

DIN EN 62351-3/A1



ICS 35.030; 35.240.50

Einsprüche bis 2018-07-11
Vorgesehen als Änderung von
DIN EN 62351-3:2015-06

Entwurf

Datenmodelle, Schnittstellen und Informationsaustausch für Planung und Betrieb von Energieversorgungsunternehmen – Daten- und Kommunikationssicherheit – Teil 3: Sicherheit von Kommunikationsnetzen und Systemen – Profile einschließlich TCP/IP (IEC 57/1976/FDIS:2018); Deutsche und Englische Fassung EN 62351-3:2014/FprA1:2018

Power systems management and associated information exchange –
Data and communications security –
Part 3: Communication network and system security – Profiles including TCP/IP
(IEC 57/1976/FDIS:2018);
German and English version EN 62351-3:2014/FprA1:2018

Gestion des systèmes de puissance et échanges d'informations associés –
Sécurité des communications et des données –
Partie 3: Sécurité des réseaux et des systèmes de communication – Profils comprenant TCP/IP
(IEC 57/1976/FDIS:2018);
Version allemande et anglaise EN 62351-3:2014/FprA1:2018

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2018-05-11 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 17 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Nationales Vorwort

Die Deutsche Fassung des europäischen Dokuments EN 62351-3:2014/FprA1:2018 „Datenmodelle, Schnittstellen und Informationsaustausch für Planung und Betrieb von Energieversorgungsunternehmen – Daten- und Kommunikationssicherheit – Teil 3: Sicherheit von Kommunikationsnetzen und Systemen – Profile einschließlich TCP/IP“, (Schluss-Entwurf) ist unverändert in diesen Norm-Entwurf übernommen worden.

Die Internationale Elektrotechnische Kommission (IEC) und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein bei IEC erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dem entsprechend ist das internationale Dokument IEC 57/1976/FDIS:2018 „Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP“ unverändert in den Schluss-Entwurf EN 62351-3:2014/FprA1:2018 übernommen worden.

Da die Deutsche Fassung noch nicht endgültig mit der Englischen und Französischen Fassung abgeglichen ist, ist die englische Originalfassung des IEC/FDIS entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigefügt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom TC 57 „Power systems management and associated information exchange“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet.

Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Für dieses Dokument ist das nationale Arbeitsgremium K 952 „Netzleittechnik“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. IEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

**Datenmodelle, Schnittstellen und Informationsaustausch für Planung und Betrieb
von Energieversorgungsunternehmen –
Daten- und Kommunikationssicherheit –
Teil 3: Sicherheit von Kommunikationsnetzen und Systemen – Profile einschließlich
TCP/IP**

2 Normative Verweisungen

Ersetze die vorhandene Verweisung IEC TS 62351-9 mit der folgenden neuen Verweisung:

IEC 62351-9, *Power systems management and associated information exchange – Data and communications security – Part 9: Key Management*

Ersetze die vorhandene Verweisung IEC/ISO 9594-8 mit der folgenden neuen Verweisung:

ISO/IEC 9594-8:2017, Rec. ITU-T X.509 (2016), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*

4.1 Operative Anforderungen, die die Nutzung von TLS in der Fernwirkumgebung beeinflussen

Ersetzung des vorhandenen Textes des fünften Absatzes von 4.1 durch den nachfolgenden neuen Text:

Zu beachten ist, dass TLS für die Authentifizierung X.509-Zertifikate verwendet (siehe ISO/IEC 9594-8 oder RFC 5280). In dieser Norm bezieht sich der Begriff „Zertifikate“ immer auf öffentliche Schlüsselzertifikate (im Gegensatz zu Attributzertifikaten).

4.2 Sicherheitsbedrohungen, denen entgegengewirkt wird

Ersetzung des vorhandenen Textes des zweiten Absatzes von 4.2 durch den nachfolgenden neuen Text:

TCP/IP und die Sicherheitsspezifikationen in diesem Teil der IEC 62351 gelten nur für die Kommunikationstransportschichten (OSI-Schichten 4 und darunter). Dieser Teil der IEC 62351 behandelt keine sicherheitsspezifischen Funktionen für die Kommunikationsanwendungsschichten (OSI-Schichten 5 und darüber) bzw. die Sicherheit von Anwendung zu Anwendung.

ANMERKUNG Die Anwendung von TLS entsprechend der Darstellung in diesem Dokument unterstützt den Schutz von Daten, die über die mit TLS geschützte Verbindung übertragen werden.

