MANUALE OPERATIVO SPID

File/Oggetto	MANUALE OPERATIVO		
Redatto da	Stefania Ficara	Firma:	
Revisionato da	Claudio Sichili	Firma:	
Approvato da	Claudio Sichili	Firma:	
Archivio			
Stato	Bozza ☐	In fase di Approvazione ☐	Pubblicato ☒

LISTA DI DISTRIBUZIONE

Classificazione	Riservato (ambito reparto) ☐	Riservato (ambito azienda) ☐	Riservato (azienda - cliente) ☒	Pubblico ☐
Distribuzione a	Nominativo:		Funzione/Azienda	
			AgID	
N. Copie Distribuite				

STATO DELLE REVISIONI

REV.	CAP.	DESCRIZIONE MOTIVO	DATA
00	TUTTI	EMISSIONE BOZZA IN CONFORMITÀ AL COMMA 3 REGOLAMENTO PER L'ACCREDITAMENTO E VIGILANZA GESTORI DELL'IDENTITA' DIGITALE SPID	15/03/2021
01	TUTTI	REVISIONE AZIONI CORRETTIVE	15/11/2021
02	7.3,7.5,8.3,13,14.2	DESCRIZIONE ARCHITETTURA DI AUT., REFUSI SU PROCESSI DI VERIFICA IDENTITA', LIVELLI DI SERVIZIO AGGIORNATI, NUOVI OBBLIGHI PER LA CESSAZIONE, REVISIONE NORMATIVE	30/06/2022

Sommario

1. Versione del Manuale Operativo SPID

Data ultimo aggiornamento:	**30/06/2022**
Responsabile del documento:	Stefania Ficara
Verifica del documento:	Claudio Sichili
Approvazione del documento:	Claudio Sichili
Classificazione documento:	Pubblico

2. Scopo del Manuale Operativo SPID

Il presente manuale operativo ha lo scopo di illustrare e definire le modalità operative adottate da ETNA HITECH S.C.P.A. nell'attività di Gestore dell'Identità Digitale in ossequio al DPCM 24 ottobre 2014 "*Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese*" (Gazzetta Ufficiale n. 285 del 9 dicembre 2014) e relative modifiche del DPCM del 19 ottobre 2021.

Il manuale illustra le modalità di richiesta, registrazione, validazione, verifica, rilascio, utilizzo, sospensione, revoca, scadenza e rinnovo delle Identità digitali e le responsabilità e gli obblighi del gestore dell'identità digitale, dei gestori degli attributi qualificati, dei fornitori di servizi, degli utenti titolari dell'identità digitale e di tutti coloro che accedono al sistema pubblico per la gestione dell'identità digitale per la verifica delle identità digitali.

In ottemperanza all'obbligo di informazione richiesto dalla legge (DPCM 24 ottobre 2014 e DPCM 19 ottobre 2021), ETNA HITECH S.C.P.A., come prestatore di servizi fiduciari, redige e pubblica il presente manuale operativo SPID in modo da permettere ad ogni utente di valutare previamente il grado di affidabilità del servizio offerto.

3. Dati identificativi del Gestore SPID

ETNA HITECH S.C.P.A. (di seguito "la Società") è Gestore dell'Identità Digitale in funzione del quale rilascia, previa verifica dell'identità dell'individuo, le credenziali di accesso al soggetto Richiedente, operando in conformità al DPCM Citato.

Ragione sociale:	**Etna Hitech S.C.p.A.**
Legale rappresentante	Emanuele Spampinato
DPO	Antonio Di Giovanni
Sede legale:	Catania (CT), Viale Africa, n. 31, CAP 95129
Sedi operative:	Catania (CT), Viale Africa, n. 31, CAP 95129
Data Center:	Netalia

Partita IVA:	04323210874
Iscrizione Registro Delle Imprese:	04323210874
REA:	CT - 287790
Capitale sociale:	2.500.000 euro
Sito Web:	www.etnahitech.com
PEC:	**etnahitech@pec.it**
Telefono:	**+39 095 8738230**
Fax	**+39 095 8738234**

4. Requisiti normativi, legislativi e standard tecnici

L'azienda ha acquisito le seguenti certificazioni del proprio sistema di gestione:

ISO 9001:2015 – scopo del certificato: Progettazione, sviluppo, produzione, installazione, assistenza e manutenzione, supporto specialistico e gestione applicativa di software. Progettazione ed erogazione di interventi formativi e di servizi di orientamento, inserimento ed accompagnamento al lavoro. (Settori EA 33, 35, 37, 38).

ISO / IEC 27001:2013 - scopo del certificato: Progettazione, sviluppo e manutenzione di soluzioni software anche su piattaforme cloud in modalità SAAS (software as a service) e PASS (platform as a service) con l'utilizzo della linea guida ISO/IEC 27018:2014 e della linea guida ISO/IEC 27017:2015.
Progettazione, sviluppo, manutenzione e assistenza software. Servizio di identity provider aderente al sistema SPID (SISTEMA PUBBLICO IDENTITA' DIGITALE). (Settore EA 33) con i controlli previsti dalle ISO / IEC 27017: 2015 e ISO / IEC 27018:2019.

SPID CSQA n.70191 – certifica che EHT è conforme ai requisiti applicabili definiti:

- all'Art. 24 del Regolamento (UE) 910/2014 eIDAS;
- al DPCM 24 Ottobre 2014;
- al Regolamento di attuazione UE 2015/1502 della Commissione;
- alla norma ETSI EN 319 401;

come definito dalla Circolare di ACCREDIA nr. 35/2016 per la Gestione delle Identità Digitali "SPID".

I principali requisiti legislativi sono di sottoindicati:

DPCM - DPCM del 29-10-2014 (pubblicato in GU Serie Generale n.285 del 9-12-2014), adottato a norma dell'articolo 64, comma 2-sexies del CAD: "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e

imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese" (di seguito DPCM), modificato dal DPCM 19 ottobre 2021, pubblicato nella GU Serie Generale n.296 del 14 dicembre 2021.
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

Codice Privacy - Codice in materia di protezione dei dati personali – D.lgs. 30 giugno 2003 n. 196

Decreto legislativo n.101 del 10 agosto 2018 - 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).

Regolamento (UE) n. 910/2014 ("Regolamento EIDAS") del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche (Gazzetta Ufficiale dell'Unione Europea – serie L257 del 28 agosto 2014)

Determinazione n. 44 del 28 luglio 2015 – Emanazione dei regolamenti SPID previsti dall'art. 4, commi 2, 3 e 4, del DPCM 24 ottobre 2014

I principali **Regolamenti AgID**

Regolamento AgID per l'accreditamento – "Modalità attuative per la realizzazione dello SPID (articolo 4, comma 2, DPCM del 24 ottobre 2014)".
Regolamento AgID recante "le regole tecniche (articolo 4, comma 2, DPCM del 24 ottobre 2014)"
Regolamento AgID recante "le modalità per l'accreditamento e la vigilanza dei gestori dell'identità digitale (articolo 1, comma 1, lettera l), DPCM del 24 ottobre 2014"
Determinazione n.44 del 28 luglio 2015 "Emanazione dei regolamenti SPID previsti dall'art.4, commi 2,3 e 4 del DPCM 24 ottobre 2014".
Regolamento AgID recante le procedure per consentire ai gestori dell'identità digitale, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID, il rilascio dell'identità digitale ai sensi del DPCM 24 Ottobre 2014;

Standard tecnici

FIPS 140-2 FIPS PUB 140-2 Security requirements for cryptographic modules
ISO-IEC 18014 Time-stamping
ISO-IEC 19790:2012 Security requirements for cryptographic modules
ISO-IEC 24760-1 A framework for identity management -- Part 1: Terminology and concept

ISO-IEC 27001 Information security management
ISO-IEC 29003 Identity proofing
ISO-IEC 29100 Basic privacy requirements
ISO-IEC 29115:2013 Entity authentication assurance framework
ITU-T X.1254 Entity Authentication Framework
ITU-T Rec. X.1252 (2010) Baseline identity management terms and definitions
SPID-TabAttr Tabella Attributi (http://www.agid.gov.it/sites/default/files/regole_tecniche/tabella_attributi_la società.pdf)
SPID-TabErr Tabella Codici di Errore (http://www.agid.gov.it/sites/default/files/regole_tecniche/tabella_codici_Errore.pdf)

5. Definizioni e Acronimi

AgID	***Agenzia per l'Italia Digitale***
Attributi identificativi	***Nome, cognome, luogo e data di nascita, sesso, ovvero ragione o denominazione sociale, sede legale, il codice fiscale o la partita IVA e gli estremi del documento d' identità utilizzato ai fini dell'identificazione.***
Attributi secondari	***Il numero di telefonia mobile, l'indirizzo di posta elettronica, il domicilio fisico e digitale, eventuali altri attributi individuati dall'Agenzia, funzionali alle comunicazioni.***
Attributi qualificati	***Qualifiche, abilitazioni professionali, poteri di rappresentanza e qualsiasi altro tipo di attributo attestato da un gestore di attributi qualificati.***
Autenticazione multi-fattore (2FA)	***Autenticazione con almeno due fattori di autenticazione indipendenti***
Codice identificativo	***Il particolare attributo assegnato dal gestore dell'identità' digitale che consente di individuare univocamente un'identità digitale nell'ambito dello SPID***

Credenziali di accesso al servizio	***Attributi di cui l'Utente si avvale tramite autenticazione informatica, per accedere ai servizi erogati in rete dai fornitori di servizi che aderiscono allo SPID***
Gestore dell'Identità Digitale	***Persona giuridica accreditata allo SPID che, in qualità di gestore di servizio pubblico, fornisce il servizio di identità digitale***
Fornitore di servizi o Service Provider (SP)	***Definiti dall'art. 2, comma 1, lettera a), del decreto legislativo 9 aprile 2003, n. 70, sono soggetti pubblici o privati che erogano servizi agli utenti attraverso sistemi informativi accessibili in rete. I fornitori di servizi inoltrano le richieste di identificazione informatica dell'Utente ai gestori dell'identità digitale e ne ricevono l'esito. I fornitori di servizi, nell'accettare l'identità digitale, non discriminano gli utenti in base al gestore dell'identità digitale che l'ha fornita.***
Gestore degli attributi qualificati o Attribute Authority (AA)	***Soggetti accreditati ai sensi dell'art. 16 che hanno il potere di attestare il possesso e la validità di attributi qualificati, su richiesta dei fornitori di servizi.***
Identità digitale	***La rappresentazione informatica della corrispondenza biunivoca tra un Utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo quanto richiesto dal DPCM.***
OTP	***One-Time Password (password usata una sola volta) è una password che è valida solo per una singola transazione***
PIN	***Personally Identifiable Number***

Richiedente	***Persona fisica o giuridica che richiede una o più identità da attribuire ai Titolari. Può coincidere con l'Utente Titolare o con l'intestatario della fattura.***
SPID	***Sistema pubblico dell'identità digitale, istituito ai sensi dell'art. 64 del CAD, modificato dall'art. 17-ter del decreto-legge 21 giugno 2013, n. 69, convertito, con modificazioni, dalla legge 9 agosto 2013, n. 98***
SLA	***Service Level Agreement rappresentano i Livelli di Servizio a contratto***
SSL	***Secure Socket Layer***
Titolare	***Soggetto (persona fisica o giuridica) a cui è attribuito l'identità digitale corrisponde all'Utente del DPCM art. 1 comma 1 lettera v).***

6. Procedure per l'aggiornamento del Manuale Operativo

6.1 Responsabile del Manuale Operativo

La società è responsabile della definizione, pubblicazione ed aggiornamento di questo documento. Eventuali Domande, osservazioni e richieste di chiarimento in ordine al presente manuale dovranno essere rivolte all'indirizzo ed alla persona sottoindicata:

Responsabile del Manuale Operativo	
Nome	Stefania
Cognome	Ficara
E-mail	**stefania.ficara@etnahitech.com**
Telefono	

6.2 Revisione del Manuale Operativo ed approvazione delle modifiche

La società si riserva di apportare variazioni al presente documento per esigenze tecniche o per modifiche organizzative alle procedure derivanti da norme di legge,

regolamenti e miglioramento dei processi inerenti alla gestione delle identità digitali.

