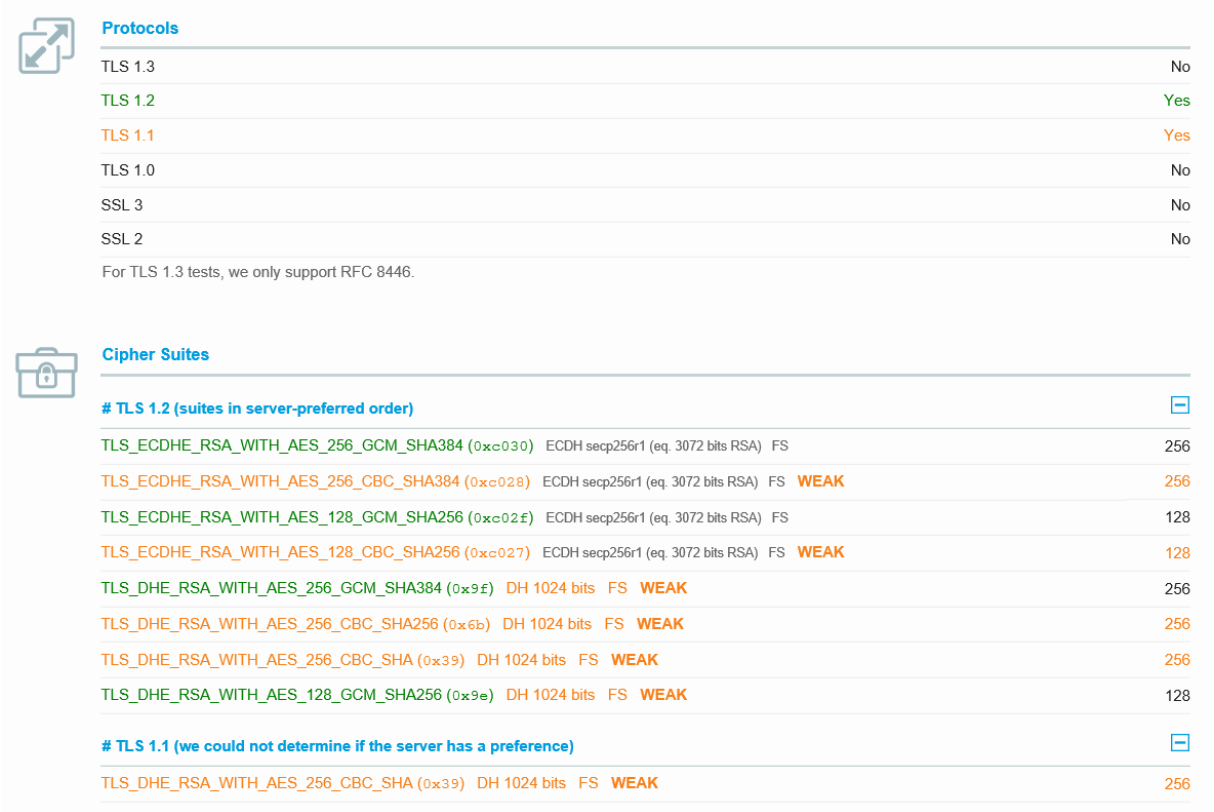
Technické odporúčania pre komunikáciu so systémom eKasa

1. *Sieťová komunikácia*

HTTP protokol a TLS

Použite 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 rámcom[1] budú reflektované v revízii tohto dokumentu.

SSL spojenie umožňuje uzavretú množinu šifier:



Protocols

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 Suites

 # TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 1024 bits FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 1024 bits FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 1024 bits FS **WEAK**	128

 # TLS 1.1 (we could not determine if the server has a preference)

TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits FS **WEAK**	256

SOAP protokol

Pre komunikáciu so systémom eKasa je nutné použiť SOAP protokol vo verzii 1.2[2]. Akékoľvek potrebné zmeny vo vzťahu k iným legislatívnym rámcom[3] budú reflektované v revízii tohto dokumentu.

