MANUALE OPERATIVO

Politiche e pratiche per Servizio di convalida di firme e sigilli SVS e QSVS

CODICE DOCUMENTO	ICERT-INDI-QSVS
VERSIONE	1.3
DATA	07/05/2025

tinexta infocert

SOMMARIO

INDICE DELLE FIGURE

tinexta infocert

1 INTRODUZIONE

1.1 Concetti generali

Una firma elettronica è un insieme di dati allegati a un documento elettronico, oppure ad altri dati che forniscono un'indicazione riguardo all'intenzione di una persona di accettare il contenuto del documento o dei dati a cui si riferisce la firma. Un sigillo elettronico è un insieme di dati allegati a un documento elettronico o ad altri dati, che garantisce l'origine e l'integrità dei dati su cui il sigillo è apposto. Una marca temporale elettronica è un dato in forma elettronica che lega altri dati in forma elettronica ad un orario particolare, provando che questi ultimi esistevano in quel momento specifico.

Questo documento ha lo scopo di descrivere le policy e le procedure operative adottate da InfoCert S.p.A. (nel prosieguo, anche semplicemente, "**InfoCert**") per la fornitura del servizio fiduciario qualificato per la convalida di firme elettroniche, sigilli e marche temporali qualificate (di seguito QSVS) secondo il regolamento eIDAS, nonché per la fornitura del servizio fiduciario non-qualificato per la convalida di firme elettroniche, sigilli e marche temporali (di seguito SVS). La struttura del documento segue la raccomandazione dell'allegato A di ETSI TS 119 441.

Il servizio di validazione InfoCert è stato progettato e sviluppato secondo gli standard elencati nel paragrafo 1.5.

1.1.1 Identificazione del TSP

InfoCert S.p.A è il fornitore dei servizi SVS e QSVS. InfoCert è iscritta al registro delle imprese di Roma con partita IVA 07945211006.

1.1.2 Policy supportate per il servizio di convalida della firma

La validazione di firme / sigilli / marche temporali elettroniche viene sempre eseguita dai servizi SVS e QSVS secondo le rispettive policy del servizio di convalida delle firme.

Questo documento è associato alle policy dei servizi di convalida della firma, qualificata per QSVS e non qualificata per SVS, identificata dagli Object Identifier (OID) descritti di seguito.

L'Object Identifier (OID) che identifica InfoCert è **1.3.76.36**

Descrizione	*OID*
QSVSP – Policy del servizio di convalida della firma InfoCert conforme ai criteri di convalida qualificati ETSI TS 119 441, che includono i requisiti specificati nell'annex B	1.3.76.36.1.1.90 in base a 0.4.0.19411.1.2
SVSP – Policy del servizio di convalida della firma InfoCert conforme ai criteri di convalida ETSI TS 119 441, ad esclusione dei requisiti specificati	1.3.76.36.1.1.91 In base a 0.4.0.19411.1.1

Descrizione	OID
nell'annex B	

Tabella 1 – OID

Sia SVS che QSVS utilizzano la seguente policy di convalida delle firme:

Nome	Descrizione	Conformità
Ad/Q-ESig Ad/Q-ESeal Ad-ESigQC Ad-ESealQc TL	Validates electronic signatures and seals, indicating whether they are Advanced electronic Signatures (AdESig), AdES supported by a Qualified Certificate (AdESigQC), Qualified electronic Signature (QESig) validated against the EU Member State Trusted Lists (this includes signer's certificate and certificates used to validate certificate validity status services - CRLs, OCSP, and time-stamps), Advanced electronic Seals (AdESeal), AdES supported by a Qualified Seal (AdESealQC), Qualified electronic Seal (QESeal).	Conforme all'OID 0.4.0.191724.1.1 definito in ETSI TS 119 172-4 [7]

Tabella 2 – Policy di convalida delle firme

L'esistenza della firma in un dato istante temporale (PoE, Proof of Existence) viene verificata considerando il timestamp della marcatura temporale dove presente, altrimenti l'attributo firmato "signing time" della firma. Nel caso in cui anche quest'ultimo fosse assente, verrebbe considerato come istante temporale l'istante di validazione della firma da parte del SVS o QSVS.

1.2 Componenti del servizio di convalida della firma

1.2.1 Attori del SVS

Le attività, sia di SVS che di QSVS, includono la partecipazione dei seguenti attori:

- il firmatario, considerando anche che la validità della firma può essere limitata/influenzata dall'utilizzo di policy di creazione delle firme o da certificati di firma non validi;
- il QTSP che ha rilasciato i certificati di firma;
- il QTSP che ha rilasciato i certificati di marcatura temporale;
- i provider della trusted list degli stati membri dell'Unione Europea;
- la Commissione Europea che fornisce la lista delle trusted lists.

1.2.2 Architettura del servizio

SVS e QSVS espongono due funzionalità:

- la validazione di un documento firmato e/marcato;

- la validazione di un certificato, ovvero la verifica che un dato certificato non sia scaduto, sospeso o revocato al momento della richiesta di convalida.

Per quanto riguarda la validazione di un documento, SVS e QSVS eseguono il controllo del formato della firma, l'identificazione dei certificati di firma, l'inizializzazione del contesto di convalida, il controllo dell'aggiornamento della revoca, la convalida del certificato X.509, la convalida crittografica e la convalida dell'accettazione della firma secondo i requisiti di ETSI EN 319 102-1.

SVS e QSVS implementano il protocollo di convalida della firma lato server. In particolare:

- eseguono il protocollo del servizio di convalida delle firme ed elaborano la convalida della firma lato SVSP;
- eseguono l'applicazione di convalida della firma (SVA) che implementa l'algoritmo di validazione definito in ETSI EN 319 102-1. A tal fine, il servizio può richiamare attori esterni, ad esempio:
- La CA che ha emesso il certificato di firma (per ottenere informazioni sullo stato del certificato o per ottenere la CRL)
- La CA delle TSA che hanno fornito le marche temporali all'interno della firma
- Le trusted list degli Stati Membri dell'Unione Europea, la lista delle Trusted Lists della Commissione Europea (nel caso di QSVS)
- e/o altre trusted lists (nel caso di SVS)

- creano il report di convalida della firma relativo alla richiesta;
- costruiscono la risposta della convalida della firma.

Per quanto riguarda la validazione di un certificato, SVS e QSVS eseguono la convalida del certificato X.509 tramite l'algoritmo di validazione definito in ETSI EN 319 102-1. Il servizio può richiamare attori esterni, ad esempio la CA che ha emesso il certificato di firma, per ottenere informazioni sullo stato del certificato o per verificare la catena di certificazione, oppure i servizi di OCSP o di CRL remoti per verificare lo stato del certificato.

