MANUALE OPERATIVO SPID

ICERT-MO-SPID

InfoCert
GRUPPO TECNOINVESTIMENTI

SOMMARIO

INDICE DELLE FIGURE

INDICE DELLE TABELLE

1 DATI IDENTIFICATIVI DEL GESTORE

InfoCert S.p.A. è il Gestore dell'Identità Digitale che rilascia, previa verifica dell'identità del soggetto Utente Titolare, in modalità sicura le credenziali di accesso operando in conformità al DPCM, alle Regole Tecniche e secondo quanto prescritto dal CAD. In questo documento si usa il termine Identity Provider, o per brevità IdP, per indicare InfoCert.
I dati completi dell'organizzazione che svolge la funzione di IdP sono i seguenti:

Denominazione Sociale	**InfoCert Società per Azioni**
Sede legale	Piazza Sallustio 9 00187 Roma
Sede operativa	Via Marco e Marcelliano 45, 00147 Roma
Rappresentante legale	Daniele Vaccarino In qualità di Presidente del Consiglio d'Amministrazione
Amministratore Delegato	Danilo Cattaneo
N° telefono	06 836691
N° Iscrizione Registro Imprese	07945211006
N° partita IVA	07945211006
Sito web	http://www.infocert.it/
Responsabile Manuale Operativo	Responsabile del Servizio SPID Antonio Dal Borgo

TABELLA 1 - DATI IDENTIFICATIVI DEL GESTORE

1.1 SISTEMI DI QUALITÀ

Tutti i processi operativi del Gestore descritti in questo Manuale Operativo, come ogni altra attività del Gestore, sono conformi allo standard ISO9001.
InfoCert possiede le seguenti certificazioni:

- **ISO 9001:2008**, conseguita il 10 aprile 2008, è il **Sistema di Gestione per la Qualità** finalizzato a rispondere agli obiettivi aziendali di garantire un miglioramento continuo della soddisfazione delle esigenze dei clienti, ottimizzare l'organizzazione delle risorse e le interazioni tra i processi aziendali, ridurre il più possibile il verificarsi di situazioni e condizioni di non conformità dei prodotti e/o servizi. Il sistema di gestione qualità InfoCert conferma la struttura affidabile dell'azienda che garantisce la riproducibilità delle sue performance, il mantenimento e il miglioramento dello standard qualitativo dei propri servizi/prodotti e costituisce inoltre una garanzia di affidabilità dei processi produttivi per i clienti, per i fornitori ma anche dipendenti e collaboratori.
- **ISO 27001:2013**, conseguita il 31 marzo 2011 come ISO 27001:2005 e come ISO 27001:2013 nel marzo 2015, è il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), certificato per le attività EA:33-35.
- **ISO 20000:2011,** conseguita il 23 marzo 2012, è il Sistema di Gestione dei Servizi conforme allo standard internazionale per l'IT Service Management, con lo scopo di mantenere e

migliorare l'allineamento e la qualità dei servizi di business erogati in relazione ai requisiti cliente, attraverso un ciclo costante di monitoraggi, reporting e revisione degli SLA concordati. Il modello di Service Management System [SMS] InfoCert permette di mappare ed integrare i Livelli di Servizio (SLA) garantiti ai clienti in relazione a tutta la catena del valore dei servizi [OLA e UC], facilitare l'allineamento tra i requisiti del cliente e l'offerta InfoCert impostando/definendo accordi di servizio formalizzati e misurabili (SLA) e garantiti, garantire un controllo dei fornitori che concorrono alla erogazione dei nostri servizi

- **ISO 14001:2004**, conseguita il 29 novembre 2013, è il Sistema di Gestione Ambientale e risponde alla strategia aziendale di attuare un controllo del rispetto delle normative ambientali, un miglioramento di efficienza nei processi, una attenta risposta alle richieste dei clienti e della comunità con l'obiettivo di rispondere ad un comportamento responsabile dell'impresa.

I certificati relativi alle certificazioni e ai modelli di gestione adottati da InfoCert sono presenti sul sito www.infocert.it.

2 DATI IDENTIFICATIVI DEL MANUALE

2.1 GENERALITÀ

Il presente Manuale Operativo, compilato dal IdP nel rispetto delle indicazioni legislative, è stato consegnato in copia all'Agenzia.
Al momento della richiesta di accreditamento, InfoCert fornisce all'Agenzia i dati identificativi richiesti, che vengono da quest'ultima sottoscritti, conservati e pubblicati.
Questo documento è denominato "Sistema Pubblico Identità Digitale – Manuale Operativo InfoCert" ed è caratterizzato dal codice documento: **ICERT-MO-SPID**.
La versione e il livello di rilascio sono identificabili in testa ad ogni pagina.
Questo documento è pubblicato in formato elettronico presso il sito Web dell'IdP all'indirizzo: https://www.identitadigitale.infocert.it.

Novità introdotte rispetto alla precedente versione:

Versione/Release n°	3.0	Data Versione/Release	18/06/2018
Descrizione Modifiche	- Cambio numero Call Center; - Aggiornamento riferimento alla normativa in materia di trattamento dei dati personali.		
Motivazioni	- Sostituzione Call Center; - Attuazione Regolamento Europeo (GDPR) UE 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali, pienamente vincolante dal 25 maggio 2018		

Versione/Release n°	2.0	Data Versione/Release	10/04/2017
Descrizione Modifiche	- Previsione della modalità di riconoscimento in presenza in uno degli InfoCert point aderenti; - Aggiornamento layout grafico.		
Motivazioni	- Adeguamento del documento rispetto alle modalità di identificazione poste in essere da InfoCert; - Adeguamento del layout del documento alla nuova visual identity InfoCert.		

Versione/Release n°	1.0	Data Versione/Release	18/12/2015
Descrizione Modifiche	Nessuna		
Motivazioni	Prima Emissione		

2.2 SCOPO DEL DOCUMENTO

Il documento ha lo scopo di descrivere le regole e le procedure operative adottate dal gestore di identità digitali InfoCert per la messa a disposizione e la gestione degli attributi utilizzati dagli utenti al fine di identificazione informatica nel Sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), di cui all'art. 64 del decreto legislativo n. 82 del 2005.

Il presente Manuale Operativo si riferisce a:

- Identità Digitali SPID di **livello 1**
- Identità Digitali SPID di **livello 2**

Alla data della presente versione, l'IdP non eroga e gestisce Identità Digitali SPID di livello 3.

Nel presente documento, inoltre, sono descritti i servizi necessari a gestire l'attribuzione dell'identità digitale degli utenti, la distribuzione e l'interoperabilità delle credenziali di accesso, la riservatezza delle informazioni gestite e l'autenticazione informatica.
Il contenuto si basa sulle norme vigenti alla data di emissione. Il diritto d'autore sul presente documento è di InfoCert S.p.A.; è riservato ogni diritto e utilizzo.

2.3 RESPONSABILE DEL MANUALE OPERATIVO

InfoCert è responsabile della definizione, pubblicazione ed aggiornamento di questo documento. Domande, reclami, osservazioni e richieste di chiarimento in ordine al presente Manuale Operativo dovranno essere rivolte all'indirizzo e alla persona di seguito indicate:

InfoCert S.p.A.	
Responsabile del Servizio di Identità Digitale	
	Piazza Luigi da Porto 3
	35131 Padova
Telefono	06836691
Fax	049 097 8914
Call Center	0654641489
Web	https://www.identitadigitale.infocert.it
PEC	infocert@legalmail.it

TABELLA 2 - RESPONSABILE DEL MO

L'Utente può richiedere copia della documentazione a lui relativa, compilando e inviando il modulo disponibile sul sito https://www.identitadigitale.infocert.it e seguendo la procedura ivi indicata.

La documentazione verrà inviata in formato elettronico all'indirizzo di email indicato nel modulo.
Il presente Manuale Operativo è reperibile:

- In formato elettronico presso il sito web dell'IdP
- In formato cartaceo, richiedibile all'IdP

2.4 PROCEDURE PER L'AGGIORNAMENTO DEL MANUALE OPERATIVO

L'IdP si riserva di apportare variazioni al presente documento per esigenze tecniche o per modifiche alle procedure intervenute sia a causa di norme di legge o regolamenti, sia per ottimizzazioni del ciclo lavorativo.
Ogni nuova versione del Manuale Operativo annulla e sostituisce le precedenti versioni.

Variazioni che non hanno un impatto significativo sugli utenti comportano l'incremento del numero di release del documento, mentre variazioni con un impatto significativo sugli utenti (come ad esempio modifiche rilevanti alle procedure operative) comportano l'incremento del numero di versione del documento. In ogni caso il manuale sarà prontamente pubblicato e reso disponibile secondo le modalità previste.
Ogni variazione al manuale operativo sarà preventivamente comunicata all'Agenzia che, per approvazione, provvederà a sottoscrivere e pubblicare sul proprio sito la nuova versione o release.

2.5 METODI DI GESTIONE DEI RAPPORTI CON GLI UTENTI

I rapporti con i clienti, riguardanti eventuali problematiche o richieste di qualsiasi tipo aventi ad oggetto le credenziali SPID, saranno gestite attraverso le seguenti modalità:

Canali di contatto	
Call Center	0654641489
From online	https://help.infocert.it/contatti/
Chat	https://help.infocert.it/contatti/
PEC	infocert@legalmail.it
Fax	049.0978914

TABELLA 3 – CANALI DI CONTATTO PER GLI UTENTI

Per maggiori dettagli e informazioni in merito alle modalità di assistenza si rimanda alla sezione Assistenza Clienti InfoCert.

2.6 GUIDA UTENTE

La guida utente è denominata "Manuale Utente_SPID" [8]. La guida utente è un documento esplicativo e di facile comprensione per l'Utente che potrà essere reperito sul sito https://www.identitadigitale.infocert.it.
All'interno del documento è possibile avere una descrizione dettagliata delle modalità d'uso e di attivazione delle credenziali, le modalità per richiedere la sospensione o la revoca e le cautele in capo al Titolare per la conservazione e la protezione delle credenziali.

2.7 RIFERIMENTI

2.7.1 RIFERIMENTI NORMATIVI

[1] Decreto Legislativo 7 marzo 2005, n.82 (G.U. n.112 del 16 maggio 2005) – Codice dell'amministrazione digitale (nel seguito referenziato come **CAD**) e successive modifiche e integrazioni
[2] 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.

Referenziato nel seguito come **DPCM**

[3] Regolamento Europeo UE 2016/679 del 27 aprile 2016 (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento e alla libera circolazione dei dati personali**,** pienamente vincolante dal 25 maggio 2018.

[4] Regolamento (UE) n. 910/2014 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)

[5] 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

2.7.2 ALTRI RIFERIMENTI

[6] **ICERT-PEC-MO** – Manuale Operativo - Servizio di Posta Elettronica Certificata InfoCert S.p.A.

[7] **ICERT-INDI-MO** – Manuale Operativo Certificati di Sottoscrizione InfoCert S.p.A.

[8] **Manuale Utente_SPID** – Guida Utente del servizio

[9] **Manuale di Conservazione** – Manuale del sistema accreditato del sistema di conservazione elettronica dei documenti

2.8 DEFINIZIONI

Vengono di seguito elencate le definizioni utilizzate nella stesura del presente documento. Per i termini definiti dal **CAD** e dal **DPCM** si rimanda alle definizioni in essi stabilite. Dove appropriato viene indicato tra parentesi quadre il termine inglese corrispondente, generalmente usato nella pubblicistica, negli standard e nei documenti tecnici.

Agenzia – cfr. DPCM

Autorità per la marcatura temporale *[Time-stamping authority]*

È il sistema software/hardware, gestito dal ***Certificatore***, che eroga il servizio di marcatura temporale.

