Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)
Organismo designato, ai sensi del comma 1 dell'art. 30 del Regolamento (UE) n. 910/2014, e notificato, ai sensi del comma 2 dello stesso articolo, come ente responsabile in Italia per l'accertamento di un dispositivo per la creazione di una firma elettronica o di un sigillo elettronico qualificato ai requisiti di sicurezza espressi nell'Allegato II al suddetto Regolamento.

Procedura di Accertamento di Conformità di un Dispositivo per la Creazione di Firme Elettroniche e di Sigilli Elettronici Qualificati ai Requisiti di Sicurezza previsti dall'Allegato II al Regolamento (UE) n. 910/2014

Attestato di Conformità n. 1/22

Dispositivo: ADSS Server SAM Appliance v7.0.2

Sviluppato da: Ascertia Ltd.

Il dispositivo per la creazione di firme elettroniche e di sigilli elettronici qualificati indicato in questo attestato è risultato conforme ai requisiti di sicurezza previsti dall'Allegato II al Regolamento (UE) n. 910/2014

Il Direttore
(Dott.ssa Eva Spina)

Firmato digitalmente da
Eva Spina
Data: 2022.05.23
09:03:19 +02'00'

Roma, 23 maggio 2022

Il presente Attestato di Conformità è stato emesso dall'Organismo di certificazione della Sicurezza Informatica (OCSI) ai sensi del comma 5 dell'art. 35 del DL 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale", modificato ed integrato dal DL 26 agosto 2016, n. 179.
La validità del presente Attestato di Conformità è soggetta alle condizioni e alle ipotesi esplicitate nel rapporto di Accertamento (OCSI/ACC/ASC/01/2022/RA) ad esso allegato, che ne costituisce parte integrante e sostanziale.

Questa pagina è lasciata intenzionalmente vuota

Organismo di Certificazione della Sicurezza Informatica

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Procedura di Accertamento di Conformità di un dispositivo per la creazione di firme e sigilli elettronici qualificati ai requisiti di sicurezza previsti dall'Allegato II al Regolamento (UE) n. 910/2014

Rapporto di Accertamento

ADSS Server SAM Appliance v7.0.2

OCSI/ACC/ASC/01/2022/RA

Versione 1.0

23 maggio 2022

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	23/05/2022

2 Indice

3 Elenco degli acronimi

CC	Common Criteria
CM	Cryptographic Module
DL	Decreto Legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
EAL	Evaluation Assurance Level
EC-DSA	Elliptic Curve - Digital Signature Algorithm
eIDAS	electronic IDentification Authentication and Signature
EN	European Norm
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
OTP	One-Time Password
PCIe	Peripheral Component Interconnect Express
PP	Profilo di Protezione
QSCD	Qualified Signature/Seal Creation Device
QTSP	Qualified Trust Service Provider
RSA	Rivest, Shamir, Adleman
SAD	Signature Activation Data
SAM	Signature Activation Module
SCA	Signature Creation Application
SCAL2	Sole Control Assurance Level 2
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
TDS	Traguardo di Sicurezza (Security Target)

TOE Target of Evaluation

TSF TOE Security Functions

TW4S Trustworthy System Supporting Server Signing

4 Riferimenti

[CAD] Decreto legislativo 7 marzo 2005, n. 82, recante “Codice dell'amministrazione digitale”, modificato ed integrato dal decreto legislativo 26 agosto 2016, n. 179, G.U. n. 214 del 13 settembre 2016

[eIDAS] “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”, Gazzetta ufficiale dell’Unione europea L 257, 28 agosto 2014

[ESI-CS] “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”, ETSI TS 119 312 V1.4.2 (2022-02)

[ESI-PR] “Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation”, ETSI TS 119 432 V1.2.1 (2020-10)

[PP-CM] Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services, EN 419221-5:2018, May 2018

[PP-SAM] Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing, EN 419241-2:2019, February 2019

