TC042

Jaarlijkse update cipher suites

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 TC042
Datum 03-07-2019
Versie 1.0
Status Vastgesteld ALV NEDU

Opsteller(s) Wim de Olde (TC)

Inhoudsopgave

Colofon

Versiebeheer

Versie	Status	Wijziging	Auteur	Datum
0.1	Concept	Eerste opzet	Wim de Olde	16-01-2019
0.2	Concept	Aanpassingen nav commentaar TC	Wim de Olde	25-01-2019
0.3	Concept	Herzien en aanpassingen nav commentaar SC	Wim de Olde	23-04-2019
0.4	Ter goedkeuring Goedgekeurd in TC 24-05-2019	Aanpassingen nav review	Wim de Olde / Gerrit Fokkema / Eline Spauwen	16-05-2019
0.9	Ter vaststelling	Ophoging versienummer	Eline Spauwen	17-06-2019
1.0	Vastgesteld ALV NEDU			03-07-2019

Distributie

Gremium	Verstuurd (versie/datum)									
	0.1	0.2	0.3	0.4	0.9	1.0				
TC	25-01-2019	10-04-2019		17-05-2019	17-06-2019					
SC		10-04-2019			17-06-2019					
SPC				14-06-2019						
ALV NEDU					25-06-2019	03-07-2019				
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

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. Hieronder is kort de ontwikkeling tot nu toe aangegeven.

2.1 TC038 v3.0, d.d. 23-05-2018

Tabel 1: Advies voor 2019:

Cipher Group	Prio	TLS ID1	TLS ID2	CipherName	Name (OpenSSL)	Cipher Suite Name (RFC)
Goed	**1**	**0xc02c**	**0xC0 0x2C**	**TLS(1.2)-ECDHE-ECDSA-AES256-GCM-SHA384**	**ECDHE-ECDSA-AES256-GCM-SHA384**	**TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**
	2	**0xc02b**	**0xC0 0x2B**	**TLS(1.2)-ECDHE-ECDSA-AES128-GCM-SHA256**	**ECDHE-ECDSA-AES128-GCM-SHA256**	**TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256**
	3	**0xc030**	**0xC0 0x30**	**TLS(1.2)-ECDHE-RSA-AES256-GCM-SHA384**	**ECDHE-RSA-AES256-GCM-SHA384**	**TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384**
	4	**0xc02f**	**0xC0 0x2F**	**TLS(1.2)-ECDHE-RSA-AES128-GCM-SHA256**	**ECDHE-RSA-AES128-GCM-SHA256**	**TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256**
	5	0x9d	0x00 0x9D	TLS(1.2)-AES256-GCM-SHA384	AES256-GCM-SHA384	TLS_RSA_WITH_AES_256_GCM_SHA384
	6	0x9c	0x00 0x9C	TLS(1.2)-AES128-GCM-SHA256	AES128-GCM-SHA256	TLS_RSA_WITH_AES_128_GCM_SHA256
Tijdelijk in 2019	7	0x9f	0x00 0x9F	TLS(1.2)-DHE-RSA-AES256-GCM-SHA384	DHE-RSA-AES256-GCM-SHA384	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
	8	0x9e	0x00 0x9E	TLS(1.2)-DHE-RSA-AES128-GCM-SHA256	DHE-RSA-AES128-GCM-SHA256	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
Matig	*9*	*0xc024*	*0xC0 0x24*	*TLS(1.2)-ECDHE-ECDSA-AES256-SHA384*	*ECDHE-ECDSA-AES256-SHA384*	*TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*
	10	*0xc023*	*0xC0 0x23*	*TLS(1.2)-ECDHE-ECDSA-AES128-SHA256*	*ECDHE-ECDSA-AES128-SHA256*	*TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256*
	11	*0xc028*	*0xC0 0x28*	*TLS(1.2)-ECDHE-RSA-AES-256-SHA384*	*ECDHE-RSA-AES256-SHA384*	*TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384*
	12	*0xc027*	*0xC0 0x27*	*TLS(1.2)-ECDHE-RSA-AES-128-SHA256*	*ECDHE-RSA-AES128-SHA256*	*TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256*
	13	0x3d	0x00 0x3D	TLS(1.2)-AES-256-SHA256	AES256-SHA256	TLS_RSA_WITH_AES_256_CBC_SHA256
	14	0x3c	0x00 0x3C	TLS(1.2)-AES-128-SHA256	AES128-SHA256	TLS_RSA_WITH_AES_128_CBC_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 volgorde zoals die aangeboden wordt door de software.

Per 1-1-2019 worden alleen nog de cipher suites 1 t/m 8 toegestaan.

2.2 Tijdens invoering van TC038: RFC038.1, d.d. 12-10-2018

1. De tijdelijke Cipher Suites met Prio 7&8 bleken in de bouw problemen te geven voor de systemen P4, TMR en de hub Nexus. Naar aanleiding hiervan is door NEDU een Market Readiness uitvraag gedaan onder haar leden en de ODA's. Uit de representatieve resultaten is gebleken dat niemand gebruik wil maken van de tijdelijke Cipher Suites.
2. Bij de Dry Run bleek dat de Cipher Suites met prio 1 &2 type ECDSA niet werkten. Door NEDU is i.s.m. EDSN onderzoek gedaan wat de root cause is: het bleek dat er andere beveiligingscertificaten met elliptische curve cryptografie voor deze suites te worden toegepast dan de huidige beveiligingscertificaten - die daar dus niet geschikt voor zijn.
3. TC038 bleek niet in lijn met de vastgestelde en geïmplementeerde TC027 waarin wordt beschreven dat de hele sector werkt onder PKI Overheid private root.
4. 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 2019 het geval zal zijn.

