Podrška za donošenje odluke o izboru metode šifriranja u komunikaciji s dm-om

Više informacija o šifriranju e-mailova u dm-u pronaći ćete na https://www.dm.hr/informacije-o-sifriranju-e-mailova-456828

Metoda	Princip	Prednosti	Uvjeti
S/MIME **(prvi izbor dm-a)**	E-mailovi se šifriraju na bazi industrijskog standarda S/MIME. U tu svrhu dm-u je za svaku e-mail adresu društava koja su poslovni partneri neophodan certifikat S/MIME koji osigurava da su svi mailovi poslani na adrese poslovnih partnera automatski šifrirani. Prilikom slanja dm svakom e-mailu pridružuje certifikat S/MIME u obliku elektroničkog potpisa. Na taj način je omogućeno da se dm-u kao primatelju e-mailovi vraćaju u šifriranom obliku.	S/MIME je najrasprostranjenija metoda za šifriranje-mailova u korporativnom okruženju, a podržavaju ga gotovo svi uobičajeni programi za elektroničku poštu (npr. Microsoft Outlook, Mozilla Thunderbird, Lotus Notes, Apple Mail). Pritom nema potrebe za dodatnim programima ni troškovima. Certifikati S/MIME se mogu pribaviti od komercijalnih certifikacijskih tijela ili samostalno generirati kako bi bili besplatni.	Kod osjetljivih e-mailova koje je potrebno zaštiti korisnici moraju prije slanja voditi računa o aktivaciji šifriranja. Za svaki poštanski sandučić uključen u komunikaciju mora se naručiti ili generirati certifikat S/MIME koji se potom lokalno postavlja u program za elektroničku poštu korisnika. Proces postavljanja certifikata mora biti ponovno proveden u slučaju promjene kontakt-osoba ili e-mail adrese. Budući da proces nije automatiziran, trajno nastaje trošak za aktivnost postavljanja certifikata. Ako je pretincu elektroničke pošte paralelno potrebno pristupati putem pametnog telefona ili tableta, certifikat S/MIME mora biti postavljen i na ovim uređajima kako bi se i na njima mogli čitati šifrirani e-mailovi.
PGP	E-mailovi se šifriraju pojedinačno na bazi internetskog standarda PGP. Istovjetno kao i kod metode S/MIME dm-u se moraju staviti na raspolaganje PGP-ključevi e-mail adresa uključenih u komunikaciju. Poslovni partner zauzvrat dobiva PGP ključeve za e-mail adrese dm-a.	PGP-ključeve moguće je samostalno besplatno generirati. Metoda je kompatibilna s OpenPGP, Autocrypt i pEp.	U pravilu se mora instalirati dodatni program koji je podrška PGP-u, npr. Enigmail ili Gpg4win. Zahtjevi prethodno navedeni za metodu S/MIME jednako se primjenjuju na korištenje PGP-a.

S/MIME s certifikatom za domenu ili PGP s ključevima domene **(prvi izbor dm-a)**	Princip je sličan metodama S/MIME i PGP, no upotrebljava se samo jedan certifikat ili ključ koji se koristi za šifriranje svih adresa e-pošte domene. Ova se metoda u pravilu koristi na prevoditeljima protokola za šifriranje e-pošte.	Pomoću S/MIME-certifikata za domenu ili PGP-ključa domene mogu se šifrirati svi mailovi poslani na sve e-mail adrese neke domene (npr. na *@dm.hr). Promjena kontakt-osobe ili promjena e-mail adrese stoga ne uzrokuje dodatne troškove. Ako se koristi rješenje prevoditelj protokola (Gateway), za korisnike ne nastaje dodatni trošak, šifriranje se odvija transparentno putem prevoditelja protokola.	Za šifriranje e-mailova potrebno je rješenje prevoditelj protokola jer programi za e-mail u pravilu ne prihvaćaju certifikate za cijelu domenu. Ako se još ne raspolaže takvim prevoditeljem protokola, kupnjom nastaju troškovi postavljanja i troškovi licence.
Šifriranje prijenosa putem TLS-a	Između prevoditelja protokola za e-mailove društva koje je poslovni partner i prevoditelja protokola dm-a uspostavlja se šifrirana veza putem koje se potom sigurno prenose e-mailovi.	Šifriranje se provodi samo jednom i automatski obuhvaća sve e-mailove koji se prenose između poslovnog partnera i dm-a, što znači da nije moguće zaboraviti šifrirati osjetljive e-mailove. Za korisnika ne nastaje nikakav dodatni trošak. Šifriranje se provodi transparentno putem prevoditelja protokola za e-mailove.	Budući da se kod šifriranog prijenosa šifrira samo veza do sljedećeg poslužitelja na kojem se e-mailovi ponovno mogu čitati, taj sljedeći poslužitelj mora biti na raspolaganju isključivo poslovnom partneru. Navedeno isključuje da radom prevoditelja protokola za e-mailove upravljaju pružatelji usluge zajedničkog dijeljenja resursa poslužitelja (Shared Hosting Provider) odnosno usluge sigurnosti hostiranih e-mailova (Hosted Email Security Services). Svi poslužitelji koji sudjeluju u komunikaciji e-mailovima moraju u svakom trenutku raspolagati važećim certifikatima izdanim od strane ovlaštenog certifikacijskog tijela.

Šifriranje putem privitka	E-mail je zaštićen lozinkom, a šalje se kao privitak e-mailu koji ima funkciju nosača. Ova se metoda primjenjuje uvijek kada se putem e-maila treba prenijeti osjetljive podatke, a nije dostupan niti jedna druga metoda koja pruža sigurnost.	Za otvaranje šifriranog e-maila nisu neophodni posebni programi ili posebna znanja.	Za otvaranje e-maila se svaki puta unosi osobna lozinka, a potom se e-mail kao običan tekst može pohraniti u vlastitom programu za e-mail. Korisnik mora imati pouzdan sustav za upravljanje lozinkom jer bez poznavanja vlastite lozinke više neće moći čitati šifrirane mailove dm-a.