Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Strassen ASTRA

DOKUMENTATION

IAM BSA - BENUTZER-AUTHENTIFIZIE-RUNG, BERECHTIGUNGEN, ZUGRIFFSPORTALE

Ausgabe 2025 V1.00
ASTRA 83056

Impressum

Autoren / Arbeitsgruppe

Geringer Jolanda	ASTRA DS-DTI Vorsitz
Gähwiler Daniel	CSI Consulting AG
Grau Rolf	CSI Consulting AG

Arbeitsgruppe (Revision)

Crausaz Bernard	ASTRA DS-UARS
Jehli Martin	GE V
Widrig Bruno	GE XI
Schlup Markus	Amstein + Walthert Progress AG

Originalsprache
Deutsch

Herausgeber
Bundesamt für Strassen ASTRA
Abteilung Strassennetze N
Standards und Sicherheit der Infrastruktur SSI
3003 Bern

Bezugsquelle
Das Dokument kann kostenlos von www.astra.admin.ch heruntergeladen werden.

Inhaltsverzeichnis

1 Einleitung

1.1 Zweck der Dokumentation

Diese Dokumentation ergänzt und detailliert das Kapitel 7.2.3 (GS16) der ASTRA Richtlinie 13030 „OT-Security“ [2] und hat zum Ziel, für das ganze IP-Netz BSA ein einheitliches Identitäts- und Zugriffsmanagement einzuführen.

1.2 Geltungsbereich

Diese Dokumentation ist ein Zusatzdokument zur ASTRA Richtlinie 13030 „OT-Security“ [2] und hat denselben Geltungsbereich.

Die langfristige Sicherung der Kommunikation mittels Zertifikate einer zentralen Zertifizierungsstelle (PKI) innerhalb des IP-Netz BSA ist nicht Teil dieser Dokumentation.

1.3 Adressaten

Das Dokument richtet sich an folgende Stakeholder:

- Fachspezialisten OT/BSA der Gebietseinheiten;
- Projektleiter des ASTRA (bei Projekten mit Steuer- und Leittechnik);
- Planer und Unternehmungen, die im Auftrag des ASTRA Tätigkeiten an den OT (Operational Technology) / BSA ausführen;
- Fachspezialisten und Erhaltungsplaner BSA des ASTRA
- Projektleiter SA-CH des ASTRA.

1.4 Inkrafttreten und Änderungen

Dieses Dokument tritt am 19.06.2025 in Kraft. Die „Auflistung der Änderungen“ ist auf Seite 17 dokumentiert.

2 Begriffe

2.1 IAM BSA mit MFA

Beim IAM BSA handelt es sich um ein zentrales, einheitliches und sicheres Identity and Access Management (IAM), mit einer Multifaktorauthentisierung (MFA), spezifisch ausgelegt für die Bedürfnisse der BSA. Das IAM BSA soll eine erhöhte Zugangssicherheit zu den BSA gewährleisten, ohne die Autonomie der BSA zu gefährden. Das IAM BSA ist wesentlich für die Rechtevergabe und -kontrolle im IP-Netz BSA und muss somit selbst in Not- und Katastrophensituationen in einer Minimalversion funktionieren.

Das IAM BSA stellt die zentrale Verwaltung aller personenbezogenen Identitäten der Basisdienste und aller Gebietseinheiten inkl. VMZ-CH sicher, abgesehen von Notzugängen und Systemadministrationskonten. Das System wird in der finalen Ausbaustufe durch rund 6000 Mitarbeitende der Gebietseinheiten-, der Lieferanten und auch des Bundes genutzt.

Im IAM BSA werden dabei Personaldaten sowohl von Gebietseinheits-, von Lieferanten- als auch von Bundesmitarbeitern bearbeitet. Alle Benutzer registrieren sich und müssen eine Ausweiskopie ablegen.

