TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

TLS cipher suitet turvallisuusluokille IV -III

NCSA-toiminto, ncsa@traficom.fi

Yleistä

Tässä dokumentissa on mainittu ne TLS-protokollan cipher suitet, jotka täyttävät kansalliset kryptografiset vähimmäisvaatimukset turvallisuusluokille IV-III.

Turvallisuusluokitellun tiedon välittäminen TLS:llä edellyttää vaatimusten mukaisen cipher suiten lisäksi kansallisesti hyväksytyn järjestelmän käyttöä sen käyttöpolitiikan mukaisesti. Hyväksytyn suiten käyttäminen ei yksinään takaa järjestelmän hyväksyntää.

TL IV –hyväksytyt TLS cipher suitet

DH- ja signature-ryhmät:

- DHE:lla ja RSA:lla vähintään 3072-bittinen ryhmä
- ECDHE:lla ja ECDSA:lla vähintään 256-bittinen käyrä (P-256, P-384 tai P-521)

TLS 1.2 Cipher suitet (OpenSSL:n käyttämillä nimillä):

- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-CHACHA20-POLY1305
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-CHACHA20-POLY1305
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305

TL IV –hyväksytyt TLS cipher suitet

TLS 1.3

Vaatimukset DH-ryhmille ja signature-ryhmille kuten TLS 1.2:n tapauksessa

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_CCM_SHA256

0-RTT ei ole hyväksytty käyttöön.

TL III –hyväksytyt TLS cipher suitet

DH- ja signature-ryhmät:

- DHE:lla ja RSA:lla vähintään 7680-bittinen ryhmä
- ECDHE:lla ja ECDSA:lla vähintään 384-bittinen käyrä (P-384 tai P-521)

TLS 1.2 Cipher suitet:

- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES256-SHA384

- DHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384

TL III –hyväksytyt TLS cipher suitet

TLS 1.3 Cipher suitet:

④ TLS_AES_256_GCM_SHA384

0-RTT ei ole hyväksytty käyttöön.