Ogni nuova versione annulla e sostituisce le precedenti.

Ogni aggiornamento del contenuto sarà sottoposto a validazione a cura dell'Agenzia per l'Italia Digitale.

7. Architettura

7.1 Architettura applicativa

Il Sistema Pubblico di identità Digitale (SPID) mette in relazione gli attori del sistema per le attività necessarie alla richiesta e fruizione di un servizio online, erogato da un Fornitore di servizi a seguito della richiesta da parte di un Utente Titolare ed a seguito di eventuali accertamenti di ruoli e qualifiche presso i Gestori degli attributi qualificati.
Le principali funzionalità sono quella di Registrazione degli utenti e quella di Autenticazione degli utenti.

- La funzione di Registrazione, alla quale vengono demandate le procedure di registrazione dei soggetti per i quali l'IdP gestisce l'identità digitale, di associazione delle credenziali di autenticazione al soggetto stesso e di gestione del ciclo di vita della specifica identità digitale e delle credenziali associate
- la funzione di Autenticazione, alla quale vengono demandate le procedure di autenticazione dei soggetti da essa gestiti, di verificare le credenziali di autenticazione e di generare una asserzione di autenticazione dove indicare gli attributi identificativi richiesti dal Fornitore dei Servizi per la specifica applicazione.

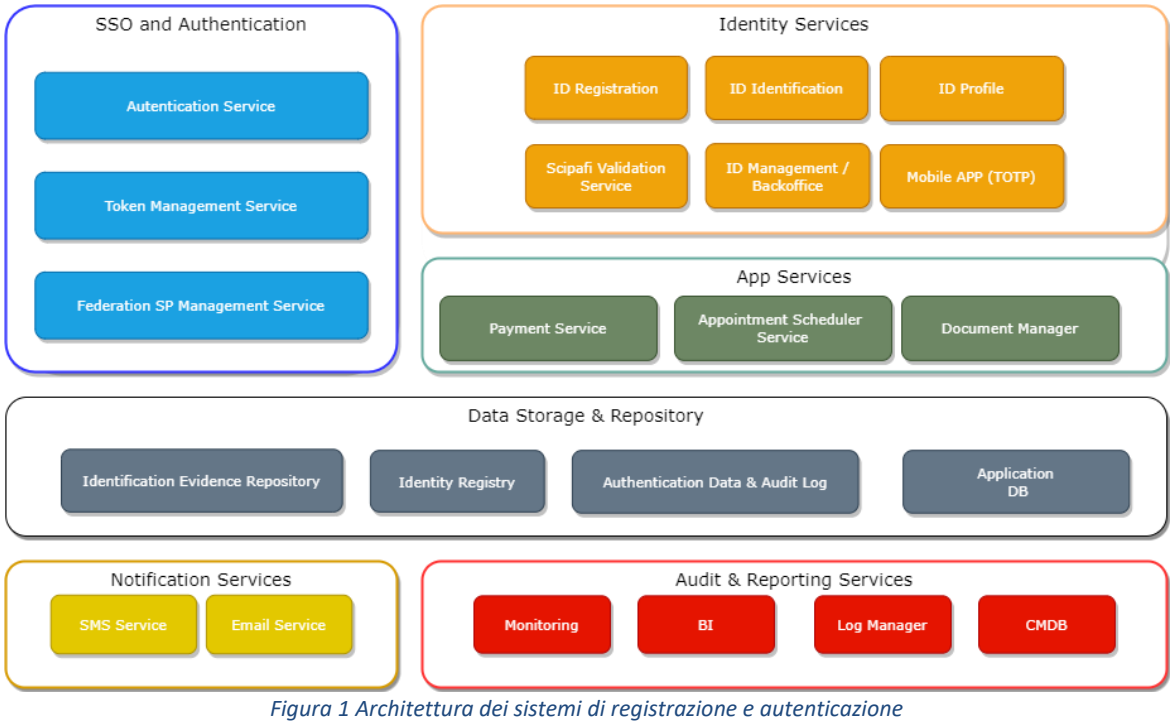


Figura 1 Architettura dei sistemi di registrazione e autenticazione

Il Servizio di Gestione delle Identità digitali può essere logicamente suddiviso nelle seguenti aree e componenti:

- *SSO & Authentication*: raccoglie tutte le componenti legate al processo di autenticazione degli utenti che necessitano utilizzare la propria identità digitale, secondo i tre livelli di servizio; in particolare, le componenti coinvolte saranno in grado di validare le credenziali del soggetto e generare le asserzioni di autenticazione con gli attributi identificativi richiesti dal Fornitore dei Servizi per la specifica applicazione.
- *Identity Services:* afferiscono a questa area tutte le componenti legate ai servizi erogati dall'IdP, in particolare:
    - *ID Registration*: componente software responsabile delle procedure di registrazione dei soggetti per i quali l'IdP gestisce l'identità digitale;
    - *ID Identification*: componente software che eroga tutte le funzionalità per la verifica e validazione della richiesta di creazione di una nuova identità digitale;
    - *ID Management / Backoffice*: raccoglie tutte le componenti responsabili del ciclo di vita dell'identità digitale, ivi comprese le funzionalità per la sospensione e la revoca.
    - *Mobile App*: consente agli utenti di ottenere il codice OTP in aderenza al principio della MFA.
    - *ID Profile*: offre all'utente le funzionalità di consultazione del ciclo di vita della propria identità digitale.
- *APP Services*: raccoglie le componenti aggiuntive di backend necessarie per erogare i servizi offerti dall'IdP
- *Data Storage & Repository*: area destinata a raccogliere ed organizzare in database applicativi e repository documentali tutti i dati coinvolti nei processi erogati. In questa area è possibile individuare i sistemi software per la memorizzazione dei dati di identificazione, come le video-registrazioni eseguite durante la fase di identificazione, gli audit log comprendenti le transazioni di autenticazione degli utenti, e la stessa anagrafica utente.
- *Notification Services*: servizi per la gestione di sms ed e-mail.
- *Audit & Reporting Services*: comprende tutte le componenti per la gestione resiliente ed affidabile del servizio, secondo le normative vigenti di qualità:
    - *Monitoring:* monitoraggio proattivo del servizio e dell'infrastruttura
    - *Business Intelligence:* servizio di analytics e reporting
    - *Log Manager:* conservazione centralizzata e strumenti di analisi dei log applicativi e delle componenti infrastrutturali
    - *CMDB:* strumento di configuration management

7.2 Architettura fisica

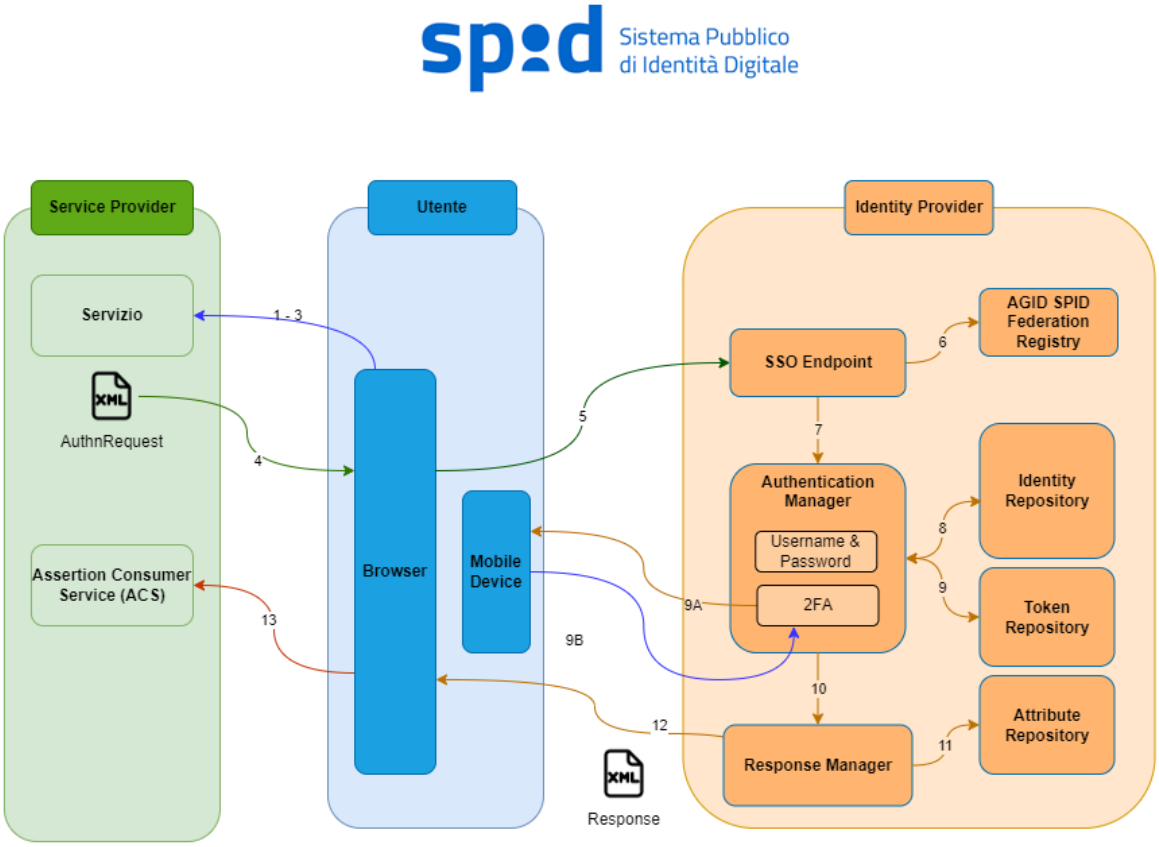
Il Sistema Pubblico di identità Digitale (SPID) di EtnaHiTech è basato sulle seguenti infrastrutture di elaborazione strutturate al fine di garantire un elevato livello di affidabilità e di continuità di servizio, presso i due siti sotto riportati:

Sito	Locazione

Sito primario	Genova Data Center
Sito di Disaster Recovery	Milano Data Center

7.3 Architettura del Sistema di autenticazione

Il modulo di autenticazione recupera le informazioni relative ai servizi erogati in SPID in modalità applicativa secondo i protocolli e le specifiche previsti dalle regole tecniche di cui all'Art 4, comma 2 del DPCM.



