Requirement for closed user groups for the provision of control reserve

Status: 01.05.2023

Version history

Version	Date	Comment
1.0	22/04/2016	First valid version (consolidated version for all RL products)
2.0	26/10/2018	Revision as part of the renewal of the PQ conditions
3.0	01/05/2023	Addition for mobile connections

Contents

1 Introduction 5

1.1 Structure of this document 7

2 Security requirements for the data transfer 8

2.1 Confidentiality of information 8

2.2 Authentication of the communication partner 9

2.3 Protecting the integrity of a message 10

2.4 Protection from replaying old messages 11

2.5 Secondary security requirements 11

2.5.1 Perfect Forward Secrecy 11

2.5.2 Refreshing key material (re-keying) 12

3 Implementation with IPsec 13

3.1 Implementation of the requirements with IPsec/IKEv1 14

3.1.1 Confidentiality of information 14

3.1.2 Authentication of the communication partner 14

3.1.3 Protecting the integrity of a message 15

3.1.4 Protection from replaying old messages 15

3.1.5 Perfect Forward Secrecy 15

3.1.6 Refreshing key material (re-keying) 15

3.2 Implementation of the requirements with IPsec/IKEv2 16

3.2.1 Confidentiality of information 16

3.2.2 Authentication of the communication partner 16

3.2.3 Protecting the integrity of a message 17

3.2.4 Protection from replaying old messages 17

3.2.5 Perfect Forward Secrecy 17

3.2.6 Refreshing key material (re-keying) 17

4 Implementation with OpenVPN 19

4.1 Confidentiality of information 19

4.2 Authentication of the communication partner 19

4.3 Protecting the integrity of a message 19

4.4 Protection from replaying old messages 20

4.5 Perfect Forward Secrecy 20

4.6 Refreshing key material (re-keying) 20

5 Alternative connection option to the SDH/PDH technology based on secure MPLS connections 21

6 List of references 23

1 Introduction

The connection of the technical units to a reserve provider's control system and the connection of this control system to the transmission system operators' transmission points must have a comparable security level to the transmission system operators.

The IT requirements for types of control reserve require "closed user groups" as well as encryption technologies, etc., whose requirements are specified in this document. This document is an annex to the current version of the IT requirements for types of control reserve and is subject to their validity.

The establishment of closed user groups requires a "secure system architecture" [12], which should not just be realised by a single protection measure but by additional security measures across several levels.

For connections between technical units, control systems and transfer points of the transmission system operators this means that this should be realised as a two-stage solution with a separate network exclusively for the control system's network traffic (used to provide the active power reserve) with a separate, additional encryption via VPN. The network used for this control system must not be routed via the public Internet (i.e. must not contain any publicly accessible IP addresses). For example, this is possible by using private APNs in the mobile network, private DSL connections or dedicated lines. The reserve provider must be fully responsible for the configuration of the additional encryption with a VPN and must not be known by the carrier (e.g. the APN provider) so that an end-to-end encryption independent of the underlying network can be ensured.

Only VPNs based on IPsec or OpenVPN are permitted for encryption within the 'closed user groups for providing control reserve) within the scope of the conditions described in this document.
Both the IPsec and OpenVPN technologies can satisfy the key security requirements for a VPN within the framework conditions stipulated below and can be used to securely connect networks.

As the incorrect configuration of IPsec and OpenVPA can quickly lead to the non-existence of a ‘closed user group’, this document provides product-independent requirements for a secure configuration.

1.1 Structure of this document

Chapter 2 initially mentions the security requirements for every VPN technology. These security requirements are then transferred to IPsec and OpenVPN in chapter 3 and 4.

As several possibilities for implementing almost every requirement from chapter 2 exist, chapters 3 and 4 on IPsec and OpenVPN specify the approach to be taken.

As certain choices exist, the reserve provider must stipulate the technology used to realise every closed user group and how the individual security requirements were implemented as part of the pre-qualification.

2 Security requirements for the data transfer

The cryptographic procedures used for implementation can be divided into symmetric or asymmetric procedures. The main difference between the two procedures is based on the fact that, for a symmetric procedure, both communication partners know a secret while, for an asymmetric procedure, one communication partner protects a secret. When using this procedure to realise a VPN, these cryptographic secrets exist in the form of keys, either as temporary or permanent keys. In this context, a temporary key has a temporary validity for a maximum of the duration of a VPN connection.