1.2.3 Processo

SVS e QSVS ricevono le richieste di convalida della firma e/o del certificato, e restituiscono le sue risposte ai client che le richiedono. La risposta può essere fornita in modo sincrono o asincrono. Il canale di comunicazione tra i client che richiedono la convalida delle firme e il SVS o QSVS copre l'autenticazione del SVS/QSVS e può supportare anche l'autenticazione del client.

SVS e QSVS invocano altri servizi TSP solo per recuperare lo stato dei certificati di firma e/o di marcatura temporale.

Il processo svolto dal QSVS può essere suddiviso nei seguenti passaggi.

Step 1. SVS e QSVS ricevono una richiesta di convalida della firma.

Se è una richiesta di convalida della firma, la richiesta include:

- I documenti firmati (Signer's Document, SD) e le firme (Signed Data Object, SDO) che li firmano; oppure
- Le rappresentazioni dei documenti firmati (SDR) e le firme che li firmano, per evitare di esporre il contenuto del documento al servizio di convalida.
- (opzionale) vincoli di convalida, come definiti in ETSI EN 319 102-1.

Se è una richiesta di convalida di un certificato, la richiesta include:

1. Il certificato formattato in Base64;
2. (opzionale) vincoli di convalida, come definiti in ETSI EN 319 102-1.

Step 2. SVS e QSVS eseguono il processo di convalida.

Il processo di convalida è conforme alle specifiche ETSI EN 319 102-1.

La convalida è effettuata dal SVSP o QSVSP secondo dei vincoli che possono essere forniti sia dal client che richiede la convalida della firma e/o dal servizio stesso.

1. Se non fornito dalla richiesta del client, il SVS implementa una policy di convalida della firma con "valore predefinito".
2. Se fornito dal client, allora la policy di convalida della firma del client può essere completata come richiesto dalle pratiche SVSP.

Step 3. SVS e QSVS preparano e inviano la risposta di convalida.

La risposta di convalida include i report di convalida. Riporta l'OID della policy di servizio e include l'OID della policy di convalida della firma che è stata utilizzata.

Il report di convalida è conforme alla specifica ETSI TS 119 102-2. Solo nel caso di QSVS, il report è sigillato da un certificato eSeal InfoCert. Esso riporta su ciascun vincolo di convalida:

- quando il vincolo è stato elaborato, con il relativo esito,
- quando il vincolo non è stato elaborato con un'indicazione che il vincolo è stato ignorato, o sovrascritto, dove pertinente.

Esiste un rapporto di convalida per ciascuna firma digitale convalidata.

1.3 Definizioni e abbreviazioni

1.3.1 Definizioni

Convalida della firma: processo di verifica e conferma che una firma digitale è tecnicamente valida

Vincolo di convalida della firma: criteri tecnici in base ai quali una firma digitale può essere convalidata

Policy di convalida della firma: insieme di **vincoli di convalida della firma** elaborati o da elaborare da parte dell'applicazione di convalida della firma (Signature Validation Application, SVA)

1.3.2 Abbreviazioni

Descrizione	OID
0.4.0.19441.1.1	SVSP conforme a ETSI TS 119 441 OID
0.4.0.19441.1.2	QSVSP conforme a ETSI TS 119 441 OID
DA	driving application: in ETSI EN 319 102-1, applicazione che utilizza un'applicazione di convalida della firma (SVA) per convalidare le firme digitali
QSVS	Qualified Signature Validation Service
QSCD	Qualified Signature/Seal Creation Device
QSVSP	Qualified Signature Validation Service Provider
QSVSPS	Qualified Signature Validation Service Practice Statement
(SVS) policy and practice statement	insieme di regole o/e dichiarazione di pratica che indica l'applicabilità di un servizio di convalida della firma a una particolare comunità e/o classe di applicazione con requisiti di sicurezza comuni
SVSP	Un Trust Service Provider (TSP) che esegue la convalida di una firma digitale si chiama Signature Validation Service Provider
SVR	Signature Validation Report. Il risultato del SVS
SVA	signature validation application: in ETSI EN 319 102-1, applicazione che convalida una firma rispetto a una policy di convalida della firma, e che genera un'indicazione di stato (ovvero lo stato di convalida della firma) e un report di convalida della firma
SVS	Signature Validation Service
SD	Signer's document, il documento da firmare
SDO	Signed Data Object, l'oggetto firmato
SDR	Signer's Document Representation, la rappresentazione di un documento da firmare

Tabella 3 – Abbreviazioni

1.4 Policy e pratiche

1.4.1 Organizzazione che gestisce la documentazione del TSP

InfoCert è responsabile della gestione dell'insieme delle pratiche relative ai servizi SVS e QSVS.

InfoCert è responsabile della definizione, aggiornamento e pubblicazione di questo documento.

InfoCert 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.

Le procedure di revisione del Manuale Operativo sono analoghe alle procedure di redazione. Le revisioni sono apportate di concerto con il Responsabile del Servizio di Certificazione, il Responsabile della Sicurezza, il Responsabile della Privacy, l'Ufficio Legale e l'Area di Consulenza e approvate dal management.

Questo Manuale Operativo viene verificato dal Responsabile della Sicurezza e delle policies, dal Responsabile della Privacy, dal Responsabile del Servizio, dal Responsabile Legale, dal Responsabile Regulatory e approvato dalla Direzione Aziendale. Questi SVSPS e QSVSPS saranno riesaminati almeno una volta all'anno.

Questi SVSPS e QSVSPS sono pubblicati sul sito istituzionale di InfoCert anche in lingua inglese.

Informazione	*Dettaglio*
Versione/Release n°:	**1.3**
Data Versione/Release:	**05/05/2025**
Descrizione modifiche:	Aggiornamento logo e sede operativa e legale Roma Revisione CPS integrando SVS e QSVS Aggiornamento recapito telefonico InfoCert Revisione generale degli stili e dei formati del documento
Motivazioni:	**Revisione generale del documento, accessibilità, aggiornamenti, correzioni** e introduzione della validazione non qualificata (SVS)

Tabella 5 - Versione 1.3

Informazione	*Dettaglio*
Versione/Release n°:	**1.2**
Data Versione/Release:	**04/06/2024**
Descrizione modifiche:	§ 1.4.1 spostato contenuto da 1.4.3; § 1.4.3 aggiunto contenuto secondo Annex A; § 2.1.1 aggiunto sub-contractor AWS; § 2.6 aggiornate versioni delle librerie crittografiche;

Informazione	Dettaglio
	Aggiunta Appendice A con documentazione relativa ai test.
Motivazioni:	revisione del documento per riorganizzazione contenuti secondo Annex A

