## TC046

# Jaarlijkse update cipher suites - 2021

| Heeft het issue impact op..? | |
|---|---|
| Grootverbruik | x |
| Kleinverbruik | x |
| Elektriciteit | x |
| Gas | x |
| RNB | x |
| LNB | x |
| LV | x |
| MV | x |
| PV | x |
| EDSN | x |
| Codes | |
| Berichten | |
| Ketenprocessen | |
| Privacy | |
| **Is het issue release afhankelijk/onafhankelijk en welke invoeringsdatum heeft het issue.** | |
| Release-afhankelijk | |
| Release-onafhankelijk | x |

**Nummer** TC046
**Datum** 30-09-2020
**Versie** 0.4
**Status** Vastgesteld ALV NEDU

**Opsteller(s)** Eline Spauwen (TC)

# Inhoudsopgave

# Colofon

## Versiebeheer

| Versie | Status | Wijziging | Auteur | Datum |
|---|---|---|---|---|
| 0.1 | Concept | Eerste opzet | Eline Spauwen | 20-08-2020 |
| 0.2 | Concept - ter goedkeuring TC en SC | Review en input van Gerrit Fokkema verwerkt | Eline Spauwen | 27-08-2020 |
| 0.3 | Ter vaststelling ALV | Goedkeuring door SC, TC met kleine redactionele wijzigingen | Eline Spauwen | 17-09-2020 |
| 0.4 | Vastgesteld ALV NEDU | | | 30-09-2020 |
| | | | | |
| | | | | |

## Distributie

| Gremium | Verstuurd (versie/datum) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | 0.1 | 0.2 | 0.3 | 0.4 | | | | | | |
| TC | | 27-08-2020 | | | | | | | | |
| SC | | 27-08-2020 | | | | | | | | |
| SPC | | | 17-09-2020 | | | | | | | |
| ALV NEDU | | | 22-09-2020 | 30-09-2020 | | | | | | |
| Allen | | | | | | | | | | |
| | | | | | | | | | | |

# 1 Probleemdefinitie

| Onderdeel | Omschrijving |
|---|---|
| Het probleem betreft: | Het gebruik van onveilige cipher suites voor de beveiliging (via TLS) van de verbindingen in ketenprocessen |
| En raakt: | Alle met TLS beveiligde verbindingen tussen marktpartijen die gebruikt worden voor ketenprocessen |
| Als gevolg waarvan: | De beveiligingsgraad onder druk staat |
| Een goede oplossing moet: | Een lijst cipher suites opleveren die voldoende veilig zijn |
| Of deze doelen worden behaald, kan worden gevalideerd door: | Jaarlijks de lijst cipher suites te evalueren (SC en TC) |
| Opdrachtgever te realiseren oplossing | NEDU |
| Probleemeigenaar | Technische Commissie |

# 2 Overwegingen

### 2.1 Afspraak jaarlijkse update en relatie TLS1.3

In TC037 “Beheer van cipher suites” is een proces afgesproken om in gebruik zijnde cipher suites te evalueren en onveilige cipher suites uit productie te nemen. In dit proces heeft de Security Commissie de taak om de cipher suites te evalueren en de Technische Commissie om onveilige cipher suites uit productie te laten nemen. Dit heeft geleid tot issues TC038 (2018) en TC042 (2019) met jaarlijkse updates.

In 2019 was de veronderstelling dat de invoering van TLS1.3 binnen afzienbare tijd (1 á 2 jaar) gepland en uitgevoerd zou worden, waarmee het jaarlijks updaten van de lijst toegestane cipher suites via issues overbodig zou worden, omdat TLS1.3 dit op een andere manier al regelt.

Tijdens het inventariseren van de status quo en readiness voor TLS1.3 is al geconstateerd dat de invoering later zal plaatsvinden dan verwacht (op moment van schrijven is de verdere aanpak nog niet vastgesteld).

Daarom heeft de Security Commissie opnieuw de set toegestane cipher suites geëvalueerd en een advies gegeven aan de Technische Commissie voor de lijst voor 2021, als opvolger van TC042. De TC neemt in dit issue het advies van de SC over.

### 2.2 Afspraak PKI-Overheid

1. Afspraak in TC027: de hele sector werkt onder PKI Overheid private root.
2. Logius heeft verklaard dat tot medio 2019 onder PKI Overheid alleen type RSA zijn toegestaan, maar dat daarna ook beveiligingscertificaten met elliptische curve cryptografie worden toegestaan. De providers zullen de nieuwe certificaten nog wel moeten kunnen uitgeven alvorens deze gebruikt kunnen worden, hetgeen waarschijnlijk eind 2020 het geval zal zijn.

### 2.3 Cipher suites met RSA voor sleuteluitwisseling

1. Er is een dringend advies van de NCSC om geen RSA te gebruiken voor sleuteluitwisseling, deze cipher suites zouden dus moeten vervallen. Dit zijn de cipher suites die (in de in onderstaande Tabel 1) met prio 3 & 4 worden aangeduid. (Vaak wordt RSA niet gebruikt in het eerste deel van de naam maar is deze impliciet aanwezig. Voor ondertekening mag RSA wel gebruikt worden, deze staat dan verderop in de naam).
2. Indien dit advies gevolgd wordt dan zouden er slechts 2 toegestane cipher suites overblijven, namelijk de suites met prio 1 & 2 in Tabel 2.
3. De voorgestelde oplossing is om het geheel afschaffen van RSA-gebruik voor sleuteluitwisseling uit te stellen, mede in afwachting van een (volledige) invoering van TLS1.3. Een van de cipher suites waarin RSA-versleuteling voor sleuteluitwisseling wordt gebruikt, wordt met dit issue niet langer toegestaan.

