4. Decorso inutilmente il termine di cui al comma 3, ovvero qualora le osservazioni presentate dagli interessati non si ritengano accoglibili, si provvede alla rimozione dall'elenco dandone comunicazione agli interessati a mezzo PEC o con altro mezzo idoneo.

5. In caso di rimozione dall'elenco di uno o più nominativi delle personalità indipendenti, secondo le modalità stabilite dai commi 3 e 4, si procede tempestivamente alla relativa sostituzione e alla comunicazione alla Commissione europea.

Il presente decreto sarà pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 4 marzo 2021

Il Ministro: FRANCO

21A01780

DECRETO 18 marzo 2021.

Modifica del decreto 3 giugno 2020 concernente le 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.

IL RAGIONIERE GENERALE DELLO STATO
DEL MINISTERO DELL'ECONOMIA
E DELLE FINANZE

DI CONCERTO CON

IL SEGRETARIO GENERALE
DEL MINISTERO DELLA SALUTE

Visto l'art. 50 del decreto-legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, e successive modificazioni ed integrazioni, concernente il Sistema tessera sanitaria gestito dal Ministero dell'economia e delle finanze;

Visto l'art. 6 del decreto-legge 30 aprile 2020, n. 28, convertito, con modificazioni, dalla legge 25 giugno 2020, n. 70, concernente il Sistema di allerta Covid-19;

Visto il decreto del Ministero dell'economia e delle finanze, di concerto con il Ministero della salute, del 3 giugno 2020, pubblicato nella *Gazzetta Ufficiale* dell' 8 giugno 2020 n. 144, il quale prevede le funzionalità rese disponibili dal Sistema tessera sanitaria per le finalità di cui al citato art. 6 del decreto-legge 30 aprile 2020, n. 28, convertito, con modificazioni, dalla legge 25 giugno 2020, n. 70;

Visto l'art. 20 del decreto-legge 28 ottobre 2020, n. 137, il quale prevede l'istituzione del servizio nazionale di risposta telefonica per la sorveglianza sanitaria e che i dati relativi ai casi diagnosticati di positività al virus SARS-Cov-2 sono resi disponibili al predetto servizio nazionale anche attraverso il Sistema tessera sanitaria ovvero tramite sistemi di interoperabilità;

Vista l'Ordinanza n. 34 del 19 dicembre 2020 della Presidenza del Consiglio dei ministri - Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica Covid-19, concernente il Servizio di supporto telefonico sblocco Immuni, in attuazione del citato art. 20 del decreto-legge 28 ottobre 2020, n. 137, la quale prevede, tra l'altro, in materia di Sistema tessera sanitaria:

all'art. 4, la gestione da parte del Sistema tessera sanitaria del Codice univoco nazionale (CUN) che identifica univocamente a livello nazionale gli esiti dei test per l'accertamento della positività al virus SARS-Cov-2;

agli articoli 3, 5 e 6, la comunicazione dei dati degli esiti dei test da parte delle Regioni e province autonome al Sistema tessera sanitaria;

all'art. 8, le funzionalità del Sistema Tessera sanitaria a supporto per il Call center di Immuni per lo sblocco dell'app Immuni, attraverso l'utilizzo del CUN;

all'art. 7, che il Sistema tessera sanitaria associa ad ogni CUN l'eventuale sblocco dell'app Immuni effettuato, qualsiasi stata la modalità di sblocco effettuato e che, a tal fine, i Dipartimenti di prevenzione delle ASL comunicano anche il codice fiscale del paziente, fra i dati di cui al citato decreto del Ministero dell'economia e delle finanze, di concerto con il Ministero della salute, del 3 giugno 2020;

Visto il documento aggiornato, predisposto dal Ministero della salute, di valutazione di impatto di cui al citato art. 6, comma 2 del decreto-legge 30 aprile 2020, n. 28, convertito, con modificazioni, dalla legge 25 giugno 2020, n. 70, il quale, tra l'altro, prevede anche la funzione di sblocco dell'app Immuni in autonomia da parte del paziente, per la quale il Sistema tessera sanitaria deve rendere disponibili al *backend* del Sistema di allerta Covid-19 le necessarie funzionalità definite nel presente decreto;

