Europäische Smart-Metering Normungs- und Standardisierungslandschaft - ein Vergleich

Bachelorthesis
im Studiengang Wirtschaftsinformatik
vorgelegt von

Toni Michael Richter
Matrikelnummer: 23311

am 15.09.2020
an der Hochschule Merseburg

Erstprüfer: Prof. Dr. Uwe Heuert
Zeitprüfer: Dipl.-Ing. (FH) Oliver Punk

Bearbeitungszeitraum: 22.07.2020 – 15.09.2020

Danksagung

Ich bedanke mich recht herzlich bei Herrn Prof. Dr. Heuert und Herrn Dipl.-Ing. (FH) Punk, beide Geschäftsführer der Firma Exceeding Solutions GmbH, die mir als Praxispartner ermöglicht haben meine Bachelorarbeit umzusetzen und mir während der Ausarbeitung zur Seite standen.

Ein großes Dankeschön gilt meiner Familie, insbesondere meiner Mutter und meiner Oma, die mich während meiner Studienzeit in allen Lebenslagen sehr unterstützt haben. Ich danke euch für die konstruktive Kritik und für ein allzeit offenes Ohr.

Vielen Dank für alles!

Toni Michael Richter

Eidesstattliche Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit eigenständig und ohne fremde Hilfe angefertigt habe. Textpassagen, die wörtlich oder dem Sinn nach auf Publikationen oder Vorträgen anderer Autoren beruhen, sind als solche kenntlich gemacht.

Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

_____ _____

Ort, Datum Unterschrift

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AMI	Advanced Metering Infrastructure
B3S	Branchenspezifische Sicherheitsstandards
BDEW	Bundesverband der Energie- und Wasserwirtschaft
BFE	Bundesamt für Energie
BMWI	Bundesministerium für Wirtschaft und Energie
BSI	Bundesamt für Sicherheit in der Informationstechnik
CBA	Cost–benefit analysis
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Électrotechnique
CRM	Customer-Relationship-Management
CSV	Comma-separated values
DSGVO	Datenschutz-Grundverordnung
DSL	Digital Subscriber Line
E.DSO	European Distribution System Operators
ENCS	European Network for Cyber Security
ENISA	European Union Agency for Cybersecurity
ESMIG	European Smart Metering Industry Group
ESO	European Standards Organizations
ETSI	European Telecommunications Standards Institute
EU	Europäische Union
GQL	Graph Query Language
HES	Head End System
IEA	International Energy Agency
iMSys	Intelligentes Messsystem

IoT	Internet of Things
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
IT	Informationstechnik
KRITIS	Kritische Infrastrukturen
LAN	Local Area Network
LN	Local Network
LNAP	Local Network Access Point
LTE	Long Term Evolution
M2M	Machine-to-Machine
mME	moderne Messeinrichtung
MsbG	Messstellenbetriebsgesetz
NIST	National Institute of Standards and Technology
NN	Neighborhood Network
NNAP	Neighborhood Network Access Point
PLC	Powerline Communication
RFC	Request for Comments
SM-CG	Smart Meters Coordination Group
SM-Gw	Smart Meter Gateway
TC	Technical Committees
TR	Technische Richtlinie
UMTS	Universal Mobile Telecommunications System
WAN	Wide Area Network
WLAN	Wireless Local Area Network

1.Einleitung

1.1 Relevanz des Themas

Elektrische Energie ist neben Wasser, eine der wichtigsten Ressourcen, die das heutige Leben benötigt. Strom ist allgegenwärtig und für viele mittlerweile selbstverständlich. Die Abhängigkeit zum Strom ist enorm. Ein „Blackout“[1] würde verheerende infrastrukturelle Folgen mit sich bringen. Bei einem globalen Anteil von 81% fossiler Energieträger (vgl. IEA, 2019, S. 6) und steigendem Energiebedarf (vgl. IEA, 2018) ist es essenziell, die Treibhausgas-Emission zu senken. Mit dem „Kyoto-Protokoll“[2] wurden 1997 verbindliche Zielwerte festgelegt, um die globale Erderwärmung zu verlangsamen. Somit kann das „Kyoto-Protokoll“ als Grundstein und als Beginn einer weltweiten Energiewende angesehen werden.

In Europa stellt die Richtline 2009/28/EG[3] den Dreh- und Angelpunkt für die Energiewende und das Instrument für den Ausbau erneuerbarer Energien in Europa dar. Bis 2030 sollen mindestens 27% des Energieverbrauches aus erneuerbaren Energien stammen (vgl. BMWI, o. J.). Solar, Wasser und Wind sind die wichtigsten Energie-Ressourcen im Bereich der erneuerbaren Energie[4]. Diese Formen der Energiegewinnung weisen einen dezentralen Charakter auf, ganz im Gegenteil zum ursprünglich etablierten Stromnetz. Bisher lag der Fokus auf der zentralen Energieversorgung. Solarparks und Windanlagen sind jedoch häufig dezentral und weit entfernt von Kraftwerken. Sinkende Kosten und kompakter werdende Wind- und Solaranlagen ermöglichen es dem Endverbraucher, Strom zu erzeugen und einzuspeisen und unterstützen den Charakter einer dezentralen Versorgungsstruktur. Zu beachten ist dabei, dass anders als bei konventionellen Energieträgern, bei erneuerbaren Energien keine Kontinuität vorausgesetzt werden kann. Die Energiegewinnung aus Solar- und Windenergie ist volatil, da diese von der Wetterlage und Tageszeit abhängig ist. An Tagen eines Überangebotes muss für sonnen- und windschwache Tage eine Möglichkeit zur Zwischenspeicherung vorhanden sein. Aktuell lassen sich oben beschriebene Umstände schwer monitoren und erschweren die Planung des Netzbetreibers im Hinblick auf die Versorgungssicherheit und den

[1] Totaler Stromausfall (vgl. Dudenredaktion, (o.J.))
[2] Protokoll von Kyoto zum Rahmenübereinkommen der Vereinten Nationen über Klimaänderungen
[3] Richtlinie für erneuerbare Energien - Teil des Europäischen Klima- und Energiepakets
[4] Wasser wird in dieser Arbeit nicht als Energiequelle berücksichtig, da von Ihr eine Konstanz geht, und somit nicht zwingend gemonitort werden muss

Netzausbau. Mit Hilfe der Informations- und Telekommunikationsgeräte, in denen moderne Messeinrichtungen (mME) und Smart Meter Gateways[5] (SM-Gw) eine zentrale Rolle einnehmen, soll das Netz digitalisiert werden, um die genannten Umstände zu bewältigen.

1.2 Problemstellung

Der Energiesektor bewegt sich in einem Spannungsfeld zwischen Wirtschaftlichkeit, Versorgungssicherheit und Umweltschutz. Alle Säulen gleichberechtigt zu berücksichtigen ist schwer und wird durch ein digitalisiertes Stromnetz nicht zwingend einfacher. Ein intelligentes Stromnetz bietet viele neue Möglichkeiten für den Betreiber und Endkunden, aber auch ein Betätigungsfeld für kriminelle Handlungen.

Die Energieversorgung in Deutschland ist seit 2016 Teil der KRITIS-V[6] und somit eine kritische Infrastruktur[7] (vgl. Apel, 2017, S. 7). Auch in anderen europäischen Ländern muss sich durch die Richtline 2008/114/EG mit dieser Thematik auseinandergesetzt werden. Energieversorger unterliegen besonderen Anforderung, die erfüllt werden müssen, um Angriffe auf das Stromnetz durch Cyberkriminelle zu erschweren. Bei diesen speziell formulierten Anforderungen werden Cyber-Sicherheitsanforderung an die Einrichtung selbst formuliert und nicht an moderne Messeinrichtungen oder Smart Meter Gateways. Durch den Ausbau des digitalen Stromnetzes vergrößert sich somit die Angriffsfläche auf das Stromnetz und verlagert sich zudem zusätzlich nach extern und fällt deshalb aus dem Bereich der strengen Anforderung der KRITIS-V heraus. Es ist somit zwingend erforderlich, dass moderne Messeinrichtungen und SM-Gw's durch gesonderte Richtlinien, technische Anforderungen und Standards abgesichert werden, um eine sichere Kommunikation aus Datenschutzgründen und Sicherheitsaspekten zu gewährleisten.

Im Laufe der Zeit haben sich eine Vielzahl von Richtlinien, Standards und technische Anforderungen etabliert. Problematisch ist, dass dabei schnell der Überblick verloren gehen kann. Auf europäischer Ebene existieren derzeit keine einheitlichen klaren Anforderungen an eine mME oder an ein SM-Gw. Jeder Staat innerhalb der

[5] Kommunikationsschnittstelle intelligenter Stromzähler zum Netzbetreiber
[6] Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz
[7] „Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“ (BSI & BMWi, o. J.)

EU darf die Anforderungen selbst formulieren. Darüber hinausgehend gibt es Organisationen die „Best-Practise“ Dokumente veröffentlichen oder an verschiedenen Richtlinien arbeiten. Den Herstellern oder den Prüfstellen von modernen Messeinrichtungen oder Gateways wird dabei nicht der Eindruck von Einigkeit vermittelt, sondern eher von einem parallelen Betrieb der Organisationen ohne Kommunikation untereinander. Ein einheitlicher Rollout oder eine Interoperabilität ist dadurch nur bedingt gewährleistet.

1.3 Ziel der Arbeit

Auf Datenbasis der Länder Deutschland, Schweiz, Österreich, Niederlande und dem europäischen Protection Profile[8] soll ein Überblick über die in Europa aktuell geltenden Standards und Richtlinien erlangt werden.

Mit den erhobenen Daten soll die beschriebene Problematik aus Kapitel 1.2 Problemstellung versucht werden zu beheben. Nach Beendigung der Datenerhebung soll ein Daten- und Kenntnisstand erreicht sein, der es ermöglicht, im Anschluss der Arbeit einen Anforderungskatalog zu erarbeiten, der auf EU-Ebene eingesetzt werden kann.

1.4 Aufbau der Arbeit

Die Arbeit besteht aus einem theoretischen Teil, der sich mit den Grundlagen der elektrischen Energieversorgung und dessen Aufbau befasst, übergehend zu den Grundsteinen der Digitalisierung der Stromnetze, deren Notwendigkeit und bis hin zu den Grundkomponenten mit deren Standards und europäischen Richtlinien. Der zweite Teil betrachtet die Lage und die Ausgangssituation der Standards und Richtlinien, die für das digitale Stromnetz unverzichtbar sind und werden durch Hilfsmittel visuell aufgearbeitet und ausgewertet und ist somit praktischer Natur.

[8] Eine Zusammenstellung von Sicherheitsanforderungen nach ISO/IEC 15408

2. Grundlagen

2.1 Elektrische Energieversorgung

2.1.1 Konventionelles Stromnetz

Die aktuelle „Form“ des Stromnetzes existiert seit einigen Jahrzehnten und wurde damals für eine zentrale Stromerzeugung (2.2 (De-)zentral - Konzepte der Stromerzeugung) und Versorgung konzipiert und sah eine Versorgung durch fossile Energieträger oder Kernenergie vor. Diese Art der Energieversorgung findet aufgrund der Größe und Funktionsweise eines Kraftwerkes zentral und unidirektional[9] statt. Abbildung 1 stellt den Aufbau eines aktuellen Stromnetzes stark vereinfacht dar. Kraftwerke werden an Flüssen geplant, da diese für den Betrieb eine essenzielle Funktion einnehmen. Kohle- und Atomkraftwerke benötigen eine permanente Kühlung der Kreisläufe, um ein Überhitzen zu verhindern. Diese Aufgabe übernehmen die nahegelegenen Flüsse.

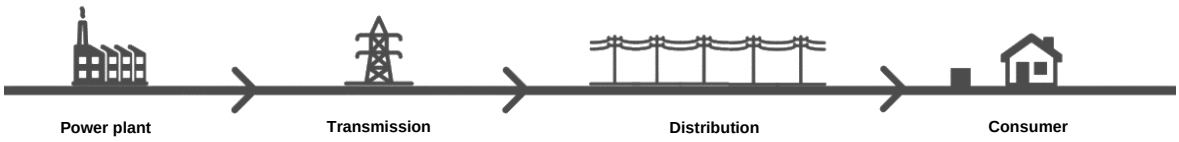


Abbildung 1: Konventionelles Stromnetz
Quelle: in Anlehnung an E.DSO, o. J.

Die Übertragung der elektrischen Energie erfolgt dabei in vier verschiedenen Spannungsebenen. Diese Ebenen kann man in zwei Gruppen aufteilen (siehe Tabelle 1). Höchst- und Hochspannung sind dabei für die Übertragung weiterer Strecken ausgelegt und Mittel- und Niederspannung für die Versorgung von kleinen Städten und Haushalten.

Die Vorteile eines solch angelegten Netzes und die Art der Versorgung sind die Wetterunabhängigkeit und die bestehende Infrastruktur. Der Endkunde muss sich über keine Neuinstallationen oder zusätzliche Kosten Gedanken machen und bei nicht optimalen Wetterbedingungen keine Versorgungsängste haben. Der maßgebliche Nachteil dieser Versorgungsart liegt in den ökologischen Problemen. Die Gewinnung elektrischer Energie wird zu großen Teilen aus Atomenergie oder Kohle

[9] Die Übertragung des Stroms erfolgt in eine Richtung – in die des Verbrauchers

gewonnen. 2017 lag der weltweite Anteil bei 32%[10]. Beispielsweise werden für den Abbau von Kohle große Flächen trockengelegt, Wälder abgeholzt oder tief in das Erdreich vorgedrungen. Dadurch können Probleme wie Engpässe in der Trinkwasserversorgung oder Verunreinigungen des Grundwassers und der Flüsse entstehen, mit Folgen für die Trinkwasseraufbereitung und Fauna. Um die ökologischen Folgen zu minimieren, ist es notwendig auf andere Energieträger umzusteigen.

	Ebene	Spannung	Funktion
Tansmission[11]	Höchstspannung	220 kV / 380 kV	Überregionale Transportnetze &Verbindung der Nachbarstaaten
	Hochspannung	60kV bis 110kV	Verteilnetze Verbindung / Anbindung von Städten und/oder stromintensiver Industrie
Distribution[12]	Mittelspannung	6kV bis 30kV	Verteilnetze Verbindung / Anbindung von Kleinstädten und Industriebetrieben
	Niederspannung	230V / 400V	Verteilnetze Anbindung privater Haushalte und kleineren Betrieben

Tabelle 1: Spannungsebenen
Quelle: eigene Darstellung, Daten entnommen aus: EnBW, o. J.

[10] Energieerzeugung aus Kohle 27%; Kernenergie 5%
[11] Dt. Übertragung
[12] Dt. Verteilung

2.1.2 Smart Grid – Das weiterentwickelte Stromnetz

> *„Smart Grids sind Stromnetze, welche durch ein abgestimmtes Management mittels zeitnaher und bidirektionaler Kommunikation zwischen Netzkomponenten, Erzeugern, Speichern und Verbrauchern, einen energie- und kosteneffizienten Systembetrieb für zukünftige Anforderungen unterstützen“ (Smart Grids Austria, 2016).*

Die Energiewende erfordert eine Transformation des bisher bekannten Stromnetzes. Es gibt drei Treiber, die für die Entwicklung des Stromnetzes verantwortlich sind[13] (vgl. Agora Energiewende, 2017, S. 10).

1. Physikalische Grenzen von Wind- und Solarenergie
2. Technologische Entwicklungen (Stromspeicher, Elektromobilität, Wärmepumpen, Photovoltaik-Anlagen)
3. Informations- und Kommunikationstechnik

Mit dem Einsatz moderner Messeinrichtungen in Kombination mit Smart Meter Gateways wird die Option geschaffen, eine bedarfs- und verbrauchsorientierte Verknüpfung zwischen Erzeugern, Speichern und Verbrauchern herzustellen (siehe Abbildung 2). Mit dieser Ausgestaltung des Netzes ist es möglich, die Energiewende effizienter und schneller zu vollziehen.

Es muss ergänzt werden, dass man bei der Transformation, hin zum digitalen Stromnetz, nur teilweise von Digitalisierung gesprochen werden kann, denn Überwachung, Steuerung und Kommunikation findet im Übertragungsnetz bereits heute digital statt (Bundesnetzagentur, 2011, S. 9). Es wäre also treffender, wenn man von einer Digitalisierung des Verteilernetzes sprechen würde.

[13] Bezüglich Dezentralisierung und Digitalisierung

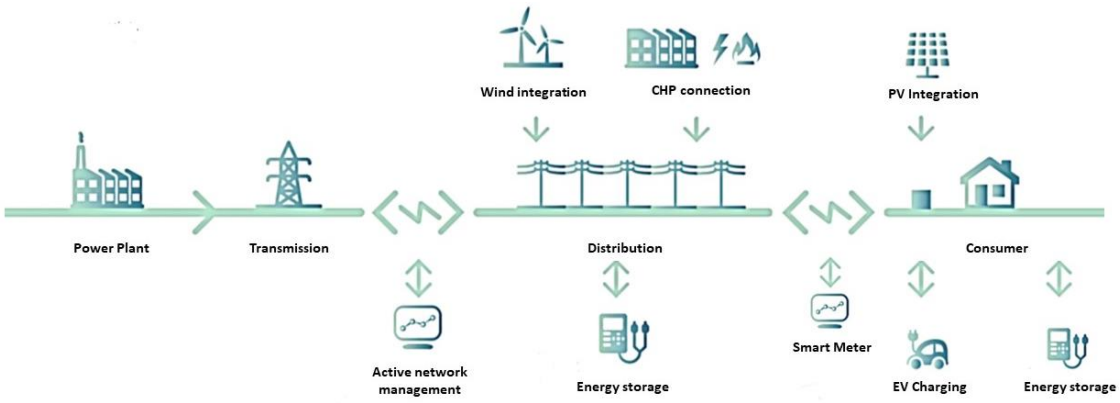


Abbildung 2: Smart Grid
Quelle: in Anlehnung an E.DSO, o. J.

Vorteile und Chancen

Ungeachtet dessen, dass das Smart Grid in erster Linie der Umwelt zugutekommt, liefert es dem Verbraucher und Erzeuger gleichermaßen Vorteile, die nachfolgend betrachtet werden sollen.

Für den Verbraucher ist wohl der offensichtlichste Vorteil, dass er uneingeschränkte Kontrolle über seinen Stromverbrauch und die daraus resultierenden Kosten erhält. Durch diese Transparenz ist es möglich, den exakten Stromverbrauch zu ermitteln und somit eventuelle „Stromfresser“ zu identifizieren. So können beim Kunden Anreize entstehen und ihn nachhaltig beim Denken und Handeln beeinflussen – unter Umständen besteht ein durchschnittliches Einsparpotenzial von 10% (vgl. Gensrich, 2017). Anders als bisher könnte der Energieversorger dem Verbraucher eine monatsgenaue Stromabrechnung liefern. Für den Endkunden entfallen somit die monatlichen Abschlagszahlungen, da mit der monatlichen Stromabrechnung der monatliche Stromverbrauch exakt in Rechnung gestellt werden kann.

Nicht zu vergessen sind die positiven Nebeneffekte, die durch diese Art der Stromabrechnung sichtbar werden. Der Verwaltungsaufwand kann minimiert werden und daraus entsteht schlussfolgernd eine Personal- und Kostenersparnis, welches die Wirtschaftlichkeit des Versorgers positiv beeinflussen kann. Ebenfalls besteht die Möglichkeit, intelligente Stromzähler aus der Ferne ablesen zu können. Beim Versorger entsteht ein zusätzliches Einsparpotenzial und der Verbraucher profitiert von mehr Komfort. Durch die Kommunikation zwischen Verbraucher und Versorger

entsteht so ein besserer Einblick in die Konsumgewohnheiten des Verbrauchers, womit eine bessere Lastplanung vorgenommen werden kann. Es entsteht somit ein besseres Verhältnis von Angebot zu Nachfrage, wodurch ein Rückgang der CO2-Emmisionen zu erwarten ist.

Während der Übergangsphase, hin zur vollständigen Stromversorgung über erneuerbare Energien, bietet das Smart Grid eine bessere Integrations- und Planungsmöglichkeiten von Wind- und Solarparks. Ein gravierender Nachteil sind die hohen Investitions- und Entwicklungskosten, um das Smart Grid aufzubauen.

2.2 (De-)zentral - Konzepte der Stromerzeugung

Im Rahmen der Energiewende wird häufig der Begriff „Dezentralisierung“ verwendet. Man könnte Anlass zur Vermutung haben, dass der Einsatz von Wind- und Solarenergie automatisch immer mit einer dezentralen Versorgungsstruktur einhergeht. Ob es sich bei dem neuen Netz tatsächlich um ein dezentrales Netz handelt, soll im folgenden Kapitel genauer betrachtet werden.

Generell ist es nicht falsch, bei der Energiewende und Smart Grid, von einer dezentralisierten Netzstruktur zu sprechen – aber nur partiell. Wann von einem dezentralen oder zentralen Netz gesprochen werden kann, veranschaulicht Abbildung 3.

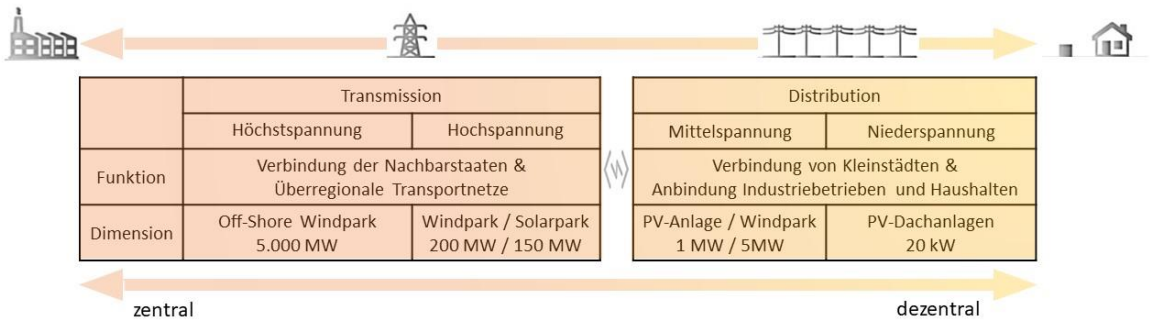


Abbildung 3:Zuordnung Netzstruktur – Spannungsebene
Quelle: eigene Darstellung, in Anlehnung an: Leopoldina, acatech & Akademiunion, 2020, S.25

Abbildung 3 zeigt, dass nicht die Art der Energieerzeugung entscheidend ist, ob es sich um ein zentrales oder dezentrales Netz handelt, sondern wieviel Leistung die jeweilige stromproduzierende Anlage erzeugt bzw. erzeugen kann. Je nach Menge der theoretisch erzeugbaren Energie, wird entschieden an welchen Teil des Netzes die Anlage angebunden wird. In Tabelle 1 wurde anhand der Spannungsebenen

aufgezeigt, dass das Netz in zwei Teilbereiche aufgeteilt wird. Somit sind die Spannungsebenen Nieder- und Mittelspannung dem dezentralen Netz und Hoch- und Höchstspannung dem zentralen Netz zugeordnet (siehe Abbildung 3).

