Informations
Technik
Zentrum Bund

ITZBund, Postfach 30 16 45, 53196 Bonn An alle Clearing Center per E-Mail	Dienstsitz Frankfurt am Main Wilhelm-Fay-Str. 11, 65936 Frankfurt Bearbeitet von: RA Riesler Tel. 0800/8007-545-1 servicedesk@itzbund.de 09.03.2026

Betreff: ATLAS – Info 0926/2026

Bezug:
GZ: **06010302#0015#0926 – 0926/2026** (bei Antwort bitte angeben)

ATLAS-Allgemein

Bekanntgabe über bevorstehende Anpassungen der IPsec-Parameter für die Anbindung an die Fachverfahren ATLAS/EMCS über einen öffentlichen VPN-Zugang

Sehr geehrte Damen und Herren,

im Rahmen der kontinuierlichen Weiterentwicklung unserer Sicherheitsstandards informieren wir Sie hiermit über bevorstehende Anpassungen der IPsec-Parameter für öffentliche VPN-Zugänge.

1 - Abkündigung von IKEv1

Aus Gründen der IT-Sicherheit sowie zur Einhaltung aktueller Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) werden wir die Unterstützung von IKEv1 zum **01. Sept. 2026** einstellen.

Ab diesem Zeitpunkt werden **ausschließlich Verbindungen über IKEv2** unterstützt. Wir bitten Sie daher, bestehende IKEv1-Tunnel rechtzeitig, in terminlicher Absprache mit uns, auf IKEv2 umzustellen. Beachten Sie dabei bitte, dass aufgrund der Menge an Teilnehmern ein entsprechender terminlicher Vorlauf von zwei Wochen einzuplanen ist.

2 - Erweiterung der IKEv2-Parameter (GCM, 256 Bit)

Zum **1. April 2026** ergänzen wir zudem unsere Parameter für IKEv2 um den kryptografisch stärkeren GCM-Algorithmus.

Folgende VPN-Parameter werden nunmehr seitens des ITZBund unterstützt:

Phase 1 – IKE SA	
IKE Version	IKEv2 only
Encryption / AEAD	AES-256-GCM / AES-256-CBC
PRF	SHA384 / SHA512
Diffie-Hellman (DH / ECDH)	DH Group 20 (ECP384) / DH Group 21 (ECP521)
Authentication Method	Pre-Shared Key (PSK)
Lifetime (IKE SA)	86400 s (24 Stunden)

Phase 2 – IPsec SA	
ESP Encryption / AEAD	AES-256-GCM
Integrity	SHA256 (CBC) / - bei AES-GCM nicht erforderlich –

PFS	DH Group 20 (ECP384) /
	DH Group 21 (ECP521)
Mode	Virtual Tunnel Interface (VTI)
Lifetime (IPsec SA)	4608000 kilobytes/
	3600 s (1 Stunde)

Wir empfehlen zusätzlich die Implementierung einer Dead Peer Detection (DPD).

Die Erweiterung erfolgt zur weiteren Härtung der Kommunikationssicherheit sowie zur Sicherung der BSI–Konformität.

Erforderliche Maßnahmen:

Bitte prüfen Sie:

- ob aktuell noch IKEv1 eingesetzt wird
- ob Ihre Systeme die genannten IKEv2 Parameter (vorzugsweise AES-256-GCM und SHA512) unterstützen
- ob ggf. Firmware- oder Software-Updates erforderlich sind

Für Rückfragen oder zur Abstimmung eines Migrationszeitplans stehen wir Ihnen selbstverständlich gerne zur Verfügung. Bitte eröffnen Sie zur Kontaktaufnahme ein Ticket über unseren Servicedesk (Betreff: IPSec-Anpassungen ATLAS/EMCS-Anbindungen Kommsys).

Vielen Dank für Ihre Unterstützung bei der weiteren Absicherung unserer gemeinsamen Kommunikationsinfrastruktur.

Im Auftrag
Bösenberg
Dieses Dokument wurde elektronisch erstellt und ist ohne Unterschrift gültig.