utenti all'interno del CRM e di profilarli sull'apposita "coda" di servizio (Profilo Operatore di Call Center).

Gli operatori di call center e gli amministratori si autenticano sul sistema di CRM tramite login e password nominale (nota solo all'operatore e non all'Amministratore di sistema) e, come secondo fattore, un codice pin.

L'operatore, una volta loggato sul CRM, raccoglierà i dati dell'utente tramite apposita interfaccia che, tramite collaborazione applicativa, richiamerà gli specifici Web Service accessibili tramite IP dedicato:

- Servizio Verifica Positività
- Sblocco codice Immuni
- Conferma Sblocco Immuni

Tutti gli intervalli IP del CRM sono forniti con notazione CIDR (Classless Inter-Domain Routing), pertanto le chiamate verso i Web Service da parte della piattaforma CRM passeranno tramite uno specifico IP di Proxy Server pre-configurato ed abilitato sul sistema TS.

Tutte le chiamate ai Web Service, pubblici ed accessibili tramite HTTPS (TLS 1.2), prevedono l'invio di un certificato d'autenticazione e dell'identificativo dell'operatore che effettua la chiamata al Web Service. L'identificativo dell'operatore corrisponde al proprio codice fiscale, precedentemente abilitato sul Sistema TS dall'Amministratore di Sicurezza.

#### 4.1 TRACCIATO DEL SERVIZIO

L'operatore di Call Center, nella scheda del Case assegnato univocamente a ciascuna richiesta, digita in appositi campi i dati manuali necessari all'invocazione dei servizi di cui al paragrafo 3.3. Il CRM completa in automatico, con i dati restituiti dal Sistema TS, le restanti informazioni.

- Per il servizio di Verifica Positività:

Tabella 15 Servizio di verifica positività - messaggio di richiesta

Campo	Descrizione	Fonte
<b>Codice Fiscale Operatore</b>	Il CRM integra in automatico la chiamata con il CF dell'Operatore	CRM
<b>Numero tessera sanitaria</b>	Viene digitato manualmente dall'Operatore di CC (solo ultime 8 cifre)	Assistito
<b>CUN</b>	Viene digitato manualmente dall'Operatore di CC	Assistito

Tabella 16 Servizio di verifica positività - messaggio di risposta

Campo	Descrizione	Fonte
<b>Identificativo transazione</b>	Identificativo transazione (a scopo di controlli tecnici)	Sistema TS
<b>Esito</b>	Esito della transazione	Sistema TS
<b>Descrizione esito</b>	Descrizione dell'esito della transazione	Sistema TS
<b>ID Verifica Tampone</b>	ID da comunicare al servizio di caricamento OTP Immuni	Sistema TS
<b>Data prelievo</b>	Data in cui è stato eseguito il prelievo relativo al tampone	Sistema TS

- Per il servizio di Sblocco Codici Immuni:

Qualora l'esito della transazione di cui al punto precedente sia positivo, l'Operatore di CC potrà completare le informazioni necessarie allo sblocco.

Tabella 17 Servizio di sblocco codice immuni - messaggio di richiesta

Campo	Descrizione	Fonte
<b>Codice OTP</b>	Viene digitato manualmente dall'Operatore di CC	Assistito
<b>Data inizio sintomi</b>	Viene digitato manualmente dall'Operatore di CC	Assistito
<b>Codice Fiscale Operatore</b>	Il CRM integra in automatico questa informazione	CRM
<b>ID Verifica Tampone</b>	Il CRM integra in automatico questa informazione	CRM

Tabella 18 Servizio di sblocco codice immuni - messaggio di risposta

Campo	Descrizione	Fonte
<b>Identificativo transazione</b>	Identificativo transazione (a scopo di controlli tecnici)	Sistema TS
<b>Esito</b>	Esito della transazione	Sistema TS
<b>Descrizione esito</b>	Descrizione dell'esito della transazione	Sistema TS
<b>Data-ora</b>	Data-ora-minuti-secondi-millisecondi in cui si è conclusa la transazione	Sistema TS

- Per il servizio di Conferma Sblocco Immuni:

Qualora l'esito della transazione di cui al punto precedente sia positiva, l'Operatore di CC potrà confermare o annullare lo Sblocco.

Tabella 19 Servizio di conferma sblocco Immuni - messaggio di richiesta

Campo	Descrizione	Fonte
<b>ID Tipo Comunicazione</b>	Manuale, l'Operatore di CC clicca l'opzione Conferma oppure l'Opzione Annulla,	Assistito



	secondo la volontà dell'Assistito	
<b>Codice Fiscale Operatore</b>	Il CRM integra in automatico questa informazione	CRM
<b>ID Verifica Tampone</b>	Il CRM integra in automatico questa informazione	CRM
<b>CUN</b>	Il CRM integra in automatico questa informazione	CRM

Tabella 20 Servizio di conferma sblocco Immuni - messaggio di risposta

<b>Campo</b>	<b>Descrizione</b>	<b>Fonte</b>
<b>Identificativo transazione</b>	Identificativo transazione (a scopo di controlli tecnici)	Sistema TS
<b>Esito</b>	Esito della transazione	Sistema TS
<b>Descrizione esito</b>	Descrizione dell'esito della transazione	Sistema TS

## **4.2 REGISTRAZIONE DEGLI ACCESSI APPLICATIVI E TEMPI DI CONSERVAZIONE**

Il servizio non costituisce né alimenta, con i dati degli assistiti, alcuna banca dati contenuta nel CRM, in quanto la sua finalità è la chiamata ai servizi del Sistema TS. In nessun caso sono tracciati i dati dell'assistito (OTP, data inizio sintomi, tessera sanitaria, CUN, ecc.), né su banca dati né su file di log, né su altro mezzo.

