Bundesamt für Sozialversicherungen

Weisungen für den Anschluss der AHV-Ausgleichskassen und IV-Stellen ans AHV/IV-Netz (WAN)

Gültig ab 1. Juli 2006

Stand: 1. Januar 2016

318.106.05 d WAN

01.16

Vorwort

Aufgrund des gesetzlichen Auftrags (nach Art. 176, Abs. 4 AHVV) sorgt das Bundesamt für Sozialversicherungen (BSV) u.a. für einen zweckmässigen Einsatz der technischen Einrichtungen zwischen den einzelnen Durchführungsstellen AHV/IV, der Zentralen Ausgleichsstelle (ZAS) sowie anderen, mit der Durchführung betrauten Institutionen.

Infolge der immer weiter ausgebauten Nutzung der Informations- und Kommunikationstechnologie bei den AHV/IV-Durchführungsstellen und aufgrund der in die Jahre gekommenen verschiedenen Telekommunikationsnetze sowie des Datennetzes der Ausgleichskassen und IV-Stellen TELEZAS 2, über welches sämtliche Informationen (MZR-Verfahren, Abfragen Versicherten-/Rentenregister, Intranet-Anschluss, IK-Übermittlungen/Eintragungen) erfolgen, wurde beschlossen, ein gemeinsames Datennetz für die Durchführungsorgane der 1. Säule aufzubauen.
Dieses Datennetz verbindet die AHV/IV-Durchführungsstellen untereinander und zu den zentralen Rechenzentren bzw. zu weiteren Datenquellen und Netzwerken.

Das AHV/IV-Netz erfüllt zudem alle Anforderungen an die Datensicherheit, erleichtert die elektronische Kommunikation und steht für künftige Entwicklungen offen.

Vorwort zum Nachtrag 1, gültig ab 1. Januar 2016

Die vorgeschlagenen Anpassungen verfolgen das Ziel den Sonderfall der Heimarbeit zu klären mit Rz 3010.

Die veralteten Anhänge 3 und 4 werden gestrichen. Die Randziffern 3004, 3005, 3006, 4018, 4019 und 4020 sind dementsprechend angepasst.

Das Antragsformular befindet sich unter:
www.bsv.admin.ch > Praxis > Vollzug > eGov > Formulare.

Inhaltsverzeichnis

Abkürzungen

AHV	Alters- und Hinterlassenenversicherung
AHVV	Verordnung über die AHV
AK	AHV-Ausgleichskasse
BSV	Bundesamt für Sozialversicherungen
BIT	Bundesamt für Informatik und Telekommunikation
IRB	Informatikrat Bund
IVS	IV-Stelle
KBI	Koordinations- und Bewilligungsinstanz
RZ	Rechenzentrum
SAP	Service Access Point
SLA	Service Level Agreement
VPN	Virtual Private Network
WIsB	Weisung des BR über die Informatiksicherheit in der Bundesverwaltung

Kapitel I

1. Allgemeines

1001 Die nachstehenden Weisungen regeln die Rahmenbedingungen für den Anschluss der AHV/IV-Durchführungsstellen und weiteren von den Durchführungsstellen bezeichneten Dritten ans AHV/IV-Netz aufgrund der in Rz 2001 bezeichneten Grundlage.

2. Geltungsbereich und Grundlage

2001 Grundlage dieser Weisung bildet Artikel 176 Absatz 4 der Verordnung über die Alters- und Hinterlassenenversicherung (AHVV).

Kapitel II

3. AHV/IV-Netz

3.1 Zweck

3001 Das AHV/IV-Netz besteht aus mehreren logischen Datennetzen, die auf der Übertragungsinfrastruktur der Bundesverwaltung aufsetzen. Es verbindet die Durchführungsorgane der AHV/IV untereinander und stellt den Zugang zu den zentralen Anwendungen der ZAS (u.a. Zentrale Register) sicher. Es erleichtert die Kommunikation der verschiedenen angeschlossenen Institutionen und steht für künftige Entwicklungen zur Verfügung.
Die Betriebskosten für die Grundleistungen werden durch die Versicherungen getragen.

3.2 Leistungsumfang

3002 Der Leistungsumfang des AHV/IV-Netzes ist wie folgt festgelegt:

- Verschiedene logische Netze auf Basis der Übertragungsinfrastruktur der Bundesverwaltung.
- Zentrale Firewall-Infrastruktur, welche die logischen Netzwerke des AHV/IV-Netzes untereinander sowie gegenüber weiteren Netzen der Bundesverwaltung und daran angeschlossenen Netzen abgrenzt.
- Zentraler Internetaccess und Anschluss an den Mailgateway der Bundesverwaltung inkl. standardisiertem Mailware- und Spamfilter.

3.3 Anschlussregelungen

3003 Im Zusammenhang mit dem Anschluss von Standorten der Netzbenutzer (Definition Rz 4015ff) ans AHV/IV-Netz gelten Regelungen für:

- den Anschluss von AHV/IV-Durchführungsstellen (Rz 3004);
- den Anschluss von Rechenzentren (Rz 3005);
- den Anschluss von Dritten (Partner der AHV/IV-Durchführungsstellen – Rz 3006);
- den Service Access Point AHV/IV-Netz (Rz 3007);
- die Verwendung des zentralen Internetaccesses und dem Mailgateway (Rz 3008).

3004 1/16 AHV/IV-Durchführungsstellen werden grundsätzlich mit einem einfachen Anschluss und einer Grundleistung gemäss BSV am AHV/IV-Netz angeschlossen.
Benötigt eine AHV/IV-Durchführungsstelle mehr als einen Anschluss kann dies gemäss Rz 3009 in Ausnahmefällen genehmigt werden.
Andere Anschlussvarianten (bspw. Höherer Service Level aufgrund sehr hoher Benutzerzahl am Standort) können

gemäss Rz 3009 in Ausnahmefällen bewilligt werden.

3005 1/16 Rechenzentren, Backupzentren und Druckzentren, die Informatikanwendungen und Daten zugunsten von AHV/IV-Durchführungsstellen in ihren eigenen Räumlichkeiten betreiben und verwalten, werden auf Antrag beim BSV am AHV/IV-Netz angeschlossen.
Die AHV/IV-Stellen bezeichnen die Rechenzentren, die als solche am AHV/IV-Netz anzuschliessen sind. Die Anzahl der Anschlüsse richtet sich nach den Bedürfnissen der AHV/IV-Durchführungsstellen.
Der Anschluss von Rechenzentren muss gemäss Rz 3009 bewilligt werden.

3006 1/16 Der Anschluss von Dritten am AHV/IV-Netz ist grundsätzlich unter den nachgenannten Kriterien möglich:
Der Anschluss von Dritten ans AHV/IV-Netz ist gemäss Rz 3009 grundsätzlich bewilligungspflichtig.
Kriterien für den Anschluss von Dritten ans AHV/IV-Netz sind:

- Der Dritte erbringt eine Dienstleistung zugunsten einer oder mehrer AHV/IV-Durchführungsstelle(n), die nur mit einem Anschluss am AHV/IV-Netz wirtschaftlich durchführbar ist und die einen engen Zusammenhang mit dem AHV/IV-Vollzug hat.
- Der Dritte liefert resp. bezieht Daten im Rahmen des AHV/IV-Vollzugs an eine oder mehrere AHV/IV-Durchführungsstellen, die ohne einen Direktanschluss des Dritten am AHV/IV-Netz nicht wirtschaftlich ausgetauscht werden könnten.

