

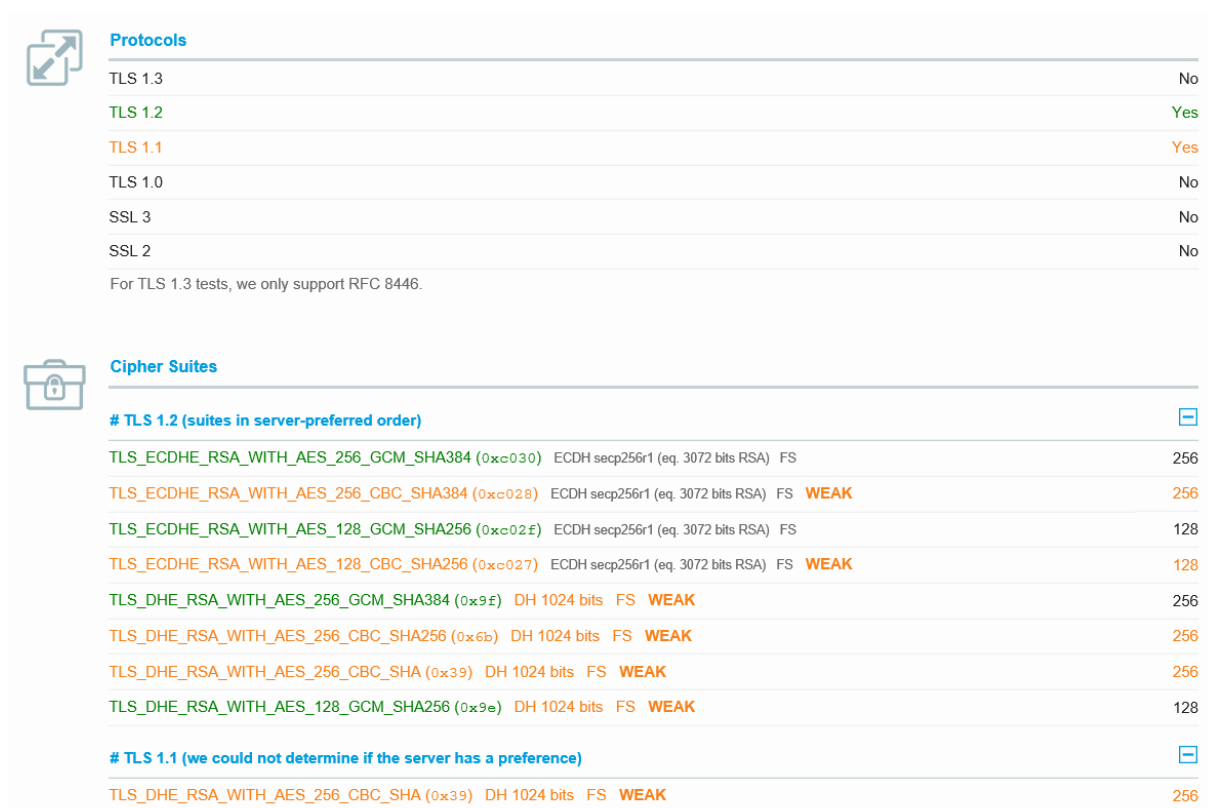
Technické odporúčania pre komunikáciu so systémom eKasa

1. Sieťová komunikácia

HTTP protokol a TLS

Použitie protokolu HTTP/1.1 je povinné. Ďalej je povinné použitie chráneného prenosu údajov cez kryptografický protokol Transport Layer Security minimálne vo verzii 1.1. Akékoľvek potrebné zmeny vo vzťahu k iným legislatívnym rámcom¹ budú reflektované v revízii tohto dokumentu.

SSL spojenie umožňuje uzavretú množinu šifriec:



The screenshot shows a security console with two sections: 'Protocols' and 'Cipher Suites'. The 'Protocols' section lists TLS 1.3 (No), TLS 1.2 (Yes), TLS 1.1 (Yes), TLS 1.0 (No), SSL 3 (No), and SSL 2 (No). A note below states: 'For TLS 1.3 tests, we only support RFC 8446.' The 'Cipher Suites' section is divided into two groups. The first group, '# TLS 1.2 (suites in server-preferred order)', lists several suites with their bit lengths and strengths: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (256), TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (256, WEAK), TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (128), TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (128, WEAK), TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (256, WEAK), TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (256, WEAK), TLS_DHE_RSA_WITH_AES_256_CBC_SHA (256, WEAK), and TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (128, WEAK). The second group, '# TLS 1.1 (we could not determine if the server has a preference)', lists TLS_DHE_RSA_WITH_AES_256_CBC_SHA (256, WEAK).

Protocol	Status
TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	No
SSL 3	No
SSL 2	No

For TLS 1.3 tests, we only support RFC 8446.

Cipher Suite	Strength
# TLS 1.2 (suites in server-preferred order)	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	256 WEAK
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	128 WEAK
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0xc9f)	256 WEAK
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0xc6b)	256 WEAK
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0xc39)	256 WEAK
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0xc9e)	128 WEAK
# TLS 1.1 (we could not determine if the server has a preference)	
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0xc39)	256 WEAK

SOAP protokol

Pre komunikáciu so systémom e-kasa je nutné použiť SOAP protokol vo verzii 1.2². Akékoľvek potrebné zmeny vo vzťahu k iným legislatívnym rámcom³ budú reflektované v revízii tohto dokumentu.

¹ Výnos č. 55/2014 Z. z. Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy

² <https://www.w3.org/TR/soap12-part1/>

³ Výnos č. 55/2014 Z. z. Ministerstva financií Slovenskej republiky o štandardoch pre informačné systémy verejnej správy

2. Firewall

V prípade využívania firewall je potrebné nastaviť nasledovné:

- zariadenia pre evidenciu bločkov: 194.1.0.21, 194.1.0.19, 213.81.129.184, 213.81.129.187
- eKasa zóna: 213.81.129.185, 213.81.129.188, 194.1.0.20, 194.1.0.22