Mit dem Projekt IAM BSA sollen folgende übergeordnete Ziele erreicht werden:

- Gewährleistung einer erhöhten Zugangssicherheit zu den BSA, ohne die Autonomie der BSA zu gefährden;
- Standardisierung der Verwaltung von Benutzern im Bereich der BSA durch den Aufbau einer gemeinsamen Lösung, die eine GE-bezogene Verwaltung von Identitäten und Berechtigungen / Rollen ermöglicht;
- Die Überprüfung der Identität eines Benutzers erfolgt eindeutig, einheitlich und nach dem gleichen Massstab.
- Jede GE als auch die VMZ-CH muss eigene Berechtigungen vergeben können;
- Ausgeführte Aktionen werden personenbezogen aufgezeichnet.

➢ *Alle Benutzer und Administratoren Accounts (ausser Domain-Administratoren) werden künftig über IAM BSA verwaltet und in die jeweiligen AD provisioniert.*

2.2 Active Directory

Das Active Directory (AD) ist ein Verzeichnis zur Verwaltung verschiedener Objekte in einem IP-Netzwerk wie beispielsweise Benutzer, Gruppen, Computer, Dienste, Server, Dateifreigaben und andere Geräte wie Drucker und Scanner und deren Eigenschaften. Mit Hilfe von Active Directory kann ein Administrator die Informationen der Objekte organisieren, bereitstellen und überwachen.

Den Benutzern des IP-Netzwerkes können Zugriffsbeschränkungen erteilt werden. So darf zum Beispiel nicht jeder Benutzer jede Datei ansehen oder auf jede Fachanwendung zugreifen.

2.3 Zugangsportal

Um die Identitäten und Zugriffe zu verwalten, zu prüfen und zu bewirtschaften, wird als Teil des IAM BSA ein zentrales Zugangsportal inkl. Workflows erstellt (IAM BSA Web-Portal). Dieses Portal ist öffentlich erreichbar und ermöglicht es den Benutzern, die wichtigsten Aufgaben direkt aus dem Portal abzuwickeln. Das Portal bietet folgende Funktionen an:

- Selbstständige Benutzerregistrierung;
- Passwort setzen / zurücksetzen;
- Hilfe zu häufigen Benutzerfragen.

2.4 Workflows

Workflows legen die Abfolge von Arbeitsschritten und die Zuständigkeiten fest und beinhalten die Registrierungsprozesse, die Antragsprozesse für Identitätsprüfung, Rollenvergabe, Berechtigungsvergabe und Sistierung.

Nachfolgende Geschäftsprozesse sind für die Benutzer umgesetzt und werden durch Workflows unterstützt:

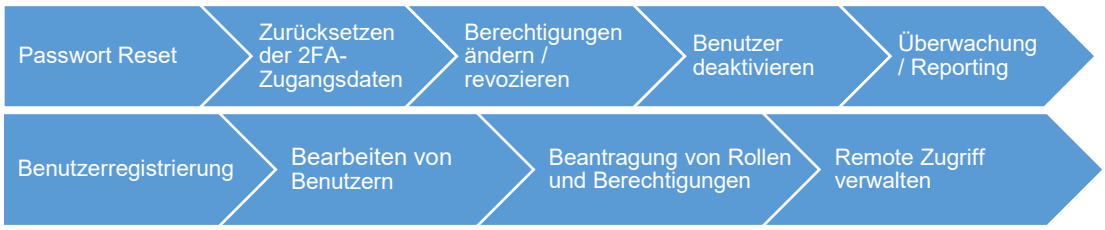

Abb. 2.1 Übersicht Geschäftsprozesse

2.5 PAM / RAS / PRA

PAM (Privileged Access Management) dient zur Absicherung von administrativen Zugriffen auf BD-Systeme. Insbesondere werden administrative Accounts aller Serversysteme gesichert.

Die Remote Access Lösung RAS (Remote Access Service) ersetzt den bestehenden VPN-Zugang und limitiert den Zugriff auf dedizierte Systeme zu bestimmten Zeiten und definierbaren Rollen. Das Ziel von PRA (Privileged Remote Access) ist eine Zugriffssicherheitslösung, die vor Cyberbedrohungen schützt.

Durch die Einführung einer PAM/RAS (Privilege Access Management / Remote Access Service) wird eine moderne Möglichkeit zur Verfügung gestellt, die OT-Systeme per Remotezugriff verfügbar zu machen, ohne den Remote-Usern komplizierte Netzwerk-Konfigurationen aufzuerlegen.