2.1 Confidentiality of information

When transferring data via third party networks, the encryption of data to protect confidentiality is essential. To do so, the data are transferred in a form that does not permit any conclusions to be drawn in relation to the original data and only those who possess the secret cryptographic key receive access to the content of the message. In this respect, a key requirement for the encryption of the data is that the confidentiality is exclusively based on knowledge of the secret key used. The encryption methods and key lengths used must always be assumed to be known.

When encrypting data, symmetric encryption methods have considerable speed advantages compared to asymmetric procedures, so only symmetric encryption methods are used in this respect. In this case, the term ‘symmetric’ once again means that both parties are aware of the secret key and the same key is used for encryption and decryption. A key security requirement is that a secure encryption method with an adequate key length is used.

A secret key must be distributed on both sides of the communication in order to use a symmetric encryption method. According to the current state of cryptography, the same key is no longer used for more than one connection. The use of appropriate cryptographic procedures enables a secret key required for the symmetric encryption to be created when establishing a connection. Two procedures have established themselves in everyday practice in this respect. Firstly, a randomly generated secret session key can be encrypted with a public permanent key and transmitted to the communication partner. This partner can decrypt the session key using the corresponding public key and use it for secure communication. Secondly, the Diffie-Hellmann algorithm can be used to generate a secret session key on both sides without this being transmitted in the data connection. To do so, both parties generate two keys based on public Diffie-Hellmann parameters. One of these keys is transmitted to the communication partner in each case. Using the Diffie-Hellmann algorithm, both sides calculate the secret session key from their own, non-transferred key and the key received from the partner. To ensure the secure use of the Diffie-Hellmann algorithm, the public parameters must be an adequate length. The predefined parameters are combined in groups so that a secure group generally has to be selected.

Another requirement to be considered as part of the symmetric encryption is that repetitions in plain text must not create the same ciphertext at the same position in each case. For this purpose, the plain text data is additionally modified by the sender before encryption and by the recipient after decryption according to a previously arranged cipher modes of the symmetric encryption method (for example, current cipher modes are CBC, CFB or CTR). In addition, a secure cipher mode must be selected to ensure confidentiality.

The cipher mode, together with the encryption method and the key length, defines the manner in which the data are encrypted and can generally be identified in a configuration based on the designation, e.g. AES-256-CBC.

2.2 Authentication of the communication partner

The secure authentication of the communication partner is a necessary basis for fulfilling the security requirements stipulated in this chapter. Without secure authentication, a middleman can access and pretend to be the relevant communication partner in a connection. As a result, the security requirements described in these chapters are implemented in communication with a middleman and they lose their protective function. It is therefore essential that authentication occurs on both sides and that it is implemented as securely as possible.

The authenticity of the communication partner is ensured using a cryptographic secret. In this case, a distinction is made between symmetric and asymmetric procedures. In a symmetric procedure, a secret key is first distributed on both sides and used as proof of the authenticity of the communication partner when establishing a connection. Due to the necessary secure distribution in advance, this symmetric key is often referred to as the “pre-shared key” in the context of a VPN.

In an asymmetric procedure, a pair of keys, consisting of a private and public key, is used to prove the authenticity of the communication partner via the knowledge of the private key. In this case, the communication partner is checked using the corresponding public key. The necessity of securely distributing the public key is generally realised via certificates. To ensure a secure distribution, a certificate contains a signature that was created by a trusted certification body.

A comparison of the two procedures shows that authentication with an asymmetric procedure has significant security advantages. These particularly including the following advantages:

- The storage of the private key on only one side of the communication significantly minimises the attack target.
- The public key can be distributed via a certificate.
- The key lengths of asymmetric keys are generally sufficiently long, while, in practice, the use of a pre-shared key is often derived from a relatively short user password. The pre-shared key therefore has a low entropy and is also susceptible to dictionary attacks.

The clear, security-enhancing benefits of the asymmetric authentication procedures means that the use of asymmetric procedures should be a key security requirement to be implemented.