2.3 Kernkomponenten im Smart Grid

Im Zusammenhang mit intelligenten Stromnetzen werden häufig Smart Meter und Smart Meter Gateways genannt. Im Sprachgebrauch wird jedoch häufig nicht auf das Detail geachtet. Eine genauere Betrachtung der eingesetzten Komponenten und Begrifflichkeiten ist für das Verständnis eines digitalen Stromnetzes wichtig und kann bei unsachgemäßer Verwendung der Wörter für Verwirrung sorgen. Das folgende Kapitel soll deshalb für Aufschluss in der Verwendung der Begrifflichkeiten sorgen und einen Überblick über die eingesetzten Komponenten geben. Ein zusammenfassender Überblick und eine Gegenüberstellung der einzelnen Komponenten findet in Abbildung 6 statt.

2.3.1 Moderne Messeinrichtung

Die moderne Messeinrichtung ist die Vorstufe des intelligenten Messsystem (iMSys) und wird im allgemeinen Sprachgebrauch gerne als Smart Meter bezeichnet, muss aber klar getrennt voneinander betrachtet werden.

Die moderne Messeinrichtung ist die Grundkomponente der intelligenten Messsysteme, welche ohne Kommunikationseinheit die reine Ablöse für den alten Ferraris-Zähler darstellt und somit wenig „Intelligenz“ einziehen lässt. Erst beide Komponenten ergeben das iMSys. Im direkten Vergleich bringt die moderne Messeinrichtung gegenüber dem Ferraris-Zähler natürlich Vorteile mit sich, aber nicht die kommunizierten Vorteile der Smart Meter. Die mME bietet dem Kunden die Möglichkeit, den tatsächlichen Energieverbrauch auszulesen oder sich die historischen tages-, wochen-, monats- und jahresbezogenen Werte ausgeben zu lassen.

Abbildung 4:links: Ferraris-Zähler; rechts: Moderne Messeinrichtung
Quelle: Stadtwerke Kempen, o. J.

In dieser Ausführung (siehe Abbildung 4) kann eine moderne Messeinrichtung nicht aus der Ferne abgelesen werden. Der Kunde oder der Messstellenbetreiber muss somit, wie bisher, die Stromverbräuche ablesen. Diese und weitere Funktionen können erst mit dem Hinzufügen einer Kommunikationseinheit (Smart Meter Gateway) ermöglicht werden.

2.3.2 Smart Meter Gateway

Smart Meter Gateways sind für die Kommunikation zwischen Verbraucher und Versorger erforderlich, ohne sie kann keine Kommunikation stattfinden und viele Vorteile des intelligenten Stromnetzes wären nicht abrufbar. Smart Meter Gateways empfangen, verarbeiten und speichern Messwerte jedes verbauten Zählers in einem Haushalt – egal ob Strom, Wasser, Wärme oder Gas. Die gespeicherten Daten können von verschiedenen Akteuren über die jeweiligen dafür vorgesehenen Schnittstellen abgerufen werden (siehe Abbildung 5). Die Übertragung der Daten zu den entsprechenden Marktteilnehmern erfolgt dabei verschlüsselt und wahrt somit Integrität, Authentizität und Vertraulichkeit (3.2.4 Schutzziele).

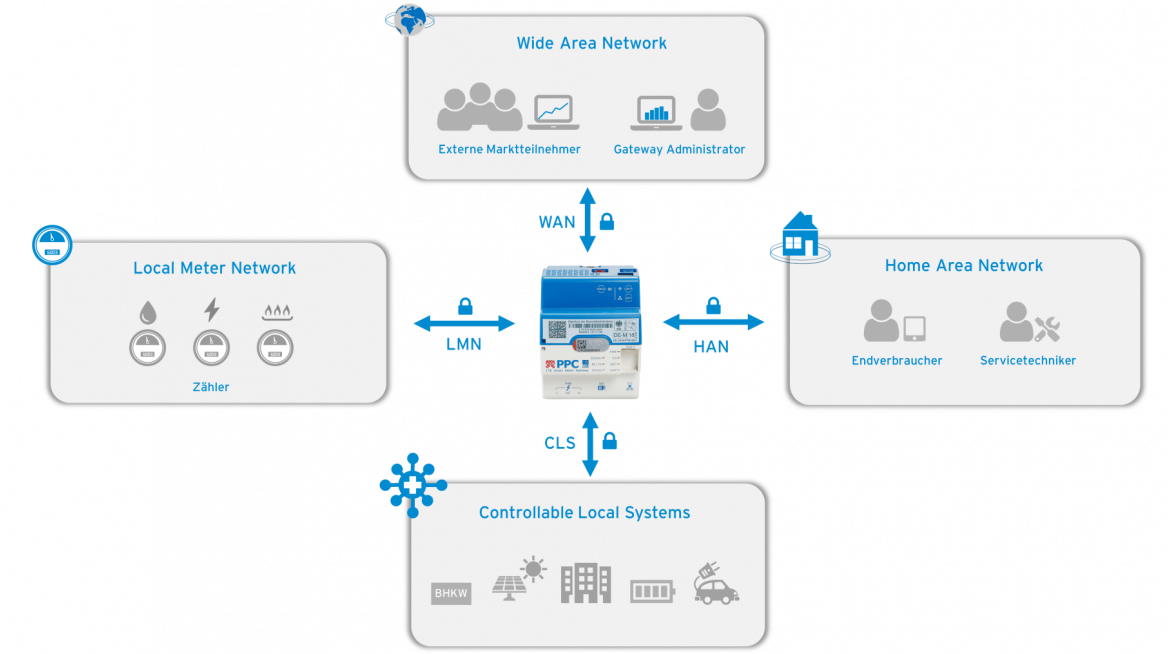


Abbildung 5:Zuordnung Marktteilnehmer – Schnittstelle
Quelle: PPC-AG, 2020

	Ferraris-Zähler	*Moderne Messeinrichtung*	*Intelligentes Messsystem*	*Kommunikationseinheit = Smart-Meter-Gateway*
Zählertyp	analoger Zähler	digitaler Zähler **ohne** Kommunikationseinheit	digitaler Zähler **mit** Kommunikationseinheit	Kommunikationsschnittstelle
Funktionen des Zählers	○ Aktueller Zählerstand	○ Aktueller Zählerstand ○ gespeicherte Werte: • tages- • wochen- • monats- • jahresgenau 2 Jahre im Rückblick	○ Aktueller Zählerstand ○ Abrufbar in Viertelstundenwerten • Tages- • Wochen- • Monats- • Jahresanzeige	○ Schnittstelle zwischen Zähler und Kommunikationsnetz ○ kann einen oder mehrere Zähler anbinden ○ automatische Datenübertragung zum Messstellenbetreiber

Abbildung 6: Gegenüberstellung mME, iMSys und SM-Gw
Quelle: In Anlehnung an Bundesnetzagentur, o. J.

2.3.3 European Mandat M/441

Die Smart Meter Coordination Group (SM-CG), bestehend aus drei europäischen Normungsorganisationen, hat im März 2009 das European Mandat M/441 verabschiedet. Das M/441[14] verfolgt das Ziel einer offenen Referenzarchitektur (siehe Abbildung 7) für Smart Metering-Systeme (Gas, Wasser, Wärme oder Elektrizität), mit der durch einheitliche Kommunikationsprotokolle, für Interoperabilität gesorgt werden soll. Aufbau der SM-CG und Standards, die aus ihnen hervorgehen, werden in Kapitel 4.4 Smart Meter Coordination Group genauer betrachtet.

Ziele des Mandats im Detail:

- Offene Referenz Architektur für Hard- und Software
- Standardisierte Schnittstellen
- Sichere Kommunikation (bidirektional)
- Kommunikationsmedium und Anpassbarkeit
- Skalierbare Architektur
- Unterstützung aller Anwendungen

[14] Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability

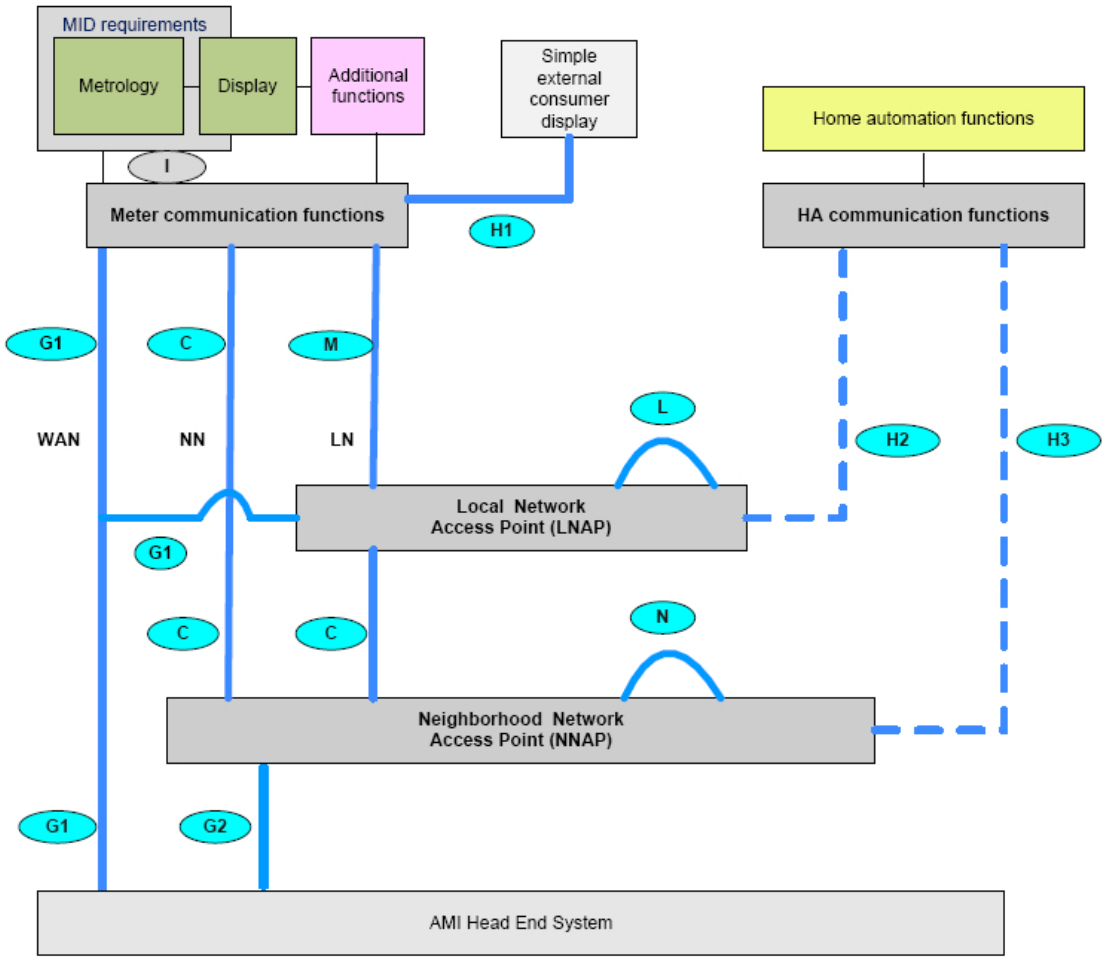


Abbildung 7: M/441 - Referenz Architektur
Quelle: CEN/CLC/ETSI, 2011, S.18

- Wide Area Network (WAN) verbindet das zentrale System mit lokalen Netzwerken
- Neighborhood Network (NN) Zusammenschluss diverser LN (optional),
- Local Network (LN) Innerhalb der Räumlichkeit (optional)

In der Referenz Architektur werden vier Komponenten und fünf Schnittstellen referenziert.[15] Diese sollen nachfolgend betrachtet werden.

[15] Unterschiede zu einzelnen Mitgliedstaaten möglich, da sie im Rahmen des Mandates die eigenen Gesetze und Ziele umsetzen dürfen

Metering End Devices

Sind moderne Messgeräte [16], die zum Erfassen von Verbräuchen (Strom, Wasser, Gas und Wärme) eingesetzt werden, den Anforderungen der Messgeräterichtlinie[17] unterliegen und mindestens eine Schnittelle (WAN, NN, LN) aufweisen.

Local Network Access Point (LNAP)

Ein LNAP ist vergleichbar mit dem SM-Gw (2.3 Kernkomponenten im Smart Grid). Die LNAP fungiert im lokalen Netzwerk als zentrale Einheit für weitere Messgeräte und andere intelligente Komponenten und ermöglicht dabei die Kommunikation untereinander sowie zum WAN oder NN. Der lokale Access Point hat dabei mindestens eine oder mehrere M- und H2-Schnittstellen, um mit den Komponenten im lokalen Netz zu kommunizieren und eine oder mehrere C- oder G-Schnittstellen, um mit dem Neighborhood Netzwerk oder mit dem WAN zu kommunizieren.

Neighborhood Network Access Point (NNAP)

Neighborhood Network Access Point sind sogenannte Datenkonzentratoren. Sie sind vergleichbar mit einem Smart Meter Gateway, da sie, wie die lokalen Access Points, zwei oder mehr Informationssysteme miteinander verbinden. Die Kernaufgabe des Konzentrators ist es, die Daten des ihm zugehörigen Netzes an das Head End System weiterzuleiten (siehe Abbildung 8). Durch diese Art der Übertragung lässt sich eine Reduktion des Datentransfers hervorrufen. Die Möglichkeiten der Übertragung sind vielfältig und kann bei Bedarf gewechselt werden (PLC[18], LTE[19], 5G[20] oder DSL[21]). Ausgestattet ist der Konzentrator mit bis zu drei Schnittstellen. Diese werden als C-, G- und H-Schnittstelle bezeichnet

[16] Kommunikation wird ermöglicht
[17] Measuring Instruments Directive (MID)
[18] Powerline Communication
[19] Long-Term-Evolution
[20] 5 Generation – aufbauend auf LTE
[21] Digital Subscriber Line

AMI Head End System (HES)

In Abbildung 7 wird das AMI[22] und Head End System als Einheit betrachtet. Diese zwei Systeme gehören zwar grundlegend zusammen, müssen aber getrennt voneinander betrachtet werden. Abbildung 8, stellt den Kommunikationsablauf besser dar. Das HES ist die Kommunikationseinheit, mit der die Datenkonzentratoren oder lokalen Access Points kommunizieren und stellt somit das Bindeglied zwischen AMI und lokalen Access Points dar. Ein Head End System hat einen hohen Stellenwert, da alle Gateways (lokale Access Points) mit ihm kommunizieren und die unterschiedlichen Datenformate in ein einheitliches Format für das AMI bereitstellen muss. Die Advanced Metering Infrastructure übernimmt die Analyse und Verarbeitung der Daten, um sie im nächsten Schritt im Rechnungswesen und CRM[23] einzuleiten.

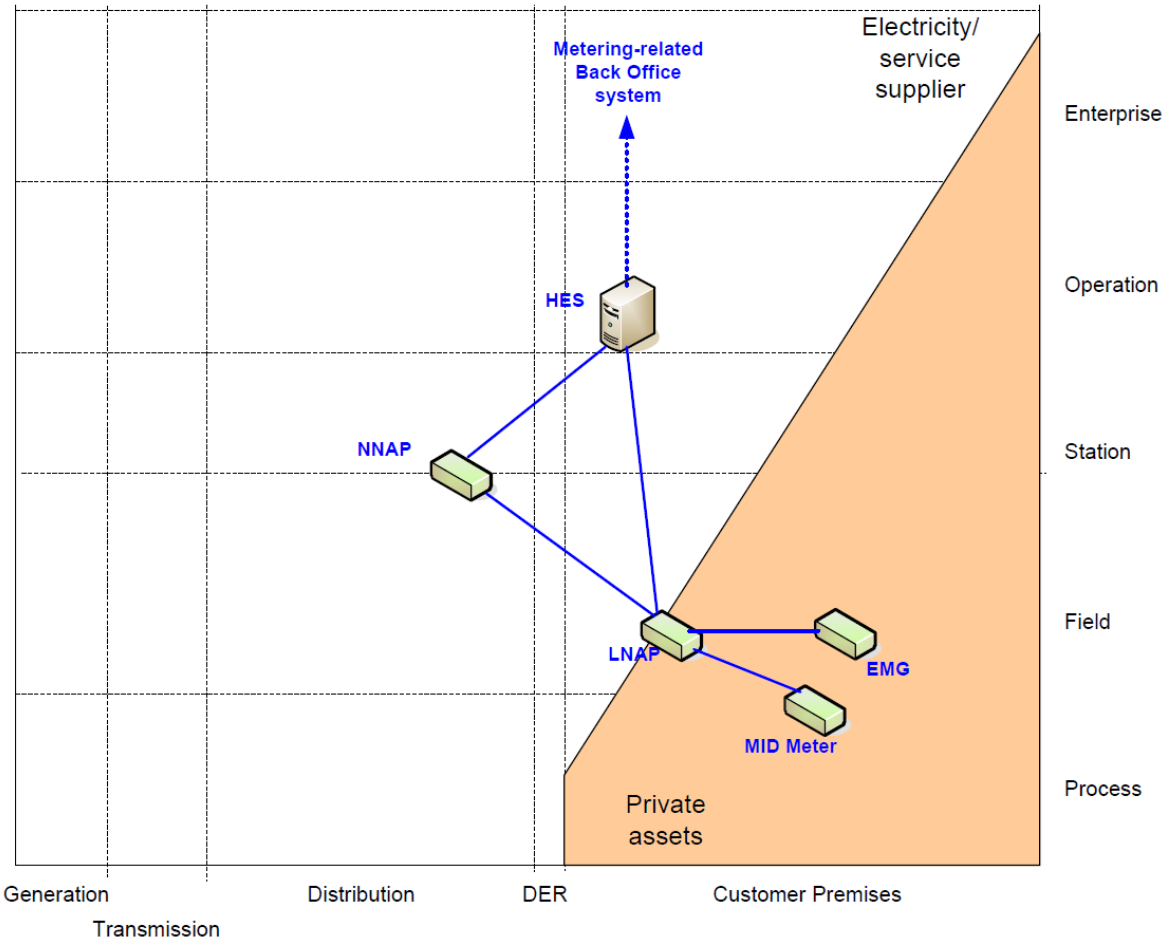


Abbildung 8: Verteilung der Systemkomponenten
Quelle: CEN-CENELEC-ETSI, 2017, S.117

[22] Advanced Metering Infrastructure
[23] Customer-Relationship-Management

G-Interface

Die Wahl der Schnittstelle ist abhängig von der gewählten Kommunikationsstruktur. UMTS[24], DSL, Glasfaser und Kabelnetz sind mögliche Medien über welche die Kommunikation stattfinden kann.

G1-Interface - Intelligenter Zähler – AMI Head End System

G2-Interface - NNAP – AMI Head End System

C-Interface

Es wird für die Kommunikation zwischen NNAP und LNAP oder intelligenten Zähler und NNAP eingesetzt. Sollte der Neighborhood Network Access Point direkt mit dem Zähler verbunden sein, treffen die Anforderungen und Beschreibung des **M-Interfaces** auch für das **C-Interface** zu. Folgende Kommunikationsmedien stehen zur Auswahl: PLC, WLAN oder LAN (Ethernet).

M-Interface

Das M-Interface regelt die Kommunikation zwischen dem Local Network Access Point und dem Zähler (Unabhängig vom Verbrauchsgut). Es stellt die internen Zählerdaten bereit und unterstützt den Zugang zum LNAP.

H-Interface

regelt die unten aufgelistete Kommunikation der verschiedenen Varianten

H1-Interface - Intelligenter Zähler – ext. Display

H2-Interface - LNAP – Zusatzgeräte

H3-Interface - NNAP – Zusatzgeräte

[24] Universal Mobile Telecommunications System

L- & N-Interface

Beide Schnittstellen sind optional und würden eine Verbindung mehrerer LNAP's (L-Interface) oder NNAP's (N-Interface) ermöglichen.

Jede der oben aufgeführten Schnittstellen hat ein Technical Committee (TC), welches für die spezielle Formulierung der Schnittstellen verantwortlich ist. Die Technical Committees werden in Kapitel 4.4 Smart Meter Coordination Group genauer betrachtet. Tabelle 2 listet die Zuordnung von Schnittstellen zu Technical Committee auf.