3 Umsetzung im IP-Netz BSA

3.1 Grundsatz

Das IAM BSA System stellt die zentrale Verwaltung aller personenbezogenen Identitäten der Basisdienste und aller Gebietseinheiten inkl. VMZ-CH sicher. Alle Dienste im IP-Netz BSA nutzen das IAM BSA für Identitäts- und Zugriffsmanagement. Das IAM BSA stellt die Verknüpfungen zu den Active Directories der GE sicher, sodass sich alle Benutzer der OT-Systeme über das Active Directory authentisieren und authorisieren können. Die OT-Systeme können sich über Windows Domain-Join, LDAP / LDAPS oder Radius an die AD anbinden.

3.2 IAM BSA

Die Daten werden über die Benutzer-Registrierung erfasst, um neue Accounts zu erstellen.

Weitere Daten werden innerhalb der IAM BSA Komponente Sailpoint erfasst, um die Rollen und Berechtigungen der Organisationen einzustellen und diese auf die AD-Gruppen abzubilden. Im weiteren Verlauf der Berechtigungen werden die Daten zwischen den IAM BSA, AD und MFA-Systemen automatisch abgeglichen.

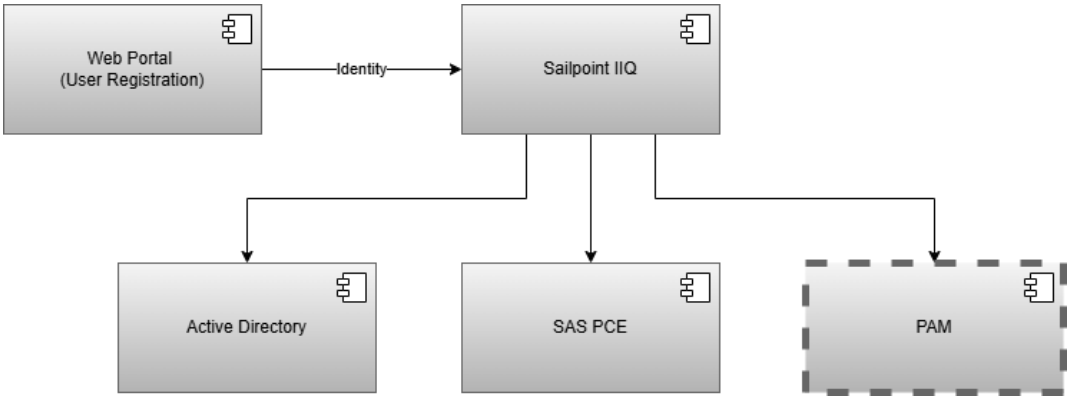

Abb. 3.2 Datenfluss Identity

Die Ausweisfotos werden auf einem eigenen, geschützten IIS-Server gespeichert. Die Sailpoint Identity Datenbank enthält einen Link auf das jeweilige Ausweisfoto. Damit die IIS-Server in BD-A und BD-B auf dem gleichen Stand sind, müssen diese Verzeichnisse mit den Ausweisfotos zwischen BD-A und BD-B synchronisiert werden. Dadurch ist ein Failover im Fehlerfall gewährleistet.

Die eingegebenen Daten werden nur innerhalb des IAM BSA Systems verarbeitet.

3.3 Zugriffsberechtigungen und Rollen

Im IP-Netz BSA wird Role-Based Access Control (RBAC) umgesetzt. Dies ist ein Sicherheitskonzept, das den Zugriff auf Ressourcen auf Grundlage der Rolle eines Benutzers strukturiert. RBAC ermöglicht eine effiziente und granulare Verwaltung von Berechtigungen, indem Zugriffsrechte auf Basis von definierten Rollen zugewiesen werden.

RBAC basiert auf folgenden grundlegenden Prinzipien:

1. **Benutzer-Rollen-Verknüpfung:** Jeder Benutzer wird einer oder mehreren definierten Rollen zugeordnet. Eine Rolle repräsentiert dabei eine Gruppe von Aufgaben oder Verantwortlichkeiten. Diese Zuordnung erfolgt im IAM BSA;
2. **Rollen-Berechtigungsgruppen-Verknüpfung**: Jede Rolle wird mit den erforderlichen Berechtigungsgruppen ausgestattet (nachfolgend Servicegroup genannt);

diese Zuordnung erfolgt ebenfalls im IAM BSA. Die Servicegroups werden vom IAM BSA ins AD provisioniert;

3. **Berechtigungen auf Systemen**: in den Systemen werden die Servicegroups entsprechend berechtigt.

