DECISIONE DI ESECUZIONE (UE) 2022/2519 DELLA COMMISSIONE

del 20 dicembre 2022

sulle specifiche tecniche e sugli standard tecnici per il sistema e-CODEX, anche per la sicurezza e i metodi di verifica dell'integrità e dell'autenticità

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2022/850 del Parlamento europeo e del Consiglio, del 30 maggio 2022, relativo a un sistema informatizzato per lo scambio elettronico transfrontaliero di dati nel settore della cooperazione giudiziaria in materia civile e penale (sistema e-CODEX) e che modifica il regolamento (UE) 2018/1726 ([1]), in particolare l'articolo 6, paragrafo 1, lettera a),

considerando quanto segue:

(1) A norma dell'articolo 5 del regolamento (UE) 2022/850, il sistema e-CODEX si compone di un punto di accesso e-CODEX, di standard procedurali digitali e dei software, della documentazione e delle altre risorse di supporto elencati nell'allegato di tale regolamento.

(2) Il punto di accesso e-CODEX si compone di un gateway costituito da un software, basato su una serie comune di protocolli, che consente lo scambio sicuro di informazioni attraverso una rete di telecomunicazioni con altri gateway che utilizzano la stessa serie comune di protocolli e di un connettore che consente di collegare i sistemi connessi al gateway, costituito da un software, basato su una serie comune di protocolli aperti.

(3) Per il buon esito della procedura del passaggio e della presa di consegne del sistema e-CODEX a eu-LISA nonché per consentire lo svolgimento dei compiti che incombono a eu-LISA, è opportuno stabilire le specifiche tecniche minime e gli standard tecnici minimi, anche per la sicurezza e i metodi di verifica dell'integrità e dell'autenticità, su cui si basano le componenti del sistema e-CODEX.

(4) A norma degli articoli 1 e 2 del protocollo n. 22 sulla posizione della Danimarca, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, la Danimarca non ha partecipato all'adozione del regolamento (UE) 2022/850 e pertanto non è vincolata né soggetta all'applicazione della presente decisione.

(5) A norma degli articoli 1 e 2 nonché dell'articolo 4 *bis*, paragrafo 1, del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, e fatto salvo l'articolo 4 di tale protocollo, l'Irlanda non ha partecipato all'adozione del regolamento (UE) 2022/850 e pertanto non è vincolata né soggetta all'applicazione della presente decisione.

(6) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([2]), il garante europeo della protezione dei dati è stato consultato e ha espresso un parere il 24 novembre 2022.

(7) Le misure di cui alla presente decisione sono conformi al parere del comitato istituito dall'articolo 19, paragrafo 1, del regolamento (UE) 2022/850,

([1]) GU L 150 dell'1.6.2022, pag. 1.

([2]) Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39).

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Le specifiche tecniche minime e gli standard tecnici minimi, anche per la sicurezza e i metodi di verifica dell'integrità e dell'autenticità, su cui si basano le componenti del sistema e-CODEX di cui all'articolo 5 del regolamento (UE) 2022/850 figurano nell'allegato della presente decisione.

Articolo 2

La presente decisione entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Fatto a Bruxelles, il 20 dicembre 2022

Per la Commissione
La presidente
Ursula VON DER LEYEN

ALLEGATO

Specifiche tecniche e standard tecnici per il sistema e-CODEX, anche per la sicurezza e i metodi di verifica dell'integrità e dell'autenticità

1. **INTRODUZIONE**

Il presente allegato stabilisce le specifiche tecniche minime e gli standard tecnici minimi per le componenti del sistema e-CODEX, anche per la sicurezza e i metodi di verifica dell'integrità e dell'autenticità.

2. **COMPONENTI DEL SISTEMA e-CODEX**

2.1. A norma dell'articolo 5 del regolamento (UE) 2022/850 del Parlamento europeo e del Consiglio ([1]), il sistema e-CODEX si compone:

a) di un punto di accesso e-CODEX, composto:

i) di un gateway;

ii) di un connettore.

b) di standard procedurali digitali;

c) dei software, della documentazione e delle altre risorse di supporto elencati nell'allegato del regolamento (UE) 2022/850:

i) il codice sorgente della piattaforma centrale di prova;

ii) il codice sorgente dello strumento di gestione della configurazione;

iii) lo strumento «Metadata Workbench»;

iv) il vocabolario di base dell'UE della giustizia elettronica;

v) la documentazione dell'architettura.

