Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Office fédéral des routes OFROU

DOCUMENTATION

IAM BSA - AUTHENTIFICATION UTILISATEUR, AUTORISATIONS, PORTAILS D'ACCÈS

Édition 2025 V1.00
ASTRA 83056

Impressum

Auteurs

Geringer Jolanda	OFROU DS-DTI Présidence
Gähwiler Daniel	CSI Consulting AG
Grau Rolf	CSI Consulting AG

Groupe de suivi (révision)

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

Traduction
CSI Consulting AG, la version originale en allemand fait foi.

Éditeur
Office fédéral des routes OFROU
Division Réseaux routiers N
Standards et sécurité de l'infrastructure SSI
3003 Berne

Sources
Le document peut être téléchargé gratuitement sur le site www.ofrou.admin.ch.

Table des matières

Impressum **2**

1 Introduction **5**
1.1 Objectif de la documentation 5
1.2 Champ d'application 5
1.3 Destinataires 5
1.4 Entrée en vigueur et modifications 5

2 Termes **6**
2.1 IAM BSA avec MFA 6
2.2 Active Directory 6
2.3 Portail d'accès 6
2.4 Flux de travail 7
2.5 PAM / RAS / PRA 7

3 Mise en œuvre dans le réseau IP EES **8**
3.1 Principe 8
3.2 IAM BSA 8
3.3 Autorisations d'accès et rôles 8
3.4 Interaction entre IAM BSA et Active Directory 9
3.5 Durée de conservation et effacement 11
3.6 Web-Portail 11
3.7 MFA 11
3.8 Directives relatives au mot de passe 12
3.9 Accès à distance aux services du réseau IP EES 12
3.9.1 Accès via VPN 12

4 Glossaires **13**
4.1 Glossaire réseau IP EES 13
4.2 Glossaire IAM BSA 14
Bibliographie **15**
Liste des modifications **17**

1 Introduction

1.1 Objectif de la documentation

Cette documentation complète et détaille le chapitre 7.2.3 (GS16) de la directive OFROU 13030 « OT Security » [1] et a pour but d'introduire une gestion uniforme des identités et des accès pour l'ensemble du réseau IP EES.

1.2 Champ d'application

Cette documentation est un document complémentaire à la directive OFROU 13030 « OT Security » [2] et a le même champ d'application.

La sécurisation à long terme de la communication au moyen de certificats d'une autorité de certification centrale (PKI) au sein du réseau IP EES ne fait pas partie de cette documentation.

1.3 Destinataires

Le document s'adresse aux parties prenantes suivantes :

- Spécialistes OT/EES des unités territoriales ;
- Chef de projet de l'OFROU (pour les projets impliquant des systèmes de commande et de gestion) ;
- Planificateurs et entreprises qui exécutent des activités sur les OT (Operational Technology) / EES sur mandat de l'OFROU ;
- Spécialistes et gestionnaires du patrimoine EES de l'OFROU ;
- Chef de projet SA-CH de l'OFROU.

1.4 Entrée en vigueur et modifications

Ce document entre en vigueur le 19.06.2025 . La "liste des modifications " est documentée à la page 17.

2 Termes

2.1 IAM BSA avec MFA

L'IAM BSA est un système de gestion des identités et des accès (IAM) centralisé, uniforme et sécurisé, avec une authentification multifactorielle (MFA), conçu spécifiquement pour les besoins des EES. L'IAM BSA doit garantir une sécurité d'accès accrue aux EES, sans pour autant compromettre l'autonomie des EES. L'IAM BSA est essentiel pour l'attribution et le contrôle des droits dans le réseau IP EES et doit donc fonctionner dans une version minimale, même dans les situations d'urgence et de catastrophe.

L'IAM BSA assure la gestion centrale de toutes les identités personnelles des services de base et de toutes les unités territoriales, y compris VMZ-CH, à l'exception des accès d'urgence et des comptes d'administration système. Dans sa version finale, le système est utilisé par environ 6000 collaborateurs des unités territoriales, des fournisseurs et également de la Confédération.