Attributi identificativi – cfr. DPCM

Nome, cognome, luogo e data di nascita, sesso, ovvero ragione o denominazione sociale, sede legale, nonché' il codice fiscale o la partita IVA e gli estremi del documento d'identità utilizzato ai fini dell'identificazione.

Attributi secondari – cfr. DPCM

Il numero di telefonia fissa o mobile, l'indirizzo di posta elettronica, il domicilio fisico e digitale, nonché' eventuali altri attributi individuati dall'Agenzia, funzionali alle comunicazioni.

Attributi qualificati – cfr. DPCM

Le qualifiche, le abilitazioni professionali e i poteri di rappresentanza e qualsiasi altro tipo di

attributo attestato da un gestore di attributi qualificati.

Certificato Qualificato – cfr. CAD

Certificatore *[Certification Authority]* – cfr. CAD

Certificatore Accreditato – cfr. CAD – art.27

Certificatore Qualificato – cfr. CAD – art. 29

Certification Service Provider

Autorità di certificazione di firma digitale accreditata presso l'Agenzia dell'Italia Digitale. È InfoCert o un altro Certificatore Accreditato in caso di utente già dotato di firma digitale.

Credenziali di accesso – cfr. DPCM

il particolare attributo di cui l'utente si avvale, unitamente al codice identificativo, per accedere in modo sicuro, tramite autenticazione informatica, ai servizi qualificati erogati in rete dai fornitori di servizi che aderiscono allo SPID.

Dispositivo sicuro per la creazione della firma

Un dispositivo rispondente ai requisiti di cui all'Allegato III della Direttiva EU EC/99/93 (che verrà sostituita dal luglio 2016 del Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche [4] che indirizza lo stesso tema nell'Allegato II).

Distributore o Rivenditore che funge da Ufficio di Registrazione

Persona Giuridica che si impegna a compiere le preliminari operazioni di raccolta dei dati relativi ai richiedenti le credenziali SPID, la loro identificazione nonché il successivo eventuale rilascio delle medesime credenziali, nel pieno rispetto degli obblighi definiti dalla Convenzione sottoposta dall'IdP e successivamente sottoscritta.

Evidenza Informatica

Sequenza di simboli binari (bit) che può essere oggetto di una procedura informatica.

Firma elettronica – cfr. CAD

Firma elettronica qualificata – cfr. CAD

Firma digitale *[digital signature]* – cfr. CAD

Identità digitale [ID]:

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 le modalità di cui al DPCM e dei suoi regolamenti attuativi.

Identity provider [IdP]

È il gestore dell'identità digitale di cui alla lett. l) dell'art. 1 del DPCM. Nel presente documento è InfoCert nella sua qualità di soggetto accreditato allo SPID.

Intestatario della Fattura

Persona fisica o giuridica cui è emessa la fattura relativa al servizio di emissione dell'identità digitale attribuita al Titolare. Può coincidere con l'Utente Titolare e/o con il Richiedente.

Incaricato alla Registrazione [IR]

Persona fisica o giuridica cui è affidato lo svolgimento delle attività di identificazione dell'Utente. Gli Incaricati alla Registrazione operano sulla base delle istruzioni ricevute

dall'IdP con il quale hanno stipulato apposita Convenzione.

Intermediario Finanziario

Entità soggetta alla vigilanza di Banca d'Italia che ha l'obbligo di identificare i propri clienti ai sensi della normativa antiriciclaggio in ossequio a quanto previsto dal D.Lgs 231/2007.

Manuale Operativo

Il Manuale Operativo definisce le procedure che l'IdP applica nello svolgimento del servizio. Nella stesura del Manuale sono state seguite le indicazioni espresse dall'Autorità di vigilanza e quelle della letteratura internazionale.

Persona Fisica

Soggetto dotato di capacità giuridica.

Persona Giuridica

Organismo unitario, caratterizzato da una pluralità di individui o da un complesso di beni, al quale viene riconosciuta dal diritto capacità di agire in vista di scopi leciti e determinati.

Pubblico ufficiale

Soggetto che, nell'ambito delle attività esercitate, è abilitato in base alla legge di riferimento ad attestare l'identità di persone fisiche.

Registration Authority Officer – Ufficio di Registrazione [RAO]

Soggetto incaricato a verificare l'identità di un Utente Titolare, nonché ad attivare la procedura di certificazione per conto del Certificatore.

Richiedente [Subscriber]

Persona fisica o giuridica che richiede una o più identità SPID da attribuire ai Titolari, sostenendone i costi. Può coincidere con l'Utente Titolare e/o con l'Intestatario della Fattura.

Sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID)

È il sistema di cui all'art. 64 del CAD.

Tempo Universale Coordinato [Coordinated Universal Time]

Scala dei tempi con precisione del secondo come definito in ITU-R Recommendation TF.460-5

Utente Titolare

Persona fisica o giuridica cui è attribuita una identità digitale SPID. Corrisponde all'utente del DPCM. È il soggetto che deve essere identificato dall'IdP, può coincidere con il Richiedente e/o con l'Intestatario della Fattura.

WebCam

Videocamera di ridotte dimensioni, destinata a trasmettere immagini in streaming via Internet e catturare immagini fotografiche. Collegata ad un pc o integrata in altri device, è utilizzata per chat video o per videoconferenze.

2.9 ACRONIMI E ABBREVIAZIONI

AgID – Agenzia per l'Italia Digitale (già CNIPA, già DigitPA).

CIE – Carta di Identità Elettronica

CNS – Carta Nazionale dei Servizi

HSM – Hardware Secure Module

È un dispositivo sicuro per la creazione della firma, con funzionalità analoghe a quelle delle smart card, ma con superiori caratteristiche di memoria e di performance.

IETF - Internet Engineering Task Force

IETF è una comunità aperta ed internazionale di progettisti di rete, operatori, venditori e ricercatori coinvolti nell'evoluzione dell'architettura Internet e delle normali operazioni su Internet.

ID – Identità Digitale

IdP – Identity Provider

Gestore dell'Identità Digitale SPID

ISO - International Organization for Standardization

Fondata nel 1946, l'ISO è un'organizzazione internazionale costituita da organismi nazionali per la standardizzazione.

ITU - International Telecommunication Union

Organismo intergovernativo mediante il quale le organizzazioni pubbliche e private sviluppano le telecomunicazioni. L'ITU fu fondato nel 1865 e diventò l'ente regolatore per gli standard nelle telecomunicazioni.

OTP – One-Time Password

Una One-Time Password (password usata una sola volta) è una password che è valida solo per una singola transazione. L'OTP viene generata e resa disponibile al Titolare in un momento immediatamente antecedente all'utilizzo delle credenziali di livello 2. Può essere basata su dispositivi hardware o su procedure software.

PIN – Personal Identification Number

Codice associato ad un dispositivo sicuro di firma, utilizzato dal Titolare per accedere alle funzioni del dispositivo stesso.

SPID – Sistema Pubblico di Identità Digitale

SP – Service Provider

3 OBBLIGHI E RESPONSABILITÀ

In questo capitolo si descrivono le condizioni generali con cui sono erogati i servizi di rilascio delle identità digitali descritti in questo manuale.

3.1 OBBLIGHI E RESPONSABILITÀ DEL GESTORE DI IDENTITÀ DIGITALI

In qualità di Gestore di Identità Digitali (**IdP**), InfoCert è tenuta a (cfr. articoli 1 lettera l, 7, 8 e 11 del **DPCM**):

1. 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
2. Rilasciare l'identità digitale su domanda dell'Utente Titolare e acquisire e conservare la relativa richiesta;
3. Verificare l'identità dell'Utente Titolare prima del rilascio dell'identità digitale;
4. Conservare per un periodo pari a venti anni decorrenti dalla scadenza o revoca dell'identità digitale i seguenti dati e documenti
    a. Copia per immagine del documento di identità esibito dall'Utente Titolare;
    b. Il modulo di adesione (nel caso di identificazione in presenza presso un incaricato dell'IdP);
    c. Il log di transazione (nel caso di identificazione da remoto tramite l'utilizzo di una carta CIE, CNS o TS-CNS in possesso del Titolare)
    d. Il log di transazione (nel caso di identificazione tramite l'utilizzo di una identità digitale SPID rilasciata dall'IdP InfoCert già in possesso del Titolare)
    e. Il modulo di adesione sottoscritto con firma elettronica qualificata o digitale
5. Cancellare la documentazione di cui al punto precedente trascorsi venti anni dalla scadenza o revoca dell'identità digitale
6. Trattare i dati personali nel rispetto del Codice in materia di protezione dei dati personali [3]
7. Attenersi alle misure di sicurezza previste dal Regolamento in materia di protezione dei dati personali [3], nonché alle indicazioni fornite nell'informativa pubblicata sul sito https://www.identitadigitale.infocert.it
8. Informare tempestivamente AgID e il Garante per la Protezione dei Dati Personali su eventuali violazioni di dati personali
9. Consegnare in modalità sicura le credenziali di accesso all'utente
10. Verificare gli attributi identificativi del Titolare
11. Verificare e aggiornare tempestivamente le informazioni per le quali il Titolare ha comunicato una variazione, nonché notificarne la richiesta di aggiornamento e l'aggiornamento effettuato
12. Verificare la provenienza della richiesta di sospensione da parte del Titolare, quando non inviata via PEC o sottoscritta con firma elettronica qualificata o digitale
13. Fornire al Titolare la conferma della ricezione della richiesta di sospensione o di revoca

dell'identità

14. Effettuare tempestivamente e a titolo gratuito su richiesta del Titolare la sospensione (per massimo 30 giorni) o la revoca di una identità digitale, ovvero la modifica degli attributi secondari e delle credenziali di accesso
15. Revocare l'identità digitale quando se ne riscontra l'inattività per un periodo superiore a 24 mesi, per scadenza del contratto o in caso si venga a conoscenza del decesso della persona fisica o dell'estinzione della persona giuridica, ovvero per acquisizione della conoscenza di cause limitative della capacità dell'utente, per perdita del possesso o compromissione della segretezza, per sospetti di abusi o falsificazioni, su provvedimento dell'AgID
16. Ripristinare o revocare l'identità digitale sospesa se non riceve entro 30 giorni dalla sospensione una richiesta di revoca da parte del Titolare
17. Ripristinare l'identità digitale sospesa se non riceve entro 30 giorni dalla sospensione copia della denuncia presentata all'autorità giudiziaria per gli stessi fatti sui quali è basata la richiesta di sospensione
18. Revocare l'identità digitale sospesa se riceve dal Titolare copia della denuncia presentata all'autorità giudiziaria
19. Segnalare su richiesta del Titolare ogni avvenuto utilizzo delle sue credenziali di accesso, inviandone gli estremi a uno degli attributi secondari indicati dal Titolare
20. All'approssimarsi della scadenza dell'identità digitale, comunicarla al Titolare e, dietro sua richiesta, provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella scaduta
21. Utilizzare sistemi affidabili che garantiscono la sicurezza tecnica e crittografica dei procedimenti, in conformità a criteri di sicurezza riconosciuti a livello internazionale
22. Adottare adeguate misure contro la contraffazione, idonee anche a garantire la riservatezza, l'integrità e la sicurezza nella generazione delle credenziali di accesso
23. Proteggere le credenziali dell'identità digitale contro abusi e usi non autorizzati adottando le misure richieste dalla normativa
24. Effettuare un monitoraggio continuo al fine di rilevare usi impropri o tentativi di violazione delle credenziali di accesso dell'identità digitale di ciascun utente, procedendo alla sospensione dell'identità in caso di attività sospetta
25. In caso di guasto o di upgrade tecnologico provvedere tempestivamente alla creazione di una nuova credenziale sostitutiva e alla revoca di quella sostituita
26. Effettuare con cadenza almeno annuale un'analisi dei rischi
27. Definire, aggiornare e trasmettere a AgID il piano per la sicurezza dei servizi SPID
28. Allineare le procedure di sicurezza agli standard internazionali, la cui conformità è certificata da un terzo abilitato
29. Condurre con cadenza almeno semestrale il *penetration test*
30. Garantire la continuità operativa dei servizi afferenti allo SPID
31. Effettuare ininterrottamente l'attività di monitoraggio della sicurezza dei sistemi, garantendo la gestione degli incidenti da parte di una apposita struttura interna