Interface	Beschreibung	Messwesen Einfluss	Verantwortlichkeit OSI-Schicht 1-4	Verantwortlichkeit OSI-Schicht 4-7	Hauptverantwortlichkeit
I	Zähler Eigenschaften	Ja	Anforderung nicht im Mandat definiert		
M	Zähler - NNAP	Nein	TC 13 & 294	TC 13 & 294	TC 13 & 294
C	Zähler / LNAP - NNAP	Nein	TC 13 & 294	TC 13 & 294	TC 13 & 294 & 57
G1	Zähler / LNAP - HES	Nein	ETSI	TC 13 & 294	TC 13 & 294
G2	NNAP - HES	Nein	ETSI	TC 13 & 294 & ETSI M2M	TC 13 & 294 & 57
H1	Zähler – ext. Display	Nein	TC 205	TC 205	TC 205
H2+3	LNAP / NNAP – ext. Geräte	Nein	TC 205	TC 205	TC 205
L	Peer Interface LNAP	Nein	ETSI	ETSI	ETSI M2M
N	Peer Interface NNAP	Nein	ETSI	ETSI	ETSI M2M

Tabelle 2: Verantwortlichkeiten der Schnittstellen
Quelle: eigene Darstellung, In Anlehnung an CEN/CLC/ETSI, 2011, S.23

3. Sicherheit und Datenschutz

3.1 Bedenken

Vorteile und Chancen, die aus dem Smart Grid hervorgehen bzw. hervorgehen können, wurden bereits erwähnt (2.1.2 Smart Grid – Das weiterentwickelte Stromnetz). Der Großteil der entstehenden Möglichkeiten, für Versorger und Verbraucher, sind auf einen dauerhaften Datenaustausch zurückzuführen. Analysemethoden für das Berechnen und Vorhersagen des Strombedarfs können gleichermaßen Aufschluss über Leben und Verhaltensmuster der Endverbraucher geben und somit einen Eingriff in die Privatsphäre darstellen, besonders dann, wenn eingebundene Endgeräte ebenfalls intelligent werden. So könnte ein noch detaillierteres Bild des Endverbrauchers entstehen. Daten mit einem hohen Informationsgehalt, können ein detailliertes Verbraucherprofil liefern und sind in kriminellen Händen nicht erwünscht und erfordern somit ein besonders hohes Maß an Informationssicherheit.

3.2 Informationssicherheit

Wenn die Rede von Sicherheit in der Informationstechnik ist, steht die Einhaltung der Schutzziele an oberster Stelle. Die Informationssicherheit ist ein Zusammenspiel verschiedener Bereiche, die in ihrer Gesamtheit der Informationssicherheit dienen (siehe Abbildung 9). Die Unterschiede der einzelnen Bereiche sind so gering, dass sie zunächst unwichtig erscheinen, sind aber entscheidend, da sie den Teilbereichen eine komplett andere Bedeutung geben und somit ausschlaggebend für die Aufgaben entsprechender Bereiche sind.

> *„Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Die Schutzziele oder auch Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit […]“ (BSI, o. J.)*

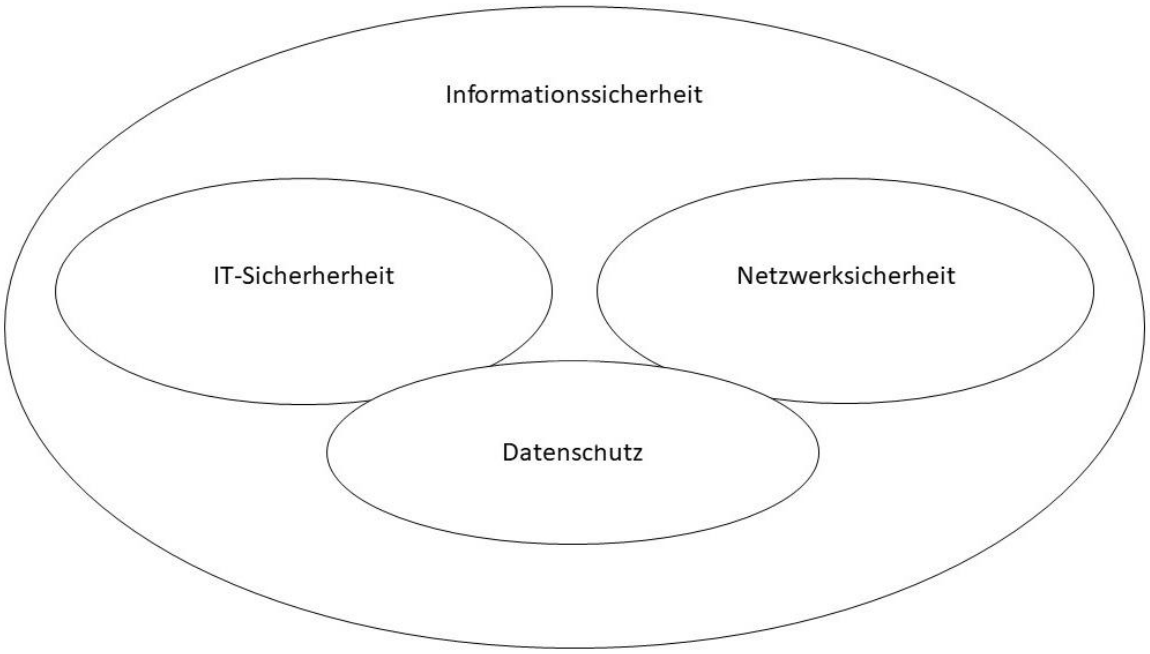


Abbildung 9: Kernbereiche der Informationssicherheit
Quelle: eigene Darstellung

3.2.1 Datenschutz

> *„[…] Mit Datenschutz wird […] der Schutz personenbezogener Daten vor etwaigem Missbrauch durch Dritte bezeichnet […]“ (BSI, o.J.)*

Die Europäische Union sieht mit der Datenschutz-Grundverordnung (DSVGO) in Artikel 5 Satz1 Absatz a - f (Grundsätze für die Verarbeitung personenbezogener Daten) folgende Eckpunkte vor:

Personenbezogene Daten müssen

a) […] für die betroffene Person nachvollziehbaren Weise verarbeitet werden **(„Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“)**

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden […] **(„Zweckbindung“)**

c) dem Zweck angemessen und erheblich, sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein **(„Datenminimierung“)**

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein […] **(„Richtigkeit“)**

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist […] **(„Speicherbegrenzung“)**

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet […] **(„Integrität und Vertraulichkeit“)**

Als „unterstützende“ Maßnahme zum Datenschutz sieht die DSGVO den Einsatz der „Pseudonymisierung“ vor. Dadurch lässt sich die Menge personenbezogener Daten minimieren. Die Pseudonymisierung soll ermöglichen, dass Daten nicht mehr einer spezifischen Person zugeordnet werden können (§ 4 Verordnung (EU) 2016/679).

3.2.2 IT-Sicherheit

Abweichend vom Datenschutz befasst sich die IT-Sicherheit nicht mit allen Daten, sondern nur mit den Daten, die sich auf IT-Systemen befinden. Weiterhin wird der IT-Sicherheit auch der Schutz der Systeme zugeschrieben, die die Daten verarbeiten. Es geht also um das Aufrechterhalten der Tätigkeiten im Unternehmen, die durch Ausfälle der IT entstehen können.

3.2.3 Netzwerksicherheit

Von der IT-Sicherheit gibt es einen fließenden Übergang zur Netzwerksicherheit und umgekehrt. Der Grad der Vernetzung innerhalb eines Unternehmens, aber auch die weltweite Vernetzung, hat in den letzten Jahren stark zugenommen. Es ergibt sich somit die Notwendigkeit der Netzwerkabsicherung. Ohne abgesicherte Netzwerke können Daten abgefangen, zweckentfremdet oder manipuliert werden. Ausfälle durch Überlastungen sind ein weiteres Szenario, welches es durch die Netzwerksicherheit zu vermeiden gilt. Aus diesem Grund müssen Netzwerke überwacht und gegen unerlaubte Zugriffe abgesichert werden.

3.2.4 Schutzziele (CIA)

Durch die 2009 in Kraft getretene Richtline 2008/114/EG, ist es erforderlich sogenannte Sicherheitspläne zu entwerfen, um Sicherheitslösungen zu ermitteln. In Deutschland werden diese B3S (Branchenspezifische Sicherheitsstandards) genannt. In den zu entwerfenden Sicherheitsplänen dreht es sich, um die Sicherstellung der Schutzziele und so die Informationssicherheit zu gewährleisten.

Als Beispiel zur Darstellung der Schutzziele soll der branchenspezifische Sicherheitsstandard des Energiesektors dienen (BDEW, 2019, S.11)

(C) Confidentiality: Vertraulichkeit

Es muss sichergestellt werden, dass Informationen, deren Offenlegung die zugesagte Bereitstellung/Einspeisung der durch die Anlage aggregierten elektrischen Leistung oder die Einhaltung anderer relevanter Anforderungen im Bezug auf den sicheren Netzbetrieb in relevantem Umfang gefährden würde, Unberechtigten nicht bekannt werden.

Mit anderen Worten verkürzt ausgedrückt bedeutet dies, dass Informationen, die Einfluss auf die Einspeisung haben könnten, nicht an Unbefugte preisgegeben werden dürfen.

(I) Integrity / authenticity: Integrität / Authentizität

Es muss die Integrität, Authentizität und korrekte Verarbeitung von Informationen sichergestellt werden, deren fehlerhafte, manipulierte oder unvollständige Übertragung, Speicherung oder Verarbeitung die planmäßige Bereitstellung/Einspeisung der durch die Anlage aggregierten elektrischen Leistung in relevantem Umfang beeinträchtigen oder die Einhaltung anderer Anforderungen in Bezug auf den sicheren Netzbetrieb gefährden würden.

Zusammengefasst heißt das, dass die Echtheit von Informationen oder einer Identität garantiert sein muss. Im speziellen Bezug auf Smart Metering bedeutet das, dass der gemessene Energieverbrauch nicht verfälscht sein darf, da dieser die Basis für die Berechnung darstellt.

(A) Availability: Verfügbarkeit

Es muss sichergestellt werden, dass Informationen, Systeme, Komponenten oder Prozesse, die für die planmäßige Bereitstellung/Einspeisung der durch die Anlage aggregierten elektrischen Leistung oder die Einhaltung anderer relevanter Anforderungen in Bezug auf den sicheren Netzbetrieb notwendig sind, im benötigten Umfang zur Verfügung stehen.

Zusammengefasst bedeutet das beispielsweise, dass ein Smart Meter ständig verfügbar sein muss, da sonst keine Stromverbräuche aufgezeichnet werden können.

Abbildung 10 veranschaulicht das Zusammenspiel der Kernbereiche und den Schutzzielen. Durch dieses Zusammenspiel kommt es zur gewünschten Informationssicherheit. Folglich kann so der einwandfreie und reibungsloser Einsatz der IT gewährleistet werden.

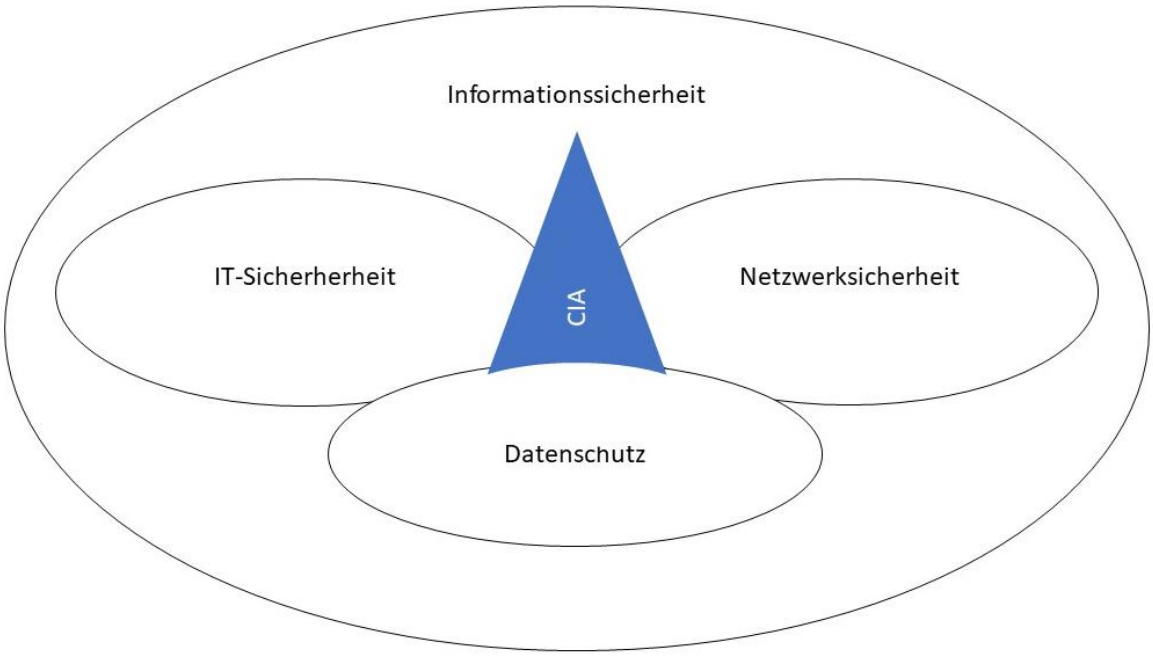


Abbildung 10: Zusammenspiel CIA – Kernbereiche
Quelle: eigene Darstellung

3.4 Sicherheitsprobleme

3.4.1 Akteure

In diesem Abschnitt soll der Personenkreis genauer bestimmt werden, welcher mit dem Smart Meter oder dem Smart Meter Gateway interagiert, ebenso eine Gruppierung derer, die potentiell die Absicht eines Angriffes oder Manipulation haben.

Grundsätzlich kommen drei Personengruppe in Frage, die autorisiert mit dem Smart Meter oder Gateway interagieren. An erster Stelle steht der Nutzer (Endverbraucher) selbst, denn er möchte tendenziell seine Verbräuche betrachten oder eigene Analysen anstreben. Die anderen zwei Gruppen sind dem Versorger zuzuordnen. Zu diesen Gruppen gehören zum einen der Gateway Administrator und zum anderen der Servicetechniker. Beide dienen mehr der Instandhaltung und der Gewährleistung des sicheren Betriebes. Natürlich findet auch auf dieser Seite eine Auswertung der Daten statt.

Umfeld		Rolle	Funktion/Nutzen
Autorisiert	Intern	Nutzer	Auswerten des Stromverbrauches und eigene Analysen
		Servicetechniker	Instandhaltung und Fehlersuche und -behebung
	Extern	SM-GW Admin	Konfiguration, Monitoring und Kontrolle des Smart Meter Gateways

Abbildung 11: Autorisierte Benutzergruppen
Quelle: eigene Darstellung, Daten entnommen aus BSI, 2014, S. 29

3.4.2 Potenzielle Angreifer

Die Anzahl der Angreifer sind nicht vorhersehbar bzw. kalkulierbar. Angreifer gehen weit über den klassischen Hacker hinaus. Im Grunde genommen kann jeder Besitzer eines Computers zu einem potenziellen Angreifer werden. Alle Angreifer lassen sich in zwei Gruppen unterteilen - interne und externe Angreifer.

Angreifer sind dabei nicht automatisch unautorisierte Zugriffe. Im Falle dessen, dass der Endkunde selbst der Angreifer ist, wäre er in diesem Moment eigentlich autorisiert, obwohl er einen Manipulationsversuch unternehmen würde.

Der externe Angreifer hingegen ist unautorisiert. Ihm wird im normalen Umfeld keine Rolle zugesprochen, deshalb unautorisiert. Den Endkunden unter Generalverdacht zu stellen wäre falsch, dennoch ist es theoretisch denkbar und wird somit als Angreifer aufgeführt. Dem Hacker wird eine kriminelle Energie zugesprochen, da es in der Natur des Hackers liegt anderen Schaden zu zufügen. Er wird im Vergleich als dauerhafte Gefahrenquelle eingestuft.

3.4.3 Potenzielle Bedrohungen / Angriffsszenarien

Diese Arbeit hegt nicht den Anspruch sämtliche Angriffsszenarien darstellen zu können. So wird es in naher Zukunft immer wieder neue Szenarien geben, da diese einer ständigen Veränderung ausgesetzt sind. Aus diesen Gründen sollen in diesem Abschnitt exemplarische Szenarien aufgezeigt werden, die theoretisch denkbar sind – in der Gegenwart oder der Zukunft.

Zeitmanipulation	Ein Angreifer (intern oder extern) versucht bei einem Datenaustausch zwischen dem Zähler und Gateway die Daten zu manipulieren. Ziel könnte dabei sein, die Zeit zu manipulieren, um so günstigere Strompreise zu erzielen.
Datenmissbrauch	Ein externer Angreifer ist, der mit abgefangenen Daten zwischen Gateway und WAN-Teilnehmern die Privatsphäre verletzen könnte. Im Falle eines Mehrfamilienhauses ist es denkbar, dass ein Mieter einer anderen Wohnung diese gleiche Art des Angriffes durchführt und Daten zwischen Gateway und Zähler abfängt (interner Angriff)
Infiltrierung	Durch gewaltsames Eindringen (umgehen von Sicherheitsmechanismen) kann ein Angreifer Kontrolle über die am Gateway angeschlossenen Geräte übernehmen und diese ein- und ausschalten oder dauerhaft manipulieren.

Infrastruktur	Einige Endkunden sind durch Photovoltaik-Anlagenzusätzlich mit Strom versorgt. Wenn diese den Strom nicht benötigen (Überangebot), wird er in das Stromnetz eingespeist. Hier können Angreifer die Menge an eingespeistem Strom manipulieren und so erheblichen Einfluss[25] auf das Stromnetz haben (externe Angreifer). Durch Manipulation interner Angreifer könnte ein finanzieller Vorteil für sie entstehen, da die „Vergütung“ nach eingespeister Menge stattfindet.
Preismanipulation	Durch Manipulation der eingespielten Preise in das Gateway lassen sich abrechnungsrelevante Veränderungen vornehmen.
Versorgung	Fernabschaltefunktionen (vgl. Anderson & Fuloria, 2010, S.6) können von Angreifern ausgenutzt werden und so hunderte bis tausende Kunden vom Netz nehmen und so unter Umständen für das Erliegen des öffentlichen Lebens sorgen.
Versorger	Einfallstor zum Versorger über das SM-Gw

[25] Es müsste sich hierbei um einen groß angelegten Angriff handeln, um nachweislich erheblichen Schaden anzurichten.

4.Regulatorische Rahmenbedingungen

4.1 Notwendigkeit

Ralf Hoffmann, 2010 Vizepräsident der ESMIG, Chairman der SM-CG und Vorstands Vorsitzender sagte gegenüber SmarterWorld:

> *„Fehlende bzw. veraltete Standards behindern die rasche Umsetzung von Smart-Metering-Lösungen in Europa“ (Arnold, 2010).*

Einheitliche Normen sind die Basis für eine schnelle und flächendeckende Ausbreitung von Smart Meter Systemen. Sie bieten den Firmen das Potential einer Massenproduktion und würden somit ein Einsparpotenzial bedeuten. Ein einheitliches Vorgehen innerhalb Europas bei der Herstellung von Smart Meter Systemen würde Europa in eine wichtige Rolle rücken.

4.2 National

Im September 2016 ist das Gesetz zur Digitalisierung der Energiewende verabschiedet worden und hat in Deutschland mit dem Messstellenbetriebsgesetz (MsbG) zur Grundlage für die Einführung von modernen Messeinrichtungen und intelligenten Messsystemen geführt.

Im Messstellenbetriebsgesetz werden unter anderem folgende Punkte geregelt:

- technischen Anforderungen an die Geräte (mME, SM-Gw)
- Einbau, Betrieb und die Wartung der Messeinrichtungen
- Datenkommunikation (Ab- bzw. Auslesen der Daten und ihre Übermittlung)

Für die technischen Anforderungen an die Geräte verweist das Gesetz im Kapitel 3 auf das BSI, welches die technischen Richtlinien und Schutzprofile beherbergt. In diesen Dokumenten werden die Anforderungen auf technischer Ebene genauer spezifiziert. Nur unter Einhaltung dieser Anforderungen kann ein intelligentes Messsystem zertifiziert werden und beim Endkunden verbaut werden. Durch die Einhaltung der Richtlinien und Schutzprofile wird nach bestandener Zertifikatsprüfung, dem Gateway eine Interoperabilität bescheinigt. Die Zertifizierung dokumentiert gleichzeitig, dass Datensicherheit und Datenschutz gewährleistet sind und die Schutzziele (3.2.4 Schutzziele (CIA) eingehalten sind.

4.3 Europa

Die 3. Binnenmarkt-Richtlinie Strom und Gas (2009/72/EU und 2009/73/EU) stehen für den Ausbau einer Smart-Metering Infrastruktur (vgl. Bundesnetzagentur, o. J.-a). Die technischen Anforderungen, wie im Messstellenbetriebsgesetz in Deutschland, werden in der Binnenmarkt-Richtlinie der EU nicht weiter spezifiziert. Zum Zeitpunkt des Inkrafttretens der Richtlinie wurde festgehalten, dass der Ausbau[26] intelligenter Stromnetze bis 2020 zu 80% durchgeführt sein muss (Bundesministerium für Wirtschaft und Energie, o. J.). Voraussetzung dafür war eine vorausgegangene positiv bewertete Kosten-Nutzen-Analyse.

Einen aktuellen Stand - mit belegbaren Daten - (Mitte 2020) zum Rollout innerhalb der EU gibt es nicht. Lediglich ein aktuell veröffentlichter Bericht der europäischen Kommission, der auf Daten aus 2018 zurückgreift, lässt zum damaligen Zeitpunkt vermuten, dass die angestrebten 80% nicht einzuhalten sind.[27]

	Initial CBA[28] result	**Revised CBA result**	**Latest CBA**
Austria	Positive	No new CBA	2010
Belgium	Negative/Inconclusive	Positive/inconclusive	2017
Bulgaria	N/A	Negative	2013
Croatia	N/A	Positive	2017
Cyprus	N/A	Inconclusive	2014
Czech Republic	Negative	Negative	2016
Denmark	Positive	N/A	N/A
Estonia	Positive	No new CBA	2011
Finland	Positive	No new CBA	2008

[26] Einbau von Zählern bei Verbrauchern
[27] Derer Staaten, die eine positive Kosten-Nutzen-Analyse aufgezeigt haben
[28] Cost–benefit analysis (dt. Kosten-Nutzen-Analyse)

France	Positive	Positive	2013
Germany	Negative	Negative	2013
Greece	Positive	No new CBA	2012
Hungary	Inconclusive	Pending	2018
Ireland	Positive	Negative	2017
Italy	N/A	Positive	2014
Latvia	Negative	Positive	2017
Lithuania	Negative	Inconclusive	2018
Luxembourg	Positive	Positive	2016
Malta	NO CBA	No new CBA	NO CBA
Netherlands	Positive	No new CBA	2010
Poland	Positive	Positive	2014
Portugal	Inconclusive	Positive	2015
Romania	Positive	No new CBA	2012
Slovakia	Negative	Inconclusive	2013
Slovenia	N/A	Positive	2014
Spain	No CBA	No CBA	No CBA
Sweden	Positive	N/A	2015
UK	Positive	Positive	2016

Tabelle 3: Auswertung durchgeführter Kosten-Nutzen-Analysen
Quelle: In Anlehnung an Europäische Kommission, 2020, S.40 f

In Abbildung 12 wird der ausgewertete Datenstand der Kosten-Nutzen-Analyse grafisch dargestellt. Aus ihr kann der angestrebte Zeitraum entnommen werden, den ein Mitgliedstaat der EU anstrebt, um einen 80 prozentigen Ausbaustatus zu erreichen.