3007 Der Anschlusspunkt ans AHV/IV-Netz liegt grundsätzlich in den Räumlichkeiten des Netzbenutzers. Als Service Access Point (SAP) wird dabei die LAN-Schnittstelle des/der Anschlussgeräte(s) (Router) am Standort verstanden.
Der Verantwortungsbereich des Netzanbieters endet am Service Access Point.

3008 Am AHV/IV-Netz angeschlossene Netzbenutzer verwenden grundsätzlich den zentralen Internetaccess und den Mailgateway der Bundesverwaltung.
Ausnahmen können in begründeten Fällen durch die Koordinations- und Bewilligungsinstanz (Rz 5001ff) genehmigt werden.

3009 Änderungen bezüglich den Netzleistungen, insbesondere im Bereich der Bandbreite, aber auch im Zusammenhang mit den im Anhang 2 (Teilbereich „Bewilligung“) beschriebenen Leistungen müssen mittels Bewilligungsverfahren (KBI) beantragt und genehmigt werden.

3010 1/16 Für den Sonderfall Heimarbeit im Inland, müssen folgende Dokumente zusammengestellt und auf Anfrage den Revisoren oder Auditoren zur Verfügung gestellt werden:

- Internes Reglement über Heimarbeit
- Weisungen oder Policy über die sichere Benutzung der Daten ausserhalb des Arbeitsortes mit der technischen Darstellung der Komponenten, die Heimarbeit ermöglichen.

Kapitel III

4. Definition und Begriffsbestimmungen

4.1 Organisation und Struktur

4001 Organisationsstruktur des AHV/IV-Netzes ist wie folgt aufgebaut:

- Netzbetreiber
- Netzanbieter
- Netzbenutzer

Der Netzanbieter ist zudem gleichzeitig Koordinations- und Bewilligungsinstanz (KBI) gemäss Rz 5001.

4.2 Netzbetreiber

4.2.1 Definition und Begriffsbestimmung

4002 Das Bundesamt für Informatik und Telekommunikation (BIT) betreibt im Auftrag des Bundesamtes für Sozialversicherungen (BSV) das AHV/IV-Netz. Das BIT ist damit Betreiber des AHV/IV-Netzes.

4.2.2 Anforderungen und Aufgaben

4003 Der Netzbetreiber erbringt die in Rz 3002 aufgeführten Telekommunikationsleistungen zugunsten der Netzbenutzer.

4004 Der Netzbetreiber stellt den Betrieb des AHV/IV-Netzes bis und mit dem Anschlusspunkt (SAP) beim Netzbenutzer gem. Rz 3007 mittels wirkungsvollem Netzwerk-Management sicher.

4005 Bandbreitenerhöhungen werden auf Antrag der Netzbenutzer vom Netzanbieter genehmigt und vom Netzbetreiber umgesetzt. Der Netzbetreiber sorgt dabei für eine rasche Umsetzung der Leistungserhöhung.

4006 Der Netzbetreiber ist innerhalb dem AHV/IV-Netz zuständig für die Einhaltung der in Rz 6002 genannten Weisungen im Bereich Datensicherheit.

4007 Der Netzbetreiber stellt den Durchführungsorganen einen Supportdienst zur Verfügung und betreibt ein zentrales Helpdesk.

4.3 Netzanbieter

4.3.1 Definition und Begriffsbestimmung

4008 Aufgrund des gesetzlichen Auftrags (nach Art. 176, Abs. 4 AHVV) sorgt das Bundesamt für Sozialversicherungen (BSV) u.a. für einen zweckmässigen Einsatz der technischen Einrichtungen für die diversen Kontakte zwischen den einzelnen Durchführungsstellen AHV/IV, der Zentralen Ausgleichsstelle (ZAS) sowie anderen, mit der Durchführung betrauten Institutionen.

4009 Das BSV vertritt die AHV/IV als Netzanbieter und ist in dieser Funktion Koordinations- und Bewilligungsinstanz (KBI) für Neuanschlüsse sowie kosten- und sicherheitsrelevante Aspekte. Die Details im Bereich KBI werden im Anhang 2 erläutert.

4010 Der Netzanbieter ist Vertragspartner des BIT als Netzbetreiber im Rahmen des Service Level Agreement AHV/IV-Netz und der Kostenübernahmevereinbarung.

4011 Der Netzanbieter ist Eigentümer der Domänenpolicy AHV/IV-Netz (vgl. Anhang 1) und damit verantwortlich für deren Durchsetzung bei den Netzbenutzern und dem Netzbetreiber.

4.3.2 Anforderungen und Aufgaben

4012 Der Netzanbieter ist verantwortlich für die Durchsetzung der vorliegenden Weisungen bei den Netzbenutzern und dem Netzbetreiber.

4013 Der Netzanbieter schliesst mit dem Netzbetreiber ein Service Level Agreement für das AHV/IV-Netz ab, in dem die Leistungen des Netzbetreibers, die gegenseitigen Pflichten und Rechte sowie die Kosten geregelt sind.

4014 Als Netzanbieter vertritt das BSV die Anliegen der Netzbenutzer gegenüber dem Netzbetreiber.

4.4 Netzbenutzer

4.4.1 Definition und Begriffsbestimmung

4015 Grundsätzlich ist jede am AHV/IV-Netz angeschlossene Stelle ein Netzbenutzer. Gemäss Rz 3003 werden dabei die folgenden Netzbenutzer unterschieden:

- AHV/IV-Durchführungsstellen (AHV-Ausgleichskassen und IV-Stellen)
- Rechenzentren
- Dritte (Partner der AHV/IV-Durchführungsstellen)

4016 AHV/IV-Durchführungsstellen können in einer Poolorganisation zusammengeschlossen sein. In diesem Fall delegieren diese Durchführungsstellen ihre Rechte und Pflichten als Netzbenutzer an die Poolorganisation. Die Poolorganisation ist dann stellvertretend für ihre Mitglieder für die Einhaltung der geltenden Weisungen AHV/IV-Netz verantwortlich.

4.4.2 Anforderungen und Aufgaben

4017 Die Netzbenutzer sind verantwortlich für den Schutz Ihrer Daten. Sie haben diese mittels geeigneter Massnahmen zu schützen. Darin eingeschlossen sind auch Daten bei Rechenzentren (RZ). In diesem Zusammenhang verweisen wir auf Rz 6001ff.