1. Il soggetto titolare della identità digitale (utente) richiede l'accesso ad un servizio collegandosi tramite un browser al portale del fornitore dei servizi (Service Provider)
2. Il Service Provider sottopone all'Utente la possibilità di scegliere l'Identity Provider da utilizzare per inizializzare il processo di autenticazione
3. L'Utente sceglie il gestore della identità digitale direttamente dall'elenco proposto.
4. Il servizio del Service Provider, tenendo conto della scelta dell'utente, genera una richiesta di autenticazione (AuthnRequest) che restituisce al browser dell'utente sotto forma di redirect
5. Il browser, in modo trasparente all'utente, prende la redirect e rigira la richiesta verso il punto di ricezione delle richieste di autenticazione dell'Identity Provider

6. Al fine di verificare che la richiesta provenga da un Service Provider accreditato, l'IdP consulta il Registro AGID presente nella propria cache
7. La richiesta viene passata all'Authentication Manager dove viene decodificata, individuando il livello SPID richiesto, e dove viene presentato all'utente la schermata per autenticarsi
8. Viene interrogato il sistema "Identity Repository" per verificare se l'utente effettivamente possiede una identità digitale attiva e le credenziali inserite sono corrette
9. Nel caso di autenticazione di livello 2, viene interrogato il repository contenente i token associati all'utente
    a. Viene inviata la notifica via SMS o APP sul dispositivo dell'utente
    b. L'utente inserisce il codice ricevuto per completare il processo di autenticazione
10. Viene interrogato il servizio responsabile per la generazione delle risposte (*Response*) di autenticazione
11. Vengono recuperati gli attributi associati all'identità digitale che devono essere inclusi nella *Response*
12. La *Response* viene imbustata all'interno di una richiesta HTTP che, in modo trasparente all'utente, viene rinviata al Service Provider attraverso una redirect sul browser dell'utente

Il servizio di autenticazione SPID soddisfa le specifiche di messaggistica e codifica dei casi di errore previste dalle regole tecniche di cui all'Art 4, comma 2 del DPCM e descritte nella tabella indicata in APPENDICE A..

7.4 Livelli di sicurezza

Livello di sicurezza 1: Si basa su di un sistema di autenticazione ad un solo fattore, basato su password. A questo livello vengono rilasciate all'Utente uno Username ed una Password.

Il Repository delle Identità SPID impone l'uso delle raccomandazioni baseline per l'ottenimento di password complesse e difficilmente attaccabili:

a. lunghezza minima di otto digit;

b. uso di caratteri maiuscoli e minuscoli;

c. inclusione di uno o più caratteri numerici;

d. non deve contenere più di due caratteri identici consecutivi;

e. inclusione di almeno un carattere speciali ad es #, $, % ecc.

Il Repository SPID inoltre impone i seguenti meccanismi di protezione

- Impedisce l'uso di formati comuni (ad es. codice fiscale, patente auto, sigle

documenti, date, includere nomi, ecc.).

- Fissa la scadenza delle password non oltre i 180 giorni e ne impedisce il riuso o che abbiano elementi di similitudine prima di 5 variazioni o comunque non prima di 15 mesi.

- Implementa una procedura di sollecito con la quale invita l'utente a modificare la Password secondo le raccomandazioni sopra indicate

- Memorizzazione cifrata delle password: Le password non sono mai memorizzate in chiaro se non in forma irreversibile (tramite hash crittografico) all'unico scopo di verificare la validità della credenziale sottoposta dall'utente in fase di autenticazione

Il primo livello di autenticazione viene utilizzato nei casi in cui il rischio derivante dall'utilizzo indebito dell'identità digitale, abbia un basso impatto per le attività del cittadino/impresa/pubblica amministrazione.

Livello di sicurezza 2: Si basa su di un sistema di autenticazione a due fattori non necessariamente basato su certificati digitali. A questo livello vengono rilasciate all'Utente uno Username, una Password ed un codice di sicurezza (OTP - One- Time Password) gestiti tramite sistema SMS ed applicazioni.

Questo livello di autenticazione viene utilizzato per i servizi che possono subire un danno consistente in caso di utilizzo indebito dell'identità digitale.

Livello di sicurezza 3: Si basa su di un sistema di autenticazione informatica basata su certificati digitali le cui chiavi private sono custodite su dispositivi sicuri che soddisfano i requisiti di cui all'Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo.

Corrisponde al livello di garanzia maggiore associato ai servizi che possono subire un danno serio e grave in caso di utilizzo indebito dell'identità digitale.

7.5 Misure Anticontraffazione

Le misure di anticontraffazione delle identità digitali, messe in atto da EHT in qualità di gestore di identità, sono di fondamentale importanza per prevenire il verificarsi del furto d'identità. Queste ci assicurano un'identità certa per l'accesso ai servizi telematici che fanno utilizzo di SPID nel rispetto delle norme e sfruttando gli standard tecnologici presenti nel mercato. Vale la pena sicuramente precisare che l'identità digitale non è esattamente la corrispondenza dell'identità fisica in quanto ci sono aspetti della personalità che ne contraddistinguono l'univocità. Questo concetto evidenzia che per accedere a dei servizi telematici attraverso un'identità digitale è necessario rispettare la tutela della privacy, con riferimento al personale ed essere certi dell'identità di chi si sta autenticando.
La norma che più si avvicina ed affronta queste tematiche è la ISO/IEC 29115; pertanto, per combattere possibili sistemi di contraffazione, le procedure più certe sono:

- l'identificazione remota, ovvero l'accertamento dell'identità tramite strumenti audio/video remoti;
- la firma digitale o CNS, ovvero la ricezione delle richieste di iscrizione, sospensione e revoca firmate digitalmente con certificati emessi da certificatori accreditati a livello nazionale;

La verifica dell'identità viene compiuta attraverso l'accesso alle fonti autoritative, effettuato secondo le convenzioni di cui all'articolo 4, comma 1, lettera c) del DPCM del 24 ottobre 2014.
I controlli effettuati da EHT per la validazione dell'autenticità dei dati si basano sull'utilizzo di sistemi quali:

- Crimnet;
- sito dell'Agenzia delle Entrate;
- Scipafi.

Il riscontro si configura, quindi, come efficace strumento di prevenzione per i furti d'identità sia totali che parziali.
Nell'attesa che i gestori di identità digitale ottengano le autorizzazioni all'accesso alle fonti autoritative, EHT esegue una serie di controlli manuali accedendo ai sistemi pubblici resi disponibili dagli Enti competenti. I controlli possono essere eseguiti dall'operatore nel caso di riconoscimento a mezzo webcam oppure direttamente nelle sedi di EHT.
I controlli eseguiti durante il processo di identificazione sono i seguenti:

- il codice fiscale viene verificato tramite il servizio messo a disposizione dall'Agenzia delle Entrate sul suo portale;
- il codice del documento presentato viene verificato presso il servizio presente sul portale della Polizia di Stato per verifica e smarrimento, furto e contraffazione del documento di identità.

Inoltre, le procedure di identificazione prevedono ulteriori livelli di controllo:

- l'operatore che esegue il riconoscimento a mezzo webcam, non ammette documenti in fotocopia, ma solo documenti in originale;
- l'immagine della documentazione raccolta è conservata a norma di legge in maniera non modificabile;
- il riconoscimento a mezzo webcam è accessibile solamente ai Titolari che dichiarano di voler presentare i documenti previsti dal regolamento (patente, carta di identità e passaporto elettronico), le cui caratteristiche sono riscontrabili anche da remoto. Le misure anticontraffazione si avvalgono anche di elementi tecnologici:
- sono utilizzati algoritmi crittografici robusti per garantire riservatezza e integrità dei dati, sulla base di quanto prescritto normativamente e allineato con le linee guida internazionali e per la generazione e protezione dei codici OTP;
- la firma digitale, ove utilizzata, deve essere basata su certificati emessi da un certificatore qualificato.

7.6 Controllo degli accessi logici, Fisici e degli utenti

Accessi Logici
Vengono identificati utenti **privilegiati a cui sono assegnate specifiche credenziali personali ed univoche caratterizzate da un livello di sicurezza commisurato alle operazioni richieste al sistema.**

Accessi fisici

L'accesso ai locali è reso possibile solo a coloro che ne hanno effettiva necessità, previa registrazione.

I server del sistema sono ospitati in Netalia srl. Solo il personale autorizzato può accedere alle sale server.

Accessi Utenti

L'accesso degli utenti viene registrato sui propri sistemi di monitoraggio attraverso il log file specifico che contiene le seguenti informazioni:

- Indirizzo IP pubblico di provenienza
- Identificativo univoco dell'utente
- Operazione effettuata
- Riferimento temporale dell'operazione

La società archivia questi log in un registro delle transazioni che ha una data retention di 24 mesi.

8. Modalità di richiesta e creazione delle Identità Digitali

8.1 Richiesta di adesione al Servizio SPID

La richiesta avviene attraverso una istanza mediante form di adesione ove vengono richiesti i seguenti dati:

a) cognome e nome;

b) sesso, data e luogo di nascita;

c) codice fiscale;

d) estremi del documento di riconoscimento presentato per l'identificazione;

e) indirizzo di posta elettronica;

f) recapito di telefonia mobile.

La società provvede a validare sia l'indirizzo di posta elettronica che il recapito di telefonia mobile nel seguente modo:

1. indirizzo di posta elettronica: attraverso invio di una mail di conferma con link per verifica e certificazione;
2. recapito di telefonia mobile del titolare, attraverso invio di SMS con codice di controllo che dovrà essere riportato in un form.

8.2 Procedura di registrazione online per lo SPID

Il richiedente accede alla pagina https://etnaid.etnahitech.com/ e procede seguendo l'iter di cui sotto.

STEP 1 – SCELTA MDALITÀ DI IDENTIFICAZIONE

a) a vista da remoto per riconoscimento via webcam

b) informatica via CNS/TS-CNS

c) firma digitale

d) sportello pubblico

STEP 2 – VERIFICA E-MAIL

Viene inviata una mail all'indirizzo inserito con un "codice di controllo" che deve essere inserito nell'apposito campo del form.