Considerato che il Ministero della salute, in qualità di titolare del trattamento ai sensi del predetto art. 6, comma 1 l'art. 6 del decreto-legge 30 aprile 2020, n. 28, convertito, con modificazioni, dalla legge 25 giugno 2020, n. 70, designa il Ministero dell'economia e delle finanze quale responsabile esterno del trattamento dei dati di cui al presente decreto;

Visto il decreto legislativo 7 marzo 2005 n. 82 e successive modificazioni, concernente il Codice dell'amministrazione digitale;

Visto il regolamento n. 2016/679/UE del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

Visto il decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni, concernente il Codice in materia di protezione dei dati personali, come modificato dal decreto legislativo 10 agosto 2018 n. 101, concernente «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)»;

Acquisito il parere favorevole del Garante per la protezione dei dati personali espresso con il provvedimento n. 66 del 25 febbraio 2021, ai sensi dell'art. 36, paragrafo 4, del regolamento (UE) 2016/679;

Decreta:

Art. 1.

Modifiche al decreto del Ministero dell'economia e delle finanze, di concerto con il Ministero della salute, del 3 giugno 2020

1. Al decreto del Ministero dell'economia e delle finanze, di concerto con il Ministero della salute, del 3 giugno 2020, sono apportate le seguenti modifiche:

a) all'art. 1, comma 1, dopo la lettera *g)*, sono aggiunte le seguenti lettere:

«*h)* «CUN», Codice univoco nazionale, generato dal Sistema TS, che identifica univocamente a livello nazionale gli esiti dei test, ai sensi dell'ordinanza n. 34 del 19 dicembre 2020 della Presidenza del Consiglio dei ministri - Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica Covid-19;

i) «app Immuni», componente mobile (app) del Sistema di allerta Covid-19;

l) «sblocco dell'app Immuni», insieme di operazioni che consentono all'utente dell'app Immuni di procedere al caricamento delle proprie TEK. »

b) all'art. 2, comma 3, dopo la lettera *b)*, è aggiunta la seguente lettera: «*c)* il codice fiscale del paziente»

c) dopo l'art. 2, è aggiunto il seguente articolo:

«Art. 2-*bis* Utilizzo del CUN per lo sblocco dell'app Immuni tramite il Sistema TS

1. Oltre alle modalità previste dall'Ordinanza n. 34 del 19 dicembre 2020 della Presidenza del Consiglio dei Ministri - Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica Covid-19, per le finalità di sblocco dell'app Immuni in autonomia da parte del paziente, il Sistema TS, secondo le modalità descritte nell'Allegato A, rende disponibili al *backend* del Sistema di allerta Covid-19 le funzionalità per:

a) la verifica dell'esistenza del CUN con esito positivo associato al paziente per il quale risulti assegnata la tessera sanitaria che termini con le 8 cifre comunicate dal paziente in fase di sblocco dell'app Immuni;

b) a fronte del completamento del caricamento delle TEK da parte del paziente, invalidare il codice CUN, così da impedirne utilizzi successivi per lo sblocco dell'app Immuni dallo stesso paziente;

c) in caso di assistiti asintomatici, rendere disponibile la data del prelievo del tampone abbinato al CUN.

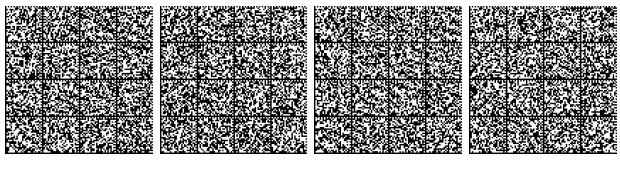
2. Ai sensi dell'art. 7 dell'Ordinanza n. 34 del 19 dicembre 2020 della Presidenza del Consiglio dei Ministri - Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica Covid-19, il Sistema Tessera Sanitaria associa ad ogni CUN l'eventuale sblocco dell'app Immuni effettuato, qualsiasi stata la modalità di sblocco effettuato.»

d) l'Allegato A è sostituito dall'Allegato A del presente decreto. Il presente decreto sarà pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 18 marzo 2021

Il Ragioniere generale dello Stato
MAZZOTTA

Il Segretario generale
RUOCCO



ALLEGATO *A*

Modalità di trasmissione dei dati dagli operatori sanitari per il tramite del Sistema TS e modalità di sblocco dell'app Immuni 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 del Sistema di allerta Covid-19, ai sensi dell'art. 2 comma 3 del presente decreto. Sono anche descritte le modalità di sblocco dell'app Immuni tramite il sistema TS.

