Servizio di Firma Elettronica Avanzata

BMW Bank GmbH – Succursale Italiana

Caratteristiche tecniche e conformità

Il presente documento, (il "***Documento***") è redatto da BMW Bank GmbH – Succursale Italiana (in seguito "***BMW Bank***") al fine di adempiere alle prescrizioni imposte dal Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013, denominato *"Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2 e 71"* (in seguito "**DPCM**").

In particolare, il Documento ha l'obiettivo di descrivere le caratteristiche del sistema di Firma Elettronica Avanzata (in seguito "**FEA**" o "***Soluzione di FEA***") realizzato in conformità agli artt. 55 e successivi del DPCM e le soluzioni tecnologiche adottate, adempiendo dunque *inter alia* agli obblighi imposti dall'articolo 57 comma 1 lett. e) ed f) del DPCM.

In conformità a quanto disposto dall'articolo 57 comma 1 lett. g) questo documento è pubblicato sul sito internet di BMW Bank.

1) Firma Elettronica Avanzata

La firma elettronica avanzata è stata introdotta nel nostro ordinamento dal decreto legislativo 30 dicembre 2010, n. 235 di modifica del D. Lgs n. 82/2005, c.d. "Codice dell'Amministrazione Digitale" (in seguito "***CAD***"), che ha inserito una nuova definizione alla lettera q-bis) dell'articolo 1 del CAD: *"insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati".*

L'articolo 21 comma 2 del CAD stabilisce che *"il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, che garantiscano l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento, ha l'efficacia prevista dall'articolo 2702 del codice civile."* In base all'articolo 21 comma 2-bis del CAD, "*le scritture private di cui all'articolo 1350, primo comma, numeri da 1 a 12 del Codice Civile, se fatte con documento informatico sono sottoscritte a pena di nullità, con firma elettronica qualificata o con firma digitale. Gli atti di cui all'articolo 1350, numero 13, del Codice Civile soddisfano comunque il requisito della forma scritta se sottoscritti con firma elettronica avanzata, qualificata o digitale".*

2) Soggetti della soluzione di Firma Elettronica Avanzata

BMW Bank, per il tramite dei Concessionari BMW propri incaricati, è il soggetto che eroga la Soluzione di FEA per i propri clienti ai sensi dell'art. 55 comma 2 lettera a) ed art. 56 comma 1

lettera f), mentre Sefin S.p.A ed itAgile Srl sono i soggetti che hanno realizzato la soluzione di FEA erogata da BMW Bank ai sensi dell'art. 55 comma 2 lettera b).

Ai sensi dell'art. 60 del DPCM, i documenti firmati con la Soluzione di FEA possono essere utilizzati limitatamente ai rapporti giuridici intercorrenti tra il soggetto sottoscrittore e BMW Bank.

BMW Bank è dotata di adeguata copertura assicurativa per la responsabilità civile secondo quanto previsto dall'art. 57 comma 2 del DPCM. In particolare BMW Bank ha sottoscritto con la Società ACE EUROPE una polizza assicurativa con massimale pari a € 500.000.

3) Infrastruttura tecnologica di FEA

Al fine di adempiere ai requisiti imposti dal CAD e dal DPCM con riferimento alla firma elettronica avanzata, e in particolare ai requisiti imposti dall'articolo 56 del DPCM la Soluzione di FEA adottata da BMW Bank si avvale dell'infrastruttura tecnologica del servizio *cloud* di firma elettronica Qualified CoSign Cloud realizzato e gestito da ItAgile Srl.

Il servizio Qualified CoSign Cloud viene usato sia per la firma elettronica qualificata (remota o automatica) come definita dall'articolo 1 comma 1 lett. r) del CAD (la "***Firma Elettronica Qualificata***") sia per le soluzione di firma elettronica avanzata come definita dall'articolo 1 comma 1 lett. q-bis) del CAD ed è costituito da una infrastruttura PKI ad alta sicurezza basata sugli HSM CoSign ed ospitata nella server farm di Aruba.

