Anforderung für geschlossene Benutzergruppen zur Erbringung von Regelreserve

Stand: 26. Oktober 2018

Versionsverlauf

Version	Datum	Bemerkung
1.0	22.04.2016	Erste gültige Version (konsolidierte Fassung für alle RL-Produkte)
2.0	26.10.2018	Überarbeitung im Rahmen der Neuerstellung der PQ-Bedingungen

Inhalt

1 Vorwort

Die Anbindung der Technischen Einheiten an das Leitsystem eines Reservenanbieters und die Anbindung dieses Leitsystems an die Übergabepunkte der Übertragungsnetzbetreiber müssen ein vergleichbares Sicherheitsniveau zu den Übertragungsnetzbetreibern aufweisen.

Hierfür werden in den IT-Anforderungen für Regelreservearten unter anderem „geschlossene Benutzergruppen“ sowie Verschlüsselungstechniken gefordert, deren Anforderungen mit diesem Dokument konkretisiert werden sollen. Dieses Dokument ist eine Anlage zu den jeweils aktuellen IT-Anforderungen für Regelreservearten und unterliegt deren Gültigkeit.

Für den Aufbau von geschlossenen Benutzergruppen wird eine „sichere Systemarchitektur“ gefordert [12], welche nicht nur durch eine einzelne Schutzmaßnahme, sondern durch ergänzende Sicherungsmaßnahmen auf mehreren Ebenen realisiert werden sollte.

Für die Anbindungen zwischen Technischen Einheiten, Leitsystemen und Übergabepunkten der Übertragungsnetzbetreiber bedeutet dies, dass diese zweistufig durch ein ausschließlich für den Netzwerkverkehr des (für die Erbringung der Wirkleistungsreserve genutzten) Leitsystems separiertes Netz mit einer eigenen, zusätzlich Verschlüsselung mittels VPN realisiert werden sollen. Das für dieses Leitsystem genutzte Netzwerk darf nicht durch das öffentliche Internet geroutet werden (also keine öffentlich angreifbaren IP-Adressen beinhalten). Das ist z.B. durch Nutzung privater APNs im Mobilfunknetz, privaten DSL-Anschlüssen oder Standleitungen möglich. Die Konfiguration der zusätzlichen Verschlüsselung mit einem VPN muss dabei vollständig in der Verantwortung des Reservenanbieters liegen und bei dem Carrier (z.B. dem APN-Anbieter) nicht bekannt sein, damit eine von dem zugrunde liegenden Netzwerk unabhängige Ende-zu-Ende-Verschlüsselung gewährleistet werden kann.

Für die Verschlüsselung innerhalb der ‚geschlossenen Benutzergruppen zur Erbringung von Regelreserve‘ sind ausschließlich VPNs auf Basis von IPsec oder OpenVPN im Rahmen der in diesem Dokument beschriebenen Bedingungen erlaubt.
Die beiden Technologien IPsec und OpenVPN können innerhalb der unten aufgeführten Rahmenbedingungen die wesentlichen Sicherheitsanforderungen an ein VPN erfüllen und für die sichere Kopplung von Netzwerken eingesetzt werden.

Da durch Falsch-Konfiguration bei IPsec und OpenVPN sehr leicht eine ‚geschlossene Benutzergruppe' nicht mehr gegeben ist, werden in diesem Dokument produktunabhängige Vorgaben für eine sichere Konfiguration getroffen.

1.1 Aufbau dieses Dokumentes

In Kapitel 2 werden zunächst die Sicherheitsanforderungen, die an jede VPN-Technologie gestellt werden müssen, aufgeführt. Diese Sicherheitsanforderungen werden anschließend in Kapitel 3 und 4 auf IPsec und OpenVPN übertragen.

Da es für nahezu jede Anforderung aus Kapitel 2 mehrere Möglichkeiten gibt diese umzusetzen, wird in Kapitel 3 und 4 zu IPsec und OpenVPN festgelegt, wie dies zu geschehen hat.

Da es gewisse Wahlmöglichkeiten gibt, ist im Rahmen der Präqualifikation vom Reservenanbieter für jede geschlossene Benutzergruppe aufzuführen, mit welcher Technologie diese realisiert wurde und wie die einzelnen Sicherheitsanforderungen umgesetzt wurden.

2 Sicherheitsanforderungen an die Datenübertragung

Die zur Umsetzung genutzten kryptografischen Verfahren lassen sich im Folgenden stets in symmetrische oder asymmetrische Verfahren unterteilen. Der wesentliche Unterschied beider Verfahren beruht darauf, dass bei einem symmetrischen Verfahren beide Kommunikationspartner ein Geheimnis kennen, wohingegen bei einem asymmetrischen Verfahren nur ein Kommunikationspartner ein Geheimnis schützt. Im Zuge der Nutzung dieser Verfahren zur Realisierung eines VPNs liegen diese kryptografischen Geheimnisse in Form von Schlüsseln entweder als Kurzzeitschlüssel oder als Langzeitschlüssel vor. Ein Kurzzeitschlüssel besitzt in diesem Kontext eine zeitliche Gültigkeit von maximal der Dauer einer VPN-Verbindung.