2.3 Protecting the integrity of a message

When transferring encrypted data, it must also be ensured that these data have not been modified along the transmission path. A symmetric encryption method does not ensure the protection of the data integrity, so this must also be ensured. Additional data in the form of a checksum of the actual data are generally appended for this purpose. The checksum allows the integrity of the data to be verified. Due to the performance advantages, symmetric procedures are generally used to create a secure checksum. The secret key generated using the symmetric procedure is generally created when establishing a connection. As a result, a secure checksum can only be created with knowledge of the secret key and therefore enables the identification of manipulations on the encrypted data, including the checksum.

An oft-used, secure procedure for creating secure checksums is the “Keyed-Hash Message Authentication Code” (HMAC) procedure, which is detailed in RFC 2104. It is essentially based on the use of cryptographic hash functions, such as SHA-256.

2.4 Protection from replaying old messages

When transferring encrypted data, a potential attacker must not be able to upload previously recorded, encrypted data traffic in a new connection (replay attack). This type of attack must be explicitly addressed and is not prevented by implementing other security requirements. As a measure to protect a replay attack, a connection must has a feature that distinguishes an old connection from a new connection and which can be verified by the communication partner. The following features are suitable for this purpose:

- Unique session ID
- Random data
- Sequence number
- Time stamp

In addition, protection against replaying old messages must exist when establishing a connection as well as during the data transmission.

2.5 Secondary security requirements

2.5.1 Perfect Forward Secrecy

The fulfilment of the “Perfect Forward Secrecy” property essentially means that compromising a secret key only discloses the data that were protected with this key. For instance, compromising a secret key must not disclose another secret key that has been used to encrypt other data.

Specifically, this means that if a secret, generally asymmetric permanent key is compromised, this does not allow a recorded connection from the past to be decrypted; i.e. knowledge of a permanent key must not be able to be used to derive the secret session key from a past connection. This situation exists if, to arrange a secret session key when establishing a connection, a private permanent key was used in a manner such that the secret session key was encrypted with the private permanent key and transmitted to the communication partner.

2.5.2 Refreshing key material (re-keying)

Another security requirement consists of refreshing temporary key material. This is necessary because, when linking networks, the duration of the link is not foreseeable without further information. Depending on the data to be transferred, this can result in continuous data traffic so that a VPN remains in place for a long period of time. Moreover, this situation may also have been desired and deliberately established. This situation means that a secret session key is used over an extended period of time. A potential attacker can use this period to cryptographically attack the secret session key. The necessary period for a potential attack therefore depends on the encryption algorithm used and the key length.

To protect against a cryptographic attack on a data connection, the timeframe for an attack must be kept as short as possible. Moreover, the regeneration of key material must not be caused by a disconnection and connection; rather it must be supported by a corresponding network protocol.

3 Implementation with IPsec

IPsec refers to a collection of numerous network protocols that enable the secure establishment and operation of a VPN. The network protocols, which overwhelmingly originate from the 1990s, can be divided into protocols for establishing connections and data transfer. Only a small number of protocols from the protocol collection are considered for the implementation of the requirements formulated in chapter 2 and the linking of networks covered here. Only the IKE protocol, used to establish connections, fulfils the requirement that a new secret key is created for every connection. Likewise, only the ESP protocol, used to transfer data, fulfils the requirement that data is encrypted before transfer. When considering linking networks, this can only take place in IPsec tunnel mode and represents a fundamental IPsec configuration together with the IKE and ESP protocols.

Either version 1 (IKEv1) or the newer, revised version 2 (IKEv2) of the IKE protocol can be used to establish a connection to a VPN tunnel. A key difference in version 2 is that the number of necessary packages for establishing a connection has reduced significantly (from 9 packages in “Main Mode” and 6 packages in “Aggressive Mode” to just 4 packages). Moreover, the establishment of a connection no longer has to be divided into two phases, as was the case in version 1, without negatively affecting security. Phase 1 of IKEv1 provides for the establishment of a secure, authenticated connection between two VPN end points. In phase 2, this connection is used to create new key material for the actual VPN tunnel or renew key material for an existing connection. But, the connection is not just used to create key material, it also enables the secure and encrypted transmission of status or error messages. A corresponding equivalent phase 2 is realised with IKEv2 via the “CREATE_CHILD_SA” message type.

