

## Inhalt

	Seite
Vorwort .....	2
Europäisches Vorwort zur Änderung A1 .....	3
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen .....	4
1 Anwendungsbereich .....	6
1.1 Anwendungsbereich .....	6
1.2 Zielgruppe .....	6
2 Normative Verweisungen .....	6
3 Begriffe und Abkürzungen .....	7
3.1 Begriffe und Abkürzungen .....	7
3.2 Zusätzliche Abkürzungen .....	7
4 Sicherheitsfragen im Sinne dieser Norm .....	7
4.1 Operative Anforderungen, die die Nutzung von TLS in der Fernwirkumgebung beeinflussen .....	7
4.2 Sicherheitsbedrohungen, denen entgegengewirkt wird .....	8
4.3 Angriffsverfahren, denen entgegengewirkt wird .....	8
5 Zwingende Anforderungen .....	9
5.1 Missbilligung von Verschlüsselungssuiten .....	9
5.2 Versionsaushandlung .....	9
5.3 Sitzungswiederaufnahme .....	10
5.4 Sitzungsneuaushandlung .....	10
5.5 Nachrichtenauthentifizierungscode .....	11
5.6 Zertifikatunterstützung .....	11
5.6.1 Mehrere Zertifizierungsstellen (CAs) (en: Certificate Authorities) .....	11
5.6.2 Zertifikatgröße .....	12
5.6.3 Zertifikataustausch .....	12
5.6.4 Überprüfung des öffentlichen Schlüssels .....	13
5.7 Koexistenz mit unsicherem Protokollverkehr .....	16
6 Unterstützung optionaler Sicherheitsmaßnahmen .....	16
7 Anforderungen verweisender Normen .....	16
8 Übereinstimmung .....	17
Literaturhinweise .....	18