# Korisničko uputstvo

## *Dodavanje digitalnog potpisa i digitalno potpisivanje e-mailova u Microsoft Outlook*

## Sadržaj

Uvod ..... 3
1 Dodavanje automatskog digitalnog potpisa na odlazne e-mailove u Microsoft Outlook ..... 4
2 Dodavanje digitalnog potpisa na odlazne e-mailove u Microsoft Outlook po potrebi..... 9
3 Dodatne informacije i napomene.....11

# Uvod

„JP BH POŠTA“ d.o.o. Sarajevo je uspostavila infrastrukturu javnih kriptografskih ključeva - Public Key Infrastructure – PKI i djeluje kao ovjerilac u skladu s Zakonom o elektronskom potpisu. Kao ovjerilac, JP BH POŠTA pruža usluge izdavanja kvalificiranih elektronskih potvrda i upravljanja njihovim životnim ciklusom, kao i izdavanja kvalificiranih elektronskih vremenskih žigova pod imenom: Ovjerilac JP BH POŠTA.

Za uspješno korištenje kvalificirane elektronske potrvde (digitalnog certifikata) Ovjerioca JP BH Pošta potrebno je da su obezbjeđeni slijedeći preduslovi:

1. instalirani CA certifikati Ovjerioca JP BH Pošta na računaru korisnika
2. instaliran driver za token (tkz. middleware software)
3. PIN kod za pristup tokenu
4. Pristup Internetu za provjeru CRL liste

Kvalificirane elektronske potvrde koje izdaje Ovjerilac JP BH Pošta mogu se koristiti za potpisivanje elektronskih dokumenata kao i za autentikaciju prilikom pristupa nekoj računarskoj platformi (računar, server, web aplikacija i sl.). Digitalni dokumenti se mogu potpisati u okviru aplikacija Microsoft Office, Acrobat Reader, kao i aplikacija koje su namjenski razvijene za pružanje specifičnih servisa na Internetu (prijava poreza, podnošenje zahtjeva prema organima uprave,...). Internet servisi koji daju uslugu na teritoriji BiH prihvatanjem kvalificirane elektronske potvrde Ovjerioca JP BH Pošta  izvršili su sigurnu identifikaciju osobe koja je pristupila servisu.

Prije nego što počnemo sa digitalnim potpisivanjem dokumenata, još jednom ističemo da je potrebno da su ispunjeni gore navedeni preduslovi za prepoznavanje i korištenje tokena sa digitalnim certifikatom koji već posjedujete. Zamolite svoj tim za tehničku podršku da provjeri postavke digitalnog potpisa na vašem računaru, ukoliko je to potrebno.

Ovo uputsvo je namjenjeno za prikaz koraka potrebnih za digitalno potpisivanje dokumenta u programu Microsoft Oulook od vezije 2010 i dalje pomoću tokena ovjerioca JP BH Pošta sa kvalificiranom elektronskom potvrdom (digitalnim certifikatom). Prilikom samog potpsivanja potrebno je koristiti i PIN tokena, kako bi se izvršila dodatna autorizacija. Moguće su manja odstupanja među verzijama.

# 1 Dodavanje automatskog digitalnog potpisa na odlazne e-mailove u Microsoft Outlook

Digitalni potpis je elektronski, šifrovani pečat autentifikacije na digitalnim informacijama kao što su poruke e-pošte, makroi ili elektronski dokumenti poput onih kreiranih u Microsoft Word alatu. Potpis potvrđuje da informacije potiču od potpisnika i da nisu mijenjane.

Da biste kreirali digitalni potpis, potreban vam je certifikat za potpisivanje, koji dokazuje identitet. Kada pošaljete digitalno potpisan makro ili dokument, šaljete i svoj certifikat i javni ključ. Certifikate izdaje tijelo za certifikaciju, a kao i vozačka dozvola, mogu se oduzeti. Certifikat vrijedi određeni vremenski period, nakon čega potpisnik mora obnoviti ili dobiti novi potpisni certifikat kako bi utvrdio identitet. U slučaju ovjerioca JP BH Pošta navedeno se nalazi na tokenu.

Tijelo za izdavanje certifikata (CA), kao što je ovjerioc JP BH Pošta, je entitet sličan javnom bilježniku. Izdaje digitalne certifikate, potpisuje sertifikate radi provjere njihove valjanosti i prati koji su certifikati opozvani ili su istekli.