A deviation from the fundamental configuration leads to the non-fulfilment of the requirements stipulated in chapter 2.

The following chapters describe how the IPsec protocol collection implements the requirements specified in chapter 2 and which specific cryptographic procedures need to be used to achieve an adequate protective function by using cryptography. As a result of the fundamental changes with the introduction of the IKEv2 protocol, the implementations are specified for the relevant IKE versions.

3.1 Implementation of the requirements with IPsec/IKEv1

When implementing the requirements described in chapter 2, it is important to note that, due to the revised IKE version 2, current recommendations almost exclusively relate to version 2. This chapter is therefore primarily based on recommendations from the BSI Basic Protection Catalogue [4] and the recommendations of the “BetterCrypto” project [7].

3.1.1 Confidentiality of information

The use of the IKE protocol from the IPsec protocol suite allows a new session key to be created for every connection. For this purpose, the protocol is based on the Diffie-Hellmann algorithm to create a secret, symmetric key.

The use of symmetric encryption methods, including the operating mode as well as the parameters of the Diffie-Hellmann algorithm, are variable due to the IKE and are negotiated between the VPN end points via corresponding numbers. Assignment takes place via the “Internet Assigned Numbers Authority” (IANA) according to protocol IKEv1. A new procedure receives a corresponding number from the IANA if the procedure is adequately described. The procedures are generally described in detail by an RFC. It must be noted that the number of supporting procedures in phase 1 is much fewer than those in phase 2.

Implementation:

- **Phase 1:** symmetric encryption method AES-256 and the Diffie-Hellmann groups 14-18 to ensure confidentiality [7]
- **Phase 2:** symmetric encryption methods AES-CTR, AES-256, AES-GCM, AES-CCM and the Diffie-Hellmann groups 14-18 to ensure confidentiality [7]
- **Key length:** adequate key length of at least 128 bits [4]
- **Key exchange:** Diffie-Hellmann groups 2 or 5 [4]

3.1.2 Authentication of the communication partner

Protocol IKEv1 enables the mutual authentication of the communication partner by the use of certificates.

Implementation:

- Use of certificates using the RSA procedure with a minimum key length of 2048 bits [7]

- Pre-shared keys must be avoided [4]

3.1.3 Protecting the integrity of a message

The IKEv1 protocol supports a range of cryptographic hash functions in connection with the HMAC procedure in order to protect the integrity of messages. Hash functions must be selected on the configuration side.

Implementation:

- The following hash algorithms from the hash group SHA-2 are permitted: SHA-224, SHA-256, SHA-384 and SHA-512

3.1.4 Protection from replaying old messages

The IKEv1 protocol provides for the use of random data (“Nonces”) to establish a connection in order to ensure protection against the replaying of old messages. The ESP protocol to be used for the data transfer ensures replay protection with ascending sequence numbers.

3.1.5 Perfect Forward Secrecy

The IKEv1 protocol supports “Perfect Forward Secrecy” by using the Diffie-Hellmann algorithm in phase 2. However, this must be explicitly configured because phase 2 can also be used without the Diffie-Hellmann algorithm.

3.1.6 Refreshing key material (re-keying)

The refreshing of key material is supported by the IKEv1 protocol and is negotiated between the communication partners according to the configuration. The key material is then periodically renewed during the data transfer.

Implementation:

- A maximum service life of the key of 24 hours must be selected for phase 1 and a maximum service life of 4 hours for phase 2. [3]

3.2 Implementation of the requirements with IPsec/IKEv2

Numerous up-to-date recommendations from various institutions exist for the secure use of IPsec/IKEv2. This chapter is primarily based on the recommendations of the Federal Office for Information Security [3] as well as the European Union Agency for Network and Information Security (ENISA) [5].

3.2.1 Confidentiality of information

The use of the IKEv2 protocol allows a new session key to be created for every connection. For this purpose, the protocol is based on the Diffie-Hellmann algorithm to create a secret, symmetric key. The manner in which the symmetric encryption is executed depends on the relevant configuration and is negotiated between the parties when establishing the connection.

