Pomoč pri izbiri standarda za zagotavljanje varnosti pri izmenjavi elektronske pošte z dm-om

Več informacij o šifriranju elektronske pošte pri dm-u najdete na: https://www.dm.si/digitalno-podpisovanje

Protokol oz. standard	Načela delovanja	Prednosti	Predpostavke
S/MIME (ga prednostno uporablja tudi dm)	Šifriranje elektronskih sporočil s standardom S/MIME. V tem primeru dm za šifriranje elektronskih sporočil potrebuje potrdila S/MIME za vse elektronske naslove poslovnih partnerjev. Posledično se vsa sporočila, poslana na te elektronske naslove, samodejno šifrirajo. Vsako elektronsko sporočilo, poslano iz dm-a, vsebuje tudi pripadajoče potrdilo pošiljatelja v obliki digitalnega podpisa. Tako lahko prejemnik tudi nazaj pošlje šifrirano elektronsko sporočilo.	Standard S/MIME je med podjetji najbolj razširjen način šifriranja elektronske pošte in ga podpirajo skoraj vsi e-poštni odjemalci oz. programi za izmenjavo elektronske pošte (npr. Microsoft Outlook, Mozilla Thunderbird, Lotus Notes, Apple Mail). Za uporabo šifriranja S/MIME tako ni potrebna dodatna programska oprema in pri šifriranju ne nastajajo dodatni stroški. Potrdila S/MIME lahko izdajo agencije oz. overitelji digitalnih potrdil (CA, ang. Certificate Authority) ali uradi za registracijo (RA, ang. Registration Authority), ki delujejo kot posredniki med strankami in overitelji, ali jih brezplačno ustvarite sami.	Uporabniki morajo pred pošiljanjem zaupnih elektronskih sporočil (z občutljivimi podatki) aktivirati šifriranje. Za vsak e-poštni predal, ki je vključen v komunikacijo, je treba pridobiti (naročiti ali ustvariti) potrdilo S/MIME in ga namestiti v uporabnikovem programu za izmenjavo elektronske pošte. Pri vsaki spremembi kontaktnih oseb ali elektronskih naslovov je treba proces ponoviti, saj le-ta ne poteka samodejno. Če uporabnik do e-poštnega predala dostopa tudi s pametnim telefonom ali tablico, je potrdilo S/MIME treba namestiti tudi na teh napravah. Tako bo lahko šifrirana elektronska sporočila bral tudi na telefonu ali tablici.
PGP	Šifriranje posamičnih elektronskih sporočil s standardom PGP. Podobno kot pri standardu S/MIME morajo biti dm-u za vse elektronske naslove poslovnega partnerja, ki so vključeni v komunikacijo, na voljo (javni) ključi PGP. Poslovni partner pa prejme (javne) ključe PGP za dm-ove elektronske naslove.	Ključe PGP lahko brezplačno ustvarite sami. Standard je združljiv s sistemi OpenPGP, Autocrypt in pEp.	Za uporabo standarda PGP morate namestiti dodatno programsko opremo, kot sta npr. vtičnik Enigmail ali program Gpg4win. Za uporabo standarda PGP veljajo enake predpostavke kot pri uporabi standarda S/MIME.
S/MIME s potrdili za domeno ali PGP s ključi za	Ta princip je podoben standardoma S/MIME in PGP, le da se tu uporablja samo eno potrdilo oz.	S potrdilom S/MIME za domeno ali s ključem PGP za domeno se lahko šifrirajo vsa sporočila, poslana na	Ker programi za izmenjavo elektronske pošte načeloma ne sprejmejo potrdil za domene, je za šifriranje elektronskih sporočil

domeno (ga prednostno uporablja tudi dm)	ključ za šifriranje vseh elektronskih naslovov ene domene. Postopek je implementiran na [1]prehodu za šifriranje e-poštnih sporočil.	elektronske naslove ene domene (npr. domene dm.si). Posledično tudi spremembe kontaktnih oseb ali elektronskih naslovov ne pomenijo dodatnega dela. Če se za zaupnost elektronske pošte uporablja tak varnostni sistem, se uporabnik sam ne ukvarja s šifriranjem svoje elektronske pošte, saj le-to poteka na ravni e-poštnih prehodov.	treba iskati rešitev na ravni e-poštnih prehodov. Če takšnega šifriranja nimate, a ga želite imeti, morate upoštevati stroške nakupa, namestitve in licenc.
TLS	Med e-poštnim prehodom poslovnega partnerja ter e-poštnim prehodom dm-a se vzpostavi varna povezava, preko katere potem poteka izmenjava e-poštnih sporočil.	Šifriranje je treba vzpostaviti samo enkrat in samodejno zajame vsa elektronska sporočila, posredovana med poslovnim partnerjem in dm-om. Prednost takšnega šifriranja na ravni prenosa je tudi ta, da uporabniku pri pošiljanju zaupnih elektronskih sporočil z občutljivimi podatki ni treba misliti na šifriranje, saj do tega pride samodejno. Prav tako ni treba uporabniku ničesar naknadno spreminjati, saj šifriranje poteka pregledno na ravni e-poštnih prehodov.	Ker je pri šifriranju po standardu TLS šifrirana samo komunikacija do strežnika, kjer prejemnik ponovno lahko prebere elektronsko sporočilo, mora biti ta strežnik na voljo tudi poslovnemu partnerju. To izključuje delovanje e-poštnih prehodov preko storitev Shared Hosting Provider oz. Hosted Email Security Services. Vsi e-poštni strežniki, vključeni v komunikacijo, morajo imeti vedno na voljo veljavna potrdila agencije oz. overitelja digitalnih potrdil.
Priponka kot šifrirano elektronsko sporočilo	Zaupno sporočilo je poslano kot priponka, ki je zaščitena z geslom in priložena elektronskemu sporočilu. Ta standard uporabljate vedno, ko z elektronsko pošto posredujete občutljive podatke in ni na voljo drugih varnostnih standardov.	Za odpiranje takih šifriranih elektronskih sporočil ne potrebujete posebnega znanja ali dodatne programske opreme.	Za odpiranje takšnega elektronskega sporočila je vsakič treba vnesti geslo. To elektronsko sporočilo lahko kot besedilo shranite v svojem programu za izmenjavo elektronskih sporočil. Uporabnik mora imeti zanesljiv sistem za upravljanje z gesli (Passwort Management), saj če ne pozna svojega lastnega gesla, šifriranih elektronskih sporočil, ki mu jih je poslal dm, ne bo mogel prebrati.

[1] E-poštni prehod omogoča različnima e-poštnima storitvama, da komunicirata med seboj.