Die Rollen werden ausschliesslich im IAM BSA verwaltet. Ebenso werden die Servicegroups grundsätzlich im IAM BSA verwaltet und im Active Directory als Domain Local Security Groups provisioniert.

Dienste wie LDAP, LDAPS, Kerberos etc. werden weiterhin über Microsoft AD geliefert.

3.4 Zusammenspiel IAM BSA und Active Directory

Im gesamten IP-Netz BSA erfolgt das Benutzermanagement zentral über das IAM BSA (Produkt: Sailpoint) in den Basisdiensten. D.h. ein Benutzer einer Gebietseinheit kann über das Portal selbstständig einen Benutzeraccount bestellen (Self Registration Portal). Dieser wird dann über das IAM BSA von der jeweiligen Gebietseinheit angelegt, verwaltet / berechtigt (Zuweisung Benutzer zu Rollen/ Rollen zu Service Groups) und gesperrt / gelöscht. Das IAM BSA provisioniert dabei neu angelegte Benutzer und Service Groups automatisch ins Active Directory der jeweiligen Gebietseinheit, der VMZ-CH und der Basisdienste.

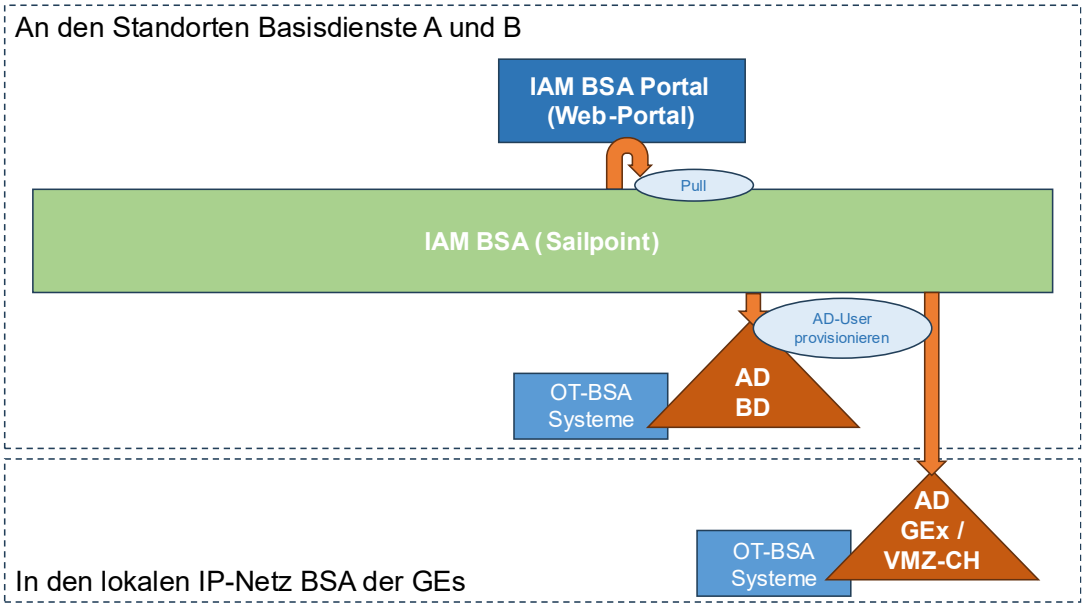

Abb. 3.3 Zusammenspiel IAM – AD

Users und Servicegroups werden im IAM BSA verwaltet und ins AD in die Standard-OUs „IAM Managed Users“ und „IAM Managed Service Groups“ provisioniert.

Alle ADs sind unabhängig voneinander (kein übergeordneter Forest): Die Gebietseinheiten, die Basisdienste und die VMZ-CH erhalten jeweils einen eigenen Forest und gleichnamige Domäne. Die Domänen sind eigenständig und untereinander nicht getrustet.

Getrennte Identitäten für die Produktionsumgebung (PROD) und Integrationsumgebung (INT) sind verfügbar.

