NOTE TECNICHE
allegate al
"MANUALE OPERATIVO ALLA CLIENTELA"
PER GLI ADEMPIMENTI VERSO DI ESSA PRESCRITTI IN MATERIA DI FIRMA ELETTRONICA AVANZATA

(Documento [1] predisposto ai sensi del DPCM 22.2.2013 [2])

[1] Aggiornato al 27/10/2014

[2] DPCM 22 febbraio 2013, Regole Tecniche in materia di generazione, apposizione, e verifica delle firme elettroniche avanzate, qualificate e digitali

Contenuti

Glossario degli Acronimi

DPCM	Decreto del Presidente del Consiglio dei Ministri della Repubblica Italiana
FEA	Firma Elettronica Avanzata
CC EAL 4+	Common Criteria Evaluation Assurance Level 4+
HSM	Hardware Security Module
SSCD	Secure Signature-Creation Device, o Dispositivo Sicuro di Firma
LBDU	Log and Document Builder Unit
TSA	Time Stamping Authority
X.509	Standard relativo ai certificati digitali dei sistemi a chiave pubblica
OTP	One Time Password

1. ASPETTI GENERALI DELL'ARCHITETTURA TECNICA DELLA FEA

1.1 Certificazioni e Criteri di Sicurezza

L'architettura tecnica utilizzata per la realizzazione della **F**irma **E**lettronica **A**vanzata (**FEA)** da BNL è conforme agli standard di sicurezza più elevati stabiliti dalle normative vigenti italiane ed europee.

In particolare gli apparati utilizzati sono conformi ai profili di sicurezza internazionali **C**ommon **C**riteria **EAL 4+**[1]**.**

Tali criteri di sicurezza hanno in estrema sintesi lo scopo (oltre alla conformità con le normative vigenti) di assicurare:

- Il controllo **esclusivo** da parte del firmatario delle operazioni di firma dei documenti
- La corrispondenza **univoca** tra la identità del soggetto firmatario e le chiavi private utilizzate per la sottoscrizione
- La **protezione** delle chiavi private utilizzate e della loro segretezza
- La associazione **biunivoca** e **permanente** tra la firma e il documento firmato

1.2 Mezzi Tecnici

La infrastruttura di FEA si avvale di un **dispositivo crittografico Hardware** di sicurezza denominato **HSM** (**H**ardware **S**ecurity **M**odule) che ha lo scopo di generare le chiavi di sottoscrizione e custodirle oltre che di effettuare le operazioni di firma quale **D**ispositivo **S**icuro di **F**irma.

Una delle caratteristiche principali di tale dispositivo è la impossibilità di ottenere o utilizzare all'esterno di esso qualunque chiave privata generata o ospitata dal dispositivo stesso.

La infrastruttura si avvale inoltre di un ulteriore specifico dispositivo (anche esso dotato di meccanismi crittografici Hardware di sicurezza) che provvede alle operazioni di formattazione e costruzione dei documenti firmati e da firmare secondo gli standard normativi italiani e europei .

Questo secondo dispositivo denominato **LBDU** (**L**og and **D**ocument **B**uilder **U**nit) ha principalmente il compito di mantenere il registro delle operazioni e delle transazioni e di apporre

[1] Common Criteria è un set di standards internazionale (ISO/IEC 15408) che fornisce uno schema per la valutazione delle funzionalità di sicurezza dei prodotti nell'ambito dell'nformation Technology. EAL 4+ rappresenta il livello piu' alto

le marche temporali (trusted timestamp), prodotte e fornite da una **TSA**[1] esterna, in modo sicuro per identificare e mantenere nel tempo la integrità dei documenti e del registro stesso.

1.3 Comunicazioni Tra Gli Apparati

Durante le operazioni che implicano operazioni relative alla **FEA** ogni forma di comunicazione tra gli apparati coinvolti avviene su **canali sicuri e cifrati** allo scopo di garantire la esclusività di controllo delle operazioni al firmatario da ogni possibile ingerenza da parte di terzi compresi gli operatori di BNL stessa.