4018 1/16 Jeder Netzbenutzer stellt pro Standort eine Ansprechstelle, welche im Störungsfall telefonisch Auskunft geben kann. Diese muss zudem in der Lage sein unter Anleitung einfache Handgriffe (an Router und Modem) auszuführen.
Die Erreichbarkeit der Ansprechstelle muss während den

Servicezeiten gewährleistet sein.
Die Netzbenutzer bezeichnen zudem eine Stelle (Helpdesk, Superuser), die im Normalfall für Störungsmeldungen usw. zuhanden des Call Centers des Netzbetreibers zuständig ist.

4019 1/16 Der Netzbenutzer ist für den Schutz vor unerlaubten Zugriffen oder Manipulationen an der Infrastruktur des Netzbetreibers (BIT) verantwortlich. Zudem ist er dafür verantwortlich, dass die Gerätschaften des Netzbetreibers in angemessenen Räumen mit den vorgegebenen Rahmenbedingungen platziert sind. Die Anforderungen an den Standort folgende:
Die Räumlichkeiten für den Netzanschluss AHV/IV-Netz müssen abschliessbar sein und dürfen sich nicht in einer Kundenzone befinden.

Der Zugang zu den Netzanschlussgeräten darf nur für die dazu berechtigten Personen möglich sein (z.B. Begleitung des Servicepersonals durch Netzbenutzer, manuelle Eingriffe an Netzkomponenten nur unter Anleitung des Netzbetreibers, usw.)

4020 1/16 Der Netzbenutzer stellt den Zutritt zum Standort, der bei einer allfälligen Störungsmeldung vor Ort nötig ist, während den Servicezeiten wie folgt sicher:

- Standorte mit Service Level ‚Kritisch' während den Bürozeiten (Mo–Fr zwischen 07.30 bis 17.00 Uhr);
- Standorte mit Service Level ‚Hochverfügbar' während 7 x 24h.

4021 IT-Sicherheitsverantwortlicher Netzbenutzer

- Jeder Netzbenutzer definiert einen IT-Sicherheitsverantwortlichen.
- Dieser ist verantwortlich für die Erstellung und Pflege der Domänenpolicy des Netzbenutzers.
- Er teilt dem Netzbetreiber die berechtigten IP-Subnetzadressen für „einfache Anschlüsse" mit.
- Er definiert die Regeln in der Firewall-Policy für zentrale

Netzübergänge, welche den Netzbenutzer betreffen.
- Er ist Ansprechstelle für den Netzbetreiber und den Netzanbieter bei sicherheitsrelevanten Vorkommnissen.

Die Rolle des IT-Sicherheitsverantwortlichen kann von einer AK/IVS einer Poolorganisation übertragen werden.

Kapitel IV

5. Koordinations- und Bewilligungsinstanz (KBI)

5.1 Grundlagen

5001 Die Koordinations- und Bewilligungsinstanz (KBI) wird durch das BSV wahrgenommen und übernimmt die Funktion der Verbindungsstelle des Netzanbieters zum Netzbetreiber. In dieser Funktion ist sie zuständig für konkrete operative Fragestellungen der Netzbenutzer im Zusammenhang mit dem AHV/IV-Netz.

5002 Die KBI ist zuständig für folgende Aufgaben und Teilbereiche:
- Koordination
- Bewilligung
- Planung und Steuerung
- Kontrolle
- Steuerung Service Level Agreement
- Security-Management Ombudsstelle
- Administration

5.2 Aufgaben

5003 In Anhang 2 werden die obenerwähnten Aufgaben im Detail erläutert.

Kapitel V

6. Sicherheitsanforderungen und Datenschutzauflagen

6.1 Prinzipien zu Datenschutz und Datensicherheit

6001 Grundlagen für die Netzwerksicherheit bilden die Weisung des BR über die Informatiksicherheit in der Bundesverwaltung sowie die Domänenpolicy AHV/IV-Netz.

6002 Bezüglich Datenschutz und Datensicherheit gelten folgende Grundsätze:

- Die ans AHV/IV-Netz angeschlossenen Durchführungsorgane sind für die strikte Einhaltung von Datenschutz und Datensicherheit verantwortlich. Sie haben ihre Daten mittels geeigneter Massnahmen zu schützen.
- Darin eingeschlossen sind auch die Rechenzentren (RZ), bei denen die Ausgleichskassen und IV-Stellen ggf. ihre Daten gespeichert haben.
- Die Daten werden während der Übertragung über das AHV/IV-Netz verschlüsselt. Anfangs- resp. Endpunkt der Verschlüsselung ist dabei jeweils der Service Access Point AHV/IV-Netz gemäss Rz 3007.
- Die Zentrale Ausgleichsstelle (ZAS) untersteht den Sicherheitsbestimmungen der Bundesverwaltung. Sie bleibt weiterhin für den Schutz der zentralen Register verantwortlich.

6003 Prinzipien für den Anschluss von Drittnetzen:

- Anschlüsse von Dritten erfolgen in erster Linie über das AHV/IV-Netz. Dieses stellt eine einfache Zugangskontrolle sicher.
- Anhang 1, Abs. 4.2.4 nennt Bedingungen, unter denen Dritte (Fremddomänen) direkt bei einer Durchführungsstelle oder einem Rechenzentrum (Partnerdomänen) angeschlossen werden können.

6004 Domänenpolicy angeschlossener Stellen
- Jede AK/IVS definiert für ihre Systeme und Daten eine eigene Domänenpolicy gemäss den Vorgaben in Anhang 1, Abs. 2.4.

6.2 Massnahmen bei Nichteinhaltung

6005 Stellt der Netzbetreiber (BIT) Mängel resp. Vorfälle in Datensicherheit und Datenschutz fest, spricht er mit dem Netzanbieter (BSV) geeignete Massnahmen ab.

6006 Der Netzbetreiber kann sofort, ohne vorgängige Absprache mit dem Netzanbieter, bestimmte Massnahmen (z.B. Sperrung eines Netz-Zuganges (SAP) ergreifen, wenn er dies zur Sicherstellung der Netzwerksicherheit als notwendig erachtet.

6007 Eine solche Massnahme ist u.a. gerechtfertigt, wenn es sich beim Vorfall um die Verletzung der Domänenpolicy AHV/IV-Netz handelt oder ein Ereignis eingetroffen ist, welches das gesamte AHV/IV-Netz beeinträchtigt.

Kapitel VI

7. Inkrafttreten

7001 Diese Weisungen treten auf den 1. Juli 2006 in Kraft.

Anhang 1

Bundesamt für Informatik und Telekommunikation BIT
Office fédéral de l'informatique et de la télécommunication OFIT
Ufficio federale dell'informatica e della telecomunicazione UFIT
Uffizi federal d'informatica e telecommunicaziun UFIT

BSV / OFAS / UFAS /

AHV/IV-Netz

Domänenpolicy

Stand: 1. Juli 2006

Inhaltsverzeichnis

1 Allgemeines

1.1 Grundlagen

A. Weisung für den Anschluss der AHV-Ausgleichskassen und IV-Stellen ans AHV/IV-Netz (WAN)
B. Weisung des BR über die Informatiksicherheit in der Bundesverwaltung (WIsB) inkl. deren Anhänge 1 (Minimale Sicherheitsanforderungen und Verantwortlichkeiten für den generellen Schutzbedarf) und 2 (Definition und Sicherheitsvorgaben für die Netzwerksicherheit).