Tabella 6 – Versione 1.2

Informazione	Dettaglio
Versione/Release n°:	**1.1**
Data Versione/Release:	**14/04/2024**
Descrizione modifiche:	§ 1.1.2 descrizione della policy di convalida delle firme e della Proof of Existence; § 1.2 aggiunta la validazione di un certificato; Aggiornamento del logo aziendale.
Motivazioni:	revisione del documento per riorganizzazione contenuti secondo Annex A

Tabella 7 – Versione 1.1

Informazione	Dettaglio
Versione/Release n°:	**1.0**
Data Versione/Release:	**22/02/2024**
Descrizione modifiche:	prima emissione
Motivazioni:	prima emissione del documento

Tabella 8 – Versione 1.0

1.4.2 Contatti

Per domande, reclami, commenti e richieste di chiarimento in merito a questa Dichiarazione delle Pratiche di Servizio, si prega di contattare:

Denominazione sociale	**Infocert – Società per azioni** **Responsabile del Servizio di Certificazione Digitale** **Piazza Luigi da Porto n. 3, 35131 Padova (PD)**
N. di telefono	0683669635
Contact Center	**https://help.infocert.it/contatti/ per maggiori dettagli**
Web	**https://www.firma.infocert.it, https://www.infocert.it**
E-mail	**firma.digitale@legalmail.it**

1.4.3 Applicabilità della documentazione TSP (pubblica)

Vedere l'intestazione del documento e il paragrafo 1.1.2.

La documentazione relativa ai servizi di convalida si compone dei seguenti oggetti:

- il presente CPS, o Manuale Operativo, ICERT-INDI-QSVS definito dagli OID 1.3.76.36.1.1.90 per QSVS e 1.3.76.36.1.1.91 per SVS. Si applica l'ultima versione pubblicata sul sito istituzionale di InfoCert;
- le CGC, Condizioni Generali di Contratto, che regolano i rapporti con i clienti che sottoscrivono il servizio. Si applica l'ultima versione pubblicata sul sito istituzionale di InfoCert;
- le pratiche di servizio descritte dal presente CPS e definite al paragrafo 1.1.2. Lo stesso

paragrafo identifica anche le policy di convalida della firma che sono supportate da SVS e QSVS e definite da un OID formale, ritornato anche nelle risposte del servizio;

- l'analisi del rischio e le policy di sicurezza delle informazioni adottate (Security Checklist e Privacy Checklist), aggiornate annualmente nello spazio documentale InfoCert, ma non rese pubbliche all'esterno;
- il piano di test e i test report con i risultati, secondo quanto descritto nell'Appendice A di questo CPS.

1.5 Riferimenti

I seguenti documenti referenziati sono necessari per l'applicazione del presente documento.

[1] ETSI TS 119 101: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation".

[2] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[3] ETSI TS 119 441: "Electronic Signatures and Infrastructures (ESI); Policy requirements for TSP providing signature validation services".

[4] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation".

[5] ETSI TS 119 102-2: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report".

[6] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[7] ETSI TS 119 172-4: "Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 4: Signature applicability rules (validation policy) for European qualified electronic signatures/seals using trusted lists".

[8] ETSI EN 319 142-1: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures".

[9] ETSI EN 319 142-2: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles".

[10] ETSI TS 103 172: "Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile".

[11] ETSI TS 103 171: "Electronic Signatures and Infrastructures (ESI); XAdES Baseline

Profile".

[12] ETSI EN 319 132-1: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures".

[13] ETSI EN 319 132-2: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 2: Extended XAdES signatures ".

[14] ETSI TS 103 173: "Electronic Signatures and Infrastructures (ESI); CAdES Baseline Profile".

[15] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[16] ETSI EN 319 122-2: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures".

[17] ETSI TS 103 174: "Electronic Signatures and Infrastructures (ESI); ASiC Baseline Profile".

[18] ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC baseline containers".

[19] ETSI EN 319 162-2: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 2: Additional ASiC containers".

[20] ETSI TS 119 182-1: "Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures".

2 GESTIONE E FUNZIONAMENTO DEL SERVIZIO FIDUCIARIO

2.1 Organizzazione interna

La struttura organizzativa interna a supporto dell'attività del QTSP è descritta nel documento “Servizi di Posta Elettronica Certificata e Certificazione Digitale – Struttura Organizzativa” (ICERT-CAPEC-ORG). Il servizio è erogato tramite una struttura informatica di proprietà di InfoCert e sotto il completo controllo e responsabilità di InfoCert.

2.1.1 Affidabilità dell’organizzazione

Come definito nel documento “Trust Service Provider InfoCert – Certificate Practice Statement”, avente ID ICERT-INDI-MO.

I dati firmati non vengono mai archiviati da SVS e QSVS. I servizi SVS e QSVS sono erogati su Cloud AWS, il quale è un sub-contractor gestito secondo la policy aziendale.

2.1.2 Segregazione dei compiti

Le attività e i compiti del personale del QTSP sono ben definiti e documentati. Il sistema di organizzazione della sicurezza si basa su un robusto principio di sicurezza di tipo logico (operatori a vari livelli, amministratori di sistema, ecc.).

La segregazione logica dei compiti è fornita dal sistema di controllo accessi. Per gli amministratori di sistema vengono registrate le operazioni di accesso e disconnessione, come previsto dal GDPR. Il tempo di conservazione di tali registrazioni è di 6 mesi, le registrazioni possono essere verificate da personale non amministratore.

2.2 Risorse umane

Come definito in “Certificate policy & Certificate Practice Statement - ICERT-INDI-MO” del Trust Service Provider InfoCert.

2.3 Gestione degli asset

Come definito in “Certificate policy & Certificate Practice Statement - ICERT-INDI-MO” del Trust Service Provider InfoCert.

2.4 Controllo accessi

Come definito in “Certificate policy & Certificate Practice Statement - ICERT-INDI-MO” del Trust Service Provider InfoCert.

2.5 Controlli crittografici

Come definito in “Certificate policy & Certificate Practice Statement - ICERT-INDI-MO” del Trust Service Provider InfoCert.

Per fornire il proprio servizio, il QSVSP deve generare una coppia di chiavi utilizzata per firmare i report di convalida.

Tali chiavi sono generate esclusivamente dal personale addetto a tale funzione. La generazione di chiavi e firme avviene all'interno di moduli crittografici dedicati e certificati, come previsto dalla normativa vigente.

Il certificato che firma il report di convalida è emesso da un servizio CA/QC di InfoCert.

La protezione della chiave privata del QSVS è garantita dalla generazione della chiave e dall'utilizzo del modulo crittografico. La chiave privata può essere generata solo se sono contemporaneamente presenti due dipendenti per la generazione della chiave. La generazione delle chiavi avviene in presenza del responsabile del servizio.