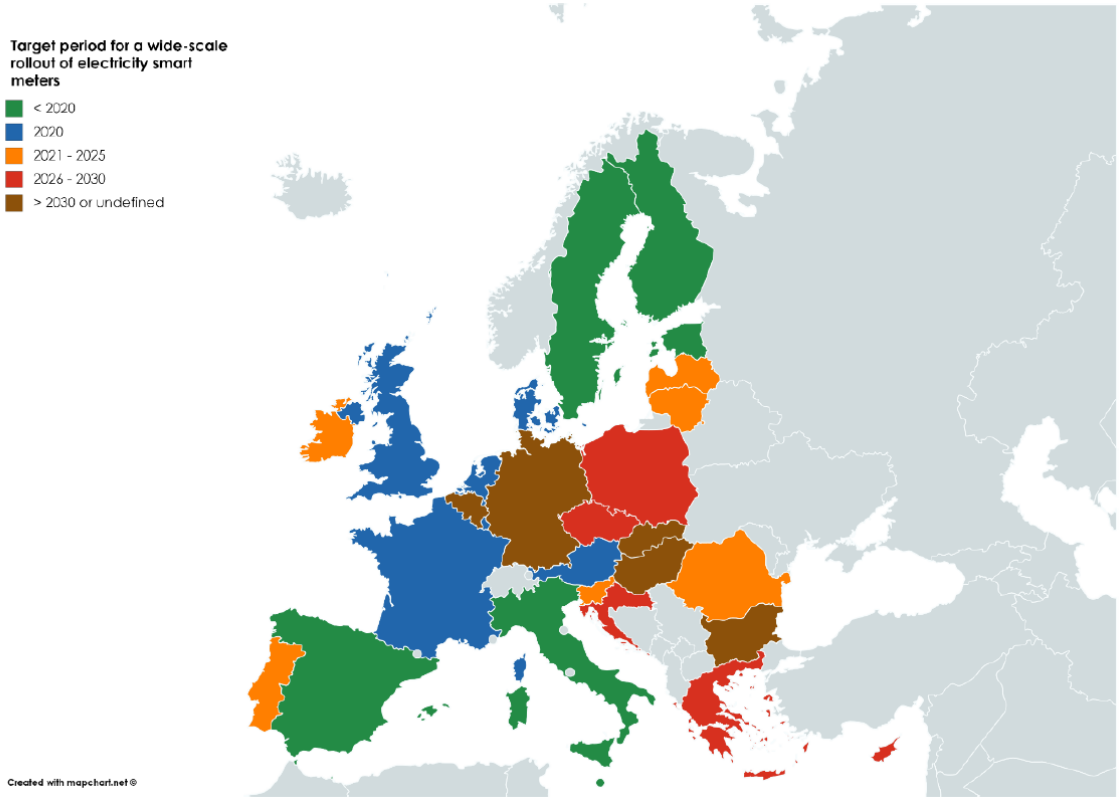


Abbildung 12: Zeitlich angestrebtes Ziel
Quelle: Europäische Kommission, 2020, S.21

4.4 Smart Meter Coordination Group

Die wohl bisher wichtigste Arbeit der Vereinigung ist das Mandat M/441, auf welches oben schon näher eingegangen wurde (2.3.3 European Mandat M/441). In diesem Kapitel soll sich mit dem Aufbau und der Funktion dieses Fachkreises und dessen Stellenwert in Europa auseinandergesetzt werden.

2009 fiel der Startschuss für die Arbeiten an diesem Standard. Mit dem Beginn dieser Arbeit erfolgte auch zeitgleich der Zusammenschluss der drei europäischen Normungsorganisationen. Das europäische Komitee für Normung (CEN)[29], das europäische Komitee für elektrotechnische Normung (CENELEC)[30] und das europäische Institut für Telekommunikationsnormen (ETSI)[31] sind für das M/441 verantwortlich und „Gründer“ der Smart Meter Coordination Group. Sie können unter dem Begriff „ESO’s“[32] zusammengeschlossen werden.

[29] fr. Comité Européen de Normalisation
[30] fr. Comité Européen de Normalisation Électrotechniqu
[31] en. European Telecommunications Standards Institute
[32] European Standards Organizations

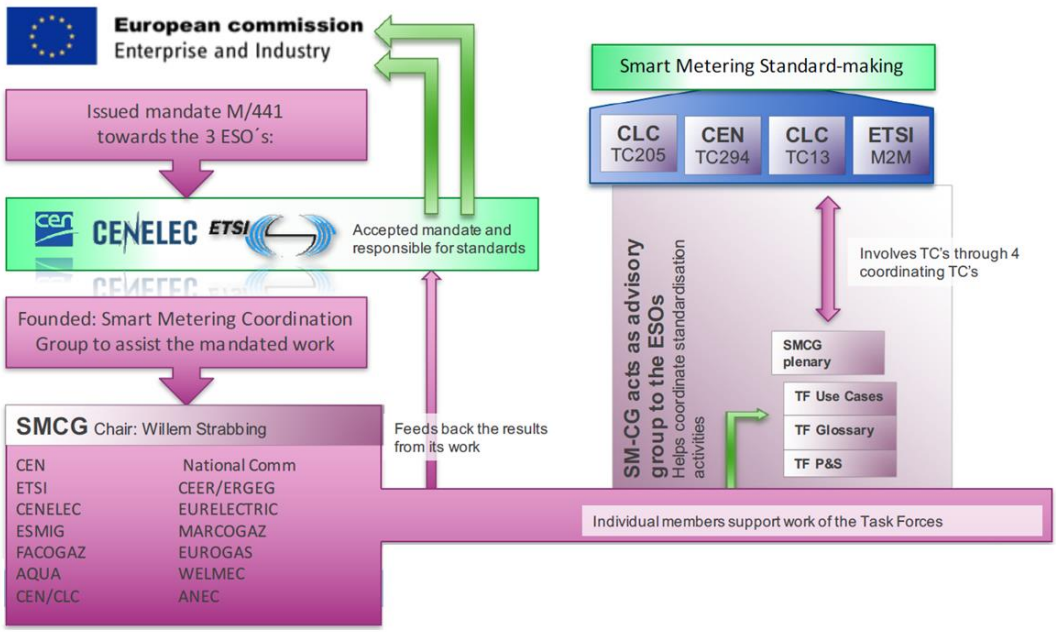


Abbildung 13: Struktur SM-CG
Quelle: In Anlehnung an ESMIG, 2017, S.2

Wie aus Abbildung 13 zu entnehmen ist, besteht die SM-CG nicht nur aus den Gründungsmitgliedern, sondern aus mehreren Organisationen, die den verschiedenen Bereichen der Energieversorgung zuzuordnen sind. Die Mitglieder erarbeiten dabei verschiedene Anforderungen für die jeweiligen Bereiche. Bei der Erarbeitung oder Überarbeitung der Standards nehmen CEN, CENELEC und ETSI selbstverständlich teil, behalten aber die Oberhand und erhalten Zuarbeit der anderen Mitglieder.

Es gibt vier Kernbereiche, die sich mit Standards im Smart Metering Bereich auseinandersetzen, sogenannte Technical Committees (TC). Jeder davon kann einer Normungsorganisation zugeteilt werden. So sind TC205 und TC13 der Normungsorganisation CENELEC, M2M dem ETSI und TC294 dem CEN zuzuordnen. Im Folgenden sollen die einzelnen Technical Committees betrachtet werden. Eine Betrachtung der bereits hervorgegangenen Standards wird an dieser Stelle nicht vorgenommen, da dies den Umfang übersteigen würde.

TC 13

Der Zuständigkeitsbereich der TC13 liegt seit 1990 in der Normung von Elektrizitätsmesstechnik (Einrichtungen oder Systeme) einschließlich intelligenter Messsysteme sowie Tarif- und Laststeuerung. Ebenfalls das Erarbeiten von Normen für Zählerprüfeinrichtungen und -verfahren.

Die Normen für Schnittstellen, die Verwendung in Netzleitsystemen finden, werden in der TC 57 geregelt.

TC 205

Erarbeitung von Normen, die die Integration von Steuer- und Regelanwendungen einschließlich Gateways unter verschiedenen Übertragungsmedien und öffentlichen Netzen unter Berücksichtigung elektrischer und funktionaler Sicherheit gewährleisten.

TC 294

Zuständig für das Erarbeiten von Normen für die Kommunikationssysteme von Zählern, sowie das Normen von Fernablesungen. Unabhängig vom gelieferten Medium.

M2M/SmartM2M

Wie der Name erahnen lässt, kümmert sich das TC Smart M2M um die Spezifikationen von Machine to Machine Kommunikationen und verfolgen so das Vorantreiben des Internet of Things (IoT)

5. Methodik

5.1 Datenerhebung

Um sich einen weitreichenden Überblick über momentan eingesetzte Standards und Normen verschaffen zu können, ist es notwendig sich die eingesetzten bzw. einzusetzenden Standards und Normen einzelner Länder anzusehen. Eine Betrachtung der 47 Länder in Europa oder nur der EU mit aktuelle 27 Mitgliedsstaaten, wäre theoretisch möglich, übersteigt aber den Umfang für diese Arbeit. Um sich dennoch einen aussagekräftigen Überblick verschaffen zu können, ist es erforderlich, eine Eingrenzung der zu betrachtenden Länder vorzunehmen. Fokussiert werden Deutschland, Österreich, Schweiz und die Niederlande. Die Entscheidung fiel in gemeinsamer Absprache mit dem Praxispartner und ist durch eine hervorragende Dokumentenlage zu begründen, die für den Aufbau einer Datenbasis entscheidend ist.

Um einen einheitlichen Datenstand zu erhalten und somit die Vergleichsprozesse zu optimieren, sind im Vorfeld Kategorien festgelegt worden (5.2 Evaluierung und Analyse), die es nach Möglichkeit zu erfassen gilt. Da davon auszugehen ist, dass bei vier zu betrachtenden Ländern, eine große Datenmenge anfallen wird, werden die Daten mittels einer Graphendatenbank aufgearbeitet und visuell dargestellt. Diese Art der Aufarbeitung ermöglicht einen schnelleren Überblick über eingesetzte Standards und Normen und daraus eventuelle Zusammenhänge bzw. Abhängigkeiten zu erkennen.

5.2 Evaluierung und Analyse

Für den länderübergreifenden Vergleich muss ein einheitliches Vorgehen bei der Auswahl der Dokumente, sowie eine einheitliche Datenerhebung vorliegen. Die Dokumente wurden von öffentlichen Einrichtungen oder non Profit Organisationen bezogen, welche für den Rollout von Smart Metering in ihrem Land verantwortlich sind oder aktiv bei der Gestaltung der Sicherheitsanforderungen mitwirken.

Da im Normallfall mehrere Dokumente gleichzeitig zur Verfügung stehen und aktiv eingesetzt werden, wurde sich am ranghöchsten Dokument orientiert und dieses als Basis für die weitere Datenerhebung zugrunde gelegt.

Ausgehend von diesem Dokument wurden referenzierte Quellen erfasst, mit denen sich im nächsten Schritt befasst wird und auch bei diesen Dokumenten die referenzierten Quelle dokumentiert werden (Abbildung 14).

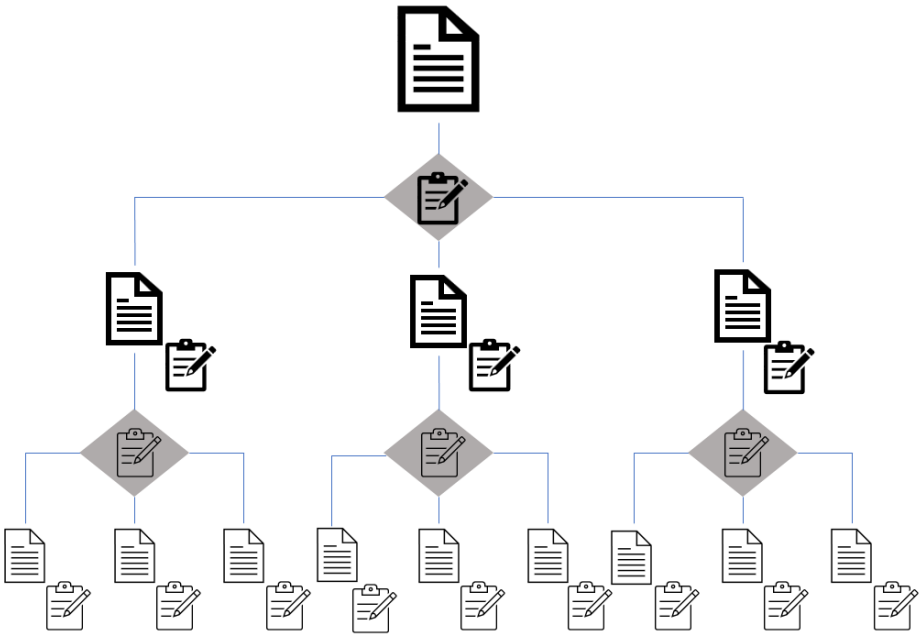


Abbildung 14: 2-Ebenen Struktur
Quelle: eigene Darstellung

Wie bereits zuvor erwähnt, ist es bei der Erfassung der referenzierten Dokumente wichtig, sich auf die exakt gleichen Kernpunkte zu fokussieren, um die Vergleichbarkeit zu gewährleisten. Dabei sind die wichtigsten Daten der Titel und die Version des Dokumentes. Anhand dieser beiden Angaben lässt sich ein Vergleich unter den Ländern vollziehen um gegebenenfalls Gemeinsamkeiten und Unterschiede erkennen zu können.

Um einen Anhaltspunkt über den Stellenwert des referenzierten Dokumentes zu erhalten, wird dokumentiert, wie oft jene Referenz im Dokument erwähnt wird – im Zusammenhang mit Graphendatenbanken, wird von sogenannten Kantengewichten gesprochen.

Da die gesammelten Daten nicht ausschließlich für den Zeck des Vergleiches erhoben worden, sondern später noch weiterverwendet werden sollen, wurde die Erfassung um folgende Punkte erweitert: Topic, Range, Tags, Comment, Link. Tabelle 4 fast alle Eckpunkte zusammen und beschreibt diese.

Eckpunkte	Ziel / Aussagekraft
Title*	Identifikation, Vergleichbarkeit
Version*	Identifikation, Vergleichbarkeit
Date	Dient zur Eingrenzung bei Recherchearbeiten
Topic	Dient der Gruppierung
Range	Gibt Aufschluss über Reich- Tragweite
Comment**	Zusätzliche Informationen (Bspw. Dokument bereits abgelöst)
Link	Dient dem schnellen Zugriff auf entsprechendes Dokument
Edge weight*	Aussagekraft über Stellenwert des referenzierten Dokumentes

* Mindestangaben
** Optional - nur im Bedarfsfall auszufüllen

Tabelle 4: Eckpunkte der Datenerhebung
Quelle: eigene Darstellung

5.3 Aufarbeitungsinstrument – Graphendatenbanken

Um die Zusammenhänge innerhalb eines untersuchten Landes oder bei einem Vergleich untereinander zu erkennen, ist die einfachste Möglichkeit, die gesammelten Daten visuell darzustellen. Durch eine visuelle Darstellung lassen sich komplexe Sachverhalte schneller überblicken und verstehen.

Einer der entscheidenden Vorteile, im Vergleich zu relationalen Datenbanken, sind die schnellen Zugriffszeiten. Neben der außerordentlich schnellen Zugriffszeit[33] können solche Datenbanken noch weitere Vorteile aufweisen (Eifrem, 2014):

Leistung: Der Grund für die schnelleren Zugriffszeiten liegt darin, dass die Beziehungen nicht zum Abfragezeitpunkt erzeugt werden müssen. Bei Graphendatenbanken werden Beziehungen beim Einfügen der Daten erzeugt, und sind ab diesen Zeitpunkt immer verfügbar.

Einfachheit: Anders als bei relationalen Datenbanken sind bei dieser Form der Datenspeicherung keine Normalisierung (Vermeidung von Redundanzen und Konsistenzfehlern) oder Denormalisierung (zur Beschleunigung des Datenzugriffs) notwendig. Es können also schnell neue Strukturen oder Prozesse abgebildet werden.

[33] bis zu 1000x schneller

Zuverlässigkeit: Durch die ACID-Prinzipien[34] kann von einer fehlerfreien Umgebung und von konsistenten Daten ausgegangen werden.

5.3.1 Neo4j

Neo4j ist aktuell der führende Anbieter im Sektor der Graphdatenbanken und hebt sich durch die eigene Abfragesprache Cypher hervor – Einer der ausschlaggebenden Entscheidungsgründe. Cypher ist eine deklarative Abfragesprache, deren Vorteil darin besteht, dass die Abfrage nicht aussagen muss, wie gesucht werden soll, sondern was gefunden werden soll (vgl. Litzel, 2020). Des Weiteren dient Cypher als Grundlage für die Entwicklung einer nach ISO/IEC standardisierten Graph Query Language (GQL), welches einen zukunftsorientierten Vorteil darstellt und einen nachhaltigen Ansatz verfolgt. Ein weiterer Vorteil gegenüber anderen Anbietern ist, das Neo4j eine der größten und aktivsten Community bietet und somit ein aktiver Austausch auf Plattformen wie Stackoverflow oder anderen Plattformen garantiert ist.

5.3.2 Importmöglichkeiten

Neo4j bietet eine Vielzahl an Importmöglichkeiten an. Angefangen bei dem klassischen Import mittels CSV[35]-Dateien über JSON[36] bis hin zum Neo4j Import Tool oder dem Import-Tool für Daten aus relationalen Datenbanken. Das Tool für den Datenimport aus relationalen Datenbanken wurde nicht berücksichtigt, da die Daten nicht in dieser Form zur Verfügung stehen. Der Import mit JSON schied ebenfalls aus, da resultierend aus der speziellen Notation die Datenerhebung erschwert worden wäre. Vorteil bei diesem Import wäre jedoch gewesen, dass nach dem Import die Datentypen nicht angepasst hätten werden müssen. Das Neo4j Import Tool ist ähnlich zum CSV Import, bedarf aber einer speziellen Notation in den CSV Dateien und erfolgt über das Command Line Tool. Durch diese Art des Imports können, im Vergleich zu dem normalen Import über CSV, deutlich mehr Optionen ausgewählt werden, die den Import erleichtern können. Typischerweise wird diese Variante des Imports erst bei größeren Datenmengen angewendet, da die zu erwartende Datenmenge der erhobenen Daten sich noch im Rahmen bewegte, fiel die Wahl auf den normalen CSV Import. Bei einer ordentlichen und einheitlichen Datenerhebung stellt der Import über die normale CSV Dateien kein Problem dar. Als Nachteil kann

[34] Atomicity, Consistency, Isolation, Durability - Regeln und Eigenschaften einer Transaktion
[35] Comma-separated values
[36] JavaScript Object Notation

angesehen werden, dass alle zu importierenden Daten als String erzeugt werden und somit eine teilweise Anpassung notwendig ist. Da während des Imports keine Datentypen angepasst werden können, wird dies automatisch im zweiten Teilschritt erfolgen.

Beide Teilschritte sind mittels Skripte erfolgt, welche im Anhang 01 eingesehen werden können.

6. Betrachtung der untersuchten Länder

Bei den jeweiligen Ländern erfolgte die Betrachtung immer von einem Ausgangsdokument und entsprechend des Schemas aus 5.2 Evaluierung und Analyse.

Bei der Erhebung der Daten ist aufgefallen, dass eine Vielzahl an Dokumenten im Literaturverzeichnis aufgelistet wurden aber nicht referenziert wurden. Aus diesem Grund wurden bei allen Abbildungen in diesem Abschnitt, nur Dokumente aufgelistet, die mindestens einmal referenziert wurden. Die numerische Angabe der gefundenen Dokumente erfolgt nach folgender Notation: *a(b)* wobei *a* für die Anzahl der Referenzierungen > 0 steht und *b* die Summe aller Dokumente (>= 0) darstellt. Bei der Betrachtung dieser Grafiken sollte bedacht werden, dass immer vom Ursprungsdokument aus anderer Literatur referenziert wird. Das bedeutet im Umkehrschluss, dass das jeweilige Hauptdokument (Ursprungsdokument) auf Basis der referenzierten Literatur entstanden ist beziehungsweise sich den Erkenntnissen bereits existierenden Dokumente bedient.

Alle Abbildungen in diesem Kapitel können im Anhang in einer größeren Darstellung betrachtet werden.

6.1 Deutschland

Beginnend mit der Datenerhebung für Deutschland ergaben sich 158(192) erfasste Dokumente und 228(266) Beziehungen zueinander (Abbildung 15). Als Ursprungsdokument für die Erfassung der Daten wurde das nach Common Criteria zertifizierte Dokument „BSI-CC-PP 0073“ zugrunde gelegt. Mit dem “Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)“ nimmt Deutschland eine Vorreiterrolle ein. Unter den untersuchten Ländern existiert kein weiterer Anforderungskatalog, welcher nach Common Critera zertifiziert ist. Ebenfalls zu erwähnen ist, dass das „BSI-CC-PP 0077“ ein weiteres Dokument ist, welches nach Common Criteria zertifiziert ist. Das „Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP)” weist Sicherheitsstandards wie im Online-Banking auf und ist somit einzigartig in Europa (Bundesministerium für Wirtschaft und Energie, 2020).

Die Grafik veranschaulicht, dass ein Großteil der verwendeten Dokumente sich aus RFCs[37] (Blau dargestellt) und technische Richtlinien des BSI (Gelb dargestellt) zusammensetzen. So besteht knapp die Hälfte[38] aller Dokumente aus RFCs und den technischen Richtlinien des BSI.