2.2. Da un punto di vista funzionale, tali elementi sono suddivisi in due categorie: il pacchetto di strumenti di e-CODEX e le risorse utilizzabili di e-CODEX.

2.3. **Il pacchetto di strumenti di e-CODEX si compone:**

a) della documentazione dell'architettura di e-CODEX;

b) del codice sorgente della suite del connettore;

c) del codice sorgente dello strumento di gestione della configurazione;

d) del codice sorgente della piattaforma centrale di prova;

e) di una licenza Metadata Workbench rilasciata da terzi;

f) del vocabolario di base dell'UE della giustizia elettronica;

g) di standard procedurali digitali.

a) Documentazione dell'architettura di e-CODEX

La documentazione dell'architettura è una serie di documenti a cui si ricorre per fornire ai portatori di interessi conoscenze tecniche e informative sulla scelta degli standard ai quali devono essere conformi altre risorse del sistema e-CODEX. Definisce i requisiti e i principi che si applicano nella creazione di comunicazioni transfrontaliere interoperabili al fine di facilitare lo scambio elettronico di dati, che comprende qualsiasi contenuto trasmissibile per via elettronica. Elenca inoltre le metodologie e gli standard scelti su cui si basa il sistema e-CODEX. L'architettura garantisce l'autonomia del sistema e-CODEX.

b) Codice sorgente della suite del connettore

Il codice sorgente della suite del connettore è utilizzato per creare gli elementi utilizzabili descritti nel capitolo 2.4.2.

([1]) Regolamento (UE) 2022/850 del Parlamento europeo e del Consiglio, del 30 maggio 2022, relativo a un sistema informatizzato per lo scambio elettronico transfrontaliero di dati nel settore della cooperazione giudiziaria in materia civile e penale (sistema e-CODEX) e che modifica il regolamento (UE) 2018/1726 (GU L 150 dell'1.6.2022, pag. 1).

c) Strumento di gestione della configurazione

Lo strumento di gestione della configurazione è uno strumento basato sul web per la gestione dei file di configurazione associati al gateway di e-Delivery e al connettore e fornisce una modalità standardizzata per gestire il flusso di lavoro di configurazione. L'entità che gestisce il punto di accesso e-CODEX autorizzato può accedere allo strumento di gestione della configurazione tramite un portale disponibile a livello globale e caricare i propri dati di configurazione di e-Delivery. I dati caricati devono includere le informazioni sulla configurazione del punto terminale di rete del gateway, tutti i certificati di sicurezza necessari per la connessione, nonché i progetti, gli ambienti e i casi d'uso specifici a cui partecipa. Lo strumento di gestione della configurazione verifica automaticamente la validità dei dati caricati e, in caso di errori, fornisce un riscontro all'entità che gestisce i punti di accesso e-CODEX autorizzati.

Nel caso venga notificata una qualunque modifica dei dati forniti da un'entità che gestisce un punto di accesso e-CODEX autorizzato, deve essere generato un nuovo pacchetto di configurazione di e-CODEX (cfr. punto 2.4.3.) utilizzando tale strumento. Tutte le entità che gestiscono punti di accesso e-CODEX autorizzati devono essere informate della creazione del nuovo pacchetto di configurazione e-CODEX e possono scaricarlo direttamente dallo strumento di gestione della configurazione in qualsiasi momento. Lo strumento di gestione della configurazione può fornire pacchetti di configurazione e-CODEX per diversi ambienti informatici, in particolare TEST, CCEPTANCE o PRODUCTION.

I nuovi pacchetti di configurazione e-CODEX devono entrare in vigore sette giorni dopo la loro creazione e, se del caso, le entità che gestiscono i punti di accesso e-CODEX autorizzati devono installare il nuovo pacchetto nel proprio ambiente entro tale termine.

