Changelog

rifBelow the history of release version:

Description	Version	RPM version (default value: 1.0 if not specified)	Release date
• Added method signPadesMultiFieldName, allow to sign one or more signatures field using only one request	2.5.57		20 Nov 2023
• Improved healtcheck with information about memory used • Added flag "serial" on CadesPreferences allow to make a "matrioska" signature • Add method to extract info about signature field in a PDF	2.5.56	1.1	02 Oct 2023
• Added method verifyTimestamp with preferences • Fix on gui • Fix for signatures made by other libraries	2.5.55		04 May 2023
• Fix during set of default variable • Fix REST interface added JSON property on field xPathQuery • Added flag withoutPlainDocument on verify	2.5.54		16 Mar 2023
• Fix DSS method used to return the certificate chain without the root	2.5.53	1.3	23 Dec 2022
• Fix SDK param for REST Interface	2.5.53	1.2	06 Dec 2022
• Forced proxy credentials when a proxy is used	2.5.53	1.1	
• Fix Pades signature without page number on signature field • Fix flag scaled on signature Pades • Added flag scaledText on pades signature • Fix compliant on Pdf/UA	2.5.53		
• Fix idOtp on REST signPades	2.5.52	1.1	24 Oct 2022
• Added REST interface	2.5.52		06 Sep 2022
• Added SECTIGO root CA to truststore.jks file	2.5.51	1.1	02 Aug 2022
• Removed dependeny of log4j	2.5.51		01 Jul 2022
• Added information on suspended certificate on verify	2.5.50		
• Information Disclosure remedation	2.5.49		
Fixed security problem on GUI Padest template	2.5.48		
• Datadaog integration • Webpages with i18n in English support	2.5.47		
• Fixed appereance on rotate PDF	2.5.46		

• Add login on Amazon SWS appliance	2.5.45		
• Add feature for apply Adobe Timestamp on method "timestamp" • Add method getAvailableTimestamps • Added integration with datadog	2.5.44		
• Nel caso in cui la CA di un certificato di cui si sta verificando la firma abbia associato contemporaneamente un TSP di autenticazione e uno di firma, si procede prima ad analizzare i vincoli della FEQ e successivamente quelli della FEA	2.5.43		
• Ora i parametri del proxy vengono utilizzati anche per le richieste CRL e OCSP	2.5.42		
• Aggiunta la possibilità di specificare i parametri del proxy attraverso le variabili di sistema http.proxyHost, https.proxyHost, http.proxyPort, https.proxyPort • Aggiunta gestione di font esterni tramite il path assoluto	2.5.40		
• Risolto bug relativo al font della firma PAdES	2.5.38		
• Aggiunto parametro per l'adozione o meno nella firma XAdES delle regole tecniche contenute nell'ETSI EN319132	2.5.37		
• Aggiunti metodi timestamp e extendCAdEST nell'interfaccia REST • Aggiunto parametro per l'abilitazione del pulsante "Esporta log"	2.5.36		
• Rilassato il vincolo sulla presenza del QSCD per quei certificati che sono stati emessi da una CA tedesca prima dell'entrata in vigore di eIDAS • Modificata la gestione degli errori nell'interfaccia REST in modo da passare l'errorCode e l'errorMessage attraverso specifici header • Sistemato bug relativo alla firma PAdES dell'interfaccia REST per cui, in caso di errore, invece di sollevare un'eccezione veniva restituito un file vuoto • Migliorata la verifica dell'algoritmo di firma	2.5.34		
• Migliorata la gestione degli errori relativi al servizio di marcatura temporale quando si firma e marca • Aggiunto controllo sulla mancata corrispondenza tra il certificato del firmatario e la sezione IssuerAndSerial nella verifica della firma XAdES • Modificata la pagina help.xhtml in modo da poter essere utilizzata per recuperare i file di log e testare la connessione al servizio di firma • Aggiunti i metodi openSession e closeSession nell'interfaccia REST • ggiornati i certificati dei firmatari della TSL europea	2.5.33		
• Ora viene loggato il nome del metodo e i suoi parametri nel caso in cui la proprietà sws.debug.enabled sia true	2.5.32		
• Aggiunto metodo nell'interfaccia REST per la firma PAdES di grandi dimensioni • Aggiunto metodo nell'interfaccia REST per il listaggio degli OTP associati ad un utente • Aggiunto metodo nell'interfaccia REST per l'invio del codice OTP via SMS • Risolto bug che causava l'innalzamento della CPU a fronte della verifica di un particolare certificato • Aggiunta la verifica di firme apposte con certificati emessi da SubCA • Aggiunta la verifica di una catena di certificati • Rimossa vulnerabilità ad attacchi clickjacking • Aggiornamento a PrimeFaces 8	2.5.31		
• Aggiunti log per ogni chiamata • Sistemato il problema legato alla company negli SWS SaaS	2.5.30		