2.1 Vertraulichkeit von Informationen

Bei der Übertragung von Daten über fremde Netzwerke spielt die Verschlüsselung von Daten zum Schutz der Vertraulichkeit eine wesentliche Rolle. Hierzu werden die Daten in eine Form überführt, die keine Rückschlüsse auf die ursprünglichen Daten zulässt und nur diejenigen Zugriff auf den Inhalt der Nachricht erhalten, die im Besitz des geheimen kryptografischen Schlüssels sind. In diesem Zusammenhang ist eine wesentliche Anforderung an die Verschlüsselung der Daten, dass die Vertraulichkeit ausschließlich auf der Kenntnis des eingesetzten geheimen Schlüssels beruht. Die eingesetzten Verschlüsselungsverfahren und Schlüssellängen müssen stets als bekannt angenommen werden.

Bei der Verschlüsselung von Daten zeigen symmetrische Verschlüsselungsverfahren erhebliche Geschwindigkeitsvorteile gegenüber asymmetrischen Verfahren, so dass in diesem Zusammenhang ausschließlich symmetrische Verschlüsselungsverfahren zum Einsatz kommen. Der Begriff symmetrisch bedeutet auch hier, dass beide Parteien einen geheimen Schlüssel kennen und zur Verschlüsselung und Entschlüsselung derselbe Schlüssel benutzt wird. Eine wesentliche Sicherheitsanforderung ist es, dass ein sicheres Verschlüsselungsverfahren mit ausreichender Schlüssellänge benutzt wird.

Zur Nutzung eines symmetrischen Verschlüsselungsverfahrens ist die Verteilung von einem geheimen Schlüssel auf beiden Seiten der Kommunikation erforderlich. Nach heutigem Stand der Kryptografie ist es nicht mehr zeitgemäß, denselben geheimen Schlüssel für mehr als eine Verbindung zu nutzen. Die Nutzung entsprechender kryptografischer Verfahren ermöglicht es, im Verbindungsaufbau ein für die symmetrische Verschlüsselung notwendigen, geheimen

Schlüssel zu erzeugen. Hier haben sich insbesondere zwei Verfahren in der Praxis etabliert. Zum einen kann ein zufällig generierter geheimer Sitzungsschlüssel mit einem öffentlichen Langzeitschlüssel verschlüsselt und dem Kommunikationspartner übermittelt werden. Dieser kann unter Nutzung des korrespondierenden öffentlichen Schlüssels den Sitzungsschlüssel entschlüsseln und für die sichere Kommunikation nutzen. Zum anderen kann unter Nutzung des Diffie-Hellmann-Algorithmus ein geheimer Sitzungsschlüssel auf beiden Seiten erzeugt werden, ohne dass dieser in der Datenverbindung übermittelt wird. Dazu generieren beide Parteien auf Basis von öffentlichen Diffie-Hellmann-Parametern zwei Schlüssel. Einer dieser Schlüssel wird jeweils an den Kommunikationspartner übermittelt. Unter Nutzung des Diffie-Hellmann-Algorithmus berechnen beide Seiten den geheimen Sitzungsschlüssel aus dem eigenen, nicht übertragenen und dem vom Partner empfangenen Schlüssel. Zum sicheren Einsatz des Diffie-Hellmann-Algorithmus ist es erforderlich, dass die öffentlichen Parameter in ausreichender Länge vorliegen. Die vordefinierten Parameter werden in Gruppen zusammengefasst, so dass meist die Wahl einer sicheren Gruppe notwendig ist.

Eine weitere, im Zuge der symmetrischen Verschlüsselung zu berücksichtigende Anforderung ist es, dass Wiederholungen im Klartext nicht denselben Geheimtext an jeweils gleicher Position erzeugen dürfen. Zu diesem Zweck werden die Klartextdaten zusätzlich vor einer Verschlüsselung beim Sender und nach einer Entschlüsselung bei Empfänger gemäß einer vorab vereinbarten Betriebsart des symmetrischen Verschlüsselungsverfahrens modifiziert (zum Beispiel sind gängige Betriebsarten CBC, CFB oder CTR). Es ist zur Gewährleistung der Vertraulichkeit ebenfalls erforderlich, dass eine sichere Betriebsart gewählt wird.

Die Betriebsart definiert zusammen mit dem Verschlüsselungsverfahren und der Schlüssellänge die Art und Weise, wie die Daten verschlüsselt werden und ist in einer Konfiguration meist anhand der Bezeichnung zu identifizieren, z.B. AES-256-CBC.

2.2 Authentisierung der Kommunikationspartner

Die sichere Authentisierung des Kommunikationspartners stellt eine notwendige Grundlage zur Erfüllung der in diesem Kapitel aufgeführten Sicherheitsanforderungen dar. Ohne eine sichere Authentisierung kann ein Mittelsmann in die Kommunikation eingreifen und vortäuschen, der jeweilige Kommunikationspartner in einer Verbindung zu sein. In Folge dessen werden die in diesen Kapiteln beschriebenen Sicherheitsanforderungen in der Kommunikation mit einem Mittelsmann umgesetzt und verlieren damit an Schutzwirkung. Es ist daher

wesentlich, dass eine Authentisierung zum einen gegenseitig erfolgt und zum anderen so sicher wie möglich umgesetzt wird.