32. 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
33. Non mantenere alcuna sessione di autenticazione con l'utente in caso di utilizzo di credenziali SPID di livello 2 o 3
34. Garantire la disponibilità delle funzioni, l'applicazione dei modelli architetturali e il rispetto delle disposizioni previste dalla normativa, assicurando l'adeguamento in seguito all'aggiornamento della normativa
35. Sottoporsi con cadenza almeno biennale a una verifica di conformità alle disposizioni vigenti
36. Tenere il Registro delle Transazioni contenente i tracciati delle richieste di autenticazione servite nei 24 mesi precedenti, curandone riservatezza, integrità e inalterabilità, adottando idonee misure di sicurezza e utilizzando meccanismi di cifratura
37. Inviare all'AgID in forma aggregata i dati richiesti a fini statistici
38. In caso di cessazione dell'attività comunicarlo a AgID e ai Titolari almeno 30 giorni prima, indicando gli eventuali gestori sostitutivi ovvero segnalando la necessità di revocare le identità digitali rilasciate. Revocare le identità rilasciate per le quali non si abbia avuto subentro
39. In caso di subentro a un gestore cessato, gestire le identità digitali prese in carico e conservarne le relative informazioni
40. Informare espressamente il Titolare in modo compiuto e chiaro sugli obblighi che assume in merito alla protezione della segretezza delle credenziali, sulla procedura di autenticazione e sui necessari requisiti tecnici per accedervi

3.2 OBBLIGHI E RESPONSABILITÀ DEL DISTRIBUTORE O RIVENDITORE CHE FUNGE DA UFFICIO DI REGISTRAZIONE

Il Gestore di Identità Digitali, previa sottoscrizione di apposite Convenzioni che rispettano il dettato normativo nazionale ed internazionale[1], delega a Distributori o Rivenditori le attività di raccolta dei dati relativi ai Richiedenti le credenziali SPID, la loro identificazione, nonché il successivo eventuale rilascio delle medesime credenziali.

Il Distributore o rivenditore che funge da Ufficio di Registrazione pertanto si obbliga a:

1. Garantire che l'Utente Titolare sia espressamente informato riguardo agli obblighi da quest'ultimo assunti in merito alla protezione della segretezza delle credenziali SPID;
2. Garantire che l'Utente Titolare sia espressamente informato in modo compiuto e chiaro sulla procedura di identificazione e rilascio dell'identità digitale e sui requisiti tecnici necessari;
3. Adempiere a tutte le obbligazioni derivanti dalla normativa vigente per la protezione dei dati personali;
4. Verificare l'identità dell'Utente Titolare, controllare e registrare i dati dello stesso, secondo le procedure di identificazione e registrazione previste nel presente Manuale Operativo;

[1] In tema di servizi fiduciari (rif. art. 24, comma 2, Regolamento UE n. 910/2014) Le informazioni di cui al primo comma sono verificate dal prestatore di servizi fiduciari qualificato direttamente o ricorrendo a un terzo conformemente al diritto nazionale.
In tema di servizi fiduciari (rif. art. 2.4.1 Allegato al Regolamento di Esecuzione UE 2015/1502) I fornitori sono responsabili del rispetto di qualsiasi impegno affidato a un'entità esterna e della relativa conformità alla politica del regime, come se fossero essi stessi a svolgere le funzioni.

5. Inviare tempestivamente al Gestore delle Identità Digitali gli originali delle richieste di credenziali SPID;
6. Qualora vengano da esso nominati degli Incaricati al Riconoscimento, a comunicare tempestivamente all'IdP la nomina nonché l'eventuale revoca della nomina stessa, ad erogare una adeguata formazione all'Incaricato al Riconoscimento e a fornire all'IR medesimo, gli strumenti adeguati ai fini del riconoscimento e della registrazione;
7. Tenere direttamente i rapporti con il Richiedente e con gli Utenti Titolari e ad informarli circa le disposizioni contenute nel presente Manuale Operativo.

3.3 OBBLIGHI DEGLI UTENTI TITOLARI

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

1. Esibire a richiesta dell'IdP i documenti richiesti e necessari ai fini delle operazioni di emissione e gestione dell'identità digitale e le credenziali
2. Fornire al soggetto che effettua l'identificazione, per la richiesta delle credenziali di accesso solamente dati, informazioni e documenti corretti, veritieri e completi, assumendosi le responsabilità previste dalla legislazione vigente in caso di dichiarazioni infedeli o mendaci
3. Accertarsi della correttezza dei dati registrati dal Gestore al momento dell'adesione e segnalare tempestivamente eventuali inesattezze
4. Informare tempestivamente l'IdP di ogni variazione degli attributi previamente comunicati
5. Mantenere aggiornati, in maniera proattiva e/o a seguito di segnalazione da parte dell'IdP, i contenuti dei seguenti attributi identificativi:
    a. Se persona fisica: estremi e immagine del documento di riconoscimento e relativa scadenza, numero di telefono fisso o mobile, indirizzo di posta elettronica, domicilio fisico e digitale
    b. Se persona giuridica: indirizzo sede legale, codice fiscale o Partita IVA, rappresentante legale della società, numero di telefono fisso o mobile, indirizzo di posta elettronica, domicilio fisico e digitale
6. Utilizzare in via esclusiva e personale le credenziali connesse all'Identità Digitale, compresi gli eventuali dispositivi su cui sono custodite le chiavi private
7. Non utilizzare le credenziali in maniera tale da creare danni o turbative alla rete o a terzi utenti e a non violare leggi e regolamenti
8. Utilizzare le credenziali di accesso per gli scopi specifici per cui esse sono rilasciate e, in particolare, per scopi di autenticazione informatica nello SPID, assumendo ogni eventuale responsabilità in caso di diverso utilizzo delle stesse
9. Adottare ogni misura tecnica o organizzativa idonea a evitare danni a terzi
10. Proteggere e conservare con la massima accuratezza, al fine di garantirne l'integrità e la riservatezza, la componente riservata delle credenziali di accesso, gli eventuali dispositivi sui cui sono trasmesse le OTP e le OTP medesime nonché, se presenti, dei dispositivi crittografici contenenti le chiavi private associate a credenziali di livello 3

11. Non violare diritti d'autore, marchi, brevetti o altri diritti derivanti dalla legge e dalle consuetudini
12. sporgere immediatamente denuncia alle Autorità competenti in caso di smarrimento o sottrazione delle credenziali attribuite e chiedere immediatamente all'IdP la sospensione delle credenziali
13. Accertarsi dell'autenticità del fornitore di servizi o dell'IdP quando viene richiesto di utilizzare l'identità digitale
14. Attenersi alle indicazioni fornite dall'IdP in merito all'uso del sistema di autenticazione, alla richiesta di sospensione o revoca dell'identità, alle cautele da adottare per la conservazione e protezione delle credenziali
15. In caso di utilizzo per scopi non autorizzati, abusivi o fraudolenti da parte di un terzo soggetto chiedere immediatamente al Gestore la sospensione delle credenziali

3.4 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:

1. Conoscere l'ambito di utilizzo delle identità digitali, le limitazioni di responsabilità e i limiti di indennizzo del IdP, riportati nel presente Manuale Operativo;
2. Osservare quanto previsto dall'art. 13 del DPCM e dagli eventuali Regolamenti di cui all'art. 4 del DPCM medesimo;
3. Adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

3.5 OBBLIGHI DEL RICHIEDENTE

Il **Richiedente** che, avendo presa visione del presente Manuale Operativo, richiede il rilascio delle identità digitali è tenuto ad attenersi a quanto disposto dal presente Manuale Operativo.

3.6 TUTELA DEI DATI PERSONALI

Le informazioni relative all'Utente Titolare ed al Richiedente di cui l'IdP viene in possesso nell'esercizio delle sue tipiche attività, sono da considerarsi, salvo espresso consenso, riservate e non pubblicabili, con l'eccezione di quelle esplicitamente destinate ad uso pubblico in base alla normativa.
Inparticolare i dati personali vengono trattati dall'IdP in conformità a quanto indicato nel Regolamento Europeo 2016/679 (GDPR).

3.7 CLAUSOLA RISOLUTIVA ESPRESSA AI SENSI DELL'ART. 1456 CC

L'inadempimento da parte del Titolare o del Richiedente dei rispettivi obblighi descritti nei precedenti paragrafi 3.3 e 3.5 costituisce inadempimento essenziale ai sensi dell'art. 1456 c.c. e dà facoltà al IdP di risolvere il contratto eventualmente intercorso con tali soggetti. La risoluzione

opererà di diritto al semplice ricevimento di una comunicazione, inviata dall'IdP tramite raccomandata A.R. o posta elettronica certificata, contenente la contestazione dell'inadempienza e l'intendimento di avvalersi della risoluzione stessa.

4 DESCRIZIONE DELLE ARCHITETTURE APPLICATIVE

Nel presente capitolo sono descritte le architetture, applicative e di dispiegamento, adottate per i sistemi run-time che realizzano i protocolli previsti dalle regole tecniche. Inoltre, si descrivono anche le architetture dei sistemi di autenticazione delle credenziali che compongono il sistema di gestione delle identità digitali InfoCert.

Nell'immagine sotto riportata è possibile individuare i principali Attori e componenti dell'architettura SPID realizzata:

