Úprava konfigurace kryptografických prostředků ISZR

Seznam cipher suites, které budou povoleny na vnějším rozhraní ISZR po provedení změn:

CIPHER SUITE	ID	BITS	PROTOCOL	ENCRYPT	KEYX	MAC
TLS_RSA_WITH_AES_128_CBC_SHA	0x00002F	128	TLS1.2	AES	RSA	SHA
TLS_RSA_WITH_AES_256_CBC_SHA	0x000035	256	TLS1.2	AES	RSA	SHA
TLS_RSA_WITH_AES_128_CBC_SHA256	0x00003C	128	TLS1.2	AES	RSA	SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256	0x00003D	256	TLS1.2	AES	RSA	SHA256

Ověření přístupu z ISZR po provedení změn:

- Zkontrolujte, zda váš AIS má povoleny protokoly TLS 1.0 a 1.1 pro komunikaci s ISZR v testovacím prostředí.
    - Jestliže ano, pak protokoly TLS 1.0 a 1.1 ve vašem AIS pro komunikaci s ISZR vypněte pro testovací prostředí.
- Zkontrolujte, zda váš AIS má pro komunikaci s ISZR v povolen protokol TLS 1.2 pro testovací prostředí.
    - Jestliže ne, pak ve vašem AIS povolte pro komunikaci s ISZR v testovacím prostředí TLS 1.2.
- Zkontrolujte, zda váš AIS má pro komunikaci s ISZR pro testovací prostředí povolenu alespoň jednu cipher suite z výše uvedeného seznamu.
    - Jestliže ne, pak ve vašem AIS povolte pro komunikaci s ISZR v testovacím prostředí alespoň jednu cipher suite z výše uvedeného seznamu.
- V období od 1. 8. 2017 do 31. 12. 2017 otestujte v testovacím prostředí, že váš AIS bezproblémově komunikuje s ISZR i s takto změněným nastavením kryptografických protokolů.
- Do 2. 1. 2018 proveďte analogické změny vašeho AIS, jaké jste udělali v testovacím prostředí, i v produkčním prostředí.