Microsoft Corporation
Japan Parameter Sheet
Cryptographic Features
Microsoft Global Trade Compliance
Date issued: 21 November 2013

Windows Server 2008 R2

Version 6.1

暗号関連パラメータシート（日本）
マイクロソフト・グローバル・トレード・コンプライアンス

The cryptographic set of capabilities of the Windows Server 2008 R2 family of products is identical across the product line.

This parameter sheet applies to all editions of Windows Server 2008 R2:

Windows Server 2008 R2 Standard
Windows Server 2008 R2 Enterprise
Windows Server 2008 R2 Datacenter
Windows Server 2008 R2 Foundation
Windows Web Server 2008 R2
Windows Server 2008 R2 HPC Edition
Windows HPC Pack 2008 R2 Express
Windows HPC Pack 2008 R2 Enterprise
Windows HPC Pack 2008 R2 for Workstation
Windows HPC Server 2008 R2 Suite
Windows Server 2008 R2 for Itanium-Based Systems
Hyper-V Server 2008 R2
Windows Storage Server 2008 R2

And the corresponding Microsoft Embedded Server products:

Windows Server® 2008 R2 for Embedded Systems - Essentials
Windows Server® 2008 R2 for Embedded Systems - Telecommunications

1. 暗号機能 / Cryptographic Capabilities

暗号機能は認証、デジタル署名又は複製することを防止されたプログラムの実行以外の目的を有するか。 The cryptographic capabilities are for purposes other than certification, digital signature, or execution of a copy-protected program.	☐ NO	☒ YES

暗号機能は本製品に搭載されているものか。[1] The cryptographic capabilities are self-contained in the product	☐ NO	☒ YES
暗号機能は次のいずれかに該当するものか。 The cryptographic strength exceeds the following: A. 対称アルゴリズムを用いたものであって、アルゴリズムの鍵の長さが 56 ビットを超えるもの Symmetric algorithms with key length exceeding 56 bit B. 非対称アルゴリズムを用いたものであって、 (a) 512 ビットを超える整数の素因数分解（RSA 等）に基づくもの、 Asymmetric algorithms based on factorization of integers in excess of 512 bits (e.g. RSA), or (b) 有限体の乗法群における 512 ビットを超える離散対数の計算（Diffie-Hellman 等）に基づくもの、 Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g. Diffie-Hellman), or (c) 上記に規定するもの以外の群における 112 ビットを超える離散対数の計算（楕円曲線上の Diffie-Hellman 等）に基づくもの Discrete logarithms in a group other than (B.b) in excess of 112 bits (Diffie-Hellman over Elliptic Curve).	☐ NO	☒ YES

2. アルゴリズム及び鍵長 / Algorithms and Key Lengths

アルゴリズム/ Algorithm	鍵長/ Key Length	プロトコル/アプリケーション/コメント Protocol/Application/Comment
CYLINK MEK	40	CryptoAPI
RC2, RC4	40-128	CryptoAPI/CNG
DES, 3DES	56, 168	CryptoAPI/CNG
AES	128, 192, 256	CryptoAPI/CNG
MD2, MD4, MD5	128	CryptoAPI/CNG
SHA-1, SHA-2	160, 256, 384, 512	CryptoAPI/CNG
RSA	512-16384	CryptoAPI/CNG
DH	1024-4096	CryptoAPI/CNG
HMAC-SHA1, HMAC-SHA2	160, 256, 384, 512	CryptoAPI/CNG
DSA_SIGN	1024	CryptoAPI/CNG

[1] API を通じて OS から提供される場合は除く。/As opposed to that provided by the Operating System through API.

ECDH		NIST P-256, P-384, P-521 curves, CryptoAPI/CNG
ECDSA		NIST P-256, P-384, P-521 curves, CryptoAPI/CNG
GMAC		AES Galois message authentication code, CryptoAPI/CNG
PRNG		CTR_DRBG (« Counter » Deterministic Random Bit Generation) of NIST SP 800-90.

3. 市販暗号プログラム該当性 / Mass Market Consideration

製品が以下の要件を満たすものかどうか。(The product satisfies the following requirements):

1) 購入に際して何らの制限を受けず、(i) 店頭において(ii) 又は郵便、信書便(iii) 若しくは電気通信の送信による注文により、販売店の在庫から販売されるもの又は使用者に対し何ら制限なく無償で提供されるもの Generally available to the public by being sold, without restriction, from stock at retail selling points by means of (i) over-the-counter transactions, (ii) mail order transactions, (iii) telecommunication transactions, or available free without restriction;	☐ NO	☒ YES
2) 暗号機能が使用者によって変更できないもの The cryptographic functionality cannot easily be changed by the user ;	☐ NO	☒ YES
3) 使用に際して供給者又は販売店の技術支援が不要であるように設計されているもの Designed for use without technical support by the supplier or the distributor	☐ NO	☒ YES

4. 該非判定 / Conclusion

上記 3.に照らして、市販暗号プログラムと判断される結果、適用法上、規制非該当となるプログラムか。 In light of 3 above, is the software a mass-market crypto program that is not controlled under applicable law?	☐該当 NO	☒非該当 YES