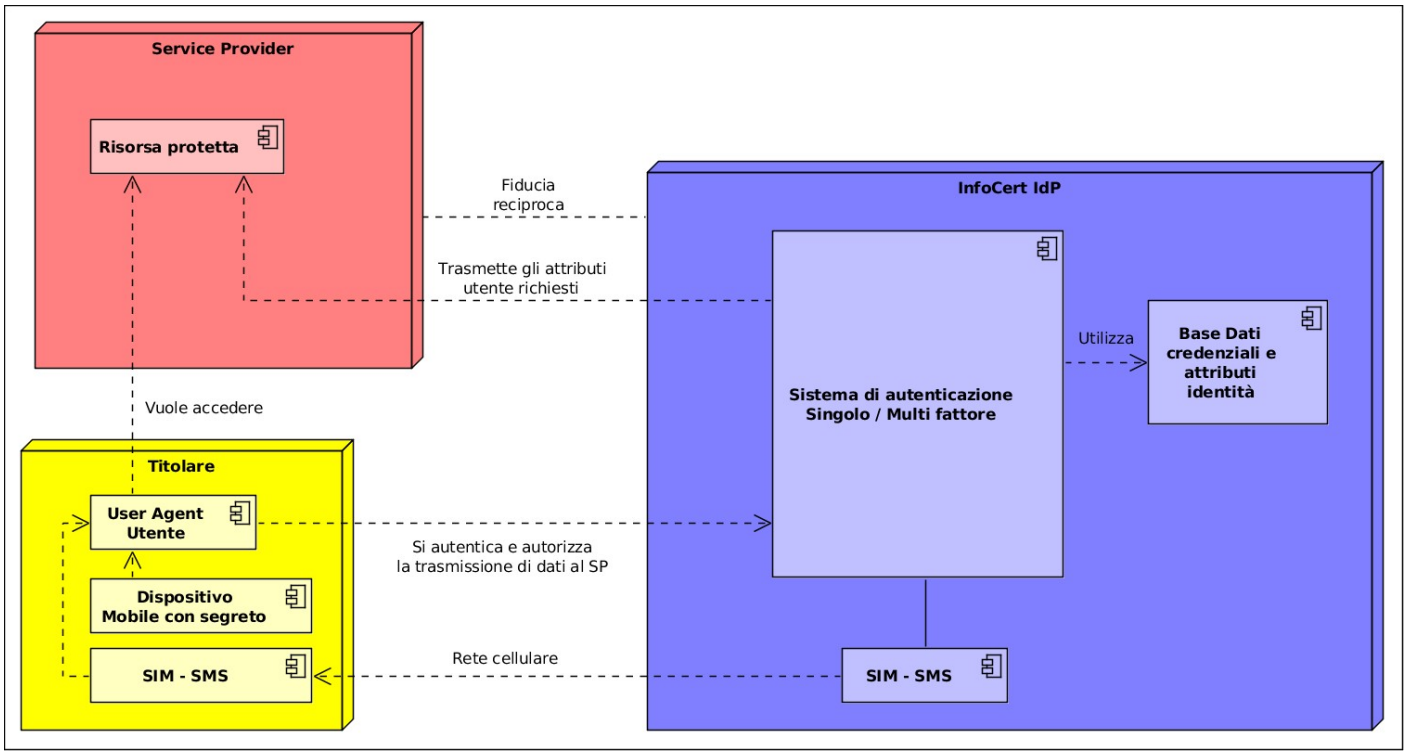

FIGURA 1 - ARCHITETTURA DI MASSIMA INFOCERTID

4.1 USER AGENT / UTENTE

Rappresenta il Titolare che intende accedere alle risorse disponibili presso il Service Provider; per ottenere l'accesso a tali risorse deve provare di possedere l'identità SPID tramite una verifica delle credenziali al Identity Provider.

4.2 SERVICE PROVIDER

Provider di servizi dei quali il titolare intende fruire. Ogni servizio può necessitare di livelli di autenticazione e insieme di attributi qualificativi differenti; all'atto della richiesta di autenticazione

specifica questi requisiti firmandola digitalmente.

4.3 INFOCERT IDP

L'identity provider è l'insieme degli applicativi e servizi atti a:

- Ricevere e verificare la validità delle richieste di autenticazione secondo un sistema di trust tra IdP e SP basato su firma digitale come previsto dal DPCM;
- Presentare al titolare una richiesta di credenziali come prova di possesso di una identità secondo le modalità descritte nel DPCM in maniera semplice, chiara ed altamente sicura sulla base della richiesta precedentemente validata;
- Raccogliere dalla base di dati interna le informazioni richieste dal SP per espletare il servizio richiesto al titolare;
- Inviare in maniera sicura, confidenziale e non ripudiabile l'asserzione di identità costruita sulla base della metodologia di autenticazione utilizzata e degli attributi qualificati che il titolare ha autorizzato a concedere al SP.

L'identity server di InfoCert si basa su tecnologia WSO2, ed è rappresentato come di seguito:

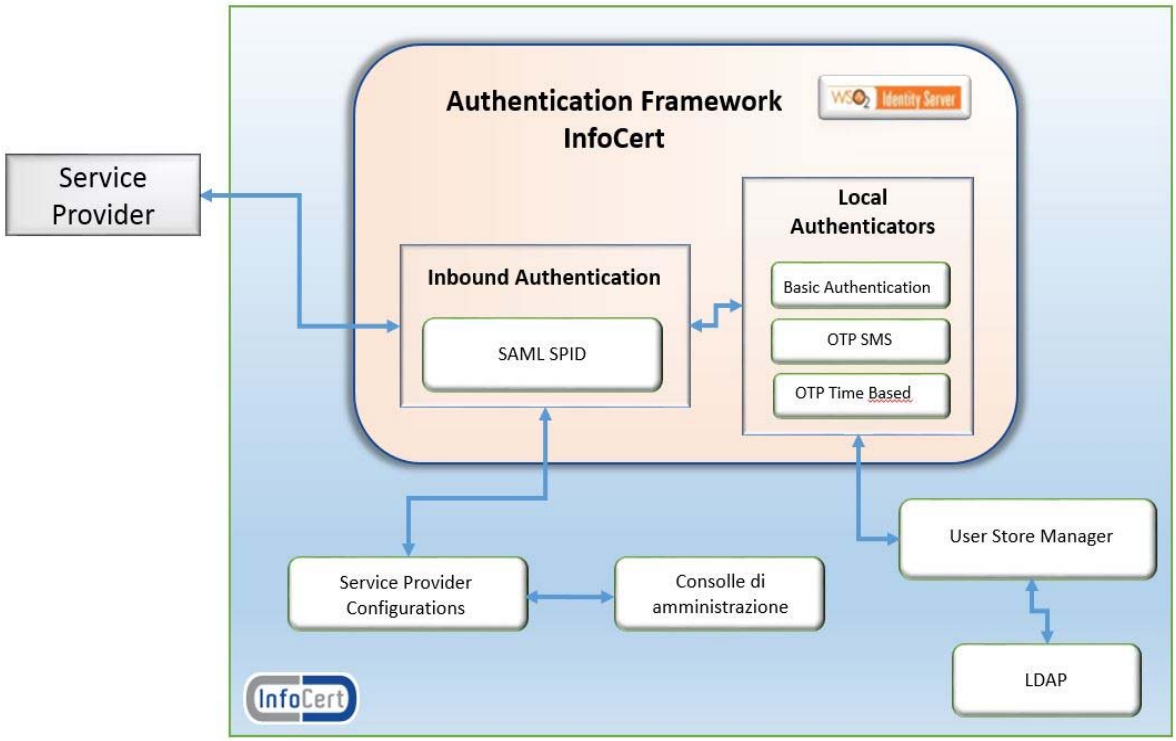

FIGURA 2 - ARCHITETTURA WSO2

L'Identity Server WSO2 fornisce una gestione sicura delle identità per applicazioni web aziendali e i servizi per la gestione delle identità. Il Server WSO2 permette la gestione delle identità, compreso il

controllo di accesso basato sui ruoli (RBAC), il controllo capillare basato su policy di accesso, e il Single-Sign-On (SSO) bridging.
Rispetto all'architettura standard WSO2, le principali componenti di personalizzazione del sistema sono indicate nel sottoparagrafi seguenti.

4.3.1 LOCAL AUTHENTICATORS

Sono stati sviluppati due autenticatori basati su tecnologia Java JSP che realizzano le specifiche di autenticazione SPID Livello 1 e 2.
InfoCert, rende disponibile al Titolare tre metodi di autenticazione denominati:

- Basic Authentication (Livello SPID 1, LoA 2)
- One Time Password via SMS (Livello SPID 2, LoA 3)
- Time Based One Time Password (Livello SPID 2, LoA 3)

Per i dettagli relativi ai sistemi di autenticazione, si veda il paragrafo 4.7.

4.3.2 SERVICE PROVIDER CONFIGURATIONS

Modulo che tramite interfaccia JDBC gestisce la persistenza dei dati relativi ai Service Provider. Il modulo non è stato personalizzato rispetto all'implementazione standard.

4.3.3 USER STORE MANAGER

Modulo che tramite interfaccia LDAP gestisce la lettura delle informazioni degli utenti (credenziali di primo livello e attributi). Viene utilizzato anche per l'accesso all'interfaccia di amministrazione del prodotto.

4.3.4 INBOUND AUTHENTICATION

Modulo che *astrae* il protocollo utilizzato per veicolare le richieste dei Service Provider (SAML, OID Connect) agli autenticatori, è incaricato anche di costruire le *Response SAML* ed è in questa parte del flusso che è stato personalizzato come da specifiche SPID. Il modulo utilizza la libreria Open SAML per la de/serializzazione del SAML.

4.3.5 CONSOLE DI AMMINISTRAZIONE

Il sistema dispone di una console di amministrazione, raggiungibile solo da rete interna, l'accesso alla quale è regolato tramite username e password di amministratore.
Tramite detta console è possibile modificare le informazioni dei Service Provider (*AssertionConsumerServiceURL*, certificato di chiave pubblica, autenticatori associati) ma non è possibile modificare le informazioni delle identità in quanto la connessione LDAP è di sola lettura.

4.3.6 DIRECTORY SERVER

Come implementazione della directory server è stato utilizzato il protocollo LDAP Oracle.
Le password nelle Entry LDAP non sono conservate in chiaro ma come risultato della funzione di hash *Salted SHA-512*.
L'accesso in lettura/scrittura alla base di dati è possibile solo da rete interna e regolato tramite username e password di amministratore.

4.4 PROCESSI DI PROVISIONING - FRONT-END

I processi di provisioning implementati per la parte di front end, cioè le maschere che l'utente vede, gestiscono sia la fase di registrazione, sia il "SelfCare", cioè l'interfaccia che l'utente utilizza per la gestione della propria identità.

Il componente di front end è composto di soli elementi statici ed è basato sul framework AngularJS con Bootstrap e si appoggia alla componente per l'autenticazione dell'utente; mentre le funzionalità sono ottenute tramite servizi REST messi a disposizione dalla componente di back-end.

4.5 PROCESSI DI PROVISIONING - BACK-END

I processi di provisioning implementati, sono la parte di back-end del provisioning dei prodotti InfoCert; nel contesto SPID la componente gestisce i cambiamenti "automatici" degli stati di vita delle utenze e fornisce servizi REST sia per gestire la fase di registrazione delle richieste di nuove utenze, sia per gestirne il ciclo di vita da parte dell'utente finale.

Tale componente fornisce anche una interfaccia, accessibile da sola rete interna dagli operatori di BackOffice, per gestire le identità. Il sistema può inoltre richiamare altri componenti tramite chiamate REST o SOAP.

Questa componente comprende:

- un pacchetto Java Enterprise contenente il codice applicativo (JAVA).
- una parte di connessione a una base di dati RDMS.
- una parte per l'interfaccia applicativa basata su tecnologia REST.
- un sistema di gestione dei messaggi basato tecnologia JMS.
- Application Server basato su Redhat JBoss.

4.6 LIVELLI DI SICUREZZA

I livelli di sicurezza dei sistemi di autenticazione sono conformi a quanto previsto dal DPCM e dai Regolamenti attuativi qui di seguito riportati:

- **Primo Livello**: sono rilasciati sistemi di autenticazione ad un fattore, basati su password.

Tale livello corrisponde al Level of Assurance LoA2 dello standard ISO/IEC 29115. A questo livello sono rilasciate all'Utente una userID (indirizzo email) ed una password.

- **Secondo Livello**: sono rilasciati sistemi di autenticazione a due fattori non basati necessariamente su certificati digitali, le cui chiavi private sono custodite su dispositivi che soddisfano i requisiti di cui all'Allegato II del Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio. Tale livello corrisponde al Level of Assurance LoA3 dello standard ISO/IEC 29115. A questo livello sono rilasciate all'Utente una userID, una password e dei sistemi OTP (One-Time Password) gestiti tramite protocollo SMS e/o applicazioni che assicurano il soddisfacimento dei requisiti previsti dalla normativa. Possono essere utilizzati anche sistemi biometrici di accesso, nel rispetto delle previsioni del Garante per la Protezione dei Dati Personali.
- **Terzo Livello**: (**non ancora gestito dall'IdP)**, sono rilasciati sistemi di autenticazione a due fattori basati su certificati digitali, le cui chiavi private sono custodite su dispositivi che soddisfano i requisiti di cui all'Allegato II del Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio. Tale livello corrisponde al Level of Assurance LoA4 dello standard ISO/IEC 29115.

