Visa Business News

Processing

23 July 2020

Visa File Exchange Service Key Exchange Key Algorithm for SSH and Session Connection Cipher Changes

Global | *Acquirers, Issuers, Processors, Agents*

Visa Network

Overview: To meet Payment Card Industry Security Standards Council (PCI SSC) compliance commitments and maintain high standards of system security, Visa will be upgrading the Visa File Exchange Service (VFES) platform to utilize stronger key exchange key algorithms and session connection cipher suites, while concurrently decommissioning older and less secure algorithms and TLS cipher suites effective 21 October 2020. Clients must ensure that their systems are ready or updated to support new requirements in order to successfully connect to the VFES platform once these changes are in effect.

The VFES platform that Visa provides to clients is designed to enable the safe and secure transfer of files from Visa's host systems to clients' host systems and vice versa. It is the primary file delivery channel used for critical files and reports related to card processing and settlement exchanged between Visa and all clients.

Mark Your Calendar:

- VFES key exchange key algorithm (SSH) and session connection ciphers (TLS) will be decommissioned **(21 October 2020)**

VFES provides the following connectivity options:

- File Transfer Protocol over SSL (FTP/S)
- File Transfer Protocol over SSH (SFTP)
- HyperText Transfer Protocol Secure (HTTPS)
- Connect:Direct Secure+

Changes to **ONLY** the **SFTP** option are outlined below, and **will take effect on 21 October 2020**. Clients using this connectivity option in VFES must ensure that their systems are updated to include and **use** one of the supported key exchange key algorithms and TLS session connection ciphers specified in this document.

SFTP—SSH Key Exchange Key Algorithms

Current SSH Key Exchange Key Algorithms That Will Continue To Be Supported as of 21 October 2020	Current SSH Key Exchange Key Algorithms No Longer Supported as of 21 October 2020
• Diffie-Hellman-Group14-SHA1 • Diffie-Hellman-Group-Exchange-SHA256	• Diffie-Hellman-Group1-SHA1

Note: Clients currently using a 1024 bit KEK for VFES access must request a new 2048 bit KEK from Visa.

SFTP—TLS Cipher Changes

Current TLS Session Connection Ciphers That Will Continue To Be Supported as of 21 October 2020	Current TLS Session Connection Ciphers No Longer Supported as of 21 October 2020
• aes128-cbc: AES with 128-bit key • aes128-ctr: AES in CTR mode with 128-bit key • aes192-cbc: AES with 192-bit key • aes192-ctr: AES in CTR mode with 192-bit key • aes256-cbc: AES (Rijndael) in CBC mode, with 256-bit key • aes256-ctr: AES (Rijndael) in CTR mode, with 256-bit key	• 3des-cbc: three-key 3DES in CBC mode, with 168-bit key (effective 112-bit) • blowfish-cbc: Blowfish in CBC mode, with 128-bit key

Clients' systems currently utilizing VFES that are not updated to support the above requirements **by 21 October 2020** will not be able to establish connectivity with Visa's VFES platform and will not be able to transmit or receive files and reports. Clients' systems already updated with the supported key exchange key algorithms and TLS cipher suites and clients that make the necessary changes to their systems will be able to view their changes in the Visa certification environment, which has already been updated to support the new requirements.

For More Information

Merchants and third party agents should contact their acquirer.