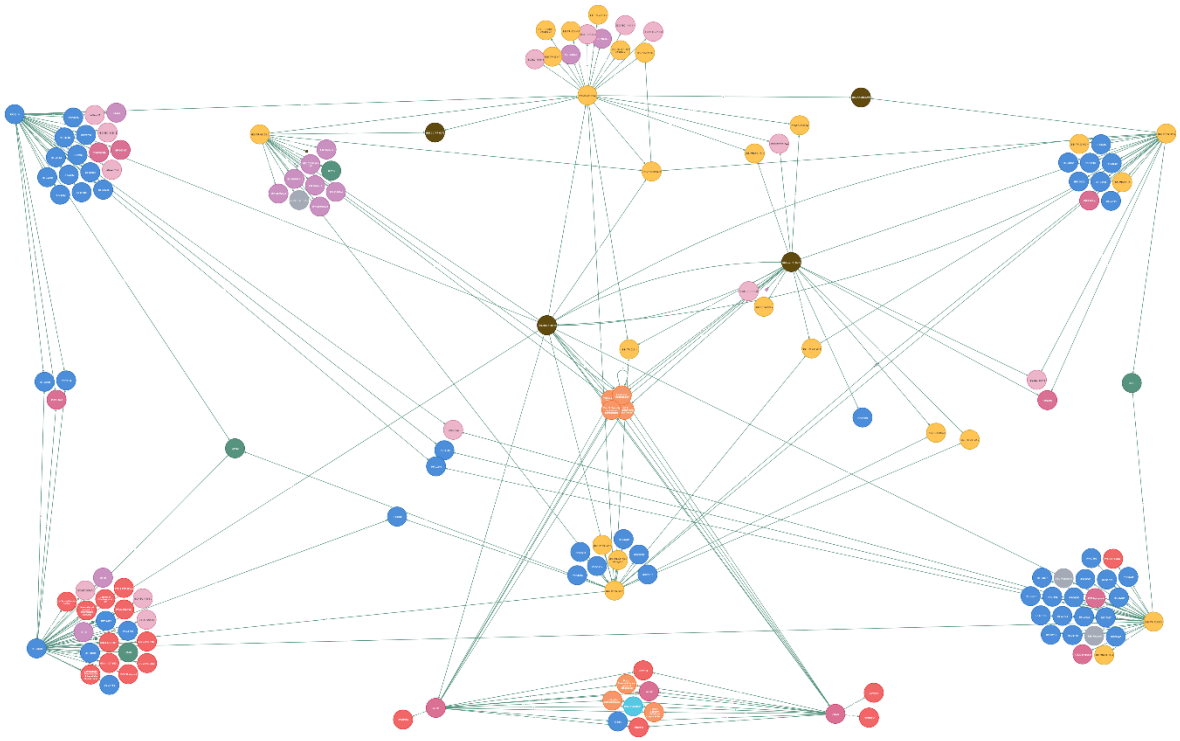


Abbildung 15: Darstellung Deutschland
Quelle: eigene Darstellung

[37] Request for Comments sind technische Spezifikationen die frei zur Verfügung gestellt werden und durch Internet Engineering Task Force (IETF) finanziert werden
[38] Rund 40%

Abbildung 16 veranschaulicht den direkten Einfluss der RFC auf die Erstellung des BSI-CC-PP 0073.

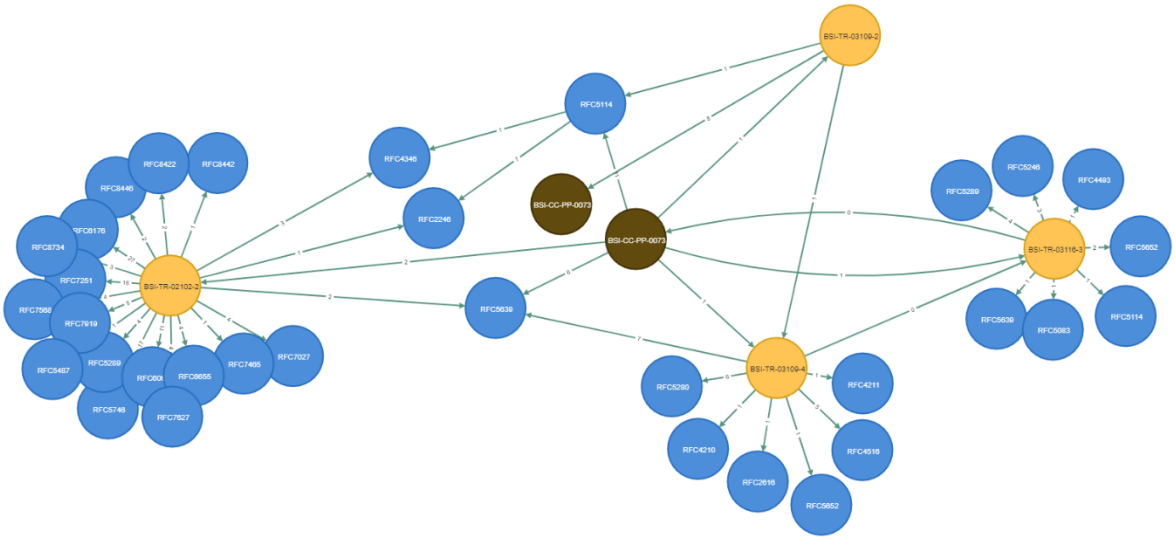


Abbildung 16: Einfluss RFC
Quelle: eigene Darstellung

6.2 Schweiz

Als Ausgangspunkt für die Betrachtung wurde das Dokument des Bundesamtes für Energie (BFE) „Richtlinien für die Datensicherheit von intelligenten Messsystemen“ zugrunde gelegt. Dieses Dokument besteht aus insgesamt drei Dokumenten, dem Hauptdokument und zwei weiteren Anhängen. Wobei nur das Hauptdokument auf weitere Dokumente verweist und somit auch nur das Hauptdokument in der Grafik ersichtlich ist. Ausgehend davon wurden 41(69) Dokumente und daraus resultierend 50(77) Beziehungen erfasst.

Die Zusammenhänge unter den Dokumenten kann grafisch wie folgt dargestellt werden:

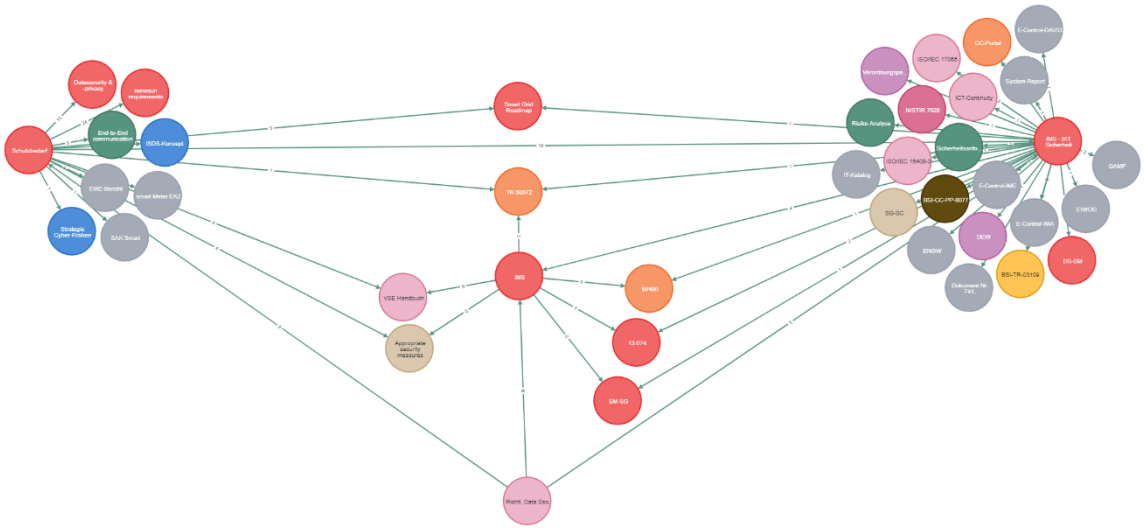


Abbildung 17: Darstellung Schweiz
Quelle: eigene Darstellung

Die Abbildung zeigt auf, dass die Schweiz bei der Formulierung an Smart Meter Anforderungen vorwiegend auf Dokumente des Bundesamtes für Energie zurückgreift – hier rot dargestellt. Eine weitere Erkenntnis ist, dass die Schweiz, im Vergleich zu anderen Ländern, wenig auf international anerkannte Standards setzt, beziehungsweise diese nicht direkt referenziert. Anhand der Kantengewichte lassen sich zwei Kerndokumente erkennen, die bei Erstellung des ursprünglichen Dokumentes, einen offensichtlichen Einfluss gehabt haben müssen. „Grundlagen der Ausgestaltung einer Einführung intelligenter Messsysteme beim Endverbraucher in der Schweiz“ und „Ansätze zur Gewährleistung der IKT-Sicherheit von intelligenten Messsystemen bei Endverbrauchern“ sind jeweils Dokumente des BFE und wurden am häufigsten referenziert. Beide setzen sich mit der Gewährleistung zur Einhaltung der Datensicherheit auseinander, wobei sich letzteres Dokument vordergründig auf verschiedene Szenarien konzentriert, wie die Datensicherheit gewährleistet werden kann – in Abhängigkeit zu Aufwand und Nutzen.

Das erst genannte Dokument verwies bezugnehmend auf Datensicherheit auf ein Dokument der European Union Agency for Cybersecurity (ENISA) – „Appropriate security measures for smart grids“. Es liegt nah, dass die in Anhang zwei des Ursprungsdokumentes aufgelisteten Standards (Anhang 03-1) sich am Dokument der ENISA orientieren.

Da bei allen anderen Ländern ein einheitliches Vorgehen verwendet wurde, können die Mindestanforderungen der Schweiz nicht grafisch aufgezeigt werden und stehen somit auch nicht im internationalen Vergleich zur Verfügung.

6.3 Österreich

Ausgehend vom Anforderungskatalog, der durch „Österreichs Energie“ in Zusammenarbeit mit ENCS[39] formuliert wurde, konnten für Österreich 226(254) Dokumente und 307(341) Relationen erfasst werden, die zur Datensicherheit beitragen. Das sich daraus ergebende Bild ist gegensätzlich zur Schweiz und weist, wie zu erwartend, wieder einen ähnlichen Charakter auf wie Deutschland.

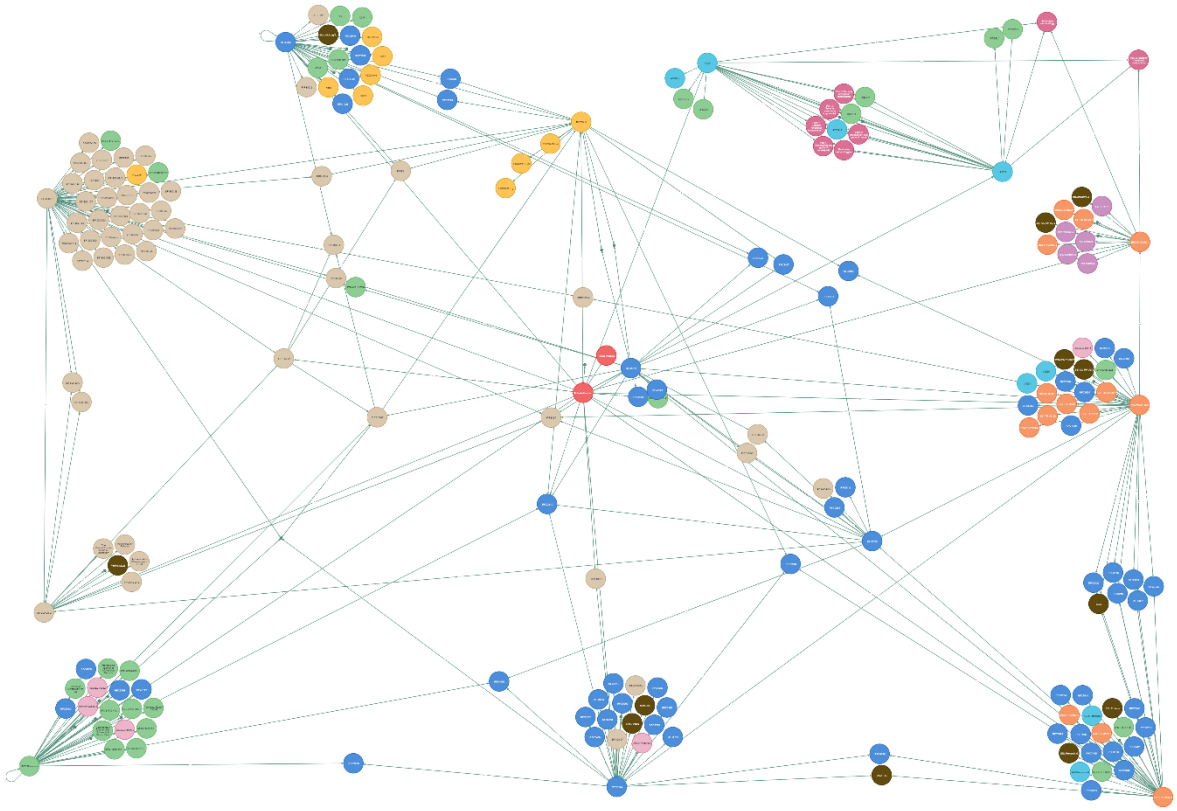


Abbildung 18: Darstellung Österreich
Quelle: eigene Darstellung

Trotz der Restriktion, dass nur Dokumente angezeigt werden, die mindestens einmal referenziert wurden, musste die Grafik weiter angepasst werden. Alle Dokumentengruppen, die nur ein Dokument enthielten, wurden mit einer einheitlichen Farbe versehen und sind minimiert. Die Abbildung zeigt, dass der Fokus von

[39] The European Network for Cyber Security – Eine non-profit Organisation, die einen Anforderungskatalog angefertigt haben und forciert in den Niederlanden zum Einsatz kommt (6.4 Niederlande)

Österreich auf zwei Dokumentengruppen liegt, nämlich RFC (Blau) und Beige dargestellt die Dokumente der US-Behörde „National Institute of Standards and Technology“ (NIST). Summiert man diese, machen diese beiden allein fast die Hälfte[40] aller Dokumente aus.

6.4 Niederlande

Das Erfassen der niederländischen Daten gestaltete sich etwas schwieriger. Es gibt nur wenige Informationen über die verwendeten Standards in den Niederlanden beziehungsweise ist es generell schwieriger als bei den anderen Ländern an Informationen zu gelangen, da auch keine Informationen zu Prüfstellen erlangt werden konnten. Durch Kontaktaufnahme zu dem holländischen Unternehmen NMI[41], welches auf dem Gebiet des Messwesens Spezialist ist, konnte sich in gemeinsamer Absprache auf ein Dokument geeinigt werden, welches als Grundlage für die Datenerhebung genutzt werden konnte. Das Dokument SM-301-2020 (Security requirements for procuring smart meters) der ebenfalls holländischen Firma ENCS, welche auch bei dem Erstellen des Anforderungskatalog von Österreich mitgewirkt hat, wurde als Basis zur Datenerhebung genommen.

Mit 485(681) Dokumenten und 508(726) Beziehungen ist Niederlande mit Abstand das umfangreichste Land. Diese Vielzahl an Dokumenten bereitete diverse Schwierigkeiten seitens Neo4j. So ist es in diesem Fall leider nicht möglich, eine Grafik bereitzustellen, um die Ausmaße und Zusammenhänge darstellen zu können, da das Tool leider nur 300 Nodes und die entsprechenden Beziehungen dazu zeitgleich anzeigen kann. Das machte die Auswertung nicht so einfach und komfortabel, wie man es sich von einer Graphendatenbank erhofft und es bei den anderen Ländern der Fall gewesen ist. Die Auswertung konnte leider nur in tabellarischer Form durch Cypher-Abfragen erfolgen. Anhang 05 und Anhang 06 dienen als Ersatz für die nicht erstellbaren Grafiken und soll die beschriebenen Daten nachvollziehbar veranschaulichen

Wie im Anhang 06 zu erkennen ist, liegt der Fokus, ebenfalls wie in Österreich und Deutschland, auf den Standards und Richtlinien von RFC und NIST. Der Großteil, ist aber den Publikationen zuzuschreiben, die beispielsweise im Rahmen von

[40] 112 von 226

[41] Nederlands Meetinstituut (NMI) ist ein weltweit anerkanntes unabhängiges Unternehmen, welches sich auf dem Gebiet des Messwesens durch Prüf- und Zertifizierungsangebote einen hervorragenden Ruf erarbeitet hat

jährlichen Tagungen, wie den „Journal of Cryptology“ oder der „EUROCRYPT“ entstehen. Der höhere Stellenwert ist aber den RFC’s und den Richtlinien des NIST zuzuordnen, da sie offizielle Standards und Richtlinien sind. Die Journals sind hingegen sehr aktuell[42], aber mehr darauf ausgerichtet, über derzeit vorherrschende Probleme gegenwärtiger Standards zu informieren.

6.5 Protection Profile EU

Das erst im Dezember 2019 veröffentlichte “Protection Profile for Smart Meter - Minimum Security requirements” ist nach dem Mandat M/411 das wohl wichtigste Dokument, was die Smart Meter Coordination Group veröffentlicht hat und könnte in Zukunft einen ähnlichen Stellenwert erlangen wie das Mandat M/411. Aus dem bereits genannten Dokument, welches die Basis darstellt, sind insgesamt 9(10) Dokumente und 23(24) Beziehungen untereinander hervorgegangen. Somit ist das Protection Profile der EU das Dokument mit der geringsten Dokumentendichte.

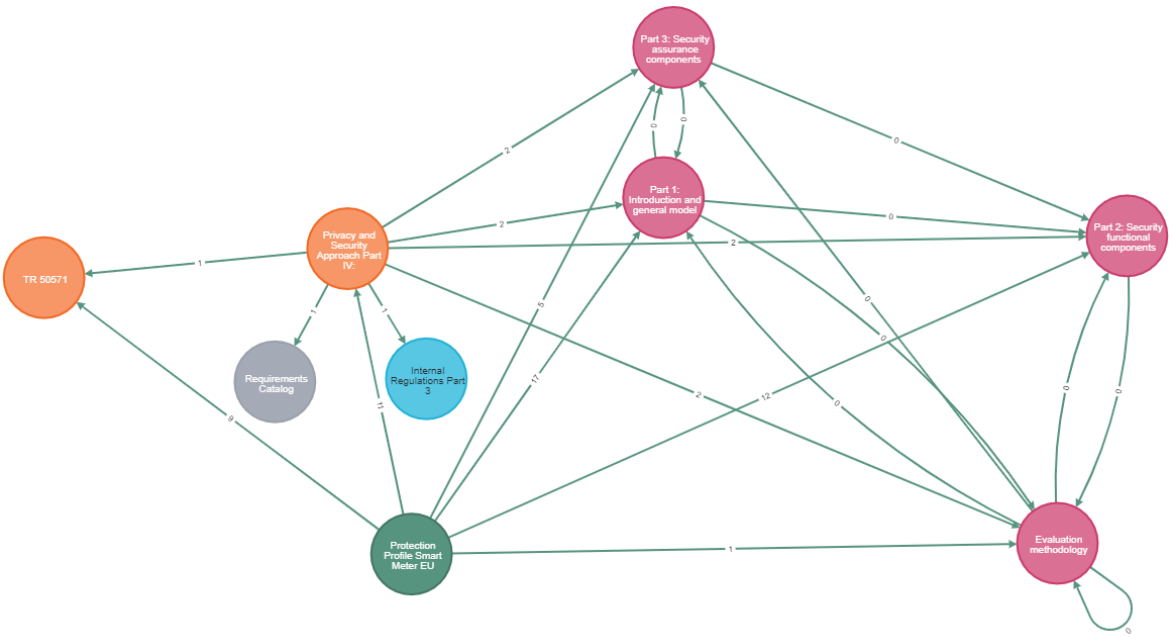


Abbildung 19: Darstellung Protection Profile EU
Quelle: eigene Darstellung

Da die geringe Anzahl der Dokumente es zulassen, können an dieser Stelle ergänzend zu der Grafik einige Anmerkungen getroffen werden. Die auf der rechten Seite angeordneten Dokumente (rötlich eingefärbt) sind alles Dokumente des

[42] Meist jährlich stattfindende Treffen, aus denen die Journals hervorgehen

CommonCriteria und haben eher formellen Charakter, wie beispielsweise den Aufbau eines Protection Profiles.

Das blau eingefärbte Dokument zeigt interne Regularien der CEN/CENELEC, die das Wording der Anforderungen spezifizieren. Durch den Umstand, dass der „Requirements Catalog“ (Grau eingefärbt) und die „TR 50571“ (Orange eingefärbt) nicht zugänglich sind, konnte nur das Dokument „Privacy and Security Approach – Part IV: Minimum security requirements for AMI components“ (Orange eingefärbt - mittig angeordnet) genauer betrachtet werden, zusätzlich zu dem Ursprungsdokument.

.

7. Auswertung und Ergebnisdarstellung

Die bisher erhobenen Daten geben Aufschluss über die Dokumentenarten, die für die Datensicherheit eine wichtige Rolle spielen. Wichtiger ist es, die Daten der einzelnen Länder in ihrer Gesamtheit zu betrachten, um daraus noch bessere Rückschlüsse ziehen zu können. Durch die Betrachtung aller erhobenen Daten können Schnittmengen zwischen den Ländern gebildet werden und daraus Kerndokumente ermittelt werden, die für die Einhaltung der Datensicherheit eine absolut unerlässliche Rolle spielen und berücksichtigt werden müssen. Damit diese Rückschlüsse gezogen werden können, wurden alle bereits gesammelten Daten in einem einzigen Graphen vereint.

Für die Interpretation der Schnittmengen im Ländervergleich wurde auf die Kanten zwischen den Dokumenten verzichtet, da diese keinerlei Auswirkung auf die Interpretation der Ergebnisse liefern. Dennoch wurden die Kantengewichte den entsprechenden Dokumenten zugeordnet, um weiterhin den Stellenwert der Dokumente nachvollziehen zu können.