4.7 SISTEMI DI AUTENTICAZIONE

InfoCert, rende disponibile al Titolare tre metodi di autenticazione, descritti di seguito, denominati:

1. Basic Authentication (Livello SPID 1, LoA 2)
2. One Time Password via SMS (Livello SPID 2, LoA 3)
3. Time Based One Time Password (Livello SPID 2, LoA 3)

Nei prossimi paragrafi sono descritte le caratteristiche dei sistemi di autenticazione sopra citati.

4.7.1 BASIC AUTHENTICATION

Il metodo prevede credenziali a singolo fattore di tipo username e password, le quali sono scelte dal Titolare in fase di creazione delle stesse. Le credenziali non sono mai memorizzate in chiaro dal IdP se non in forma irreversibile (tramite funzione crittografica di hash) al solo scopo di verificarne la validità in fase di autenticazione.
Tutte le password devono essere cambiate almeno ogni 6 mesi a cura dei titolari delle credenziali e sono vincolate a policy di robustezza.
Sono attivi meccanismi proattivi per la gestione della scadenza del periodo di validità (expiration): messaggi inviati via email avvisano l'utente prima della scadenza del periodo di validità della password o prima che venga definitivamente disabilitata.
Quando l'utente sceglie la prima password o modifica la password iniziale una procedura automatica garantisce l'applicazione delle policy.
Tutto il protocollo per l'autenticazione con l'IdP avviene secondo le specifiche del protocollo SAML 2.0 come descritto nell'RFC 6595 dell'Internet Engineering Task Force (IETF) dell'aprile 2012 e

secondo le specifiche di interfaccia SPID definite da AGID.
L'autenticazione viene gestita dal componente BasicAuthenticator ed avviene in due fasi a seguito della validazione dei dati di input:

1. Search su Directory Server (LDAP) della entry identificata dal username fornito;
2. Bind su Directory Server (LDAP) del Common Name risolto al punto 1. e della password fornita dall'utente, il Directory Server confronta l'hash della password con quello memorizzato nella entry e restituisce lo stato del bind.

Se la fase 2 va a buon fine (e la password non risulta scaduta o bloccata) l'autenticazione può considerarsi conclusa con successo. In seguito viene installato nel browser dell'utente un cookie con un identificativo (sicuro) che sarà utilizzato per identificare la sessione di SSO attivata.

4.7.2 ONE-TIME PASSWORD VIA SMS

Il metodo prevede, in seguito alla corretta verifica delle credenziali di primo livello, l'invio di una OTP sul numero di telefono verificato in possesso del Titolare: il meccanismo si identifica come secondo fattore di identificazione in quanto prova il possesso della SIM mobile. La One-Time Password generata è casuale, unica e con validità limitata nel tempo.
L'OTP sarà generato e ne sarà gestita la persistenza su database tramite il componente predisposto che avrà una durata limitata nel tempo e sarà associato alla specifica richiesta tramite una chiave alfanumerica, generata casualmente, posta davanti all'OTP che verrà visualizzata al momento della richiesta dell'OTP da parte dell'IdP.
Nel caso in cui l'OTP ricevuto si rivelasse corretto entro il limite di 3 tentativi (ognuno di questi invalidante il precedente OTP per mitigare il riuso) l'autenticazione può considerarsi conclusa con successo. In seguito viene installato nel browser dell'utente un cookie con un identificativo che sarà utilizzato per identificare la sessione di SSO attivata. Per l'invio dei messaggi si utilizza un pool di dispositivi appositi, che si occupano del colloquio con la rete GSM.

4.7.3 TIME BASED ONE-TIME PASSWORD

InfoCert ha sviluppato un sistema di generazione di OTP per dispositivi mobili basati su iOS e Android che rispettano le specifiche descritte nella RFC 6238 dell'Internet Engineering Task Force (IETF) del maggio 2011. Il metodo prevede che il Titolare installi una app gratuita sul proprio smartphone, a partire dai principali app-store.
Tale metodo è basato su un'estensione dell'algoritmo per la generazione di One Time Password basato su funzione HMAC (definito nella RFC 4226) per aggiungere al calcolo un fattore legato al tempo corrente.
In sintesi il sistema a partire da un algoritmo noto che calcola la funzione HMAC (funzione di hash con chiave, definita dall'IETF nell'RFC 2104) ed un seme (definito seed nel seguito) condiviso tra l'App dell'utente ed il modulo autenticatore dell'IdP, calcola l'hash dell'ora corrente espressa in secondi, opportunamente arrotondato per avere una finestra di ampiezza predefinita, utilizzando il seme come chiave (quantità di sicurezza).

In seguito alla corretta verifica delle credenziali di primo livello e all'autenticazione con le stesse nella app, viene simultaneamente generata una OTP sia dall'App mobile che dall'autenticatore. Questo meccanismo si identifica come secondo fattore di identificazione in quanto prova la conoscenza del segreto comune utilizzato per la generazione degli OTP. Il segreto è scambiato in fase di consegna della credenziale e non è ottenibile nemmeno intercettando la serie di OTP generati.
La sincronizzazione tra la device mobile ed il server dell'IdP sarà garantita attraverso l'utilizzo di server NTP o semplicemente abilitando sensori GPS sempre più disponibili sulle device mobili.
Il seme, generato al momento dell'emissione utilizzando l'output di una funzione crittografica di hash, sarà memorizzato sulla device mobile cifrato, utilizzando un PIN scelto dall'utente. Il PIN dovrà essere inserito dall'utente ad ogni utilizzo o sarà legato allo screensaver del dispositivo.
La sincronizzazione tra la device mobile ed il server dell'IdP sarà garantita attraverso l'utilizzo di server NTP o semplicemente abilitando sensori GPS sempre più disponibili sulle device mobili.

4.7.4 CARATTERISTICHE DELLE COMPONENTI DI AUTENTICAZIONE

Le principali caratteristiche, dei componenti di autenticazione implementati sono descritte nei paragrafi seguenti.

4.7.4.1 GENERATORE NUMERICO OTP

Il generatore numerico OTP è la componente per la generazione e la gestione dei seed che sono alla base della generazione di OTP per le App mobile. Inoltre., tale componente, si occupa di verificare la validità di un OTP.

Questo modulo comprende:

- un pacchetto Java Enterprise contenente il codice applicativo (JAVA)
- una parte di connessione a una base di dati RDMS
- una parte per l'interfaccia applicativa basata su tecnologia REST
- Application Server basato su Redhat JBoss

4.7.4.2 SISTEMA DI INVIO SMS

Il sistema di invio SMS è la componente utilizzata per l'invio di messaggi SMS ad un determinato numero di telefono cellulare. Per l'invio materiale dei messaggi si appoggia ad un pool di dispositivi dedicati, che si occupano del colloquio con la rete GSM.
Questo modulo comprende:

- un pacchetto Java Enterprise contenente il codice applicativo (JAVA)
- una parte di connessione a una base di dati RDMS
- una parte per l'interfaccia applicativa basata su tecnologia REST
- un sistema di gestione dei messaggi basato tecnologia JMS
- Application Server basato su Redhat JBoss

4.7.4.3 GENERAZIONE TOKEN E VERIFICA

La componente genera i token temporanei e si occupa della loro gestione. In particolare, in ambito SPID, è utilizzato per la generazione e la verifica di:

- OTP via SMS;
- URL temporanei (come ad esempio dell'URL inviata all'utente per la verifica dell'email).

Questo modulo comprende:

- un pacchetto Java Enterprise contenente il codice applicativo (JAVA).
- una parte di connessione a una base di dati RDMS.
- una parte per l'interfaccia applicativa basata su tecnologia REST.
- Application Server basato su Redhat JBoss.

5 DESCRIZIONE DI CODICI E FORMATI DEI MESSAGGI DI ANOMALIA

Il sistema di gestione identità digitale segnala eventuali anomalie riscontrate sia ai protocolli che ai dispositivi di autenticazione utilizzati.
L'IdP ha recepito la tabella degli errori indicata dall'Agenzia, che è disponibile in Appendice A.

6 TRACCIATURE DEGLI ACCESSI AL SERVIZIO

Gli accessi al servizio sono registrati sotto forma di log certificato. Il log certificato è composto da un file di testo prodotto dall'applicativo che gestisce il processo di autenticazione e dialogo con i Service Provider, il quale viene firmato e marcato temporalmente prima della conservazione nel sistema di conservazione InfoCert descritto in [9]. È garantita l'integrità nonché la disponibilità secondo quanto previsto dal **DPCM**.
Contiene, tra l'altro, le seguenti informazioni corrispondenti a quanto richiesto nonché consigliato nelle regole tecniche:

- lo SPID code (come chiave del tracciato)
- la richiesta del SP
- la risposta del IdP
- ID della richiesta
- timestamp della richiesta
- SP richiedente autenticazione (issuer richiesta)
- ID della risposta
- timestamp della risposta
- IdP autenticante (issuer risposta)
- ID dell'asserzione di risposta
- soggetto dell'asserzione di risposta (subject)

6.1 PROCEDURA PER LA RICHIESTA DEL LOG CERTIFICATO

Il Titolare dell'identità si collega con le proprie credenziali al portale di gestione dell'identità, da cui inoltra una richiesta di informazioni contenute nel log certificato indicando l'intervallo di date dell'utilizzo delle credenziali SPID di cui intende ricevere informazioni. La richiesta è validata con l'inserimento delle credenziali SPID di livello 2 ovvero con l'inserimento di una OTP ricevuta via SMS sul numero di telefono cellulare verificato.

InfoCert provvede alla produzione della/delle attestazione/i richiesta/e dal Titolare e la/e mette a disposizione per il download sul portale di gestione dell'identità.
Previo accordo con il Titolare, la/le attestazione/i possono in alternativa essere inviate alla casella e-mail verificata nel sistema SPID, sulla quale è inviato un link al sistema di file sync & sharing certificato InfoCert, da cui il Titolare può scaricare le attestazioni entro un termine di 30 giorni dalla ricezione del messaggio.
Le attestazioni rilasciate potranno essere utilizzate dal Titolare per gli usi consentiti dalla legge.

6.2 REGISTRAZIONE DEGLI EVENTI RELATIVI ALLA RICHIESTA DELL'IDENTITÀ

Tutte gli eventi relativi alla richiesta dell'identità SPID, funzionali alla tipologia di registrazione e contrattualizzazione utilizzata, sono registrati in appositi log:

- log accesso applicazione da parte dell'IR
- log verifica numero di cellulare
- log verifica e-mail
- log con verifiche su attributi identificativi

Sono inoltre registrate anche le evidenze documentali poste a corredo della richiesta dell'identità, che sono conservate a norma nel sistema di conservazione elettronica documentale certificato, secondo le procedure descritte in [9]:

- contratto sottoscritto con firma digitale;
- foto fronte/retro del documento di identità presentato
- foto fronte/retro della Tessera Sanitaria presentata
- in caso di riconoscimento a mezzo webcam: dichiarazione di riconoscimento firmata dall'IR
- in caso di riconoscimento a mezzo webcam: streaming audiovideo della sessione di riconoscimento

7 PROCESSI DI IDENTIFICAZIONE E RILASCIO

Questo capitolo descrive le procedure usate per:

- l'identificazione dell'Utente Titolare al momento della richiesta di rilascio della ID;
- le procedure di Rilascio delle credenziali.

