# Hyväksyttävät salausalgoritmimääritykset järjestelmille, jotka eivät ole kansallisesti turvallisuusluokiteltuja

**Hyväksytyt protokollat:**

- TLS 1.2
- TLS 1.3

**Hyväksytyt avaimet:**

- ECDHE, min 256 bit
- DHE, min 2048 bit
- ECC, suositeltavat käyrät: BrainpoolP256r1, BrainpoolP384r1, BrainpoolP512r1, NIST Curve P-224, NIST Curve P-256, NIST Curve P-384 ja NIST Curve P-521.

**Hyväksytyt allekirjoitusavaimet:**

- ECDSA, min 256 bit
- RSA, min 2048 bit

**Symmetrinen salaus:**

- Salausalgoritmi: AES128 tai AES256
  Salausmoodi: GCM

**Tiivistefunktio:**

- SHA-256
- SHA-384
- SHA-512
- SHA-3

**Esimerkisi** (OpenSSL CipherSuite):

```
DHE-RSA-AES256-GCM-SHA384
ECDHE-ECDSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-GCM-SHA256
```