2. SBLOCCO TRAMITE ASL

2.1 DESCRIZIONE DEL SERVIZIO DI INVIO DEL CODICE OTP

In riferimento all'articolo 2 comma 2 del presente decreto, il servizio di invio dei dati al backend del Sistema di allerta Covid-19 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 TS attraverso sistemi software con interfacce web o web services, oppure per il tramite di sistemi regionali (SAR).

ID	Utente	Modalità	Autenticazione	Note
1	Operatore sanitario che accede tramite SAR	Web service tramite SAR	Autenticazione a 2 fattori, CNS, CIE, SPID	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 tramite software gestionale	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.

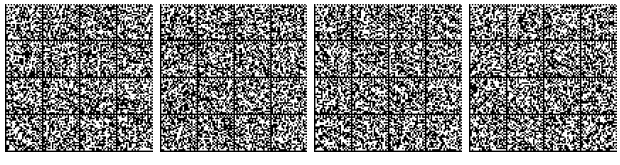
La modalità 2 si rivolge al singolo operatore sanitario che tramite un software gestionale sviluppato ad hoc si connette al servizio utilizzando la propria TS-CNS oppure le proprie credenziali rilasciate dal Sistema TS.

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 e delle relative tempistiche:

- 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 (entro 60 giorni dalla data di adozione del decreto);



- implementazione dell'autenticazione a 2 fattori con OTP temporaneo (entro 90 giorni dalla data di adozione del decreto);
- introduzione delle asserzioni SAML per i sistemi regionali necessarie per l'autenticazione per l'accesso al Sistema TS (entro 90 giorni dalla data di adozione del decreto).

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
Codice fiscale assistito	Codice fiscale dell'assistito	SI

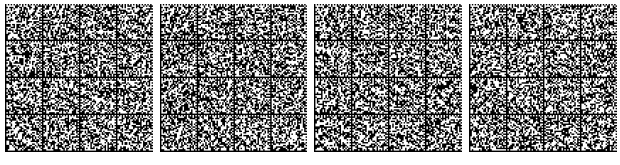
Messaggio di risposta

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 Immuni.

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.

L'unica finalità della trasmissione del codice fiscale dell'assistito nel presente servizio è la cancellazione irreversibile dello stesso codice fiscale che è stato precedentemente associato con il CUN dal servizio di invio esecuzione test, nell'ambito dei servizi che Sistema TS offre alle regioni per l'associazione del CUN con l'esito del tampone (Ordinanza 34 del 19 dicembre 2020). La cancellazione del codice fiscale viene effettuata in tempo reale senza tracciatura del dato. In aggiunta, il codice fiscale dell'assistito non viene in alcun modo trasmesso al backend di Immuni.

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

Nel caso di utente che accede tramite SAR (punto 1 della Tabella 1): 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 che accede tramite credenziali rilasciate dal sistema TS (punti 2 e 3 della Tabella 1): 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 al massimo per dodici mesi.

Ai sensi della normativa citata nelle premesse del presente decreto, l'utilizzo dei servizi, delle applicazioni e della piattaforma del Sistema TS, nonché ogni trattamento di dati personali effettuato ai sensi della normativa di riferimento sono interrotti dalla data di cessazione delle esigenze di protezione e prevenzione sanitaria, legate alla diffusione del COVID-19, e comunque non oltre il 31 dicembre 2021, ed entro la medesima data tutti i dati personali trattati saranno cancellati o resi definitivamente anonimi.

3. SBLOCCO TRAMITE APP IMMUNI

Lo sblocco tramite app Immuni prevede il colloquio tra il backend dell'app Immuni e il Sistema TS.