Gli HSM CoSign sono dotati di certificazione di sicurezza Common Criteria EAL4+, la server farm di Aruba dotata di una certificazione di sicurezza 27001 (in allegato le certificazioni).

I requisiti di sicurezza soddisfatti dal servizio Qualified CoSign Cloud sono quelli richiesti dalla Firma Elettronica Qualificata. Per questo gli apparati HSM CoSign - opportunamente ridondati per assicurare la necessaria continuità di servizio - hanno la certificazione di sicurezza Common Criteria EAL4+ (il "***Certificato***") e l'attestato di conformità ai requisiti di sicurezza per la firma elettronica richiesti dalla normativa europea ("***Attestato***") e integrano ampiamente i requisiti di sicurezza richiesti dal DPCM per la firma elettronica avanzata.

La Certificazione e l'Attestato sono stati ottenuti in Italia presso OCSI (Organismo per la Certificazione della Sicurezza Informatica presso il Ministero dello Sviluppo Economico).

Al fine di garantire per la Firma Elettronica Avanzata il pieno rispetto dei requisiti di sicurezza dettati dall'art. 56 comma 1 del DPCM, sono state replicate le medesime caratteristiche tecnologiche e di sicurezza già adottate per la Firma Elettronica Qualificata.

4) Caratteristiche del sistema di FEA

Ai sensi dell'articolo 56 comma 1 del DPCM, le soluzioni di firma elettronica avanzata garantiscono:

(a) l'identificazione del firmatario del documento;

(b) la connessione univoca della firma al firmatario;

(c) il controllo esclusivo del firmatario del sistema di generazione della firma;

(d) la possibilità di verificare che il documento informatico sottoscritto non abbia subito modifiche dopo l'apposizione della firma;

(e) la possibilità per il firmatario di ottenere evidenza di quanto sottoscritto;

(f) l'individuazione del soggetto di cui all'articolo 55 comma 2 lett. a) del DCM;

(g) l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello stesso rappresentati;

(h) la connessione univoca della firma al documento sottoscritto.

La Soluzione di FEA adottata da BMW Bank risponde ai requisiti imposti dall'articolo 56 del DPCM e sopra elencati, in quanto:

(i) colui che intende avvalersi della Soluzione di FEA al fine di sottoscrivere un documento con BMW Bank (il ***"Firmatario***") viene previamente identificato presso un concessionario BMW autorizzato (il "***Concessionario BMW***") tramite un valido documento di riconoscimento e informato dei termini e delle condizioni e limitazioni relative all'uso del servizio;

(ii) il Firmatario al fine di poter utilizzare la Soluzione di FEA è tenuto a sottoscrivere, su supporto cartaceo, un'apposita dichiarazione di accettazione delle condizioni di utilizzo del servizio di firma elettronica avanzata;

(iii) il Firmatario può prendere visione completa dei documenti da sottoscrivere tramite apposita APP eseguita sull'iPAD del Concessionario BMW prima di procedere e durante la il processo di sottoscrizione;

(iv) al momento della sottoscrizione il sistema Qualified CoSign Cloud genera, per l'utente di firma un certificato di firma X509 valido per un tempo limitato ed invia al cellulare del firmatario un SMS contenente un codice One Time Password che il Firmatario deve riportare sull'applicazione per completare il processo di firma. Le firme generate sono di tipo PAdES;

(v) al termine delle operazioni di firma il certificato e le relative chiavi vengono cancellate dal sistema (certificato ONE SHOT). L'utilizzo del OTP tramite SMS consente di garantire il controllo esclusivo dello strumento di firma;

(vi) il servizio Qualified CoSign Cloud registra in modo formale tutte le operazioni di generazione e relativa distruzione dei certificati. Ogni giorno al file di log di queste operazioni viene apporta una marca temporale. Viene quindi garantita l'integrità e la data certa di queste registrazioni;