[PR] “Procedura di Accertamento di Conformità di un dispositivo per la creazione di firme e sigilli elettronici qualificati ai requisiti di sicurezza previsti dall’Allegato II al Regolamento (UE) n. 910/2014”, OCSI/ACC/01/2016/PROC, versione 1.0, 21 dicembre 2016

[RA] Rapporto di Accertamento “ADSS Server SAM Appliance v6.0”, OCSI/ACC/ASC/01/2019/RA, versione 1.0, 1 luglio 2019

[RC-CM1] Certification Report “CryptoServer CP5 Se12 5.1.0.0, CryptoServer CP5 Se52 5.1.0.0, CryptoServer CP5 Se500 5.1.0.0, CryptoServer CP5 Se1500 5.1.0.0”, NSCIB-CC-222073-CR, v1.2, 27 May 2020

[RM-CM1] Assurance Continuity Maintenance Report “CryptoServer CP5 Se12 5.1.0.0, CryptoServer CP5 Se52 5.1.0.0, CryptoServer CP5 Se500 5.1.0.0, CryptoServer CP5 Se1500 5.1.0.0”, NSCIB-CC-222073-3MA1, v1, 20 November 2020

[RC-CM2] Certification Report “Entrust nShield Solo XC Hardware Security Module v12.60.15”, NSCIB-CC-0368256-CR, v1, 17 March 2021

[RM-CM2] Assurance Continuity Maintenance Report “nShield Solo XC Hardware Security Module v12.60.15”, NSCIB-CC-0368256-MA, v1, 22 July 2021

[RC-CM3] Certification Report “Thales Luna K7 Cryptographic Module”, NSCIB-CC-195307-CR, v1, 6 October 2020

[RC-SAM] Rapporto di Certificazione “Ascertia ADSS Server Signature Activation Module v7.0.2”, OCSI/CERT/CCL/11/2021/RC, versione 1.0, 29 aprile 2022

[TDS-CM1] “Security Target Lite for CryptoServer Se-Series Gen2 CP5”, v2.0.4, Utimaco IS GmbH, 18 November 2020

[TDS-CM2] “nShield Solo XC HSM Security Target”, v1.1.1, nCipher Security Limited, 11 June 2021

[TDS-CM3] “Thales Luna K7 Cryptographic Module - Security Target”, Rev J, Thales, 25 September 2020

[TDS-SAM] “Security Target of Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2”, v8, Ascertia Ltd., 19 April 2022

5 Ambito dell'Accertamento di Conformità

L'OCSI (Organismo di Certificazione della Sicurezza Informatica) è l'organismo designato, ai sensi del comma 1 dell'articolo 30 del Regolamento (UE) n. 910/2014 sull'identità digitale – eIDAS (*Electronic IDentification, Authentication and Signature*) [eIDAS] e notificato ai sensi del comma 2 dello stesso articolo, come ente responsabile in Italia per l'accertamento della conformità di un dispositivo per la creazione di una firma elettronica e di un sigillo elettronico qualificati ai requisiti di sicurezza espressi nell'Allegato II al suddetto Regolamento (UE) n. 910/2014.

L'affidamento all'OCSI dell'accertamento di cui sopra è specificato dal comma 5 dell'articolo 35 del DL 7 marzo 2005, n. 82, recante "Codice dell'amministrazione digitale" [CAD], modificato ed integrato dal DL 26 agosto 2016, n. 179.

L'Accertamento è stato condotto dall'OCSI in accordo a quanto indicato nella "Procedura di Accertamento di Conformità di un dispositivo per la creazione di firme e sigilli elettronici qualificati ai requisiti di sicurezza previsti dall'Allegato II al Regolamento (UE) n. 910/2014", OCSI/ACC/01/2016/PROC, versione 1.0, 21 dicembre 2016 [PR] (nel seguito indicata come Procedura).

L'oggetto dell'Accertamento di Conformità è il dispositivo denominato "ADSS Server SAM Appliance v7.0.2", sviluppato dalla società Ascertia Ltd. (nel seguito indicato brevemente come "ADSS Server SAM Appliance", "dispositivo oggetto dell'Accertamento", o semplicemente "dispositivo").

