AGID
Agenzia per l'Italia Digitale

Allegato alla Determinazione n. 426/2020

Versione 1.0

Introduzione

La procedura oggetto del presente documento è il risultato dei lavori del Tavolo tecnico, istituito in occasione del Comitato Guida SPID del 31 marzo 2020.
Ai lavori, presieduti dal responsabile AgID del progetto SPID, hanno partecipato tutti i gestori di identità digitale SPID (IdP) condividendone gli esiti.

Obiettivo

Il Tavolo tecnico si è posto, tra gli altri, l'obiettivo di individuare procedure di identificazione a vista da remoto adeguatamente sicure ma, al contempo, più agevoli rispetto a quelle già in essere per consentire di velocizzare e incrementare il rilascio di SPID.
L'esigenza, nata nel periodo dell'emergenza covid-19, deriva dalla crescita esponenziale di richieste dell'identità digitale SPID anche in ragione delle misure adottate per il contrasto alla diffusione del virus.

Applicazione

La procedura può essere utilizzata, a far data dalla sua approvazione, da tutti i gestori di identità digitale SPID che, in ogni caso, ove decidessero di avvalersene, dovranno essere autorizzati dall'AgID.

Sinossi

La nuova modalità di identificazione a vista da remoto si basa sull'utilizzo di una registrazione audio/video assistita che, a differenza delle procedure già in essere, senza compromettere la sicurezza, non necessita della presenza contestuale di un operatore. La registrazione, infatti, acquisita e conservata unitamente a tutti i log generati dalla procedura anche a fini probatori, sarà visionata in differita.

L'assenza di un operatore al momento della registrazione dell'audio/video, inoltre, è stata bilanciata dall'introduzione di un meccanismo di enforcement basato sull'esecuzione di un bonifico bancario da parte del soggetto che richiede SPID.

Il gestore dell'identità, oltre ad assolvere gli obblighi scaturenti della presente procedura, deve ottemperare a tutte le verifiche di back-office previste dalla normativa vigente.

Allegato 1

Obblighi e vincoli applicabili

Vincoli e obblighi
1. Modalità limitata al rilascio di credenziali di livello 1 e 2.
2. Verifica dei documenti rubati o smarriti dopo almeno 36 ore dalla richiesta.
3. Verifica congruità fra numero seriale delle tessere sanitarie o tessere del codice fiscale con il codice fiscale.
4. Verifica (cd. *certificazione*) della casella di posta elettronica dichiarata dal richiedente.
5. Verifica (cd. *certificazione*) del possesso del cellulare dichiarato dal richiedente.
6. Visione e ascolto da parte degli operatori addetti dell'intera evidenza audio/video
7. La procedura prevede un processo di registrazione online durante il quale l'utente sceglie le proprie credenziali di livello 1, fornisce il consenso al trattamento, i propri dati personali previsti dalla normativa, la propria mail e numero di cellulare, può prendere visione (e salvare) le condizioni d'uso, la guida utente, l'informativa sul trattamento dei dati personali e dichiara di averne preso visione.
8. Acquisizione dell'immagine (fronte e retro) della TS o del tesserino del CF.
9. Acquisizione dell'immagine (fronte e retro) del documento di riconoscimento del richiedente.
10. Il gestore deve implementare un sistema che garantisca, preliminarmente all'instaurazione della sessione audio/video, la cifratura del canale di comunicazione mediante l'adozione di meccanismi standard, applicativi e protocolli aggiornati alle versioni più recenti
11. Gli operatori devono essere adeguatamente formati.
12. Applicazione delle misure di sicurezza e di contrasto al furto dell'identità.
13. L'IdP effettua l'analisi dei rischi e l'individuazione delle contromisure utilizzando il framework ISO 27001.

Vincoli e obblighi
14. Le immagini e il video sono a colori e consentono una chiara visualizzazione dell'interlocutore in termini di luminosità, nitidezza, contrasto, fluidità delle immagini. L'audio è chiaramente udibile e sincronizzato con il video, privo di evidenti distorsioni o disturbi. La qualità del video e delle immagini dei documenti e Tessera sanitaria (o CF) deve essere ritenuta adeguata dall'operatore.
15. La sessione audio/video deve essere effettuata in ambienti privi di particolari elementi di disturbo.
16. Durante la sessione audio/video l'utente è invitato a compiere una o più azioni casuali volte a rafforzare l'autenticità della richiesta.
17. Facoltà dell'operatore addetto alla verifica delle evidenze di rifiutare il rilascio dell'identità a fronte di dubbi in merito alla reale identità del soggetto o all'autenticità delle evidenze fornite.
18. L'IdP limita, fino a diversa indicazione dell'AgID, l'uso delle identità rilasciate all'ambito nazionale.
19. L'IdP associa ad ogni identità rilasciata la modalità utilizzata in modo da essere individuabile con procedure automatiche.
20. L'IdP conserva nei log tutte le informazioni e le evidenze raccolte durante il processo di rilascio dell'identità per il periodo previsto dall'art. 7, comma 8, del DPCM 24 ottobre 2014, applicando tutte le misure necessarie in tema di protezione dei dati personali.
21. L'IdP si impegna ad adoperarsi al fine di apportare eventuali modifiche indicate da AgID al fine di eliminare la limitazione di cui al punto 18.
22. L'IdP adotta, per quanto applicabile, quanto previsto dalla normativa vigente in materia.
23. L'IdP sottopone la procedura alla valutazione di conformità a quanto disposto dal presente provvedimento da parte di un CAB autorizzato entro 12 mesi dalla sua adozione inviando il report della valutazione ad AgID entro i successivi 30 giorni.