Die Authentizität des Kommunikationspartners wird dazu unter Nutzung eines kryptographischen Geheimnisses sichergestellt. Hierzu unterscheidet man zwischen symmetrischen und asymmetrischen Verfahren. Bei symmetrischen Verfahren wird vorab ein geheimer Schlüssel auf beiden Seiten verteilt und dient bei einem Verbindungsaufbau als Beweis der Authentizität des Kommunikationspartners. Aufgrund der notwendigen, sicheren Verteilung vorab wird dieser symmetrische Schlüssel im Kontext eines VPNs vielfach als „Pre-Shared Key“ bezeichnet.

Bei asymmetrischen Verfahren wird auf Basis eines Schlüsselpaares, das sich aus einem privaten und einem öffentlichen Schlüssel zusammensetzt, die Authentizität des Kommunikationspartners durch die Kenntnis des privaten Schlüssels bewiesen. Die Prüfung des Kommunikationspartners erfolgt dabei unter Nutzung des korrespondierenden öffentlichen Schlüssels. Die damit einhergehende Notwendigkeit, den öffentlichen Schlüssel sicher zu verteilen, wird in der Regel über Zertifikate realisiert. Zur Gewährleistung einer sicheren Verteilung enthält ein Zertifikat dazu eine Signatur, die von einer vertrauenswürdigen Zertifizierungsstelle erstellt wurde.

Im Vergleich der beiden Verfahren können wesentliche, sicherheitsrelevante Vorteile bei der Authentisierung mit einem asymmetrischen Verfahren verzeichnet werden. Dazu gehören insbesondere die folgenden Vorteile:

- Mit der Speicherung des privaten Schlüssels auf nur einer Seite der Kommunikation verringert sich die Angriffsfläche deutlich.
- Die Verteilung des öffentlichen Schlüssels kann sicher über ein Zertifikat erfolgen.
- Die Schlüssellängen von asymmetrischen Schlüsseln sind in der Regel ausreichend lang, wohingegen der Einsatz eines Pre-Shared Keys in der Praxis häufig von einem vergleichsweise kurzen Nutzer-Passwort abgeleitet wird. Damit weist der Pre-Shared Key zum einen eine geringe Entropie auf und ist zum andern anfällig für Wörterbuch-Attacken.

Aufgrund der deutlichen, sicherheitserhöhenden Vorteile der asymmetrischen Authentisierungsverfahren sollte die Nutzung von asymmetrischen Verfahren eine wesentliche umzusetzende Sicherheitsanforderung darstellen.

2.3 Schutz der Integrität einer Nachricht

Bei der Übertragung von verschlüsselten Daten muss zusätzlich sichergestellt werden, dass diese auf dem Übertragungsweg nicht verändert wurden. Ein Schutz der Datenintegrität wird von einem symmetrischen Verschlüsselungsverfahren nicht gewährleistet und muss daher zusätzlich sichergestellt werden. Zu diesem Zweck werden in der Regel zusätzliche Daten in Form einer Prüfsumme den eigentlichen Daten angehängt. Durch die Prüfsumme kann die Integrität der Daten verifiziert werden. Aufgrund von Performancevorteilen kommen in der Regel zur Erstellung einer sicheren Prüfsumme symmetrische Verfahren zum Einsatz. Der dem symmetrischen Verfahren zugrunde liegende geheime Schlüssel wird meist im Verbindungsaufbau erzeugt. In Folge dessen kann eine sichere Prüfsumme nur mit Kenntnis des geheimen Schlüssels erstellt werden und ermöglicht damit die Entdeckung von Manipulationen an den verschlüsselten Daten inklusive der Prüfsumme.

Ein häufig angewandtes und als sicher geltendes Verfahren zur Erstellung von sicheren Prüfsummen ist das Verfahren „Keyed-Hash Message Authentication Code" (HMAC), das im RFC 2104 näher beschrieben ist. Es stützt sich im Kern auf die Verwendung von kryptografischen Hashfunktionen, wie beispielsweise SHA-256.

2.4 Schutz vor Wiedereinspielen alter Nachrichten

Bei der Übertragung von verschlüsselten Daten muss zudem sichergestellt werden, dass ein potentieller Angreifer zuvor aufgezeichneten, verschlüsselten Datenverkehr nicht wieder in eine neue Verbindung einspielt (Replay-Attacke). Diese Art des Angriffs muss explizit adressiert werden und wird nicht durch die Umsetzung anderer Sicherheitsanforderungen verhindert. Als Maßnahme zum Schutz einer Replay-Attacke muss eine Verbindung ein Merkmal aufweisen, mit dem eine alte Verbindung von einer neuen Verbindung unterschieden und durch die Kommunikationspartner verifiziert werden kann. Hierzu eignen sich die folgenden Merkmale:

- Eindeutige Sitzungs-ID
- Zufällige Daten
- Sequenznummer
- Zeitstempel

Darüber hinaus ist zu beachten, dass ein Schutz vor Wiedereinspielen alter Nachrichten sowohl beim Verbindungsaufbau als auch bei der Datenübertragung bestehen muss.

2.5 Sekundäre Sicherheitsanforderungen

2.5.1 Perfect Forward Secrecy

Die Erfüllung der Eigenschaft „Perfect Forward Secrecy“ bedeutet im Allgemeinen, dass die Kompromittierung eines geheimen Schlüssels ausschließlich die Daten offenlegt, die mit diesem Schlüssel geschützt wurden. Es darf also nicht durch die Kompromittierung eines geheimen Schlüssels ein weiterer geheimer Schlüssel offengelegt werden, der zur Verschlüsselung anderer Daten genutzt wurde.