Dans l'IAM BSA, les données personnelles des employés de l'unité territoriale, des fournisseurs et des employés fédéraux sont traitées. Tous les utilisateurs de s'enregistrent et doivent déposer une copie de leur carte d'identité.

Le projet IAM BSA doit permettre d'atteindre les objectifs généraux suivants :

- assurer une plus grande sécurité d'accès aux EES sans compromettre l'autonomie des EES ;
- standardiser la gestion des utilisateurs dans le domaine de l'EES en construisant une solution commune qui permette une gestion des identités et des autorisations / rôles spécifiques aux UT ;
- vérifier l'identité d'un utilisateur est effectuée de manière univoque, uniforme et selon les mêmes critères ;
- Chaque UT ainsi que la VMZ-CH doivent pouvoir attribuer leurs propres autorisations ;
- Les actions effectuées sont enregistrées en fonction de la personne.

➢ *Tous les comptes d'utilisateurs et d'administrateurs (à l'exception des administrateurs de domaine) seront désormais gérés par IAM BSA et provisionnés dans les AD correspondants.*

2.2 Active Directory

L'Active Directory (AD) est un répertoire permettant de gérer les différents objets d'un réseau IP, tels que les utilisateurs, les groupes, les ordinateurs, les services, les serveurs, les partages de fichiers et autres équipements tels que les imprimantes et les scanners, ainsi que leurs propriétés. A l'aide d'Active Directory, un administrateur peut organiser, mettre à disposition et surveiller les informations des objets.

Des restrictions d'accès peuvent être attribuées aux utilisateurs du réseau IP. Par exemple, chaque utilisateur ne peut pas consulter n'importe quel fichier, ou accéder à n'importe quelle application métier.

2.3 Portail d'accès

Afin de gérer, de vérifier et d'administrer les identités et les accès, un portail d'accès central, y compris les flux de travail, est créé dans le cadre de IAM BSA (portail web IAM BSA). Ce portail est accessible au public et permet aux utilisateurs d'effectuer les principales tâches directement à partir du portail. Le portail offre les fonctions suivantes :

- Enregistrement autonome de l'utilisateur ;
- Définition / réinitialisation le mot de passe ;
- Aide pour les questions fréquentes des utilisateurs.

2.4 Flux de travail

Les workflows définissent la séquence des étapes de travail et les responsabilités et comprennent les processus d'enregistrement, les processus de demande de vérification d'identité, d'attribution de rôles, d'attribution de droits et de suspension.

Les processus de gestion suivants sont mis en œuvre pour les utilisateurs et sont soutenus par des workflows :

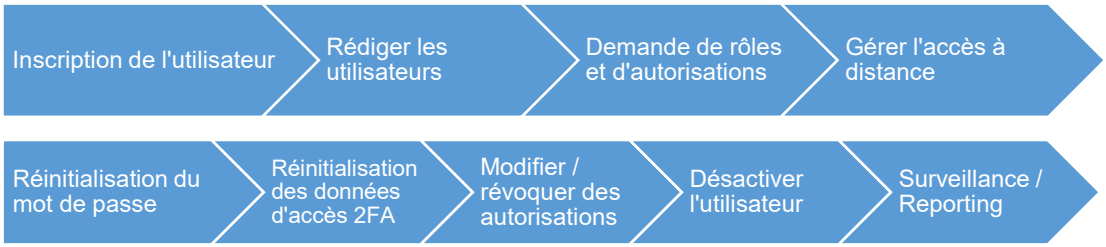

Fig. 2.1 Aperçu des processus

2.5 PAM / RAS / PRA

PAM (Privileged Access Management) sert à sécuriser les accès administratifs aux systèmes BD. En particulier, les comptes administratifs de tous les systèmes de serveurs sont sécurisés.

La solution d'accès à distance RAS (Remote Access Service) remplace l'accès VPN existant et limite l'accès à des systèmes dédiés à des heures précises et à des rôles définissables. L'objectif de PRA (Privileged Remote Access) est une solution de sécurité d'accès qui protège contre les cybermenaces.

