2025/1929

30.9.2025

REGOLAMENTO DI ESECUZIONE (UE) 2025/1929 DELLA COMMISSIONE

del 29 settembre 2025

recante modalità di applicazione del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio per quanto riguarda il collegamento della data e dell'ora ai dati e la determinazione dell'accuratezza delle fonti di misurazione del tempo per la validazione temporale elettronica qualificata

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il 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 ([1]), in particolare l'articolo 42, paragrafo 2,

considerando quanto segue:

(1) Le validazioni temporali elettroniche qualificate svolgono un ruolo cruciale nell'ambiente digitale, promuovendo la transizione dai processi cartacei tradizionali ai loro equivalenti elettronici. Collegando le informazioni su data e ora ai dati elettronici, le validazioni temporali elettroniche qualificate contribuiscono a garantire l'accuratezza della data e dell'ora da essi indicate e l'integrità dei documenti digitali ai quali sono vincolate la data e l'ora.

(2) La presunzione di conformità di cui all'articolo 42, paragrafo 1 *bis*, del regolamento (UE) n. 910/2014 dovrebbe applicarsi solo se i servizi fiduciari qualificati per il rilascio di validazioni temporali qualificate sono conformi alle norme stabilite nel presente regolamento. Tali norme dovrebbero rispecchiare le prassi consolidate ed essere ampiamente riconosciute nei settori pertinenti. Esse dovrebbero essere adattate in modo da includere controlli supplementari che garantiscano la sicurezza e l'affidabilità dei servizi fiduciari qualificati e del collegamento della data e dell'ora ai dati e l'accuratezza delle fonti di misurazione del tempo.

(3) Se un prestatore di servizi fiduciari rispetta i requisiti di cui all'allegato del presente regolamento, gli organismi di vigilanza dovrebbero presumere la conformità ai pertinenti requisiti del regolamento (UE) n. 910/2014 e tenere debitamente conto di tale presunzione per la concessione o la conferma della qualifica del servizio fiduciario. Un prestatore di servizi fiduciari qualificato può comunque fare affidamento su altre pratiche per dimostrare la conformità ai requisiti del regolamento (UE) n. 910/2014.

(4) La Commissione valuta periodicamente le nuove tecnologie, pratiche, norme o specifiche tecniche. Conformemente al considerando 75 del regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio ([2]), la Commissione dovrebbe riesaminare e, se necessario, aggiornare il presente regolamento di esecuzione per mantenerlo in linea con gli sviluppi globali e le nuove tecnologie, norme o specifiche tecniche e per seguire le migliori pratiche nel mercato interno.

(5) Il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([3]) e, se del caso, la direttiva 2002/58/CE del Parlamento europeo e del Consiglio ([4]) si applicano alle attività di trattamento di dati personali a norma del presente regolamento.

([1]) GU L 257 del 28.8.2014, pag. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale (GU L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([3]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([4]) Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj.

(6) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([5]), il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 6 giugno 2025.

(7) Le misure di cui al presente regolamento sono conformi al parere del comitato istituito dall'articolo 48 del regolamento (UE) n. 910/2014,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Le norme di riferimento e le specifiche di cui all'articolo 42, paragrafo 2,del regolamento (UE) n. 910/2014 figurano nell'allegato del presente regolamento.

Articolo 2

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

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 29 settembre 2025

Per la Commissione
La presidente
Ursula VON DER LEYEN

([5]) 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

ALLEGATO

Elenco delle norme di riferimento e delle specifiche per i servizi di validazione temporale qualificata

Le norme ETSI EN 319 421 V1.3.1 ([1]) («ETSI EN 319 421») ed ETSI EN 319 422 V1.1.1 ([2]) («ETSI EN 319 422») si applicano con gli adeguamenti seguenti.

1. Per ETSI EN 319 421

1) 2.1 Riferimenti normativi

— [3] ISO/IEC 15408:2022 (parti da 1 a 5) «Information security, cybersecurity and privacy protection – Evaluation criteria for IT security».

— [4] ETSI EN 319 401 V3.1.1 (2024-06) «Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers».

— [5] ETSI EN 319 422 V1.1.1 (2016-03) «Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles».

— [6] vuoto.

— [9] gruppo europeo per la certificazione della cibersicurezza, sottogruppo sulla crittografia: «Agreed Cryptographic Mechanisms» (meccanismi crittografici concordati) pubblicati dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA) ([3]).

— [10] Regolamento di esecuzione (UE) 2024/482 della Commissione, del 31 gennaio 2024, recante modalità di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC) ([4]).

— [11] Regolamento di esecuzione (UE) 2024/3144 della Commissione ([5]), del 18 dicembre 2024, che modifica il regolamento di esecuzione (UE) 2024/482 per quanto riguarda le norme internazionali applicabili e che rettifica tale regolamento di esecuzione.