Lo strumento di gestione della configurazione tiene inoltre aggiornata l'entità che gestisce i punti di accesso e-CODEX autorizzati in merito ai tempi di esecuzione dei certificati di sicurezza e notifica in anticipo, tramite posta elettronica, i punti di accesso e-CODEX autorizzati in merito all'imminente scadenza dei certificati. Qualora un'entità che gestisce un punto di accesso e-CODEX autorizzato lasciasse scadere i propri certificati di sicurezza, tali certificati devono essere automaticamente rimossi all'atto della creazione del pacchetto successivo.

Lo strumento di gestione della configurazione deve essere ospitato a livello centrale ed essere disponibile 24 ore su 24, 7 giorni su 7, per i partecipanti a e-CODEX. Il servizio di assistenza deve essere disponibile unicamente durante l'orario di lavoro.

d) Piattaforma centrale di prova

La piattaforma centrale di prova di e-CODEX è un'infrastruttura di prova automatizzata. Consente all'entità che gestisce un punto di accesso e-CODEX autorizzato di effettuare prove di connettività e prove end-to-end tra la sua infrastruttura e-CODEX e un punto di prova centrale fisso, senza che sia necessario coinvolgere un altro partner (ad esempio un altro punto di accesso e-CODEX autorizzato) per testare le funzionalità di comunicazione. Consente di inviare e ricevere messaggi di prova personalizzabili, riducendo così lo sforzo necessario per testare un'infrastruttura e-CODEX sia al momento iniziale (installazione) che al momento della prova di regressione. Lo stato di avanzamento dei messaggi individuali, i registri di prova e di errori relativi alla posta elettronica registrata (REM) dell'Istituto europeo delle norme di telecomunicazione (ETSI) sono tracciati e presentati alle entità che gestiscono i punti di accesso e-CODEX autorizzati attraverso processi visivi appositamente progettati.

La piattaforma centrale di prova consiste in un gateway e-CODEX, in un connettore, un connettore-client e un'interfaccia grafica utente web associata (attualmente un'interfaccia web front-end e back-end basata su Nuxt.js) che possono essere utilizzati per inviare messaggi al gateway di un partner e per visualizzare i messaggi inviati alla piattaforma centrale di prova dallo stesso gateway. Attualmente la piattaforma centrale di prova memorizza importanti informazioni operative (variabili locali) su un'istanza MongoDB e legge le informazioni di configurazione (parte) dalla banca dati del connettore. Inoltre, utilizza l'interfaccia per programmi applicativi (API) del trasferimento di stato rappresentativo (REST) connettore-client per estrarre informazioni sui messaggi e-CODEX e inviare nuovi messaggi al connettore e al gateway.

Per fornire una soluzione personalizzabile per ciascun ambiente di e-CODEX, la piattaforma centrale di prova è utilizzata in varie istanze (copie) presenti in vari ambienti di e-CODEX. Ciascuna istanza della piattaforma centrale di prova è attualmente utilizzata in un ambiente UNIX (CentOS 7), in cui tutti i componenti coesistono. Ciò facilita la gestione e l'accesso al sistema di file, permettendo al contempo di apportare modifiche per tenere conto degli impianti in cui l'infrastruttura di messaggistica e-CODEX è tenuta separata.

Ogni utente della piattaforma centrale di prova è collegato a un (1) gateway. Per utilizzare la piattaforma centrale di prova per effettuare test, l'unico requisito è che il gateway di tale punto di accesso e-CODEX autorizzato esista nei P-modes per tale ambiente specifico dello strumento di gestione della configurazione di e-CODEX.

e) Metadata Workbench

Il Metadata Workbench è uno strumento di gestione del vocabolario di base dell'UE della giustizia elettronica. Consente ai modellatori semantici di mantenere il vocabolario in modo sostenibile rispettando la norma di modellizzazione delle specifiche tecniche delle componenti di base quali definite nella documentazione dell'architettura e-CODEX. Si tratta di una soluzione di servizio a livello di software (SaaS) basata sul web con accesso limitato ai soli amministratori del vocabolario di base dell'UE della giustizia elettronica. Il Metadata Workbench è sviluppato e gestito per conto del ministero della Giustizia e della sicurezza dei Paesi Bassi. Sulla base di un accordo di licenza da concludersi tra il ministero della Giustizia e della sicurezza ed eu-LISA, quest'ultima avrà accesso al Metadata Workbench per amministrare e gestire il vocabolario di base dell'UE della giustizia elettronica.

