MINISTERO DELL'ECONOMIA E DELLE FINANZE

DECRETO 8 giugno 2023

Modifica al decreto 30 dicembre 2020, concernente l'adozione delle modalita' di accesso al Sistema TS mediante l'autenticazione a due o piu' fattori. (23A03402)

(GU n.138 del 15-6-2023)

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 (Sistema tessera sanitaria);

Visto il decreto del Ministero dell'economia e delle finanze, di concerto con il Ministero della salute del 30 dicembre 2020, pubblicato nella Gazzetta Ufficiale 15 gennaio 2021, n. 11, concernente la dematerializzazione delle ricette farmaceutiche non a carico del Servizio sanitario nazionale (SSN);

Visto il parere n. 400 del 24 novembre 2022 del Garante per la protezione dei dati personali sullo schema di decreto di modifica del predetto decreto del Ministero dell'economia e delle finanze, di concerto con il Ministero della salute del 30 dicembre 2020;

Visto il decreto del Ministero dell'economia e delle finanze, di concerto con il Ministero della salute, del 1° dicembre 2022, pubblicato nella Gazzetta Ufficiale del 9 dicembre 2022, n. 287, di modifica del predetto decreto 30 dicembre 2020, il quale prevede, in particolare, al capitolo 3 dell'allegato disciplinare tecnico le modalita' di autenticazione per l'accesso al Sistema tessera sanitaria;

Viste le indicazioni fornite dal Dipartimento della trasformazione digitale della Presidenza del Consiglio dei ministri e da Agid in merito alle modalita' di autenticazione informatica a 2 o piu' fattori;

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, nonche' 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, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)»;

Decreta:

Art. 1

Modifiche al decreto 30 dicembre 2020
e successive modificazioni

1. All'art. 4-bis del decreto 30 dicembre 2020 sono apportate le seguenti modifiche:

a) al comma 1, dopo la parola «tecnico,», aggiungere le seguenti «allegato 1,»;

b) dopo il comma 2, e' aggiunto il seguente:

«2-bis. Le modalita' per l'accesso al Sistema TS mediante l'autenticazione a due o piu' fattori prevista dal capitolo 3 dell'allegato 1, sono contenute nel disciplinare tecnico, allegato 2, che costituisce parte integrante del presente decreto.».

Il presente decreto sara' pubblicato nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 8 giugno 2023

Il Ragioniere generale dello Stato
Mazzotta

Il Segretario generale
Leonardi

Allegato 2

DISCIPLINARE TECNICO
Sistema TS: servizi telematici
Ricetta bianca elettronica
Autenticazione forte

Indice

1. Introduzione.

Il presente documento descrive le modalita' tecniche di evoluzione verso un'autenticazione forte, tra cui e' compresa anche l'autenticazione a 2 o piu' fattori, necessaria per le seguenti operazioni:

la trasmissione al Sistema TS da parte dei medici dei dati relativi alle prescrizioni su ricetta bianca elettronica;

la trasmissione al Sistema TS da parte delle farmacie e parafarmacie dei dati relativi alle erogazioni di farmaci prescritti su ricetta bianca elettronica.

Le specifiche tecniche dei servizi e le informazioni a supporto dello sviluppo degli stessi, per entrambi gli argomenti trattati, sono pubblicati nel portale del Sistema TS www.sistemats.it - nel caso dovessero insorgere necessita' informatiche che prevedono la modifica sia della definizione dei campi dei tracciati tecnici sia dei valori da trasmettere ma che non cambiano la logica del trattamento descritto in questo documento, verranno apportate

modifiche unicamente alle specifiche tecniche pubblicate nel portale del Sistema TS.

2. Servizi per la comunicazione dei dati delle ricette bianche elettroniche.

2.1. Accesso ai servizi in autenticazione forte.

Le possibilita' di accesso ai servizi da parte degli attori coinvolti nel processo sono riassunte nella seguente tabella:

ID	Utente	Modalita'	Autenticazione	Note
1	Medico	Web	Autenticazione di base (ID utente e password) con codice PIN come fattore di autenticazione. Autenticazione forte con SPID/SPID professionale/CIE/TS-CNS	Il medico utilizza una applicazione web del Sistema TS. Le credenziali di autenticazione sono rilasciate dal Sistema TS. Nel caso di SPID, le credenziali sono distribuite dagli Identity Provider previsti. Nel caso di CIE, l'Identity Provider e' il Ministero dell'interno.
2	Medico	Web service	TS-CNS oppure CNS oppure autenticazione di base (ID utente e password) con codice PIN come fattore di autenticazione. Autenticazione forte (2 o piu' fattori, certificato client in mutua autenticazione)	Il medico invoca il servizio tramite software gestionale. Credenziali di autenticazione rilasciate dal Sistema TS.
			Autenticazione di base (ID utente e password) con codice PIN come fattore di	L'operatore della farmacia o della parafarmacia utilizza una applicazione web del Sistema TS. Le credenziali di autenticazione sono rilasciate dal Sistema TS. Nel caso di SPID, le credenziali sono distribuite dagli Identity Provider previsti. Nel caso di CIE,