Le chiavi private del QSVS sono duplicate al solo scopo di essere recuperate dopo un guasto del dispositivo di firma sicura. La duplicazione avviene attraverso una procedura controllata mediante la quale la chiave e il suo contesto vengono duplicati su più dispositivi come richiesto dai criteri di sicurezza dei dispositivi HSM.

Il modulo crittografico utilizzato per la generazione delle chiavi e per la firma è conforme ai requisiti che garantiscono:

- la conformità della coppia di chiavi ai requisiti minimi imposti dagli algoritmi di generazione e di verifica utilizzati;
- una giusta probabilità per la generazione di possibili coppie di chiavi;
- l'identificazione del soggetto che attiva la procedura di generazione;
- che la generazione della firma avvenga all'interno del dispositivo in modo che il valore della chiave privata in uso non possa essere intercettato.

2.6 Sicurezza fisica e ambientale

Come definito in "Certificate policy & Certificate Practice Statement - ICERT-INDI-MO" del Trust Service Provider InfoCert.

Le librerie crittografiche utilizzate da SVS e QSVS permettono di gestire gli algoritmi crittografici e le dimensioni definite in ETSI TS 119 312. Vengono utilizzate le librerie crittografiche dss-framework 6.2 e bouncycastle 1.80.

2.7 Sicurezza operativa

Come definito in "Certificate policy & Certificate Practice Statement - ICERT-INDI-MO" del Trust Service Provider InfoCert.

Il sistema operativo dei computer utilizzati nelle attività di validazione coinvolte nella generazione delle chiavi, nella convalida e nella creazione delle firme è rinforzato, ovvero è configurato per ridurre al minimo l'impatto di eventuali vulnerabilità eliminando funzionalità non necessarie per le operazioni e la gestione dei servizi SVS e QSVS.

Gli amministratori di sistema, incaricati per questo scopo ai sensi della normativa vigente, accedono al sistema tramite un'applicazione root su richiesta, che consente di utilizzare i privilegi di utente root solo previa autenticazione individuale. Ogni accesso viene tracciato, registrato e archiviato per 12 mesi.

Le librerie utilizzate nelle operazioni di validazione sono ben testate e regolarmente riviste e aggiornate, controllando soprattutto eventuali annunci di bug o vulnerabilità.

SVS e QSVS utilizzano protocolli sicuri come il Transport Layer Security o una connessione tramite una VPN sicura, in modo che tutti i dati sensibili siano protetti da crittografia, inoltre viene definita e implementata una policy relativa alla sicurezza delle chiavi e alla gestione delle chiavi secondo i requisiti di ETSI TS 119 312.

2.8 Sicurezza della rete

Come definito in "Certificate policy & Certificate Practice Statement - ICERT-INDI-MO" del Trust Service Provider InfoCert.

SVS e QSVS non memorizzano dati riservati e non eseguono alcuna connessione a sistemi di archiviazione o elaborazione di dati riservati.

2.9 Gestione degli incidenti

Come definito in "Certificate policy & Certificate Practice Statement - ICERT-INDI-MO" del Trust Service Provider InfoCert.

2.10 Raccolta delle evidenze

I record per ogni evento principale dei servizi SVS e QSVS vengono redatti e archiviati. I log degli eventi sono raccolti e archiviati nel sistema di conservazione InfoCert secondo le modalità descritte nel manuale di sicurezza del sistema di conservazione. I log degli eventi sono conservati per un periodo di 7 anni nel sistema di conservazione di InfoCert.

2.11Gestione della continuità operativa

Come definito in "Certificate policy & Certificate Practice Statement - ICERT-INDI-MO" del Trust Service Provider InfoCert.

Nel caso di QSVS, i report di convalida delle firme sono firmati digitalmente e includono i timestamp delle firme. Eventuali ulteriori aumenti delle firme dei report di convalida, per essere validate a lungo termine, sono a carico dei sottoscriventi.

2.12 Cessazione e piano di cessazione del TSP

Come definito in "Certificate policy & Certificate Practice Statement - ICERT-INDI-MO" del Trust Service Provider InfoCert.

2.13 Conformità

Come definito in “Certificate policy & Certificate Practice Statement - ICERT-INDI-MO” del Trust Service Provider InfoCert.

Nessun dato personale viene elaborato da terze parti. Dopo il completamento dell'elaborazione, i dati firmati non vengono mai archiviati dai servizi SVS e QSVS.

3 ARCHITETTURA DEL SERVIZIO DI CONVALIDA DELLA FIRMA

3.1 Requisiti del processo di convalida della firma

I servizi SVS e QSVS InfoCert consentono a un sottoscrivente di fornire dati firmati e/o firme da convalidare tramite un’API. SVS e QSVS eseguono il processo di convalida secondo l’algoritmo di validazione definito in ETSI EN 319 102-1. La convalida dei requisiti per AdES/QC e QES è eseguita secondo la policy di convalida della firma di ETSI TS 119 172-4. Attraverso la stessa API menzionata sopra, verrà restituito al sottoscrivente un report di validazione in formato XML, che nel caso di QSVS viene anche sigillato con un certificato di sigillo elettronico qualificato InfoCert la cui chiave privata è protetta da un QSCD.

Nella figura sottostante, estratta da ETSI EN 319 102-1, c'è una rappresentazione degli elementi di base utilizzati per implementare l'algoritmo di convalida e del modo in cui questi blocchi sono correlati tra loro per ottenere la convalida delle firme.