(vii) in conformità a quanto previsto dall'articolo 56 comma 1 lettera d) del DPCM e al fine di garantire l'integrità dei documenti informatici, in termini di non modificabilità ed inalterabilità del loro contenuto i documenti vengono sottoscritti in formato PDF. Nel caso un documento venga modificato, anche solo minimamente, all'apertura dello stesso verrà visualizzato un messaggio che indica che il documento è stato modificato in data posteriore all'apposizione della firma stessa. Tale processo garantisce, sotto il profilo tecnico, l'integrità del documento e dunque, sotto il profilo giuridico, soddisfa il requisito dell'integrità richiesto dalle norme vigenti.

Al termine della sottoscrizione tramite FEA da parte del Cliente, i documenti sono inoltre soggetti alla sottoscrizione da parte di incaricati della BMW Bank tramite l'apposizione di una firma digitale.

(viii) al termine delle operazioni di firma il Firmatario potrà avere evidenza del documento sottoscritto che gli verrà inviato in formato PDF via mail all'indirizzo indicato dal Firmatario stesso. Il Firmatario, inoltre potrà richiedere di ottenere copia cartacea del documento sottoscritto;

5) Conservazione e accesso ai documenti

Secondo quanto disposto dall'art. 57 comma 1 lettere b) e c), BMW Bank conserva tutta la documentazione relativa alla Soluzione di FEA per il tempo previsto dalla legge e comunque per almeno 20 anni, garantendone la disponibilità, integrità, leggibilità e autenticità.

Su richiesta scritta del Firmatario, da inviare all'indirizzo email contactcenter.it@bmw.it oppure all'indirizzo di posta elettronica certificata ("***PEC***"): info.bmwcic@bmwcert.it, BMW Bank fornisce al Firmatario: (i) la copia della dichiarazione di accettazione delle condizioni generali di utilizzo della Soluzione di FEA sottoscritta da quest'ultimo, (ii) ulteriori informazioni in merito alla polizza assicurativa sottoscritta da BMW Bank, e (iii) ogni altra informazione in possesso di BMW Bank atta a dimostrare l'ottemperanza a quanto previsto dall'articolo 56 comma 1 del DPCM.

BUREAU VERITAS
Certification

Allegato al Certificato di Conformità
N° IT257061/A

ARUBA SPA

Sede Legale:
Località Palazzetto, 4 – 52011 BIBBIENA (AR)

Bureau Veritas Italia spa certifica che il sistema di gestione dell'organizzazione sopra indicata è stato valutato e giudicato conforme ai requisiti della norma di sistema di gestione seguente

Norma

ISO 9001:2008

Elenco Siti

Siti	Scopo
SITO OPERATIVO: Via Gobetti, 96 52100, AREZZO (AR)	Progettazione, sviluppo ed erogazione di software e servizi di: - Data Center (Server Dedicati, Server Virtuali, Housing, Hosting) - Soluzioni Cloud oriented in modalità IaaS, SaaS e PaaS - Posta elettronica convenzionale e certificata (PEC) - Firma digitale e firma qualificata, firma grafometrica e altre soluzioni tecnologiche di firma elettronica avanzata, firma remota, servizi di Certification Authority - Infrastrutture a chiave pubblica PKI o attinenti alla sicurezza informatica - Conservazione digitale sostitutiva - Backup e Disaster Recovery - Consulenza in ambito ICT e relativa assistenza specialistica anche tramite Call Center. Produzione e personalizzazione di carte a microprocessore (Smart Card). Commercializzazione, installazione ed assistenza di prodotti hardware e software attinenti alla sicurezza informatica. Emissione e gestione di "Identità Digitale" e delle relative credenziali di autenticazione per l'accesso ai servizi "SPID" in qualità di Identity Provider

3/3

Rev. N. 3 del: **11 aprile 2016**

ANDREA FILIPPI – Local Technical Manager

Indirizzo dell'organismo di certificazione:
Bureau Veritas Italia S.p.A., Via Miramare, 15 - 20126 Milano, Italia

