Baarnsche Dijk 4 D
3741 LR Baarn
www.edsn.nl
T (035) 54 80 180
F (035) 54 80 184

NEDU
Nederlandse Energie Data Uitwisseling

Issue TC024 Overgang op TLS1.2

Status	Vastgesteld door ALV		
Versienummer	2.0	**Versiedatum**	14 december 2015
Documentnaam	TC024 Overgang op TLS1.2 v2.0		

Behandeld door de Technische Commissie

Raakt aan	Kleinverbruik	Grootverbruik	Wholesale
Elektriciteit	**X**	**X**	**X**
Gas	**X**	**X**	**X**

Impact op keten	Ja/Nee
Codewijziging	**Nee**
Berichten	**Nee**
Ketenprocessen	**Nee**

Mogelijke impact marktrollen en EDSN	Ja/Nee
LV	**Ja**
PV	**Ja**
MV	**Ja**
RNB	**Ja**
LNB	**Ja**
EDSN	**Ja**

Vastgesteld door NEDU op 1 april2015
Invoering in markt uiterlijk 1 juni 2016

Contact	
Technische Commissie	TC@edsn.nl

TC024: Overgang op TLS1.2

Managementsamenvatting

Op het gebied van beveiligingsstandaarden volgt de sector de overheidsrichtlijnen zo veel mogelijk.
De recent ingevoerde situatie waarbij SSLv3 uitgezet is en minimaal TLS1.0 gebruikt mag worden krijgt een vervolg met de invoering van TLS1.2. De overheid heeft als regel uitgevaardigd over te gaan op minimaal TLS 1.2 (op de lijst voor 'pas toe of leg uit'). De ondersteuning voor het TLS 1.2 protocol is echter nog niet aanwezig in alle software die door de marktpartijen gebruikt wordt. Partijen moeten dus bewust gemaakt worden van dit feit en zullen voldoende tijd moeten krijgen om de systemen te updaten. De stap van SSLv3 naar TLS1.0 is naar verwachting qua (software) inspanningen een kleinere dan naar TLS1.2.

TLS is een protocol dat tot doel heeft om beveiligde verbindingen over het internet te verzorgen.
TLS 1.2 geldt als een, aan de huidige veiligheidseisen voldoende ,upgrade van de voorganger SSL.

Situatieschets:

Ondanks het feit dat de sector pas in 2014 volledig overgaat/is gegaan op het gebruik van minimaal TLS1.0 is dit een reeds verouderde versie, waar gekende tekortkomingen in zitten. De overheid heeft als regel uitgevaardigd over te gaan op minimaal TLS 1.2 (op de lijst voor 'pas toe of leg uit'). De overgang naar TLS 1.2 is een grotere stap dan van SSL naar TLS 1.0, het TLS 1.2 protocol moet ondersteund worden in alle software die door de marktpartijen gebruikt wordt. Er moeten dus upgrades ingepland worden door een aantal marktpartijen, dit issue creëert bewustwording en tijd voor implementatie.

Vraag:

Gezien het principe de overheidsrichtlijnen voor beveiligingsstandaarden te volgen wanneer wil de sector een veiliger versie van TLS afdwingen, ergo minimaal verbindingen beveiligen met TLS1.2.
Hierbij kan aangetekend worden dat we geen 'early adopter' willen zijn en dat het risico vs. implementatie-inspanning afgewogen wordt.

Overwegingen

De sector heeft medio 2014 als minimale eis TLS1.0 geïntroduceerd als beveiligingsprotocol voor de verbindingen.
TLS1.0 is van 1999 en kent een aantal tekortkomingen.
De overheidsrichtlijn is om TLS 1.2 te gebruiken tenzij ernstige redenen zijn om er van af te wijken (ref.: Expertadvies TLS v1.2 | Forum Standaardisatie | 12 februari 2014).
Oudere versies van standaard software ondersteunen TLS 1.2 niet (zoals Java 6, Oracle versies lager dan 11). Partijen zullen in hun releaseplanning moeten opnemen om tijdig te upgraden.
Voor nieuw in te voeren protocollen, zoals AS4, zal het gebruik van TLS 1.2 afgedwongen worden.