Tabel 2: TC038, na goedkeuring RFC038.1 , hierin worden alleen de volgende suites ondersteund *in de centrale systemen*:

Cipher Group	Prio	TLS ID1	TLS ID2	CipherName	Name (OpenSSL)	Cipher Suite Name (RFC)
	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**
	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 volgorde zoals die aangeboden wordt door de software.

2.3 CBC cipher suites en DHE-keys

CBC cipher suites, zoals voor 2019 al is afgesproken in TC038 ("Matig" / geel in TC038), zijn in 2020 niet meer toegestaan.
De Diffie Helman keys (DHE) worden nog voldoende veilig geacht (tijdelijk toegestaan in 2019, in grijs weergegeven in TC038 v3.0), echter worden ze niet ondersteund in de centrale systemen (RFC038.1). Deze zijn in 2020 niet meer toegestaan.

2.4 Cipher suites met RSA voor sleuteluitwisseling

1. Er is een dringend advies is om geen RSA te gebruiken voor sleuteluitwisseling, deze cipher suites zouden dus moeten vervallen. Dit zijn de cipher suites die

in de in Tabel 2 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 oplossing is om het afschaffen van RSA-gebruik voor sleuteluitwisseling uit te stellen en de huidige 4 cipher suites voorlopig te behouden, mede in afwachting van een overgang op TLS1.3, waarbinnen andere cipher suites en beveiligingscertificaten worden gebruikt.
4. De Security Commissie is van mening dat uitstel van het afschaffen van RSA-gebruik voor sleuteluitwisseling beperkt moet worden in de tijd tot (maximaal) twee jaar. Daarnaast beveelt de SC aan om monitoring te starten op het gebruik van deze minst veilige cipher suites (met prio 3 & 4 in Tabel 2) en het gebruik daarvan actief te ontmoedigen.

3 Gekozen oplossing

3.1 TLS 1.2 cipher suites advies 2020

Het advies van de TC is om de huidige sets met ECDHE en GCM cipher suites te blijven gebruiken.

In volgorde van security en algemeen gebruik geldt dan:

Tabel 3 – 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 volgorde zoals die aangeboden wordt 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.

3.1.1 Aanbeveling

Tevens ziet de SC graag dat er voor de centrale communicatiesystemen wordt onderzocht of het mogelijk is om al transparant naast de bestaande suites ook cipher suites en digitale certificaten met elliptische curve cryptografie te ondersteunen en zo mogelijk dit ook in te voeren. Dit geeft partijen de mogelijkheid om al eerder over te gaan op cipher suites en digitale certificaten met elliptische curve cryptografie, waarmee de beveiligingsrisico's verder worden gemitigeerd.

Betreffende cipher suites (met prio 1 &2 uit de originele Tabel 1):

0xc02c	0xC0 0x2C	TLS(1.2)-ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE-ECDSA-AES256-GCM-SHA384	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
0xc02b	0xC0 0x2B	TLS(1.2)-ECDHE-ECDSA-AES128-GCM-SHA256	ECDHE-ECDSA-AES128-GCM-SHA256	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

3.1.2 TLS1.3

In de (nabije) toekomst zal worden overgegaan naar TLS 1.3, hierover legt de Security Commissie (SC) een besluit aan de ALV voor. Op basis van een dergelijk besluit kan de impact en planning en wijze van invoering van TLS1.3 onderzocht worden door de TC. Partijen wordt gevraagd om te anticiperen op de invoering van TLS1.3, met name bij wijzigingen in hun ICT landschap/systemen.

3.1.3 Referenties

https://testssl.sh/openssl-rfc.mapping.html
https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml
https://www.openssl.org/docs/manmaster/man1/ciphers.html
https://www.cloudinsidr.com/content/known-attack-vectors-against-tls-implementation-vulnerabilities/
https://www.cloudinsidr.com/content/tls-1-3-and-tls-1-2-cipher-suites-demystified-how-to-pick-your-ciphers-wisely/
https://www.thesslstore.com/blog/bleichenbachers-cat-rsa-key-exchange/

4 Impact

Partijen beperken de cipher suites tot de hierboven voorgestelde set (zoals ook goedgekeurd in TC038 v3 met RFC038.1) voor de systemen betrokken bij de ketenprocessen.
Het voorstel is om het gebruik van cipher suites te monitoren en op basis daarvan conclusies te trekken en mogelijk de gebruikte cipher suites te beperken tot de voldoende veilige set.
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	X	
Sectorrelease		
Specifieke datum		

6 Te vervallen issues

Geen.
NB: Dit issue is een update op TC038 & RFC038.1 in zoverre dat het de gewenste situatie in 2020 beschrijft.
Inhoudelijk wijzigt dit issue de toegestane cipher suites niet t.o.v. TC038+RFC038.1.