STEP 3 – RICHIESTA DEI DATI SPECIFICI DEL RICHIEDENTE

Dati personali

- Nome
- Cognome
- Sesso
- Data nascita
- Luogo nascita (Stato, Provincia, Comune)
- Codice fiscale
- Numero di carta di identità
- Numero di Tessera Sanitaria
- E-mail PEC
- Luogo domicilio (Provincia, Comune)
- Indirizzo domicilio (via, numero civico, CAP)

STEP 4 – DICHIARAZIONE OBBLIGATORIA SOSTITUTIVA DI ATTO DI NOTORIETA'

Richiesta della spunta circa la veridicità dei dati comunicati rendendo edotto il richiedente sul fatto che chi rende dichiarazioni mendaci è punibile ai sensi del Codice penale e delle leggi speciali in materia (art. 76 del DPR 445/2000)

STEP 5 – SPUNTA OBBLIGATORIA DEI CONSENSI AL TRATTAMENTO DEI DATI PERSONALI

Richiesta del consenso al trattamento dei dati (art. 13 del Regolamento UE 2016/279)

STEP 6 – SPUNTA OBBLIGATORIA SULLE CONDIZIONI CONTRATTUALI DI EROGAZIONE DEL SERVIZIO SPID

Viene richiesta una spunta obbligatoria per provare la consapevolezza sulle condizioni contrattuali di erogazione del servizio SPID.

STEP 7 – VERIFICA CELLULARE

Viene inviato un SMS al numero di telefonia mobile con un "codice di controllo" che

deve essere inserito nell'apposito campo del form.

Nel caso non arrivino tempestivamente i messaggi è possibile fare una nuova richiesta o procedere a cambiare i dati inseriti.

STEP 8 – CARICAMENTO DOCUMENTI

Upload file specifici

- File con scansione fronte retro del Documenti di Identità
- File con scansione fronte retro della Tessera Sanitaria

STEP 9 – RIEPILOGO ORDINE

Il richiedente visualizza le condizioni contrattuali che dovranno essere accettate. In questo step, il richiedente dovrà effettuare il pagamento, se previsto.

STEP 10 – RIEPILOGO DATI E CONFERMA PER ATTIVAZIONE DEL PROCESSO DI IDENTIFICAZIONE SELEZIONATO

Il richiedente riceve la Password temporanea e potrà proseguire con la modalità di identificazione scelta.8.3 Procedura di identificazione del richiedente per il rilascio dello SPID. La verifica dell'identità del richiedente può essere svolta attraverso varie modalità:

a. Identificazione attraverso sessioni in webcam con device;
b. Identificazione mediante TS-CNS, CNS;
c. Identificazione mediante Firma digitale;
d. Identificazione sportello RAO pubblico.

OPZIONE A – IDENTIFICAZIONE TRAMITE SESSIONI IN WEBCAM CON DEVICE

La procedura di Identificazione attraverso la sessione audio video consente all'operatore o incaricato del Gestore di identificare in maniera certa i richiedenti l'identità digitale mediante l'ausilio di strumenti di registrazione audio/video e nel rispetto delle misure prescritte dal Garante in merito al trattamento dei dati personali.

Così come previsto dai regolamenti di cui all'Art 4 comma 2 del DPCM, l'identificazione da remoto avviene in una modalità tale da consentire la raccolta di elementi probanti, utili in caso di un eventuale disconoscimento dell'identità da parte del Richiedente della stessa e perciò devono essere rispettate le condizioni di seguito illustrate:

a) le immagini video devono essere a colori e consentire una chiara visualizzazione dell'interlocutore in termini di luminosità, nitidezza, contrasto, fluidità delle immagini;

b) l'audio deve essere chiaramente udibile, privo di evidenti distorsioni o disturbi.

c) la sessione audio/video, che ha ad oggetto le immagini video e l'audio del soggetto richiedente l'identità e dell'operatore, deve essere effettuata in ambienti privi di particolari elementi di disturbo.

Il gestore è responsabile della valutazione in merito alla sussistenza delle condizioni suddette e l'operatore preposto all'attività può sospendere o non avviare il processo di identificazione nel caso in cui la qualità audio/video sia scarsa o ritenuta non adeguata a consentire la verifica dell'identità del soggetto.

Il richiedente l'identità digitale dovrà collegarsi attraverso idoneo gateway predisposto e l'incaricato alla identificazione procederà ad effettuare l'attività nel rispetto delle misure prescritte dal Garante in merito al trattamento dei dati biometrici.

Il Richiedente può effettuare la procedura di riconoscimento come di seguito a seconda dei device in uso:

1. Con un normale PC che soddisfi i seguenti requisiti minimi:
    - webcam;
    - sistema audio dotato di casse e microfono;
    - browser aggiornato con supporto alla tecnologia webrtc;
    - connessione dati a banda larga;
2. Con un dispositivo mobile, smartphone o tablet, che soddisfi i seguenti requisiti:
    - sistema operativo Android / iOS di ultima generazione;
    - fotocamera frontale;
    - sistema audio dotato di casse e microfono;
    - connessione dati che supporti lo stream audio/video.

Prima di iniziare la registrazione del processo di identificazione, l'operatore richiede espresso assenso alla registrazione audio e video, informando il soggetto interessato circa le modalità di conservazione dei dati per 20 anni come previsto dalla normativa vigente in materia.

L'operatore durante la sessione audio/video ha la possibilità di catturare le immagini, di iniziare una registrazione e di interromperla.

L'operatore che effettua l'identificazione accerta l'identità del richiedente tramite la verifica di un documento di riconoscimento in corso di validità, purché munito di fotografia recente e riconoscibile e firma autografa del richiedente stesso, rilasciato da un'Amministrazione dello Stato e verifica il codice fiscale tramite la tessera sanitaria in corso di validità.

L'operatore che effettua l'identificazione può escludere l'ammissibilità della sessione audio/video per qualunque ragione, inclusa l'eventuale inadeguatezza del documento presentato dal richiedente.

Al momento dell'identificazione, l'operatore effettuerà i seguenti passaggi, chiedendo al richiedente di riportare i suoi dati o di confermare espressamente quelli riportati nella richiesta o il consenso. La Registrazione si compone dei seguenti passaggi:

a) l'operatore dichiara i propri dati identificativi;

b) l'operatore chiede l'accettazione espressa delle condizioni contrattuali e del consenso all'operazione di riconoscimento web e del consenso espresso al trattamento dei dati personali con finalità di rilascio dell'identità digitale, alla sua conservazione per 20 anni come previsto dalla normativa vigente in materia. L'operatore informa che la videoregistrazione sarà conservata in modalità protetta;

c) il soggetto deve conferma le proprie generalità;

d) il soggetto deve confermare la data e l'ora della registrazione;

e) il soggetto conferma di volersi dotare di un'identità digitale e conferma i dati inseriti nella modulistica online in fase di preregistrazione: l'operatore in ordine causale chiede conferma di alcuni dei dati presentati dal richiedente che dovrà esplicitare le informazioni inserite in precedenza sul modulo.

f) il soggetto conferma il proprio numero di telefonia mobile e l'indirizzo mail;

g) l'operatore chiede e ottiene conferma dal soggetto circa la conoscenza delle tipologie di credenziali di cui disporrà per l'accesso ai servizi in rete;

h) l'operatore chiede di inquadrare, fronte e retro, il documento di riconoscimento utilizzato dal soggetto, assicurandosi che sia possibile visualizzare chiaramente la fotografia e leggere tutte le informazioni contenute nello stesso e la verifica dell'autenticità del documento presentato; analogamente l'operatore chiede al richiedente di mostrare la tessera sanitaria);

i) il soggetto conferma di aver preso visione e di accettare le condizioni contrattuali e d'uso disponibili sul sito web del gestore di identità;

j) l'operatore riassume sinteticamente la volontà espressa dal soggetto di dotarsi di identità digitale e raccoglie conferma dallo stesso.

Terminata la sessione di videoconferenza il sistema provvederà, autonomamente, ad elaborare le tracce audio-video per la produzione del file di registrazione.
I file così generati verranno inviati al sistema di conservazione con protezione tramite cifratura 128 bit che li archivierà per un periodo pari a 20 anni decorrenti dalla scadenza o dalla revoca dell'identità digitale secondo quanto indicato nell'art. 7, comma 8, del DPCM.

Il sistema di conservazione salverà i file in modo garantirne l'accesso di AgID, del titolare dell'identità SPID e della autorità giudiziaria in caso di procedimenti giudiziari e/o disconoscimento della stessa.

OPZIONE B – IDENTIFICAZIONE TRAMITE TS-CNS, CNS E FIRMA DIGITALE

Nel caso di scelta dell'identificazione via CNS o TS-CNS, viene richiesto all'utente di inserire la smartcard e di autenticarsi. Verrà presentato il modulo digitale di richiesta e adesione allo SPID che dovrà essere firmato elettronicamente con il certificato CNS.

Si considera effettuata la verifica dell'identità del soggetto richiedente per effetto ed in conseguenza della verifica dell'identità già espletata dal gestore che ha rilasciato il

documento digitale di identità.

Nel caso in cui il richiedente abbia un certificato di firma, viene richiesto di compilare un modulo di richiesta di adesione in formato elettronico sottoscritto con firma elettronica qualificata o digitale.

Si considera effettuata la verifica dell'identità del soggetto richiedente per effetto ed in conseguenza della verifica dell'identità già espletata dal gestore che ha rilasciato certificato di firma digitale.

OPZIONE C – Identificazione sportello RAO pubblico

L'IdP si avvale della procedura di identificazione effettuata presso lo sportello da un RAO (Registration Authority Officer) Pubblico, cioè un operatore che è un pubblico ufficiale espressamente incaricato da una Pubblica Amministrazione per l'espletamento dell'attività di identificazione.
L'operatore di uno sportello pubblico effettua l'identificazione dell'utente, accertando l'identità del Richiedente tramite la verifica di un documento di riconoscimento integro e in corso di validità, munito di fotografia e firma autografa dello stesso, e controlla la validità del codice fiscale, verificando che anche la tessera sanitaria sia in corso di validità.
Se i documenti presentati dal Richiedente risultano carenti delle caratteristiche di cui sopra, il processo di identificazione viene sospeso fino all'esibizione di documenti validi ed integri.
L'operatore, effettuato il riconoscimento, compila a sistema la scheda anagrafica con i seguenti dati dell'utente:

- Nome e Cognome;
- Luogo e Data di nascita;
- Sesso;
- Codice Fiscale;
- Estremi del documento d'identità in corso di validità utilizzato ai fini dell'identificazione;
- Numero di cellulare;
- Indirizzo di posta elettronica;
- Domicilio.

Il sistema permette la generazione del codice di attivazione e consente la creazione del token, necessari per concludere con esito positivo le procedure di identificazione e attivazione.
L'operatore consegna all'utente metà del codice di attivazione in modalità cartacea e l'altra metà viene inviata all'indirizzo e-mail fornito dall'utente, unitamente al token.
La lunghezza del codice di attivazione è di 12 caratteri, generati in maniera casuale, e deve contenere almeno una lettera maiuscola, una lettera minuscola, un carattere

numerico e un carattere speciale. Come sopra detto, ai fini del processo, il codice di attivazione è diviso in due parti da 6 caratteri ciascuno.
Il token ha validità di 30 giorni, periodo in cui l'utente, a cui fanno riferimento le informazioni contenute nel token, può utilizzarlo per ottenere l'Identità Digitale.
L'utente si collega al sito https://etnaid.etnahitech.com e seleziona la modalità "Sportello Pubblico". Esegue l'upload del token e gli viene quindi richiesto l'inserimento del codice di attivazione.
Bisogna tenere presente che superati i 5 tentativi errati di inserimento del codice di attivazione, il token non viene più accettato dall'IdP.
I RAO Pubblici si assumono la responsabilità della corretta verifica dell'identità personale dell'utente e sono tenuti a mantenere le evidenze per individuare il singolo operatore che ha effettuato il riconoscimento.