L'introduction d'un PAM/RAS (Privilege Access Management / Remote Access Service) offre un moyen moderne de rendre les systèmes OT accessibles à distance, sans imposer des configurations réseau compliquées aux utilisateurs distants.

3 Mise en œuvre dans le réseau IP EES

3.1 Principe

Le système IAM BSA assure la gestion centralisée de toutes les identités personnelles des services de base et de toutes les unités territoriales, y compris VMZ-CH. Tous les services du réseau IP EES utilisent le système IAM BSA pour la gestion des identités et des accès. L'IAM BSA assure les liens avec les Active Directories de l'UES, de sorte que tous les utilisateurs des systèmes OT puissent s'authentifier et s'autoriser via l'Active Directory. Les systèmes OT peuvent se connecter à l'AD via Windows Domain-Join, LDAP / LDAPS ou Radius.

3.2 IAM BSA

Les données sont saisies via l'enregistrement des utilisateurs afin de créer de nouveaux comptes.

D'autres données sont collectées au sein du composant IAM BSA Sailpoint afin de paramétrer les rôles et les autorisations des organisations et de les faire correspondre aux groupes AD. Au fur et à mesure de l'évolution des autorisations, les données sont automatiquement rapprochées entre les systèmes IAM BSA, AD et MFA.

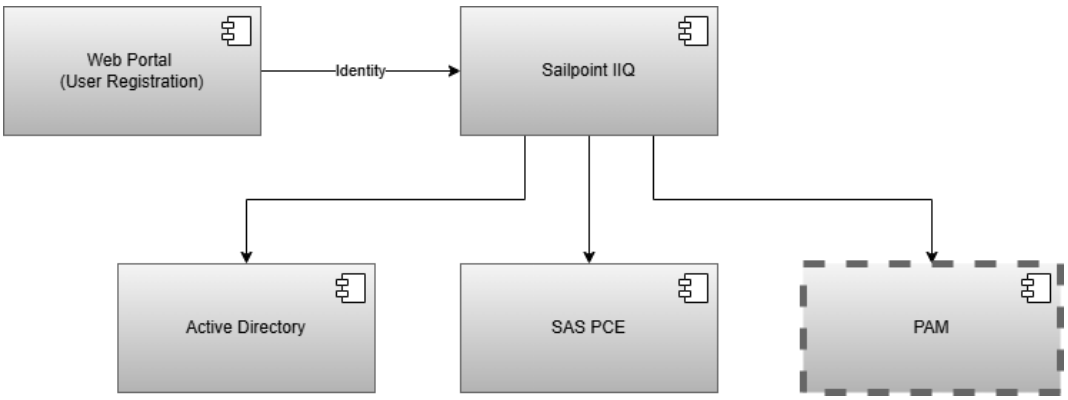

Fig. 3.2 Flux de données Identity

Les photos d'identité sont stockées sur un serveur IIS protégé qui leur est propre. La base de données Sailpoint Identity contient un lien vers la photo d'identité correspondante. Pour que les serveurs IIS de BD-A et BD-B soient au même niveau, ces répertoires avec les photos d'identité doivent être synchronisés entre BD-A et BD-B. Cela permet de garantir un basculement en cas d'erreur.

Les données saisies ne sont traitées qu'au sein du système IAM BSA.

3.3 Autorisations d'accès et rôles

Dans le réseau IP EES, le contrôle d'accès basé sur les rôles (RBAC) est mis en œuvre. Il s'agit d'un concept de sécurité qui structure l'accès aux ressources sur la base du rôle d'un utilisateur. RBAC permet une gestion efficace et granulaire des autorisations en attribuant des droits d'accès sur la base de rôles définis.

Le RBAC est basé sur les principes de base suivants :

1. **Lien utilisateur-rôle :** chaque utilisateur est associé à un ou plusieurs rôles définis. Un rôle représente un groupe de tâches ou de responsabilités. Cette attribution s'effectue dans l'IAM BSA ;

2. **Lien entre les rôles et les groupes d'**autorisation : chaque rôle est doté des groupes d'autorisation nécessaires (appelés ci-après servicegroup) ; cette attribution s'effectue également dans l'IAM BSA. Les servicegroups sont provisionnés dans l'AD à partir de l'IAM BSA ;
3. **Autorisations sur les systèmes** : dans les systèmes, les servicegroups sont autorisés en conséquence.