Vincoli e obblighi
24. L’IdP sottopone la procedura alla valutazione di AgID al fine della sua approvazione preventiva.
25. Per le richieste non andate a buon fine, L’IdP conserva per un periodo di un anno la data della richiesta, il CF, e-mail e cellulare del richiedente; per un periodo di 90 giorni la registrazione audio-video.

Allegato 2

Modalità basata sulla verifica dell'identità da remoto con l'ausilio di un bonifico bancario

La modalità, oltre a quanto prescritto nell'Allegato 1, è basata su un audio-video guidato del richiedente su piattaforma o APP gestita nel perimetro di sicurezza dell'IdP e su un bonifico. L'IdP rende disponibili adeguate informazioni relative al processo e l'Informativa sul trattamento dei dati personali ai sensi dell'art. 13 GDPR.

L'IdP provvede ad acquisire il consenso alla videoregistrazione e il consenso al trattamento dei dati personali.

L'IdP provvede ad avvisare il richiedente che le false dichiarazioni sull'identità personale rese a un gestore di un servizio pubblico, qual è il gestore dell'identità digitale SPID:

- sono penalmente rilevanti ai sensi dell'articolo 496 del codice penale e sono punite con la pena della reclusione da uno a cinque anni;
- comportano anche conseguenze di natura civile.

L'interessato esegue la procedura di registrazione (punto 7 Allegato 1), quindi procede ad effettuare la sessione audio-video, durante la quale conferma la data e l'ora, i dati personali (quantomeno il nome e il cognome) forniti nella fase di registrazione, mostra il fronte e il retro del documento di riconoscimento e del tesserino del CF o della TS e conferma la volontà di dotarsi dello SPID.

Al richiedente è richiesto di visionare l'audio-video prodotto e di verificare che le immagini e l'audio siano di buona qualità. Il richiedente può, quindi, confermare o effettuare nuovamente la registrazione.

La procedura prevede che l'utente esegua un bonifico da un c/c con IBAN italiano a lui intestato o cointestato con causale "SPID per *nome cognome* – richiesta SPID *nnn*", dove *nnn* è un codice per correlare la richiesta dell'identità al bonifico stesso (da esempio: SPID per Mario Rossi – richiesta SPID 1570/2020". L'IdP verifica che il nome e il cognome corrispondano al richiedente e che vi sia congruenza fra il numero della richiesta presente nella causale del bonifico e la richiesta.

Durante la sessione audio-video l'IdP fornisce al richiedente un codice numerico random che il richiedente deve leggere durante la sessione stessa. Detto codice può essere fornito via SMS al richiedente l'identità SPID o tramite apposita App dell'IdP preventivamente installata dal richiedente sul cellulare dichiarato all'IdP. L'IdP pone in essere quanto necessario per assicurarsi che l'App sia installata sul cellulare associato dal richiedente alla propria identità digitale.

L'operatore visiona con attenzione l'audio-video, ascolta e riporta nel sistema di back-office il codice numerico letto dal richiedente durante la fase di audio-video. Il sistema

provvede a verificare la congruenza del codice inviato al cittadino con quello digitato dall'operatore.

Gli IdP si impegnano a sospendere almeno il 2% delle richieste giornaliere la cui finalizzazione è vincolata alla verifica dell'audio-video da parte di un secondo operatore. Dopo sei mesi dall'emanazione del presente provvedimento, gli IdP inviano ad AgID e al Garante per la protezione dei dati personali l'esito delle seconde verifiche al fine di valutarne gli esiti. A seguito di detta valutazione tale previsione potrà essere rivista modificando il presente provvedimento.

L'IdP, effettuate tutte le verifiche di back-office e quanto prescritto in Allegato 1, rilascia l'identità digitale.

Gli IdP si impegnano a inserire nelle statistiche settimanali inviate ad AgID il numero delle richieste accettate e delle richieste complete ma respinte a prescindere dalla ragione.

Gli IdP si impegnano, inoltre, a segnalare settimanalmente ad AgID il numero delle richieste respinte che possono presentare elementi riconducibili a tentativi di furto di identità rilevati durante i controlli di back-office quali, a titolo esemplificativo, l'utilizzo di documenti di identità che appaiono poter essere stati manomessi, contraffatti o che risultano essere rubati o smarriti, il tentativo non giustificabile di associare ad una identità un cellulare o un indirizzo e-mail già associato ad altra identità. AgID provvede all'invio di tali segnalazioni al Garante per la protezione dei dati personali.