24.5.2023

OHJELMISTOTALOTIEDOTE 2/2023

TLS salausprotokollan vanhojen versioiden tuki päättyy

Aineistosiirtokanavamme osoitteessa ws.samlink.fi tukee edelleen heikkoja salausprotokollia ja -algoritmeja. Lopetamme tuen heikoille salausmenetelmille 2.6.2023. Teemme tämän, jotta pystymme paremmin varmistamaan riittävät, turvalliset ja toimintavarmat tietojärjestelmät. Muutos koskee kaikkia Samlinkin asiakaspankkeja (Säästöpankit, POP Pankit, OmaSp, Handelsbanken, Aktia) ja heidän asiakkaitaan.

Tuki vanhentuneille salausmenetelmille on ollut tarpeen, koska osa pankkien asiakkaista käyttää edelleen pankkiyhteysohjelmistoja, jotka muodostavat yhteytensä vanhentuneilla salausmenetelmillä. Tuen lopettaminen tarkoittaa, että kyseisten asiakkaiden on päivitettävä pankkiyhteysohjelmistonsa ajantasaiseen versioon.

Tulevaisuudessa tuemme aineistosiirtokanavassa seuraavia salausmenetelmiä:

- TLS13-AES128-GCM-SHA256/TLS1.3
- TLS13-AES256-GCM-SHA384/TLS1.3
- ECDHE-RSA-AES128-GCM-SHA256/TLS1.2
- ECDHE-RSA-AES256-GCM-SHA384/TLS1.2
- ECDHE-ECDSA-AES256-GCM-SHA384/TLS1.2

Vanhojen versioiden tuki siis loppuu 2.6.2023.

Lisätietoja: Samlink Service desk, info@samlink.fi.

Terveisin
Oy Samlink Ab

samlink
A Kyndryl Company

24.5.2023

SOFTWARE HOUSE RELEASE 2/2023

End of support for old versions of the TLS encryption protocol

Our data transfer channel at ws.samlink.fi still supports weak encryption protocols and algorithms. We will end support for weak encryption methods on 2.6.2023. We are doing this to better ensure adequate, secure and reliable information systems. The change will apply to all Samlink's client banks (Savings Banks, POP Banks, OmaSp, Handelsbanken, Aktia) and their customers.

Support for obsolete encryption methods has been necessary because some of the banks' customers still use banking connection software that establish their connections using obsolete encryption methods. Ending this support means that these customers will have to upgrade their banking software to the latest version.

In the future, we will support the following encryption methods in the data transfer channel:

TLS13-AES128-GCM-SHA256/TLS1.3
TLS13-AES256-GCM-SHA384/TLS1.3
ECDHE-RSA-AES128-GCM-SHA256/TLS1.2
ECDHE-RSA-AES256-GCM-SHA384/TLS1.2
ECDHE-ECDSA-AES256-GCM-SHA384/TLS1.2

Support for old versions will therefore end on 2.6.2023.

For additional information please contact the Samlink Service desk, info@samlink.fi.

Best regards
Oy Samlink Ab