

DIN EN 62351-3

ICS 35.040; 33.200

Einsprüche bis 2014-03-10

Entwurf

**Management von Systemen der Energietechnik und zugehöriger
Datenaustausch –
Daten- und Kommunikationssicherheit –
Teil 3: Sicherheit von Kommunikationsnetzen und Systemen – Profile
einschließlich TCP/IP
(IEC 57/1319/CDV:2013);
Deutsche Fassung FprEN 62351-3:2013**

Power systems management and associated information exchange –
Data and communications security –
Part 3: Communication network and system security – Profiles including TCP/IP
(IEC 57/1319/CDV:2013);
German version FprEN 62351-3:2013

Gestion des systèmes de puissance et échange d'informations associé –
Sécurité des communications de données –
Partie 3: Sécurité des réseaux et des systèmes de communication – Profils comprenant
TCP/IP
(CEI 57/1319/CDV:2013);
Version allemande FprEN 62351-3:2013

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2014-01-10 wird der Öffentlichkeit zur Prüfung und
Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de 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@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme 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 im DIN und VDE (Hausanschrift: 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 18 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Nationales Vorwort

Die Deutsche Fassung des europäischen Dokuments FprEN 62351-3:2013 „Management von Systemen der Energietechnik und zugehöriger Datenaustausch – Daten- und Kommunikationssicherheit – Teil 3: Sicherheit von Kommunikationsnetzen und Systemen – Profile einschließlich TCP/IP“ (Entwurf in der Umfrage) 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 auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und 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 57/1319/CDV:2013 „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 Entwurf FprEN 62351-3:2013 übernommen worden.

Da die Deutsche Fassung noch nicht endgültig mit der Englischen und Französischen Fassung abgeglichen ist, ist die englische Originalfassung des IEC-CDV 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.

Bei der Abstimmung zu dem Europäischen Schluss-Entwurf bei CENELEC und dem Internationalen Schluss-Entwurf bei IEC [Final Draft International Standard (FDIS)] sind jeweils nur „JA/NEIN“-Entscheidungen möglich, wobei „NEIN“-Entscheidungen fundiert begründet werden müssen. 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 im DIN und VDE (www.dke.de) zuständig.

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

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

Der Zusammenhang der zitierten Normen mit den entsprechenden Deutschen Normen 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.

**Management von Systemen der Energietechnik und zugehöriger Datenaustausch –
Daten- und Kommunikationssicherheit –
Teil 3: Sicherheit von Kommunikationsnetzen und Systemen – Profile einschließlich
TCP/IP**

Inhalt

	Seite
1 Anwendungsbereich und Zweck	2
1.1 Anwendungsbereich	2
1.2 Zweck	2
1.3 Zielgruppe	2
2 Normative Verweisungen	2
3 Begriffe und Abkürzungen	3
3.1 Definitionen und Abkürzungen	3
3.2 Zusätzliche Abkürzungen	3
4 Sicherheitsfragen im Sinne dieser Norm	3
4.1 Operative Anforderungen, die die Nutzung von TLS in der Fernwirkumgebung beeinflussen	3
4.2 Sicherheitsbedrohungen, denen entgegengewirkt wird	4
4.3 Angriffsverfahren, denen entgegengewirkt wird	4
5 Zwingende Anforderungen	4
5.1 Missbilligung unverschlüsselnder Verschlüsselungs-Suiten	4
5.2 Versionsaushandlung	5
5.3 Sitzungswiederaufnahme	5
5.4 Sitzungsneuaushandlung	5
5.5 Nachrichtenauthentifizierungscode	6
5.6 Zertifikatunterstützung	6
5.7 Koexistenz mit unsicherem Protokollverkehr	9
6 Unterstützung optionaler Sicherheitsmaßnahmen	9
7 TC 57-Anforderungen verweisender Normen	9
8 Übereinstimmung	9

1 Anwendungsbereich und Zweck

1.1 Anwendungsbereich

Dieser Teil von IEC 62351 legt fest, wie Vertraulichkeit, Sabotageerkennung und Authentifizierung auf Nachrichtenebene für SCADA und Fernwirkprotokolle, die TCP/IP als Nachrichtentransportschicht nutzen, vorgesehen werden kann.