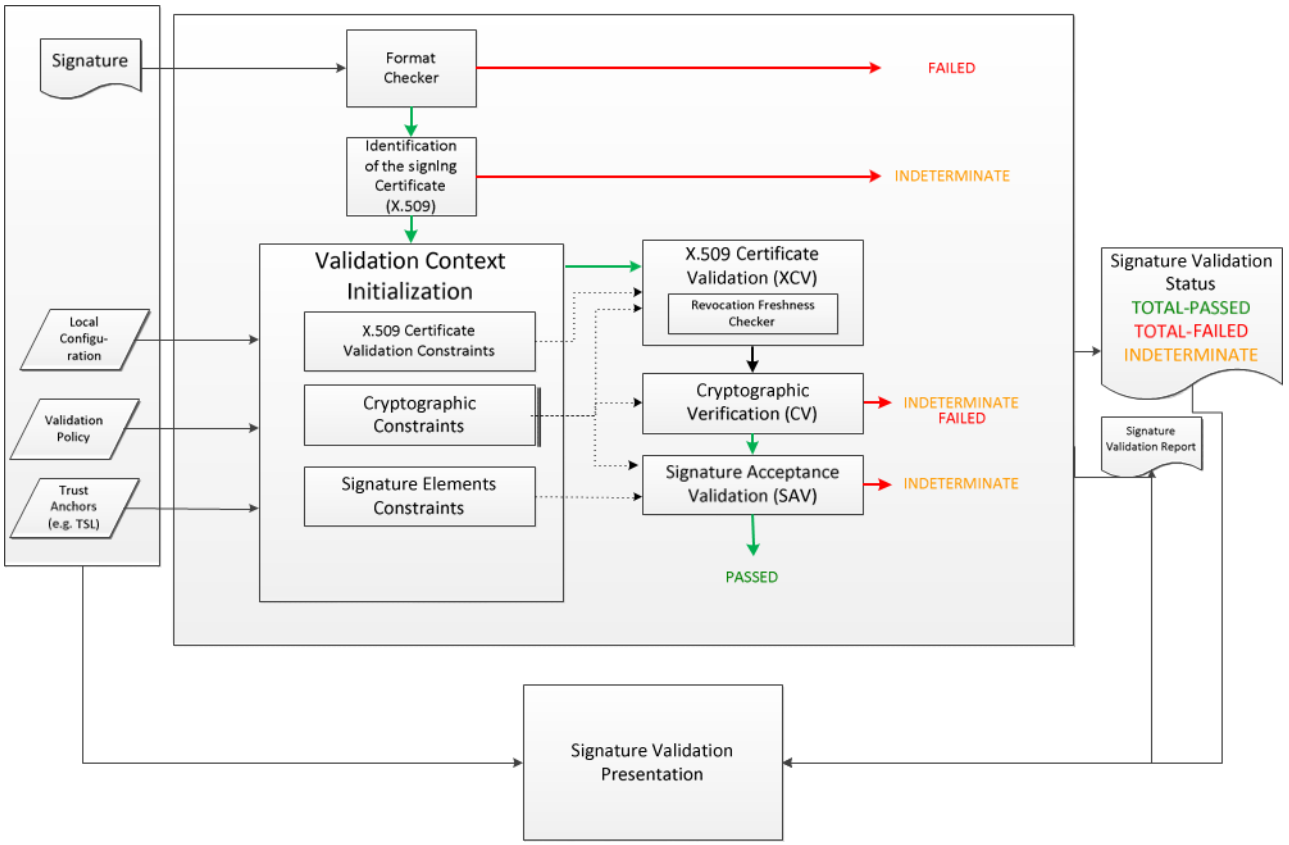


Figura 1 – Convalida della firma di base

I servizi SVS e QSVS InfoCert supportano solamente una policy di convalida della firma che permette di validare AdES/QC e QES secondo ETSI TS 119 172-4.

SVS e QSVS InfoCert supportano la validazione dei seguenti formati di firma: ETSI TS 103 172 e ETSI EN 319 142 per PAdES, ETSI TS 103 171 e ETSI EN 319 132 per XAdES, ETSI TS 103 173 e ETSI EN 319 122 per CAdES, ETSI TS 103 174 e ETSI EN 319 162 per ASiC, ETSI TS 119 182-1 per JAdES.

Il processo eseguito dal SVS e dal QSVS può essere suddiviso nei 4 passaggi seguenti.

1. Il servizio riceve una richiesta di convalida della firma. La richiesta deve includere:
    a. il SDO con le firme incorporate, oppure
    b. il SD e le corrispondenti firme detached.
2. Il SVS o QSVS esegue il processo di validazione secondo le specifiche ETSI EN 319 102-1.
3. Il SVS o QSVS prepara il report di convalida, che nel caso di QSVS è anche sigillato. In entrambi i casi il report è comunque conforme alle specifiche ETSI TS 119 102-2 e viene incluso nella risposta di convalida della firma.
4. Il SVS o QSVS invia la risposta di convalida della firma al sottoscrivente che ha richiesto la convalida della firma.

Una sonda verifica quotidianamente l'integrità dei componenti dei servizi SVS e QSVS. In caso di rilevamento di modifiche non autorizzate ai componenti critici di SVS e QSVS, come ad esempio i file di configurazione, tali componenti vengono ripristinati o disabilitati fino a quando il loro ripristino non sia possibile.

3.2 Requisiti del protocollo di convalida della firma

Non è possibile per il sottoscrivente fornire una policy di convalida della firma.

Il sottoscrivente deve:

- invocare il SVS o QSVS InfoCert tramite le API fornite;
- nel caso di QSVS verificare il sigillo elettronico qualificato apposto sul report di convalida.

Le parti che fanno affidamento sul servizio QSVS dovrebbero:

- validare il sigillo elettronico qualificato apposto sul report di convalida.

3.3 Interfacce

Secondo il modello concettuale del processo di convalida delle firme / marche temporali definito in ETSI EN 319 102-1, la SVA riceve richiesta da una DA come mostrato nella figura seguente estratta da ETSI EN 319 102-1.