f) Vocabolario di base dell'UE della giustizia elettronica

Il vocabolario di base dell'UE della giustizia elettronica costituisce una risorsa per termini e definizioni semantici riutilizzabili a cui si ricorre per garantire la coerenza e la qualità dei dati nel tempo e in tutti i casi d'uso. Tutte le strutture di messaggi specifiche per i casi d'uso (schemi XML) si basano sul suo archivio semantico.

Le evoluzioni future del vocabolario di base della giustizia elettronica potrebbero avvenire nel rispetto dei vocabolari di base ([2]). Al fine di convalidare la conformità alle specifiche, potrebbe essere istituito un validatore basato su XML utilizzando il banco di prova dell'interoperabilità offerto dalla Commissione.

g) Standard procedurali digitali

Per standard procedurale digitale si intendono le specifiche tecniche per i modelli di processo operativo e per i modelli preesistenti di dati che definiscono la struttura elettronica dei dati scambiati attraverso il sistema e-CODEX sulla base del vocabolario di base dell'UE della giustizia elettronica. Il modello di processo operativo descrive l'attuazione tecnica della procedura elettronica dello strumento giuridico supportata dal sistema e-CODEX.

Il modello di processo operativo, insieme al vocabolario di base dell'UE della giustizia elettronica, si traduce in schemi XML che descrivono la struttura elettronica degli standard procedurali digitali. Gli schemi XML consentono ai punti di accesso autorizzati di inviare e ricevere documenti come previsto da uno strumento di cooperazione giudiziaria transfrontaliera.

2.4. Risorse e-CODEX che possono essere utilizzate

Le risorse e-CODEX che possono essere utilizzate sono componenti di e-CODEX utilizzate dalle entità che gestiscono un punto di accesso e-CODEX autorizzato nel loro ambiente e-CODEX. Ad eccezione del gateway, devono essere distribuite da eu-LISA alle entità che gestiscono un punto di accesso e-CODEX autorizzato.

Le risorse utilizzabili sono le seguenti:

a) il gateway (punto 2.4.1);

b) la suite del connettore (punto 2.4.2);

c) il pacchetto di configurazione e-CODEX (comprese le P-mode, i certificati pubblici e le impostazioni di sicurezza) (punto 2.4.3);

d) la struttura della collaborazione operativa o il modello di processo nell'ambito degli standard procedurali digitali;

e) gli schemi XML, che sono strutture di messaggi che fanno parte degli standard procedurali digitali.

2.4.1. *Il gateway*

Nell'ambito del sistema e-CODEX il gateway è l'elemento costitutivo responsabile dello scambio di comunicazioni di base. Attualmente un gateway prevede l'attuazione dei seguenti standard:

a) standard OASIS ([3]) ebMS 3.0: messaggi di interscambio tra gateway conformi allo standard ebXML; tale standard definisce la struttura che deve avere l'intestazione di un messaggio affinché sia intelligibile nell'ambito dell'infrastruttura e-CODEX;

b) profilo di messaggistica della dichiarazione di applicabilità OASIS 4 (AS4): si tratta di un profilo di conformità della specifica OASIS ebMS 3.0;

([2]) https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/core-vocabularies
([3]) Organizzazione per la promozione delle norme sulle informazioni strutturate.

c) il profilo comune del profilo AS4 di eDelivery ([4]).

È possibile utilizzare qualsiasi soluzione di gateway che soddisfi tali requisiti.