1.2 Fokus der Domänenpolicy AHV/IV-Netz

Die minimalen Sicherheitsanforderungen in der WIsB beziehen sich auf:

- Organisation der Sicherheit
- Umgang mit Informationen und Daten
- Physische Sicherheit
- Netzwerk- und Systemmanagement
- Zugriffskontrolle
- Systementwicklung und Unterhalt
- Umgang mit Störungen und Notfällen

Die Domänenpolicy AHV/IV-Netz baut auf diesen Grundlagen auf und definiert die darüber hinausgehenden Sicherheitsanforderungen, die sich im Speziellen auf das AHV/IV-Netz beziehen.

1.3 Prinzipien zu Datenschutz und Datensicherheit

Die im AHV/IV-Netz geltenden Prinzipien zu Datenschutz und Datensicherheit sind in der WAN festgelegt (vgl. Kapitel V, Abs. 6.1).

2 Domänenmodell

2.1 Domänenmodell

In der vorliegenden Domänenpolicy werden die folgenden Domänen unterschieden:

- Domäne AHV/IV-Netz
- Partnerdomänen
- Fremddomänen

Die Domänen sind mit Netzübergängen miteinander verbunden.

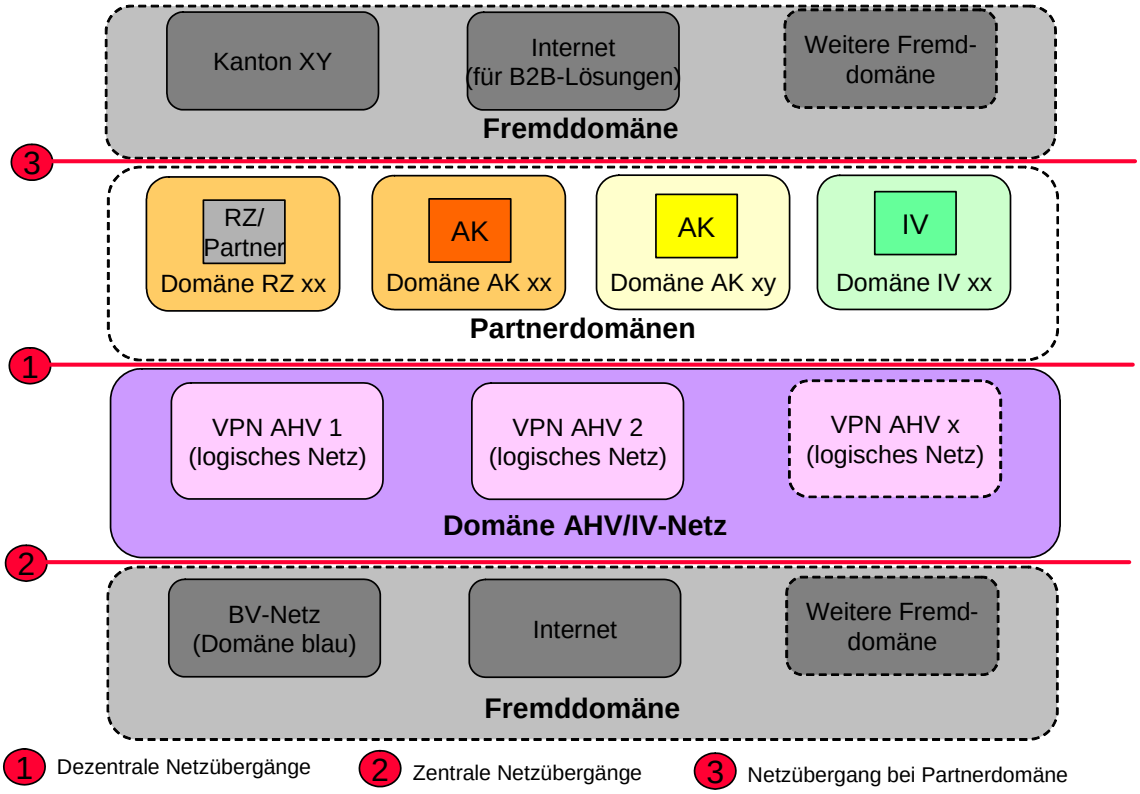


Abbildung 1: Domänenmodell AHV/IV-Netz

2.2 Domäne AHV/IV-Netz

Beschreibung

- Die Domäne AHV/IV-Netz ist das gemeinsame Netz, an dem alle Durchführungsorgane der AHV/IV, deren Rechenzentren sowie Dritte (Partner der AHV/IV-Durchführungsorgane) angeschlossen sind.
- Das AHV/IV-Netz ist, ähnlich dem KOMBV-KTV[1], ein reines Transportnetzwerk.
- Das AHV/IV-Netz besteht aus mehreren logischen Netzen und verwendet die Übertragungsinfrastruktur des Carriernetzes Bund.

Domänengrenze

- Die Domänengrenze liegt beim Service-Access-Point des AHV/IV-Netzes (vgl. WAN Rz 3007).
- Die zentralen und dezentralen Netzübergänge sind Teilbereiche der Domäne AHV/IV-Netz.
- Die lokalen Netze (LAN) sowie Systeme der AK/IVS, deren Rechenzentren und Partner befinden sich ausserhalb der Domäne AHV/IV-Netz. Sie sind mit Netzübergängen mit dieser verbunden.
- Die Systeme der ZAS befinden sich ausserhalb der Domäne AHV/IV-Netz[2]. Der Zugriff aus dem AHV/IV-Netz geschieht über einen Netzübergang.

Anforderungen an Systeme in der Domäne AHV/IV-Netz

- Die Domäne AHV/IV-Netz dient ausschliesslich dem Datentransport und beinhaltet keine Systeme im Sinne der WIsB.
- Es sind daher keine Anforderungen an Systeme notwendig.

Domäneninhaber

- Inhaber der Domäne AHV/IV-Netz ist das Bundesamt für Sozialversicherungen (BSV).

---

[1] Kommunikationsnetz, welches sämtliche Kantone der Schweiz untereinander und mit den Stellen des Bundes verbindet. Das KOMBV-KTV wird wie das AHV/IV-Netz auf Basis des Carriernetz Bund betrieben.

[2] Sie befinden sich in der sog. „Domäne blau“ der Bundesverwaltung.

2.3 Weitere Domänen

Partnerdomänen

Als Partnerdomänen der Domäne AHV/IV-Netz gelten (abschliessende Aufzählung):

- Durchführungsorgane der AHV/IV (Ausgleichskassen oder IV-Stellen)
- Rechenzentrum, welches Anwendungen oder Systeme für ein Durchführungsorgan betreibt.
- Partner eines Durchführungsorgans, der Entwicklungs- oder Supportaufgaben im IT-Bereich zu Gunsten der AHV/IV erbringt.