Im konkreten Fall bedeutet dies, dass bei einer Kompromittierung eines geheimen, meist asymmetrischen Langzeitschlüssel eine aufgezeichnete Verbindungen aus der Vergangenheit nicht entschlüsselt werden kann, also durch Kenntnis eines Langzeitschlüssels nicht der geheime Sitzungsschlüssel aus einer vergangenen Verbindung abgeleitet werden kann. Diese Situation ist gegeben, wenn zur Vereinbarung eines geheimen Sitzungsschlüssels im Verbindungsaufbau ein privater Langzeitschlüssel in der Weise verwendet wurde, dass der geheime Sitzungsschlüssel mit dem privaten Langzeitschlüssel verschlüsselt und an den Kommunikationspartner übermittelt wurde.

2.5.2 Auffrischen von Schlüsselmaterial (Re-Keying)

Eine weitere Sicherheitsanforderung besteht in der Auffrischung von kurzzeitigem Schlüsselmaterial. Dies ist notwendig, weil bei der Kopplung von Netzwerken die Dauer der Kopplung nicht ohne weiteres absehbar ist. In Abhängigkeit von den zu übertragenden Daten kann ein kontinuierlicher Datenverkehr entstehen, der ein VPN über einen längeren Zeitraum bestehen lässt. Darüber hinaus kann diese Situation auch erwünscht und bewusst herbeigeführt worden sein. Diese Situation führt dazu, dass ein geheimer Sitzungsschlüssel über einen längeren Zeitraum genutzt wird. Ein potentieller Angreifer kann diesen Zeitraum nutzen, um den geheimen Sitzungsschlüssel kryptografisch anzugreifen. Der notwendige Zeitraum für einen potentiellen Angriff ist damit abhängig vom verwendeten Verschlüsselungsalgorithmus und der verwendeten Schlüssellänge.

Zum Schutz vor einem kryptografischen Angriff auf eine Datenverbindung sollte der Zeitraum für einen Angriff möglichst klein gehalten werden. Ferner sollte eine Erneuerung von Schlüsselmaterial nicht durch einen Verbindungsabbau und -aufbau herbeigeführt werden, sondern durch ein entsprechendes Netzwerkprotokoll unterstützt werden.

3 Umsetzung mittels IPsec

Unter dem Begriff IPsec ist eine Sammlung zahlreicher Netzwerkprotokolle zu verstehen, die den sicheren Aufbau und Betrieb eines VPN ermöglichen. Die überwiegend aus den 1990er Jahren stammenden Netzwerkprotokolle können in Protokolle für den Verbindungsaufbau und die Datenübertragung unterteilt werden. Für die Umsetzung der in Kapitel 2 formulierten Anforderungen und der hier betrachteten Kopplung von Netzwerken kommt lediglich eine kleine Menge von Protokollen der Protokoll-Sammlung in Betracht. So erfüllt nur das für den Verbindungsaufbau nutzbare Protokoll IKE die Anforderung, dass für jede Verbindung ein neuer geheimer Schlüssel erzeugt wird. Gleichermaßen erfüllt nur das für die Datenübertragung nutzbare Protokoll ESP die Anforderung, dass Daten verschlüsselt übertragen werden. Im Zuge der Betrachtung einer Kopplung von Netzwerken kann dies nur im IPsec-Tunnel-Modus erfolgen und stellt zusammen mit den Protokollen IKE und ESP eine grundlegende IPsec-Konfiguration dar.

Das Protokoll IKE zum Verbindungsaufbau eines VPN-Tunnels ist entweder in der Version 1 (IKEv1) oder der neueren, überarbeiteten Version 2 (IKEv2) nutzbar. Ein wesentlicher Unterschied der Version 2 ist es, dass die Anzahl der notwendigen Pakete für einen Verbindungsaufbau erheblich reduziert wurden (von 9 Paketen im „Main Mode“ bzw. 6 Paketen im „Aggressive Mode“ auf lediglich 4 Pakete). Ferner ist eine Unterteilung des Verbindungsaufbaus in zwei Phasen, wie es die Version 1 vorsieht, ohne eine Beeinträchtigung der Sicherheit nicht mehr notwendig. Die Phase 1 von IKEv1 sieht den Aufbau einer sicheren, authentisierten Verbindung zwischen zwei VPN-Endpunkten vor. Diese Verbindung wird in der Phase 2 genutzt, um neues Schlüsselmaterial für den eigentlichen VPN-Tunnel zu erzeugen beziehungsweise neues Schlüsselmaterial einer bestehenden Verbindung zu erneuen. Die Verbindung wird aber nicht nur zur Erzeugung von Schlüsselmaterial genutzt, sondern ermöglicht auch die sichere und verschlüsselte Übertragung von Status- oder Fehler-Nachrichten. Ein entsprechendes Äquivalent der Phase 2 wird mit IKEv2 über den Nachrichten-Typ „CREATE_CHILD_SA“ realisiert.

Eine Abweichung der grundlegenden Konfiguration führt zu einer Nicht-Erfüllung der im Kapitel 2 aufgeführten Anforderungen.

