Microsoft Corporation
Japan Parameter Sheet

Cryptographic Features
Microsoft Global Trade Compliance
Date issued: 17 October 2023

Azure Stack Edge

Version 2.0

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

This parameter sheet applies to Azure Stack Edge, version 2.0 and all its previous versions, as well as to all declinations and editions of the product such as:

Azure Stack Edge Pro
Azure Stack Edge Pro 2
Azure Stack Edge Pro R
Azure Stack Edge Mini 2

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）	☐ NO	☒ YES

[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.

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), or (d) 格子に関連する最短ベクトル又は最近接ベクトル問題（NewHope、Frodo、NTRUEncrypt、Kyber、Titanium 方式を含む。）に基づくもの Shortest vector or closest vector problems associated with lattices (e.g., NewHope, Frodo, NTRUEncrypt, Kyber, Titanium), or (e) 超特異楕円曲線の同種写像の探索（超特異同種写像鍵カプセルを含む。）に基づくもの Finding isogenies between Supersingular elliptic curves (e.g., Supersingular isogeny Key Encapsulation), or (f) ランダムな符号の復号（McEliece、Niederreiter 方式を含む。）に基づくもの Decoding random codes (e.g., McEliece, Niederreiter).		

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
RSA	2048	TPM 2.0 RSA • encrypt job secrets exchanged between SaaS Service and Azure Stack Edge Appliance • encrypt Bitlocker key that is persisted on Azure Stack Edge Appliance used to unlock data drives SFTP/SSH used for server key authentication
AES	256	Bitlocker XTS AES 256 • Encrypt OS Boot drive (uses TPM only key protector)

		Encrypt Data drives where customer data is stored (uses external key protector)
TLS	Varied	TLS 1.2 (1.1, 1.0) Default is 1.2 used for all HTTPS traffic over the network. Note HTTP is not supported.
AES	128	SMB 3.0 use AES-CCM. SMB 3.1 and higher uses ASE-GCM • Used to read customer data from Azure Stack Edge Appliance and upload to customer's Azure storage account Optionally used at customer site to copy data onto the Azure Stack Edge Appliance
NTLMv2	Customer chosen	Used to login to Azure Stack Edge Appliance. Note the Azure Stack Edge Appliance is a stand-alone system, and these creds are only valid to login to the Azure Stack Edge Appliance and no other system (not even another Azure Stack Edge Appliance).
RC4	128-bit	OpenClusterCryptProvider using PROV_RSA_FULL Encrypts secrets stored in the cluster database on the Azure Stack Edge Appliance
SHA1	160-bit	SHA1 is used for TPM commands that uses SHA1
SHA256	256-bit	SHA256 is used for TPM commands that support SHA256
RNGCryptoServiceProvider	256-bit	Used for cryptographic random 256-bit key
RMCP + Authenticated Key Exchange Protocol (RAKP)	96-bit or 160-bit	Used for key exchange to secure the channel for IPMI commands issued to BMC

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	☐ NO	☒ YES

Designed for use without technical support by the supplier or the distributor		

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