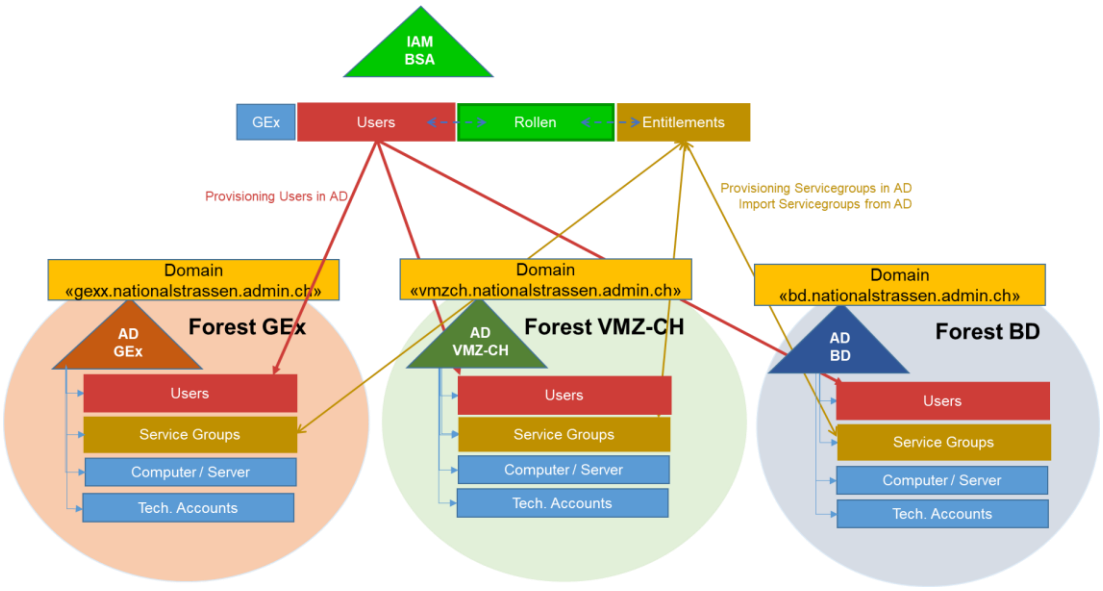

Abb. 3.4 Einbindung IAM – AD

Nachfolgend eine Übersicht über die im Prozess «Zugriffsberechtigung» involvierten Rollen und ihre Interaktion.