Die nachfolgenden Kapitel beschreiben zum einen, wie die Protokoll-Sammlung IPsec die im Kapitel 2 aufgeführten Anforderungen umsetzt und zum anderen, welche kryptografischen Verfahren im Detail genutzt werden müssen, um eine ausreichende Schutzwirkung durch den Einsatz von Kryptografie zu erreichen. Aufgrund der grundlegenden Änderungen mit Einführung des Protokolls IKEv2 sind die Umsetzungen für die jeweiligen IKE-Versionen aufgeführt.

3.1 Umsetzung der Anforderungen mittels IPsec / IKEv1

Bei der Umsetzung der in Kapitel 2 beschriebenen Anforderungen ist zu berücksichtigen, dass aufgrund der überarbeiteten IKE Version 2 aktuelle Empfehlungen fast ausschließlich für die Version 2 ausgesprochen werden. Dieses Kapitel stützt sich daher überwiegend auf Empfehlungen des BSI-Grundschutz-Kataloges [4] und Empfehlungen des Projektes „BetterCrypto“ [7].

3.1.1 Vertraulichkeit der Informationen

Durch den Einsatz des Protokolls IKE der Protokoll-Suite IPsec kann für jede Verbindung ein neuer Sitzungsschlüssel erzeugt werden. Das Protokoll stützt sich hierzu auf den Diffie-Hellmann-Algorithmus zur Erzeugung eines geheimen, symmetrischen Schlüssels.
Der Einsatz von symmetrischen Verschlüsselungsverfahren inklusive Betriebsart sowie Parameter des Diffie-Hellmann-Algorithmus sind durch IKE variabel und werden zwischen den VPN-Endpunkten über korrespondierende Nummern ausgehandelt. Die Zuordnung wird gemäß des Protokolls IKEv1 durch die „Internet Assigned Numbers Authority“ (IANA) durchgeführt. Ein neues Verfahren erhält durch die IANA eine entsprechende Nummer, wenn das Verfahren ausreichend beschrieben ist. Meist sind die Verfahren durch ein RFC detailliert beschrieben. Es ist anzumerken, dass die Anzahl der unterstützten Verfahren der Phase 1 wesentlich geringer ausfällt als die der Phase 2.

Umsetzung:

- **Phase 1:** symmetrische Verschlüsselungsverfahren AES-256 und die Diffie-Hellmann-Gruppen 14-18 zur Gewährleistung der Vertraulichkeit [7]

- **Phase 2 :** symmetrische Verschlüsselungsverfahren AES-CTR, AES-256, AES-GCM, AES-CCM und die Diffie-Hellmann-Gruppen 14-18 zur Gewährleistung der Vertraulichkeit [7]
- **Schlüssellänge:** ausreichende Schlüssellänge von min. 128 Bit [4]
- **Schlüsselaustausch:** Diffie-Hellmann-Gruppen 2 oder 5 [4]

3.1.2 Authentisierung der Kommunikationspartner

Das Protokoll IKEv1 ermöglicht die gegenseitige Authentisierung des Kommunikationspartners durch den Einsatz von Zertifikaten.

Umsetzung:

- Nutzung von Zertifikaten unter Einsatz des RSA-Verfahrens mit einer Mindestschlüssellänge von 2048 Bit [7]
- Auf Pre-Shared Keys ist zu verzichten [4]

3.1.3 Schutz der Integrität einer Nachricht

Das Protokoll IKEv1 unterstützt eine Vielzahl kryptografischer Hashfunktionen in Verbindung mit dem HMAC-Verfahren, um die Integrität von Nachrichten zu schützen. Eine Auswahl der Hashfunktionen muss konfigurationsseitig erfolgen.

Umsetzung:

- Folgende Hash-Algorithmen aus der Hashgruppe SHA-2 sind erlaubt: SHA-224, SHA-256, SHA-384 und SHA-512

3.1.4 Schutz vor Wiedereinspielen alter Nachrichten

Das Protokoll IKEv1 sieht für den Verbindungsaufbau den Einsatz von zufälligen Daten (sogenannte „Nonces“) vor, um einen Schutz vor dem Wiedereinspielen von alten Nachrichten zu gewährleisten. Das für die Datenübertragung einzusetzende Protokoll ESP sichert den Replay-Schutz durch aufsteigende Sequenznummern.

3.1.5 Perfect Forward Secrecy

Das Protokoll IKEv1 unterstützt „Perfect Forward Secrecy“ durch die Verwendung des Diffie-Hellmann-Algorithmus in Phase 2. Dies muss allerdings explizit konfiguriert werden, weil die Phase 2 auch ohne den Diffie-Hellmann-Algorithmus nutzbar ist.

3.1.6 Auffrischen von Schlüsselmaterial (Re-Keying)

Das Erneuern von Schlüsselmaterial wird vom Protokoll IKEv1 unterstützt und wird zwischen den Kommunikationspartnern gemäß der Konfiguration ausgehandelt. Das Schlüsselmaterial wird anschließend während der Übertragung der Daten periodisch erneuert.

Umsetzung:

- Es ist eine maximale Lebensdauer der Schlüssel von 24 Stunden für die Phase 1 und eine maximale Lebensdauer von 4 Stunden für Phase 2 zu wählen. [3]

3.2 Umsetzung der Anforderungen mittels IPsec / IKEv2

Für die sichere Verwendung von IPsec / IKEv2 existieren zahlreiche aktuelle Empfehlungen verschiedener Institutionen. Dieses Kapitel stützt sich überwiegend auf die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik [3] sowie der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) [5].