Insgesamt enthält der Graph 1435 Dokumente. Das ist mehr als die bereits erzeugte Menge an Dokumenten aus den vorherigen Graphen. Der Unterschied resultiert aus den teilweise doppelt erzeugten Dokumenten. Das liegt daran, dass sonst nicht nachweisbar ist, aus welchem Land dieses Dokument stammt. Eine weitere Veränderung der Daten zu den vorherigen ist, das den Knoten (die Dokumente) eine Eigenschaft „Country“ hinzugefügt wurde, um zu erkennen welches Land dieses Dokument verwendet hat. Ebenfalls werden die Dokumente nicht mehr nach Datum und Version getrennt, da es bei diesem Vergleich keine Rolle spielt, welche Version von einem Dokument verwendet wurde, sondern ob das Dokument verwendet wurde.

7.1 Schnittmenge Niederlande – DACH-Nationen – Protection Profile EU

Für den Vergleich zwischen den untersuchten Ländern und dem Protection Profile der EU hat sich bei folgender Restriktion*: Kantengewicht > 0 und mindestens von zwei Ländern referenziert*, folgendes Bild ergeben (Abbildung 20). Zu erkennen ist, dass von den 63 gemeinsamen Dokumenten, wieder ein Großteil durch 21 RFC Dokumente eingenommen wird. An zweiter und dritter Stelle reihen sich 12 NIST Dokumente und 8 technische Richtlinien vom BSI ein. Somit ist über die Hälfte der

gesamten Dokumente aus drei Dokumentengruppen bestehend – RFC, NIST und BSI TR. Abbildung 20[43] ist in Form einer Tabelle im Anhang 09 – 1-2 dargestellt, um die Schnittmenge in Wort aufzuzeigen. Aus der Tabelle kann entnommen werden, welche Dokumente von einem oder mehreren Ländern Berücksichtigung fanden, sowie eine stichwortartige Beschreibung mit dem Kerninhalt dieses Dokumentes.

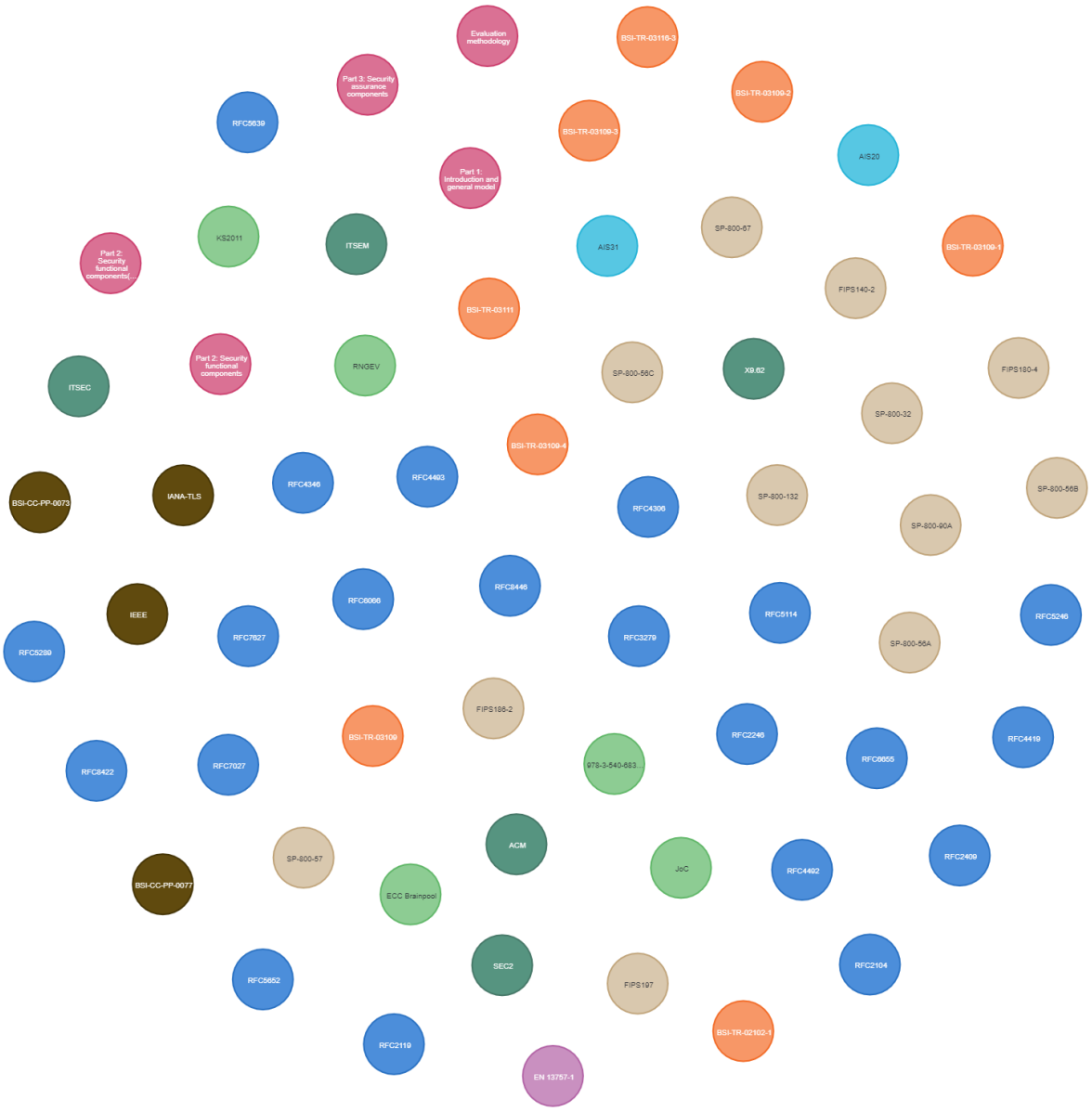


Abbildung 20: Vergleich Niederlande und DACH-Nationen
Quelle: eigene Darstellung

[43] Detailansicht im Anhang 08

7.2 Schnittmenge zu Smart Grid Set of Standards

Im Verlauf der Datenerhebung ist bei der Recherche ein Dokument aufgefallen, welches einen vielversprechenden Inhalt erwarten lies. Da nach genauerer Betrachtung diesem Dokument ein hoher Stellenwert zugesprochen werden konnte, erfolgte außerhalb des gesteckten Rahmens ebenfalls eine Datenerhebung. Bei diesem Dokument handelt es sich um das „Smart Grid Set of Standards“ in der Version 4.1 aus dem Jahr 2017, welches von der CEN-CENELEC-ETSI Coordination Group on Smart Energy Grids (CG-SEG) verfasst wurde (CEN-CENELEC-ETSI, 2017). Dieses Dokument bietet einen nahezu vollumfänglichen Überblick über bereits bestehende oder noch erscheinende Standards, welche Kommunikationsprotokolle und Datenmodelle spezifizieren, um den Datenaustausch zu gewährleisten. Es wurde dafür vorgesehen, ein Rahmenwerk zu stellen, welches den Ausbau eines Smart Grid in Europa unterstützen kann.

Die in Anhang 10 1-3 aufgeführten Standards entstammen dem oben genannten Dokument und sind auf die Referenzarchitektur des Mandats M/411 zugeschnitten. Um die Schnittmenge zwischen diesem Dokument und den bereits erfassten Daten zu ermitteln, wurde auch bei diesem Dokument das gleiche Vorgehen angewandt wie bei den anderen Ländern. Abbildung 21 zeigt die Schnittmenge.

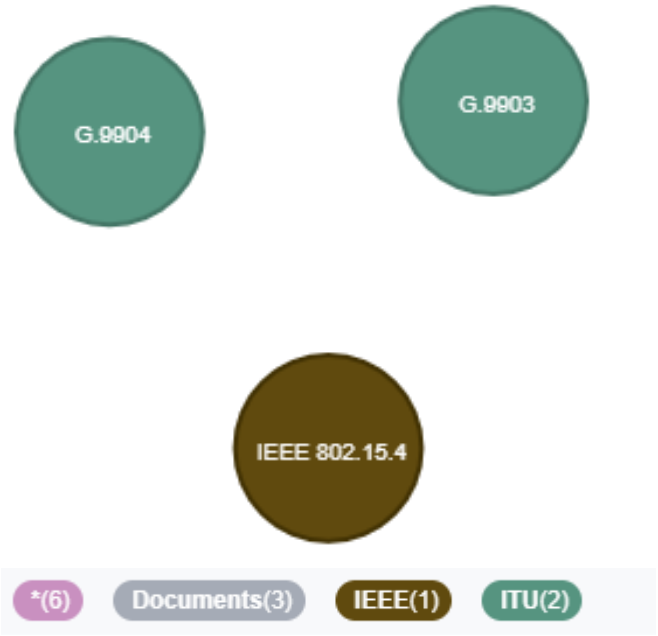


Abbildung 21: Schnittmenge Set of Standards - untersuchte Länder
Quelle: eigene Darstellung

Das Resultat der Schnittmengen ist unerwartet gering ausgefallen. Das kann zwei Gründe haben. Erstens, es wurden beispielsweise keine Standards für Kryptografie verwendet oder zweitens, es wurden andere kryptografische Standards als in den bisher erhobenen Daten verwendet.[44] Praktisch kommt aber nur der zweite Grund infrage, da die Wahrscheinlichkeit gegen Null tendiert, dass keine kryptografischen Standards berücksichtigt wurden.

[44] Möglich ist dabei auch, dass einige Standards in der Zwischenzeit durch eine neue Version (bspw. TLS Version 1.2 zu 1.3) überholt wurden und die neuere Version eine andere Bezeichnung erhalten obwohl es theoretisch bei dem gleichen Standard geblieben ist

8. Fazit

8.1 Zusammenfassung

Der Wandel zu einem neuaufgelegten Stromnetz durch vermehrten Einsatz von Informations- und Telekommunikationssysteme hat bereits begonnen. Ein wichtiger Bestandteil für die Umwandlung vom klassischen zum neuen Stromnetz – Smart Grid. Smart Grids sind digitalisierte Stromnetze deren Hauptkomponente intelligente Stromzähler, bestehend aus modernen Messeinrichtungen und Gateways, sind. Durch den Einsatz dieser Komponenten entstehen für Versorger und Verbraucher neue Möglichkeiten. Durch verbesserte Analysemöglichkeiten können Stromressourcen effizienter eingesetzt und gespeichert werden, um Lastspitzen und Schwankungen in der Versorgung durch erneuerbare Energien abzufangen, beziehungsweise diesen vorzubeugen. Mit dem vermehrten Einsatz von Informations- und Telekommunikationssysteme entstehen neben den Vorteilen auch Risiken. Bisher war es wichtig, den Versorger vor Cyberangriffe zu schützen. Durch den Einsatz von intelligenten Stromzählern wird die Angriffsfläche vergrößert und erhöht somit die potenzielle Anzahl der Angriffe. Nicht nur der Versorger ist dadurch gefährdeter als jetzt, sondern auch der Verbraucher. Durch einen ständigen Datenaustausch zwischen Verbraucher und Versorger können durch Angriffe sensible Daten in falsche Hände geraten. Damit Verbraucher, wie auch Versorger, weiterhin gut geschützt sind, müssen strikte Richtlinien und Anforderungen an die eingesetzten intelligenten Stromzähler formuliert und angewendet werden.

Standards, Richtlinien und formulierte Anforderungen an moderne Messeinrichtungen und Gateways existieren viele, jedoch ohne einheitliches Vorgehen auf europäischer Ebene. Die einzelnen Mitgliedsstaaten dürfen zum Großteil selbst bestimmen wie die Anforderungen umgesetzt werden. Bereits existierende europäische Dokumente formulieren lediglich einen groben Rahmen, in dem sich bewegt werden muss – wie die Anforderungen umgesetzt werden, bleibt den Ländern überlassen. Die erhobenen Daten veranschaulichen diese Situation teilweise. Länder wie Deutschland und Österreich haben eine sehr gut ausgearbeitete Dokumentenstruktur und klare Anforderungen, nach denen vorgegangen beziehungsweise gearbeitet werden muss. Die Schweiz hingegen hat eine geringe Dokumentenstruktur und weist nicht den soliden Charakter wie Deutschland und Österreich auf. Die

Dokumente von Deutschland und Österreich vermitteln den Eindruck von Transparenz und einem Rundum-sorglos-Paket.

Niederlande und die Schweiz nehmen unterdessen eine gewisse hybride Rolle ein. Die Schweiz kommuniziert klar ihr Vorgehen im Punkto Sicherheitsüberprüfung, schwächelt aber bei der Qualität ihrer Dokumente. Es werden Anforderungen (Anhang 03-1) formuliert, dem Leser dabei aber nicht mitgeteilt, auf welche Standards gesetzt werden muss. Im direkten Vergleich mit Deutschland und Österreich wird ein eher oberflächlicherer Eindruck vermittelt. Auch die Niederlande schneiden bei der Dokumentenqualität bessert als die Schweiz ab. Der Kritikpunk an den Niederlanden ist der generell schlechte Informationsfluss im Hinblick auf Sicherheitsüberprüfung und eventuell existierende Dokumente.

Die Untersuchung hat mehrere Erkenntnisse hervorgebracht. Zum einen wurde sich über die Länder ein umfassender Über- und Einblick verschafft und somit Wissen über die dort jeweiligen Standardisierungen- und Prüfeinrichtungen erlangt. Weiterhin wurde sich damit ein Bild über die meistverwendeten Standards verschafft und daraus resultierend erkannt, welche Organisationen entscheidende Rollen einnehmen. Durch diese Informationen ist es möglich, diese Standards bei einem europaweiten einheitlichen Vorgehen zu berücksichtigen und damit bereits einen Großteil an Anforderungen abgedeckt wird. Neben diesen Resultaten hatten die Untersuchungen noch einen Nebeneffekt. Durch die tiefreichende Betrachtung der länderspezifischen Dokumente, konnten neben den einschlägigen Organisationen noch weitere Organisationen ermittelt werden, die einen Eindruck hinterließen, der es notwendig erscheinen lässt, sich diese genauer zu betrachten und für zukünftige Schritte zu berücksichtigen. Neben den positiv zu erwähnenden Erkenntnissen sind während der Arbeit auch negativ zu erwähnende Umstände aufgefallen. Es stellt sich die Frage, wieso auf europäischer Ebene nicht ein Weg vorgegeben wird, den es umzusetzen gilt, sondern nur grobe Rahmen formuliert werden in denen sich bewegt werden soll. Ein einheitliches Vorgehen würde Herstellern und Ländern einen deutlich schnelleren Prozess erlauben. Im Hinblick auf das europaweit stark vernetzte Stromnetz ist dieser Fakt ein nicht unwichtig erscheinender Punkt und Vorteil, der verspielt wird. Hinzu kommt, warum ein europaweit veröffentlichtes Dokument von einer extra dafür gebildeten Einheit nicht ihre eigenen Dokumente

referenziert, in denen geltende Standards aufgelistet sind, die speziell auf die Referenzarchitektur zugeschnitten sind.

Eine nicht themenspezifische Auffälligkeit, die aber nachdenklich stimmen sollte, ist die Erkenntnis, dass teilweise weltweit tätige Normungsorganisationen ihre formulierten Richtlinien nicht frei zur Verfügung stellen. Somit kann eine gewisse Art von Benachteiligung entstehen. Als Beispiel kann die Entwicklung des Internets beziehungsweise allgemein der Telekommunikationstechnik genannt werden, die unter diesen Umständen nicht so schnell vollzogen gewesen wäre. Die öffentliche kostenfreie Bereitstellung hat wesentlich ihren Teil dazu beigetragen, diese rasante Entwicklung zu ermöglichen.

8.2 Ausblick

Das in Kapitel 7.2 Schnittmenge zu Smart Grid Set of Standards hinzugezogene Dokument und die darin erwähnten Standards müssen genauer betrachtet und kategorisiert werden, um die aufgeworfene Frage final beantworten zu können. Dadurch ist eine Validierung der bisher herausgefilterten Schnittmenge zu erwarten.

Unabhängig vom Ausgang der oben genannten Betrachtung können mittels der erfassten Daten Anforderungen formuliert werden und so eine Zusammenstellung der Anforderungen erarbeitet werden, mit denen der europäische Markt bedient werden kann.

Literaturverzeichnis

Agora Energiewende. (2017). Energiewende und Dezentralität. Zu den Grundlagen einer politisierten Debatte. Abgerufen von https://www.agora-energiewende.de/fileadmin2/Projekte/2016/Dezentralitaet/Agora_Dezentralitaet_WEB.pdf

Anderson, R. & Fuloria, S. (2010). Who controls the off switch? Abgerufen von https://www.cl.cam.ac.uk/~rja14/Papers/meters-offswitch.pdf

Apel, N. (2017, Juni 8). Die Umsetzung des IT-Sicherheitsgesetzes aus Sicht des BSI. Abgerufen 02. September 2020, von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/2GS-Tag_2017/Apel_Die_Umsetzung_des_IT_Sicherheitsgesetzes.pdf?__blob=publicationFile&v=2

Arnold, H. (2010, November 17). Europäische Standards für Smart Metering. Abgerufen 02. September 2020, von https://www.smarterworld.de/smart-energy/smart-meter/goerlitz-eu-hilft-smart-meter-herstellern.30603.html

BDEW. (2019, März). BDEW Bundesverband der Energie- und Wasserwirtschaft e.V. Reinhardtstraße 32 10117 Berlin Branchenspezifischer Sicherheitsstandard für Anlagen oder Systeme zur Steuerung / Bündelung elektrischer Leistung (B3S Aggregatoren). Abgerufen von https://www.bdew.de/media/documents/Awh_20190301_B3S-fuer-Anlagen-zur-Steuerung-und-Buendelung-elektrischer-Leistung.pdf

BMWI. (o. J.). EU-Klima- und Energierahmen 2030. Abgerufen 02. September 2020, von https://www.erneuerbare-energien.de/EE/Navigation/DE/Recht-Politik/EU_Klima_Energierahmen/eu_klima_und_energierahmen.html

BSI. (o. J.). BSI - IT-Grundschutz-Kompendium - Glossar. Abgerufen 22. Juni 2020, von https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/vorkapitel/Glossar_.html

BSI. (2014, März). Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP). Abgerufen von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0073b_pdf.pdf?__blob=publicationFile&v=1

BSI & BMWi. (o. J.). KRITIS - Einführung. Abgerufen 02. September 2020, von https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html

Bundesministerium für Wirtschaft und Energie. (o. J.). BMWi - Gibt es einen europarechtlichen Hintergrund für den Einbau von Smart Metern? Abgerufen 02. September 2020, von https://www.bmwi.de/Redaktion/DE/FAQ/Smart-Meter/BMWi/faq-intelligente-netze-intelligente-zaehler-frage-07.html

Bundesministerium für Wirtschaft und Energie. (2020, März). Smart-Meter und digitale Stromzaehler. Abgerufen von https://www.bmwi.de/Redaktion/DE/Publikationen/Energie/smart-meter-und-digitale-stromzaehler.pdf?__blob=publicationFile&v=4

Bundesnetzagentur. (o. J.). Bundesnetzagentur - Messeinrichtungen / Zähler. Abgerufen 02. September 2020, von https://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Verbraucher/Metering/SmartMeter_node.html

Bundesnetzagentur. (2011, Dezember). „Smart Grid“ und „Smart Market“. Abgerufen von https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/NetzzugangUndMesswesen/SmartGridEckpunktepapier/SmartGridPapierpdf.pdf?__blob=publicationFile&v=2

CEN-CENELEC-ETSI. (2017, Januar). SmartGridSetOfStandards. Abgerufen von ftp://ftp.cencenelec.eu/EN/EuropeanStandardization/Fields/Energy-Sustainability/SmartGrid/SmartGridSetOfStandards.pdf

CEN/CLC/ETSI. (2011, Dezember). Technical Report 50572. Abgerufen von https://courses.edx.org/c4x/DelftX/NGI102x/asset/Functional_reference_architecture_for_communications_in_smart_metering_systems.pdf

Dudenredaktion (Hrsg.). (o. J.). „Blackout“. In Duden. Abgerufen von https://www.duden.de/node/23267/revision/23296 (Abrufdatum: 10.06.2020)

E.DSO. (o. J.). Why smart grids? | E.DSO. Abgerufen 12. Juni 2020, von https://www.edsoforsmartgrids.eu/home/why-smart-grids/

Eifrem, E. (2014, Dezember 9). Graphendatenbanken: Fünf gute Gründe für den Umstieg. Abgerufen 7. August 2020, von https://entwickler.de/online/datenbanken/graphendatenbanken-fuenf-gute-gruende-fuer-den-umstieg-115004.html

EnBW. (o. J.). Stromnetz. Abgerufen 02. September 2020, von https://www.enbw.com/energie-entdecken/verteilung-und-transport/stromnetz/

ESMIG. (2017, Februar). Public and private partnership in certification. Abgerufen von https://esmig.eu/sites/default/files/esmig_presentation_-_cyber_security_certification.pdf

Europäische Kommission. (2020, März). Benchmarking smart metering deployment in the EU-28. https://doi.org/10.2833/492070

Gensrich, E. (2017, Juni 29). So realisieren Sie mit Smart Home Einsparpotenziale. Abgerufen 02. September 2020, von https://partner.mvv.de/blog/so-realisieren-sie-mit-smart-home-einsparpotenziale

IEA. (2018). World Energy Outlook 2018. Abgerufen 02. September 2020, von https://www.iea.org/reports/world-energy-outlook-2018

IEA. (2019). World Energy Balances. Abgerufen von https://iea.blob.core.windows.net/assets/8bd626f1-a403-4b14-964f-f8d0f61e0677/World_Energy_Balances_2019_Overview.pdf

Leopoldina, acatech & Akademiunion. (2020, Januar). Zentrale und dezentrale Elemente im Energiesystem. Abgerufen von https://www.leopoldina.org/uploads/tx_leopublication/2020_ESYS_Stellungnahme_Energiesystem.pdf

Litzel, N. (2020, März 11). Was ist Cypher? Abgerufen 02. September 2020, von https://www.bigdata-insider.de/was-ist-cypher-a-912813/