4.3 Angriffsverfahren, denen entgegengewirkt wird

Ersetzung des vorhandenen Textes des ersten Aufzählungspunktes von Unterabschnitt 4.3 durch den nachfolgenden neuen Text:

- Mittelsmann (en: man-in-the-middle): Dieser Bedrohung wird durch Benutzung eines Mechanismus mit Nachrichtenauthentifizierungscode oder digitalen Signaturen, der in diesem Dokument festgelegt ist, entgegengewirkt.

5.1 Missbilligung von Verschlüsselungssuiten

Einfügen des nachfolgenden Textes vor dem letzten Absatz von 5.1:

Die Unterstützung von SHA-1 dient der Rückwärtskompatibilität. SHA-256 muss unterstützt werden und ist der bevorzugt zu verwendende Signaturalgorithmus.

SHA-1 wird hinsichtlich der Kollisionssicherheit nicht mehr als sicher anerkannt; daher wird vor Nutzung dieses Algorithmus nachdrücklich eine Risikobewertung empfohlen. Falls SHA-256 nicht verwendet werden kann, ist es ebenfalls empfehlenswert, zusätzliche Sicherheitsmaßnahmen anzuwenden. Die Verwendung von SHA-1 wird in der nächsten Ausgabe dieser Norm untersagt werden.

ANMERKUNG Die Empfehlungen in Bezug auf Hash-Signatur-Algorithmen werden ständig überprüft und sind in NIST SP800-57, BnetZA (BSI) oder der NSA Suite B zu finden.

Ersetzung des letzten Absatzes von 5.1:

Die Liste der untersagten Suiten umfasst unter anderem:

- TLS_NULL_WITH_NULL_NULL
- TLS_RSA_WITH_NULL_MD5

5.2 Versionsaushandlung

Einfügen des folgenden neuen Textes am Ende von Unterabschnitt 5.2:

Der Vorschlag der Version TLS 1.0 oder TLS 1.1 sollte eine Sicherheitswarnung auslösen („Warnung: Unsichere TLS-Version“). Die Implementierungen sollten einen Mechanismus zum Melden von Sicherheitswarnungen enthalten.

5.3 Sitzungswiederaufnahme

Ersetzung des vorhandenen Textes von Unterabschnitt 5.3 durch den nachfolgenden neuen Text:

Die Sitzungswiederaufnahme in TLS berücksichtigt die Wiederaufnahme einer Sitzung basierend auf der Sitzungs-ID, verbunden mit einem dedizierten (bestehenden) geheimen Hauptschlüssel; dies resultiert in einem neuen Sitzungsschlüssel. Dies minimiert den Einfluss des asymmetrischen Quittungsbetriebes auf die Leistung und kann während einer laufenden Sitzung, oder nachdem eine Sitzung innerhalb eines festgelegten Zeitraumes geendet hat, durchgeführt werden (TLS schlägt im RFC 5280 nicht mehr als 24 h vor). Diese Norm folgt dieser Empfehlung. Die Sitzungswiederaufnahme sollte mindestens alle 24 Stunden bei aktiven Sitzungen und spätestens nach 24 Stunden bei beendeten Sitzungen erfolgen. Die tatsächlichen Parameter sollten auf Grundlage einer Risikobewertung anhand der verweisenden Norm definiert werden. Es ist zu erwarten, dass die Sitzungswiederaufnahme häufiger als die Sitzungsneuaushandlung auftritt.

Praktische Umsetzungen, die Übereinstimmung mit dieser Norm für sich beanspruchen, müssen festlegen, dass die symmetrischen Sitzungsschlüssel innerhalb des maximalen Zeitraums erneuert werden. Es ist zu erwarten, dass diese maximale Wiederaufnahmezeit in einem PIXIT (Zusatzinformationen zur Prüfung der Protokollimplementierung) der verweisenden Norm festgelegt wird. Der maximale Zeitraum bis zur Sitzungswiederaufnahme muss mit der Aktualisierungszeit der CRL abgestimmt sein.

Sitzungswiederaufnahmeintervalle müssen konfigurierbar sein, sofern sie innerhalb des festgelegten maximalen Zeitraumes liegen.

Clients müssen die Sitzungswiederaufnahme mittels der *ClientHello*-Nachricht initiieren. Eine vom Server initiierte Aktualisierung der Sitzungsparameter muss die *HelloRequest*-Nachricht verwenden, um den Client zum Senden einer *ClientHello*-Nachricht über die zu diesem Zeitpunkt aktive Verbindung zu veranlassen.

ANMERKUNG Gemäß RFC 5246 ist *HelloRequest* eine optionale Nachricht, die der Server an einen Client senden kann.