Implementation:

- To ensure confidentiality, one of the following combinations of encryption methods and modes must be used: [5]
    - AES-CTR
    - CAMELLIA-CTR
    - AES-CCM-12, AES-CCM-16
    - CAMELLIA-CCM-12, CAMELLIA-CCM-16
    - AES-GCM-12, AES-GCM-16
- In addition, the following groups must be used for the Diffie-Hellmann algorithm: [5]
    - At least 3072 bits for residue class groups (3072 bits corresponds to group 15)
    - At least 256 bits for groups on elliptic curves

3.2.2 Authentication of the communication partner

Just like its predecessor, the IKEv2 protocol supports the use of certificates to authenticate the communication partner. It must be noted that hybrid authentication is possible with the IKEv2 protocol, i.e. one party can be authenticated via a pre-shared key and the other via a certificate. In a configuration, attention must therefore be paid to the use of certificates on both sides.

Implementation:

- The RSA procedure must be used in connection with certificates. [3]
- The SHA-2 signature procedure must be used in the certificate.

3.2.3 Protecting the integrity of a message

The IKEv2 protocol supports a range of cryptographic hash functions in connection with the HMAC procedure in order to protect the integrity of messages.

Implementation:

- One of the following procedures must be used to guarantee data integrity: [5]
  - HMAC-SHA2-256
  - HMAC-SHA2-384
  - HMAC-SHA2-512

3.2.4 Protection from replaying old messages

The IKEv2 protocol provides for the use of random data (“Nonces”) to establish a connection in order to ensure protection against the replaying of old messages. The ESP protocol to be used for data transmission ensures replay protection with ascending sequence numbers.

3.2.5 Perfect Forward Secrecy

The IKEv2 protocol supports “Perfect Forward Secrecy”, which must be explicitly configured for IKEv1. Instead of using the Diffie-Hellmann algorithm in phase 2, the IKEv2 protocol provides for the “CREATE_Child_SA” message type for this purpose.

3.2.6 Refreshing key material (re-keying)

Refreshing key material is also supported by the IKEv2 protocol. However, in contrast to the IKEv1 protocol, the service life of secret keys is no longer negotiated between the parties, rather it takes place when the service life of a key is reached for a party.

Implementation:

- According to the BSI [3], the service life of temporary key material must be defined depending on the security requirement. However, a maximum service life of 24 hours must be selected for the IKE-SA and a maximum service life of 4 hours for IPsec-SA.

4 Implementation with OpenVPN

The OpenVPN protocol, which originates from an open source project of the same name, is suitable for implementing the requirements formulated in chapter 2. It uses the SSL/TLS technology to establish a connection and then uses the existing connection to establish an additional connection via the OpenVPN protocol. The resulting key material is then used to transfer the actual data via the OpenVPN protocol.

However, just like in the case of IPsec, OpenVPN can be configured so that the requirements described in chapter 2 are not fulfilled.
With regard to the use of OpenVPN, the fact that OpenVPN already provides a secure basic configuration must be positively assessed.

4.1 Confidentiality of information

The OpenVPN protocol uses the Blowfish encryption method in the CBC mode as standard to encrypt the data to be transferred after the SSL/TLS connection has been established.

Implementation:

- The AES-256 encryption method in the CBC mode must be used to encrypt the data. [7]

4.2 Authentication of the communication partner

The communication partner is authenticated by SSL/TLS by using SSL/TLS when establishing a connection.

Implementation:

- A key length of at least 2048 bits must be selected for the RSA method in combination with certificates. [2]

4.3 Protecting the integrity of a message

In the basic configuration, the OpenVPN protocol provides for the use of the “HMAC-SHA1” method to ensure data integrity during the data transfer.

Implementation:

- “HMAC-SHA384” must be used to ensure data integrity. [7]

4.4 Protection from replaying old messages

The SSL/TLS protocol provides for protection against replaying messages when establishing a connection. This protection is realised by using random data in every connection. The OpenVPN protocol implements a replay protection by using ascending sequence numbers, similar to IPsec.

4.5 Perfect Forward Secrecy

The “Perfect Forward Secrecy” property is not provided in a basic configuration and is only realised by a change in the basic configuration. To do so, the use of certain cipher suites, which ensure “Perfect Forward Secrecy” must be defined.