7.1 IDENTIFICAZIONE AI FINI DEL RILASCIO

L'IdP deve verificare l'identità del Titolare prima di procedere al rilascio della ID.
La procedura di identificazione comporta che l'Utente Titolare sia identificato, prima del rilascio della ID, secondo una delle procedure di seguito specificate.
I processi di rilascio della ID prevedono che:

1. la fase di identificazione sia eseguita prima della contrattualizzazione del servizio;
2. il Richiedente sottoscriva il contratto di adesione al servizio con una delle modalità previste nelle procedure di rilascio.
3. il Titolare provveda autonomamente a scegliere e configurare la coppia userID (nickname/email) e password che costituiscono le credenziali di autenticazione minime.

7.2 MODALITÀ DI IDENTIFICAZIONE

L'identità del soggetto ***Titolare*** viene accertata dall'IdP secondo le seguenti modalità:

1. da remoto, grazie all'utilizzo di una firma digitale o una firma elettronica qualificata in possesso del ***Titolare***;
2. da remoto, grazie all'utilizzo di una carta CIE, CNS o TS-CNS in possesso del ***Titolare***;
3. da remoto, grazie all'utilizzo di una identità digitale SPID rilasciata dall'IdP InfoCert già in possesso del ***Titolare***;
4. da remoto o in presenza, grazie all'utilizzo di un precedente sistema di identificazione informatica dichiarato conforme ai requisiti dello SPID con apposito accoglimento dell'istanza di recupero delle identità pregresse da parte di AgID.
5. da remoto, grazie a una sessione webcam con un IR dell'IdP in modalità sincrona;
6. in presenza, presso le sedi abilitate del Distributore o Rivenditore che svolge attività di Ufficio di Registrazione, ovvero le sedi degli IR da questi nominati (InfoCert point).

7.3 PROCEDURE PER L'IDENTIFICAZIONE E IL RILASCIO DA REMOTO

Al fine di mantenere una esperienza utente coerente e il più possibile comune tra i diversi processi di identificazione, si è definito un unico processo di rilascio dell'identità, che si distingue sulla base della modalità di identificazione da remoto scelta dal ***Titolare***.
Il processo si compone dei seguenti steps:

1 Il ***Titolare*** atterra sulle pagine di richiesta identità dell'***IdP***;
2 Il ***Titolare*** sceglie UserID e password e inserisce il proprio indirizzo di posta elettronica. Qualora lo desideri, può richiedere l'apertura di un indirizzo PEC presso il Gestore PEC InfoCert, secondo

le procedure previste da [6]. La casella di PEC sarà gratuita per i 6 mesi successivi all'attivazione al termine dei quali, in caso di mancato rinnovo, verrà revocata[2]. La revoca della casella comporta la revoca d'ufficio dell'identità digitale, secondo quanto previsto al paragrafo 10.2.2.

3 Il ***Titolare*** riceve una email con un link e lo clicca per verificare l'indirizzo.

4 Il ***Titolare*** inserisce il proprio numero di telefono cellulare su cui riceve una OTP, che inserisce nella form per certificarne l'esistenza e la piena disponibilità;

5 Il ***Titolare*** inserisce i propri dati anagrafici[3], gli estremi del documento di identità prescelto per l'identificazione, di cui carica le copie per immagine[4];

6 Il ***Titolare*** accetta le condizioni contrattuali relative al servizio e sceglie la modalità di identificazione preferita;

7 L'***IdP*** procede all'identificazione del ***Titolare***:

7.1 In caso di scelta della modalità firma digitale o firma elettronica qualificata, il ***Titolare*** sottoscrive il modulo di richiesta del servizio con il proprio certificato qualificato di firma. L'IdP riceve il documento e verifica la firma digitale apposta;

7.2 In caso di scelta della modalità CIE/CNS/TS-CNS, il ***Titolare*** si autentica con la carta e inserimento del PIN. L'IdP considera identificato il Titolare, che procede all'accettazione e sottoscrizione delle condizioni generali di servizio con firma autografa o elettronica avanzata o digitale;

7.3 In caso di scelta della modalità SPID, il ***Titolare*** si autentica con le credenziali SPID precedentemente rilasciate da InfoCert, di livello uguale o superiore a 2. L'IdP considera identificato il Titolare, che procede all'accettazione e sottoscrizione delle condizioni generali di servizio con firma autografa o elettronica avanzata o digitale;

7.4 In caso di scelta della modalità di identificazione a mezzo webcam, un Incaricato dell'IdP procede a identificare il ***Titolare*** grazie a una sessione di videoconferenza registrata, durante la quale vengono riscontrati i dati e i documenti di identità. Al termine della sessione l'IdP considera identificato il ***Titolare***, che procede all'accettazione e sottoscrizione delle condizioni generali di servizio con firma autografa o elettronica avanzata o digitale;

8 L'IdP procede alle verifiche dell'identità dichiarata, secondo quanto previsto al paragrafo 8;

9 Al buon esito delle verifiche l'IdP considera identificato il ***Titolare*** e attiva pertanto la corrispondente identità digitale InfoCert ID. Contestualmente viene trasmessa una notifica email all'Utente contente il link di accesso al portale di gestione dell'identità digitale (Selfcare).

---

[2] Secondo quanto previsto dal Manuale Operativo – Servizio di Posta Elettronica Certificata InfoCert SpA (ICERT-PEC-MO) [6], dalla revoca della casella non sarà più possibile utilizzare la casella per spedire o ricevere nuovi messaggi. Per i 30 giorni successivi alla revoca l'utente potrà consultare i messaggi presenti in casella, pervenuti prima della revoca mentre oltre il 30esimo giorno successivo alla revoca non sarà più possibile accedere alla casella di PEC. Il Gestore mantiene per i 185 giorni successivi alla revoca il contenuto della casella ne riserva il nome, che non può essere assegnato a diverso titolare: in questo periodo il titolare può quindi procedere al rinnovo della casella, ripristinandone le funzionalità e il contenuto. In seguito, tutti i contenuti della casella verranno eliminati e il nome della casella viene mantenuto riservato e non più utilizzabile per nuove attivazioni. Il titolare potrà successivamente riattivare la casella, senza il ripristino del contenuto.

[3] Per le persone fisiche i dati identificativi obbligatori sono:

- cognome e nome;
- sesso, data e luogo di nascita;
- codice fiscale;
- estremi di un valido documento d'identità;

Il Titolare ha facoltà di inserire anche i dati di cittadinanza, residenza e domicilio.

[4] I documenti di riconoscimento ammessi per l'identificazione in presenza sono tutti quelli ammessi dal DPR 445/2000, articolo 35.

Nel caso di precedente sistema di identificazione informatica, l'IdP descrive nell'apposita istanza le modalità con cui è consentito l'utilizzo delle credenziali del precedente sistema al fine di richiedere l'identità SPID.

7.4 PROCEDURE DI IDENTIFICAZIONE E RILASCIO IN PRESENZA

Al fine di mantenere una esperienza utente coerente e il più possibile comune tra i diversi processi di identificazione, si è definito che anche in caso di processo di identificazione in presenza il ***Titolare*** inizi l'inserimento delle informazioni rilevanti sulla form online dell'IdP.
Il processo si compone dei seguenti steps:

1 Il ***Titolare*** atterra sulle pagine di richiesta identità dell'***IdP***;
2 Il ***Titolare*** sceglie UserID e password e inserisce il proprio indirizzo di posta elettronica. Qualora lo desideri, può richiedere l'apertura di un indirizzo PEC presso il Gestore PEC InfoCert, secondo le procedure previste da [6]. La casella di PEC sarà gratuita per i 6 mesi successivi all'attivazione al termine dei quali, in caso di mancato rinnovo, verrà revocata[5]. La revoca della casella comporta la revoca d'ufficio dell'identità digitale, secondo quanto previsto al paragrafo 10.2.2.Il ***Titolare*** riceve una email con un link e lo clicca per verificare l'indirizzo;
3 Il ***Titolare*** inserisce il proprio numero di telefono cellulare su cui riceve una OTP, che inserisce nella form per certificarne l'esistenza;
4 Il ***Titolare*** inserisce i propri dati anagrafici[6], gli estremi del documento di identità prescelto per l'identificazione, di cui carica le copie per immagine[7];
5 Il ***Titolare*** accetta le condizioni contrattuali relative al servizio e sceglie la modalità di identificazione in presenza. Il ***Titolare*** può consultare la dislocazione territoriale delle sedi con indicazione della tipologia di servizio erogato da ciascun punto di identificazione (***InfoCert point***). Alcuni ***InfoCert point*** gestiscono le richieste attraverso la pianificazione degli appuntamenti mentre per altri punti di identificazione non è richiesta la prenotazione. A seconda della modalità scelta, il Titolare riceverà nel primo caso la conferma dell'appuntamento, ovvero potrà ottenere un *codice identificativo della richiesta* che dovrà conservare ed esibire al momento dell'identificazione nel secondo caso:
   5.1 ***InfoCert point: identificazione con appuntamento*** - Il giorno fissato per l'appuntamento, il

[5] Secondo quanto previsto dal Manuale Operativo – Servizio di Posta Elettronica Certificata InfoCert SpA (ICERT-PEC-MO) [6], dalla revoca della casella non sarà più possibile utilizzare la casella per spedire o ricevere nuovi messaggi. Per i 30 giorni successivi alla revoca l'utente potrà consultare i messaggi presenti in casella, pervenuti prima della revoca mentre oltre il 30esimo giorno successivo alla revoca non sarà più possibile accedere alla casella di PEC. Il Gestore mantiene per i 185 giorni successivi alla revoca il contenuto della casella ne riserva il nome, che non può essere assegnato a diverso titolare: in questo periodo il titolare può quindi procedere al rinnovo della casella, ripristinandone le funzionalità e il contenuto. In seguito, tutti i contenuti della casella verranno eliminati e il nome della casella viene mantenuto riservato e non più utilizzabile per nuove attivazioni. Il titolare potrà successivamente riattivare la casella, senza il ripristino del contenuto.

[6] Per le persone fisiche i dati identificativi obbligatori sono:

- cognome e nome;
- sesso, data e luogo di nascita;
- codice fiscale;
- estremi di un valido documento d'identità;

Il Titolare ha facoltà di inserire anche i dati di cittadinanza, residenza e domicilio.

[7] I documenti di riconoscimento ammessi per l'identificazione da remoto sono:

- Carta di Identità italiana
- Patente di guida italiana
- Passaporto

Qualora il Titolare desideri presentare un altro documento di riconoscimento tra quelli ammessi dal DPR 445/2000, articolo 35, il processo di identificazione dovrà essere eseguito in presenza di un incaricato dell'IdP.

Titolare incontra l'Incaricato dell'IdP il quale procede all'identificazione sulla base dell'esibizione di un valido documento di identità. Una volta completata l'identificazione, il ***Titolare*** procede all'accettazione e sottoscrizione delle condizioni generali di servizio con firma autografa o elettronica avanzata o digitale;

5.2 ***InfoCert point: identificazione senza appuntamento*** - il ***Titolare*** può recarsi presso uno degli *InfoCert point* in orario di apertura per effettuare l'identificazione. Esibisce la Tessera Sanitaria e il *codice identificativo della richiesta,* se in suo possesso. Il CF viene verificato da parte dell'Incaricato dell'IdP e riconciliato con i documenti precaricati in fase di registrazione. L'Incaricato dell'IdP procede all'identificazione del ***Titolare*** sulla base dell'esibizione di un valido documento di identità. L'incaricato dell'IdP firma digitalmente il verbale di avvenuto riconoscimento;

6 L'IdP procede alle verifiche dell'identità dichiarata;

7 Al buon esito delle verifiche l'IdP considera identificato il ***Titolare*** ed invia al suo indirizzo email il Modulo di Adesione al Servizio InfoCert ID da quest'ultimo validamente sottoscritto***.*** L'**IdP** attiva pertanto la corrispondente identità digitale InfoCert ID. Contestualmente viene trasmessa una notifica email all'Utente contente il link di accesso al portale di gestione dell'identità digitale (Selfcare).

