Tillåtna säkerhetsprotokoll för transportkryptering - Tillämpning av TLS

1.1 Tillägg till It-säkerhetsbilaga

inera
Ett företag inom SKR

Innehållsförteckning

Revisionshistorik

VERSION	DATUM	FÖRFATTARE	KOMMENTAR
1.0	2022-02-28		Beslutad version för Tjänsten Säker digital kommunikation.
1.1	2022-05-03		Mutual-TLS mellan AP-operatörers Accesspunkter samt förtydligande av kravet på TLS certifikat.
	2023-03-22		Kraven integreras i It-säkerhetsbilaga

1 Tillägg

Nedan anges tillägg till avsnitt 2.2.1 Tillåtna säkerhetsprotokoll för transportkryptering i IT-säkerhetsbilaga till Regelverk för anslutning till Säker digital kommunikation.

Användning av TLS säkerhetsprotokoll enligt 'DIGG eDelivery – Transportprofil AS4'[4] med SDK-federationens anpassning A2, A2 och A3 ska tills vidare göras enligt:

Krav	**Tillägg**
Endast acceptera för SDK specificerade certifikatsutgivare (CA)	Tillägg enligt 'DIGG eDelivery – Transportprofil AS4'[4]', avsnitt 2.4 Användning av TLS - A1 **Godkända certifikatsutgivare för TLS-trafik:** TLS ska användas och endast utgivaren SITHS ska användas. Rotcertifikat: SITHS e-id Root CA v2 (2019-05-15 till 2049-09-15) Certifikatsutgivare: SITHS e-id Function CA v1 TLS-konfigurationen ska vara åtminstone av "grade A" enligt SSL Labs gradering.
Tillämpa autentiseringsmetod enligt SDKs specifikation	Tillägg enligt 'DIGG eDelivery – Transportprofil AS4'[4]', avsnitt 2.4 Användning av TLS - A2 **Godkänd autentiseringsmetod:** Accesspunktsfunktioner som agerar i eDelivery transportinfrastruktur ska använda "Two-way TLS" baserad på trust till "SITHS e-id Funktion CA v1" (ej enskilda certifikat).
Använda för SDK specificerade kommunikationsportar för SSL/TLS	Tillägg enligt 'DIGG eDelivery – Transportprofil AS4'[4]', avsnitt 2.4 Användning av TLS - A3 **Godkända portar för SSL/TLS-trafik:** Port 443 ska användas för TLS