Per ciascuna richiesta di servizio effettuata saranno registrati su CRM i seguenti dati relativi alla richiesta: data-ora-minuti-secondi di apertura e di chiusura del case, id chiamata, id operatore, identificativi della transazione (relativi ai 3 WSDL precedentemente illustrati).

## **4.3 MISURE DI SICUREZZA**

### **4.3.1 INFRASTRUTTURA FISICA**

I servizi applicativi sono pubblicati nel Cloud, quelli infrastrutturali inerenti la connettività in modalità On Premise presso un CED. 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 che prevede l'identificazione delle persone che accedono e la registrazione degli orari di ingresso ed uscita di tali persone.

I cloud sono ubicati in Italia e in Europa occidentale. Il CED e il Cloud sono connessi tramite VPN site to site e tramite MPLS.

#### **4.3.2     *REGISTRAZIONE DEGLI UTENTI ED ASSEGNAZIONE DEGLI STRUMENTI DI SICUREZZA***

Il CRM attraverso la componente di amministrazione consente le registrazioni degli operatori e la relativa profilazione/autorizzazione all'utilizzo dei servizi di integrazione.

#### **4.3.3     *CANALI DI COMUNICAZIONE***

I servizi (Web Service) pubblicati dal Sistema TS su rete pubblica, devono essere chiamati dal CRM (Client) ubicato in Cloud. Le comunicazioni avvengono mediante protocollo SSL/TLS, con certificato rilasciato dal sistema TS inviato dal CRM e autenticato attraverso CA dal sistema TS.

L'accesso ai servizi del sistema TS avviene attraverso un unico indirizzo IP abilitato allo scopo tramite un Reverse Proxy intermedio con funzione di "redirect delle chiamate".

#### **4.3.4     *SISTEMA DI MONITORAGGIO DEL SERVIZIO***

Il monitoraggio dei servizi prevede uno specifico sistema di reportistica.

Le risorse dei server coinvolti e i servizi sono monitorati con sistemi automatici.

#### **4.3.5     *PROTEZIONE DA ATTACCHI INFORMATICI***

Il CED è protetto da Firewall con sistemi IPS attivi (Intrusion Prevention System) e il cloud dispone di adeguati sistemi di protezione (certificazione **ISO 27001**)

I sistemi e i software vengono continuamente aggiornati alle ultime versioni.

Periodicamente vengono avviate le Vulnerability Assessment, al fine di individuare le potenziali vulnerabilità dei sistemi e dei servizi.

La profilazione per l'accesso alla rete avviene tramite protocollo 802.1x.

#### **4.3.6     *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.

E' unicamente previsto il backup dei sistemi.

#### **4.3.7     *SISTEMA DI LOG ANALYSIS APPLICATIVO***

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

#### **4.3.8     *ACCESSO AI SISTEMI***

Il CRM prevede un sistema di tracciabilità degli accessi; l'accesso avviene su base di codici personali/univoci. Il sistema registra le informazioni distinguendo tra i diversi tipi di accesso:

- Accesso operatori; il sistema registra le seguenti informazioni:  
(Username, Login Time, Source IP, Login Type, Status, Browser, Platform, Application, Client Version, API Type, API Version, Login URL, Community, TLS Protocol, TLS Cipher Suite, Country Code, Country, Subdivision, City, PostalCode, Latitude, Longitude, HTTP Method)
- Accesso amministratori; il sistema registra le seguenti informazioni

(Date, User, Source, Namespace, Prefix, Action, Section, Delegate User)

- Accesso Apex; il sistema registra le seguenti informazioni  
(Action Submitted, DateSorted Descending, Job Type, Status, Status Detail,  
Total Batches, Batches Processed Failures Submitted By Completion Date  
Apex, Class Apex, Method Apex ,Job ID)

## **5. MODIFICHE PER IL SERVIZIO INVIO CODICE OTP DA PARTE DELLA ASL**

In ottemperanza all'art. 7 dell'ordinanza cui il presente disciplinare fa riferimento, i paragrafi 2.4 e 2.5 dell'allegato tecnico del decreto "DECRETO MEF 3 giugno 2020 - Modalità tecniche per il coinvolgimento del Sistema tessera sanitaria ai fini dell'attuazione delle misure di prevenzione nell'ambito delle misure di sanità pubblica legate all'emergenza COVID-19." viene modificato come specificato nei seguenti paragrafi 5.1 e 5.2.

### **5.1 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. In questo scenario il Sistema TS esegue la cancellazione irreversibile del codice fiscale dell'assistito associato al/ai CUN ove questi risultassero presenti nella banca dati costituita con i servizi di cui al capitolo 2, similmente a quanto previsto nel paragrafo 3.3.3 per il servizio di conferma dello sblocco app Immuni tramite call center. Il codice fiscale dell'assistito è utilizzato unicamente per tale scopo e in alcun modo viene trasmesso al backend di Immuni.

Messaggio di richiesta

<b>Campo</b>	<b>Descrizione</b>	<b>Obbligatorio</b>
<b>Codice OTP</b>	Codice One Time Password	SI
<b>Data inizio sintomi</b>	Data di inizio dei sintomi	NO
<b>Codice fiscale assistito</b>	Codice fiscale dell'assistito	SI

## Messaggio di risposta

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

### 5.2 ***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, codice fiscale assistito), 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.

## **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 o alla piattaforma Call Center.

### **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 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.