Odporúčanie úradu k šifrovaniu emailov pre účely prenosu služby prístupu k internetu medzi poskytovateľmi

Úrad pre reguláciu elektronických komunikácií a poštových služieb vydal dňa 17. júna 2024 Vyhlášku č. 137/2024 Z.z. o podrobnostiach týkajúcich sa zmeny podniku poskytujúceho službu prístupu k internetu (ďalej len „**Vyhláška**“), kde v § 3 ods. 1 ustanovil, že komunikácia medzi podnikmi súvisiaca so zmenou podniku poskytujúceho službu prístupu k internetu sa uskutočňuje elektronickou poštou v štruktúre a formáte vhodnom pre automatizované spracovanie podľa prílohy alebo vo forme automatizovanej komunikácie spĺňajúcej požiadavky podľa prílohy. S ohľadom na citlivosť prenášaných údajov o účastníkovi je nutné posielať tieto údaje chránene v šifrovanej podobe, kde odosielateľ zašifruje odosielanú správu pomocou verejného kľúča uvedeného spolu s adresou podľa § 1 ods. 1 Vyhlášky. Zoznam adries elektronickej pošty odovzdávajúceho podniku alebo adresu automatizovanej platformy, ako aj verejný šifrovací kľúč možno nájsť na https://www.teleoff.gov.sk/urad/odbory-oddelenia/odbor-regulacie-elektronickych-komunikacii/zmena-podniku-poskytujuceho-internet/

Ako funguje šifrovanie e-mailov

Základné šifrovanie e-mailov zahŕňa výmenu šifrovacích kľúčov, ktoré sa generujú pomocou matematických algoritmov nazývaných jednosmerné funkcie. Každá kódovaná komunikácia používa spárovaný verejný kľúč, ktorý je dostupný komukoľvek na internete, a súkromný kľúč, ktorý pozná len príjemca. Tento typ systému šifrovania e-mailov sa nazýva infraštruktúra verejného kľúča alebo PKI.S/MIME (Secure/Multipurpose Internet Mail Extensions) je v súčasnosti štandard používaný pre zabezpečenie elektronickej pošty verejným kľúčom pre šifrovanie a podpisovanie MIME dát. Je to špeciálna verzia protokolu MIME - S/MIME (Secure MIME). S/MIME je na zozname internetových štandardov IETF.

Pre šifrovanie emailov medzi operátormi je najvýhodnejšie používať S/MIME štandard. Ide o štandard, ktorý umožňuje šifrovať a podpisovať vaše e-mailové správy pomocou kryptografie s verejným kľúčom. Pomocou S/MIME sa zaistí, že e-mailové správy budú dôverné, autentické a neupravené bez ohľadu na to, komu alebo kam budú odoslané.

Výhody:

1. Široká podpora poštových klientov
2. java knižnice (ale sú aj na iné jazyky) - https://github.com/simple-java-mail/java-utils-mail-smime)
3. CLI nástroj (napr. openssl), s ktorým je to jednoduché zašifrovať

Ako nato:

1.Vygenerovanie S/MIME certifikátu

Na túto komunikáciu je potrebné vytvoriť certifikát od certifikačnej autority. Napríklad

▪ https://eidas.disig.sk/sk/certifikaty/certifikat-pre-elektronicky-podpis/ .... platená služba

▪ https://order.emsign.com/freeSmime - tu je možnosť si ho vytvoriť na 1 rok zdarma

Príklad pre adresu: prenosinternetutst@xy.sk **(doména pre príklad „xy“)**

Na nasledujúcom príklade je vysvetlený postup, ako získať bezplatne certifikát na 1 rok cez sprievodcu na stránke emSign:

Najprv je potrebné cez https://order.emsign.com/freeSmime overiť emailovú adresu - klikom na overovací link sa dostaneme do ďalšieho kroku, kde treba naloadovať CSR, ktoré si treba predtým vytvoriť pomocou - napríklad OpenSSL.