### 2.4 Lijst met advies uit vastgestelde TC042 voor 2020

| Cipher Group | Prio | TLS ID1 | TLS ID2 | CipherName | Name (OpenSSL) | Cipher Suite Name (RFC) |
|---|---|---|---|---|---|---|
| Goed | **1** | **0xc030** | **0xC0 0x30** | **TLS(1.2)-ECDHE-RSA-AES256-GCM-SHA384** | **ECDHE-RSA-AES256-GCM-SHA384** | **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** |
| | **2** | **0xc02f** | **0xC0 0x2F** | **TLS(1.2)-ECDHE-RSA-AES128-GCM-SHA256** | **ECDHE-RSA-AES128-GCM-SHA256** | **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** |
| Matig | 3 | 0x9d | 0x00 0x9D | TLS(1.2)-AES256-GCM-SHA384 | AES256-GCM-SHA384 | TLS_RSA_WITH_AES_256_GCM_SHA384 |
| | 4 | 0x9c | 0x00 0x9C | TLS(1.2)-AES128-GCM-SHA256 | AES128-GCM-SHA256 | TLS_RSA_WITH_AES_128_GCM_SHA256 |

*In de drie rechtse kolommen zijn de verschillende schrijfwijzen gegeven.*
*Identificatie vindt plaats via het TLS ID, hier zijn twee methodes voor, aangegeven als TLS ID1 resp. TLS ID2. In een aantal gevallen worden voor TLS ID1 zes posities gebruikt door op te vullen met voorloopnul(len); bijv.: '0x9d' = '0x009d'.*

Let op: De Prio is geen vaste nummering van de cipher suites, dit is de voorkeursvolgorde zoals die aangeboden dient te worden door de software.

# 3 Gekozen oplossing

### 3.1 TLS cipher suites advies 2021

Gebaseerd op de bevindingen en adviezen van het Nationale Cyber Security Centrum[1] adviseert de SC de onderste suite in de lijst voor 2020 vanaf 1-1-2021 niet meer te gebruiken in de met TLS beveiligde verbindingen.
Uit een recente meting op het berichtenverkeer op het C-AR Portaal, die de SC heeft laten uitvoeren, blijkt dat deze laatste suite niet of nauwelijks meer wordt gebruikt, waarmee uitfasering geen groot obstakel hoeft te vormen.

In volgorde van security en algemeen gebruik geldt dan:

**Tabel 2 – Cipher suites advies voor 2021:**

| Cipher Group | Prio | TLS ID1 | TLS ID2 | CipherName | Name (OpenSSL) | Cipher Suite Name (RFC) |
|---|---|---|---|---|---|---|
| Goed | **1** | **0xc030** | **0xC0 0x30** | **TLS(1.2)-ECDHE-RSA-AES256-GCM-SHA384** | **ECDHE-RSA-AES256-GCM-SHA384** | **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** |
| | **2** | **0xc02f** | **0xC0 0x2F** | **TLS(1.2)-ECDHE-RSA-AES128-GCM-SHA256** | **ECDHE-RSA-AES128-GCM-SHA256** | **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256** |
| Matig | 3 | 0x9d | 0x00 0x9D | TLS(1.2)-AES256-GCM-SHA384 | AES256-GCM-SHA384 | TLS_RSA_WITH_AES_256_GCM_SHA384 |
| ~~Slecht~~ | **4** | ~~0x9c~~ | ~~0x00 0x9C~~ | ~~TLS(1.2)-AES128-GCM-SHA256~~ | ~~AES128-GCM-SHA256~~ | ~~TLS_**RSA**_WITH_AES_128_GCM_SHA256~~ |

*In de drie rechtse kolommen zijn de verschillende schrijfwijzen gegeven.*
*Identificatie vindt plaats via het TLS ID, hier zijn twee methodes voor, aangegeven als TLS ID1 resp. TLS ID2. In een aantal gevallen worden voor TLS ID1 zes posities gebruikt door op te vullen met voorloopnul(len); bijv.: '0x9d' = '0x009d'.*

[1] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls

Let op: De Prio is geen vaste nummering van de cipher suites, dit is de voorkeursvolgorde zoals die aangeboden dient te worden door de software.

Geadviseerd wordt om de cipher suites ook in bovenstaande volgorde aan te bieden, op deze manier begint de connectie altijd met de beste cipher suite en kan dan in volgorde van prioriteit terugvallen.

# 4 Impact

Partijen beperken de toegestane cipher suites tot de hierboven voorgestelde set voor de systemen betrokken bij de ketenprocessen. In de centrale systemen wordt het gebruik van de te verwijderen cipher suite geblokkeerd. Een quick scan heeft uitgewezen dat deze suite al niet meer door veel partijen wordt gebruikt

Afhankelijk van de uitkomst van de mogelijkheid om ECDSA (met elliptische curve cryptografie) te kunnen ondersteunen met bijbehorende certificaten op de centrale systemen kan deze mogelijkheid actief gemaakt worden in betreffende ketencommunicatie.

# 5 Invoeringsstrategie

| | **Release onafhankelijk** | **Release afhankelijk** |
|---|---|---|
| **Na vaststelling ALV NEDU** | | |
| **Sectorrelease** | | |
| **Specifieke datum** | 15 januari 2021 | |

# 6 Te vervallen issues

Geen.
NB: Dit issue is een update op TC042 in zoverre dat het de gewenste situatie in 2021 beschrijft.