			autenticazione.	l'Identity	
			Autenticazione forte con	Provider e' il	
	Farmacia,		SPID/SPID	Ministero	
3	parafarmacia	Web	professionale/CIE/TS-CNS	dell'interno.	
				L'operatore	
				della farmacia	
				o della	
				parafarmacia	
				invoca il	
				servizio	
				tramite	
			Autenticazione di base	software	
			(ID utente e password)	gestionale o	
			con codice PIN come	sistema	
			fattore di	regionale. Le	
			autenticazione.	credenziali di	
			Autenticazione forte (2	autenticazione	
			o piu' fattori,	sono	
	Farmacia,	Web	certificato client in	rilasciate dal	
4	parafarmacia	service	mutua autenticazione)	Sistema TS.	

La trasmissione dei dati da parte degli utenti 1, 2, 3 e 4 di cui sopra sono da intendersi come collegamento diretto al Sistema TS (c.d. Sistema di accoglienza centrale - SAC).

Le regioni e le Province autonome di Trento e Bolzano che intendono utilizzare il loro Sistema di accoglienza regionale (SAR) per assolvere agli obblighi di trasmissione dati da parte degli utenti 1 e/o 2 e/o 3 e/o 4 si pongono come intermediari nel colloquio con il Sistema TS (SAC). Gli utenti 1 e/o 2 e/o 3 e/o 4 si autenticano al SAR con credenziali e modalita' stabilite dalla regione e provincia autonoma; a sua volta la regione o provincia autonoma si autentica e coopera con il Sistema TS attraverso i servizi descritti nel presente documento. Il colloquio tra sistema regionale e Sistema TS avviene in mutua autenticazione con certificato client. Il sistema regionale deve garantire i requisiti minimi di sicurezza adottati dal Sistema TS in termini di autenticazione forte. Le regioni e province autonome possono autenticarsi al SAC sia in basic authentication con codice PIN come fattore di autenticazione che in mutua autenticazione con certificato client.

E' prevista l'evoluzione della basic authentication con pincode verso un'autenticazione forte (2 o piu' fattori, SPID/SPID professionale/CIE/TSCNS, certificato client mutua autenticazione etc).

3. Modalita' di autenticazione.

Per l'accesso al Sistema TS, i medici, le farmacie e le parafarmacie devono essere stati preventivamente abilitati secondo procedure standard. Le credenziali di autenticazione, prodotte dal Sistema TS e contenenti utente, password da cambiare al primo accesso e pin code, vengono distribuite da un amministratore di sistema (profilo amministratore). Tali credenziali permettono al Sistema TS di riconoscere l'utente con procedure di basic authentication.

E' prevista l'evoluzione della basic authentication con pincode verso un'autenticazione forte (2 o piu' fattori, SPID/SPID professionale/CIE/TS-CNS, certificato client mutua autenticazione etc).

Nel caso specifico dell'evoluzione dell'autenticazione per le funzionalita' fruite tramite web application del Sistema TS e' possibile accedere nel seguente modo: autenticazione SPID/SPID professionale/CIE/TS-CNS tramite cui l'utente sara' indirizzato in base al codice fiscale al profilo riconosciuto e abilitato da Sistema TS.

Per quanto riguarda farmacie e parafarmacie, la soluzione prevede che una farmacia/parafarmacia esegua l'accesso utilizzando lo SPID professionale ovvero nelle more della definizione del quadro di garanzie e regole delle identita' SPID ad uso professionale anche ai sensi dell'art. 64, comma 2-duodecies, del CAD, e' ammesso l'utilizzo

di identita' SPID ad uso personale escludendo l'uso di dati personali attinenti alla sfera privata del soggetto (quali, ad esempio, e-mail personali, numeri di cellulare personali, domicilio privato, etc.) forniti dai gestori dell'identita' digitale (Identity Provider).

L'identita' digitale del titolare, puo' essere utilizzata allo stesso modo in cui attualmente l'utenza della farmacia/parafarmacia e' legata al codice fiscale del titolare. Pertanto, il titolare deve provvedere all'accesso per tutte le farmacie a lui associate. E' possibile richiedere l'accesso «delegato» attraverso cui i dipendenti di una farmacia/parafarmacia sono incaricati dal titolare ad eseguire l'accesso per conto della farmacia stessa, ma utilizzando la propria identita' digitale.

Nel caso specifico dell'evoluzione dell'autenticazione dei web services e' previsto un periodo transitorio in cui sara' comunque ancora supportata l'autenticazione di base con pincode contemporaneamente alla nuova soluzione. La durata del transitorio dipende dalla velocita' di adeguamento dei software degli utenti e dell'acquisizione dei dati di contatto dagli utenti.