2.4.2. ***Suite del connettore***

Il connettore è una componente che collega le applicazioni specifiche degli standard procedurali digitali agli standard generici di messaggistica del gateway. Pertanto, questa componente aggiunge le seguenti caratteristiche alle comunicazioni di base già stabilite dalla componente gateway:

a) **prove ETSI-REM:** si tratta di prove generate dal connettore in un formato XML firmato; lo scopo di tali prove è di informare il mittente di un messaggio in merito al trattamento del messaggio, andato a buon fine o meno; le prove sono generate e presentate dal connettore in diverse fasi del trattamento dei messaggi;

b) **token TrustOK**: il connettore mittente convalida l'integrità e l'autenticazione del documento operativo nel messaggio; l'esito di detta convalida è scritto nel dispositivo di autenticazione (token) TrustOK; tale token è generato da un sottomodulo del connettore: la biblioteca di sicurezza;

c) **contenitore ASiC-S:** conformemente alla norma ETSI EN 319 162-1 relativa alle firme e infrastrutture elettroniche nonché ai contenitori di firme associate («Associated Signature Container», ASiC); il contenitore garantisce l'autenticità e l'integrità del carico trasmesso dal connettore;

d) **WS-Security**: per aumentare la sicurezza della trasmissione dei messaggi, il connettore utilizza, per la trasmissione, ws-security sul lato del gateway, nonché la parte del sistema connesso; ciò significa che ogni messaggio trasmesso o ricevuto dal connettore è criptato e firmato;

e) **API comune**: il connettore offre un'API stabile che definisce i servizi web utilizzati per connettersi al gateway e alle applicazioni dei sistemi connessi; la struttura dei messaggi scambiati con il connettore è descritta anche nell'API del connettore.

Oltre al software del connettore stesso, la suite contiene anche un'applicazione client destinata a supportare o sostituire un sistema connesso per la gestione della messaggistica e-CODEX.

È stato inoltre sviluppato un plugin appositamente per il gateway Domibus ([5]) per collegare l'API comune del connettore alla memoria di elaborazione del gateway.

2.4.3. ***Pacchetto di configurazione e-CODEX***

Nella comunicazione basata su ebMS 3.0, una P-Mode (o modalità di elaborazione) disciplina la trasmissione di tutti i messaggi coinvolti in uno scambio di messaggi tra due gestori di servizi di messaggistica. Un pacchetto di configurazione e-CODEX comprende una raccolta di parametri di configurazione della messaggistica (file P-Mode, vari archivi di attendibilità dei certificati, indirizzi di rete) che precisano in modo dettagliato le modalità di trasmissione dei messaggi.

I parametri di configurazione della messaggistica possono essere classificati nelle cinque categorie seguenti:

a) parametri relativi al mittente, quali:

   i) l'identificativo del mittente;

   ii) il certificato utilizzato dal mittente per firmare i messaggi;

   iii) le autorità di certificazione di fiducia del mittente;

   iv) l'indirizzo o gli indirizzi di rete da cui il mittente avvierà la comunicazione;

b) parametri relativi al destinatario, quali:

   i) l'identificativo del destinatario;

   ii) il certificato che il destinatario prevede sia utilizzato per criptare messaggi;

   iii) le autorità di certificazione di fiducia del destinatario;

([4]) https://ec.europa.eu/digital-building-blocks/wikis/x/RqbXGw

([5]) Il gateway Domibus è gestito dalla Commissione (https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Domibus).

iv) l'indirizzo o gli indirizzi di rete da cui il destinatario accetterà le comunicazioni in entrata;

c) parametri relativi alla coppia mittente-destinatario, quali (se applicabile):

i) identificativo della convenzione, identificativo della P-Mode;

d) parametri relativi agli standard procedurali digitali, quali:

i) ruolo/i del mittente;

ii) ruolo/i del destinatario;

iii) servizio o servizi;

iv) azione/i all'interno del servizio;

e) parametri relativi all'uso del protocollo di messaggistica o del profilo del protocollo di messaggistica.

In e-CODEX tutti i file di configurazione relativi a un gestore di servizi di messaggistica o a un dominio sono raggruppati in un unico file principale che può essere utilizzato per la configurazione del gateway e del connettore.