Allo stesso modo gli apparati dell'infrastruttura di **FEA** operano permanentemente e esclusivamente in modalità protetta e cifrata e solo i dispositivi autorizzati e riconosciuti dalla infrastruttura stessa possono comunicare con essa.

Nessuna altra modalità di comunicazione, comprese quelle amministrative e di manutenzione, è ammessa senza alcuna eccezione.

1.4 Accesso Ai Mezzi Fisici

Gli apparati dell'infrastruttura **FEA** sono collocati in locali ad accesso controllato e i dispositivi crittografici di sicurezza dispongono di mezzi di rilevamento delle intrusioni o manomissioni non autorizzate che sono in grado di disabilitare e rendere inutilizzabili i dispositivi stessi.

[1] Time Stamping Autority, autorita' di certificazione che certifica, attraverso la marcatura temporale di un oggetto informatico, la sua integrita' da quell'istante temporale e in modo tale che qualunque soggetto interessato possa effettuarne la verifica in qualsiasi momento successivo

2. ASPETTI OPERATIVI DELLA FEA

2.1 Registrazione Dei Dati Identificativi E Autorita' Di Registrazione

I dati identificativi dei soggetti abilitati all'utilizzo della **FEA** sono contenuti in un certificato digitale di tipo standard **X.509** [1].

I dati sono raccolti in presenza del soggetto abilitato e verificando la identità del medesimo attraverso la struttura (sportelli e/o struttura di vendita) direttamente da BNL o tramite fonti di **Autorita' di Registrazione** di società appartenenti e collegate al gruppo BNL o terze ma comunque riconosciute, in quanto tali, attendibili da BNL stessa o da fonti **Interbancarie**.

Nel caso di utilizzo di strumenti di identificazione che comprendono l'utilizzo di dati biometrici, gli specimen [2] depositati dal soggetto firmatario sono raccolti in modalità cifrata tramite un apposito server di identificazione dedicato a tale scopo.

Tali operazioni sono effettuate e verificate esclusivamente in presenza di operatori di sportello BNL.

2.2 Operazioni Di Sottoscrizione

Le operazioni di sottoscrizione con FEA sono possibili solo dopo che il soggetto firmatario è stato identificato da un mezzo di identificazione sotto il controllo esclusivo del firmatario (token crittografico, dispositivo biometrico di identificazione, **OTP** [3] ecc.) consegnato esclusivamente dopo il censimento (registrazione dei dati identificativi presenti nel certificato **X.509**) al soggetto firmatario stesso.

Nessun dispositivo di identificazione non censito da BNL e non associato ai dati identificativi del firmatario da una Autorita' di Registrazione riconosciuta da BNL è utilizzabile ai fini di apporre una firma **FEA.**

Il soggetto firmatario, e titolare del dispositivo di identificazione associato ai dati del certificato, può richiedere (in caso di smarrimento o incidenti che ne compromettano il controllo e la disponibilità esclusiva da parte del titolare stesso) la revoca del consenso all'utilizzo della

[1] Standard ITU-T per le infrastrutture a chiave pubblica (PKI). X.509 definisce, fra le altre cose, formati standard per i certificati a chiave pubblica, certificati di attributo ed un certification path validation algorithm

[2] Dati comportamentali del modello grafometrico utilizzato quali ad es. ritmo, pressione, velocità, accelerazione, movimento, etc..

[3] Password (One Time Password) crittograficamente generata e utilizzabile una singola volta per una singola operazione

soluzione di FEA.

La operazione di revoca comporta la inutilizzabilità di QUALSIASI dispositivo di identificazione ai fini della esecuzione di operazioni di Firma Elettronica Avanzata fino alla eventuale riemissione di un nuovo certificato abilitato.

In fase di attuazione delle operazioni di Firma Elettronica Avanzata, e esclusivamente dopo le operazioni di identificazione e autorizzazione, il dispositivo **LDBU** provvede a registrare la operazione e i dati di identificazione e autorizzazione e a richiedere l'utilizzo della chiave privata di firma al dispositivo **HSM** che è l'unico ad avere tale chiave.

Il dispositivo **LDBU** è l'unico dispositivo connesso al dispositivo **HSM** e è quindi l'unico dispositivo a poter effetturare tale operazione.