Il dispositivo oggetto dell'Accertamento è un **Dispositivo di Tipo 2**, così come definito nel cap. 6, punto A.ii, della Procedura.

Il dispositivo comprende il software ADSS Server SAM v7.0.2 (componente SAM), certificato in conformità con il Profilo di Protezione (PP) EN 419241-2 [PP-SAM], che si avvale per le operazioni crittografiche, in particolare per la creazione e gestione delle chiavi e per le operazioni di firma, di un HSM (componente CM) certificato in conformità con il PP EN 419221-5 [PP-CM].

L'insieme del software ADSS Server SAM v7.0.2 e dell'HSM costituisce il dispositivo sicuro per la creazione di firme elettroniche e di sigilli elettronici qualificati (QSCD) conforme al Regolamento eIDAS n. 910/2014 [eIDAS].

Si noti che il dispositivo oggetto dell'Accertamento è una versione aggiornata del dispositivo denominato "ADSS Server SAM Appliance v6.0", già accertato dall'OCSI (Attestato di Conformità n. 2/19 del 1° luglio 2019 [RA]).

In seguito ad alcune modifiche apportate al prodotto da parte del Fornitore è stato necessario procedere a una ri-certificazione del componente SAM, i cui risultati sono riportati nel Rapporto di Certificazione [RC-SAM].

Pur rimanendo valide in gran parte le considerazioni e le raccomandazioni già espresse per il precedente dispositivo, per facilità di lettura il presente Rapporto di Accertamento è stato riscritto nella sua interezza in modo da costituire un documento autonomo associato al nuovo dispositivo "ADSS Server SAM Appliance v7.0.2".

6 Riepilogo dell'accertamento

6.1 Introduzione

Questo Rapporto di Accertamento riporta le risultanze del processo di Accertamento di Conformità applicato al dispositivo "ADSS Server SAM Appliance v7.0.2", prodotto dalla società Ascertia Ltd., ed è finalizzato a fornire indicazioni ai potenziali acquirenti ed utilizzatori di tale dispositivo circa la sua conformità ai requisiti prescritti dalla normativa vigente per i dispositivi sicuri per la creazione di una firma elettronica e di un sigillo elettronico qualificati.

Il dispositivo oggetto dell'Accertamento, così come descritto nel Traguardo di Sicurezza del componente principale ADSS Server SAM ([TDS-SAM]), in congiunzione con uno dei componenti CM certificati supportati ([TDS-CM1], [TDS-CM2], [TDS-CM3]), è risultato conforme ai requisiti di sicurezza espressi nell'Allegato II al Regolamento (UE) n. 910/2014, nonché agli altri requisiti di adeguatezza ai fini dell'Accertamento espressi nella Procedura per i Dispositivi di Tipo 2 (cap. 7, punto B) e può quindi essere utilizzato come dispositivo per la creazione di firme e sigilli elettronici qualificati.

Il presente Rapporto di Accertamento deve essere consultato congiuntamente al Traguardo di Sicurezza del componente SAM ([TDS-SAM]), che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto e al relativo Rapporto di Certificazione ([RC-SAM]). Per ulteriori informazioni sulle caratteristiche di sicurezza dei componenti CM supportati si consiglia di consultare i relativi Traguardi di Sicurezza ([TDS-CM1], [TDS-CM2], [TDS-CM3]) e i Rapporti di Certificazione e di Mantenimento ([RC-CM1], [RM-CM1], [RC-CM2], [RM-CM2], [RC-CM3]).

La validità dell'Attestato di Conformità rilasciato per il dispositivo oggetto dell'Accertamento è soggetta alle condizioni e alle ipotesi esplicitate nel cap. 7 del presente Rapporto di Accertamento, che ne costituisce parte integrante e sostanziale.

Il rilascio dell'Attestato di Conformità da parte dell'OCSI non rappresenta alcun tipo di sostegno o promozione all'uso del dispositivo accertato da parte di questo Organismo.

6.2 Descrizione del dispositivo accertato

Il dispositivo "ADSS Server SAM Appliance v7.0.2" è un sistema affidabile che supporta la firma lato server (TW4S) e offre servizi di firma elettronica da remoto, garantendo che le chiavi di sottoscrizione del Firmatario vengano utilizzate sotto il suo controllo esclusivo e soltanto per gli scopi previsti.

Il dispositivo fornisce un servizio con accesso da remoto per la creazione di firme elettroniche e di sigilli elettronici qualificati conformi al Regolamento eIDAS [eIDAS] con Sole Control Assurance Level 2 (SCAL2) conforme alla norma EN 419241-1.

Questa soluzione remota consiste di un ambiente locale e di uno remoto, come illustrato in Figura 1.

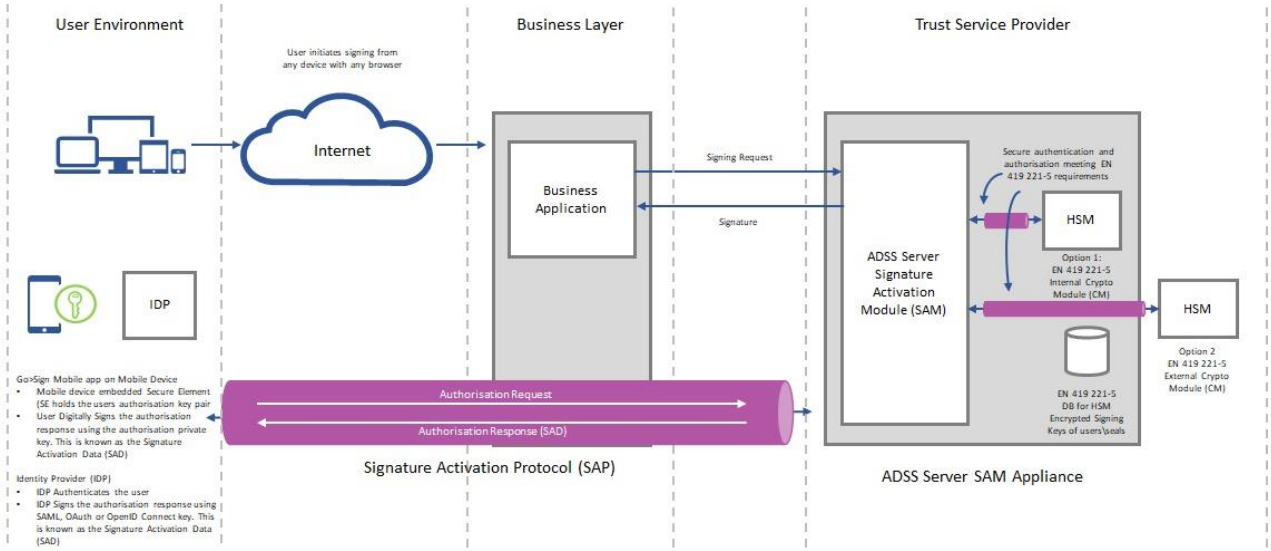

Figura 1 - Soluzione remota per firme e sigilli elettronici qualificati conformi al Regolamento eIDAS

Il dispositivo ADSS Server SAM Appliance, illustrato in Figura 2, è costituito da un apparato hardware anti-manomissione montabile su *rack* (1U) che fornisce un ambiente sicuro, certificato Common Criteria EAL4+ in conformità al PP EN 419241-2 [PP-SAM], per la creazione di firme elettroniche e sigilli elettronici qualificati sotto il controllo esclusivo del Firmatario.

Figura 2 - ADSS Server SAM Appliance: vista frontale (in alto) e posteriore (in basso)

Il confine fisico del dispositivo coincide con quello della ADSS Server SAM Appliance e comprende i seguenti componenti principali certificati:

- il software ADSS Server SAM v7.0.2 ([RC-SAM]), installato su piattaforma operativa Red Hat Enterprise Linux 8.4 e facente uso di un database Percona-XtraDB-Cluster v8.x;
- un HSM interno Utimaco CryptoServer CP5 Se500 o Se1500 ([RC-CM1], [RM-CM1]), sotto forma di scheda PCIe, certificato in conformità al PP EN 419221-5 [PP-CM].

Come configurazione alternativa, il dispositivo supporta l'utilizzo di un HSM esterno, certificato in conformità al PP EN 419221-5 [PP-CM], connesso in rete alla ADSS Server SAM Appliance mediante un canale sicuro. In questa modalità d'uso, l'ADSS Server SAM

Appliance contiene solamente il componente SAM, mentre il componente CM esterno deve essere installato nello stesso ambiente operativo del dispositivo e deve essere adeguatamente protetto da manomissione, come prescritto dal PP [PP-SAM].

Il componente principale ADSS Server SAM fornisce le seguenti funzionalità di sicurezza:

- mantiene i dettagli degli utenti Firmatari registrati;
- mantiene i dettagli dei dispositivi mobili;
- genera le richieste di autorizzazione;
- verifica le risposte di autorizzazione firmate (SAD);
- genera la coppia di chiavi di sottoscrizione all'interno dell'HSM;
- attiva la chiave di sottoscrizione all'interno dell'HSM.

Gli utenti Firmatari possono richiedere operazioni di firma da remoto interagendo con il dispositivo: vengono identificati tramite l'ID utente e autenticati durante la registrazione del dispositivo client da due password temporanee (OTP) inviate al numero di cellulare registrato e all'indirizzo Email dell'utente. Durante l'operazione di firma, i Firmatari vengono identificati tramite il loro ID utente e autenticati dalla risposta di autorizzazione firmata (SAD).

Il componente ADSS Server SAM non esegue direttamente le operazioni crittografiche per gli utenti Firmatari, vale a dire che non genera/archivia/distrugge, esporta/importa, esegue il backup/ripristino o usa la chiave di utente.

Ogni volta che è necessaria un'operazione crittografica per il Firmatario, ovvero l'autorizzazione a usare la chiave assegnata, il componente SAM richiama il componente CM (HSM) con i parametri appropriati. Le comunicazioni tra SAM e CM sono effettuate utilizzando un protocollo sicuro che soddisfa i requisiti definiti nel PP EN 419221-5 [PP-CM].

Il dispositivo può essere usato anche in Alta Affidabilità, utilizzando apparati ADSS Server SAM multipli in parallelo dei quali uno funziona come *master* e gli altri come *slave*. In questa configurazione la replica delle chiavi crittografiche da un apparato ADSS Server SAM ad un altro è gestita in modo sicuro e conforme alle prescrizioni del punto 4 dell'Allegato II al Regolamento eIDAS [eIDAS].

Per maggiori informazioni sulle caratteristiche del dispositivo e sulle politiche di sicurezza dei componenti certificati si faccia riferimento ai Traguardi di Sicurezza [TDS-SAM], [TDS-CM1], [TDS-CM2] e [TDS-CM3] e ai rispettivi Rapporti di Certificazione e di Mantenimento [RC-SAM], [RC-CM1], [RM-CM1], [RC-CM2], [RM-CM2] e [RC-CM3].

6.2.1 Configurazione certificata del dispositivo

Il dispositivo ADSS Server SAM Appliance comprende il componente certificato principale ADSS Server SAM, identificato nel Traguardo di Sicurezza [TDS-SAM] con il numero di versione 7.0.2 e un HSM, anch'esso certificato, che fornisce il necessario supporto crittografico per le operazioni di firma e di gestione delle chiavi del Firmatario.

In particolare, nella configurazione certificata del dispositivo sono supportati i seguenti modelli di HSM certificati Common Criteria in conformità al PP EN 419221-5 [PP-CM]:

- Componente CM interno all'ADSS Server SAM Appliance:
    - Utimaco CryptoServer CP5 Se500 5.1.0.0 ([RC-CM1], [RM-CM1]);
    - Utimaco CryptoServer CP5 Se1500 5.1.0.0 ([RC-CM1], [RM-CM1])
- Componente CM esterno:
    - Entrust nShield Solo XC Hardware Security Module v12.60.15 ([RC-CM2], [RM-CM2]);
    - Thales Luna K7 Cryptographic Module ([RC-CM3]).

Le configurazioni del dispositivo comprendenti il software ADSS Server SAM v7.0.2 e uno degli HSM certificati sopra elencati sono le sole considerate valide ai fini dell'accertamento di conformità.

Maggiori dettagli sono inclusi nel cap. 1.5 (*TOE Description*) del Traguardo di Sicurezza [TDS-SAM] e nel cap. 10 (*Configurazione valutata*) del Rapporto di Certificazione [RC-SAM].

Il dispositivo ADSS Server SAM Appliance v7.0.2 è risultato conforme ai requisiti di sicurezza espressi nell'Allegato II al Regolamento (UE) n. 910/2014, nonché agli altri requisiti di adeguatezza ai fini dell'Accertamento espressi nella Procedura [PR], a condizione che vengano rispettate le prescrizioni per l'utilizzo del dispositivo indicate nel cap. 8 del presente Rapporto di Accertamento.

6.3 Identificazione sintetica dell'accertamento

Richiedente l'accertamento	Ascertia Ltd.
Nome del dispositivo	ADSS Server SAM Appliance
Versione del dispositivo	7.0.2
Traguardo di Sicurezza	Componente SAM: • "Security Target of Ascertia ADSS Server Signature Activation Module (SAM) v7.0.2", v8 [TDS-SAM] Componente CM: • "Security Target Lite for CryptoServer Se-Series Gen2 CP5", v2.0.4 [TDS-CM1] • "nShield Solo XC HSM Security Target", v1.1.1 [TDS-CM2] • "Thales Luna K7 Cryptographic Module - Security Target", Rev J, [TDS-CM3]
Livello di garanzia	EAL4 con aggiunta di AVA_VAN.5
Versione dei CC	ADSS Server SAM: 3.1 Rev. 5 Utimaco CryptoServer CP5: 3.1 Rev. 4 nShield Solo XC: 3.1 Rev. 5 Thales Luna K7: 3.1 Rev. 5
Conformità a PP	EN 419241-2:2019, February 2019 [PP-SAM] EN 419221-5:2018, May 2018 [PP-CM]
Data di inizio della Procedura	16 maggio 2022
Data di rilascio Certificato CC[1]	ADSS Server SAM: 29 aprile 2022 Utimaco CryptoServer CP5: 20 novembre 2020 nShield Solo XC: 22 luglio 2021 Thales Luna K7: 6 ottobre 2020
Data di rilascio Accertamento	23 maggio 2022

[1] È riportata la data del Rapporto di Mantenimento più recente

7 Condizioni di validità dell'Attestato di Conformità

L'Attestato di Conformità rilasciato per il dispositivo oggetto dell'Accertamento deve essere ritenuto valido ed efficace unicamente sotto le seguenti ipotesi:

i. la certificazione di sicurezza ottenuta ([RC-SAM]) è in corso di validità, ovvero il Certificato non è stato revocato;

ii. il dispositivo reale è conforme a quello certificato e descritto nel TDS;

iii. l'ambiente di utilizzo reale del dispositivo è conforme a quello descritto nel TDS;

iv. sono rispettate tutte le condizioni aggiuntive di utilizzo del dispositivo riportate nel cap. 8 del presente Rapporto di Accertamento.

La violazione dell'ipotesi (i) comporta la perdita di validità dell'Attestato di Conformità.

La violazione di una o più delle ipotesi (ii), (iii) e (iv) ha come conseguenza la perdita di efficacia dell'Attestato di Conformità, che mantiene comunque la sua validità.

Eventuali situazioni che comportano la perdita di validità del presente Attestato di Conformità, siano esse rilevate direttamente dall'Organismo di Certificazione emettitore (OCSI) o portate a conoscenza di quest'ultimo da soggetti esterni, saranno rese note ai soggetti interessati attraverso i canali di informazione ufficiali dell'Organismo stesso.

Nel caso si verifichino situazioni che comportano la perdita di efficacia del presente Attestato, sarà cura dell'ente preposto alla vigilanza sui prestatori di servizi fiduciari qualificati provvedere alle misure correttive necessarie.

8 Condizioni di utilizzo del dispositivo accertato

Il dispositivo ADSS Server SAM Appliance v7.0.2 deve essere configurato ed utilizzato seguendo tutte le prescrizioni contenute nel Traguardo di Sicurezza del componente principale ADSS Server SAM (ODV) [TDS-SAM], nel relativo Rapporto di Certificazione [RC-SAM] e nella documentazione di guida per l'amministratore fornita con il dispositivo.

In particolare, la consegna, l'installazione sicura dell'ODV e la preparazione sicura del suo ambiente operativo devono avvenire in accordo agli obiettivi di sicurezza indicati in [TDS-SAM].

Inoltre, per quanto riguarda l'uso del dispositivo in conformità ai requisiti di sicurezza espressi nell'Allegato II al Regolamento (UE) n. 910/2014 [eIDAS], nonché agli altri requisiti di adeguatezza ai fini dell'Accertamento espressi nella Procedura [PR], si raccomanda di porre particolare attenzione agli aspetti di seguito descritti.

8.1 Restrizioni d'uso rispetto alla configurazione certificata

Il presente Attestato di Conformità copre unicamente il caso d'uso "Remote Server Signing" (Use Case 2), così come descritto nel PP [PP-CM]. Il dispositivo deve essere utilizzato per la creazione di firme o di sigilli elettronici qualificati da remoto e gestito per conto del Firmatario da un QTSP in conformità al Regolamento eIDAS [eIDAS].

Per poter essere utilizzato in conformità al Regolamento eIDAS, il dispositivo deve essere opportunamente configurato per utilizzare come sorgente crittografica (*Crypto Source*) di tipo hardware l'HSM interno (Utimaco CP5 Se500 o Se1500) o, in alternativa e in maniera esclusiva, un HSM esterno in modalità certificata. Il dispositivo supporta solamente gli HSM esterni certificati elencati nel par. 6.2.1.

8.2 Algoritmi crittografici

Gli algoritmi crittografici utilizzati dalle funzioni di sicurezza (TSF) del dispositivo certificato sono elencati nel Traguardo di Sicurezza, nella formulazione dei requisiti funzionali di sicurezza (SFR) della classe FCS - Cryptographic Support (si veda [TDS-SAM], par. 6.4.2).

Per quanto riguarda la generazione di coppie di chiavi crittografiche e i metodi di sottoscrizione, debbono essere utilizzati esclusivamente algoritmi crittografici, lunghezze di chiavi, funzioni *hash*, protocolli e parametri conformi alla specifica ETSI TS 119 312 [ESI-CS].

In particolare, per la generazione e la verifica di firme e/o sigilli elettronici qualificati è consentito l'uso solamente dei seguenti algoritmi crittografici, tra quelli messi a disposizione dal dispositivo oggetto dell'Accertamento:

- Funzioni di *hash*: SHA-256, SHA-384, SHA-512, SHA3-256, SHA3-384, SHA3-512.
- Metodi di sottoscrizione:

- RSASSA-PSS (raccomandato) o RSASSA-PKCS-v1_5 (*legacy*), con lunghezza di chiave non inferiore a 2048 bit.

- EC-DSA (raccomandato) con lunghezza di chiave non inferiore a 256 bit e con le seguenti curve ellittiche: P-256, P-384, P-521, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1 (si veda [ESI-CS], cap. 6.2.2.3 *EC based DSA algorithms*).

L'algoritmo RSA con lo schema di *padding* RSASSA-PKCS-v1_5 può ancora essere utilizzato per motivi di interoperabilità, ma non è raccomandato per nuove implementazioni.

In generale, per i parametri di sicurezza relativi ai metodi di sottoscrizione va tenuto conto di quanto indicato in [ESI-CS], cap. 8.4 (*Recommended key sizes versus time*).