2) 3.1 Termini

— periodo di validità dei certificati: intervallo di tempo che intercorre tra notBefore e notAfter compreso, durante il quale l'autorità di certificazione («CA») garantisce che manterrà le informazioni sulla situazione del certificato.

3) 3.3 Abbreviazioni

— EUCC Sistema europeo di certificazione della cibersicurezza basato sui criteri comuni

4) 6.2 Dichiarazione sulla pratica del servizio fiduciario

— OVR-6.2-03 La TSA include dichiarazioni sulla disponibilità del suo servizio di validazione temporale nella sua dichiarazione informativa.

5) 7.3 Sicurezza del personale

— OVR-7.3-02 Il personale della TSA in ruoli di fiducia e, se del caso, i subcontraenti della TSA in ruoli di fiducia sono in grado di soddisfare il requisito in materia di «competenze, esperienza e qualifiche» mediante formazione e credenziali formali, o effettiva esperienza, o una combinazione di entrambe.

— OVR-7.3-03 La conformità al requisito OVR-7.3-02 comprende aggiornamenti periodici (almeno ogni 12 mesi) sulle nuove minacce e sulle attuali pratiche di sicurezza.

([1]) EN 319 421 - «Electronic Signatures and Infrastructures (ESI) - Policy and Security Requirements for Trust Service Providers issuing Time Stamps», V1.3.1.
([2]) EN 319 422 - «Electronic Signatures and Infrastructures (ESI) - Time-stamping protocol and time-stamp token profiles», V1.1.1 (2016-03), https://www.etsi.org/deliver/etsi_en/319400_319499/319422/01.01.01_60/en_319422v010101p.pdf.
([3]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([4]) GU L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj.
([5]) GU L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

6) 7.6.2 Generazione delle chiavi della TSU

— TIS-7.6.2-03 La generazione della chiave o delle chiavi della TSU è effettuata all'interno di un dispositivo crittografico sicuro, che è un sistema affidabile certificato conformemente a quanto segue:

a) criteri comuni per la valutazione della sicurezza delle tecnologie informatiche, quali definiti nella norma ISO/IEC 15408 [3] o in «Common Criteria for Information Technology Security Evaluation», versione CC:2022, parti da 1 a 5, pubblicato dai partecipanti all'accordo «Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security», e certificato a livello EAL 4 o superiore; o

b) EUCC [10][11], e certificato a livello EAL 4 o superiore; o

c) fino al 31.12.2030, FIPS PUB 140-3 [7] livello 3.

Tale certificazione riguarda un obiettivo di sicurezza o un profilo di protezione, o la progettazione di un modulo e la documentazione di sicurezza, che soddisfano i requisiti del presente documento, sulla base di un'analisi dei rischi e tenendo conto delle misure di sicurezza fisiche e di altre misure di sicurezza non tecniche.

Se il dispositivo crittografico sicuro beneficia di una certificazione EUCC [10][11], tale dispositivo è configurato e utilizzato conformemente a tale certificazione.

— TIS-7.6.2-04 vuoto.

— NOTA 3 vuota.

— TIS-7.6.2-05 A L'algoritmo di generazione delle chiavi della TSU, la lunghezza della chiave di firma e l'algoritmo di firma risultanti utilizzati rispettivamente per la firma delle validazioni temporali e per la firma dei certificati a chiave pubblica della TSU sono conformi ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza [9] e pubblicati dall'ENISA.

— NOTA 4 vuota.

— TIS-7.6.2-06 La chiave di firma di una TSU è esportata e importata in un altro dispositivo crittografico sicuro solo se l'esportazione e l'importazione sono effettuate in modo sicuro e conformemente alla certificazione di tali dispositivi.

7) 7.6.3 Protezione della chiave privata della TSU

— TIS-7.6.3-02 La chiave privata della TSU è detenuta e utilizzata all'interno di un dispositivo crittografico sicuro che è un sistema affidabile certificato conformemente a quanto segue:

a) criteri comuni per la valutazione della sicurezza delle tecnologie informatiche, quali definiti nella norma ISO/IEC 15408 [3] o in «Common Criteria for Information Technology Security Evaluation», versione CC:2002, parti da 1 a 5, pubblicato dai partecipanti all'accordo «Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security», e certificato a livello EAL 4 o superiore; o

b) sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC) [10][11], e certificato a livello EAL 4 o superiore; o

c) fino al 31.12.2030, FIPS PUB 140-3 [7] livello 3.

Tale certificazione riguarda un obiettivo di sicurezza o un profilo di protezione, o la progettazione di un modulo e la documentazione di sicurezza, che soddisfano i requisiti del presente documento, sulla base di un'analisi dei rischi e tenendo conto delle misure di sicurezza fisiche e di altre misure di sicurezza non tecniche.