Obwohl es mehrere mögliche Lösungen gibt, um TCP/IP zu schützen, liegt der besondere Anwendungsbereich dieses Teiles darin, für die Sicherheit zwischen den kommunizierenden Einheiten an jedem Ende einer TCP/IP-Verbindung innerhalb der kommunizierenden Einheiten zu sorgen. Die Benutzung und Festlegung dazwischenliegender externer Sicherheitseinrichtungen (z. B. „bump-in-the-wire“) fallen nicht in diese Norm.

1.2 Zweck

Dieser Teil von IEC 62351 legt fest, wie die auf TCP/IP basierenden Protokolle durch Nebenbedingungen, die für die Festlegung von Nachrichten, Prozeduren und von Algorithmen der Transportschichtssicherheit (en: Transport Layer Security – TLS) (festgelegt in RFC 5246) gelten, zu schützen sind, sodass sie für die Fernwirkumgebung nach IEC/TC57 anwendbar sind. Diese Norm sollte in anderen IEC/TC57-Normen als normativ in Bezug genommen werden, die für ihre auf TCP/IP basierenden Protokolle Sicherheit bieten müssen. Jedoch liegt die Entscheidung zur Bezugnahme auf diese Norm bei den einzelnen Protokollsicherheitsinitiativen.

Dieser Teil spiegelt die Sicherheitsanforderungen der IEC/TC57-Protokolle wider. Sollten andere Normen neue Anforderungen stellen, so kann eine Überarbeitung dieser Norm erforderlich sein.

1.3 Zielgruppe

Als erste Zielgruppe für diese Norm sind die Mitglieder der Arbeitsgruppen vorgesehen, die innerhalb von IEC/TC57 die Protokolle entwickeln oder anwenden. Damit die in dieser Norm beschriebenen Maßnahmen wirksam werden, müssen sie durch die Protokollspezifikationen selbst – wenn die Protokolle TCP/IP anwenden – akzeptiert und in Bezug genommen werden. Dieses Dokument wurde geschrieben, um diesen Prozess in Gang zu setzen.

Als anschließende Zielgruppe für diese Norm sind Produktentwickler vorgesehen, die diese Protokolle in die Praxis umsetzen.

Teile dieser Norm können auch für Manager und Führungskräfte hilfreich sein, um den Zweck und die Anforderungen der Arbeit zu verstehen.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

IEC 62351-8, *Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control*, September 2011

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

RFC 6176, *Prohibiting Secure Sockets Layer (SSL) Version 2.0*, S. Turner, T. Polk, March 2011

RFC 5746, *Transport Layer Security (TLS) Renegotiation Indication Extension*, E. Rescorla, M. Ray, S. Dispensa, N. Oskov, February 2010

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley

RFC 5246, *The TLS Protocol Version 1.2*, T. Dierks, E. Rescorla, August 2008¹

RFC 4492, *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)*; S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk, B. Moeller; May 2006

RFC 4366, *Transport Layer Security Extensions*, S. Blake-Wilson, M. Nystrom, D. Hopwood, J. Mikkelsen, T. Wright, April 2006

RFC 2712, *Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)*, A. Medvinsky, M. Hur, October 1999

3 Begriffe und Abkürzungen

3.1 Definitionen und Abkürzungen

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC 62351-2.

3.2 Zusätzliche Abkürzungen

ECDSA	digitaler Signatur-Algorithmus mit elliptischen Kurven (en: Elliptic Curve Digital Signature Algorithm)
ECGDSA	deutscher digitaler Signatur-Algorithmus mit elliptischen Kurven (siehe ISO/IEC 15946-2) (en: Elliptic Curve German Digital Signature Algorithm)
OCSP	Online-Zertifikat Status-Protokoll (siehe RFC 2560) (en: Online Certificate Status Protocol)

4 Sicherheitsfragen im Sinne dieser Norm

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

Die IEC/TC57-Fernwirkumgebung hat aufgrund zahlreicher Protokolle der Informationstechnik (IT), die TLS für den sicheren Schutz anwenden, eine Reihe unterschiedlicher operativer Anforderungen. Hinsichtlich der Sicherheit ist das wichtigste Unterscheidungsmerkmal die Dauer der TCP/IP-Verbindung, für die die Sicherheit aufrechterhalten werden muss.