Les rôles sont exclusivement gérés dans IAM BSA. De même, les servicegroups sont en principe gérés dans l'IAM BSA et provisionnés dans l'Active Directory en tant que Domain Local Security Groups.

Les services tels que LDAP, LDAPS, Kerberos, etc. continuent d'être fournis via la Microsoft AD.

3.4 Interaction entre IAM BSA et Active Directory

Dans l'ensemble du réseau IP EES, la gestion des utilisateurs est centralisée via l'IAM BSA (produit : Sailpoint) dans les services de base. Cela signifie qu'un utilisateur d'une unité territoriale peut commander de manière autonome un compte d'utilisateur via le portail (Self Registration Portal). Celui-ci est ensuite créé, géré / autorisé (attribution de utilisateurs à des rôles / rôles à des groupes de services) et bloqué / supprimé par l'unité territoriale concernée via l'IAM BSA. L'IAM BSA approvisionne alors automatiquement les utilisateurs et les Service Groups nouvellement créés dans l'Active Directory de l'unité territoriale concernée, des VMZ-CH et des services de base.

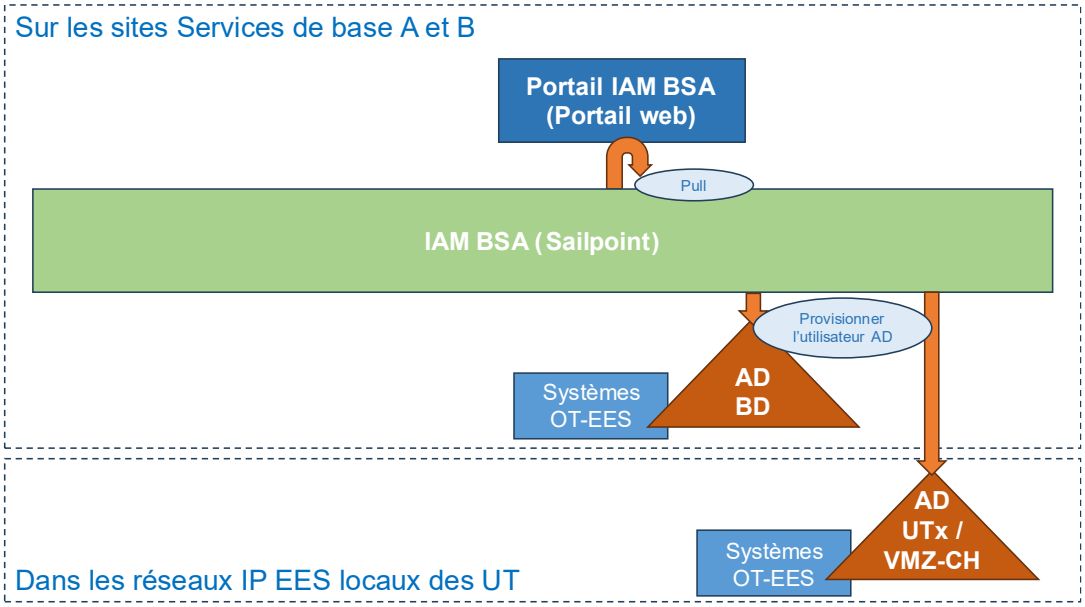

Fig. 3.3 Interaction IAM - AD

Les « users » et les « servicegroups » sont gérés dans l'IAM BSA et provisionnés dans l'AD dans les OU standardisés « IAM Managed Users » et « IAM Managed Service Groups ».

Tous les AD sont indépendants les uns des autres (pas de « forest » supérieure) : Les unités territoriales, les services de base et la VMZ-CH ont chacun leur propre forest et leur domaine du même nom. Les domaines sont autonomes et ne sont pas trustés entre eux.