8.4 Procedura di creazione ed elaborazione audio/video

Prima di iniziare la registrazione del processo di identificazione tramite webcam, l'operatore richiede espresso assenso alla registrazione audio e video, informando il soggetto interessato circa le modalità di conservazione dei dati.

Ottenuto l'assenso, l'operatore inizierà a registrare la sessione audio/video per mezzo di un software gratuito di registrazione schermo, selezionando esclusivamente la finestra relativa alla videochiamata. Durante questo processo, l'operatore ha la possibilità di interrompere e riprendere la registrazione in qualsiasi momento.

Terminata la sessione di videoconferenza, sarà cura dell'operatore verificare la qualità delle tracce audio-video nell'ambito della sua postazione locale.
Successivamente, provvederà all'upload del file suddetto nello storage centralizzato, con relativa cancellazione dal suo computer.

I file così generati verranno inviati al sistema di conservazione con protezione tramite cifratura 128 bit che li archivierà per un periodo pari a 20 anni decorrenti dalla scadenza o dalla revoca dell'identità digitale secondo quanto indicato nell'art. 7, comma 8, del DPCM.

Il sistema di conservazione salverà i file in modo garantirne l'accesso di AgID, del titolare dell'identità SPID e della autorità giudiziaria in caso di procedimenti giudiziari e/o disconoscimento della stessa.

I dati di registrazione, costituiti da file audio-video, immagini e metadati strutturati in formato elettronico, vengono conservati e trattati in base all'art. 7 commi 8 e 9 del DPCM.

8.5 Procedura di verifica degli attributi associati all'identità digitale

Dopo la fase di registrazione ed identificazione dell'identità del richiedente, la Società, nel rispetto dei regolamenti di cui all'Art 4 comma 2 del DPCM, effettua la verifica degli attributi identificativi.

La verifica degli attributi identificativi consiste nell' effettuare accertamenti tramite

fonti autoritative istituzionali, in grado di dare conferma della veridicità dei dati trasmessi e raccolti per la finalità di rilascio dello SPID.

L'accesso alle fonti autoritative ai fini dell'attività di verifica è effettuato secondo l'articolo 4, comma 1, lettera c) del DPCM e, nei casi in cui le informazioni necessarie non siano accessibili per mezzo dei servizi convenzionati, tramite verifiche sulla base di documenti, dati o informazioni ottenibili da archivi delle amministrazioni certificanti, ai sensi dell'art. 43, comma 2, del D.P.R. 28 dicembre 2000, n. 445.

Per la verifica del furto o smarrimento del documento l'operatore si avvale del servizio online disponibile sul sito della Polizia di Stato (Crimnet), assicurandosi che non ci siano denunce di furto o smarrimento.

Per la verifica e corrispondenza tra il codice fiscale e i dati anagrafici di una persona, l'Operatore si avvale del servizio online sul sito dell'Agenzia delle Entrate.

Inoltre, in caso di identificazione "Webcam", l'Operatore IdP verifica che il documento di riconoscimento caricato sia integro ed in corso di validità, rilasciato da un'Amministrazione dello Stato, munito di fotografia e firma autografa dello stesso e controlla la validità del codice fiscale/tessera sanitaria.

EHT è responsabile della valutazione in merito alla veridicità delle informazioni relative all'identità, quindi l'operatore preposto all'attività, in caso di verifiche negative o per mancanza parziale o totale della documentazione richiesta, non avvia la fase di identificazione e quindi di attivazione dell'ID, bensì contatta il Richiedente tramite mail chiedendo di caricare la documentazione valida in sostituzione a quella presentata, piuttosto che caricare quella mancante.

Il Richiedente può caricare i documenti richiesti nella form preposta, che visualizza cliccando il link all'interno della mail inviatagli. L'Operatore IdP verificherà nuovamente i documenti inseriti. Se la verifica è positiva, si procede alla fase di identificazione ed al rilascio dell'Identità Digitale.

La verifica degli attributi secondari avviene durante la procedura di richiesta.

Il rilascio dell'Identità SPID è subordinato all'esito positivo delle verifiche.

8.6 Procedura di rilascio, consegna e attivazione delle credenziali SPID

Le credenziali rilasciate al Richiedente, associate all'identità e al livello SPID richiesti, saranno consegnate in modalità sospesa.

Il Richiedente, per attivare le credenziali e poterle quindi utilizzare con la propria identità digitale, dovrà accedere al pannello di gestione dell'identità digitale e disporre l'attivazione.

9. GESTIONE DELLE IDENTITÀ DIGITALI

La procedura di gestione prevede:

1- Aggiornamento delle identità digitali a seguito delle richieste pervenute dai Titolari;

2- Aggiornamento della password o richiesta di ripristino della stessa;

3- Gestione dei dati raccolti per il termine di 20 anni decorrenti dalla revoca dell'identità digitale in ossequio al Reg. UE 679/2016: Copie dei documenti di identità, Moduli di richiesta al Servizio SPID, log di transazione (riconoscimenti via web e via CNS), Documenti firmati digitalmente (riconoscimenti con firma digitale), registrazioni audio/video (riconoscimenti con device), Modulo di adesione al Servizio SPID.

4- Gestione degli attributi: Aggiornamento anche a seguito di segnalazione da parte del gestore SPID, dei contenuti degli attributi identificativi comunicati in fase di iscrizione (attributi primari e secondari). Ad ogni variazione da operare sugli attributi relativi ad una identità, il gestore dell'identità digitale, prima di aggiornare i dati registrati, esegue le fasi di esame e verifica in relazione al livello SPID associato all'identità digitale

5- Sospensione e Revoca identità digitale. La sospensione è un provvedimento temporaneo con disattivazione delle credenziali di autenticazione assegnate al Titolare. La revoca rende inutilizzabili per sempre le credenziali digitali.

A mente dell'articolo 8, comma 3 e dell'articolo 9 del DPCM, il gestore revoca al Titolare l'identità digitale nei casi seguenti:

1. risulta non attiva per un periodo superiore a 24 mesi;
2. per decesso della persona;
3. per uso illecito dell'identità digitale;
4. per richiesta dell'utente;
5. per scadenza contrattuale.

Caso 1 e 5. Il Gestore avvisa il titolare con frequenze predeterminate ed in particolare 60, 30 e 5 giorni nonché il giorno precedente la revoca definitiva, attraverso comunicazioni mirate indirizzate alla e-mail del titolare ed al recapito di cellulare.

Caso 2. Il gestore dell'identità digitale procede alla revoca dell'identità digitale, previo accertamento utilizzando i servizi messi a disposizione dalle convenzioni di cui all'articolo 4, comma 1, lettera c) del DPCM

Caso 3. Il Titolare fa richiesta al Gestore via PEC, il quale provvede a sospendere l'identità digitale richiedendo copia della denuncia presentata presso autorità competente. Nel caso la stessa non giunga entro il termine di 30 giorni dalla richiesta, l'identità viene ripristinata.

Caso 4. Il Titolare fa richiesta al Gestore via PEC, il quale provvede a sospendere o a revocare, a seconda della istanza ricevuta, l'identità digitale del Titolare.

L'Identità Digitale nell'ambito di SPID può essere revocata su richiesta dell'UTENTE nei casi di:

A. smarrimento o furto delle credenziali di accesso;

B. smarrimento o furto della SIM con il numero di telefono indicato per la ricezione degli SMS.

La facoltà di revoca può essere esercitata dall'utente mediante invio dell'apposito modulo di revoca, disponibile per il download sia dalla sezione documenti del sito pubblico EtnaID.it, sia all'interno dell'area utente riservata (Profilo) del sito EtnaID.it. L'invio del modulo compilato e firmato può avvenire a mezzo pec all'indirizzo etnahitech@pec.it o tramite invio del modulo sottoscritto con firma digitale o firma elettronica qualificata attraverso i canali di supporto del servizio EtnaID accessibili dal sito pubblico EtnaID.it

All'interno della comunicazione di revoca, l'utente deve indicare la data a decorrere dalla quale richiede la cessazione del servizio ed allegare copia dei documenti di riconoscimento o in caso di furto/smarrimento degli stessi, allegare la relativa denuncia.

6- Gestione del ciclo di vita delle credenziali di autenticazione. Vengono seguiti i processi previsti dai regolamenti di cui all'Art 4 comma 2 del DPCM. Per l'intero ciclo di vita della credenziale conserva documentazione atta ad avere traccia delle seguenti informazioni: la creazione della credenziale, l'identificativo della credenziale; il soggetto per il quale è stata emessa; lo stato della credenziale. Per ogni sottoprocesso (creazione, emissione, attivazione, revoca, sospensione, rinnovo e sostituzione) del processo di gestione delle credenziali viene conservata idonea documentazione. Si conservano le informazioni relative alla data di creazione della credenziale, allo stato della stessa, alle date di consegna, di attivazione e di eventuale sospensione, revoca / cancellazione.

10. Gestione dei rapporti con i Titolari

I Titolari di una identità digitale possono richiedere assistenza e informazioni alla società mediante i seguenti canali:

Form Online presente all'url etnaid.it

Contatto telefonico: +39 095 8738230

Fax: +39 095 8738234

Email: info@etnahitech.com

PEC: etnahitech@pec.it

La società risponderà al Titolare utilizzando gli attributi secondari comunicati dal Titolare (E-mail e Numero di telefonia mobile)

11.MONITORAGGIO

Il sistema utilizzato per il monitoraggio delle componenti del servizio consente di valutare e di verificare continuamente, mediante l'aggiunta di appositi controlli, il regolare funzionamento di tutti i sottoservizi erogati nell'ambito dell'architettura impostata, nonché le prestazioni dei medesimi.

Offre una serie di strumenti avanzati e flessibili, che consentono di monitorare le funzionalità e l'integrità dei server fisici e virtuali in Cloud, della rete e dei servizi attraverso meccanismi visuali (mappe e grafici avanzati), utilizzando sistemi di notifica basati su e-mail, SMS e messaggistica in generale.

I parametri che vengono verificati all'interno dell'infrastruttura Cloud Privato e della piattaforma SPID sono:

- raggiungibilità sistemi;
- memoria RAM utilizzata;
- CPU utilizzate;
- raggiungibilità device di rete;
- spazio disco singoli sistemi;
- stato dei volumi/disponibilità storage;
- raggiungibilità di rete esterna /interna;
- tempo di accensione e orario di sistema.

Il sistema è configurato per rilevare anomalie ai sistemi attraverso due modalità:

- Polling – vengono interrogati ciclicamente tutti i server per verificare il loro stato.
- Trapping – il server informa la piattaforma di monitoraggio circa il verificarsi di una eccezione.