Takže, nainštalovať OpenSSL a potom príkaz: (vid https://www.ssl.com/how-to/manually-generate-a-certificate-signing-request-csr-using-openssl/)

openssl req -newkey rsa:2048 -keyout prenosinternetutst@xy.sk.key -out prenosinternetutst@xy.sk.csr -subj "/C=SK/ST=Slovakia/L=Bratislava/O=XY/OU=FX/CN=prenosinternetutst@xy.sk/emailAddress=prenosinternetutst@xy.sk"

zapamätať si PEM, bude potrebné potom pri importovaní certifikátu.

Výsledok príkazu pre vytvorenie CSR sú súbory

▪ prenosinternetutst@xy.sk.csr - toto použijeme pre generovanie S/MIME certifikátu na stránke emSign - https://order.emsign.com/freeSmime

▪ **prenosinternetutst@xy.sk.key** - toto od nás bude požadovať importovacia procedúra, keď budeme importovať do email klienta

Následne použijeme csr file pre pokračovanie na emsign - tým pádom už len preklik na vygenerovanie certifikátu. Výsledok je zip súbor - napr. 5929894494_prenos_internetu_tst.zip, ktorý obsahuje:

▪ CA_emSign SMIME CA - G1.cer

▪ **EndEntity_prenosinternetutst@xy.sk.cer** - toto budeme importovať do email klienta

▪ RootCA_emSign Root CA - G1.cer

2. Import do poštového klienta

Podľa predchádzajúceho postupu bol vygenerovaný S/MIME certifikát určený na šifrovanú komunikáciu voči emailovej adrese prenosinternetutst@xy.sk. Ale samozrejme môže byť vygenerovaný aj pre gmailovú adresu.

▪ Treba mať nainštalovaného ľubovoľného emailového klienta (napr. Thunderbird, eM Client, MS Outlook)

▪ Napríklad pre https://cz.emclient.com/ - nastaviť si tam túto svoju emailovú adresu - viď Accounts

▪ následne v Settings potom naimportovať certifikát z bodu 1, ale spolu s privátnym kľúčom, teda tieto 2 veci: ▪ **prenosinternetutst@xy.sk.key**

▪ **EndEntity_prenosinternetutst@xy.sk.cer**

▪ Môže byť, že sa vyžaduje vložiť súbor PKF12, takže tieto 2 súbory treba spojiť - napríklad prostredníctvom nástroja XCA (Windows aplikácia v MS Store) ▪ spustiť XCA

▪ File → New Database: vybrať si lokalitu, kde si XCA založí svoj súbor

▪ Záložka Private Keys → Import: nájdeme svoj private key (súbor .key)

▪ Záložka Certificates → Import: nájdeme svoj certifikát (súbor .cer)

▪ Záložka Certificates → Export: nastavíme si cestu do nového "pfx" súboru a vo výberovníku vyberieme PKCS #12 a potvrdíme

3. Odosielanie správy podnikom - odosielateľom:

Verejný certifikát od iného operátora, s ktorým chceme šifrovane komunikovať, si treba stiahnuť z webovej stránky podniku poskytujúceho službu prístupu k internetu, alebo zo stránky úradu a takisto ho treba naimportovať. Ním budú zašifrované odchádzajúce správy k danému podniku.

Pre odoslanie správy z klienta je následne možné použiť podpísanie aj zašifrovanie (odporúčané je používať obe možnosti):

eM Client

Thunderbird:

Upozornenie: Maily treba posielať ako PLAIN TEXT, aby nedošlo k problémom s formátovaním a dopĺňaniu rôznych html tagov od rôznych email klientov. Malí operátori to totiž môžu posielať manuálne a tam by k takýmto veciam mohlo dochádzať.

4. Prijatie správy podnikom - adresátom:

S použitím súkromného kľúča poštový klient u adresáta dešifruje prijatú správu. Počítač príjemcu použije súkromný kľúč na dešifrovanie správy.

Poznámka:

Šifrovanie e-mailov samo o sebe nezabráni zachyteniu správ škodlivými stranami. Bez súkromného kľúča sa však údaje v ňom budú javiť ako zmätené a pre neoprávnenú osobu nečitateľné.