Des identités séparées sont disponibles pour l'environnement de production (PROD) et l'environnement d'intégration (INT).

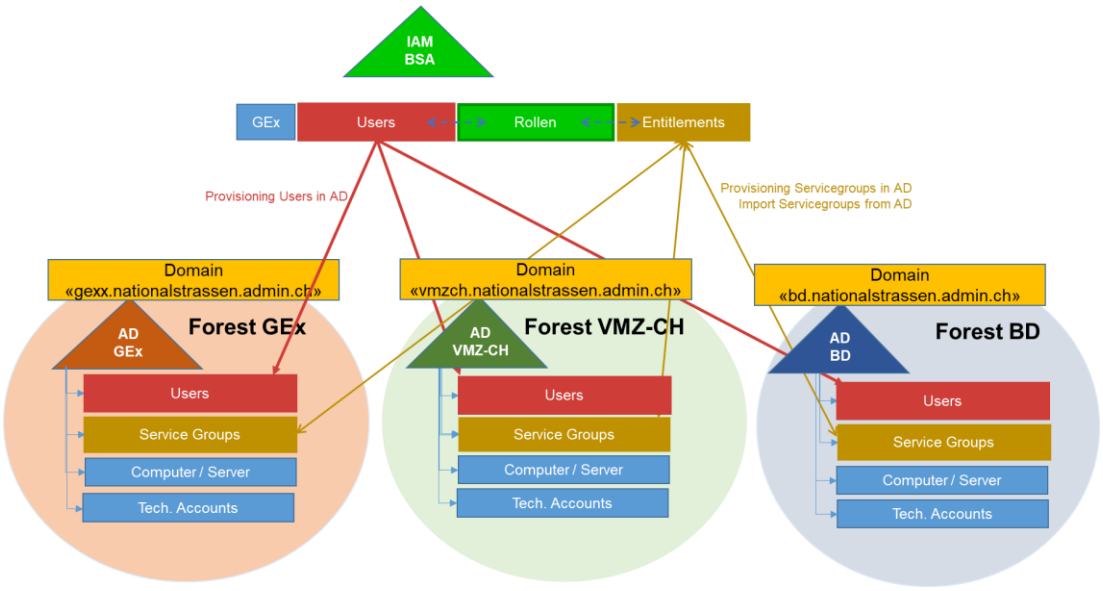

Fig. 3.4 Intégration IAM - AD

Ci-dessous, un aperçu des rôles impliqués dans le processus « autorisation d'accès » et de leur interaction.