12.SICUREZZA DEL SERVIZIO

12.1 Conservazione della documentazione relativa al ciclo di vita di un'Identità Digitale

Secondo quanto specificato dal DPCM del 24 ottobre 2014, art.7 comma 8, Etna Hitech ha l'obbligo di conservazione delle informazioni e della documentazione raccolta durante il processo di adesione per un periodo pari a venti anni decorrenti dalla scadenza o dalla revoca dell'identità digitale.

12.2 Tracciatura delle informazioni del servizio

Ai fini della tracciatura, ogni transazione di autenticazione viene marcata temporalmente e registrata all'interno di un log certificato, contenente i record delle transazioni gestite negli ultimi 24 mesi, nel rispetto dell'art. 4 del DPCM del 24 ottobre 2014. Le tracciature sono salvate in maniera persistente e nel rispetto del codice della privacy, utilizzando meccanismi di cifratura dei dati e sistemi di basi di dati (DBMS), al fine di garantirne l'integrità, il non ripudio e la disponibilità.

Formato dei LOG

In accordo con quanto suggerito nel documento delle regole tecniche di SPID, per ogni transazione di autenticazione viene memorizzato un record contenente le seguenti

informazioni:

- l'identificativo dell'identità digitale (spidCode) interessata dalla transazione;
- la richiesta SAML (<AuthnRequest>) emessa dall'SP;
- la risposta SAML (<Response>) ricevuta da EtnaID;
- l'identificativo della richiesta;
- l'identificativo della risposta;
- il timestamp della richiesta;
- il timestamp della risposta;
- l'entityID del SP (issuer della richiesta);
- l'entityID di EtnaID (issuer della risposta);
- l'ID dell'asserzione di risposta SAML (<Assertion>);
- il soggetto dell'asserzione di risposta.

12.3 Procedura per la richiesta dei log certificato

L'utente titolare di un'Identità Digitale ha facoltà di richiedere in qualunque momento una copia delle informazioni contenute nel log certificato relative alle proprie credenziali SPID. Deve accedere, con le proprie credenziali, al portale di gestione dell'identità e da qui effettuare un'apposita richiesta indicando l'intervallo di date per cui intende ricevere le informazioni sull'utilizzo delle proprie credenziali SPID. La richiesta deve essere validata attraverso l'inserimento delle credenziali SPID di livello 2, ovvero con l'inserimento dell'OTP. Etna Hitech provvede alla raccolta delle informazioni richieste e alla produzione di un report, che viene quindi messo a disposizione per il download sul portale di gestione dell'identità.

13. LIVELLI DI SERVIZIO

Vengono descritti i Livelli di Servizio (SLA – Service Level Agreement) che il gestore garantisce nelle diverse fasi di erogazione del servizio:

1. fasi della registrazione al Servizio di identità digitale;
2. fasi della gestione del ciclo di vita delle Identità Digitali;
3. fasi del processo di autenticazione.

Ove non diversamente specificato, l'intervallo temporale di riferimento per il calcolo della disponibilità è il trimestre.

13.1. Livelli di servizio per la registrazione, il ciclo di vita delle identità digitali e il processo di autenticazione

ID	Indicatore di qualità	Modalità di Funzionamento	Valore limite
IQ-01	Disponibilità del sottoservizio di registrazione identità	*Erogazione automatica*	>= 99,5%
			Singolo evento di

			indisponibilità < =6 ore
IQ-02	Tempo di risposta del sottoservizio di registrazione identità		<= 24h (ore lavorative)
IQ-03	Disponibilità del sottoservizio di gestione rilascio credenziali	*Erogazione automatica*	>= 99,5%
			Singolo evento di indisponibilità < =6 ore
IQ-04	Tempo di rilascio credenziali		<= 3 giorni lavorativi
IQ-05	Tempo riattivazione delle credenziali		<= 2 giorni lavorativi
IQ-06	Disponibilità del sottoservizio di sospensione e revoca delle credenziali		>= 99,5%
			Singolo evento di indisponibilità < =6 ore
IQ-07	Tempo di sospensione delle credenziali	Erogazione automatica	< =1 minuti
		Erogazione manuale	< =10 minuti
IQ-08	Tempo di revoca delle credenziali		<= 5 giorni lavorativi
IQ-09	Disponibilità del sotto servizio di rinnovo e sostituzione delle credenziali	*Erogazione automatica*	>= 99,5%
			Singolo evento di indisponibilità < =6 ore
IQ-10	Tempo di rinnovo e sostituzione delle credenziali		<= 2 giorni lavorativi
IQ-10-bis	Tempo di dispiegamento/aggiornamento metadata		<= 2 giorni lavorativi
IQ-11	Disponibilità del sotto servizio di autenticazione		>= 99,5%
			Singolo evento indisponibilità <= 6 ore

IQ-12	Tempo di risposta del sotto servizio di autenticazione		*Coefficiente moltiplicativo* = 300 *300: tot. eID nazionale* = x *: tot. eID gestore* x = 300 × *t*to. eID gestore tot. eID nazionali x = numero effettivo di richieste di autenticazioni al secondo *(auth sec*) correlate alle identità rilasciate dal gestore. Se x < 100, il gestore deve garantire almeno *100 auth sec*. Tempi di risposta ≤ 2 sec per il 98% delle richieste di autenticazione Per un numero di richieste di *auth sec* superiore al *coefficiente moltiplicativo*, lo SLA andrà concordato in anticipo tra AgID e gestori.

Tabella 1 SLA del Gestore

ID	Indicatore di qualità	Valore limite
IQ-13	RPO sotto servizio registrazione e rilascio delle identità	1 ora
IQ-14	RTO sotto servizio registrazione e rilascio delle identità	8 ore
IQ-15	RPO sotto servizio di sospensione e revoca delle credenziali	1 ora
IQ-16	RTO sotto servizio di sospensione e revoca delle credenziali	8 ore
IQ-17	RPO sotto servizio di Autenticazione	1 ora
IQ-18	RTO sotto servizio di Autenticazione	8 ore

Tabella 2 SLA di Continuità Operativa

13.2. Tempi di servizio per la registrazione, il ciclo di vita delle identità digitali e il processo di autenticazione

- **Richiesta online da parte dell'utente**

  Erogazione automatica con finestra 24h/24h tutti i giorni della settimana, festivi inclusi Disponibilità ≥ 99,5 %

- **Riconoscimento/Identificazione**
  - Riconoscimento/Identificazione con TS-CNS/CNS Tutti i giorni della settimana, festivi inclusi, con finestra 24h/24h
  - Riconoscimento/Identificazione con Firma Digitale, Tutti i giorni lavorativi, dalle 9:00 alle 18:00
  - Riconoscimento/Identificazione via Webcam Tutti i giorni lavorativi, dalle 9:00 alle 18:00

- **Creazione dell'identità digitali e delle relative credenziali**

  Erogazione automatica con finestra 24h, tutti i giorni della settimana, festivi inclusi. Disponibilità ≥ 99,5%

- **Attivazione dell'identità digitale**

  Erogazione automatica con finestra 24h, tutti i giorni della settimana, festivi inclusi. Disponibilità ≥ 99,5%

- **Sospensione, riattivazione revoca tramite WEB**

  Erogazione automatica con finestra 24h, tutti i giorni della settimana, festivi inclusi. Disponibilità ≥ 99,5%

- **Sospensione, riattivazione revoca tramite Telefono**

  Tutti i giorni lavorativi, dalle 9:00 alle 18:00.

  Disponibilità ≥ 99,5%

- **Sospensione, riattivazione revoca tramite PEC**

  Tutti i giorni lavorativi, dalle 9:00 alle 18:00.

  Disponibilità ≥ 99,5%

- **Autenticazione del Titolare**

  Erogazione automatica con finestra 24h, tutti i giorni della settimana, festivi inclusi.

  Disponibilità come dal riferimento IQ-12 riportato in Tabella 1 SLA del Gestore.

14.TERMINI E CONDIZIONI DEL SERVIZIO

14.1. Obblighi del Titolare

L'Utente Titolare dell'Identità Digitale si obbliga a:

Esibire a richiesta del Gestore i documenti richiesti e necessari ai fini delle operazioni per la sua emissione e gestione

all'uso esclusivamente personale delle credenziali connesse all'Identità Digitale

a non utilizzare le credenziali in maniera tale da creare danni o turbative alla rete o a terzi utenti e a non violare leggi o regolamenti.

a non violare diritti d'autore, marchi, brevetti o altri diritti derivanti dalla legge e dalla consuetudine

a garantire l'utilizzo delle credenziali di accesso per gli scopi specifici per cui sono rilasciate con specifico riferimento agli scopi di identificazione informatica nel sistema SPID, assumendo ogni eventuale responsabilità per l'utilizzo per scopi diversi

all'uso esclusivo delle credenziali di accesso e degli eventuali dispositivi su cui sono custodite le chiavi private

a Sporgere senza indugi e tempestivamente denuncia alle Autorità competenti in caso di smarrimento o sottrazione delle credenziali attribuite

a fornire/comunicare al Gestore dati ed informazioni fedeli, veritieri e completi, assumendosi le responsabilità previste dalla legislazione vigente in caso di dichiarazioni infedeli o mendaci

ad accertarsi della correttezza dei dati registrati dal Gestore al momento dell'adesione e segnalare tempestivamente eventuali inesattezze

a informare tempestivamente il Gestore di ogni variazione degli attributi previamente comunicati

a mantenere aggiornati, in maniera proattiva o a seguito di segnalazione da parte del Gestore, i contenuti dei seguenti attributi identificativi:

- estremi del documento di riconoscimento e relativa scadenza, numero di telefonia fissa o mobile, indirizzo di posta elettronica, domicilio fisico e digitale,

a conservare le credenziali e le informazioni per l'utilizzo dell'identità digitale in modo da minimizzare i rischi

ad attenersi alle indicazioni fornite dal Gestore in merito all'uso del sistema di autenticazione, alla richiesta di sospensione o revoca delle credenziali, alle cautele che da adottare per la conservazione e protezione delle credenziali.

In caso di smarrimento, furto o altri danni/compromissioni richiedere immediatamente al Gestore la sospensione delle credenziali.

ad aggiornare la propria password secondo le indicazioni e le raccomandazioni previste dai regolamenti di cui all'Art 4 comma 2 del DPCM e descritti al §7 del presente documento.