3.2.1 Vertraulichkeit der Informationen

Durch den Einsatz des Protokolls IKEv2 kann für jede Verbindung ein neuer Sitzungsschlüssel erzeugt werden. Das Protokoll stützt sich hierzu auf den Diffie-Hellmann-Algorithmus zur Erzeugung eines geheimen, symmetrischen Schlüssels. Die Art und Weise, wie die symmetrische Verschlüsselung durchgeführt wird, ist abhängig von der jeweiligen Konfiguration und wird im Verbindungsaufbau zwischen den Parteien ausgehandelt.

Umsetzung:

- Zur Gewährleistung der Vertraulichkeit muss eine der folgenden Kombinationen aus Verschlüsselungsverfahren und Betriebsart benutzt werden: [5]
    - AES-CTR

- CAMELLIA-CTR
- AES-CCM-12, AES-CCM-16
- CAMELLIA-CCM-12, CAMELLIA-CCM-16
- AES-GCM-12, AES-GCM-16

- Darüber hinaus sind für den Diffie-Hellmann-Algorithmus folgende Gruppen zu verwenden: [5]
  - Mindestens 3072 Bit für Restklassengruppen (3072 Bit entspricht der Gruppe 15)
  - Mindestens 256 Bit für Gruppen auf elliptischen Kurven

3.2.2 Authentisierung der Kommunikationspartner

Das Protokoll IKEv2 unterstützt wie der Vorgänger die Verwendung von Zertifikaten zur Authentisierung des Kommunikationspartners. Es ist anzumerken, dass mit dem Protokoll IKEv2 eine hybride Authentisierung möglich ist, also eine Partei sich über einen Pre-Shared Key und die andere über ein Zertifikat authentisieren kann. In einer Konfiguration ist daher auf den beidseitigen Einsatz von Zertifikaten zu achten.

Umsetzung:

- Das RSA-Verfahren ist in Zusammenhang mit Zertifikaten zu verwenden. [3]
- Das Signatur-Verfahren SHA-2 ist zur Nutzung im Zertifikat zu verwenden.

3.2.3 Schutz der Integrität einer Nachricht

Das Protokoll IKEv2 unterstützt eine Vielzahl kryptografischer Hashfunktionen in Verbindung mit dem HMAC-Verfahren, um die Integrität von Nachrichten zu schützen.

Umsetzung:

- Eines der folgenden Verfahren zur Gewährleistung der Datenintegrität ist zu nutzen: [5]
  - HMAC-SHA2-256
  - HMAC-SHA2-384
  - HMAC-SHA2-512

3.2.4 Schutz vor Wiedereinspielen alter Nachrichten

Das Protokoll IKEv2 sieht für den Verbindungsaufbau den Einsatz von zufälligen Daten (sogenannte „Nonces“) vor, um einen Schutz vor dem Wiedereinspielen von alten Nachrichten zu gewährleisten. Das für Datenübertragung einzusetzende Protokoll ESP sichert den Replay-Schutz durch aufsteigende Sequenznummern.

3.2.5 Perfect Forward Secrecy

Das Protokoll IKEv2 unterstützt „Perfect Forward Secrecy“, das wie bei IKEv1 explizit konfiguriert werden muss. Statt der Nutzung des Diffie-Hellmann-Algorithmus in der Phase 2 sieht das Protokoll IKEv2 hierzu den Nachrichten-Typ „CREATE_Child_SA“ vor.

3.2.6 Auffrischen von Schlüsselmaterial (Re-Keying)

Das Erneuern von Schlüsselmaterial wird durch das Protokoll IKEv2 ebenfalls unterstützt. Im Gegensatz zum Protokoll IKEv1 wird jedoch die Lebensdauer von geheimen Schlüsseln nicht mehr zwischen den Parteien ausgehandelt, sondern dann durchgeführt, wenn die Lebensdauer eines Schlüssels für eine Partei erreicht ist.

Umsetzung:

- Gemäß dem BSI [3] ist die Lebensdauer von kurzfristigem Schlüsselmaterial je nach Sicherheitsanforderung festzulegen. Es ist jedoch eine maximale Lebensdauer von 24 Stunden für die IKE-SA und eine maximale Lebensdauer von 4 Stunden für IPsec-SA zu wählen.

4 Umsetzung mittels OpenVPN

Zur Umsetzung der in Kapitel 2 formulierten Anforderungen eignet sich das Protokoll OpenVPN, das einem gleichnamigen Open-Source-Projekt entstammt. Es nutzt zum Verbindungsaufbau die SSL/TLS-Technologie und nutzt die dann bestehende Verbindung für einen weiteren Verbindungsaufbau über das OpenVPN-Protokoll. Das daraus resultierende Schlüsselmaterial wird anschließend zur Übertragung der eigentlichen Daten über das OpenVPN-Protokoll genutzt.

Ähnlich wie im Falle von IPsec kann allerdings auch OpenVPN dahingehend konfiguriert werden, dass die im Kapitel 2 beschriebenen Anforderungen nicht erfüllt werden.
In Hinblick auf eine Nutzung von OpenVPN ist positiv zu bewerten, dass OpenVPN schon eine sichere Grundkonfiguration vorsieht.

4.1 Vertraulichkeit der Informationen

Das Protokoll OpenVPN nutzt zur Verschlüsselung der zu übertragenden Daten im Anschluss an den SSL/TLS-Verbindungsaufbau standardmäßig das Verschlüsselungsverfahren Blowfish in der Betriebsart CBC.