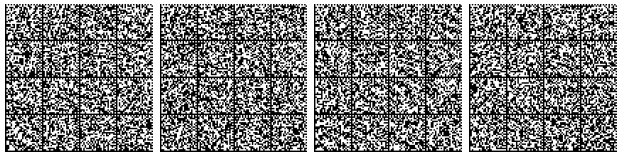
Il Sistema TS rende disponibile al backend Immuni i servizi necessari al fine di abilitare l'utente finale alla trasmissione del codice OTP generato da un dispositivo mobile dotato dell'App Immuni al Sistema di allerta Covid-19, secondo le modalità di cui all'art. 2-bis presente decreto.

Il soggetto risultato positivo al tampone comunica attraverso la app Immuni il codice (Codice Univoco Nazionale associato all'esito del tampone dal Sistema TS in base alle disposizioni dell'ordinanza n. 34 del 19 dicembre 2020), le ultime 8 cifre del numero di tessera sanitaria e la data di inizio sintomi (se sintomatico). La app Immuni trasmette tali dati al backend di Immuni il quale a sua volta richiede al Sistema TS attraverso il servizio di "Verifica Positività" di verificare la positività dell'esito del tampone associato al codice CUN e la corrispondenza tra il codice fiscale dell'esito del tampone e il numero di tessera sanitaria. Se tale verifica va a buon fine, una volta che il soggetto ha confermato l'upload delle chiavi TEK per il contact tracing e procede alla conferma, la richiesta arriva al backend Immuni che oltre a eseguire le operazioni necessarie, invoca il servizio di "Chiusura CUN" esposto dal Sistema TS: tale servizio ha lo scopo di inibire l'utilizzo dello stesso CUN per ulteriori operazioni di sblocco e di eliminare l'informazione del codice fiscale associato al CUN dalla banca dati degli esiti dei tamponi del Sistema TS.

Per mitigare i rischi di utilizzo multiplo del codice CUN, tale codice può essere utilizzato una sola volta per sbloccare l'app Immuni ed è associato al codice fiscale per 14 giorni, allo scadere dei quali non è più utilizzabile per consentire il caricamento delle chiavi dell'applicazione Immuni.

Si distinguono tre casi:

1) assistito negativo al tampone: in queso caso il CUN non è utilizzabile per lo sblocco dell'app Immuni in quanto il servizio di verifica positività risponde con esito negativo



2) assistiti positivo al tampone e CUN utilizzato per lo sblocco dell'app Immuni: in tal caso il CUN non è riutilizzabile per un secondo sblocco in quanto il servizio di chiusura CUN cancella in modo irreversibile il codice fiscale dell'assistito associato al codice CUN

3) assistito positivo al tampone e CUN non utilizzato: in tal caso trascorsi 14 giorni il Sistema TS cancella in modo irreversibile il codice fiscale dell'assistito associato al codice CUN, che quindi non è più utilizzabile

Il CUN viene conservato in banca dati al massimo per 12 mesi (ordinanza n. 34 del 19 dicembre 2020) e comunque cancellato entro la fine dell'emergenza sanitaria. Le misure di sicurezza adottate sono analoghe a quelle per lo sblocco tramite operatore del Dipartimento di prevenzione della ASL.

Come ulteriore misura di controllo per verificare l'associazione del CUN con il soggetto risultato positivo al tampone, viene inviato dall'operatore del call center una porzione del numero della tessera sanitaria ovvero le ultime 8 cifre. Tale dato non viene conservato dal Sistema TS.

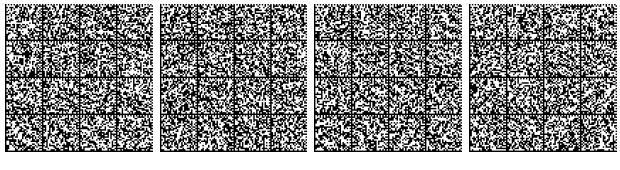
La comunicazione tra backend Immuni e Sistema TS avviene con mutua autenticazione con certificato client su canale cifrato TLSv1.2.

Di seguito si descrivono i tracciati dei servizi messi a disposizione dal Sistema TS al backend Immuni.