14.2. Obblighi e Responsabilità del Gestore dell'Identità Digitale

Ai sensi dell'Art 1 lett. l, 7, 8 e 11 del DPCM, il Gestore dell'identità Digitale è tenuto:

Attribuire l'Identità Digitale, rilasciare le credenziali e gestire le procedure connesse al ciclo di vita dell'identità e delle credenziali attenendosi al DPCM e alle Regole Tecniche tempo per tempo emanate dall'AgID

Rilasciare l'identità su domanda dell'interessato ed acquisire e conservare il relativo

modulo di richiesta

Verificare l'identità del soggetto richiedente prima del rilascio dell'Identità Digitale

Conservare copia per immagine del documento di identità esibito e del modulo di adesione, nel caso di identificazione in presenza

Conservare copia del log della transazione nei casi di identificazione tramite documenti digitali di identità, identificazione informatica tramite altra identità digitale SPID o altra identificazione informatica autorizzata

Conservare il modulo di adesione allo SPID sottoscritto con firma elettronica qualificata o con firma digitale, in caso di identificazione tramite firma digitale

Verifica degli attributi identificativi del richiedente

Consegna in modalità sicura delle credenziali di accesso all'utente

Conservare la documentazione inerente al processo di adesione al servizio SPID per un periodo pari a venti anni decorrenti dalla scadenza o dalla revoca dell'identità digitale

Cancellare la documentazione inerente al processo di adesione trascorsi venti anni dalla scadenza o dalla revoca dell'identità digitale

Trattare e conservare i dati nel rispetto della normativa in materia di tutela dei dati personali di cui al Regolamento (UE) 2016/679 ed al decreto legislativo 30 giugno 2003, n. 196 e s.m.i..

Verificare ed aggiornare tempestivamente le informazioni per le quali il Titolare ha comunicato una variazione

Effettuare tempestivamente, su richiesta dell'utente, la sospensione o revoca di un'identità digitale, ovvero la modifica degli attributi secondari e delle credenziali di accesso

Revocare l'identità digitale se ne riscontra l'inattività per un periodo superiore a 24 mesi o in caso di decesso della persona.

Segnalare su richiesta dell'utente ogni avvenuto utilizzo delle sue credenziali di accesso, inviandone gli estremi ad uno degli attributi secondari indicati dall'utente

Verificare la provenienza della richiesta di sospensione da parte dell'utente con esclusione dei casi di invio tramite PEC o sottoscrizione con firma digitale o firma elettronica qualificata

Fornire, all'utente che l'ha inviata, conferma della ricezione della richiesta di sospensione

Sospendere tempestivamente l'identità digitale per un periodo massimo di trenta giorni ed informarne il richiedente.

Rispristinare o revocare l'identità digitale sospesa, nei casi previsti

Revocare l'identità digitale se riceve dall'utente copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti su cui è basata la richiesta di sospensione

Utilizzare sistemi informatici affidabili che garantiscono la sicurezza tecnica e

crittografica dei procedimenti, in conformità ai migliori criteri di sicurezza (best practice) riconosciuti in ambito europeo o internazionale

Adottare adeguate misure contro la contraffazione, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle credenziali di accesso

Effettuare un monitoraggio continuo al fine rilevare usi impropri o tentativi di violazione delle credenziali di accesso dell'identità digitale di ciascun utente, procedendo alla sospensione dell'identità digitale in caso di attività sospetta

Effettuare con cadenza almeno annuale un'analisi dei rischi che incombono sul servizio SPID

Definire, aggiornare e trasmettere ad AGID il piano per la sicurezza dei servizi SPID

Condurre con cadenza almeno semestrale il Penetration Test sulle proprie infrastrutture e applicazioni implicate nel servizio SPID

Garantire la continuità operativa dei servizi afferenti allo SPID attraverso la formalizzazione di un piano di continuità operativa e di Disaster Recovery

Garantire la gestione sicura delle componenti riservate delle identità digitali assicurando non siano rese disponibili a terzi, ivi compresi i fornitori di servizi stessi, neppure in forma cifrata

Garantire la disponibilità delle funzioni, l'applicazione dei modelli architetturali e il rispetto delle disposizioni previste dalla normativa

Sottoporsi con cadenza almeno biennale ad una verifica di conformità alle disposizioni vigenti

Informare tempestivamente l'AgID e il Garante per la protezione dei dati personali su eventuali violazioni di dati personali nei termini prescritti dal Reg ue 679/2016

Adeguare i propri sistemi a seguito dell'aggiornamento della normativa

Inviare all'AGID in forma aggregata i dati richiesti a fini statistici, che potranno essere resi pubblici.

In caso intendesse cessare la propria attività, comunicarlo all'AGID "e ai titolari" almeno sessanta (60) giorni prima della data di cessazione, indicando i gestori sostitutivi e le modalità tecniche e operative per il trasferimento delle identità digitali, nel rispetto delle indicazioni fornite da AGID.

In caso in cui, a seguito della cessazione dell'attività o della revoca del suo accreditamento, nessun altro gestore è disponibile a subentrare, secondo le indicazioni di AGID, provvede a ridistribuire le identità digitali rilasciate tra tutti gli altri gestori che subentreranno nella relativa gestione in misura proporzionale alla ripartizione percentuale, tra gli stessi, di tutte le identità SPID rilasciate alla data della cessazione o della revoca

In caso di subentro ad un gestore cessato, gestire le identità digitali che questi ha rilasciato dal gestore cessato e ne conserva le informazioni

Informare espressamente il richiedente in modo compiuto e chiaro degli obblighi che assume in merito alla protezione della segretezza delle credenziali, sulla procedura di

autenticazione e sui necessari requisiti tecnici per accedervi

Se richiesto dal titolare, segnalargli via e-mail o via sms, ogni avvenuto utilizzo delle sue credenziali di accesso.

Notificare al titolare la richiesta di aggiornamento e l'aggiornamento effettuato agli attributi relativi della sua identità digitale

Nel caso l'identità digitale risulti non attiva per un periodo superiore a 24 mesi o il contratto sia scaduto, revocarla e informarne l'utente via posta elettronica e numero di telefono mobile

In caso di decesso del titolare, revocare previo accertamento, l'identità digitale

Nel caso in cui l'utente richieda la sospensione della propria identità digitale per sospetto uso fraudolento, fornirgli evidenza dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione dell'identità digitale, raccomandando la consegna della denuncia che il Titolare dovrà sporgere presso l'Autorità Giudiziaria competente.

Trascorsi trenta giorni dalla sospensione su richiesta dell'utente per sospetto uso fraudolento, ripristinare l'identità sospesa qualora non ricevesse copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti sui quali è stata basata la richiesta di sospensione.

Nel caso in cui l'utente richieda la sospensione o la revoca della propria identità digitale tramite PEC o richiesta sottoscritta con firma digitale o elettronica inviata via posta elettronica, fornire evidenza all'utente dell'avvenuta presa in carico della richiesta e procedere alla immediata sospensione o alla revoca dell'identità digitale.

Ripristinare l'identità sospesa su richiesta dell'utente se non riceve entro 30 giorni dalla sospensione una richiesta di revoca da parte dell'utente.

In caso di richiesta di revoca di dell'identità digitale, revocare le relative credenziali e conservare la documentazione inerente al processo di adesione per 20 anni dalla revoca dell'identità digitale.

Proteggere le credenziali dell'identità digitale contro abusi ed usi non autorizzati adottando le misure tecniche ed organizzative richieste dalla normativa.

All'approssimarsi della scadenza dell'identità digitale, comunicarla all'utente e, dietro sua richiesta, provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella scaduta

In caso di guasto o di upgrade tecnologico provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella sostituita.

Non mantenere alcuna sessione di autenticazione con l'utente nel caso di utilizzo di credenziali di livelli 2 e 3

Conservare e tenere aggiornato il Registro delle Transazioni contenente i tracciati delle richieste di autenticazione servite nei 24 mesi precedenti, curandone riservatezza, inalterabilità e integrità, mettendo in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio secondo quanto previsto dalla

normativa vigente in materia di trattamento dei dati personali ed utilizzando tecniche di cifratura

14.3. Obblighi dei fornitori di Servizi

I fornitori di servizi che utilizzano le identità digitali al fine dell'erogazione dei propri servizi hanno i seguenti obblighi:

Conoscere l'ambito di utilizzo delle identità digitali, le limitazioni di responsabilità e i limiti di indennizzo del IdP, riportati nel presente Manuale Operativo;

Osservare quanto previsto dall'art. 13 del DPCM e dagli eventuali Regolamenti di cui all'art. 4 del DPCM medesimo;

Adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

14.4. Obblighi della Registration Authority Locale (LRA)

La LRA per mezzo dei RAO è tenuta a:

- informare il Titolare in modo compiuto e chiaro, sulla procedura di rilascio SPID e sui necessari requisiti per accedervi, sulle caratteristiche, sulle precauzioni e sulle limitazioni d'uso delle identità emesse sulla base del servizio SPID;

- informare il Titolare riguardo agli obblighi da quest'ultimo assunti in merito a conservare con la massima diligenza, le credenziali (password, dispositivi otp, anche software) associate all'identità, al fine di garantirne l'integrità e la massima riservatezza;

- informare il Titolare riguardo agli obblighi da quest'ultimo assunti in merito a conservare con la massima diligenza la credenziale OTP eventualmente fornita;

- informare il titolare delle misure di sicurezza adottate per il trattamento dei dati personali;

- provvedere con certezza all'identificazione della persona che fa richiesta dell'identità SPID;

- verificare che i documenti presentati per l'identificazione non siano contraffatti;

- accertare l'autenticità della richiesta di adesione al servizio SPID;

- comunicare al Gestore tutti i dati e documenti acquisiti durante l'identificazione del Titolare e previsti dalle procedure al fine di avviare tempestivamente le attività di emissione dell'identità digitale;

- attenersi scrupolosamente alle regole impartite dal Gestore e presenti su questo documento;

- verificare ed accertarsi che l'utente abbia preso visione e compreso le regole per l'uso del sistema SPID.

I RAO sono autorizzati ad operare dal Gestore a seguito di adeguato addestramento del personale addetto. Il Gestore, salvo diritto di rivalsa, resta comunque l'unico ed il solo responsabile verso terzi dell'attività svolta dall'LRA.

Il Gestore verifica periodicamente la rispondenza delle procedure adottate dalla LRA e dai suoi RAO e quanto indicato nel presente documento. In ogni caso, a semplice richiesta del Gestore, la LRA è tenuta a trasmettere allo stesso tutta la documentazione in proprio possesso, relativa a ciascuna richiesta di emissione dell'identità digitale proveniente da ciascun Titolare.

14.5. Obblighi del Richiedente

La Persona fisica o giuridica che richiede una o più identità digitali da attribuire ai Titolari è tenuto a prendere attenta visione e a rispettare il presente Manuale Operativo.

14.6. Clausola risolutiva espressa

L'inadempimento da parte del Titolare o del Richiedente agli obblighi sopra indicati costituisce grave inadempimento ai sensi dell'art. 1456 codice civile e conferisce facoltà al Gestore dell'identità digitale di risolvere il contratto in essere, mediante invio di una comunicazione a mezzo raccomandata A/R o messaggio di PEC contenente la contestazione dell'inadempimento e l'intento di avvalersi della risoluzione stessa.

14.7. Obblighi connessi al trattamento dei dati personali

La Società ha posto in essere idonee misure tecnico organizzative per la tutela la riservatezza, integrità e disponibilità dei dati personali come previsto dal Regolamento dell'Unione Europea n. 2016/679.

In ossequio all'art. 13 vengono fornite all'utente ("Interessato") tutte le informazioni richieste dalla normativa relative al trattamento dei propri dati personali mediante apposita, specifica e preventiva informativa, resa altresì sempre disponibile all'interno del proprio sito istituzionale.