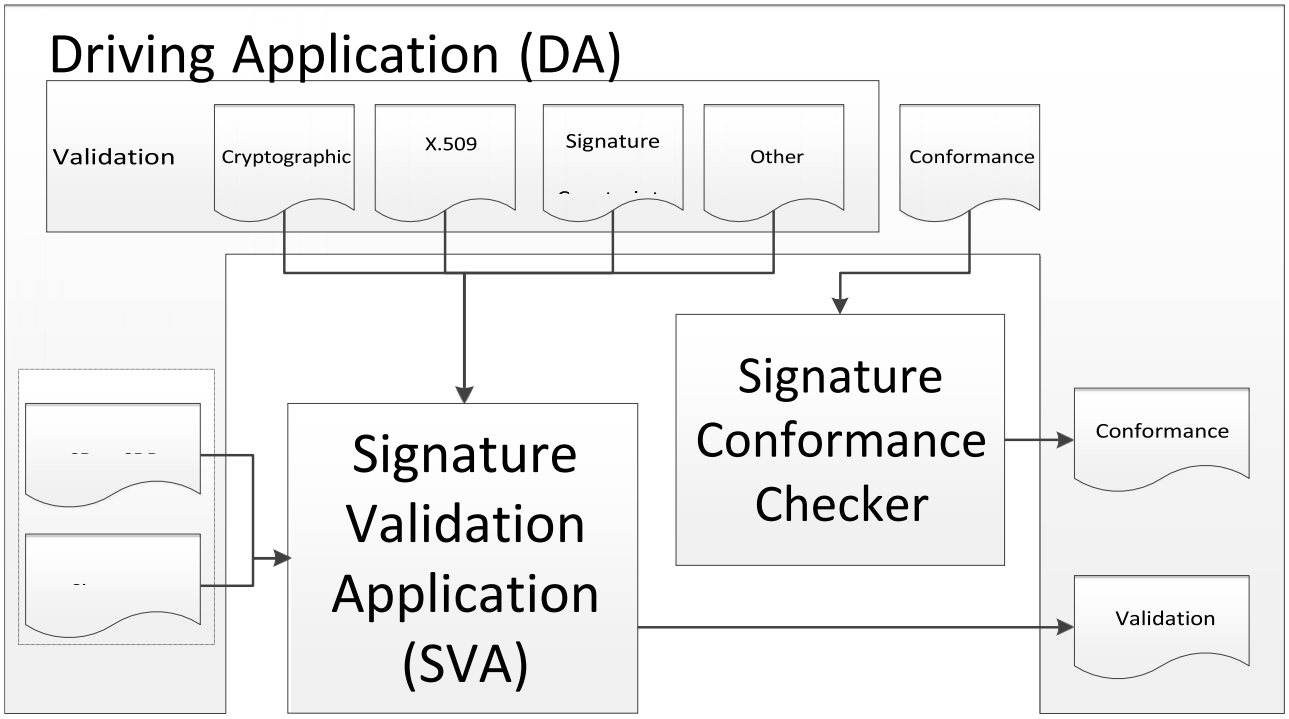


Figura 2 – Modello concettuale di convalida della firma

Al momento il sottoscrivente può passare il SD/SDR e/o la firma, ma non è autorizzato a fornire nessun altro input per il processo di validazione (ovvero qualsiasi elemento che possa parametrizzare il processo di validazione, come vincoli o requisiti di conformità).

SVS e QSVS utilizzano protocolli sicuri come il Transport Layer Security o una connessione tramite una VPN sicura. Pertanto, il canale di comunicazione tra la DA e il SVS o QSVS è protetto, consentendo al SVS o QSVS di essere autenticato dalla DA, e a tutti i dati scambiati di essere protetti da crittografia, garantendo così la riservatezza dei dati. SVS e QSVS non memorizzano il SD/SDR o la firma.

3.3.1 Canale di comunicazione

Il canale di comunicazione tra la DA (client) e il SVS o QSVS trasporta la richiesta di convalida della firma e la risposta. È sincrono. Esso permette l'autenticazione del SVS o QSVS tramite il protocollo di comunicazione TLS. Non sono accettate versioni deprecate del protocollo. I sottoscriventi del SVS e QSVS sono autenticati.

SVS e QSVS interrogano l'OCSP per i dati relativi allo stato del certificato e/o le CRL tramite le URL incorporate nelle informazioni sull'autorità nei certificati di firma e nelle estensioni cRLDistributionPoints.

3.3.2 SVSP - altri TSP

Per eseguire la fornitura del servizio, in fase di verifica della revoca, SVS e QSVS potrebbero dover comunicare con altri QTSP interrogando i loro servizi OCSP e/o i punti di distribuzione CRL. Viene utilizzato principalmente il protocollo OCSP; se l'interfaccia non è disponibile o non fornisce risposte pertinenti, viene utilizzato un punto di distribuzione CRL, se disponibile.

Il servizio di validazione OCSP è influenzato dalle pratiche, policy e SLA di altri QTSP che non sono sotto il controllo di InfoCert.

3.4 Requisiti del report di convalida della firma

I servizi SVS e QSVS nella loro risposta a una richiesta di convalida della firma forniscono un'indicazione sullo stato e un report di convalida conforme a ETSI TS 119 102-2. In base ai risultati dell'elaborazione della convalida di una firma, il report di convalida della firma indicherà uno dei tre stati TOTAL-PASSED, TOTAL-FAILED, INDETERMINATE e le relative sottoindicazioni come definito in ETSI EN 319 102-1. Il report di convalida della firma indica l'utilizzo di una policy di validazione della firma implicita per la validazione di QES, AdES QC, marche temporali qualificate, marche temporali riconosciute a livello nazionale e relativi vincoli di validazione. Il report di convalida della firma include

- l'identità di InfoCert S.p.A. come SVSP o QSVSP riportando le seguenti informazioni:
  - X509Certificate
  - X509SubjectName

    - Ds:KeyValue
    - X509SKI
    - TSP Name
    - TSP Postal and Electronic Address
    - TSP Information URI
- l'identità del firmatario
- un'indicazione di eventuali attributi firmati
- un'indicazione del processo di convalida eseguito
    - processo di convalida per firme di base
    - processo di convalida per firme con tempo e per firme con materiale di convalida a lungo termine
    - processo di convalida per firme disponibili a lungo termine e integrità del materiale di convalida
- un'indicazione della qualità delle marche temporali, se presenti nelle firme in corso di validazione
- un'indicazione sul soggetto che ha eseguito il calcolo dell'hash
- un'indicazione che l'origine di ciascun POE sia all'interno delle firme

Nel caso di QSVS, il report di convalida della firma è sigillato tramite un certificato di sigillo elettronico qualificato intestato a InfoCert. Tale sigillo elettronico è una firma XAdES-B-T.

APPENDICE A

Il piano di test è descritto con il linguaggio Gherkin. Ogni tipologia di validazione di firme è contenuta in un feature file. Ogni feature contiene uno o più scenari di test. Un esempio di feature file contenente gli scenari di validazione per firme CADES è il seguente:

```
Feature: FUN.2.0: Validate CADES signed files

 Background:
   Given I authenticated on the identity provider
   And I received an authorization token

 Scenario Outline: FUN.2.0.<funCode>: validate <type>
   When I validate a signed file of type "<type>"
   And I get a validation result
   Then I generate the validation report
   And I check the result is successful

   Examples:
   | funCode | type                          |
   | 1       | cades-b-enveloping            |
   | 2       | cades-t-enveloping            |
   | 3       | cades-lta                     |
   | 4       | cades-t-detached-full-content |
   | 5       | cades-t-detached-digest       |
```

Gli scenari di test comprendono le seguenti tipologie di validazioni di firme:

- cades-b-enveloping
- cades-t-enveloping
- cades-lta
- cades-t-detached-full-content
- cades-t-detached-digest
- pades-b-invisible
- pades-t-invisible
- pades-lta-invisible
- pades-b-2-fields
- pades-t-2-fields
- pades-lta-2-fields
- xades-b-enveloping
- xades-t-enveloping
- xades-lta-enveloping
- xades-b-enveloped
- xades-t-enveloped