Il file principale definisce una rete di comunicazioni individuali che il gestore di servizi di messaggistica può gestire durante la sua attività. È necessario che la configurazione sia generata a livello centrale perché tutte le informazioni di tutti i punti di accesso e-CODEX autorizzati devono essere disponibili per la generazione del pacchetto di configurazione e-CODEX, che è creato dallo strumento di gestione della configurazione.

3. SICUREZZA E METODI DI VERIFICA DELL'INTEGRITÀ E DELL'AUTENTICITÀ DEL SISTEMA E-CODEX

Il sistema e-CODEX è un sistema di comunicazione che fornisce un sostegno importante per rispondere ai requisiti in materia di sicurezza e di protezione dei dati. In particolare, il sistema e-CODEX fornisce le caratteristiche tecniche necessarie per soddisfare tutti i requisiti di cui al regolamento (UE) 910/2014 del Parlamento europeo e del Consiglio ([6]).

3.1. Sicurezza fin dalla progettazione

Da un punto di vista tecnico, il sistema e-CODEX è un meccanismo di trasporto. Vi sono diversi livelli pertinenti in materia di sicurezza:

a) un livello di rete;

b) un livello di trasporto;

c) un livello dei messaggi;

d) un livello dei documenti.

A ciascuno di tali livelli si applicano misure di sicurezza.

3.1.1. *Livello di rete*

e-CODEX può essere utilizzato con diversi tipi di livelli di rete. Generalmente è applicato su connessioni Internet ordinarie. La sicurezza è quindi conforme alle applicazioni di sicurezza ordinarie della tecnologia Internet (ed è rafforzata dagli altri livelli descritti nel presente punto). Per la maggior parte dei casi di uso di e-CODEX, tale livello di rete è sufficiente. Per requisiti di sicurezza più elevati potrebbe essere applicato anche un altro livello di rete. Possono essere prese in considerazione anche altre reti.

3.1.2. *Livello di trasporto*

Il livello di trasporto è generalmente protetto da TLS (Transport Layer Security) o mTLS (mutual TLS). Si tratta di uno standard consolidato per la protezione del livello di trasporto nelle tecnologie Internet e utilizzato in tutto il mondo per numerosi servizi. Lo standard TLS/mTLS prevede la cifratura e l'autenticazione sul canale di trasporto. Garantisce il percorso di trasporto tra ciascun polo del percorso di trasporto. Ciascun polo deve decriptare (unicamente) i dati relativi all'indirizzo per inoltrare il messaggio al polo successivo. Prima dell'invio, ciascun polo cripta nuovamente i dati relativi all'indirizzo. Il TLS semplice (a senso unico) è possibile e talvolta ancora utilizzato, ma si raccomanda di utilizzare il TLS a doppio senso (mTLS) in quanto sta diventando lo standard attuale di protezione del livello di trasporto.

([6]) 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 nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28.8.2014, pag. 73).

3.1.3. ***Livello dei messaggi***

Al livello dei messaggi, diverse componenti di e-CODEX applicano standard diversi:

a) Il protocollo utilizzato per la trasmissione da gateway a gateway (come livello dei messaggi) è il protocollo AS4, che firma e cripta i messaggi in funzione della configurazione di sicurezza a livello di gateway;

b) La componente di base del sistema e-CODEX è il connettore. Aumenta la sicurezza al livello dei messaggi utilizzando WS-Security per la firma e la cifratura dei messaggi per i servizi web verso il gateway e il/i back-end. Pertanto, viene applicata anche una cifratura da connettore a connettore;

c) Per le funzionalità di firma e cifratura in tutti i sistemi e-CODEX sono utilizzati certificati digitali. Tali certificati digitali di cifratura e firma sono conformi allo standard X.509.

3.1.4. ***Livello dei documenti***

I messaggi contengono documenti e allegati. Tali elementi sono raggruppati in un pacchetto denominato «contenitore». Il contenitore è creato secondo lo standard AsiC-S. Il connettore mittente firma il contenitore ASiC-S e la firma è convalidata al ricevimento da parte del connettore ricevente.