Eine Partnerdomäne ist immer direkt und ohne dazwischen liegende Domäne mit dem AHV/IV-Netz verbunden.

Fremddomänen

- Als Fremddomänen werden alle fremden Netze bezeichnet, die entweder über die zentralen Netzübergänge der Domäne AHV/IV-Netz erreicht werden können oder die mit einem Netzübergang mit einer Partnerdomäne verbunden sind.
- Beispiele sind (nicht abschliessend):
  a. BV-Netz (Netz der Bundesverwaltung)
  b. Kantonsnetz
  c. Internet

2.4 Anforderungen an Partnerdomänen

Eigene Domänenpolicy

- Jede Partnerdomäne definiert für ihre Systeme und Daten eine eigene Domänenpolicy[3], welche den Anforderungen der WIsB genügt.

[3] Mit Domänenpolicy ist eigentlich ein IT-Sicherheitskonzept gemeint, das im Minimum die in WIsB verlangten Punkte regelt.

Vereinfachung für Poolmitglieder

- Durchführungsorgane der AHV/IV, die in einem Pool zusammengeschlossen sind, können eine gemeinsame Domänenpolicy für die Poolmitglieder definieren.

Einbindung von Rechenzentren und Dritten

- Rechenzentren und Dritte (Partner der AHV/IV-Durchführungsorgane) sind in die Domänenpolicy eines Durchführungsorgans resp. einer Poolorganisation einzubinden, sofern sie über einen Anschluss am AHV/IV-Netz verfügen.

3 Schutzbedarf

3.1 Schutzbedarf der Domäne AHV/IV-Netz

Der Schutzbedarf der Domäne AHV/IV-Netz teilt sich in die folgenden Bereiche auf:

- Vertraulichkeit der übertragenen Daten
- Integrität der übertragenen Daten
- Zugangskontrolle zur Domäne AHV/IV-Netz
- Verfügbarkeit AHV/IV-Netz

Vertraulichkeit der übertragenen Daten

- Die Daten sind während der Übertragung über das AHV/IV-Netz mit kryptografischen Verfahren zu verschlüsseln. Anfangs- resp. Endpunkt der Verschlüsselung ist dabei der Service Access Point AHV/IV-Netz (vgl. WAN Rz 6002).

Integrität der übertragenen Daten

- Die Integrität der Daten ist während der Übertragung über das AHV/IV-Netz mittels kryptografischen Hashfunktionen sicherzustellen. Anfangs- resp. Endpunkt ist dabei wie bei der Verschlüsselung der Service Access Point AHV/IV-Netz.

Zugangskontrolle zur Domäne AHV/IV-Netz

- Das AHV/IV-Netz bietet den angeschlossenen Stellen einen Grundschutz, indem nur vom BSV bewilligte Netzübergänge zugelassen werden.
- An dezentralen und zentralen Netzübergängen ist der Zugang zum Netz auf Basis von berechtigten IP-Adressen zu

beschränken.

- Es findet keine Authentifikation von Benutzern an der Domänengrenze AHV/IV-Netz statt.

Verfügbarkeit AHV/IV-Netz

- Die Verfügbarkeit des AHV/IV-Netzes wird ausserhalb der Domänenpolicy AHV/IV-Netz im Service-Level-Agreement (SLA) AHV/IV-Netz beschrieben. Das SLA ist Teil des Vertrags zwischen dem Netzanbieter BSV und dem Netzbetreiber BIT.

3.2 Schutzbedarf von Partnerdomänen

Der Schutzbedarf von Partnerdomänen wird grundsätzlich von diesen festgelegt, wobei die Anforderungen an Partnerdomänen gem. Kapitel beachtet werden müssen.

Empfehlung:

- *Am AHV/IV-Netz angeschlossenen Partnerdomänen wird empfohlen, individuelle zusätzliche Schutzmassnahmen für den Schutz der eigenen Daten vor Viren, Hacking usw. zu treffen.*

4 Netzübergänge

4.1 Netzübergangstypen

4.1.1 Einfacher Anschluss

Eigenschaften

- Paketfilter
- Autorisierung einer Kommunikation aufgrund IP Quell- und Zieladressen
- Physisch meist ein Router

Regeln für einen einfachen Anschluss

- Partnerdomäne in Richtung AHV/IV-Netz (eingehend): Grundsätzlich geöffnet ist die Kommunikation für berechtigte IP-Subnetzadressen einer Partnerdomäne mit den

Zieladressen der zentralen Register.
- Weitere Kommunikationsverbindungen werden nach vorgängiger Genehmigung vom Netzbetreiber für berechtigte IP-Subnetzadressen geöffnet.

Verzeichnis berechtigter IP-Subnetzadressen
- Der Netzbetreiber führt für jeden einfachen Anschluss ein Verzeichnis der berechtigten IP-Subnetzadressen.

4.1.2 Stateful-Firewall

Eigenschaften
- Autorisierung einer Kommunikation aufgrund IP Quell- und Zieladresse und TCP/UDP-Portadresse sowie im Kontext früherer Pakete (Stateful-Firewall).
- Physisch eine Firewall

Regeln für eine Stateful-Firewall
- AHV/IV-Netz in Richtung Fremddomäne (ausgehend): Grundsätzlich geöffnet ist die Kommunikation für berechtigte IP-Subnetzadressen einer Partnerdomäne mit den Zieladressen der zentralen Register.
- Weitere Kommunikationsverbindungen werden in einer Firewall-Policy definiert.

Firewall-Policy
- Für jede Firewall ist eine Firewall-Policy und ein Betriebskonzept erforderlich, welche mindestens die in WIsB geforderten Punkte beschreiben.
- Verantwortlich für die Erstellung der Policy und des Betriebskonzeptes ist der Netzbetreiber (resp. Firewallbetreiber).

4.2 Netzübergänge im AHV/IV-Netz

4.2.1 Überblick

Ein Netzübergang verbindet zwei Netze so, dass eine Kommunikation (= zeitlich begrenzter Austausch von Datenpaketen) zwischen den beiden Netzen möglich ist.
Das AHV/IV-Netz unterscheidet dabei:

- Dezentrale Netzübergänge
- Zentrale Netzübergänge
- Netzübergang bei Partnerdomäne