PPC-AG. (2020, Februar 27). Smart Meter Gateways (SMGWs) von PPC. Abgerufen 02. September 2020, von https://www.ppc-ag.de/produkte-services/smart-meter-gateways/

Smart Grids Austria. (2016). Smart Grids - Smartgrids Austria. Abgerufen 02. September 2020, von https://www.smartgrids.at/smart-grids.html

Stadtwerke Kempen. (o. J.). Stadtwerke Kempen. Abgerufen 02. September 2020, von https://www.stadtwerke-kempen.de/de/Strom/Messstellenbetrieb/Moderne-Messeinrichtung/

Anhang

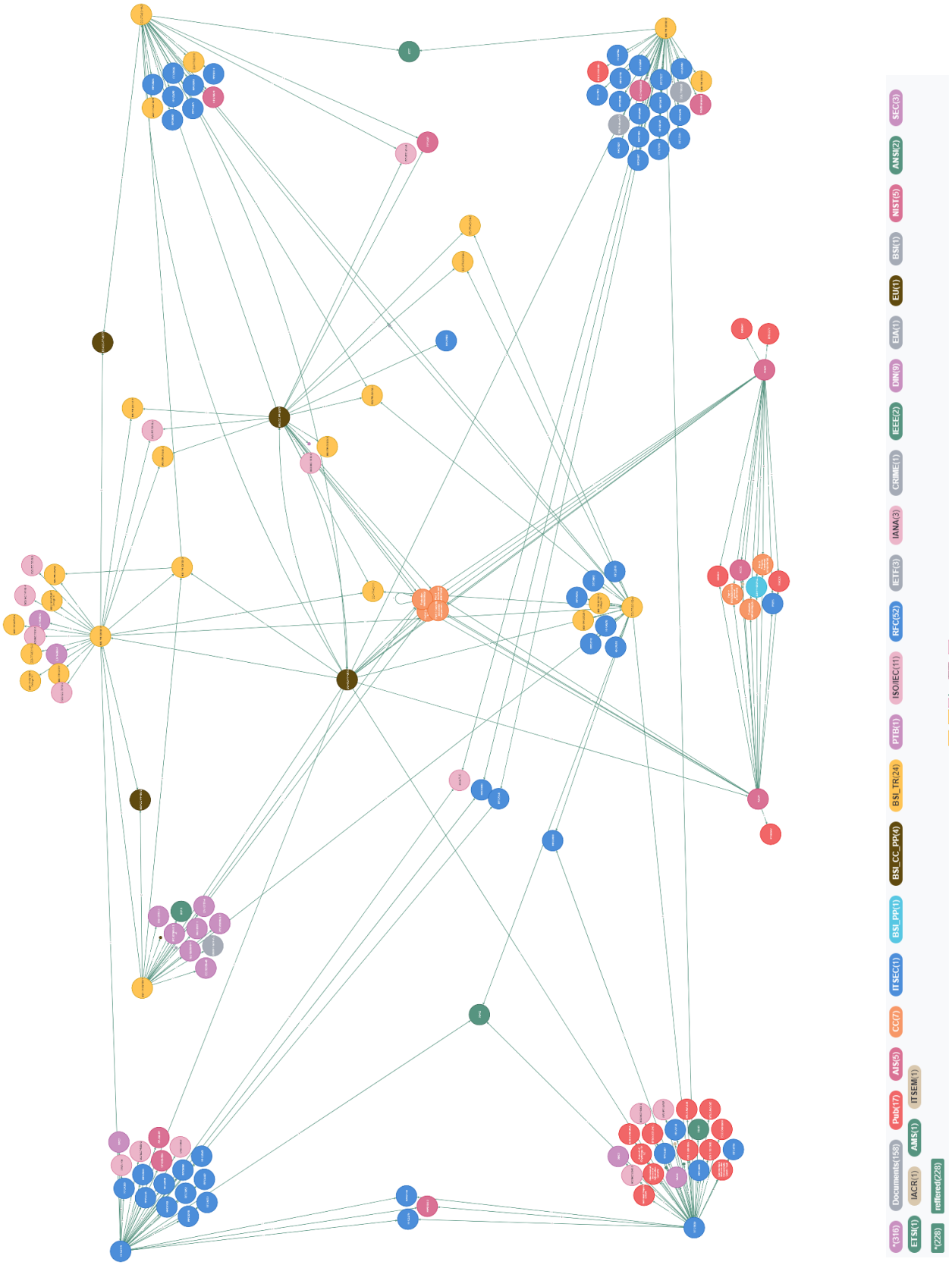
Anhang 01 – Skript Teilschritte

```
// Teilschritt 1 - Erzeugen der Dokumente (Nodes)
load csv with headers from "File:///Switzerland.csv" as row
call apoc.merge.node([row.Topic, "Documents"], {Comment:row.Comment,
Version:(row.Version), Title:row.Title, Topic:row.Topic, Link: row.Link,
Tags:row.Tags, Date:row.Date}) yield node
return node
```

```
// Teilschritt 2 - Erzeugen der Beziehungen (Kanten)
load csv with headers from "File:///swiss_test.csv" as line
match (s:Documents {Title:line.STitle, Version:(line.Sversion), Date:line.Sdate})
match (e:Documents {Title:line.Title, Version:(line.Version), Date:line.Date})
with s,e,line
match (a:Documents) where a.Date <>'-'
set a.Date = date(a.Date)
with s,e,line
match (b:Documents) where b.Version <> '-'
Set b.Version = tofloat(b.Version)
with s,e,line
Merge (s)-[r:reffered{Edge_weight:line.Edge_weight}]->(e)
with r
set r.Edge_weight = toInteger(r.Edge_weight)
return r
```

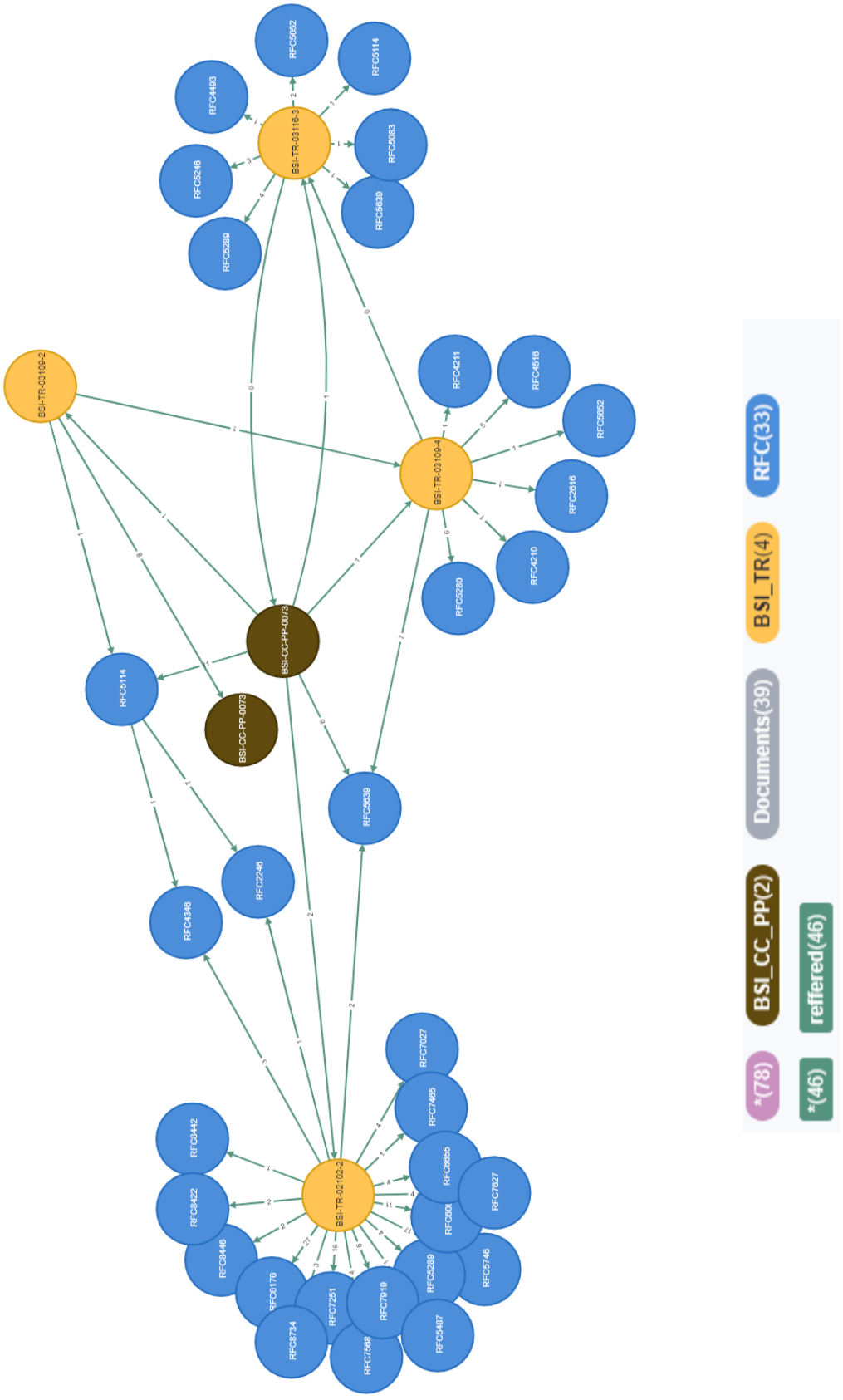
Anhang 02

Deutschland



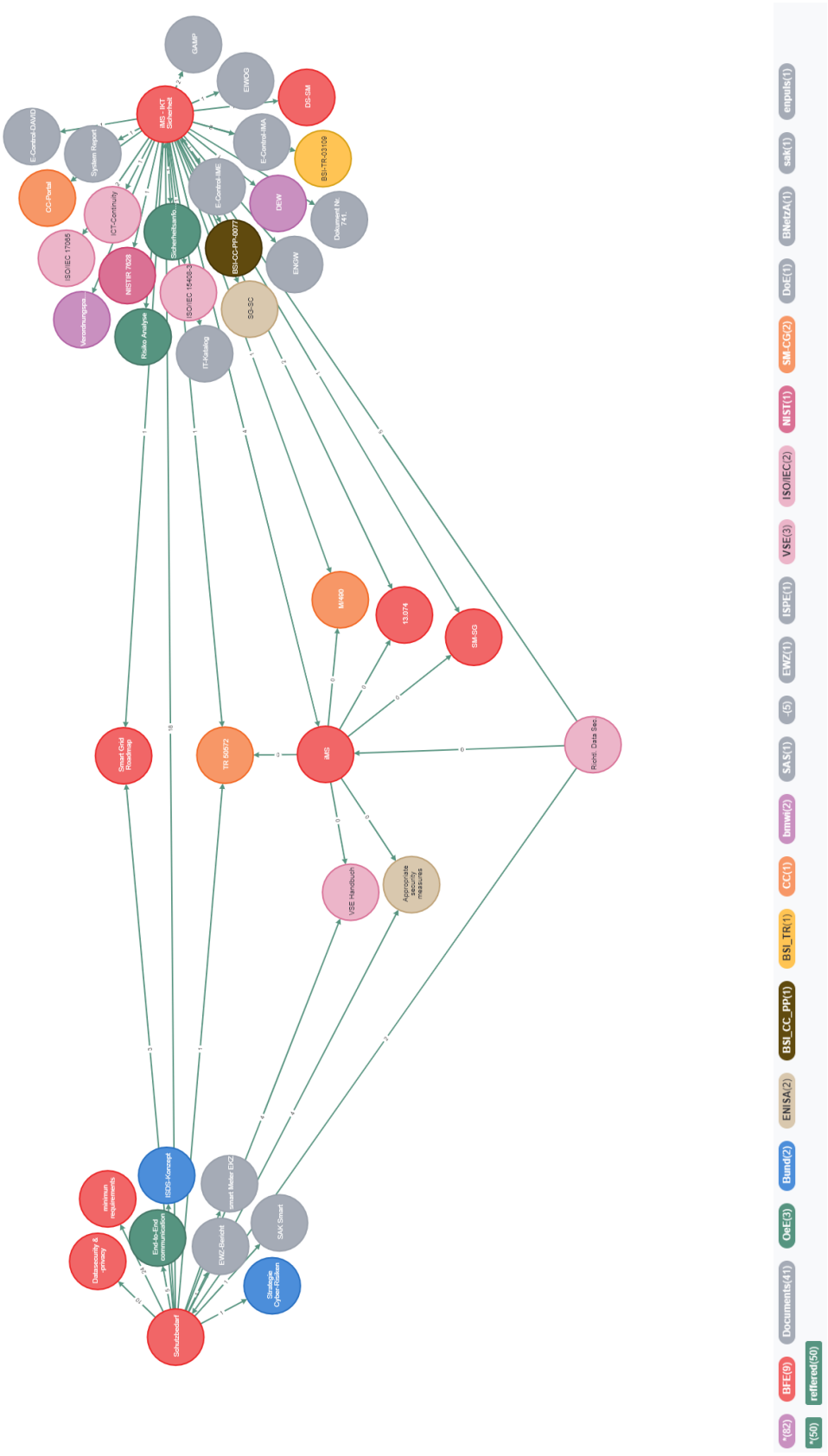
Anhang 02-1

Deutschland – Einfluss RFC



Anhang 03

Schweiz



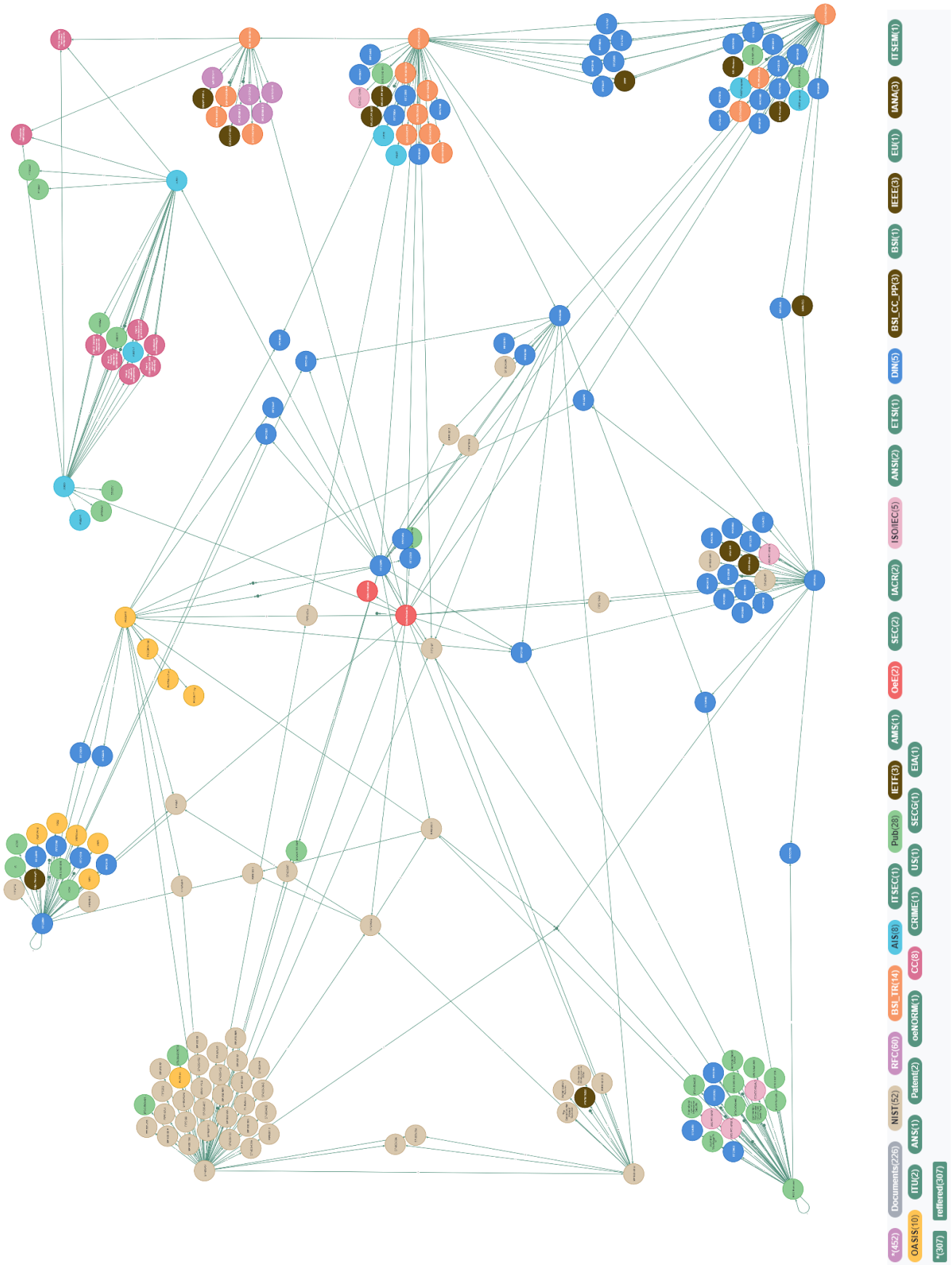
Anhang 03-1

Standards aus dem Anhang 2 des Ursprungsdokumentes

Bereich	Anwendung / Protokoll	Algorithmus /	Mindest-Werte	Bemerkungen
Verschlüsselung	symmetrisch	AES	128 bit	Transportverschlüsselung: Galois Counter Mode GCM Lokal: Cipher Block Chaining Modus CBC Stromverschlüsselung: Counter Mode CTR
	asymmetrisch	RSA, ElGamal	2048 bit	ECC
Hashfunktionen		SHA-2, SHA-3	H-Wert 256 bit	SHA-1 und MD5 nicht zulässig
Datenauthentifizierung	chiffriert und authentifiziert	AES im GCM		
	nur authentifiziert	HMAC mit SHA-2 oder SHA-3		Keyed-Hash Message Authentication Code
Elektronische Signatur		RSA, DSA	2048 bit	starke Schlüsselpaare wichtig
		ECDSA	256 bit	
Schlüsselaustausch	Diffie-Hellmann Ephemeral (DHE)	Perfect Forward Secrecy (PFS)	2048 bit	PFS gegen Replay Attacks
Transport Layer Security (TLS)	Schlüsselaustausch	DHE	2048 bit	
		ECDHE	256 bit	
	Datenübertragung	Authenticated Encryption with Additional Data (AEAD)		z.B. AES im GCM Secure Sockets Layer (SSL) nur in begründeten Ausnahmen
Secure Shell (SSH)	Schlüsselaustausch DH mit Group-Exchange			Version 2 Version 1 nur in begründeten Ausnahmen CTR und GCM CBC nur in begründeten Ausnahmen
VPN	IPsec (Internet Protocol Security)	Internet Key Exchange (IKE)		Schlüsselaustausch IKEv2 IKEv1 nur in begründeten Ausnahmen Pre-shared Keys 20 Zeichen inkl. Sonderzeichen
	OpenVPN			TLS-basiert
WLAN	WPA2			WPA und WEP nur in begründeten Ausnahmen Wi-Fi Protected Setup (WPS) nicht zulässig
Bluetooth				mindestens die Version 2.1 im Security Mode 4 Bluetooth LE3 (ab v4.0) im Security Mode 1 Level 3 „Just Works“ für das Pairing nicht zulässig (M-i-t-m Angriff)

Anhang 04

Österreich



Anhang 05

Niederlande - Anzahl Beziehungen, Ableitung der Dokumentengruppen

```
neo4j$ match()-[r:reffered]→(n) where r.Edge_weight>0 return labels(n), count(n)
```

	labels(n)	count(n)
1	["Documents", "DIN"]	6
2	["Documents", "ISO/IEC"]	34
3	["Documents", "ITU"]	11
4	["Documents", "IEC"]	16
5	["Documents", "RFC"]	59
6	["DLMS/COSEM", "Documents"]	7

labels(n)	count(n)
Pub	244
RFC	59
NIST	56
ISO/IEC	34
IEC	16
IEEE	14
IACR	13
ITU	11
ANSI	9
DLMS/COSEM	7
DIN	6
ENCS	6
3GPP	4
USENIX	3
ECRYPT	3
IETF	2
ICAR	2
ENISA	2
SEI	2
MISRA	2
debian	1
-	1
ACM	1
SSH	1
Russia	1
EMV	1
SSI Gouv	1
Keccak	1
EPC	1
BSI_TR	1
Usenix	1
Bund	1
OASIS	1
	508

```
neo4j$ match()-[r:reffered]→(n) return labels(n), count(n)
```

	labels(n)	count(n)
1	["Documents", "DIN"]	17
2	["Documents", "IEEE"]	20
3	["Documents", "ITU"]	12
4	["Documents", "ISO/IEC"]	38
5	["Documents", "IEC"]	21
6	["Documents", "RFC"]	98

labels(n)	count(n)
Pub	352
RFC	98
NIST	66
ISO/IEC	38
IEC	21
IEEE	20
IACR	19
DIN	17
ITU	12
ANSI	12
ECRYPT	10
ENCS	10
DLMS/COSEM	8
3GPP	5
ENISA	4
USENIX	3
Usenix	3
ETSI	2
IETF	2
EMV	2
ICAR	2
SEI	2
MISRA	2
ISO	1
ZigBee	1
debian	1
-	1
NDSS	1
ACM	1
SSH	1
Russia	1
SSI Gouv	1
NICT	1
Keccak	1
Talk	1
EPC	1
BSI_TR	1
Bund	1
OASIS	1
	726