---

[1] Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 o štandardoch pre informačné technológie verejnej správy

[2] https://www.w3.org/TR/soap12-part1/

[3] Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 o štandardoch pre informačné technológie 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

3. Odporúčania pre použitie znakov v názvoch tovarových položiek

Pre minimalizáciu rizika zablokovania prijatia bločku v systéme eKasa aplikačným firewallom odporúčame nasledovné:

1. V názvoch tovarových položiek používať len malé a veľké písmená (vrátane diakritiky), číslice a tzv. bezpečné znaky, t.j. interpunkčné znamienka (. , ? !), podtrhovník, pomlčku a matematické znaky (+ - * /).
2. Je možné použiť aj iné znaky, pri týchto znakoch však môže za určitých okolností dôjsť ku zablokovaniu bločku, hlavne pri kombinácii viacerých takýchto znakov bezprostredne za sebou. Problémy môže spôsobiť aj bezprostredná kombinácia viacerých bezpečných znakov, ako aj kombinácia viacerých bezpečných a iných znakov.
3. Pokiaľ je u konkrétneho zákazníka nevyhnutná potreba používať iné znaky alebo kombinácie znakov, odporúčame pred uvedením do prevádzky tieto znaky a/alebo ich kombinácie otestovať v integračnom prostredí eKasa, pokiaľ budú prepustené, v prevádzke budú takisto prepustené.

Periodicita plánovaných prevádzkových úkonov

Upozorňujeme, že finančná správa môže/bude v nasledujúcich prípadoch realizovať prevádzkové úkony spojené s údržbou systému podľa nasledujúcej tabuľky. Vo všetkých prípadoch bude o tom v dostatočnom časovom predstihu informovať.

Prevádzkový úkon údržby	Periodicita	Dopad
Výmena SSL certifikátov pre Virtuálnu registračnú pokladnicu	1 rok, exspirácia 17.3.2022	Nutnosť vydať nové verzie mobilných aplikácii VRP (Pokladnica) dostupných v obchodoch Google Play a App Store.
Výmena systémového podpisového certifikátu pre odpovede zo systému eKasa do online registračnej pokladnice eKasa klient	1 rok, exspirácia 23.2.2021	Podmienky pre overenie podpisu odpovede sú uvedené v kapitole 2.8. v dokumente Popis integračného rozhrania systému e-kasa
Aktualizácia komunikačných protokolov, šifier	Podľa potreby	Štandardy sieťovej komunikácie sú uvedené v kapitole 1.5 v dokumente Popis integračného rozhrania systému e-kasa
Zmena IP adries	Podľa potreby	Povolenie výnimiek pre nové IP adresy v prípade používania Firewallu

Životné situácie na strane podnikateľa alebo výrobcu/dovozcu/distribútora pokladničných programov

Upozorňujeme podnikateľov, resp. výrobcov/dovozcov/distribútorov pokladničných programov na nižšie uvedené životné situácie:

Životná situácia	Periodicita	Dopad
Koniec platnosti autentifikačných údajov online registračnej pokladnice eKasa klient.	2 roky od vydania	Potrebné požiadať o nové autentifikačné údaje v eKasa zóne podnikateľa.
Zaplnenie chráneného dátového úložiska.	odhad 2 až 6 rokov v závislosti od veľkosti CHDU	Potrebná výmena CHDU, pokladnica upozorní vopred na dochádzajúcu kapacitu CHDU.
Koniec platnosti rozhodnutia o certifikácii pokladničných programov a chránených dátových úložísk.	najviac 5 rokov odo dňa právoplatnosti rozhodnutia	Koniec platnosti certifikátu ORP sa viaže len na výrobcu ORP, ktorý ak chce pokračovať v predaji danej ORP, musí požiadať o certifikáciu a absolvovať certifikačný proces. Koniec platnosti certifikátu sa nevzťahuje na používateľa ORP (podnikateľa), ktorý môže ORP s exspirovaným certifikátom používať aj naďalej, a to až do doby, pokiaľ táto ORP bude spĺňať zákonné požiadavky.