Die Sitzungswiederaufnahme kann durch jede der beiden Seiten initiiert werden, sofern sowohl die Sicherheitsrichtlinien des Clients als auch jene des Servers dies gestatten. Im Fall von Fehlschlägen bei der Wiederaufnahme einer Sitzung muss die in TLS v1.2 beschriebene Fehlerbehandlung befolgt werden.

Die Sitzungswiederaufnahme kann auf Grundlage des Sitzungsbezeichners (native TLS gemäß RFC 5246) erfolgen. Alternativ kann die Sitzungswiederaufnahme auf Grundlage von Sitzungstickets (RFC 5077) erfolgen. Die letztere Option ermöglicht die Vermeidung des serverseitigen Status bei Sitzungen, die wiederaufgenommen werden können. Diese Option kann für eingeschränkte Geräte gelten, um einen größeren Sitzungscache zu vermeiden.

ANMERKUNG Die Anwendung von Sitzungstickets zur Vermeidung der sitzungsspezifischen Speicherung auf Serverseite bietet einen Vorteil in Umgebungen, in denen eine Verbindung abgebrochen und nach einer angegebenen Zeit eine neue Verbindung aufgebaut wird. Wenn die Sitzungswiederaufnahme zur Aktualisierung des Sitzungsschlüssels einer laufenden Sitzung verwendet wird, ergibt sich möglicherweise kein Vorteil.

Der Ansatz der Sitzungswiederaufnahme kann durch die verweisende Norm angegeben werden.

5.4 Sitzungsneuaushandlung

Ersetzung des vorhandenen Textes des zweiten und dritten Absatzes von 5.4 durch den nachfolgenden neuen Text:

Sitzungsneuaushandlungsintervalle müssen konfigurierbar sein, sofern sie innerhalb des festgelegten maximalen Zeitraumes liegen, und müssen mit dem Aktualisierungszeitraum der CRL abgestimmt sein. Wenn das Online Certificate Status Protocol (OCSP) für Zertifikatssperrungsprüfungen verwendet wird, muss die Sitzungsneuaushandlung mit der OCSP-Antwortcache-Zeit abgestimmt werden. In jedem Fall muss die Neuaushandlung bei lang andauernden Verbindungen mindestens alle 24 Stunden durchgeführt werden, um die Überprüfung der Zertifikatgültigkeit zu erzwingen. Kürzere Intervalle dürfen durch die verweisende Norm festgelegt werden.

ANMERKUNG Ein Beispiel für eine Abstimmung ist $\frac{1}{2}$ CRL-Aktualisierungszeit oder $\frac{1}{2}$ OCSP-Antwortcache-Zeit zur Verringerung der Wahrscheinlichkeit nicht erkannter gesperrter Zertifikate.

Praktische Umsetzungen, die Übereinstimmung mit dieser Norm für sich beanspruchen, müssen festlegen, dass der geheime Hauptschlüssel innerhalb eines maximalen Zeitraums neu ausgehandelt wird. Es ist zu erwarten, dass diese maximale Neuaushandlungszeit in einem PIXIT (Zusatzinformationen zur Prüfung der Protokollimplementierung) der verweisenden Norm festgelegt wird.

Ersetzung des vorhandenen Textes des vierten Absatzes von 5.4 durch den nachfolgenden neuen Text:

TLS-Clients müssen die Sitzungsneuaushandlung mittels der *ClientHello*-Nachricht initiieren. Eine vom TLS-Server initiierte Aktualisierung der Sitzungsparameter muss die *HelloRequest*-Nachricht verwenden, um den TLS-Client zum Senden einer *ClientHello*-Nachricht über die zu diesem Zeitpunkt aktive Verbindung zu veranlassen.

ANMERKUNG Gemäß RFC 5246 ist *HelloRequest* eine optionale Nachricht, die der Server an einen Client senden kann.

Die Sitzungsneuaushandlung kann durch jede der beiden Seiten initiiert werden, sofern sowohl die Sicherheitsrichtlinien des Clients als auch jene des Servers dies gestatten. Im Fall von Fehlschlägen bei der Neuaushandlung einer Sitzung muss die in TLS v1.2 beschriebene Fehlerbehandlung befolgt werden.