Oplossing:

Invoeren om minimaal TLS1.2 in de communicatie in de totstandkoming van de verbinding te hanteren per januari 2016, terugvallen op een lagere versie mag dan niet meer mogelijk zijn.

Waar gaat het inhoudelijk over?

TLS is een protocol, dat tot doel heeft om beveiligde verbindingen over het internet te verzorgen en wordt (in combinatie met andere standaarden) gebruikt in situaties waarin het van belang is om vast te kunnen stellen of men als gebruiker verbonden is met de juiste server of website, zodat persoonlijke of vertrouwelijke informatie kan worden uitgewisseld. De standaard wordt gebruikt bovenop standaard internet transport protocollen (TCP/IP) en biedt een beveiligde basis, waar applicatie protocollen als HTTP (webverkeer) of IMAP (mailuitwisseling) op hun beurt weer op kunnen bouwen en gebruik van kunnen maken.

TLS maakt gebruik van certificaten om zekerheid te bieden over de identiteit van beide communicerende partijen voordat communicatie plaatsvindt. Ook wordt met behulp van (het sleutelpaar van) de certificaten op betrouwbare wijze de encryptiesleutel uitgewisseld, die de standaard vervolgens gebruikt om met behulp van encryptietechniek beveiligde communicatie tussen partijen mogelijk te maken.

TLS wordt (in combinatie met andere standaarden) gebruikt in situaties waarin het van belang is om vast te kunnen stellen of men als gebruiker verbonden is met de juiste server of website, zodat persoonlijke of vertrouwelijke informatie kan worden uitgewisseld. De standaard biedt een veilige basis onder bijna alle denkbare internettoepassingen (internet browsing, mailuitwisseling, instant messaging, VoIP, etc.).

Functioneel betreft dit via certificaten beveiligen van gegevensuitwisseling tussen client- en serversystemen of tussen serversystemen onderling, voor zover deze gerealiseerd wordt met internet / IP technologie.

Impact:

Partijen die dat al kunnen, kunnen al eerder gebruik maken van TLS1.2 (maar mogen dit nog niet afdwingen): de software indien mogelijk zo instellen dat de hoogste beveiliging wordt gebruikt in de zogenaamde 'negotiation' fase (onderhandelen van hoog naar laag).

Een aantal partijen zal nog software upgrades moeten uitvoeren, de verwachting is dat dit binnen het reguliere update- en securitybeleid zal vallen waardoor de impact laag is gezien de tijdplanning.

Invoeringsstrategie:

Teneinde een verantwoorde invoeringsdatum te bepalen heeft de TC aan in overleg met de Sectorplanningscommissie een readiness/plannings uitvraag bij de marktpartijen gedaan. Op basis van de reacties beveelt de TC aan om de migratie op een nader door de SPC te bepalen datum in het voorjaar van 2016 te organiseren.

Partijen die al klaar zijn kunnen onderling TLS 1.2 gebruiken, dit wordt door de software zelf geregeld op basis van de 'negotiation' tussen systemen.

Voor het gebruik van de juiste algoritmes, cypher suites, hashing algoritmes, key exchange en encryptie mechanismen dient men zich te richten op de door ENISA goedgekeurde algoritmes en richtlijnen (deze worden periodiek vernieuwd).

Zie hiervoor:

Algorithms, Key Sizes and Parameters Report – 2014:
http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-size-and-parameters-report-2014

Study on cryptographic protocols:
http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/study-on-cryptographic-protocols

Te vervallen issues:

TC023 Beveiligde verbindingen (dan wel issue TC023 updaten naar minimaal TLS1.2).

Versieoverzicht:

0.1 eerste aanzet door Wim de Olde en Gerrit Fokkema op 9 april 2014;
0.2 .na bespreking in de TC van 25 april 2014;
0.3 enige aanscherpingen na review opmerkingen TC leden, 28 mei 2014;
0.4 na marktuitvraag met voorstel invoeringsmoment, 11 november 2014;
1.0 na vaststelling in de ALV vergadering van 15 januari 2015;
1.1 na bespreking in de TC van 6 maart 2016. de richtlijnen van ENISA voor te gebruiken technische versies toegevoegd;
1.2 vastgesteld in de ALV van 1 april 2015;
2.0 omnummering naar vol nummer op 14 december 2015.