Implementation:

- To ensure “Perfect Forward Secrecy”, the following cipher suites must be configured on the client and server side: [2]
    - DHE-RSA-AES256-GCM-SHA384
    - DHE-RSA-AES256-SHA256
    - DHE-RSA-AES128-GCM-SHA256
    - DHE-RSA-AES128-SHA256

4.6 Refreshing key material (re-keying)

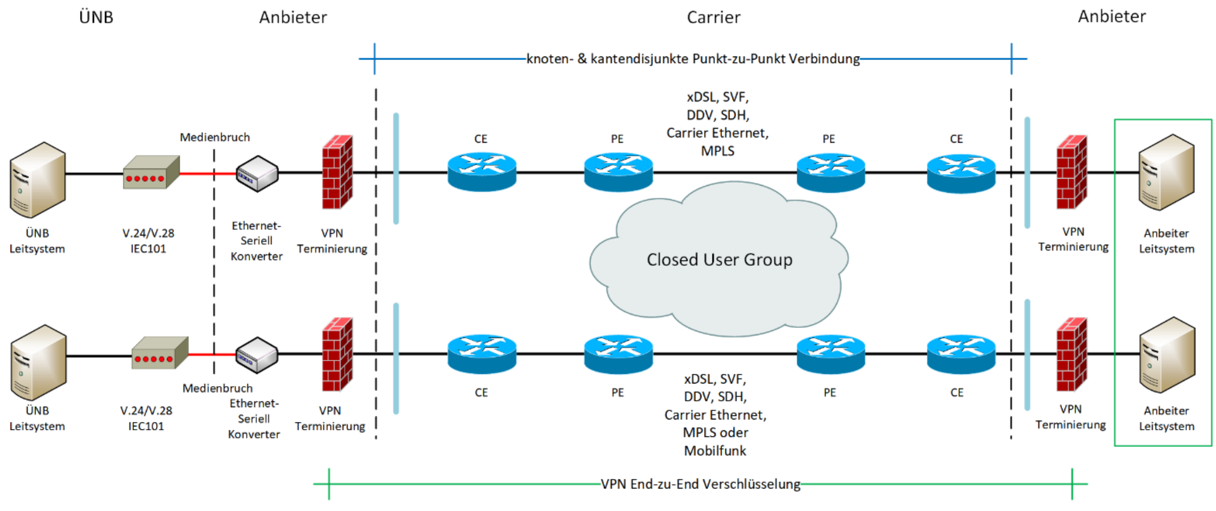
The OpenVPN protocol provides for the refreshing of key material every 3,600 seconds as standard. This corresponds to the provisions that also apply in relation to IPsec.

5 Alternative connection option to the SDH/PDH technology based on secure MPLS connections or mobile connections

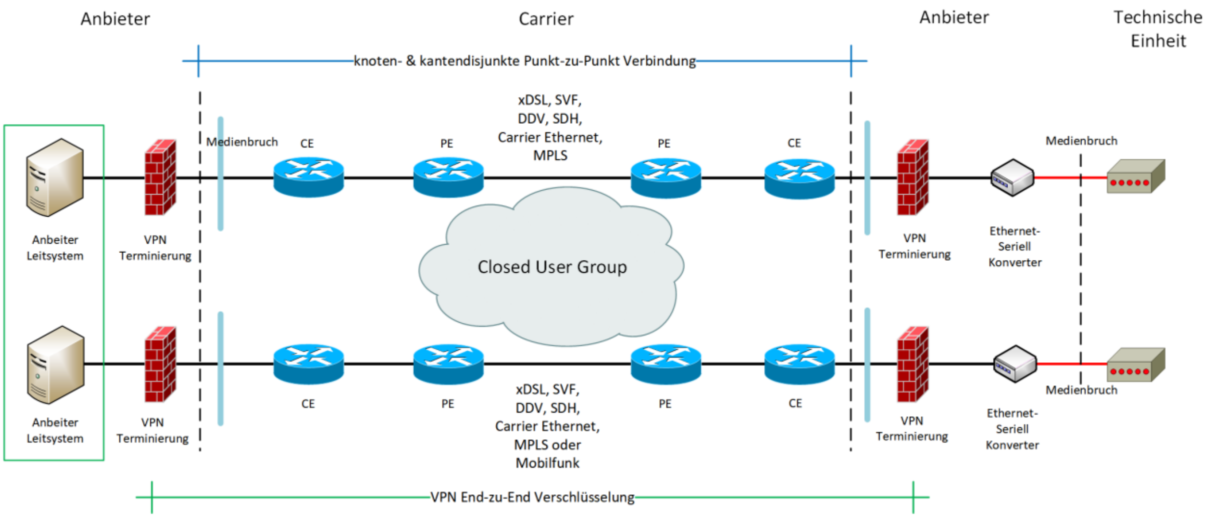
For the aFRR control reserve type, as an alternative to requesting an SDH/PDH connection according to test point A05 of the *Minimum requirements for the reserve provider's information technology for the provision of control reserve*, a secure MPLS connection may be approved by the TSO.