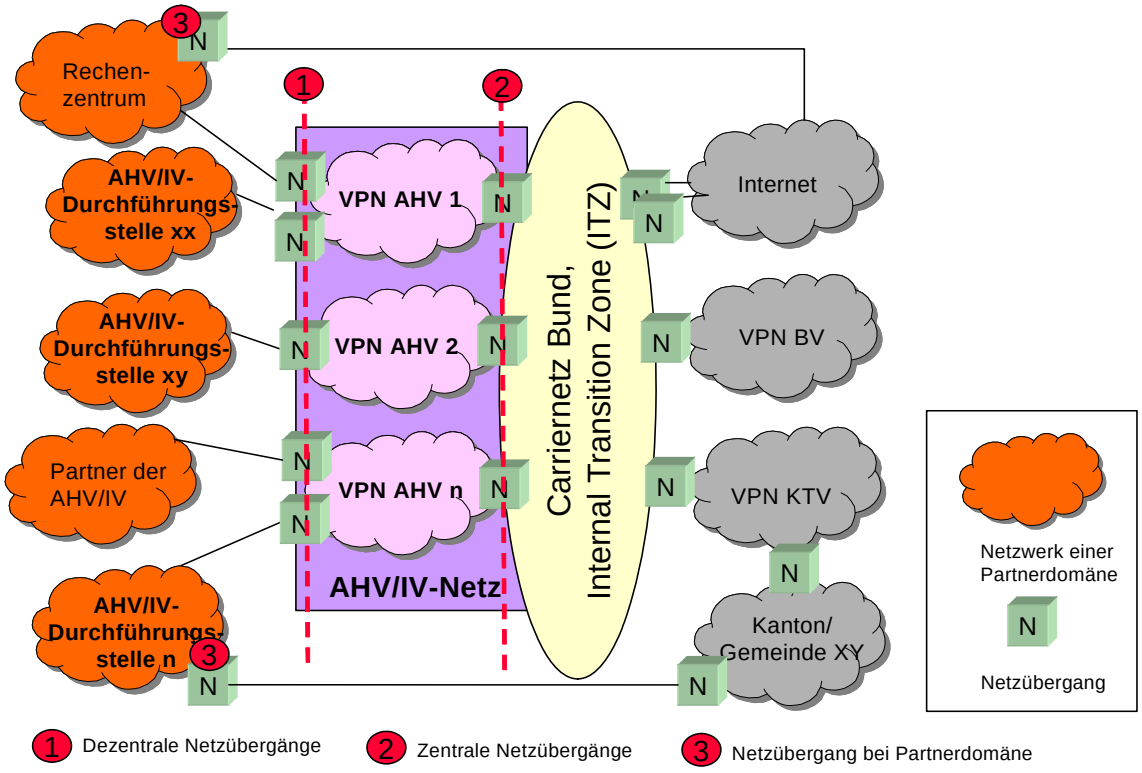


Abbildung 2: Netzübergänge AHV/IV-Netz (Beispiele physische Sicht)

4.2.2 Dezentrale Netzübergänge

Dezentrale Netzübergänge werden im Normalfall mit einem „einfachen Anschluss“ ausgeführt. Dazu müssen folgende

Bedingungen erfüllt sein:

- Bei der anzuschliessenden Stelle handelt es sich um eine Partnerdomäne. Als solche verfügt sie über eine eigene Domänenpolicy, welche den Vorgaben der WIsB genügt.
- Das Bundesamt für Sozialversicherungen hat den Anschluss genehmigt.
- Falls die Partnerdomäne einen eigenen Netzübergang zu einer Fremddomäne betreibt, erfüllt sie die minimalen Anforderungen für den Betrieb solcher Netzübergänge gemäss der vorliegenden Domänenpolicy (vgl. Kap.4.2.4).

4.2.3 Zentrale Netzübergänge

Jedes logische Netz der Domäne AHV/IV-Netz verfügt über einen zentralen Netzübergang. Dieser verbindet das logische Netz mit der sog. „Internal Transition Zone“ des Carriernetzes Bund.
Zentrale Netzübergänge werden immer mit einer Stateful-Firewall ausgeführt.
Über die zentralen Netzübergänge können die folgenden Netze erreicht werden (nicht abschliessende Aufzählung):

- Weitere logische Netze der Domäne AHV/IV-Netz
- Zugang zu den zentralen Registern der ZAS im Netz der Bundesverwaltung
- Zugang zum Internet über den Internetaccess der Bundesverwaltung
- Zugang zu kantonalen Netzen via KOMBV-KTV

4.2.4 Netzübergang bei Partnerdomäne

Minimale Anforderungen
Partnerdomänen können unter folgenden Bedingungen einen eigenen Netzübergang zu einer Fremddomäne betreiben:

- Der Netzübergang zur Fremddomäne ist dem BSV bekannt und von diesem genehmigt.

- Die Domänenpolicy der Partnerdomäne ist vom BSV genehmigt und entspricht den Vorgaben der WIsB.
- Der Netzübergang zur Fremddomäne ist in der Domänenpolicy der Partnerdomäne beschrieben.
- Die Partnerdomäne sorgt für eine effektive Zugangskontrolle am Netzübergang zur Fremddomäne.
- Ein Netzübergang ans Internet wird nur in Ausnahmefällen erlaubt und muss ebenfalls vom BSV genehmigt werden.
- Das BSV kann jederzeit ein Sicherheits-Audit bei der Partnerdomäne durchführen resp. von Dritten durchführen lassen, welches auch den Netzübergang zur Fremddomäne mit einschliesst.

Beispiele für Netzübergänge bei Partnerdomänen

- Netzübergang zu einem kantonalen Netzwerk
- Netzübergang zum Internet bei einem Rechenzentrum, welches B2B-Anwendungen für ein Durchführungsorgan betreibt.
- Netzübergang zu einem eigenen Wide-Area-Netzwerk (WAN) einer Ausgleichskasse, welches mehrere Zweigstellen dieser Ausgleichskasse miteinander verbindet.
- Netzübergang zu einer Stelle des Regionalärztlichen Dienstes (RAD).

4.3 Spezielle Netzübergänge

4.3.1 AK als Teil einer Firma/eines Verbandes

Einige Ausgleichkassen sind netzwerktechnisch vollständig in eine Firma oder einen Verband integriert. Beispiele dafür sind die AK Coop und Migros.
Am Netzübergang zur Domäne AHV/IV-Netz wird damit eigentlich das Netzwerk einer Firma oder eines Verbandes angeschlossen. Die AK ist lediglich ein Teil innerhalb dieses Netzwerkes.
Partnerdomäne ist lediglich der Netzwerkteil der Ausgleichs-

kasse.

Netzübergang

Aus folgenden Gründen wird ein solcher Netzübergang bis auf weiteres dezentral mit einem „einfachen Anschluss“ realisiert:

- Diese Anschlussart wurde im Vorgänger des AHV/IV-Netzes (TeleZas-Netz) ebenfalls toleriert.
- Es wird dieselbe Anschlussart wie bei einer Partnerdomäne verwendet, um dieselbe Funktionalität zu gewährleisten.
- Es gibt nur wenige solcher Durchführungsorgane (= Spezialfall).

Die Anschlussart mit „einfachem Anschluss“ stellt eine Ausnahme von der Regel dar, dass Partnerdomänen ohne dazwischen liegende Fremddomänen am AHV/IV-Netz anzuschliessen sind.

Massnahmen zur Risikominimierung

Die Risiken, welche sich u.a. durch diese Anschlussart ergeben, sind wie folgt:

- Auf dem Netzwerk der Firma oder des Verbandes sind die Mechanismen des AHV/IV-Netzes zur Sicherstellung der Vertraulichkeit und der Integrität der übertragenen Daten nicht vorhanden.
- Die Zugangskontrolle der Domäne AHV/IV-Netz aufgrund von berechtigten IP-Adressen ist wenig effektiv, da sich hinter diesen nebst Mitarbeitern der Ausgleichskasse auch weitere Stellen der Firma/des Verbandes verbergen können.