Viele IT-Protokolle haben Verbindungen von kurzer Dauer, die eine Neuaushandlung der Verschlüsselungsalgorithmen bei einer Verbindungswiederherstellung zulassen. Jedoch tendieren die Verbindungen innerhalb einer Fernwirkumgebung dazu, länger zu dauern und bestehen oftmals „dauerhaft“. Die Langlebigkeit der IEC/TC57-Verbindungen macht die besondere Betrachtung notwendig. In dieser Hinsicht und um Vertraulichkeit der „dauerhaften“ Verbindungen vorzusehen, wird in dieser Norm ein Mechanismus zur Aktualisierung des Sitzungs-Verschlüsselungsschlüssels festgelegt, der auf TLS-Funktionen zur Sitzungs-wiederaufnahme und Sitzungsneuaushandlung beruht, wobei ebenfalls die Beziehung mit den Status-informationen zum Sperren von Zertifikaten berücksichtigt wird.

Ein anderes Thema, das in dieser Norm angesprochen wird, ist die Herstellung der Interoperabilität zwischen verschiedenen Implementierungen. TLS zieht eine Reihe von zu unterstützenden Verschlüsselungs-Suites in

¹ Dies wird typischerweise als SSL/TLS bezeichnet.

Betracht, die bei Verbindungsaufbau ausgehandelt werden. Es ist jedoch denkbar, dass zwei Implementierungen sich gegenseitig ausschließende Reihen von Verschlüsselungs-Suites unterstützen könnten. Diese Norm legt fest, dass verweisende Normen zumindest eine gemeinsame Verschlüsselungs-Suite und einen Satz von TLS-Parametern angeben müssen, die Interoperabilität gestatten.

Zusätzlich legt diese Norm die Benutzung von besonderen TLS-Leistungsmerkmalen fest, mit denen spezifischen Sicherheitsbedrohungen begegnet werden kann die es berücksichtigen spezifischen Sicherheitsbedrohungen entgegenzuwirken.

4.2 Sicherheitsbedrohungen, denen entgegengewirkt wird

Siehe IEC 62351-1 zur Diskussion von Sicherheitsbedrohungen und Angriffsverfahren.

TCP/IP und die Sicherheitsspezifikationen in diesem Teil gelten nur für die Kommunikationstransportschichten (OSI-Schichten 4 und darunter). Dieser Teil behandelt nicht die Sicherheit für die Kommunikationsanwendungsschichten (OSI-Schichten 5 und darüber) oder die Anwendung-zu-Anwendung-Sicherheit.

Die spezifischen Bedrohungen, denen in diesem Teil für die Transportschichten entgegengewirkt wird, beinhalten:

- unautorisierter Zugriff auf Informationen durch Authentifizierung auf Nachrichtenebene und Verschlüsselung der Nachrichten;
- unautorisierte Veränderung (Sabotage) oder Diebstahl von Informationen durch Authentifizierung auf Nachrichtenebene und Verschlüsselung der Nachrichten.

4.3 Angriffsverfahren, denen entgegengewirkt wird

Den folgenden Sicherheitsangriffsverfahren wird durch die entsprechende praktische Umsetzung der Spezifikationen und Empfehlungen in diesem Teil entgegengewirkt.

- Mittelsmann (en: man-in-the-middle): Dieser Bedrohung wird durch Benutzung eines Mechanismus mit Nachrichtenauthentifizierungscode, der in diesem Dokument festgelegt ist, entgegengewirkt.
- Wiedereinspielung (en: replay): Dieser Bedrohung wird durch Benutzung spezialisierter Prozessierungs-Zustandsmaschinen, die durch die normativen Verweisungen in diesem Dokument festgelegt sind, entgegengewirkt.
- Abhören (en: eavesdropping): Dieser Bedrohung wird durch Benutzung von Verschlüsselung entgegengewirkt.

ANMERKUNG Die tatsächlichen Gebrauchseigenschaften einer praktischen Umsetzung, die Übereinstimmung mit dieser Norm für sich beansprucht, fallen nicht in diese Norm.

5 Zwingende Anforderungen

5.1 Missbilligung unverschlüsselnder Verschlüsselungs-Suiten

Jegliche Verschlüsselungs-Suite, die NULL für die Verschlüsselung festlegt, darf nicht verwendet werden.

Die Liste der abgelehnten Suites enthält, ist aber nicht beschränkt auf:

- TLS_NULL_WITH_NULL_NULL
- TLS_RSA_NULL_WITH_NULL_MD5
- TLS_RSA_NULL_WITH_NULL_SHA