3.1 SERVIZIO DI VERIFICA POSITIVITÀ

Messaggio di richiesta

Campo	Descrizione	Obbligatorio
CUN	CUN il codice univoco nazionale associato all'esito del tampone dal Sistema TS Il codice CUN viene inviato codificato secondo l'algoritmo SHA-256	SI



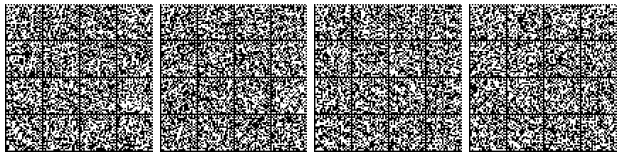
Numero tessera sanitaria	Ultime 8 cifre del numero di tessera sanitaria (TEAM)	SI
Data inizio sintomi	Data di comparsa dei primi sintomi, se la persona è sintomatica	NO

Messaggio di risposta

Campo	Descrizione	Fonte
Identificativo transazione	Identificativo alfanumerico della transazione, generato dal sistema	Sistema TS
Identificativo verifica positività	Codice identificativo da utilizzare nel servizio "Chiusura CUN". Questo codice viene restituito solo se i dati in input risultano associati correttamente a un esito positivo relativo a un tampone comunicato al Sistema TS.	Sistema TS
Esito	Esito della transazione	Sistema TS
Data del tampone	Data di effettuazione del tampone risultato positivo se la persona è asintomatica	Sistema TS

Per ciascuna transazione effettuata saranno tracciati i seguenti dati relativi all'accesso:

- CUN per il quale è stata richiesta la verifica
- Timestamp della richiesta
- Identificativo della transazione
- Codice restituito al backend Immuni (Identificativo verifica positività)
- Esito della transazione
- Data del tampone (solo per asintomatici)



I log delle transazioni così descritti sono conservati al massimo per dodici mesi.

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

3.2 SERVIZIO DI CHIUSURA CUN

Messaggio di richiesta

Campo	Descrizione	Obbligatorio
CUN	CUN il codice univoco nazionale associato all'esito del tampone dal Sistema TS Il codice CUN viene inviato codificato secondo l'algoritmo SHA-256	SI
Identificativo verifica positività	Codice identificativo restituito dal servizio "Verifica positività" in caso di esito transazione positivo associato al CUN.	SI

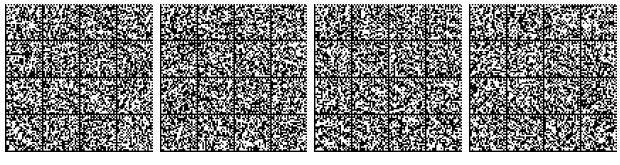
Messaggio di risposta

Campo	Descrizione	Fonte
Identificativo transazione	Identificativo alfanumerico della transazione, generato dal sistema	Sistema TS
Esito	Esito della transazione	Sistema TS

Per ciascuna transazione effettuata saranno tracciati i seguenti dati relativi all'accesso:

- CUN per il quale è stata richiesta la verifica
- Identificativo verifica positività
- Timestamp della richiesta
- Identificativo della transazione
- Esito della transazione

I log delle transazioni così descritti sono conservati al massimo per dodici mesi.



4. MISURE DI SICUREZZA

4.1 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.

4.2 REGISTRAZIONE DEGLI UTENTI ED ASSEGNAZIONE DEGLI STRUMENTI DI SICUREZZA

È 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 sono 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. Entro 60 giorni dalla data di adozione del decreto 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.

4.3 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).

4.4 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.

4.5 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.

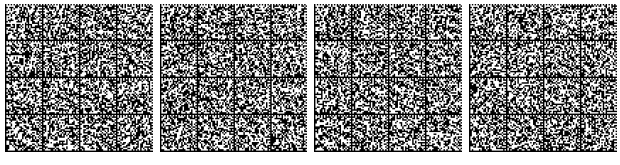
b) Adozione di una infrastruttura di sistemi firewall e sistemi IPS (Intrusion Prevention System) che consentono la rilevazione dell'esecuzione di codice non previsto e l'esecuzione di azioni in tempo reale quali il blocco del traffico proveniente da un indirizzo IP attaccante.

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.

4.6 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.

È unicamente previsto il backup dei sistemi.

4.7 SISTEMA DI LOG ANALYSIS APPLICATIVO

Non è previsto un sistema di log analysis applicativo in quanto come indicato nel par. 2.5 non è prevista la registrazione dei dati applicativi.