Nel caso di sistema regionale che agisce come intermediario tra l'utente e il SAC, il sistema regionale si autentica al SAC in mutua autenticazione con certificato client. Il sistema regionale deve utilizzare un SAML profile su WS-Security che contiene gli attributi qualificanti del soggetto che si e' autenticato al sistema regionale: codice identificativo del soggetto e livello di autenticazione. Tale profilo e' inviato nelle transazioni che il sistema regionale effettua verso il SAC. Il sistema regionale puo' richiedere in alternativa l'adozione del modello di interoperabilita' ModiPA.

Nel caso di utente che si connette direttamente al SAC utilizzando i web services tramite client applicativo (senza intermediazione del sistema regionale), e' necessario prevedere preliminarmente l'acquisizione dei dati di contatto dagli utenti: indirizzo e-mail in quanto attualmente non presenti nel SAC. L'acquisizione puo' avvenire nei seguenti modi:

attraverso una apposita applicazione web del Sistema TS, che prevede la possibilita' di inserire l'e-mail in autonomia per l'utente, dopo una autenticazione con SPID - SPID professionale o CIE o TS-CNS;

tramite forniture massive da parte del soggetto/ente che consegna le credenziali all'utente (la ASL di riferimento o comunque il soggetto di riferimento).

L'autenticazione a due fattori viene realizzata nel seguente modo:

e' requisito preliminare che l'utente abbia certificato il canale utilizzato per l'autenticazione forte (e-mail o app), come indicato nel precedente capoverso;

l'utente si autentica attraverso l'invocazione di un apposito servizio del SAC che genera un identificativo univoco della sessione di lavoro (session id) e lo invia attraverso il canale utilizzato per l'autenticazione forte tramite e-mail o app; in alternativa l'identificativo univoco puo' essere ottenuto attraverso una apposita funzionalita' web del Sistema TS;

l'utente utilizza l'identificativo ricevuto al punto precedente come token autorizzativo della transazione per le chiamate ai servizi interessati; quindi si autentica ai servizi esattamente nello stesso modo utilizzato finora (basic authentication + pincode), aggiungendo in pi l'identificativo della transazione che e' stato ottenuto tramite il secondo fattore;

l'identificativo della transazione e' utilizzabile per un determinato periodo temporale, scelto in modo da bilanciare le esigenze di sicurezza e l'operativita' degli utenti (una durata per esempio di una giornata lavorativa).

Attraverso tali modalita' sono soddisfatti i requisiti di sicurezza richiesti considerando il contesto di riferimento, che richiede di:

velocizzare le tempistiche di attuazione;

minimizzare gli impatti sull'attuale sistema considerando anche la numerosita' della platea di utenti coinvolti e del numero di transazioni giornaliere;

limitare le modifiche necessarie ai software gestionali

attualmente utilizzati.

In aggiunta viene resa disponibile per l'autenticazione per i singoli utenti che si connettono direttamente al SAC utilizzando i web services tramite client applicativo, una mutua autenticazione con certificato client che identifica l'utenza che esegue le operazioni. In questo caso, vista la numerosita' degli utenti, la soluzione presuppone la progettazione e implementazione di un processo di accreditamento e approvvigionamento (provisioning) dei certificati accessibile tramite autenticazione forte. In tal senso, il provisioning dei certificati avviene tramite una apposita funzionalita' del Sistema TS.

Tutte le chiamate ai web service avvengono tramite protocollo HTTPS (almeno TLS 1.2).

4. Misure di sicurezza.

4.1. Infrastruttura fisica.

L'infrastruttura fisica e' 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 attivita' 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.

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 dei medici, delle farmacie e delle parafarmacie avviene attraverso le credenziali rilasciate dal Sistema TS; le regioni e le province autonome possono accedere attraverso le credenziali rilasciate dal Sistema TS oppure tramite certificato client.

In particolare, per le parafarmacie il rilascio delle credenziali del Sistema TS avviene secondo le modalita' di cui al decreto del Ministero dell'economia e delle finanze del 19 ottobre 2020 e successive modificazioni, concernente la trasmissione dei dati delle spese sanitarie a carico dei cittadini.

4.3. Canali di comunicazione.

Le comunicazioni sono scambiate in modalita' 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 pi 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. Il sistema di reportistica offre funzioni per visualizzare i dati aggregati come il numero di transazioni effettuate e i relativi esiti. L'aggregazione puo' essere fatta per regione o per tipologia di utente che effettua la transazione. La finalita' e' di fornire il monitoraggio dell'andamento del progetto sia nella fase di avvio che nella fase a regime.

4.5. Protezione da attacchi informatici.

Per proteggere i sistemi dagli attacchi informatici al fine di eliminare le vulnerabilita', 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 vulnerabilita' sul codice sorgente.

4.6. Sistemi e servizi di backup e disaster recovery.

E' previsto il backup dei sistemi.

E' previsto il disaster recovery dei sistemi, che comprende anche il disaster recovery dei dati.

4.7. Sistema di log analysis applicativo.

Non e' previsto un sistema di log analysis applicativo, non e' 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, 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 integrita'.

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.