• Aggiunto metodo checkSecondFactor • Aggiunta firma XAdES detached	2.5.28		
• Migliorata la gestione delle credenziali di marcatura temporale quando si appone una firma LT/LTA: ora si possono utilizzare anche le credenziali passate in input	2.5.24		
• Modificato il comportamento della firma LTV: ora non vengono più estese le firme preesistenti	2.5.23		
• Corretto bug relativo alla verifica alla data	2.5.22		
• Migliorata la sicurezza per l'apertura della pagina delle impostazioni generali • Migliorato il login • Aggiunto il pulsante per il test della connessione all'interno della pagina delle impostazioni generali • Ora nell'archivio dei log viene inserito un file contenente i principali pacchetti installati	2.5.21		
• Corretta la gestione multilingua degli errori • Aggiunta checkbox per rendere invisibile l'immagine di sfondo della signatureAppearance • Aggiunta sezione per specificare un campo firma da firmare	2.5.19		
• Corretto bug relativo alla creazione di una signatureAppearance con testo su più linee	2.5.18		
• Customizzazione della classe ResolverDirectHTTP di Santuario per poter gestire il redirect da http a https di una risorsa esterna	2.5.17		
• Declassato a warning il controllo sul formato del signingTime	2.5.16		
• Corretta eccezione durante la verifica di un documento firmato che non presenta SignedAttributes	2.5.15		
• Aggiunto controllo per la verifica dei certificati senza SSCD emessi da CA tedesca prima del 30 luglio 2017 • Corretto bug che mandava in errore la firma PAdES se precedentemente veniva eseguita una verifica	2.5.14		
• Corretto bug che si presenta quando si setta a false il campo textVisible della classe SignerImage	2.5.13		
• Aggiunto controllo sull'effettiva apposizione delle firme LT, LTA e LTV • Aggiunta la verifica di firme detached • Aggiunta la verifica di firme fatte con algoritmo PLAIN-ECDSA	2.5.12		
• Aggiunto metodo per la gestione multilingua degli errori • Aggiunto il campo "level" nelle preferenze di firma in modo da ottenere firme LT, LTA e LTV oltre a B e T • Aggiunta nel tab "Impostazioni generali" della pagina "Impostazioni" la sezione per specificare l'account di marcatura temporale da utilizzare nella firma LT o LTA • Aggiunti nei metodi di firma i log per i conteggi di Kibana	2.5.11		
• Forzato il signatureName della firma PAdES con il commonName del certificato del firmatario • Ora la signature appearance risulta uguale a quella prodotta con sws1.3	2.5.10		
1. Gestione multipla del client SOAP in base al campo CCAName della classe Engine 2. Settato il nuovo campo CCAName della classe Engine al valore del subjectDN estratto dal certificato utilizzato in caso di strong authentication	2.5.9		

• Reintrodotti vecchi campi nelle preferenze di firma per retrocompatibilità • Correzione relativa alla verifica del byterange	2.5.7		
• Customizzazione del framework DSS in modo da consentire l'utilizzo della trasformata xmldsig-filter2 • Customizzazione del framework DSS in modo da aggiungere il KeyInfo alle reference da firmare	2.5.6		
• Aggiunto parametro nelle XAdESPreferences per evitare la trasformata XPath che esclude le altre firme dal computo dell'hash • Aggiunto un messaggio di warning nel caso in cui una firma PAdES contenga il signingTime	2.5.5		
• Aggiunto webmethod per il controllo della connessione al servizio web di Namirial • Aggiunta la disattivazione del job per l'aggiornamento della TSL • Corretta la visualizzazione dell'environment nel caso in cui si sia impostato il dominio sehp.firmacerta.it o sehp.namirialtsp.com	2.5.4		
• Aggiunto webmethod per rimuovere un certificato dalla cache • Aggiornato primefaces alla versione 6.2 in modo da evitare attacchi XSS • Aggiunta il parametro XPathQuery alle XAdESPreferences in modo da firmare solo una porzione di XML identificata dalla query XPath • Aggiunto il controllo del byterange anche sulla prima revisione del documento PDF • Aggiunta la trasformata enveloped-signature alla firma XAdES • Corretto il digest algorithm utilizzato per il calcolo dell'impronta del certificato sulla firma XAdES • Gestito il caso in cui viene verificata una firma CAdES con il campo SigningTime non codificato in UTCTime	2.5.3		
• Aggiunto metodo per il reset della cache dei certificati • Risolto bug di sicurezza relativo al ViewState	2.5.2		
• Aggiunta cache dei certificati	2.5.1		
• Sostituito il campo SignerPosition della classe SignerImage con TextPosition	2.5.0-1.2		
• Primo rilascio della nuova versione di SWS	2.5.0-1.1		