4.8 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 (anche da parte degli amministratori di sistema), 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.

21A01809

MINISTERO DELL'UNIVERSITÀ E DELLA RICERCA

DECRETO 26 febbraio 2021.

Ammissione alle agevolazioni del progetto di cooperazione internazionale «InnoSolPOWER» relativo al bando «ERA-NET Concentrated Solar Power - CSP», Call 2019. (Decreto n. 554/2021).

IL DIRETTORE GENERALE DELLA RICERCA

Vista la legge del 14 luglio 2008, n. 121 di conversione, con modificazioni del decreto-legge 16 maggio 2008, n. 85 recante: «Disposizioni urgenti per l'adeguamento delle strutture di Governo in applicazione dell'art. 1, commi 376 e 377, della legge 24 dicembre 2007, n. 244», pubblicato nella *Gazzetta Ufficiale* n. 114 del 16 maggio 2008, convertito con modificazioni nella legge 14 luglio 2008, n. 121 pubblicata nella *Gazzetta Ufficiale* n. 164 del 15 luglio 2008, con la quale, tra l'altro, è stato previsto che le funzioni del Ministero dell'università e della ricerca, con le inerenti risorse finanziarie, strumentali e di personale, sono trasferite al Ministero dell'istruzione, dell'università e della ricerca;

Visto il decreto ministeriale n. 753 del 26 settembre 2014 «Individuazione degli uffici di livello dirigenziale non generale dell'Amministrazione centrale del Ministero dell'istruzione, dell'università e della ricerca», registrato alla Corte dei conti il 26 novembre 2014, registro n. 1, foglio n. 5272, con il quale viene disposta la riorganizzazione degli Uffici del MIUR;

Visto il decreto del Presidente del Consiglio dei ministri 4 aprile 2019, n. 47 recante «Regolamento concernente l'organizzazione del Ministero dell'istruzione, dell'università e della ricerca»;

Visto il decreto del Presidente del Consiglio dei ministri 4 aprile 2019, n. 48 recante «Regolamento concernente l'organizzazione degli Uffici di diretta collaborazione del Ministro dell'istruzione, dell'Università e della ricerca»;

Visto il decreto-legge 21 settembre 2019, n. 104, convertito con legge 132 del 18 novembre 2019, recante «Disposizioni urgenti per il trasferimento di funzioni e per la riorganizzazione dei Ministeri» nella parte relativa agli interventi sull'organizzazione del Ministero dell'istruzione, dell'università e della ricerca;

Visto il decreto del Presidente del Consiglio dei ministri n. 140 del 21 ottobre 2019 (Gazzetta Ufficiale n. 290 dell'11 dicembre 2019) recante il nuovo regolamento di organizzazione del MIUR;

Visto il decreto-legge 9 gennaio 2020, n. 1 recante disposizioni urgenti per l'istituzione del Ministero dell'istruzione e del Ministero dell'università e della ricerca, convertito con modificazioni nella legge n. 12 del 5 marzo 2020 (Gazzetta Ufficiale della Repubblica italiana n. 61 del 9 marzo 2020);

Letto l'art. 4, comma 7, del decreto-legge 9 gennaio 2020, n. 1, il quale dispone «Sino all'acquisizione dell'efficacia del decreto del Ministro dell'economia e delle finanze di cui all'art. 3, comma 8, le risorse finanziarie sono assegnate ai responsabili della gestione con decreto interministeriale dei Ministri dell'istruzione, nonché dell'università e della ricerca. A decorrere dall'acquisizione dell'efficacia del predetto decreto del Ministro dell'economia e delle finanze, le risorse sono assegnate ai sensi dell'art. 21, comma 17, secondo periodo, della legge 31 dicembre 2009, n. 196. Nelle more dell'assegnazione delle risorse, è autorizzata la gestione sulla base delle assegnazioni disposte dal Ministro dell'istruzione, dell'università e della ricerca nell'esercizio 2019, anche per quanto attiene alla gestione unificata relativa alle spese a carattere strumentale di cui all'art. 4 del decreto legislativo 7 agosto 1997, n. 279»;