Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

OCSI

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'articolo 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 della conformità di un dispositivo di firma elettronica e di un sigillo elettronico qualificati 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. 2/19

Dispositivo: ADSS Server SAM Appliance v6.0

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)

Roma, 1 luglio 2019

Il presente Attestato di Conformità è stato emesso dall'Organismo di Certificazione della Sicurezza Informatica (OCSI) in conformità al comma 5 dell'articolo 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/01/2019/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

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 v6.0

OCSI/ACC/ASC/01/2019/RA

Versione 1.0

1 luglio 2019

Questa pagina è lasciata intenzionalmente vuota

1 Revisioni del documento

Versione	Autori	Modifiche	Data
1.0	OCSI	Prima emissione	01/07/2019

2 Indice

3 Elenco degli acronimi

CC	Common Criteria
CEN	Comité Européen de Normalisation
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
HSM	Hardware Security Module
ISO	International Organization for Standardization
IT	Information Technology
OCSI	Organismo di Certificazione della Sicurezza Informatica
ODV	Oggetto della Valutazione
OTP	One-Time Password
PCIe	Peripheral Component Interconnect Express
PP	Profilo di Protezione (Protection Profile)
RSA	Rivest, Shamir, Adleman
SAD	Signature Activation Data
SAM	Signature Activation Module
SHA	Secure Hash Algorithm
QSCD	Qualified Signature Creation Device
SFR	Security Functional Requirement
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 V1.2.2 (2018-09)

[PP-CM] Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services, prEN 419 221-5, v015, 29 November 2016

[PP-SAM] “Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing”, prEN 419 241-2, v0.16, 11 May 2018

[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-CM] 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, v1.1, 14 March 2019

[RC-SAM] Rapporto di Certificazione “Ascertia ADSS Server Signature Activation Module v6.0”, v1.0, 13 marzo 2019

[TDS-CM] Security Target Lite “CryptoServer Se-SeriesGen2CP5”, v2.0.0, Utimaco IS GmbH, 23 November 2018

[TDS-SAM] Security Target “Ascertia ADSS Server Signature Activation Module (SAM) v6.0”, v18, 1 October 2018

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 v6.0", sviluppato dalla società Ascertia Ltd. (nel seguito indicato brevemente come ADSS Server SAM Appliance o anche "dispositivo oggetto dell'Accertamento" o semplicemente "dispositivo").

Il dispositivo ADSS Server SAM Appliance è un sistema affidabile che supporta la firma lato server (TW4S - *Trustworthy System Supporting Server Signing*) e fornisce un servizio con accesso da remoto per la creazione di firme elettroniche e di sigilli elettronici qualificati conformi al Regolamento eIDAS n. 910/2014 [eIDAS].

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 (componente SAM), certificato in conformità con il Profilo di Protezione (PP) prEN 419 241-2 [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 prEN 419 221-5 [PP-CM].

L'insieme indissolubile del software ADSS Server SAM 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 i due PP sopra citati ([PP-SAM] e [PP-CM]) sono attualmente in corso di standardizzazione (CEN) al fine di definire una configurazione di riferimento per la certificazione di sicurezza dei dispositivi per la creazione di firme e sigilli elettronici qualificati in modalità remota.

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 v6.0, 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 il componente CM certificato ([TDS-CM]), 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 sia come dispositivo per la creazione di una firma elettronica qualificata (*qualified electronic signature creation device*), sia come dispositivo per la creazione di un sigillo elettronico qualificato (*qualified electronic seal creation device*).

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 del componente CM si consiglia di consultare il Traguardo di Sicurezza [TDS-CM] e il Rapporto di Certificazione [RC-CM1].

La validità dell'Attestato di Conformità rilasciato per il dispositivo oggetto dell'Accertamento è soggetta alle condizioni e alle ipotesi esplicitate nel presente Rapporto di Accertamento (vedi cap. 7), 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 v6.0 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 n. 910/2014 [eIDAS].