3.2. **Metodi di verifica dell'integrità e dell'autenticità**

3.2.1. ***Accesso alla configurazione e-CODEX***

La comunicazione tra i punti di accesso e-CODEX richiede una configurazione preliminare. Tale configurazione è effettuata tramite il pacchetto di configurazione e-CODEX. Il pacchetto di configurazione contiene i dati relativi agli indirizzi, la politica di sicurezza applicata e altre informazioni. Contiene inoltre gli archivi di attendibilità con i certificati pubblici di tutti i punti di accesso e-CODEX partecipanti. I file di configurazione sono creati per la configurazione di ciascun partner da parte di un «coordinatore centrale per la configurazione» utilizzando lo strumento di gestione della configurazione. L'accesso a tale strumento di gestione della configurazione è limitato ai partner ed è fornito a ciascun partner solo su richiesta personale e individuale. L'accesso amministrativo è limitato ai coordinatori per la configurazione e deve essere gestito da eu-LISA.

3.2.2. ***Firme e sigilli elettronici supportati***

Il sistema e-CODEX deve supportare tutti i tipi di sigilli elettronici e di firme elettroniche previsti dal regolamento (UE) 910/2014.

3.2.3. ***Token TrustOK di e-CODEX***

Il connettore mittente convalida la firma degli standard procedurali digitali di un messaggio. L'esito di detta convalida è scritto nel token TrustOK di e-CODEX. Il token è generato da una biblioteca di sicurezza che è un sottomodulo del connettore. La firma elettronica è convalidata dal connettore di e-CODEX utilizzando gli strumenti del servizio di firma digitale.

3.2.4. ***Token leggibile mediante dispositivo automatico (XML)***

Il token leggibile mediante dispositivo automatico è un file XML alla base di un determinato schema contenente tutte le informazioni relative alla firma del token operativo e la relazione di convalida a seguito della convalida giuridica e tecnica.

3.2.5. ***Token leggibile dall'uomo (PDF)***

Il file PDF si compone di tre parti. La prima parte presentata sulla prima pagina del token propriamente detto contiene informazioni generali sul sistema elettronico avanzato e una valutazione della validità giuridica del documento operativo. In calce alla pagina sono inoltre presenti una clausola di esonero della responsabilità e un «timbro di convalida» indicante l'esito della convalida giuridica (esito positivo/negativo).

Un sistema elettronico avanzato è un sistema connesso in grado di identificare in modo sicuro l'utente e garantire l'integrità dei messaggi inviati attraverso di esso tra il client e il connettore di e-CODEX.

La seconda parte della seconda pagina fornisce una panoramica tecnica standardizzata delle informazioni contenute nella relazione di convalida originale. Le informazioni fornite dalla panoramica tecnica variano a seconda del sistema connesso (basato sull'autenticazione o sulla firma). Un token basato sulla firma contiene le informazioni fornite dal certificato alla base, compresi gli attributi (se disponibili). Un token basato sull'autenticazione contiene il nome dell'istituzione da cui è stato inviato il documento e, se fornito, il nome dell'autore del documento.

La parte inferiore della pagina è costituita da un timbro nel colore dell'esito della convalida tecnica dei documenti (verde/giallo/rosso) e da una breve descrizione, ad esempio fornisce ulteriori informazioni sul motivo per cui un documento ha ricevuto una valutazione tecnica gialla.

La terza parte del documento è costituita dalla relazione di convalida originale così come è stata creata dal software di convalida dello Stato membro di rilascio.

4. STANDARD PROCEDURALI DIGITALI AD OGGI ELABORATI

Servizio e-Justice	Standard procedurali digitali: modello di processo	Standard procedurali digitali: schema XML	Origine del progetto
Ingiunzione di pagamento europea	√	√	e-CODEX
Controversie di modesta entità	√	√	e-CODEX
Mandato di arresto europeo	√	√	e-CODEX
Sanzioni pecuniarie	√	√	e-CODEX
AGR	√	√	e-CODEX
FD 909 (Pene detentive)	√	√	e-CODEX
Questioni in materia matrimoniale	√	√	e-SENS
Ordinanza europea di sequestro conservativo su conti bancari	√	√	e-SENS
Registro dei testamenti	√	√	e-SENS
Notificazione e comunicazione degli atti	√	√	e-CODEX