Se il dispositivo crittografico sicuro beneficia di una certificazione EUCC [10][11], tale dispositivo è configurato e utilizzato conformemente a tale certificazione.

— TIS-7.6.3-03 vuoto.

— NOTA 2 vuota.

8) 7.6.7 Fine del ciclo di vita della chiave pubblica della TSU

— TIS-7.6.7-03 A La data di scadenza delle chiavi private della TSU deve essere conforme ai meccanismi crittografici concordati [9].

— NOTA 1 vuota.

9) 7.10 Sicurezza delle reti

— OVR-7.10-05 La scansione delle vulnerabilità richiesta dal requisito REQ-7.8-13 della norma ETSI EN 319 401 [1] è eseguita almeno una volta a trimestre.

— OVR-7.10-06 Il test di penetrazione richiesto dal requisito REQ-7.8-17X della norma ETSI EN 319 401 [1] è eseguito almeno una volta all'anno.

— OVR-7.10-07 I firewall sono configurati in modo da impedire tutti i protocolli e gli accessi non richiesti per il funzionamento della TSA.

10) 7.14 Cessazione della TSA e piani di cessazione

— OVR-7.14-01 A Il piano di cessazione del TSP è conforme ai requisiti stabiliti negli atti di esecuzione adottati a norma dell'articolo 24, paragrafo 5, del regolamento (UE) n. 910/2014 [i.4].

2. Per ETSI EN 319 422

1) 2.1 Riferimenti normativi

— [5] vuoto.

— [6] vuoto.

— [8] gruppo europeo per la certificazione della cibersicurezza, sottogruppo sulla crittografia: «Agreed Cryptographic Mechanisms» (meccanismi crittografici concordati).

— [9] RFC 9110 Semantica HTTP.

2) 4.1.3 Algoritmi hash da utilizzare

— Si applica la seguente clausola:

gli algoritmi hash utilizzati per l'hashing delle informazioni oggetto di validazione temporale, la durata prevista della validazione temporale e le funzioni hash selezionate in funzione del tempo sono conformi ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [8].

— NOTA vuota.

3) 4.2.3 Algoritmi da supportare

— Si applica la seguente clausola:

gli algoritmi di firma token per la validazione temporale da supportare sono conformi ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [8].

— NOTA vuota.

4) 4.2.4 Lunghezze delle chiavi da supportare

— Si applica la seguente clausola:

le lunghezze delle chiavi dell'algoritmo di firma per l'algoritmo di firma selezionato sono conformi ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA.

— NOTA vuota.

5) 5.1.3 Algoritmi da supportare

— Si applica la seguente clausola:

gli algoritmi hash per i dati della validazione temporale da supportare e la durata prevista delle funzioni di validazione temporale e delle funzioni hash selezionate in funzione del tempo sono conformi ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [8].

— NOTA vuota.

6) 5.2.3 Algoritmi da utilizzare

— Si applica la seguente clausola:

gli algoritmi hash utilizzati per l'hashing delle informazioni oggetto di validazione temporale e gli algoritmi di firma token per la validazione temporale sono conformi ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [8].

— NOTA vuota.

7) 6.3 Requisiti relativi alle lunghezze delle chiavi

— Si applica la seguente clausola:

la lunghezza della chiave per l'algoritmo di firma selezionato del certificato della TSU è conforme ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [8].

— NOTA vuota.

8) 6.5 Requisiti relativi agli algoritmi

— Si applica la seguente clausola:

la chiave pubblica della TSU e la firma del certificato della TSU utilizzano algoritmi conformi ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [8].

— NOTA vuota.

9) 7 Profili per i protocolli di trasporto da supportare

— Il client e il server per la validazione temporale supportano il protocollo di validazione temporale tramite HTTPS [9], come definito al punto 3.4 di IETF RFC 3161 [1].

10) 8 Identificativi di oggetto degli algoritmi crittografici

— Si applica la seguente clausola:

la chiave pubblica della TSU e la firma del certificato della TSU utilizzano algoritmi conformi ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA [8].

11) 9.1 Dichiarazione di conformità al regolamento

— Se la TSA dichiara che un token di validazione temporale è una validazione temporale elettronica qualificata conformemente al regolamento (UE) n. 910/2014 [i.2], tale token contiene un esempio di estensione qcStatements nel campo dell'estensione del token di validazione temporale con la sintassi definita in IETF RFC 3739 [i.3], punto 3.2.6.

— L'estensione qcStatements contiene un esempio della dicitura «esi4-qtstStatement-1» definita nell'allegato B.

— L'estensione qcStatements non è contrassegnata come critica.