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

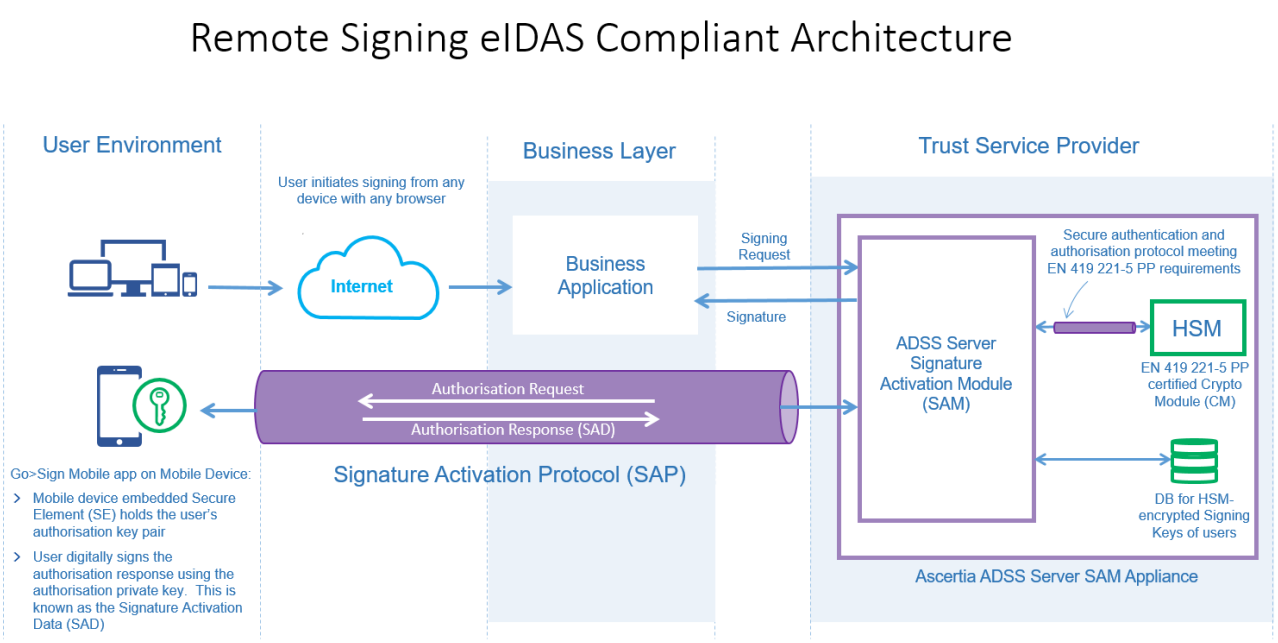

Figura 1 – Soluzione remota per firme e sigilli elettronici qualificati conformi al Regolamento eIDAS

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 Profilo di Protezione prEN 419 241-2 [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 comprende i seguenti componenti principali certificati:

- il software ADSS Server SAM, installato su piattaforma operativa Linux RedHat 7.4 e facente uso di un database Percona XtraDB;
- un HSM interno Utimaco CryptoServer CP5 Se1500, sotto forma di scheda PCIe, certificato Common Criteria EAL4+ in conformità al Profilo di Protezione prEN 419 221-5 [PP-CM].

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 da remoto operazioni di firma 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 modulo SAM richiama il modulo CM (HSM), inserito nello stesso apparato, con i parametri appropriati. Le comunicazioni tra SAM e CM sono effettuate utilizzando un protocollo sicuro che soddisfa i requisiti definiti nel PP prEN 419 221-5 [PP-CM].

Il dispositivo può essere usato anche in Alta Affidabilità, utilizzando apparati ADSS Server SAM multipli in parallelo. La replica delle chiavi crittografiche da un apparato ADSS Server SAM ad un altro è gestita dall'HSM in modo conforme a quanto prescritto nel PP prEN 419 221-5 [PP-CM].

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

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 6.0 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 è supportato unicamente il modello di HSM CryptoServer CP5 Se1500 della società Utimaco IS GmbH, certificato Common Criteria in conformità al Profilo di Protezione prEN 419 221-5 [PP-CM], identificato nel Traguardo di Sicurezza [TDS-CM] con la versione 5.1.0.0.

La configurazione del dispositivo comprendente il software ADSS Server SAM v6.0 e l'HSM CryptoServer CP5 Se1500 5.1.0.0 è la sola considerata valida 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 v6.0 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	6.0
Traguardo di Sicurezza	"Ascertia ADSS Server Signature Activation Module (SAM) v6.0" Security Target, v18, 1 October 2018 [TDS-SAM] Security Target Lite "CryptoServer Se-SeriesGen2CP5", v2.0.0, Utimaco IS GmbH, 23 November 2018 [TDS-CM]
Livello di garanzia	EAL4 con aggiunta di AVA_VAN.5
Versione dei CC	ADSS Server SAM: 3.1 Rev. 5 Utimaco CP5 Se1500 (HSM): 3.1 Rev. 4
Conformità a PP	prEN 419 241-2, v0.16, 11 May 2018 [PP-SAM] prEN 419 221-5, v015, 29 November 2016 [PP-CM]
Data di inizio della Procedura	30 aprile 2019
Data di rilascio Certificato CC	ADSS Server SAM: 13 marzo 2019 Utimaco CP5 Se1500 (HSM): 14 marzo 2019
Data di rilascio Accertamento	1 luglio 2019

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 scaduto o 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 v6.0 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 Configurazione per l'uso dell'HSM in modalità certificata

Per poter essere utilizzato in conformità al Regolamento (UE) n. 910/2014 [eIDAS], il dispositivo deve essere opportunamente configurato per utilizzare l'HSM interno Utimaco CP5 Se1500 in modalità certificata.

In particolare, all'atto della configurazione del componente ADSS Server SAM, durante la creazione di una nuova *Crypto Source* mediante l'interfaccia *ADSS Server > Key Manager*, va selezionata l'opzione "Enable Qualified Remote Signing".

8.2 Algoritmi crittografici

Gli algoritmi crittografici utilizzati dalle funzioni di sicurezza (TSF) del dispositivo certificato sono elencati nel Traguardo di Sicurezza del componente principale ADSS Server SAM, nella formulazione dei requisiti funzionali di sicurezza (SFR) della classe FCS - *Cryptographic Support* (si veda [TDS-SAM] cap. 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.
- **Metodi di sottoscrizione:**
    - RSA-PSS (raccomandato) o RSA-PKCSv1_5, con lunghezza di chiave non inferiore a 2048 bit.

- EC-DSA (raccomandato) con lunghezza di chiave non inferiore a 256 bit, a patto che vengano utilizzate esclusivamente le curve indicate in [ESI-CS], cap. 6.2.2.3 (*EC based DSA algorithms*), Tabella 3 (*Agreed Elliptic Curve Parameters*).

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*).