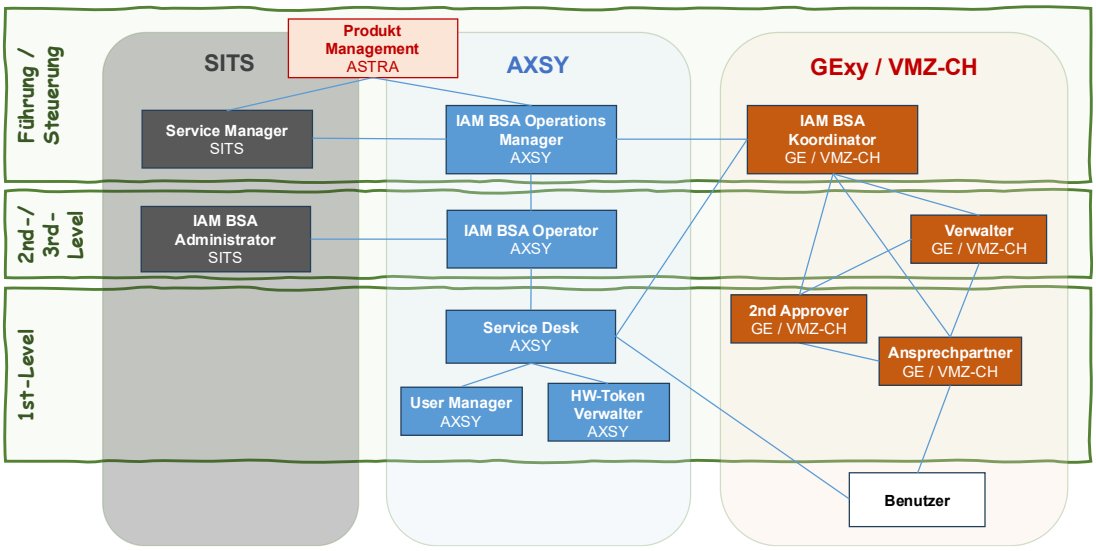

Abb. 3.5 Interaktion der Rollen im Betrieb

Tab. 3.1 Übersicht Rollenbezeichnungen

Rolle innerhalb IAM BSA	Beschreibung
Benutzer	Person, die einen oder mehrere Accounts für den Zugriff auf Anwendungen innerhalb des ASTRA benötigt.
Ansprechpartner	Identifiziert die Antragsteller von Accounts und bewilligt deren Registrierungs-Anträge oder lehnt sie ab.
2nd Approver	Zusätzliche Bewilligungsebene, die Anträge als 2. Instanz genehmigen muss, wie z.B. Registrierungsanträge externer Personen.
Verwalter GE / VMZ-CH	Verantwortlich für die Verwaltung einer Gebietseinheit (Rollenzuweisung, Revozieren von Rollen, Hinzufügen und Entfernen von Benutzern etc.). Kennt die Zuständigkeiten der Mitarbeiter zu den lokalen Aufgabengebieten.
Koordinator IAM BSA im Betriebsbereich	Sammelt und triagiert neue Anforderungen, Änderungen, Fragestellungen und Befunde rund um IAM BSA in der GE / VMZ-CH, beantwortet diese wo

Tab. 3.1 Übersicht Rollenbezeichnungen

Rolle innerhalb IAM BSA	Beschreibung
	möglich selbst und interagiert für die übrigen mit dem IAM BSA Operations Manager (AXSY). Verantwortlich für die Definition, Zuweisung und Beschreibung von AD-Rollen zu den jeweiligen Anwendungen.
Service Desk	1st-Level-Support für die Benutzer. Notifikation an Integrator und Rückmeldungen an Benutzer.
User Manager	Pflegt die Benutzer-Informationen / Attribute wie Name, Mail-Adresse etc. in Sailpoint (z.B. bei Namenswechsel). Diese Rolle erfordert kein tiefergehendes Know-How innerhalb der IAM BSA Applikation (Sailpoint).
HW-Token-Verwalter	Verwaltet die Hardware-Tokens, die für den Zugriff auf bestimmte Services / Applikationen für MFA erforderlich sind; weist sie den Benutzern in SAS PCE zu und versendet sie.
IAM BSA Operator	Diese Rolle erfordert tiefergehendes Know-How innerhalb der IAM BSA Applikation und ein End-to-End-Verständnis der Lösung. Hat erweiterte Berechtigungen in den einzelnen IAM BSA Komponenten (Sailpoint, Thales SAS, PAM, RAS). Identifiziert, analysiert und behebt Probleme im bestehenden IAM BSA System. Unterstützt bei 2nd- und 3rd-Level-Anfragen. Überwacht Monitoring.
IAM BSA Operations Manager	Technische Schnittstelle zwischen Integrator und externem Betriebsdienstleister (AXSY), Koordination der Fachgebiete im IAM BSA Servicebereich. Planen, überwachen und dokumentieren von Changes im Bereich IAM BSA; Koordination mit den Basisinfrastruktur-Diensten.
IAM BSA Administrator	Kann system-relevante Details und Funktionen der IAM BSA Anwendung steuern und ändern.

3.5 Aufbewahrungsdauer und Löschung

Identitäten werden nur deaktiviert – nicht gelöscht. Somit gibt es im IAM BSA grundsätzlich keine Löschung und auch keine begrenzte Aufbewahrungsdauer. Eine Löschung einer Identität erfolgt nur im Todesfall.

Vorherige Kopien von erneuerten Ausweisdokumenten werden hingegen nach erfolgreicher Erneuerung gelöscht.

3.6 Web-Portal

Das IAM BSA Web-Portal ist eine öffentlich zugängliche Web-Applikation, welche in den Basisdiensten betrieben wird. Über das Web-Portal können Benutzer eine Benutzer-Registrierung oder einen Passwort-Reset erfassen.