Diese Risiken können nur zusammen mit den betroffenen Firmen/Verbänden minimiert werden. Dazu sind beim Anschluss einer AK als Teil einer Firma/eines Verbandes zusammen mit den zuständigen IT-Verantwortlichen geeignete Massnahmen wie folgt zu definieren:

- Es muss sichergestellt sein, dass nur berechtigte Benutzer der Ausgleichskasse auf das AHV/IV-Netz zugreifen kön-

nen.
- AHV/IV-Daten, welche über das Netzwerk der Firma/des Verbandes übertragen werden, müssen mittels kryptografischen Verfahren verschlüsselt werden.
- Die Integrität der übertragenen Daten ist mit kryptografischen Hashfunktionen sicherzustellen.

4.3.2 AK/IVS als Teil eines Kantonsnetzes

Ausgleichskassen oder IV-Stellen, die vollständig in der IT-Infrastruktur einer Verwaltungsstelle (Kanton, Gemeinde) integriert sind, stellen einen Spezialfall dar.
Nach Möglichkeit verwenden solche Stellen die vorhandene Netzinfrastruktur der Kantone und werden nicht am AHV/IV-Netz angeschlossen:
- Die kantonalen Verwaltungen in der Schweiz sind vom Bund bereits mit dem sog. KOMBV-KTV Netzwerk erschlossen. Dieses Netz verbindet die Kantone untereinander und mit den Stellen der Bundesverwaltung.
- Die Kantone und Gemeinden verwenden bereits heute das KOMBV-KTV für den Zugang auf die zentralen Register.
- Das KOMBV-KTV kann aus dem AHV/IV-Netz über die zentralen Netzübergänge erreicht werden.

Durchführungsorgane, welche als Teil des jeweiligen Kantons mit dem KOMBV-KTV erschlossen sind, gelten aus Sicht der Domäne AHV/IV-Netz als Fremddomänen.

4.3.3 Internetverbindungen für B2B-Anwendungen

Für Business-to-Business (B2B) Anwendungen, wie sie zum Beispiel gestützt auf e-AHV/IV vorkommen, gelten die Bestimmungen dieser Domänenpolicy sinngemäss. Da es sich um eine aktuelle und immer wieder auftauchende Fragestellung handelt, wird sie nachfolgend explizit im Rahmen dieser Domänenpolicy behandelt:

- Ein B2B-System wird nie direkt an der Domäne AHV/IV-Netz angeschlossen.
- Am AHV/IV-Netz angeschlossene Partnerdomänen, welche B2B-Systeme betreiben und zu diesem Zweck Netzübergänge zu Fremddomänen (bspw. zu Internet) unterhalten, müssen die minimalen Anforderungen zum Betrieb eines Netzüberganges bei einer Partnerdomäne erfüllen.
- Eine Internetverbindung, welche speziell für eine B2B-Lösung betrieben wird, unterliegt nicht denselben Vorgaben, wie sie gemäss WAN für den Internetzugriff von Benutzern gelten. Sie kann bei einem Rechenzentrum oder einem Partner der AHV/IV sein.

4.3.4 Internet VPN / Remote Access

Für Internet VPN / Remote Access Zugriffe gelten die Bestimmungen dieser Domänenpolicy sinngemäss. Da es sich um eine aktuelle und immer wieder auftauchende Fragestellung handelt, wird sie nachfolgend explizit im Rahmen dieser Domänenpolicy behandelt:

- Bei Netzzugriffen über Internet VPN / Remote Access handelt es sich immer um einen Zugriff aus einer Fremddomäne.
- Abhängig davon, ob die Fremddomäne mit einem zentralen Netzübergang am AHV/IV-Netz angeschlossen ist oder ob sie am Netz einer Partnerdomäne hängt, gilt die jeweilige Domänenpolicy (im ersten Fall gilt die WIsB, im zweiten Fall gilt die Domänenpolicy des Durchführungsorgans).

5 Kommunikationsverbindungen

Bezüglich Kommunikationsverbindungen in der Domäne AHV/IV-Netz gelten die folgenden Vorgaben:

Kommunikation zwischen Partnerdomänen über das

AHV/IV-Netz

- Sämtliche Kommunikation zwischen Partnerdomänen über das AHV/IV-Netz muss erstmalig von den Partnerdomänen gegenseitig genehmigt und vom Netzbetreiber geschaltet werden.
- Zuständig für die gegenseitige Genehmigung sind die IT-Sicherheitsverantwortlichen der Kommunikationspartner.

Kommunikation zwischen Partnerdomänen und Fremddomänen

Fall 1: Fremddomäne kann über einen zentralen Netzübergang des AHV/IV-Netzes erreicht werden:

- Sämtliche Kommunikation muss im Rahmen der Firewall-Policy definiert sein. Zuständig für diese Definition ist der IT-Sicherheitsverantwortliche der Partnerdomäne.

Fall 2: Fremddomäne kann über das AHV/IV-Netz via eine Partnerdomäne erreicht werden:

- Die Kommunikation muss erstmalig von den beiden Partnerdomänen A (will auf Fremddomäne via B zugreifen) und B (bietet einen Zugang zur Fremddomäne für A an) genehmigt und vom Netzbetreiber geschaltet werden.
- Zuständig für die gegenseitige Genehmigung sind die IT-Sicherheitsverantwortlichen der Partnerdomänen A und B.

Kommunikation zwischen zwei Fremddomänen über das AHV/IV-Netz

- Diese Art der Kommunikation ist grundsätzlich nicht erlaubt.
- Fallweise Ausnahmen können durch das BSV genehmigt werden.

6 Organisation

Die Rollenbeschreibungen im AHV/IV-Netz finden sich in der WAN. Für die Beschreibungen der einzelnen Rollen siehe dort.

