SEMOpx Info – 11 January 2022

# ETS API Security Updates – Old Cipher Suites Decommission

## Important information – Action required

- Decommission of old cipher suites:
  - in SIMU2 end of January,
  - in PROD and SIMU1 end of February 2022 (exact date to be confirmed in a separate communication)

Dear API Clients,

We are pleased to inform you about the upcoming ETS API security updates for 2022.

## 1 ETS API Security Updates Roadmap

### 1.1 Cipher Suites Decommission

As previously announced, the following cipher suites will be decommissioned soon:
- On 31 January 2022 in SIMU2,
- End of February in SIMU1 and PROD (the exact date will be confirmed in a separate communication).

| Cipher suites | Status<br>31 January in SIMU2 | Status<br>End of February in SIMU1 and PROD |
|---|---|---|
| • TLS_RSA_WITH_AES_128_CBC_SHA256 | Decommissioned | Decommissioned |
| • TLS_RSA_WITH_AES_256_CBC_SHA256 | Decommissioned | Decommissioned |
| • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | Supported | Supported |
| • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | Supported | Supported |
| • TLS_RSA_WITH_AES_256_GCM_SHA384 | Decommissioned | Decommissioned |
| • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | Supported | Supported |
| • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | Supported | Supported |
| • TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 | Decommissioned | Decommissioned |
| • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | Supported | Supported |
| • TLS_RSA_WITH_AES_128_GCM_SHA256 | Decommissioned | Decommissioned |
| • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 | Supported | Supported |

ETS 3.5 API logs enabled us to identify the few customers that were using “old” cipher suites in PROD.
If this is your case, you should have received in December a bilateral email from our Market Operations team about this and be aware of the change to perform.

Whether you received a bilateral email from Market operations or not, we invite you to double check in early February that your API application can still connect to SIMU2 once old cipher suites are removed, to ensure you are ready for the decommission end of Q1 in PROD.

Note: no TLS change will take place before ETS API 3.6:

- Supported TLS versions in API 3.5:
  - v1.0, v1.1 (still supported)
  - v1.2 (recommended)

## 1.2 ETS API 3.6 – Old TLS Decommission End of Q2 2022

- Supported TLS versions:
  - v1.0, v1.1 NOT supported anymore
  - v1.2 supported
- List of supported/decommissioned cipher suites (unchanged):

| **Cipher suites** | **ETS API 3.6** in Q2 2022 |
|---|---|
| • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | Supported |
| • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | Supported |
| • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | Supported |
| • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | Supported |
| • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | Supported |
| • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 | Supported |