7.5 ATTIVAZIONE DEL SERVIZIO SPID

In seguito al perfezionamento delle fasi di riconoscimento, contrattualizzazione e rilascio delle credenziali il ***Titolare*** accede ad un portale di attivazione della ID. Questa fase è comune a tutti i ***Titolari***, indipendentemente dalla procedura di richiesta di rilascio, identificazione, contrattualizzazione.

41. il ***Titolare*** accede al portale con le credenziali scelte in fase di richiesta dell'ID (UserID e password);
42. Il ***Titolare*** attiva la propria identità confermando la scelta con una OTP pervenuta via SMS sul numero di cellulare certificato;
43. il ***Titolare*** deve scegliere altresì una risposta segreta da utilizzare in caso di necessità di recupero della componente segreta delle credenziali. Il sistema consente di scegliere tra alcune domande standard o di definire una domanda personalizzata.

Per tutti i processi descritti, viene rilasciata una identità con livello di autenticazione almeno 2.

7.6 ATTRIBUTI QUALIFICATI

La gestione di attributi qualificati quali le qualifiche, le abilitazioni professionali, i poteri di rappresentanza ed ogni altro attributo specifico dell'Utente Titolare è affidata ad appositi gestori di attributi qualificati, che hanno il potere di attestarli su richiesta dei fornitori di servizi.

8 MISURE ANTI CONTRAFFAZIONE

Le misure anti contraffazione sviluppate dall'IdP InfoCert mirano a prevenire il verificarsi del furto d'identità, inteso sia come impersonificazione totale (occultamento totale della propria identità mediante l'utilizzo indebito di dati relativi all'identità di un altro soggetto in vita o deceduto) sia come impersonificazione parziale (occultamento parziale della propria identità mediante l'impiego, in forma combinata, di dati relativi alla propria persona e l'utilizzo indebito di dati relativi ad un altro soggetto).

Tra le misure, rientra la verifica dell'identità, che consiste nel rafforzamento del livello di attendibilità degli attributi, compiuta attraverso l'accesso alle fonti autoritative effettuato secondo le convenzioni di cui all'articolo 4, comma 1, lettera c) del DPCM.

Attualmente i controlli si incardinano principalmente sull'utilizzo del sistema SCIPAFI, Sistema pubblico di prevenzione che consente il riscontro dei dati contenuti nei principali documenti d'identità e riconoscimento con quelli registrati nelle banche dati degli enti di riferimento. 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, l'IdP esegue una serie di controlli manuali accedendo ai sistemi pubblici esposti dagli Enti competenti. I controlli possono essere eseguiti dall'operatore di riconoscimento nel caso di riconoscimento a mezzo webcam (si veda 7.4), ovvero da un back-office InfoCert. Nelle more del pieno accesso al sistema, le identità digitali rilasciate e verificate manualmente sono rese individuabili nel sistema dell'IdP, al fine di poter eseguire ulteriori riscontri in corso d'opera.
I controlli eseguiti sono i seguenti:

- Il codice fiscale è verificato presso il servizio messo a disposizione dall'Agenzia delle Entrate sul suo portale;
- il numero di serie del documento presentato è verificato presso il servizio presente sul portale della Polizia dello Stato per verifica dell'eventuale deposito di una denuncia di smarrimento o furto dello stesso;
- il numero della tessera sanitaria è verificato presso il servizio messo a disposizione sul portale del Progetto Tessera Sanitaria;

Inoltre le procedure di identificazione prevedono ulteriori livelli di controllo:

- L'operatore che esegue il riconoscimento a mezzo webcam o in presenza, non ammette documenti in fotocopia, ma solo documenti in originale;
- L'operatore che esegue il riconoscimento a mezzo webcam o in presenza, confronta i connotati dell'Utente con quanto riportato sul documento di identità;
- L'operatore che esegue il riconoscimento a mezzo webcam o in presenza, controlla la

congruenza tra le date di emissione e scadenza dei documenti in base alla normativa di riferimento;

- L'operatore che esegue il riconoscimento a mezzo webcam o in presenza, effettua controlli specifici sui documenti presentati, in particolare sulle misure di sicurezza in questi contenute. A titolo esemplificativo si riportano alcuni controlli antifrode che gli operatori effettuano, a fronte di debita formazione: il font del numero di serie per la Carta di Identità cartacea, l'allineamento della stampa dei dati anagrafici per la patente cartacea, l'araldica del timbro sui documenti cartacei corrispondente all'autorità emettitrice, ecc.
- 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 maggiormente diffusi (patente, carta di identità e passaporto), le cui caratteristiche sono riscontrabili anche da remoto. Per gli altri tipi di documenti ammessi dal DPR 445/2000 (patente nautica, porto d'armi, tesserini ministeriali, patentino di conduzione impianti termici, ecc), stante la minore diffusione che ne comporta una minore conoscenza delle caratteristiche essenziali, l'identificazione può essere eseguita solamente in presenza per accertare la bontà del documento con l'analisi della materialità dello stesso.

Le misure anticontraffazione si poggiano anche su elementi tecnologici:

- Sono utilizzati algoritmi crittografici robusti per garantire riservatezza e integrità dei dati, sulla base di quanto prescritto normativamente e allineato con le best practice internazionali e per la generazione e protezione dei codici OTP;
- La firma qualificata e la CNS, ove utilizzate, devono essere basate su certificati emessi da un certificatore accreditato
    - se rilasciata da InfoCert, viene automaticamente verificata la congruenza tra i dati del rilascio e quelli indicati nella richiesta di identità SPID.
    - se rilasciata da altro certificatore e non revocata la responsabilità dell'uso della stessa ricade sul Titolare del certificato e vale la presunzione del controllo esclusivo
    - ove presente, l'IR convalida l'identità del Titolare con la loro firma assumendone la responsabilità anche penale
- La chiave pubblica CIE, ove utilizzata, deve essere certificata dall'Autorità Pubblica
- L'utilizzo di firma qualificata, CIE e CNS eredita le misure delle specifiche di sicurezza.

9 SISTEMA DI MONITORAGGIO

L'IdP ha sviluppato un sistema di monitoraggio del funzionamento del sistema di identità digitale composto di:

- Fraud detection
- Sistema di sonde

9.1 FUNZIONALITÀ DI FRAUD DETECTION

Per quanto riguarda l'utilizzo, verranno adottate tipiche tecniche di fraud detection, sviluppate prendendo a benchmark i sistemi di utilizzo delle carte di credito, di account bancari e i principali provider di posta elettronica.
In dettaglio viene:

- monitorato il numero consecutivo di tentativi di login falliti fissando una soglia (10) oltre la quale le credenziali vengono sospese;
- inviata una mail giornaliera di recap degli accessi effettuati;
- verificato il numero di login per fascia oraria, inviando alert qualora si superi la soglia massima (10); l'algoritmo sarà adattativo e la soglia massima viene personalizzata, con soglie massime dipendenti dalla storia precedente dell'utente;
- verificato giornalmente la provenienza geografica delle connessioni e sollevato un alert in caso di discrepanze significative;
- monitorato il cambio password e sollevato un alert in caso di frequenza superiore ad una determinata soglia (5 per mese);
- monitorato l'utilizzo delle credenziali: ad ogni login all'utente verrà indicata la data della sua ultima connessione; in caso di inattività superiore alla soglia prevista normativamente l'utenza viene sospesa.

9.2 SISTEMA DI SONDE

9.2.1 SONDA SUL SERVIZIO DI AUTENTICAZIONE

La sonda sul servizio di autenticazione ha l'obiettivo di verificare che l'intero sistema di autenticazione risponda nel modo corretto. Nel dettaglio la sonda simula il comportamento di un utente eseguendo tutti i passi richiesti dal processo:

- la richiesta di autenticazione;
- l'inserimento delle credenziali;
- la verifica della risposta;
- sfruttando lo SP di test.

La sonda di navigazione è implementata tramite il prodotto S3 Virtual User. Tale prodotto realizza le navigazioni automatiche, come descritto sopra, per il controllo dello stato dei servizi. Tale utility

viene utilizzata a supporto del processo di Incident Management e concorre di fatto al calcolo e gestione degli SLA di servizio.

9.2.2 SONDA DI SISTEMA

Le strumentazioni di controllo dei sistemi e dei servizi sono state implementate su progetti Open Source Nagios. Nello specifico viene utilizzato il prodotto Net-eye di Wuerth Phoenix, basato su una logica di Event Management e finalizzato al monitoraggio e controllo di sistemi e servizi. Il tool permette di controllare la disponibilità di tutti gli asset fisici, virtuali e di processi e componenti di servizio e di misurarne le prestazioni ed i carichi di lavoro.
Vi è una dashboard che riporta tutti i messaggi di anomalia che lo strumento rileva sulle componenti oggetto di monitor dell'infrastruttura.
Alcuni esempi di monitor implementati per il controllo dei sistemi e processi che costituiscono il servizio sono elencati di seguito.

9.2.3 MONITOR VIRTUAL MACHINE

I monitor implementati per ogni virtual machine o server fisico controllano le caratteristiche principali testandone la disponibilità:

- Ping;
- Load (cpu, ram, swap, processes);
- Spazio disco dei file system del server.

9.2.4 MONITOR WEB SERVER

Per ogni web server funzionante si controlla lo stato di disponibilità del processo httpd.

9.2.5 MONITOR APPLICATION SERVER

In ogni application server è stato posto sotto controllo lo stato di ogni istanza di Jboss.

9.2.6 MONITOR BASE DATI DEGLI SP

In ogni Oracle database server vengono controllati i seguenti processi

- processo pmon (ASM instance e Database Instance);
- processo listener;
- check connessione per ogni schema;
- check errori interni su alert log Oracle Instance.

9.2.7 MONITOR BASE DATI DELLE IDENTITÀ

In ogni LDAP server vengono controllati i seguenti processi:

- Connessione ad ogni istanza LDAP;
- Processo di replica master su slave;

9.2.8 MONITOR RETE

I monitor degli apparati di rete (switch, fire wall, load balancer) prevedono il controllo di tutte le interfacce di rete e delle risorse CPU, RAM.

10 GESTIONE DEL CICLO DI VITA DELL'IDENTITÀ

10.1 GESTIONE ATTRIBUTI

Il Titolare che deve modificare i propri attributi identificativi può farlo accedendo al portale di gestione dell'identità rilasciata. Mediante accesso con le proprie credenziali SPID di livello 2, il Titolare può modificare:

- gli estremi del documento di riconoscimento;
- la data di scadenza del documento di riconoscimento;
- il numero di telefonia mobile;
- l'indirizzo di posta elettronica;
- il domicilio.

Ogni informazione è resa dal Titolare sotto la sua piena responsabilità. In caso di modifica del numero di telefonia mobile l'IdP procede alla sua certificazione con modalità analoghe a quelle descritte nel paragrafo 7.3.

10.2 PROCEDURE DI REVOCA DELL'IDENTITÀ

La revoca o la sospensione di una Identità Digitale, ne comportano la disattivazione, definitiva o temporanea, impedendo l'utilizzo della stessa ai fini dell'accesso ai servizi in rete dei fornitori.

10.2.1 REVOCA DA PARTE DELL'UTENTE TITOLARE

Si distinguono due ipotesi di revoca da parte dell'utente Titolare:

- **Revoca Obbligatoria**: È fatto obbligo per l'utente di richiedere immediatamente la revoca della propria identità SPID nel momento in cui accerti il venir meno delle caratteristiche di riservatezza e segretezza delle proprie credenziali, ivi compresi i casi di furto e di smarrimento delle credenziali.
- **Revoca Facoltativa**: Al di fuori delle ipotesi disciplinate in caso di revoca facoltativa, l'Utente Titolare può richiedere in ogni momento, senza necessità di motivazione, la revoca della propria Identità Digitale.