Anhang 2

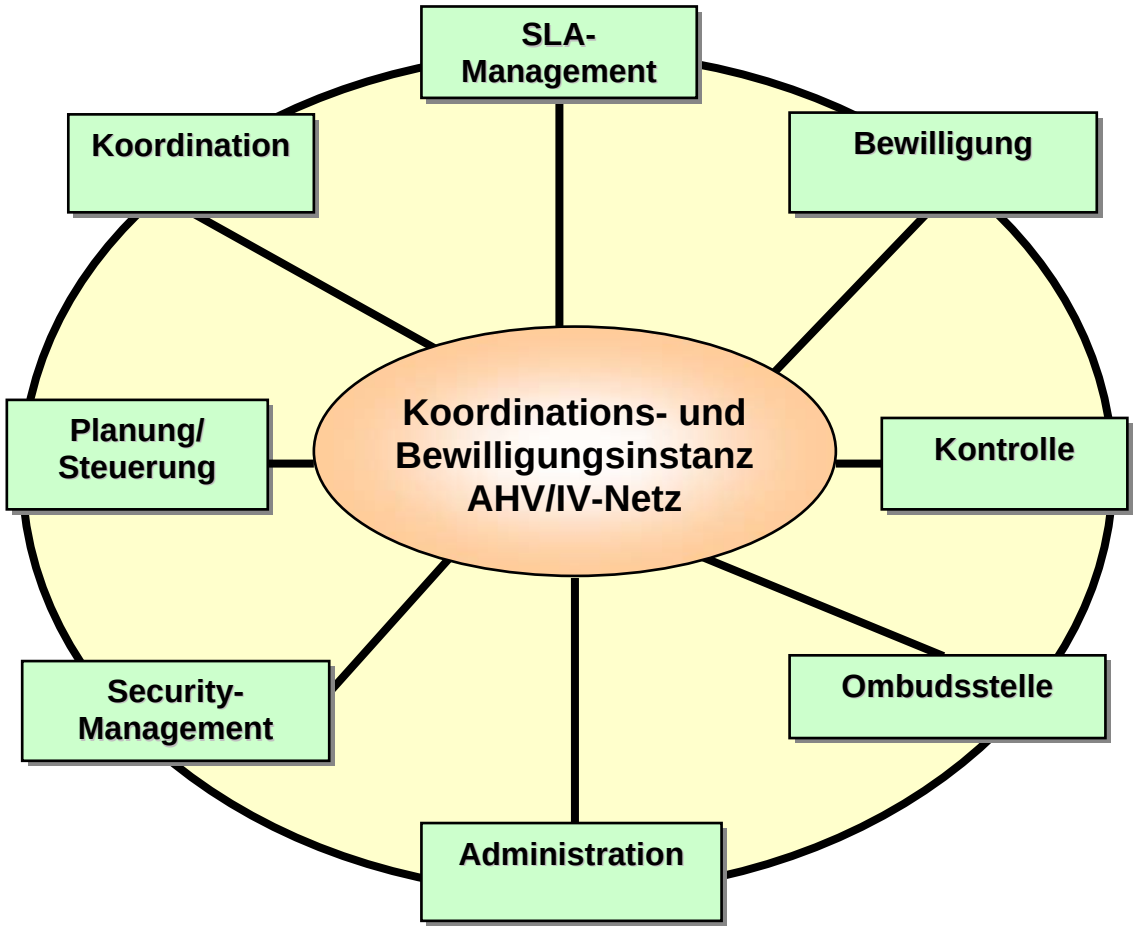
Koordinations- und Bewilligungsinstanz (KBI)

Die Aufgaben der Koordinations- und Bewilligungsinstanz wird durch das Bundesamt für Sozialversicherungen (BSV) als Netzanbieter (siehe auch Rz 5001ff) wahrgenommen.

Inhaltsverzeichnis

1. Aufgaben KBI – Grafische Übersicht

Das KBI ist zuständig für folgende Aufgaben



2. Aufgaben KBI – Teilbereiche

2.1 Koordination

- Vertretung der Interessen der Netzbenutzer gegenüber dem Netzbetreiber.
- Koordination von Änderungen/Anpassungen der Domänen-policy.
- Informationen rund um das AHV/IV-Netz gegenüber

  - Netzbenutzern
  - Netzbetreiber
  - BSV-interne sowie andere weitere Stellen (z.B. ZAS).
- Vertretung der Interessen des AHV/IV-Netzes bei der Entwicklung oder Anpassung von bestehenden Applikationen, sofern sie einen Einfluss aufs Netz haben.
- Pflege der Weisungen AHV/IV-Netz (WAN).

2.2 Bewilligung

- Neue Netzanschlüsse am AHV/IV-Netz.
- Netzübergänge zu Fremddomänen
- Kostenrelevante Änderungen (Changes) der bestehenden Anschlüsse (z.B. Bandbreitenerhöhung, Einführung nachträglicher Redundanz etc.).
- Kommunikationsverbindungen zwischen Fremddomänen über das AHV/IV-Netz.
- Domänenpolicies von Partnerdomänen, sofern diese eigene Netzübergänge zu Fremddomänen betreiben.
- Anschlüsse von Rechenzentren.
- Externe Internetanschlüsse.

2.3 Planung und Steuerung

- Mittelfristplanung AHV/IV-Netz (Ausbauplanung) zusammen mit dem Netzbetreiber.
- Planung neuer Services bzw. Produkte zusammen mit dem Netzbetreiber.
- Pro-aktive Auswertung der vom Netzbetreiber gelieferten Reports hinsichtlich zukünftiger Bedürfnisse oder mittelfristig zu erwartender Engpässe.
- Teilnahme an Koordinations-Meetings mit dem Netzbetreiber.

2.4 Kontrolle

- Der ordnungsgemässen Umsetzung der Domänenpolicy bei den Netzbenutzern sowie beim Netzbetreiber
  - Anordnung von Audits
  - Anordnung von technischen und organisatorischen Massnahmen zur Behebung von sicherheitsrelevanten Missständen
  - Überwachung der Umsetzung.
- Der Quartalsrechnung des Netzbetreibers.
- Der Qualität und der vereinbarten Services vom Netzbetreiber aufgrund regelmässiger Reports.

2.5 Steuerung Service Level Agreement (SLA)

- Aufträge an den Netzbetreiber erteilen und Umsetzung überwachen für
  - den Anschluss von neuen Standorten;
  - die Aufhebung bzw. Zusammenlegung von Standorten;
  - die Anpassung bestehender Standorte (z.B. Bandbreitenerhöhung);
  - die Einführung neuer oder Anpassung bestehender Services.

2.6 Security-Management

- Ist als Eigentümer der Domänenpolicy verantwortlich für die Pflege derselben auf Vorschlag des Netzanbieters.
- Eskalationsstelle beim Eintreten von Notfällen (Emergencies).
- Definition von Notfall-Szenarien und entspr. Massnahmen zusammen mit dem Netzbetreiber.
- Definition von Sicherheitsmassnahmen beim Anschluss von AK/IVS, welche netztechnisch Teil einer Firma/eines Verbandes sind.

- Durchführen oder Beauftragen von Sicherheitsaudits bei Partnerdomänen.
- Archivierung der Domänenpolicy und allfälliger, individueller Verschärfungen einzelner Pools.

2.7 Ombudsstelle

- Eskalationsstelle für Reklamationen und Probleme der Netzbenutzer und Netzbetreibers.
- Eskalationsstelle für Unklarheiten/Differenzen im Zusammenhang mit der Umsetzung der Weisungen AHV/IV-Netz sowie der Domänenpolicy AHV/IV-Netz.
- Adressat für Feedback zum AHV/IV-Netz.

2.8 Administration

- Verantwortlich für den Einsatz von unterstützenden Systemen und Tools (z.B. Bestell- und Mutationswesen für Anschlüsse über Intranet AHV/IV).
- Pflege von entsprechenden Angeboten im Intranet AHV/IV
- Quartalsweise Weiterverrechnung von Leistungen, die über das Grundangebot hinausgehen an die Netzbenutzer.
- Zuständig für die Übersetzung der wichtigsten Dokumente ins Französische.