Umsetzung:

- Zur Verschlüsselung der Daten ist das Verschlüsselungsverfahren AES-256 in der Betriebsart CBC zu verwenden. [7]

4.2 Authentisierung der Kommunikationspartner

Durch die Nutzung von SSL/TLS im Verbindungsaufbau wird die Authentisierung des Kommunikationspartners durch SSL/TLS realisiert.

Umsetzung:

- Beim RSA-Verfahren in Kombination mit Zertifikaten ist eine Schlüssellänge von mindestens 2048 Bit zu wählen. [2]

4.3 Schutz der Integrität einer Nachricht

Das OpenVPN-Protokoll sieht in der Grundkonfiguration eine Nutzung des Verfahrens „HMAC-SHA1“ zur Sicherung der Datenintegrität während der Datenübertragung vor.

Umsetzung:

- Zur Gewährleistung der Datenintegrität ist „HMAC-SHA384“ zu nutzen. [7]

4.4 Schutz vor Wiedereinspielen alter Nachrichten

Das Protokoll SSL/TLS sieht einen Schutz vor dem Wiedereinspielen von Nachrichten im Verbindungsaufbau vor. Dieser Schutz wird durch die Nutzung von zufälligen Daten in jeder Verbindung realisiert. Das OpenVPN-Protokoll setzt ähnlich wie IPsec einen Replay-Schutz durch die Verwendung von aufsteigenden Sequenznummern um.

4.5 Perfect Forward Secrecy

Die Eigenschaft „Perfect Forward Secrecy“ ist in einer Grundkonfiguration nicht gegeben und wird erst durch eine Änderung der Grundkonfiguration realisiert. Dazu muss die Verwendung von bestimmten Cipher-Suites, die „Perfect Forward Secrecy“ sicherstellen, vorgegeben werden.

Umsetzung:

- Zur Gewährleistung „Perfect Forward Secrecy“ sind folgende Cipher-Suites sowohl clientseitig als auch serverseitig zu konfigurieren: [2]
    - DHE-RSA-AES256-GCM-SHA384
    - DHE-RSA-AES256-SHA256
    - DHE-RSA-AES128-GCM-SHA256
    - DHE-RSA-AES128-SHA256

4.6 Auffrischen von Schlüsselmaterial (Re-Keying)

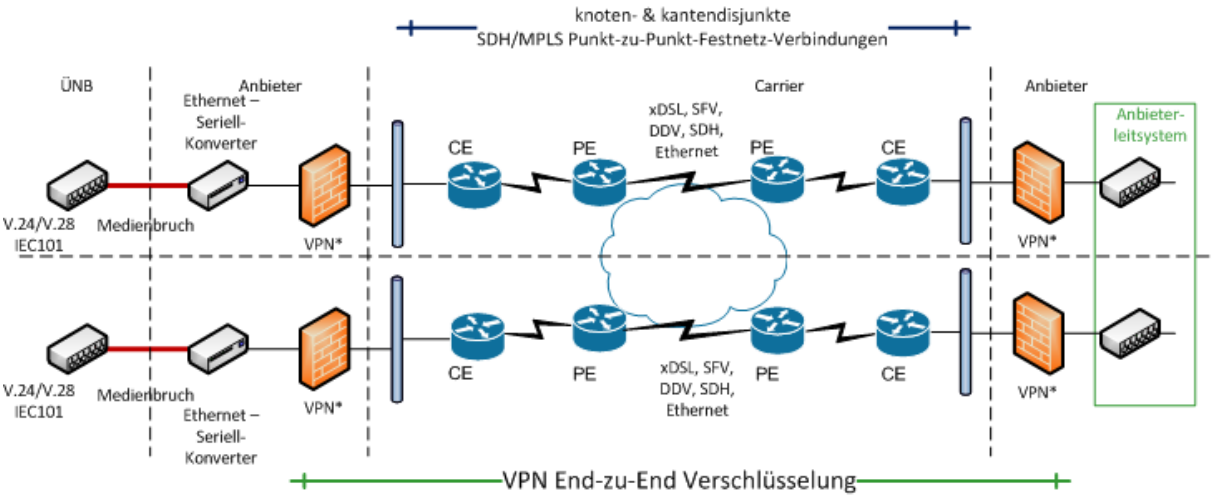
Das Protokoll OpenVPN sieht eine Erneuerung von Schlüsselmaterial standardmäßig alle 3.600 Sekunden vor. Dies entspricht den Vorgaben, die im Zusammenhang für IPsec ebenfalls gelten.