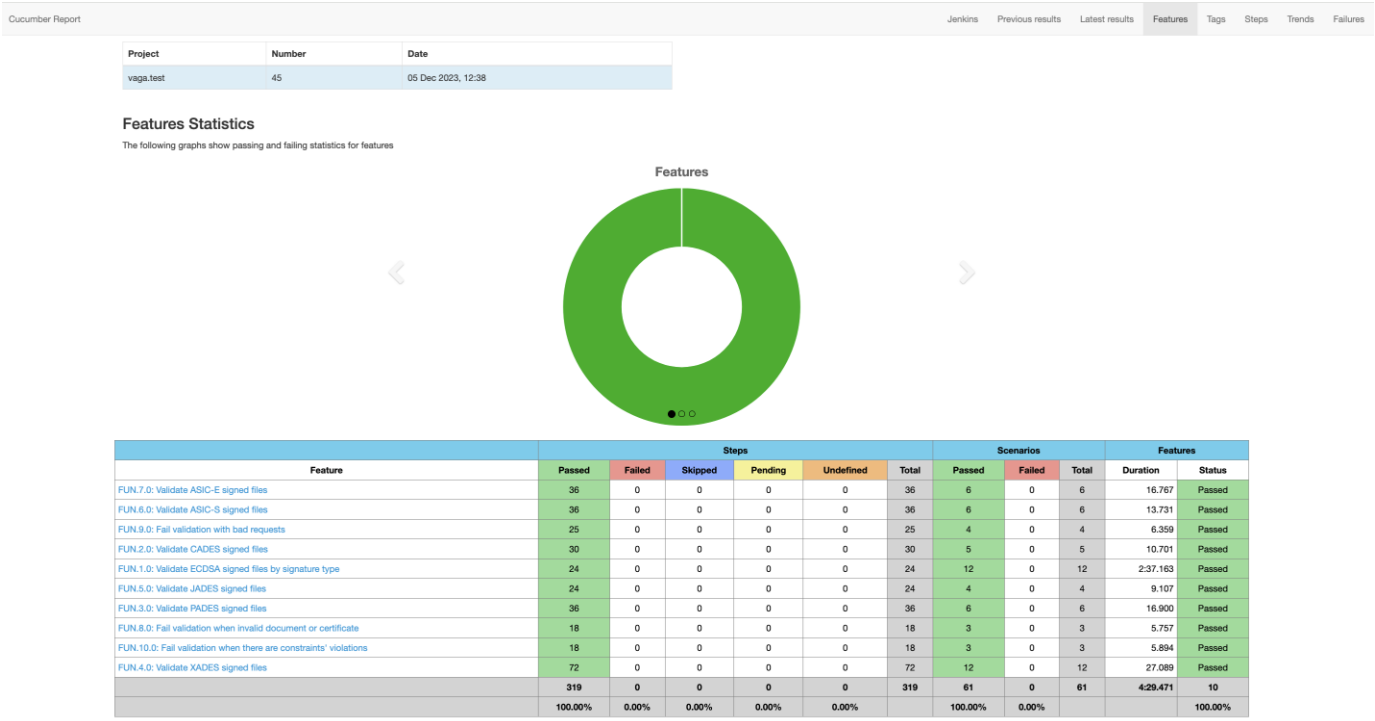
- xades-lta-enveloped
- xades-b-detached
- xades-t-detached
- xades-lta-detached
- xades-lta-detached-multiple-files
- xades-lta-enveloping-multiple-files
- xades-epes
- jades-t-enveloped
- jades-lta-enveloped
- jades-t-detached
- jades-lta-detached
- asic-s-xades-b
- asic-s-xades-t
- asic-s-xades-lta
- asic-s-cades-b
- asic-s-cades-t
- asic-s-cades-lta
- asic-e-cades-b
- asic-e-cades-t
- asic-e-cades-lta
- asic-e-xades-b
- asic-e-xades-t
- asic-e-xades-lta

E validazioni con scenari di test negativi:

- invalid-certificate
- expired-certificate
- untrusted-certificate
- document modified-after-signature
- bad-original-content-type-detached
- bad-original-content-name-detached
- unsigned-content
- bad-original-content-detached
- XCV violation revoked
- CV violation data-integrity
- SVO violation timestamp

Ciascuno step descritto nello scenario è implementato con il framework Cucumber in Java. Quando viene lanciata l'esecuzione dei test tramite comando Maven, vengono eseguite tutte le feature, tutti gli scenari e tutti gli step. Al termine dell'esecuzione, si possono visualizzare i risultati. I test possono essere lanciati sia sul servizio SVS che sul servizio QSVS, che si differenziano per l'url della validazione che viene invocato.

Il test report è riassunto dall'immagine seguente:



	Steps						Scenarios			Features	
Feature	Passed	Failed	Skipped	Pending	Undefined	Total	Passed	Failed	Total	Duration	Status
FUN.7.0: Validate ASIC-E signed files	36	0	0	0	0	36	6	0	6	16.767	Passed
FUN.6.0: Validate ASIC-S signed files	36	0	0	0	0	36	6	0	6	13.731	Passed
FUN.9.0: Fail validation with bad requests	25	0	0	0	0	25	4	0	4	6.359	Passed
FUN.2.0: Validate CADES signed files	30	0	0	0	0	30	5	0	5	10.701	Passed
FUN.1.0: Validate ECDSA signed files by signature type	24	0	0	0	0	24	12	0	12	2:37.163	Passed
FUN.5.0: Validate JADES signed files	24	0	0	0	0	24	4	0	4	9.107	Passed
FUN.3.0: Validate PADES signed files	36	0	0	0	0	36	6	0	6	16.900	Passed
FUN.8.0: Fail validation when invalid document or certificate	18	0	0	0	0	18	3	0	3	5.757	Passed
FUN.10.0: Fail validation when there are constraints' violations	18	0	0	0	0	18	3	0	3	5.894	Passed
FUN.4.0: Validate XADES signed files	72	0	0	0	0	72	12	0	12	27.089	Passed
	319	0	0	0	0	319	61	0	61	4:29.471	10
	100.00%	0.00%	0.00%	0.00%	0.00%		100.00%	0.00%			100.00%

Figura 3 – Test Report

Le feature eseguite con successo sono evidenziate in verde, eventuali fallimenti sono evidenziati in rosso.