ACCREDIA
L'ENTE ITALIANO DI ACCREDITAMENTO

Ulteriori chiarimenti sul campo di applicazione di questo certificato e sui requisiti applicabili della norma del sistema di gestione possono essere ottenuti consultando l'organizzazione.
Per controllare la validità di questo certificato consultare il sito www.bureauveritas.it

SGQ	N° 009A	PRS	N° 076C
SGA	N° 008D	SGE	N° 009M
PRD	N° 009B	EMAS	N° 004P
SCR	N° 008F	GHG	N° 008O
FSMS	N° 003I	ISP	N° 006E

Membro degli Accordi di Mutuo Riconoscimento EA e IAF
Signatory of EA and IAF mutual Recognition Agreements

BUREAU VERITAS
Certification

ARUBA SPA

Sede Legale:
Loc. Palazzetto, 4 – 52011 BIBBIENA (AR)

Certificato multisito. Il dettaglio dei siti è nell'appendice di questo certificato.

Bureau Veritas Italia Spa certifica che il sistema di gestione dell'organizzazione sopra indicata è stato valutato e giudicato conforme ai requisiti della norma di sistema di gestione seguente

Norma

ISO/IEC 27001:2013

Campo di applicazione

Progettazione, sviluppo ed erogazione di software e servizi di: Data Center (Server Dedicati, Server Virtuali, Housing, Hosting), Soluzioni Cloud oriented in modalità IaaS, SaaS e PaaS, Posta elettronica convenzionale e certificata (PEC), Firma digitale e firma qualificata, firma grafometrica e altre soluzioni tecnologiche di firma elettronica avanzata, firma remota, servizi di Certification Authority e personalizzazione di carte a microprocessore (Smart Card), Conservazione digitale sostitutiva, Backup e Disaster Recovery e relativa assistenza specialistica. Gestione e manutenzione di server, postazioni di lavoro, reti informatiche e relativi apparati e sistemi di sicurezza logica. Emissione e gestione di "Identità Digitale" e delle relative credenziali di autenticazione per l'accesso ai servizi "SPID" in qualità di Identity Provider..

DICHIARAZIONE DI APPLICABILITA': Rev. 1.1 del 26/02/2016

Settore/i EA di attività **33**

Data d'inizio del presente ciclo di certificazior**10 giugno 2016**

Soggetto al continuo e soddisfacente mantenimento del sistema di gestione questo certificato è valido fino al: **9 aprile 2018**

Data della certificazione originale: **10 aprile 2012**

Certificato NIT268394 Rev. N. **1** del: **10 giugno 2016**

ACCREDIA
ENTE ITALIANO DI ACCREDITAMENTO

SGQ	N° 009A	SGE	N° 009M
SGA	N° 008D	EMAS	N° 004P
PRD	N° 009B	GHG	N° 008O
SCR	N° 008F	ISP	N° 0016
FSMS	N° 0031	SSI	N° 013G
PRS	N° 076C		

Membro degli Accordi di Mutuo Riconoscimento EA e IAF
Signatory of EA and IAF mutual Recognition Agreements

ANDREA FILIPPI - Local Technical Manager

Indirizzo dell'organismo di certificazione:
Bureau Veritas Italia S.p.A., Via Miramare, 15 , 20126 Milano, Italia

Ulteriori chiarimenti sul campo di applicazione di questo certificato e sui requisiti applicabili della norma del sistema di gestione possono essere ottenuti consultando l'organizzazione.
Per controllare la validità di questo certificato consultare il sito www.bureauveritas.it

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. 1/17

Dispositivo: CoSign v8.2

Sviluppato da: ARX

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 Rita Forsi)

Roma, 7 febbraio 2017

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/ARX/01/2017/RA) ad esso allegato, che ne costituisce parte integrante e sostanziale.