Per procedere alla revoca dell'Identità Digitale l'Utente Titolare deve collegarsi presso il sito dell'Identity Provider provvedendo ad inoltrare l'apposita richiesta, autenticando la stessa mediante l'utilizzo delle credenziali SPID di livello 2.

10.2.2 REVOCA DA PARTE DELL'IDENTITY PROVIDER

L'Identity Provider procede alla revoca dell'Identità Digitale dell'Utente Titolare, anche senza espressa richiesta di questi, nelle seguenti ipotesi:

1. in caso di inattività dell'Identità Digitale per un periodo superiore a ventiquattro mesi o in caso di decesso della persona fisica o di estinzione della persona giuridica;

2. in caso di cessazione delle attività dell'Identity Provider decorsi trenta giorni dalla comunicazione della cessazione di cui all'art. 12, 1° comma del DPCM
3. in caso di provvedimento dell'AgID
4. in caso di scadenza del contratto intercorrente tra IdP e Titolare.

In caso di revoca per inattività dell'identità o per scadenza contrattuale, l'IdP mette in atto preventive attività di avvisi ripetuti 90, 30 e 10 giorni, nonché il giorno prima della revoca, utilizzando gli attributi secondari certificati e presenti nel sistema.

10.3 PROCEDURE DI SOSPENSIONE DELL'IDENTITÀ

La sospensione di un'Identità Digitale ne comporta la disattivazione temporanea, e la medesima non potrà essere utilizzata durante il periodo di sospensione. Un'Identità Digitale sospesa può essere riattivata o revocata al termine del periodo di sospensione.

10.3.1 SOSPENSIONE DA PARTE DELL'UTENTE TITOLARE

L'Utente Titolare, può chiedere, nei casi previsti dall'art. 9 del DPCM, ossia qualora ritenga che la propria Identità Digitale sia stata utilizzata abusivamente o fraudolentemente, la sospensione immediata dell'Identità Digitale.

Per procedere alla sospensione dell'Identità Digitale l'Utente Titolare deve collegarsi presso il sito dell'Identity Provider provvedendo ad inoltrare l'apposita richiesta, autenticando la stessa mediante inserimento della OTP trasmessa presso un attributo secondario dall'Identity Provider prima dell'inoltro della richiesta.
La sospensione può altresì essere richiesta a mezzo di posta elettronica certificata, da cui sia desumibile l'identità dell'Utente Titolare, o con documento informatico sottoscritto con firma digitale o firma elettronica qualificata, da inviarsi all'indirizzo di posta elettronica certificata dell'Identity Provider indicato sul sito Internet del servizio.

Ricevuta la richiesta di sospensione l'Identity Provider sospende l'Identità Digitale per un periodo massimo di trenta giorni, fornendo apposita informazione all'Utente Titolare. Entro tale periodo l'Utente Titolare deve trasmettere all'Identity Provider copia della denuncia presentata all'autorità giudiziaria basata sui medesimi fatti su cui è fondata la richiesta di sospensione alla ricezione della quale l'Identity Provider provvede alla revoca dell'Identità Digitale.
In caso di mancata ricezione nei termini sopra indicati della denuncia l'Identity Provider ripristina l'Identità Digitale.

10.3.2 SOSPENSIONE DA PARTE DELL'IDENTITY PROVIDER

L'Identity Provider provvede autonomamente alla sospensione dell'Identità Digitale, avvertendo tempestivamente l'Utente Titolare presso l'attributo secondario, qualora accerti attività relativa ad usi impropri o tentativi di violazione delle credenziali di accesso.

10.4 PROCEDURE DI SOSPENSIONE E REVOCA DELLE CREDENZIALI

La revoca e la sospensione delle singole credenziali, alla data del presente documento, non sono ancora gestite dall'IdP.
Il Titolare può agire sulle proprie credenziali direttamente agendo sulla identità, secondo quanto previsto dai paragrafi precedenti.

11 LIVELLI DI SERVIZIO GARANTITI

Il servizio è erogato secondo quanto descritto nella Carta dei Servizi aziendale disponibile all'indirizzo Internet https://identitadigitale.infocert.it/documentazione.

I livelli di servizio garantiti dal sistema di Gestione Identità Digitale per le diverse fasi della registrazione, della gestione del ciclo di vita dell'identità e di autenticazione sono quelle concordate nella convenzione stipulate da InfoCert con Agid.

11.1 REGISTRAZIONE UTENTE

Il processo garantisce la gestione della registrazione utente titolare con tutti gli attributi qualificati e non qualificati richiesti.

Servizio	KPI (indicatore)	SLA (livelli di servizio standard garantiti)	Modalità erogazione
Registrazione utente	Disponibilità servizio	>= 99.0 % Finestra di erogazione del servizio h 24 Durata max singolo evento indisponibilità < =6 ore	Erogazione automatica
		>= 98.0 % Con finestra di erogazione del servizio di almeno 5 ore (in media) nei giorni feriali parametrizzate al numero di sportelli a disposizione	Erogazione in presenza

11.2 RILASCIO - RIATTIVAZIONE CREDENZIALI

Il processo garantisce la gestione del rilascio di una identità digitale richiesta dal cliente con il livello di sicurezza desiderato tra quelli erogati dal servizio InfoCert.

Servizio	KPI (indicatore)	SLA (livelli di servizio standard garantiti)	Modalità erogazione
Rilascio credenziali	Disponibilità servizio	>= 99.0 % Finestra di erogazione del servizio h24 (per servizio automatico) Durata max singolo evento indisponibilità < =6 ore	Erogazione automatica
		>= 98.0 % Finestra di erogazione del servizio di almento 5 ore (in media) nei giorni feriali parametrizzate al numero di sportelli a disposizione	Erogazione in presenza

11.3 SOSPENSIONE E REVOCA CREDENZIALI

Il processo garantisce la gestione della

- sospensione a tempi determinato delle credenziali effettuata on line dal titolare
- sospensione a tempi determinato delle credenziali effettuata dall'Identity Provider InfoCert
- revoca delle credenziali effettuata dall' Identity Provider InfoCert

Servizio	KPI (indicatore)	SLA (livelli di servizio standard garantiti)
Sospensione credenziali da titolare	Disponibilità servizio	>= 99,0% Finestra di erogazione del servizio h 24 (per servizio automatico) Durata max singolo evento indisponibilità <= 6 ore

11.4 RINNOVO E SOSTITUZIONE CREDENZIALI (E DISPOSITIVI CONNESSI)

Il processo garantisce la gestione del servizio di:

- rinnovo e sostituzione credenziali effettuata on line dal titolare
- rinnovo e sostituzione effettuata dall'Identity Provider InfoCert

Servizio	KPI (indicatore)	SLA (livelli di servizio standard garantiti)	Modalità erogazione
Rinnovo e sostituzione credenziali	Disponibilità servizio	>= 99.0 % Finestra di erogazione del servizio h24	Erogazione automatica
		>= 98.0 % Finestra di erogazione del servizio di almeno 5 ore (in media) nei giorni feriali (per servizio in presenza anche telematica) parametrizzate al numero di sportelli a disposizione	Erogazione in presenza

11.5 AUTENTICAZIONE

Il processo garantisce la gestione del servizio di autenticazione del Titolare:

Servizio	KPI (indicatore)	SLA (livelli di servizio standard garantiti)
Autenticazione Titolare	Disponibilità servizio	>= 99, 0 % Finestra di erogazione del servizio h24 Durata max singolo evento indisponibilità <= 4 ore
	Tempo di ripristino in caso di problema bloccante	<= 4h
	Tempo di ripristino in caso di problema non bloccante	<= 8h

11.6 CONTINUITÀ OPERATIVA

L'erogazione dei servizi è garantita con la seguente continuità operativa:

Servizio	KPI (indicatore)	SLA (livelli di servizio standard garantiti)
Registrazione Rilascio identità	RPO - Recovery Point Objective	RPO = 1hh
	RTO - Recovery Time Objective	RTO = 8hh
Sospensione e Revoca identità	RPO - Recovery Point Objective	RPO = 1hh
	RTO - Recovery Time Objective	RTO = 8hh
Autenticazione	RPO - Recovery Point Objective	RPO = 1hh
	RTO - Recovery Time Objective	RTO = 8hh

11.7 PRESIDIO DEL SERVIZIO

InfoCert definisce come "Presidio" il requisito qualitativo che garantisce il monitoraggio e la gestione dei sistemi, delle apparecchiature e della rete funzionali all'erogazione del servizio.

Servizio	KPI (indicatore)	SLA (livelli di servizio standard garantiti)
Presidio	Orario	H24 7x7

11.8 ASSISTENZA CLIENTI

Il servizio di Assistenza InfoCert ha l'obiettivo di accogliere tempestivamente le richieste di supporto e di gestire la risoluzione del problema entro il termine massimo previsto.

Servizio	KPI (indicatore)	SLA (livelli di servizio standard garantiti)
Help Desk	Presidio	L-V : 8:30 – 19:00, Escluso Festivi
	Disponibilità	L-V : 8:30 – 19:00, Escluso Festivi
	Tempi di attesa telefonica	60sec
Delivery	Presidio	L-V : 9:00 – 18:00, Escluso Festivi

APPENDICE A - CODICI E FORMATI DEI 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 del sistema								
2	Indisponibilità Sistema	HTTP POST/HTTP Redirect	n,a.	n.a.	Utente	Messaggio di errore generico	Ripetere l'accesso al servizio più tardi	n.a.	
3	Errore di Sistema	HTTP POST/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								
4	Formato binding non corretto	HTTP Redirect	HTTP: 403	n.a.	Utente	Pagina di cortesia con messaggio "*Formato richiesta non corretto - Contatare il gestore del servzio*"	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- Contatare il gestore del servzio*"	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 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- Contatare il gestore del servzio"	Contattare il gestore del servizio	Verificare metdata Gestore dell'identita (IdP)	invio richiesta in HTTP-Redirect su entrypoint HTTP-POST dell'identity
		HTTP POST							invio richiesta in HTTP-POST su entrypoint HTTP-Redirect dell'identity
	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 - Conttatare il gestore del servizio"	Contatare il gestore del servzio	Verificare certificato o modalità di apposizione firma	Firma sulla richiesta non presente, corrotta, non conforme in uno dei parametri, con certificato scaduto o non corrispondente ad un fornitore di servizi riconosciuto o 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 all'utente	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	
10	Issuer non presente, malformato o non corrispondete all'entita che sottoscrive la richiesta	HTTP POST/HTTP Redirect	HTTP: 403	n.a.	Utente	Pagina di cortesia con messaggio "Formato richiesta non corretto - Conttatare il gestore del servizio"	Contatare il gestore del servzio	Verificare formato delle richieste prodotte	
11	Identificatore richiesta(ID) non presente, malformato o non conforme	HTTP 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 :Responder urn:oasis:names:tc:SAML:2.0:status :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
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 ill 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 presenza di uno od entrambi gli attributi AssertionConsumerServiceURL e ProtocolBinding AssertionConsumerServiceIndex non presente in assenza di almeno uno attibuti AssertionConsumerServiceURL e ProtocolBinding
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	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 nr18	Fornitore del servizio (SP)	n.a.	n.a.	riformulare la richiesta con un valore dell'indice presente nei metadati	-
	Anomalie derivante dall'utente								
19	Autenticazione fallita per ripetuta sottomissione di credenziali errate (superato numero 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	Messaggi 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	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 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	
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 entroun determinati 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 sospesie o revocate"		Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto	