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. 1/21

Dispositivo: Primus HSM FW 2.8.21 Series E, Series X

Sviluppato da: Securosys SA

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: 2021.10.22
10:40:47 +02'00'

Roma, 22 ottobre 2021

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/SEC/01/2021/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

Primus HSM FW 2.8.21 Series E, Series X

OCSI/ACC/SEC/01/2021/RA

Versione 1.0

22 ottobre 2021

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	22/10/2021

2 Indice

1 Revisioni del documento 5
2 Indice 6
3 Elenco degli acronimi 7
4 Riferimenti 9
5 Ambito dell'Accertamento di Conformità 10
6 Riepilogo dell'accertamento 11
6.1 Introduzione 11
6.2 Descrizione del dispositivo accertato 11
6.2.1 Attivazione delle chiavi di firma mediante Smart Key Attributes 13
6.2.2 Configurazione certificata del dispositivo 14
6.3 Identificazione sintetica dell'accertamento 15
7 Condizioni di validità dell'Attestato di Conformità 16
8 Condizioni di utilizzo del dispositivo accertato 17
8.1 Restrizioni d'uso rispetto alla configurazione certificata 17
8.2 Algoritmi crittografici 17

3 Elenco degli acronimi

CC	Common Criteria
CM	Cryptographic Module
DL	Decreto Legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
DTBS/R	Data To be Signed / Representation
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
PKI	Public Key Infrastructure
PP	Profilo di Protezione
QSCD	Qualified Signature Creation Device
QTSP	Qualified Trust Service Provider
RSA	Rivest, Shamir, Adleman
SAM	Signature Activation Module
SCA	Signature Creation Application
SKA	Smart Key Attributes
SAD	Signature Activation Data
SAP	Signature Activation Protocol
SCAL2	Sole Control Assurance Level 2
SFR	Security Functional Requirement

SHA	Secure Hash Algorithm
SIC	Signer Interaction Component
SSA	Server Signing Application
TDS	Traguardo di Sicurezza
TOE	Target of Evaluation
TSF	TOE Security Functions

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 V1.4.1 (2021-08)

[ESI-PR] “Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation”, ETSI TS 119 432 V1.1.1 (2019-03)

[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

[RC] “Rapporto di Certificazione Primus HSM FW 2.8.21 Series E, Series X”, OCSI/CERT/CCL/04/2020/RC, versione 1.0, 14 aprile 2021

[TDS] “PRIMUS HSM Security Target”, v1.02, Securosys SA, 19 March 2021

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 "Primus HSM FW 2.8.21 Series E, Series X", sviluppato dalla società Securosys SA (nel seguito indicato brevemente come "Primus HSM", "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 è un modulo crittografico (CM o HSM) certificato in conformità con il Profilo di Protezione (PP) EN 419221-5:2018 [PP-CM].

Il dispositivo può essere utilizzato sia autonomamente, sia in connessione con un componente software che implementa un Signature Activation Module (SAM) certificato in conformità con il PP EN 419241-2:2019 [PP-SAM].

Nella prima modalità d'uso il dispositivo certificato (ODV) costituisce il dispositivo sicuro per la creazione di firme elettroniche qualificate e sigilli elettronici qualificati (QSCD) conforme al Regolamento (UE) n. 910/2014 [eIDAS]. Nella seconda modalità d'uso il QSCD è costituito dall'insieme dell'ODV (componente CM) e del componente SAM certificato.

6 Riepilogo dell'accertamento

6.1 Introduzione

Questo Rapporto di Accertamento riporta le risultanze del processo di Accertamento di Conformità applicato al dispositivo "Primus HSM FW 2.8.21 Series E, Series X", prodotto dalla società Securosys SA, 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 relativo Traguardo di Sicurezza [TDS], 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 [TDS], che specifica i requisiti funzionali e di garanzia e l'ambiente di utilizzo previsto e al relativo Rapporto di Certificazione [RC].

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 "Primus HSM FW 2.8.21 Series E, Series X" (o Primus HSM) è un modulo crittografico di tipo HSM fisicamente sicuro, ovvero un dispositivo informatico fisico che crea, protegge e gestisce chiavi digitali per firme elettroniche e altre operazioni crittografiche.

Il dispositivo certificato (nel seguito anche indicato come ODV) include tutti i modelli di Primus HSM delle Serie E e X (indicati anche come E-Module e X-Module, rispettivamente). Tutti i moduli dell'ODV eseguono lo stesso firmware e differiscono solo per quanto riguarda le risorse di archiviazione e di elaborazione.

Il dispositivo può essere utilizzato da prestatori di servizi fiduciari qualificati (QTSP) per offrire servizi con accesso da remoto per la creazione di firme elettroniche qualificate, sigilli elettronici qualificati e marcature temporali e per operazioni e servizi di autenticazione in conformità al Regolamento (UE) 910/2014 [eIDAS]. Il dispositivo è in grado di garantire che le chiavi di sottoscrizione del Firmatario vengano utilizzate sotto il suo controllo esclusivo e soltanto per gli scopi previsti.

Le forme fisiche dell'ODV sono illustrate in Figura 1 e Figura 2. Il confine di un modulo (delimitato in rosso nelle figure) include lo chassis e tutti gli elementi al suo interno.

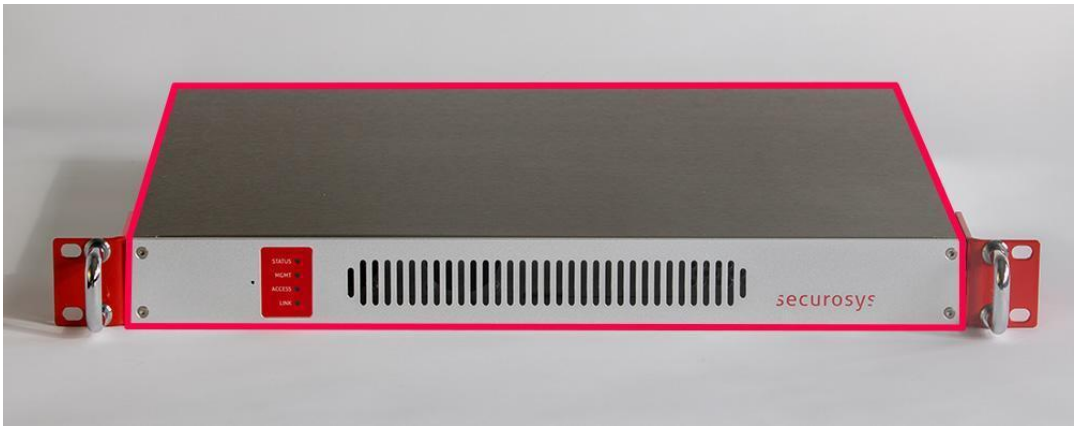

Figura 1 – Vista frontale di un E-Module

Figura 2 - Vista frontale di un X-Module

L'ODV fornisce le seguenti funzioni crittografiche:

- generazione e verifica di firme elettroniche (e sigilli elettronici);
- generazione di *message digest*;
- generazione e verifica di codici di autenticazione dei messaggi;
- cifratura e decifratura (simmetrica e asimmetrica);
- generazione di chiavi;
- scambio e distribuzione di chiavi;
- derivazione di chiavi;
- generazione di valori segreti condivisi;
- supporto crittografico per password monouso e altri meccanismi di autenticazione non basati su PKI;

- generazione di numeri casuali.

Queste funzioni possono essere utilizzate anche per supportare il sistema di un QTSP per la creazione di firme o sigilli elettronici qualificati e marcature temporali elettroniche.

L'ODV supporta la gestione sicura delle chiavi crittografiche necessarie per le funzioni crittografiche implementate, incluso:

- scambio di chiavi (compresa la generazione di chiavi);
- protezione delle chiavi custodite sia all'interno dell'ODV, sia esternamente (per l'uso da parte dell'ODV);
- controllo dell'accesso e dell'utilizzo delle chiavi da parte delle funzioni crittografiche interne dell'ODV;
- cancellazione delle chiavi all'interno dell'ODV.

L'ODV implementa autenticazione o autorizzazione separate dei seguenti tipi distinti di entità:

- amministratori dell'ODV;
- utenti applicativi delle funzioni crittografiche dell'ODV (applicazioni client esterne, autenticate mediante l'utilizzo di canali sicuri);
- utenti di chiavi private (il cui uso, nel caso di chiavi di sottoscrizione per l'apposizione di firme o sigilli elettronici qualificati, deve essere limitato ad una determinata persona fisica o giuridica).

È possibile registrare più utenti (applicazioni client) nell'ODV. Ad ogni utente (applicazione client) viene assegnata una partizione separata dell'ODV.

6.2.1 Attivazione delle chiavi di firma mediante Smart Key Attributes

Il dispositivo Primus HSM implementa un meccanismo nativo di attivazione per le Assigned Key, ossia le chiavi segrete utilizzate per la creazione di firme e sigilli elettronici così come definite in [PP-CM], denominato Smart Key Attributes (SKA). L'uso delle chiavi SKA impone che l'uso di una chiave segreta venga approvato in base a una politica delle chiavi differente per ogni soggetto.

L'autorizzazione come soggetto proprietario di una chiave privata (Firmatario o creatore di sigillo), necessaria per poterla utilizzare in una funzione crittografica (o esportarla), può essere effettuata da Primus HSM mediante le chiavi SKA, indipendentemente da qualsiasi altra autorizzazione che potrebbe essere stata stabilita per le applicazioni client.

Il meccanismo delle chiavi SKA consente o nega espressamente l'uso di una chiave di sottoscrizione sulla base di una cosiddetta "approvazione". Una "approvazione" lega fra loro l'autenticazione del Firmatario, i DTBS/R e il riferimento univoco della chiave di firma, vale a dire i tre elementi richiesti di un SAD, così come indicati in [PP-SAM].

Il meccanismo SKA rende il modulo SAM superfluo, in quanto le funzionalità del Signature Activation Protocol (SAP) descritte in [PP-SAM] sono intrinsecamente coperte dall'implementazione delle Assigned Key da parte del dispositivo Primus HSM, che soddisfa i requisiti del controllo esclusivo di livello 2 (SCAL2) definito in [ESI-PR].

Rispetto a quanto descritto in [PP-SAM], il flusso di lavoro di una richiesta di apposizione di una firma elettronica è il seguente:

- La SCA richiede di firmare i DTBS/R tramite la SSA, facendo riferimento ad una Assigned Key memorizzata nel dispositivo. La SSA può essere un componente funzionalmente vuoto, in quanto la SCA può comunicare direttamente con il dispositivo mediante un canale sicuro.

- La SCA, direttamente o indirettamente tramite la SSA, interroga la politica della Assigned Key e invia una richiesta di approvazione al SIC. La richiesta di approvazione è un blocco di dati protetto in integrità composto dal riferimento della chiave e dai DTBS/R. Al momento della verifica dell'integrità della richiesta, il SIC firma digitalmente la richiesta di approvazione con la chiave privata di approvazione generando un SAD firmato costituito dall'associazione tra il riferimento alla Assigned Key e il DTBS/R.

- L'informazione sulla chiave di firma utilizzata per creare il SAD viene inviata al dispositivo a valle del processo di autenticazione del Firmatario. Alla Assigned Key viene associato al momento della creazione un certificato valido (chiave pubblica) che consente al dispositivo di verificare l'autenticità del SAD. Inoltre, il dispositivo verifica che il DTBS/R approvato e il DTBS/R della richiesta di firma siano identici. Il dispositivo richiede nuovamente l'autorizzazione del Firmatario all'uso della chiave di firma per ogni nuovo DTBS/R o se viene specificato un riferimento ad una Assigned Key diversa.

Per maggiori informazioni sulle caratteristiche dell'ODV e sulla sua politica di sicurezza si faccia riferimento al Traguardo di Sicurezza [TDS] e al Rapporto di Certificazione [RC].

6.2.2 Configurazione certificata del dispositivo

La configurazione certificata del dispositivo "Primus HSM FW 2.8.21 Series E, Series X" include i seguenti modelli:

- Serie E: E20, E60, E150

- Serie X: X200, X400, X700, X1000

Tutti i modelli dell'ODV includono la seguente versione del firmware:

- FW 2.8.21

I vari modelli dell'ODV forniscono le stesse funzionalità e differiscono solo per quantità di memoria e risorse di calcolo.

Maggiori dettagli sono inclusi nel par. 3.4.1 del Traguardo di Sicurezza [TDS] e nel cap. 10 (Appendice B - Configurazione valutata) del Rapporto di Certificazione [RC].

Il dispositivo “Primus HSM FW 2.8.21 Series E, Series X” 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	Securosys SA
Nome del dispositivo	Primus HSM FW 2.8.21 Series E, Series X
Versione del dispositivo	FW 2.8.21
Traguardo di Sicurezza	“PRIMUS HSM Security Target”, v1.02, 19 March 2021 [TDS]
Livello di garanzia	EAL4 con l’aggiunta di AVA_VAN.5
Versione dei CC	3.1 Rev. 5
Conformità a PP	EN 419221-5:2018 [PP-CM]
Data di inizio della Procedura	26 luglio 2021
Data di rilascio Certificato CC	14 aprile 2021
Data di rilascio Accertamento	22 ottobre 2021

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]) 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 “Primus HSM FW 2.8.21 Series E, Series X” deve essere utilizzato seguendo tutte le prescrizioni contenute nel Traguardo di Sicurezza [TDS] e nel Rapporto di Certificazione [RC].

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] e seguendo le indicazioni riportate anche nel cap. 9 (Appendice A - Indicazioni per l’uso sicuro del prodotto) del Rapporto di Certificazione [RC].

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 Profilo di Protezione [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 ad [eIDAS].

Inoltre, per l’utilizzo del dispositivo Primus HSM come QSCD si applicano le seguenti restrizioni e ipotesi aggiuntive rispetto a quanto dichiarato in [TDS]:

- Il dispositivo locale e il SIC che interagiscono con la SSA e/o con l’ODV debbono essere sotto il controllo esclusivo del Firmatario e utilizzati in un ambiente sufficientemente protetto da attacchi informatici locali o remoti. In particolare, deve essere garantita un’adeguata protezione delle chiavi private utilizzate per firmare i SAD inviati al QSCD.

- Per la generazione di firme e sigilli elettronici qualificati, il dispositivo deve essere configurato per utilizzare unicamente come chiavi di sottoscrizione le chiavi SKA, ossia Assigned Key attivabili mediante il meccanismo SKA del dispositivo con opportune policy di autorizzazione che garantiscano il controllo esclusivo del Firmatario o del creatore di sigillo.

Si noti che il dispositivo può anche essere utilizzato senza particolari restrizioni in connessione con un SAM certificato in conformità con il PP [PP-SAM], ma in questo caso il QSCD è costituito dall’insieme del dispositivo Primus HSM certificato (ODV) e del componente SAM certificato.

Nella configurazione SAM + CM (ODV), il SAM deve essere opportunamente configurato per utilizzare le Assigned Key generate dal dispositivo Primus HSM.

8.2 Algoritmi crittografici

Gli algoritmi crittografici utilizzati dalle funzioni di sicurezza (TSF) del dispositivo certificato sono elencati nel Traguardo di Sicurezza (si veda [TDS] par. 3.4.2.3 - Cryptographic

Algorithms), nella formulazione dei requisiti funzionali di sicurezza (SFR) della classe FCS - Cryptographic Support (si veda [TDS], par. 7.3.1).

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 (si veda [ESI-CS], cap. 6.2.2.3 *EC based DSA algorithms*).
    - DSA con lunghezza di chiave non inferiore a 2048 bit.

L'algoritmo DSA può 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*).