3.7 MFA

Das MFA-System fügt einen zweiten Faktor zur Authentisierung hinzu, z.B. beim Aufbau einer VPN-Verbindung. Innerhalb des MFA-Systems verläuft die Kommunikation verschlüsselt und wird mit Zertifikaten abgesichert.

3.8 Passwort Richtlinien

Passwörter sind gemäss ASTRA Richtlinie 13030 GS 18 einzurichten.

3.9 Fernzugriffe auf die Dienste des IP-Netz BSA

3.9.1 Zugriff via VPN

Für den Fernzugriff auf die Dienste des IP-Netz BSA besteht die Möglichkeit vom Internet via Checkpoint Mobile Agent über die Basisdienst-Standorte BD-A und BD-B auf die Jumphosts in den BD-Standorten zu zugreifen.

Von den Jumphosts aus kann dann auf die Zielsysteme zugegriffen werden:

- Mithilfe eines Webbrowsers auf eine Web-Applikation
- Mithilfe von RDP (Remotedesktopverbindung App) auf übrige Server

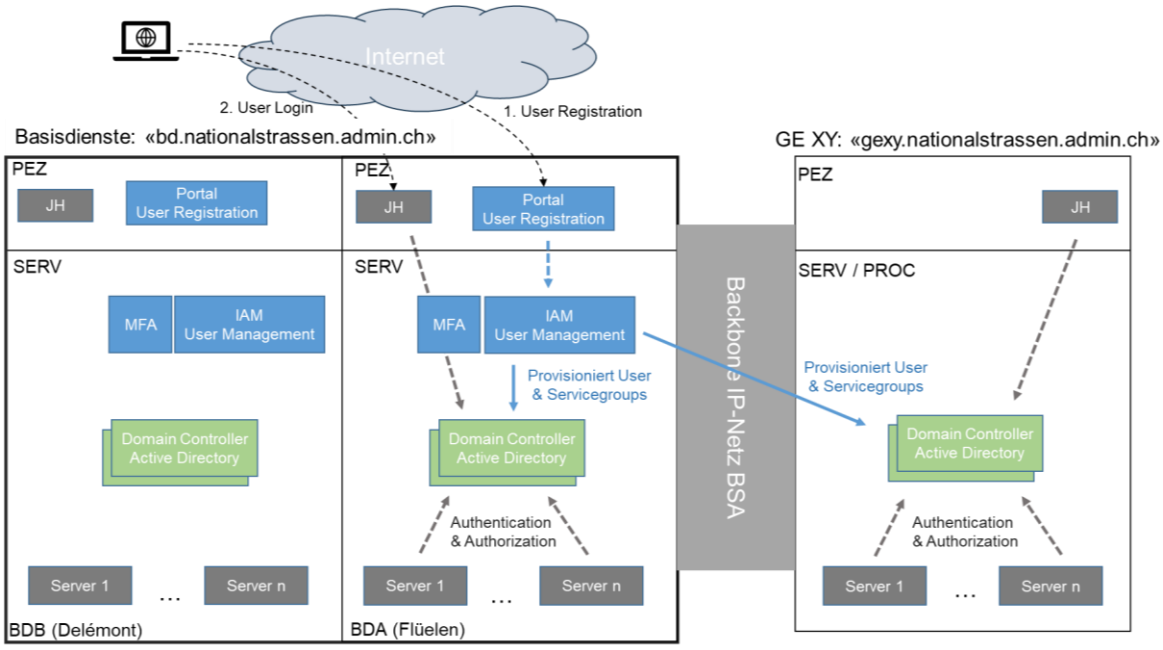

Abb. 3.6 Zugriff via Internet auf IP-Netz BSA

4 Glossare

4.1 Glossar IP-Netz BSA

Begriff/Abkürzung	terme/abréviation	Bedeutung
ASTRA	OFROU	Bundesamt für Strassen
Ausrüstung/Gerät	équipement	Jede Art von aktiven Geräten im BSA-Umfeld (auch ohne Verbindung zum IP-Netz BSA)
Backbone/BB	backbone/BB	Vom Bund (L3 durch BIT, Übertragung durch FUB) bereitgestellte nationale Vernetzung aller Teilnetze
BD (Basisdienste)	BD (services de base)	Netzwerk-Basisdienste (IPAM-Tool, DNS, Zeitquellen, …) für das gesamte IP-Netz BSA
BSA	EES	Betriebs- und Sicherheitsausrüstungen
Client/Host Server	client/hôte serveur	allgemeine ICT-Begriffe (keine BSA-spezifische Bedeutung), Verwendung bei der Beschreibung von Protokollen
Endgerät	équipement terminal	Jede Art von Ausrüstung an einem Userport des IP-Netzes BSA
F/Filiale	F/filiale	Filiale (fünf regionale Einheiten des ASTRA)
GE	UT	Gebietseinheit (11 überkantonale organisatorischen Einheiten, die ihr eigenes IP-Netz BSA GE betreiben)
IP-Netz BSA	réseau IP EES	Ein IP-Netz für die Betriebs- und Sicherheitsausrüstung der Nationalstrassen mit fol-genden Elementen (Teilnetzen): - 11 IP-Netze BSA GE - dem IP-Netz BSA Backbone (Backbone der Bundesverwaltung) - Verbindungen zur VMZ-CH - Verbindungen zu den Rechenzentren BSA - Verbindungen zu den BD (Basisdiensten des IP-Netz BSA)
Netzwerkausrüstung	équipement réseau	Alles (inkl. Firewall, Management-Systeme, …)