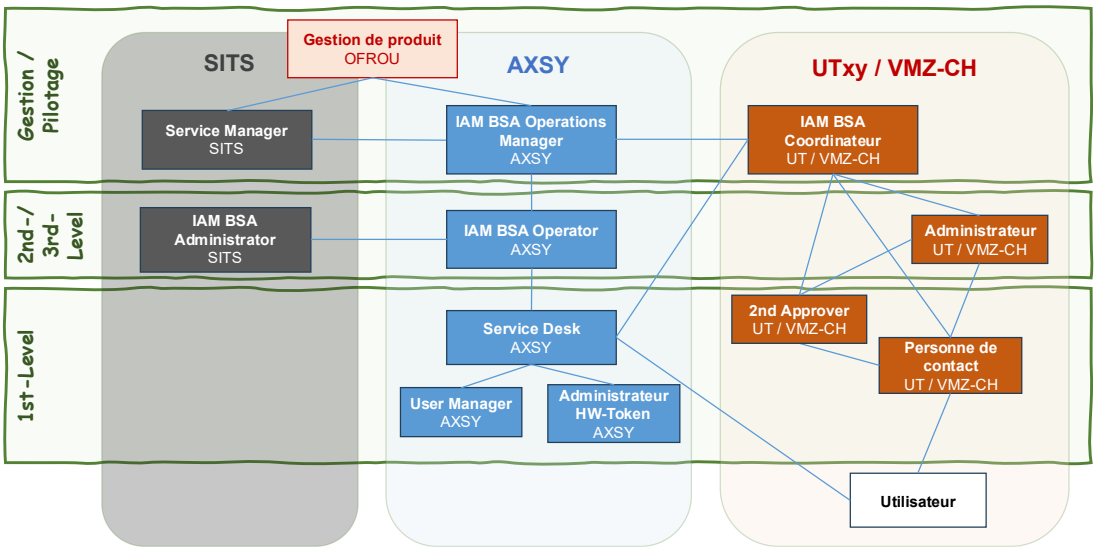

Fig. 3.5 Interaction des rôles dans l'exploitation

Tab. 3.1 Aperçu des désignations de rôles

Rôle au sein d'IAM BSA	Description
Utilisateur	Personne qui a besoin d'un ou de plusieurs comptes pour accéder aux applications au sein de l'OFROU.
Personne de contact	Identifie les demandeurs de comptes et approuve ou rejette leurs demandes d'enregistrement.
2nd Approver	Niveau d'autorisation supplémentaire qui doit approuver les demandes en tant que 2e instance, comme par exemple les demandes d'enregistrement de personnes externes.
Administrateur UT / VMZ-CH	Responsable de la gestion d'une unité territoriale (attribution de rôles, révocation de rôles, ajout et suppression d'utilisateurs, etc.) Connaît les compétences des collaborateurs concernant les domaines d'activité locaux.

Tab. 3.1 Aperçu des désignations de rôles

Rôle au sein d'IAM BSA	Description
Coordinateur IAM BSA dans zone d'exploitation	Recueille et trie les nouvelles exigences, les modifications, les questions et les résultats concernant IAM BSA dans l'UT / VMZ-CH, y répond lui-même dans la mesure du possible et interagit pour les autres avec l'IAM BSA Operations Manager (AXSY). Responsable de la définition, de l'attribution et de la description des rôles AD pour les applications concernées.
Service desk	Support 1st level pour les utilisateurs. Escalade à l'intégrateur et retour d'information aux utilisateurs.
User Manager	Gère les informations / attributs des utilisateurs tels que le nom, l'adresse e-mail, etc. dans Sailpoint (par ex. en cas de changement de nom). Ce rôle ne nécessite pas de connaissances approfondies au sein de l'application IAM BSA (Sailpoint).
Administrateur de tokens physiques	Gère les tokens physiques nécessaires pour accéder à certains services / applications par le biais de MFA et les attribue aux utilisateurs dans SAS PCE et les envoie.
IAM BSA Operator	Ce rôle requiert un savoir-faire approfondi au sein de l'appli cation IAM BSA et une compréhension de bout en bout de la solution. Possède des autorisations étendues dans les différents composants IAM BSA (Sail-point, Thales SAS, PAM, RAS). Identifie, analyse et résout les problèmes dans le système IAM BSA existant. Assiste aux demandes de 2nd et 3rd level. Surveille le monitoring.
IAM BSA Operations Manager	Interface technique entre l'intégrateur et le prestataire de services d'exploitation externe (AXSY), coordination des domaines spécialisés dans le domaine des services IAM BSA. Planifier, surveiller et documenter les changements dans le domaine IAM BSA ; Coordination avec les services de l'infrastructure de base.
IAM BSA Administrator	Peut contrôler et modifier les détails et les fonctions de l'application IAM BSA qui sont liés au système.

3.5 Durée de conservation et effacement

Les identités sont seulement désactivées - pas supprimées. Il n'y a donc en principe pas de suppression dans l'IAM BSA, ni de durée de conservation limitée. Une identité n'est supprimée qu'en cas de décès.

En revanche, les copies précédentes des documents d'identité renouvelés seront supprimées après un renouvellement réussi.

3.6 Web-Portail

Le portail web IAM BSA est une application web accessible au public, qui est exploitée dans les services de base. Le portail web permet aux utilisateurs de saisir un enregistrement d'utilisateur ou une réinitialisation de mot de passe.