For the control reserve type aFRR, a secure MPLS connection can be approved by the TSO as an alternative to the requirement for an SDH/PDH connection in accordance with checkpoint C03 of the minimum requirements for the information technology of the reserve provider for the provision of control reserve. In combination with test point C02, one of the redundant connections may also be provided via a closed user group in mobile communications.
The following specification applies for the establishment of secure MPLS networks as an alternative connection option to the SDH/PDH technology.

A05 (relates to aFRR): Connection to a TSO with more than 50 MW in the LFR zone:



C03 (relates to aFRR): Connection of technical units ≥ 50 MW:


Anbieter
Carrier
Anbieter
Technische Einheit
knoten- & kantendisjunkte Punkt-zu-Punkt Verbindung
xDSL, SVF, DDV, SDH, Carrier Ethernet, MPLS
Medienbruch
CE
PE
PE
CE
Medienbruch
Anbeiter Leitsystem
VPN Terminierung
Closed User Group
VPN Terminierung
Ethernet-Seriell Konverter
CE
PE
PE
CE
Medienbruch
Anbeiter Leitsystem
VPN Terminierung
xDSL, SVF, DDV, SDH, Carrier Ethernet, MPLS oder Mobilfunk
VPN Terminierung
Ethernet-Seriell Konverter
VPN End-zu-End Verschlüsselung

This requires a redundant Customer Edge (CE) connection with two dedicated lines to various Provider Edge (PE) routers to achieve a higher availability and additionally with the option of increasing the bandwidth with two CE routers.
The path routing between the PE and CE router must be completely node and edge disconnected. A provider (with appropriate redundancy) can also be used for the MPLS backbone if corresponding SLAs are in place.

Cross-connections (with failover) can be used between the CE routers and between the VPN gateways to increase availability.

The fixed-line connection between CE and PE should not be established based on ADSL technology or in a “shared medium” with other public participants (no public IP addresses, closed user group).

For a risk-oriented consideration of the risks and security measures on the provider side, refer to the short study of the BSI on dangers and measures when using MPLS [13]. But, the use of a VPN connection adequately compensates most risks mentioned.

6 List of references

[1] Federal Office for Information Security (BSI), Technical Guideline TR-02102-1, Cryptographic methods: recommendations and key lengths, Part 1 2014.

[2] Federal Office for Information Security (BSI), Technical Guideline 02102-2, Cryptographic methods: recommendations and key lengths, part 2 - Use of transport layer security (TLS), version 2014.

[3] Federal Office for Information Security (BSI), Technical Guideline 02102-3, Cryptographic methods: recommendations and key lengths, Part 3 - Use of IPsec, version 2014.

[4] Federal Office for Information Security (BSI), IT Basic Protection Catalogue: secure connection to an external network with IPSec, 13th supplement, 2013.

[5] European Union Agency for Network and Information Security Agency (ENISA), Algorithms, Key Sizes and Parameters Report, Version 1.0, October 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, July 2012.

[7] BetterCrypto.org, Applied Crypto Hardening, https://bettercrypto.org/static/applied-crypto-harde-ning.pdf, last accessed on 8 May 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, last accessed on 8 May 2014.

[11] Federal Office for Information Security (BSI), Technical Guideline: Cryptographic methods: recommendations and key lengths, BSI TR-02102-1, version 2015-01, 10 February 2015

[12] BDEW - Whitepaper “Requirements for Secure Control and Telecommunication Systems”

[13] Federal Office for Information Security (BSI), Short study on dangers and measures when using MPLS, version 1.5, 2009