Modification of the File Delivery Services-Platform (FDS)

Bern, June 2024

Security

To improve the protection of customers and Post data, the following technical adjustments will be implemented on the FDS platform on **August 24, 2024**:

- Key exchange method by means of « **diffie-hellman-group14-sha1**» will be deactivated.
- The encryption algorithm "**aes128-ctr**" will be deactivated.
- The MAC "**hmac-sha1**" will be deactivated.

We would request you to please review your file transfer software and to modify it accordingly if applicable. Provided that your software supports modern cipher suites, our modifications will not have any impact on your usage of the FDS platform.

Should any issues arise when establishing a connection to the FDS platform after our modifications, verify that your file transfer software supports the following cryptographic techniques (it is essential to support at least one for each category):

Key Exchange Methods	Encryption Algorithm	MAC Protection
curve25519-sha256	aes256-ctr	hmac-sha2-256
curve25519-sha256@libssh.org	aes256-gcm@openssh.com	hmac-sha2-512
diffie-hellman-group18-sha512	aes192-ctr	
diffie-hellman-group17-sha512		
diffie-hellman-group16-sha512		
diffie-hellman-group15-sha512		
diffie-hellman-group-exchange-sha256		

Further information and questions

Technical questions
FDS Operations
fds@post.ch

Security
I InfoSec
infosec@post.ch

Post CH AG
Informatik
Webergutstrasse 12
3030 Bern (Zollikofen)

E-Mail fds@post.ch