3.7 MFA

Le système MFA ajoute un deuxième facteur d'authentification, par exemple lors de l'établissement d'une connexion VPN. Au sein du système MFA, les communications sont cryptées et sécurisées à l'aide de certificats. Les utilisateurs du système MFA peuvent ainsi se connecter en toute sécurité.

3.8 Directives relatives au mot de passe

Les mots de passe doivent être mis en place conformément à la directive OFROU 13030 GS 18.

3.9 Accès à distance aux services du réseau IP EES

3.9.1 Accès via VPN

Pour accès à distance aux services du réseau IP EES il est possible d'accéder depuis Internet aux jumpstations des sites BD via Checkpoint Mobile Agent, en passant par les sites de services de base BD-A et BD-B.

Il est alors possible d'accéder aux systèmes cibles depuis les jumpstations :

- Utiliser un navigateur web pour accéder à une application web ;
- Utiliser une connexion RDP (logiciel bureau à distance) pour accéder aux autres serveurs.

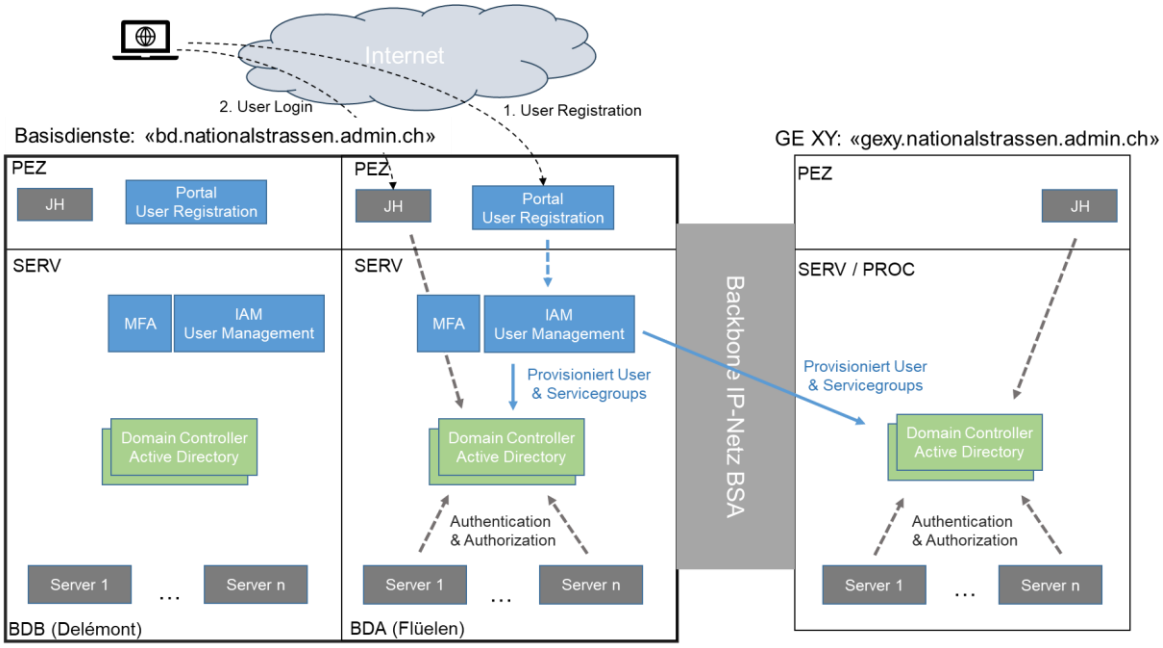

Fig. 3.6 Accès via Internet au réseau IP EES

4 Glossaires

4.1 Glossaire réseau IP EES

Begriff/Abkürzung	Terme/abréviation	Signification
ASTRA	OFROU	Office fédéral des routes
Ausrüstung/Gerät	Équipement/ appareil	Tout type d'équipement actif dans l'environnement EES (même sans connexion au réseau IP EES).
Backbone/BB	Backbone/BB	Mise en réseau nationale de tous les réseaux partiels fournie par la Confédération (L3 par l'OFIT, transmission par la FAC).
BD (Basisdienste)	BD (services de base)	Services de base du réseau (outil IPAM, DNS, sources de temps, ...) pour l'ensemble du réseau IP EES.
BSA	EES	Equipements d'exploitation et de sécurité
Client/Host Server	Client/Hôte serveur	Termes TIC généraux (pas de signification spécifique à l'EES), utilisation dans la description des protocoles.
Endgerät	équipement terminal	Tout type d'équipement sur un userport du réseau IP EES.
F/Filiale	F/filiale	Filiale (cinq unités régionales de l'OFROU)
GE	UT	Unité territoriale (11 unités organisationnelles supracantonales exploitant leur propre réseau IP IP EES UT).
IP-Netz BSA	réseau IP EES	Un réseau IP pour les équipements d'exploitation et de sécurité des routes nationales comprenant les éléments suivants (sous-réseaux) : - 11 Réseaux IP EES UT ; - le réseau IP EES Backbone (backbone de l'administration fédérale) ; - Liens avec la VMZ-CH ; - Connexions avec les centres de données EES ; - Connexions aux BD (services de base du réseau IP EES BD).
Netzwerk-ausrüstung	équipement réseau	Tout (y compris firewall, systèmes de gestion, ...).