14.8. Nullità od inapplicabilità di clausole

Se una qualsivoglia disposizione del presente Manuale Operativo, o relativa applicazione, risulti per qualsiasi motivo o in qualunque misura nulla o inapplicabile, il resto del presente Manuale Operativo (così come l'applicazione della disposizione invalida o inapplicabile ad altre persone o in altre circostanze) rimarrà valido e la disposizione nulla o inapplicabile sarà interpretata nel modo più vicino possibile agli intenti delle parti

14.9. Foro competente

Per tutte le eventuali controversie giudiziarie nelle quali risulti attore o convenuto il Gestore dell'identità digitale e relative all'utilizzo del servizio di identità digitale e, alle modalità operative e all'applicazione delle disposizioni del presente Manuale sarà competente esclusivamente il Foro di Catania.

Appendice A –Tabella messaggi di anomalia

Error Code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/StatusMessage	Destinatario notifica	Schermata Idp	Troubleshooting utente	Troubleshooting SP	Note
1	Autenticazione corretta	HTTP POST HTTP Redirect	HTTP 200	urn:oasis:names:tc:SAML:2.0:status:Success	Fornitore del servizio (SP)	n.a.	n.a.	n.a.	
Anomalie di Sistema									
2	Indisponibilità sistema	HTTP POST	n.a.	n.a.	Utente	Messaggio di errore generico	Ripetere l'accesso al servizio più tardi	n.a.	
3	Errore di sistema	HTTP Redirect	HTTP 500	n.a.	Utente	Pagina di cortesia con messaggio "Sistema di autenticazione non disponibile - Riprovare più tardi"	Ripetere l'accesso al servizio più tardi	n.a.	Tutti i casi di errore di sistema in cui è possibile mostrare un messaggio informativo all'utente
Anomalie delle richieste									
Anomalie sul binding									

Error Code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/StatusMessage	Destinatario notifica	Schermata Idp	Troubleshooting utente	Troubleshooting SP	Note
4	Formato binding non corretto	HTTP Redirect	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "Formato richiesta non corretto - Contattare il gestore del servizio"	Contattare il gestore del servizio	Verificare la conformità con le regole tecniche SPID del formato del messaggio di richiesta	Parametri obbligatori: SAMLRequest SigAlg Signature Parametri non obbligatori: RelayState
		HTTP POST							Parametri obbligatori: SAMLRequest Parametri non obbligatori: RelayState
5	Verifica della firma fallita	HTTP Redirect	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "Impossibile stabilire l'autenticità della richiesta di autenticazione - Contattare il gestore del servizio"	Contattare il gestore del servizio	Verificare certificato o modalità di apposizione firma	Firma sulla richiesta non presente, corrotta, non conforme in uno dei parametri, con certificato scaduto o con certificato non

Error Code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/StatusMessage	Destinatario notifica	Schermata Idp	Troubleshooting utente	Troubleshooting SP	Note
									associato al corretto EntityID nei metadati registrati
6	Binding su metodo HTTP errato	HTTP Redirect	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "Formato richiesta non ricevibile - Contattare il gestore del servizio"	Contattare il gestore del servizio	Verificare metadata Gestore dell'identità (IdP)	Invio richiesta in HTTP-Redirect su entry point HTTP-POST dell'identità
		HTTP POST							Invio richiesta in HTTP-POST su entry point HTTP-Redirect dell'identità
Anomalie sul formato della AuthnReq									
7	Errore sulla verifica della firma della richiesta	HTTP POST	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "Formato richiesta non corretto - Contattare il gestore del	Contattare il gestore del servizio	Verificare certificato o modalità di apposizione firma	Firma sulla richiesta non presente, corrotta, non

Error Code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/StatusMessage	Destinatario notifica	Schermata Idp	Troubleshooting utente	Troubleshooting SP	Note
						servizio"			conforme in uno dei parametri, con certificato scaduto o con certificato non associato al corretto EntityID nei metadati registrati
8	Formato della richiesta non conforme alle specifiche SAML	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester ErrorCode nr08	Fornitore del servizio (SP)	n.a.	n.a.	Formulare la richiesta secondo le regole tecniche SPID - Fornire pagina di cortesia	Non conforme alle specifiche SAML - il controllo deve essere operato successivamente alla verifica positiva della firma
9	Parametro *version* non presente, malformato o diverso da '2.0'	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:VersionMismatch ErrorCode nr09	Fornitore del servizio (SP)	n.a.	n.a.	Formulare la richiesta secondo le regole tecniche SPID - Fornire pagina di cortesia all'utente	

Error Code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/StatusMessage	Destinatario notifica	Schermata Idp	Troubleshooting utente	Troubleshooting SP	Note
10	Issuer non presente, malformato o non corrispondente all'entità che sottoscrive la richiesta	HTTP POST / HTTP Redirect	HTTP 403	n.a.	Utente	Pagina di cortesia con messaggio "Formato richiesta non corretto - Contattare il gestore del servizio"	Contattare il gestore del servizio	Verificare formato delle richieste prodotte	
11	Identificatore richiesta(ID) non presente, malformato o non conforme	HTTO POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester ErrorCode nr11	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	Identificatore necessario per la correlazione con la risposta
12	RequestAuthnContext non presente, malformato o non previsto da SPID	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:statuss:NoAuthnContext ErrorCode nr12	Fornitore del servizio (SP)	Pagina temporanea con messaggio di errore: "Autenticazione SPID non conforme o non specificata"		Informare l'utente	AUTH livello richiesto diverso da: urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL1 urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL2 urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL3

Error Code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/StatusMessage	Destinatario notifica	Schermata Idp	Troubleshooting utente	Troubleshooting SP	Note
13	IssueInstant non presente, malformato o non coerente con l'orario di arrivo della richiesta	HTTP POST / HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestDenied ErrorCode nr13	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	
14	destination non presente, malformata o non coincidente con il Gestore delle identità ricevente la richiesta	HTTP POST / HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr14	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	
15	attributo isPassive presente e attualizzato al valore true	HTTP POST / HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:NoPassive ErrorCode nr15	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	
16	AssertionConsumerService non correttamente valorizzato	HTTP POST / HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr16	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	AssertionConsumerServiceIndex presente e attualizzato con valore non riportato nei metadata AssertionConsumerServiceIndex riportato in

Error Code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/StatusMessage	Destinatario notifica	Schermata Idp	Troubleshooting utente	Troubleshooting SP	Note
									presenza di uno od entrambi gli attributi AssertionConsumerService URL e Protocol Binding
									AssertionConsumerServiceIndex non presente in assenza di almeno un attributo AssertionConsumerService URL e Protocol Binding
									La *response* deve essere inoltrata presso *AssertionConsumerService* di default riportato nei *metadata*

Error Code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/StatusMessage	Destinatario notifica	Schermata Idp	Troubleshooting utente	Troubleshooting SP	Note
17	Attributo Format dell'elemento NameIDPolicy assente o non valorizzato secondo specifica	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr17	Fornitore del servizio (SP)	n.a.	n.a.	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente	Nel caso di valori diversi dalla specifica del parametro opzionale AllowCreate si procede con l'autenticazione senza riportare errori
18	AttributeConsumerServiceIndex malformato o che riferisce a un valore non registrato nei metadati di SP	HTTO POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Requester urn:oasis:names:tc:SAML:2.0:status:RequestUnsupported ErrorCode nr18	Fornitore del servizio (SP)	n.a.	n.a.	Riformulare la richiesta con un valore dell'indice presente nei metadati	
Anomalie derivanti dall'utente									

Error Code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/StatusMessage	Destinatario notifica	Schermata Idp	Troubleshooting utente	Troubleshooting SP	Note
19	Autenticazione fallita per ripetuta sottomissione di credenziali errate (superato numero di tentativi secondo le policy adottate)	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr19	HTTP POST / HTTP Redirect	Messaggio di errore specifico ad ogni interazione prevista	Inserire credenziali corrette	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	Si danno indicazioni specifiche e puntuali all'utente per risolvere l'anomalia, rimanendo nelle pagine dello IdP. Solo al verificarsi di determinate condizioni legate alle policy di sicurezza aziendali, ad esempio dopo 3 tentativi falliti, si risponde al SP
20	Utente privo di credenziali compatibili con il livello richiesto dal fornitore del servizio	HTTO POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr20	Fornitore del servizio (SP)	n.a.	Acquisire credenziali di livello idoneo all'accesso al servizio richiesto	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	

Error Code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/StatusMessage	Destinatario notifica	Schermata Idp	Troubleshooting utente	Troubleshooting SP	Note
21	Timeout durante l'autenticazione utente	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr21	Fornitore del servizio (SP)	n.a.	Si ricorda che l'operazione di autenticazione deve essere completata entro un determinato periodo di tempo	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	
22	Utente nega il consenso all'invio di dati al SP in caso di sessione vigente	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr22	Fornitore del servizio (SP)		Dare consenso	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	Sia per autenticazione da fare, sia per sessione attiva di classe SpidL1
23	Utente con identità sospesa/revocata o con credenziali bloccate	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr23	Fornitore del servizio (SP)	Pagina temporanea con messaggio di errore: "Credenziali sospese o revocate"		Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	

Error Code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/StatusMessage	Destinatario notifica	Schermata Idp	Troubleshooting utente	Troubleshooting SP	Note
25	Processo di autenticazione annullato dall'utente	HTTP POST	n.a.	ErrorCode nr25	Fornitore del servizio (SP)	non applicabile	non applicabile	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	
26	Processo di erogazione dell'identità digitale andata a buon fine	HTTP POST	n.a.	ErrorCode nr26	Fornitore del servizio (SP)		Identità Digitale erogata con successo		
27	Utente già presente	HTTP POST	n.a.	ErrorCode nr27	Fornitore del servizio (SP)		Utente già in possesso dell'Identità Digitale con il Fornitore di Identità Digitale selezionato		
28	Operazione annullata	HTTP POST	n.a.	ErrorCode nr28	Fornitore del servizio (SP)		Operazione di richiesta identità digitale annullata dall'utente		

Error Code	Scenario di riferimento	Binding	HTTP status code	SAML Status code/Sub Status/StatusMessage	Destinatario notifica	Schermata Idp	Troubleshooting utente	Troubleshooting SP	Note
29	Identità non erogata	HTTP POST	n.a.	ErrorCode nr29	Fornitore del servizio (SP)		Il fornitore non ha erogato l'identità digitale		
30	Il SP ha richiesto di autenticare l'utente con un'identità digitale uso professionale ma l'utente ha utilizzato l'identità digitale da cittadino (non per uso professionale)	HTTP POST HTTP Redirect	n.a.	urn:oasis:names:tc:SAML:2.0:status:Responder urn:oasis:names:tc:SAML:2.0:status:AuthnFailed ErrorCode nr30	Fornitore del servizio (SP)	n.a.	Utilizzare un'identità digitale uso professionale	Fornire una pagina informative per comunicare all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto.	