Netzwerkelement	élément réseau	Nur aktive Übertragungsausrüstung (Router oder Switch)
PEZP	PEZP	Policy Enforcement Zone Proxy
RFC	RFC	Die RFC (Requests for Comments) beinhalten technische und organisatorische Dokumente über das Internet. Einige RFC, jedoch nicht alle, stellen Internetstandards dar und müssen hohe Anforderungen erfüllen und einen Gemeinschaftskonsens der Internet Engineering Task Force (IETF) darstellen.
Router	routeur	Gemeint sind immer die MPLS-Router der Erschliessungsringe, sonst (z.B. Spoke-Site-Router) explizit erwähnt
RZ(-BSA)	RZ(-BSA)	Rechenzentrum BSA
(Netzwerk-)Segment	segment (de réseau)	Segmente gemäss ASTRA 83040 pro (Teil-)Anlage (meist VLAN)
Switch	commutateur	gemeint sind immer die L2-Netzwerkelemente des Access-Layers, sonst entsprechend erwähnt
UVEK	DETEC	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
VDV	VDV	Verkehrsdatenverbund: Verbindungen der Gebietseinheiten untereinander und zu den Rechenzentren BSA; werden durch den IP-Netz BSA Backbone ersetzt
VMZ(-CH)	VMZ(-CH)	Verkehrsmanagement-Zentrale
(Netzwerk-)Zone	zone (de réseau)	Im Sinne der NSP des Bundes Si003 (getrennt durch PEZ)

4.2 Glossar IAM BSA

Begriff/Abkürzung	Bedeutung
2FA	2 Factor Authentification
AD	Active Directory
BD-A, BD-B	Basisdienste Standort A, Basisdienste Standort B
BIT	Bundesamt für Informatik und Telekommunikation
DNS	Domain Name Service
Forest	Verbund von Active Directory-Domänen mit gemeinsamem Globalen Katalog, Verzeichnisschema und Verzeichniskonfiguration.
IAM	Identity and Access Management
IIS	Internet Information Server
IKT	Informations- und Kommunikations-Technologien
IP	Internet Protocol
MFA	Multifaktor-Authentifizierung
MS	Microsoft
PAM	Privileged Access Management
PKI	Public Key Infrastructure
RAS	Remote Access Service
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
SAS PCE	SafeNet Authentication Service Private Cloud Edition

Literaturverzeichnis

Weisungen und Richtlinien des ASTRA

[1] Bundesamt für Strassen, Weisungen ASTRA 73006 „OT Security Governance, Security im Bereich BSA-Systeme“, www.astra.admin.ch.

[2] Bundesamt für Strassen, Richtlinie ASTRA 13030 „OT-Security“, www.astra.admin.ch.

Auflistung der Änderungen

Ausgabe	Version	Datum	Änderungen
2025	1.00	19.06.2025	Inkrafttreten der Ausgabe 2025 (deutsche, französische und italienische Version).