Netzwerkelement	élément réseau	Équipement de transmission actif uniquement (routeur ou commutateur).
PEZP	PEZP	Proxy de zone d'application des politiques.
RFC	RFC	Les RFC (Requests for Comments) contiennent des documents techniques et organisationnels sur l'Internet. Certains RFC, mais pas tous, constituent des normes Internet et doivent répondre à des exigences élevées et représenter un consensus communautaire de l'Internet Engineering Task Force (IETF).
Router	routeur	Il s'agit toujours des routeurs MPLS des anneaux de raccordement, sinon (p. ex. routeurs spoke-site) mentionnés explicitement.
RZ(-BSA)	RZ(-BSA)	Centre de calcul EES
(Netzwerk-) Segment	Segment (de réseau)	Segments selon OFROU 83040 par installation (partielle) (généralement VLAN)
Switch	commutateur	Il s'agit toujours des éléments réseau L2 du niveau accès, sinon mentionné en conséquence
UVEK		Département fédéral de l'environnement, des transports, de l'énergie et de la communication
VDV	VDV	Interconnexion des données de trafic : liaisons des unités territoriales entre elles et avec les centres de calcul EES ; sont remplacées par le réseau IP EES Backbone.
VMZ(-CH)	VMZ(-CH)	Centre de gestion du trafic
(Netzwerk-)Zone	Zone (réseau)	Au sens de la NSP de la Confédération Si003 (séparé par PEZ).

4.2 Glossaire IAM BSA

Terme/abréviation	Signification
2FA	2 Facteur d'authentification
AD	Active Directory
BD-A, BD-B	Services de base du site A, services de base du site B
DNS	Service de noms de domaine
Forest	Ensemble de domaines Active Directory avec un catalogue global, un schéma de répertoire et une configuration de répertoire communs.
IAM	Gestion des identités et des accès
IP	Protocole Internet
IIS	Serveur d'information Internet
MFA	Authentification multifactorielle
MS	Microsoft
OFIT	Office federal de l'informatique et des télécommunications
PAM	Gestion des accès privilégiés
PKI	Public Key Infrastructure
RAS	Service d'accès à distance
RBAC	Contrôle d'accès basé sur les rôles
RDP	Remote Desktop Protocol – protocole de bureau à distance
SAS PCE	Service d'authentification SafeNet Private Cloud Edition
TIC	Technologies de l'information et de la communication

Bibliographie

Instructions et directives de l'OFROU

[1] Office fédéral des routes, instructions OFROU 73006 « OT Security Governance, Sécurité des systèmes EES », www.astra.admin.ch.

[2] Office fédéral des routes, directive OFROU 13030 « OT Security », www.astra.admin.ch.

Liste des modifications

Édition	Version	Date	Modifications
2025	1.00	19.06.2025	Entrée en vigueur de l’édition 2025 (versions allemande, italienne et française).