Cliccando su ciascuna feature, è possibile vedere anche il dettaglio dell'esecuzione di ciascuno scenario e ciascuno step:

tinexta infocert

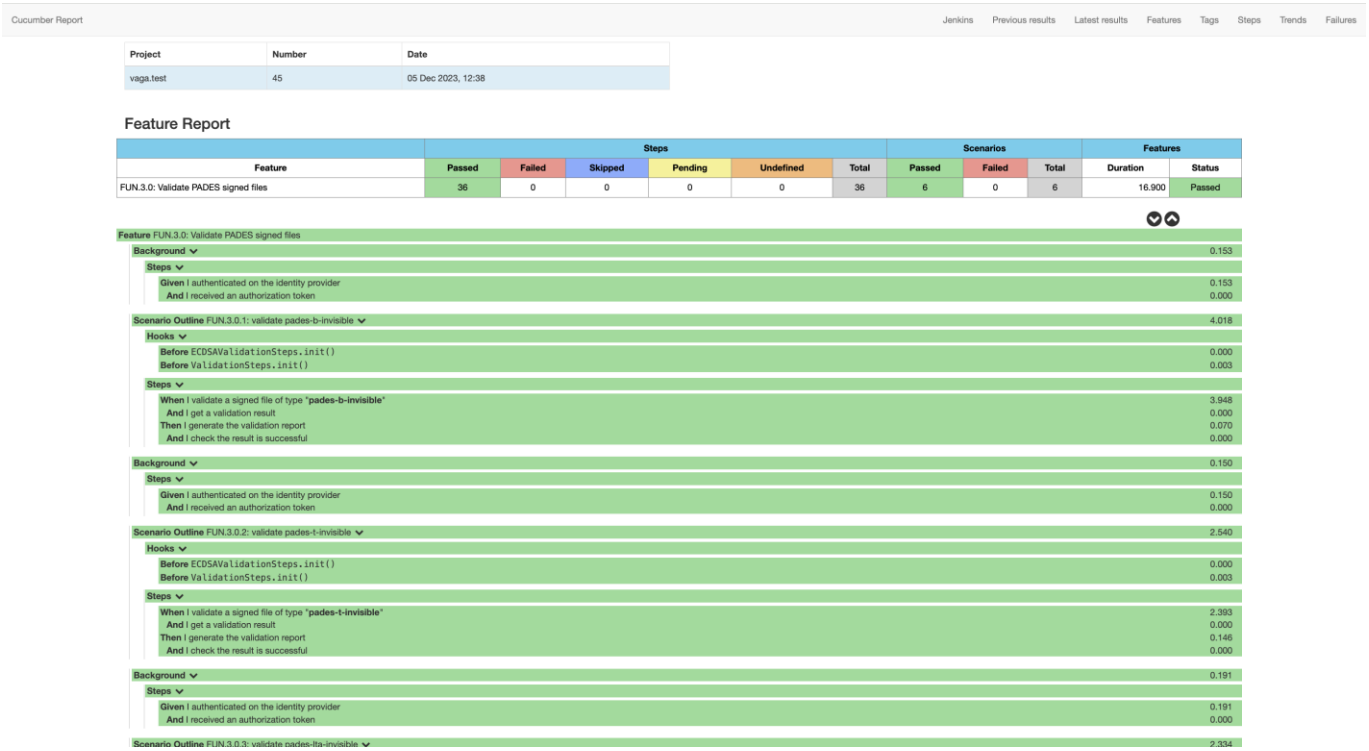


Figura 4 – Test Features

Oltre a questi report visivi, ciascuna esecuzione di scenario produce un PDF contenente la risposta JSON data dal SVS o QSVS e il relativo report ETSI XML per una consultazione di maggior dettaglio sui risultati dei test eseguiti.

I test sono automatizzati e lanciabili tramite lo strumento di Continuous Integration Jenkins su ciascun ambiente: test, collaudo e produzione. Prima di ogni nuovo rilascio di SVS e QSVS i test vengono lanciati in ambiente di collaudo e il rilascio in produzione viene eseguito solo se tutti i test terminano con successo.

I casi di test negativi sono utili a verificare il comportamento di SVS e QSVS in presenza di elementi obsoleti o revocati, oppure in presenza di algoritmi considerati non più validi (per una guida relativa agli algoritmi e alla loro validità si può fare riferimento a [6] [i.14]). In questi casi, la risposta complessiva di SVS e QSVS presenta status TOTAL_FAILED, mentre lo status delle firme risulta INDETERMINATE con i relativi dettagli nei messaggi di errore.

Il caso di test “expired-certificate” presenta due elementi obsoleti: il certificato di firma è scaduto e l’algoritmo di firma è RSA con chiavi di lunghezza a 1024 bit, non più considerato valido. La risposta JSON del QSVS presenta i seguenti messaggi di errore:

```
"messages": [
{
"level": "ERROR",
```

"section": "ADES",
"key": "BBB_XCV_SUB_ANS",
"value": "The certificate validation is not conclusive!"
},
{
"level": "ERROR",
"section": "ADES",
"key": "BBB_XCV_ICTIVRSC_ANS",
"value": "The current time is not in the validity range of the signer\u0027s certificate!"
},
{
"level": "ERROR",
"section": "ADES",
"key": "ASCCM_AR_ANS_AKSNR",
"value": "The algorithm RSA with key size 1024 is no longer considered reliable for signature creation!"
},
{
"level": "ERROR",
"section": "ADES",
"key": "TSV_IBSTBCEC_ANS",
"value": "The best-signature-time is not before the expiration date of the signing certificate!"
},
{
"level": "ERROR",
"section": "ADES",
"key": "PSV_IPSVC_ANS",
"value": "The past signature validation is not conclusive!"
},
{
"level": "WARNING",
"section": "ADES",
"key": "BBB_XCV_AIA_PRES_ANS",
"value": "The authority info access is not present!"
},
{
"level": "WARNING",
"section": "QUALIFICATION",
"key": "QUAL_IS_ADES_IND",
"value": "The signature/seal is an INDETERMINATE AdES digital signature!"
}
]

La risposta completa è consultabile nel report PDF ValidationResult-EXPIRED-CERTIFICATE.pdf, generato a fronte di un'esecuzione dei test automatici e contenente anche l'ETSI report XML.

Il caso di test “XCV violation revoked” presenta un elemento revocato: il certificato di firma. La risposta JSON del QSVS presenta i seguenti messaggi di errore:


```
"messages": [
{
"level": "ERROR",
"section": "ADES",
"key": "BBB_XCV_SUB_ANS",
"value": "The certificate validation is not conclusive!"
},
{
"level": "ERROR",
"section": "ADES",
"key": "BBB_XCV_ISCR_ANS",
"value": "The certificate is revoked!"
},
{
"level": "ERROR",
"section": "ADES",
"key": "ADEST_IRTPTBST_ANS",
"value": "The revocation time is not after best-signature-time!"
},
{
"level": "ERROR",
"section": "ADES",
"key": "PSV_IPSVC_ANS",
"value": "The past signature validation is not conclusive!"
},
{
"level": "WARNING",
"section": "ADES",
"key": "BBB_XCV_AIA_PRES_ANS",
"value": "The authority info access is not present!"
},
{
"level": "WARNING",
"section": "QUALIFICATION",
"key": "QUAL_IS_ADES_IND",
"value": "The signature/seal is an INDETERMINATE AdES digital signature!"
}
]
```


La risposta completa è consultabile nel report PDF ValidationResult-REVOKED.pdf, generato a fronte di un’esecuzione dei test automatici e contenente anche l’ETSI report XML.