5 Alternative Anbindungsmöglichkeit zur SDH/PDH Technik auf Basis sicherer MPLS-Verbindungen

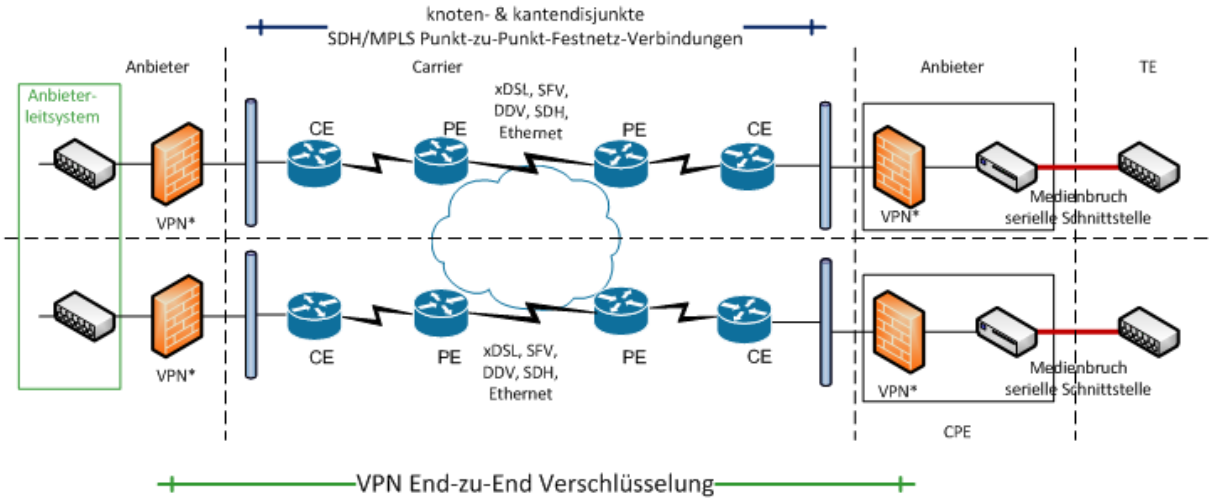
Für die Regelreserveart aFRR kann alternativ zur Forderung nach einer SDH/PDH-Verbindung gemäß der Prüfpunkte A05 und C03 der *Mindestanforderungen an die Informationstechnik des Reservenanbieters für die Erbringung von Regelreserve* eine sichere MPLS-Verbindung durch den ÜNB zugelassen werden.

Folgende Spezifikation gilt für den Aufbau von sicheren MPLS-Netzwerken als alternative Anbindungsmöglichkeit zur SDH/PDH-Technik.

A05 (betrifft aFRR): Anbindung an einen ÜNB bei mehr als 50 MW in der LFR-Zone:



C03 (betrifft aFRR): Anbindung von technischen Einheiten ≥ 50 MW:



Vorgabe ist die redundante Customer Edge (CE) Anbindung mit zwei Standleitungen zu verschiedenen Provider Edge (PE) Routern zur Erreichung einer höheren Verfügbarkeit und zusätzlich mit der Option zur Bandbreitenerhöhung mit zwei CE-Routern.
Die Pfadführung zwischen PE- und CE-Router sollte dabei vollständig knoten- und kantendisjunkt sein. Für den MPLS-Backbone kann bei entsprechenden SLAs auch ein Anbieter (mit entsprechender Redundanz) genutzt werden.

Zur Erhöhung der Verfügbarkeit können zwischen den CE-Routern bzw. zwischen den VPN-Gateways Querverbindungen (mit Failover) eingesetzt werden.

Die Festnetzverbindung zwischen CE und PE sollte nicht auf Basis von ADSL-Technik oder in einem „Shared Medium“ mit anderen öffentlichen Teilnehmern (keine öffentlichen IP-Adressen, geschlossene Benutzergruppe) geführt werden.

Für eine risikoorientierte Betrachtung der Gefährdungen und providerseitigen Sicherungsmaßnahmen wird auf die Kurzstudie des BSI zu Gefährdungen und Maßnahmen beim Einsatz von MPLS verwiesen [13]. Durch den Einsatz der VPN-Verbindung wird den meisten der aufgeführten Risiken aber ausreichend begegnet.

6 Literaturverzeichnis

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI), Technische Richtlinie TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 1 2014.

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI), Technische Richtlinie 02102-2, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 - Verwendung von Transport Layer Security (TLS), Version 2014.

[3] Bundesamt für Sicherheit in der Informationstechnik (BSI), Technische Richtlinie 02102-3, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 3 - Verwendung von IPsec, Version 2014.

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutz-Katalog: Sichere An-bindung eines externen Netzes mit IPSec, 13. Ergänzungslieferung, 2013.

[5] European Union Agency for Network and Information Security Agency (ENISA), Algorithms, Key Sizes and Parameters Report, Version 1.0, Oktober 2013.

[6] National Institute of Standards and Technology (NIST), Recommendation for Key Management – Part 1: General (Revision 3), Special Publication 800-57, Technology Administration, U.S. Department of Commerce, Juli 2012.

[7] BetterCrypto.org, Applied Crypto Hardening, https://bettercrypto.org/static/applied-crypto-harde-ning.pdf, zuletzt abgerufen am 08. Mai 2014.

[8] D. Harkins, D. Carrel, RFC 2409, The Internet Key Exchange (IKE), November 1998.

[9] C. Kaufman, P. Hoffman Y. Nir, P. Eronen, RFC 5996, Internet Key Exchange Protocol Version 2 (IKEv2), September 2010.

[10] OpenVPN, http://openvpn.net, zuletzt abgerufen am 08. Mai 2014.

[11] Bundesamt für Sicherheit in der Informationstechnik (BSI), Technische Richtlinie: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, BSI TR-02102-1, Version 2015-01, 10. Februar 2015

[12] BDEW - Whitepaper „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“

[13] Bundesamt für Sicherheit in der Informationstechnik (BSI), Kurzstudie zu Gefährdungen und Maßnahmen beim Einsatz von MPLS, Version 1.5, 2009