Einfügen des folgenden neuen Absatzes nach dem vierten Absatz:

Die rufende Einheit ist für die Prüfung, dass die Neuaushandlung der TLS-Sitzung in den erwarteten Intervallen stattfindet, verantwortlich. Wenn die rufende Einheit in den erwarteten Intervallen keine Anforderung zur Neuaushandlung der TLS-Sitzung von der gerufenen Einheit erhält, muss die rufende Einheit die Verbindung abbrechen. Der Abbruch einer Verbindung aufgrund nicht erfolgter Sitzungsneuaushandlung sollte ein Sicherheitsereignis auslösen („Ereignis: Sitzungsneuaushandlungsintervall überschritten“). Die Implementierungen sollten einen Mechanismus zum Melden von Sicherheitsereignissen enthalten.

ANMERKUNG Es wird erwartet, dass Client und Server entsprechend derselben TLS-Sicherheitsrichtlinie konfiguriert sind.

5.5 Nachrichtenauthentifizierungscode

Einfügen des folgenden neuen Textes am Ende von 5.5:

Der spezifische Algorithmus wird durch die Verschlüsselungssuite vorgegeben.

5.6.1 Mehrere Zertifizierungsstellen (CAs) (en: Certificate Authorities)

Ersetzung des vorhandenen ersten Absatzes von 5.6.1 durch den nachfolgenden neuen Text:

Eine praktische Umsetzung, die Übereinstimmung mit dieser Norm für sich beansprucht, muss mehr als einen auf eine Zertifizierungsstelle bezogenen Sicherheitsanker unterstützen. Es ist zu erwarten, dass die tatsächliche Anzahl im PIXIT-Statement der Implementierung angegeben ist.

5.6.3 Zertifikataustausch

Ersetzung des vorhandenen Textes von Unterabschnitt 5.6.3 durch den nachfolgenden neuen Text:

Der Zertifikataustausch und die Validierung müssen bidirektional sein, um eine gegenseitige Authentifizierung zu erreichen. Die Verbindung muss beendet werden, falls eine Einheit ihr Zertifikat nicht zur Verfügung stellt.

ANMERKUNG Das Server-Zertifikat wird in der *ServerHello*-Nachricht übermittelt. Das Client-Zertifikat wird in der *Certificate*-Nachricht übermittelt.

Der Abbruch der Verbindung, falls eine Einheit ihr Zertifikat nicht zur Verfügung stellt, sollte ein Sicherheitsereignis auslösen („Ereignis: Zertifikat nicht erhalten“). Die Implementierungen sollten einen Mechanismus zum Melden von Sicherheitsereignissen enthalten.

ANMERKUNG Bevorzugt wird die Möglichkeit, sicherheitsrelevante Ereignisse aus der Ferne zu überwachen.

5.6.4.4 Zertifikatssperrung

Ersetzung des vorhandenen Textes von Unterabschnitt 5.6.4.4 durch den nachfolgenden neuen Text:

Die Zertifikatssperrung muss mit den verpflichtenden Parametern und entsprechend den Verfahren erfolgen, die in ISO/IEC 9594-8 vorgegeben werden.

Die Verwaltung der Zertifikatssperrliste (CRL) ist Angelegenheit der lokalen Implementierung. Die Diskussion über CRL betreffende Verwaltungsfragen ist in IEC TS 62351-1 zu finden. Um den Sperrstatus angewandter Zertifikate zu überprüfen, darf OCSP alternativ zu lokalen CRLs verwendet werden. Die Anwendung von OCSP ist in IEC 62351-9 umrissen.

Eine praktische Umsetzung, die Übereinstimmung mit dieser Norm für sich beansprucht, muss die lokale CRL in einem konfigurierbaren Intervall überprüfen können. Der CRL-Überprüfungsprozess darf nicht zum Beenden einer aufgebauten Sitzung führen. Eine Zugriffsunfähigkeit auf die CRL darf nicht das Beenden der Sitzung verursachen.

Gesperrte Zertifikate dürfen nicht für den Aufbau oder die Neuaushandlung einer TLS-Sitzung verwendet werden. Eine Einheit, die während des Sitzungsaufbaus ein gesperrtes Zertifikat empfängt, muss die Verbindung verweigern. Eine Einheit, die während des Sitzungsneuaushandlung ein gesperrtes Zertifikat empfängt, muss die Verbindung abbrechen.

Andere auf diese Norm verweisende Normen müssen empfohlene Standardevaluationsintervalle festlegen. Die verweisende Norm muss die Aktion festlegen, die vorgenommen werden muss, falls ein gegenwärtig verwendetes Zertifikat gesperrt wurde.

Es ist zu beachten, dass durch die normale Anwendung/Verteilung von CRL(s) Verbindungen beendet werden dürfen und folglich keine Kommunikation erfolgt. Daher sollten Systemadministratoren Prozeduren