Anhang 06

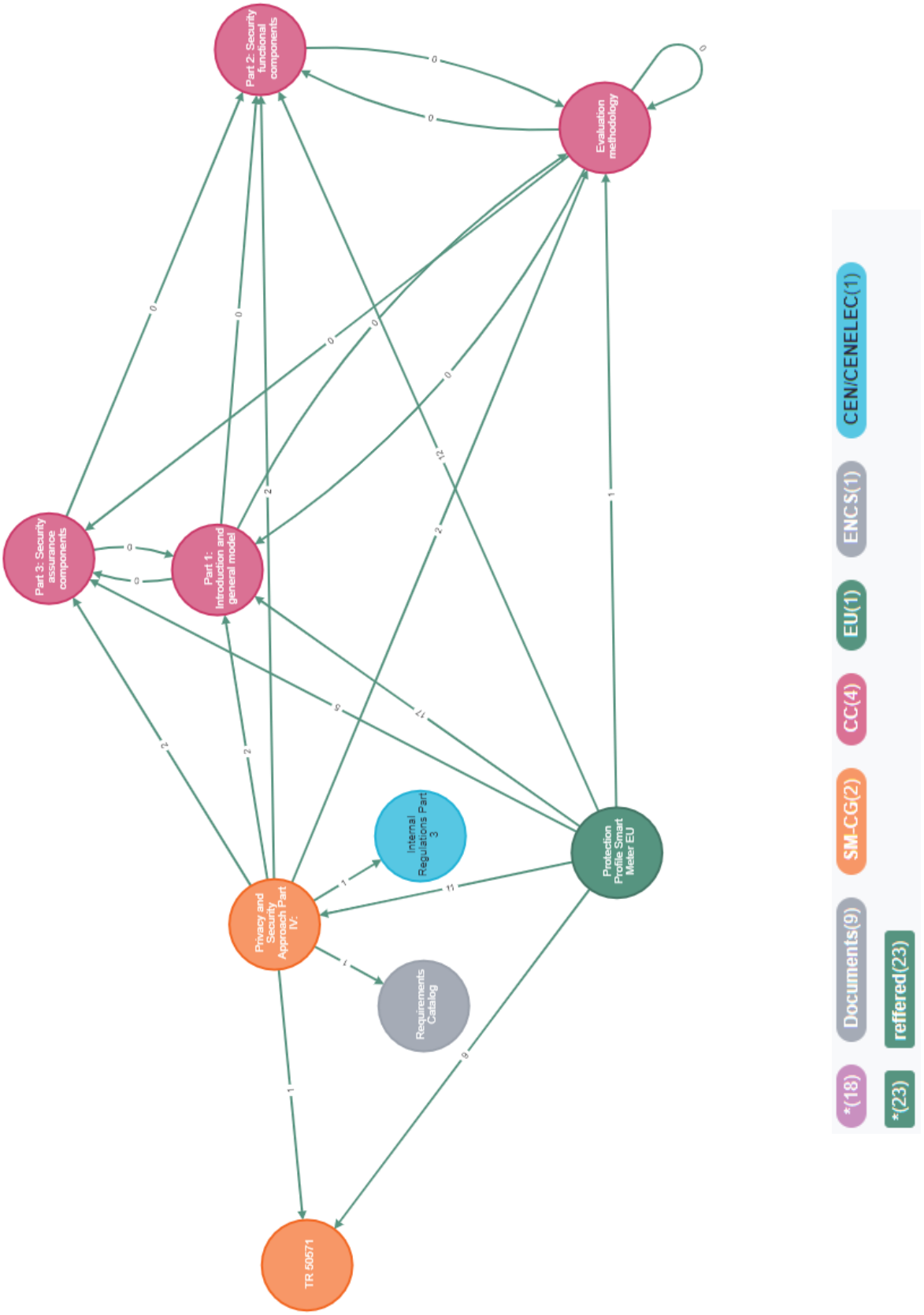
Niederlande – Anzahl Dokumente

```
MATCH (n)-[r]→(a) where r.Edge_weight>0
with id(a) as id, collect(distinct a) as node
return node
union
MATCH (n)-[r]→(a) where r.Edge_weight>0
with id(n) as id, collect(distinct n) as node
return node
```


```
MATCH (n)-[r]→(a)
with id(a) as id, collect(distinct a) as node
return node
union
MATCH (n)-[r]→(a)
with id(n) as id, collect(distinct n) as node
return node
```

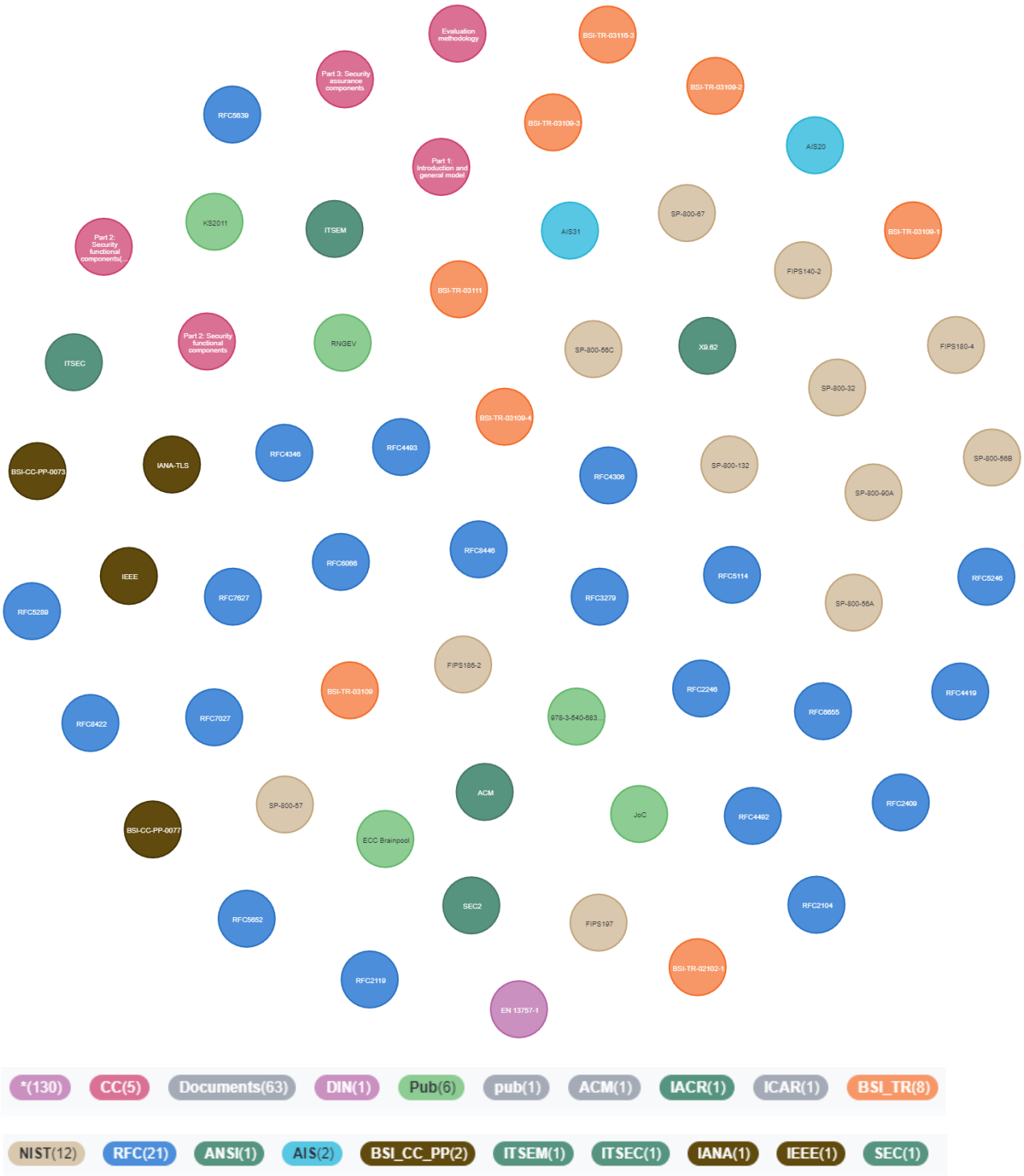
Anhang 07

Protection Profile EU



Anhang 08

Schnittmenge untersuchter Länder und Protection Profile EU



Anhang 09-1

Title	Topic	Country	Edge_weight	Tags
978-3-540-68351-3	Pub	NL,	2,1,	The mickey stream ciphers
JoC	Pub	NL,	1,2,	Instant ciphertext-only cryptanalysis ofGSM encrypted communication.
BSI-TR-03109-3	BSI_TR	DE,A,	2,5,9,	Kryptographische Vorgaben
IANA-TLS	IANA	DE,A,	1,6,2,	Transport Layer Security (TLS) Parameters
BSI-TR-03109-2	BSI_TR	DE,A,	1,60,3,2,7,	Smart Meter Gateway - Anforderungen an die Funktionalitaet und Interoperabilitaet des Sicherheitsmoduls
BSI-TR-03109-4	BSI_TR	DE,A,	1,2,4,	Public key infrastructure Smart Meter Gateway
BSI-TR-03116-3	BSI_TR	DE,A,	1,2,	Kryptographische Vorgaben fuer die Infrastruktur von intelligenten Messsystemen
BSI-TR-03111	BSI_TR	DE,A,	9,10,17,	Elliptic Curve Cryptography ECC
RFC4493	RFC	DE,A,	1,4,	AES-CMAC Algorithm
ITSEM	ITSEM	DE,A,	2,1,	-
Part 2 Security functional components(old)	CC	DE,A,	9,1,	-
RNGEV	Pub	DE,A,	1,6,5,	Evaluation of random number generators
ITSEC	ITSEC	DE,A,	1,3,4,	-
IEEE	IEEE	DE,A,	1	Triple Handshake / Cookie Cutters / Breaking and Fixing Authentication over TLS
RFC4346	RFC	DE,A,	3,1,	TLS Protocol v 1.1
RFC8446	RFC	DE,A,	2,27,4,	The Transport Layer Security (TLS) Protocol Version 1.3
RFC2119	RFC	DE,A,	7,1,	Key words for use in RFCs to Indicate Requirement Levels
SP-800-57	NIST	DE,A,	1,2,	Recommendation for Key Management
ECC Brainpool	Pub	DE,A,	1,3,	Standard Curves and Curve Generation
AIS20	AIS	DE,A,	13,1,	RNG-Random Number Generation
AIS31	AIS	DE,A,	20,1,	RNG-Random Number Generation
BSI-TR-03109-1	BSI_TR	DE,A,	5,9,	-
RFC5639	RFC	DE,A,	6,2,7,1,	Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation
BSI-CC-PP-0073	BSI_CC_PP	DE,A,	9,2,8,20,	Smart Meter Gateway
KS2011	Pub	DE,A,	1,7,	Functionality classes for random number generators
RFC5289	RFC	DE,A,	4,1,16,	TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)
RFC6066	RFC	DE,A,	11,1,2,	Transport Layer Security (TLS) Extensions Extension Definitions
RFC7027	RFC	DE,A,	4	Elliptic Curve Cryptography (ECC) Brainpool Curves
RFC7627	RFC	DE,A,	4,2,3,	Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension
RFC8422	RFC	DE,A,	2,5,	Elliptic Curve Cryptography (ECC) Cipher Suitesfor Transport Layer Security (TLS) Versions 1.2 and Earlier
RFC5652	RFC	DE,A,	1,2,	Cryptographic Message Syntax (CMS)

Anhang 09-2

FIPS186-2	NIST	DE,A,	1,6,5,	Digital Signature Standard (DSS)
RFC3279	RFC	DE,A,	4,2,1,	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
SEC2	SEC	DE,A,	1,6,	Recommended Elliptic Curve Domain Parameters
BSI-TR-03109	BSI_TR	DE,CH,	1,3,	-
ACM	Pub	NL,A,	2,1,4,3,	model and architecture for pseudo-random generationwith applications to /dev/random
BSI-TR-02102-1	BSI_TR	NL,A,	1,6,13,	Kryptographische VerfahrenEmpfehlungen und Schl ?ussell ?angen
RFC2104	RFC	NL,A,	1,2,	HMAC Keyed-Hashing for Message Authentication
SP-800-67	NIST	NL,A,	2,1,5,	Triple Data Encryption Algorithm (TDEA) Block Cipher
SP-800-132	NIST	NL,A,	1,3,	Password-Based Key Derivation / Storage Applications
SP-800-56B	NIST	NL,A,	3,24,	Assurances integer factorization cryptography key agreement key confirmation key derivation key establishment key management key recovery key transport.
SP-800-56C	NIST	NL,A,	1,2,	Key Derivation through Extraction-then-Expansion
SP-800-90A	NIST	NL,A,	1,5,3,	RNG / Deterministic Random Bit Generators
SP-800-32	NIST	NL,A,	4,1,	Introduction to Public Key Technology and the Federal PKI Infrastructure
FIPS140-2	NIST	NL,A,	18,15,1,	SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES
X9.62	ANSI	NL,A,	5,3,2,7,	the Elliptic Curve Digital Signature Algorithm (ECDSA)
RFC2246	RFC	NL,DE,A,	1,7,2	(TLS) Protocol Version 1.1
RFC5246	RFC	NL,DE,A,	2,3,1,5,17,11	(TLS) Protocol Version 1.2
RFC2409	RFC	NL,DE,A,	1,6,2,	The Internet Key Exchange (IKE).
RFC4306	RFC	NL,DE,A,	1	Internet Key Exchange (IKEv2) Protocol.
RFC4419	RFC	NL,DE,A,	1	Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol
RFC4492	RFC	NL,DE,A,	2,1,3,	Elliptic CurveCryptography (ECC) Cipher Suites for Transport Layer Security (TLS).
EN 13757-1	DIN	NL,DE,A,	2,1,	Kommunikationssysteme fuer Zaehler - Teil 1 Datenaustausch
FIPS197	NIST	NL,DE,A,	1,4,2,3,	Advanced Encryption Standard (AES)
RFC5114	RFC	NL,DE,A,	1,11,	Additional Diffie-Hellman Groups for Use with IETF Standards
RFC6655	RFC	NL,DE,A,	1,4,	AES-CCM Cipher Suites for Transport Layer Security (TLS)
SP-800-56A	NIST	NL,DE,A,	1,35,32,3,	assurances Diffie-Hellman elliptic curve cryptography finite field cryptography key agreement key confirmation key derivation key establishment key management
FIPS180-4	NIST	NL,DE,A,	1,3,2,	Secure Hash Standard (SHS)
BSI-CC-PP-0077	BSI_CC_PP	DE,CH,A,	2,1,	Security Module
Evaluation methodology	CC	EU,DE,A,	1,2,	minimum in order to conduct a CC evaluation
Part 1 Introduction and general model	CC	EU,DE,A,	17,2,1,9,	-
Part 2 Security functional components	CC	EU,DE,A,	12,2,1,34,3,	-
Part 3 Security assurance components	CC	EU,DE,A,	5,2,1,	-

Anhang 10-1

Standards aus M/490

AVAILABLE STANDARDS	Available	Coming	M	H1	H2/H3	C	G1	G2	L	N
CLC/TS 50568-4	X			x	x	x				
CLC/TS 50568-8	X			x	x	x				
CLC/TS 50590	X					x			x	x
CLC/TS 52056-8-4	X					x				
CLC/TS 52056-8-5	X					x				
CLC/TS 52056-8-7	X					x			x	x
EN 50065-1	X		x	x	x	x	x		x	x
EN 50090-3-1	X			x	x					
EN 50090-3-2	X			x	x					
EN 50090-3-3	X			x	x					
EN 50090-4-1	X			x	x					
EN 50090-4-2	X			x	x					
EN 50090-4-3	X			x	x					
EN 50090-5-1	X			x	x					
EN 50090-5-2	X			x	x					
EN 50090-5-3	X			x	x					
EN 50090-7-1	X			x	x					
CEN-CLC-ETSI/TR 50572	X		x	x	x	x	x	x	x	x

AVAILABLE STANDARDS	Available	Coming	M	H1	H2/H3	C	G1	G2	L	N
IEC 61334-4-32	X					x				
IEC 61334-4-511	X					x				
IEC 61334-4-512	X					x				
IEC 61334-5-1	X					x				
IEC 62056-1-0	X		x	x	x	x	x	x	x	x
IEC 62056-3-1	X		x			x				
IEC 62056-42	X		x	x			x			
IEC 62056-46	X		x	x		x	x			
IEC 62056-4-7	X					x	x	x		
IEC 62056-5-3	X		x	x		x	x	x		
IEC 62056-6-1	X		x	x		x	x	x		
IEC 62056-6-2	X		x	x		x	x	x		
IEC/TS 62056-6-9	X		x	x		x	x	x		
IEC 62056-7-3		X	*x*			*x*				
IEC 62056-7-5	X			x	x					
IEC 62056-7-6	X		x	x		x	x			
IEC 62056-8-20		X				*x*			*x*	
IEC 62056-8-3	X					x				
IEC 62056-8-6		X				*x*				
IEC/TS 62056-9-1	X							x		
IEC 62056-9-7	X						x			
EN 13321 series	X			x	x					
EN 13757-1	X		x	x	x	x				
EN 13757-2	X	X	x	x	x	x				
EN 13757-3	X	X	x	x	x	x				
EN 13757-4	X	X	x	x	x	x				
EN 13757-5	X		x	x	x	x				
EN 13757-6	X		x	x	x	x				
EN 13757-7		X	x	x	x	x				
EN 16836-1		X	*x*	*x*	*x*	*x*			*x*	
EN 16836-2		X	*x*	*x*	*x*	*x*			*x*	
EN 16836-3		X	*x*	*x*	*x*	*x*			*x*	
EN 14908 series	X		x	x	x	x			x	x
CLC prTR 50491-10		X		*x*	*x*					
EN 50491-11	X			x	x					
EN 50491-12		X		*x*	*x*					

Anhang 10-2

Standards aus M/490

IEEE 802.15.4 series	X		x	x	x	x	x	x	x	x
IEEE 1377	X		x			x	x	x	x	x
IEEE 1901.2	X		x	x	x	x	x	x	x	x
draft-ietf-6tisch-architecture		**X**	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*
draft-ietf-6tisch-6top-interface		**X**	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*
draft-ietf-6tisch-minimal		**X**	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*
IETF RFC 6690 (CoAP)	**X**		*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*
IETF RFC 7252(CoAP)	**X**		*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*
IETF RFC 7390(CoAP)	**X**		*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*
IETF RFC 7641(CoAP)	**X**		*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*
IETF RFC 7959(CoAP)	**X**		*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*
IETF RFC 4919	**X**		x	x	x	x	x	x	x	x
IETF RFC 4944	**X**		x	x	x	x	x	x	x	x
IETF RFC 6206	**X**		x	x	x	x	x	x	x	x
IETF RFC 6282	**X**		x	x	x	x	x	x	x	x
IETF RFC 6550	**X**		x	x	x	x	x	x	x	x
IETF RFC 6551	**X**		x	x	x	x	x	x	x	x
IETF RFC 6552	**X**		x	x	x	x	x	x	x	x

AVAILABLE STANDARDS	**Available**	**Coming**	**M**	**H1**	**H2/H3**	**C**	**G1**	**G2**	**L**	**N**
IETF RFC 6775	**X**		x	x	x	x	x	x	x	x
ETSI/ES 202 630		**X**	x	x	x	x	x	x	x	x
ETSI/TE 103 118 (Release 2)	**X**		x	x	x	x	x	x	x	x
ETSI/TR 101 531 (Release 1)	**X**		x	x	x	x	x	x	x	x
ETSI/TR 102 691 (Release 1 & Release 2)	**X**		x	x	x	x	x	x	x	x
ETSI/TR 102 886	**X**		x	x	x	x	x	x	x	x
ETSI/TR 102 935	**X**		x	x	x	x	x	x	x	x
ETSI/TR 102 966 (Release 1)	**X**		x	x	x	x	x	x	x	x
ETSI/TR 103 055	**X**		x	x	x	x	x	x	x	x
ETSI/TR 103 167 (Release 1)	**X**		x	x	x	x	x	x	x	x
ETSI/TS 101 584 (Release 2)	**X**		x	x	x	x	x	x	x	x
ETSI/TS 102 221	**X**		x	x	x	x	x	x	x	x
ETSI/TS 102 240	**X**		x	x	x	x	x	x	x	x
ETSI/TS 102 241	**X**		x	x	x	x	x	x	x	x
ETSI/TS 102 412	**X**		x	x	x	x	x	x	x	x
ETSI/TS 102 569	**X**		x	x	x	x	x	x	x	x
ETSI/TS 102 671	**X**		x	x	x	x	x	x	x	x
ETSI/TS 102 689 (Release 1 & Release 2)	**X**		x	x	x	x	x	x	x	x
ETSI/TS 102 690 (Release 1 & Release 2)	**X**		x	x	x	x	x	x	x	x
ETSI/TS 102 887-1	**X**		x	x	x	x	x	x	x	x
ETSI/TS 102 887-2	**X**		x	x	x	x	x	x	x	x
ETSI/TS 102 921 (Release 1 & Release 2)	**X**		x	x	x	x	x	x	x	x
ETSI/TS 103 092 (Release 1 & Release 2)	**X**		x	x	x	x	x	x	x	x

Anhang 10-3

Standards aus M/490

ETSI/TS 103 093 (Release 1 & Release 2)	**X**		x	x	x	x	x	x	x	x
ETSI/TS 103 104 (Release 2)	**X**		x	x	x	x	x	x	x	x
ETSI/TS 103 107 (Release 2)	**X**		x	x	x	x	x	x	x	x
ETSI/TS 103 383		**X**	x	x	x	x	x	x	x	x
ETSI/TS 103 603 (Release 2)	**X**		x	x	x	x	x	x	x	x
ETSI/TS 103 908	**X**		x	x	x	x	x	x	x	x
ETSI/TS 122 368	**X**		x	x	x	x	x	x	x	x
ETSI/TS 123 401	**X**		x	x	x	x	x	x	x	x
ETSI/TS 136 201	**X**		x	x	x	x	x	x	x	x
ETSI/TS 136 211	**X**		x	x	x	x	x	x	x	x
ETSI/TS 136 212	**X**		x	x	x	x	x	x	x	x
ETSI/TS 136 213	**X**		x	x	x	x	x	x	x	x
ETSI/TS 136 214	**X**		x	x	x	x	x	x	x	x
ETSI/TS 136 216	**X**		x	x	x	x	x	x	x	x
ETSI/TS 136 300	**X**		x	x	x	x	x	x	x	x

AVAILABLE STANDARDS	**Available**	**Coming**	**M**	**H1**	**H2/H3**	**C**	**G1**	**G2**	**L**	**N**
ETSI/TS DTS/PLT-00031		**X**	x	x	x	x	x	x	x	x
ITU-T Recommendations G.9902	X			x		x			x	
ITU-T Recommendations G.9903	X	X		x		x			x	
ITU-T Recommendations G.9904	X			x		x			x	