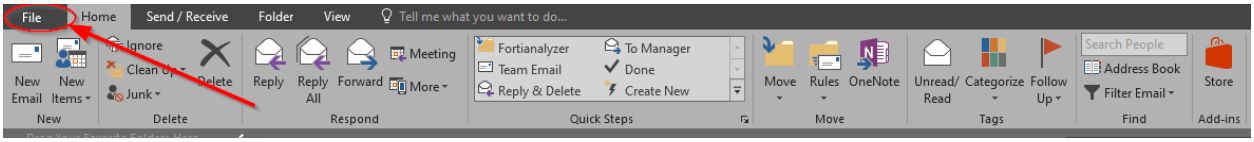
Digitalni potpisi služe da bi dali određene garancije, a to su:

- **Autentičnost** Potpisnik je potvrđen kao potpisnik.
- **Integritet** Sadržaj nije mijenjan ili neovlašten otkako je digitalno potpisan.
- **Neporicanje** Dokazuje svim stranama porijeklo potpisanog sadržaja. Odbijanje se odnosi na čin potpisnika koji negira bilo kakvu povezanost s potpisanim sadržajem.
- **Notarizacija** Potpisi u datotekama Microsoft Word, Microsoft Excel ili Microsoft PowerPoint, koji su vremenski označeni sigurnim serverom vremenskog žiga, pod određenim okolnostima, imaju valjanost ovjere.

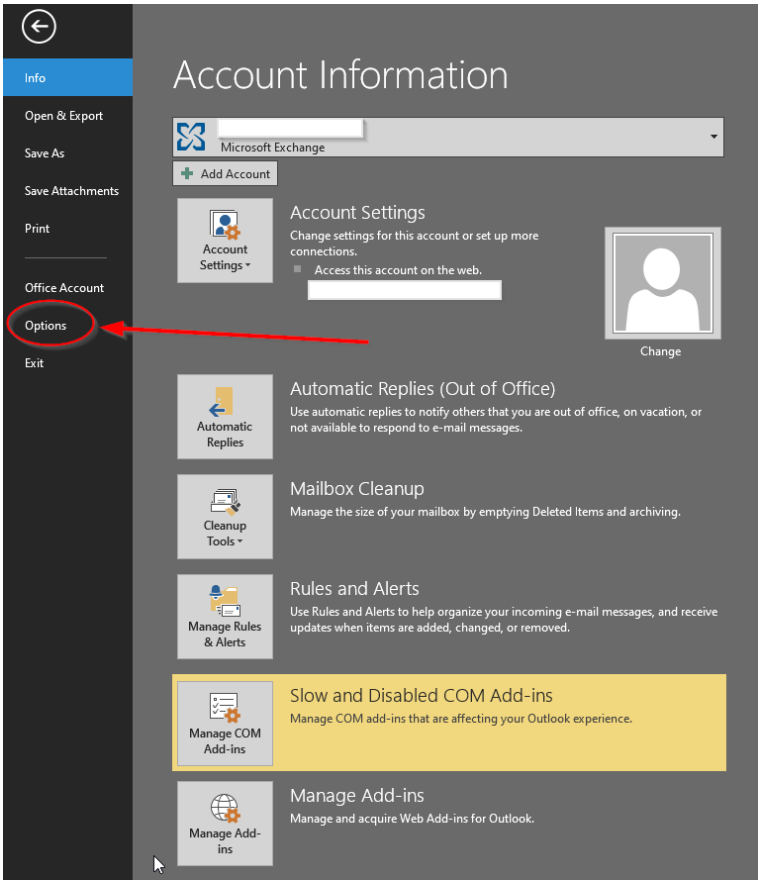
U narednim koracima prikazan je postupak za dodavanje digitalnog potpisa u određeni dokument, a u okviru Microsoft Office alata:

1. Za dodavanje digitalnog potpisa u dokument, potrebno je otvoriti Microsoft Outlook, sa već podešenom vlastitom e-mail adresom. Važno je napomenuti i istaknuti da certifikat koji će se koristiti za digitalno potpisivanje e-mailova mora u potpunosti odgovarati mail adresi koju koristimo, i za koju je Microsoft Outlook i podešen. U slučaju da adrese nisu identične nećemo biti u prilici podestiti i koristiti digitalni potpis.

   Do opcija za dodavanje digitalnog potpisa dolazimo klikom na **File** meni sa alatne trake (Slika 1), te nakon što nam se otvore dodatne opcije odabirom kratice Option/Opcije sa liste na lijevoj strani (Slika 2).

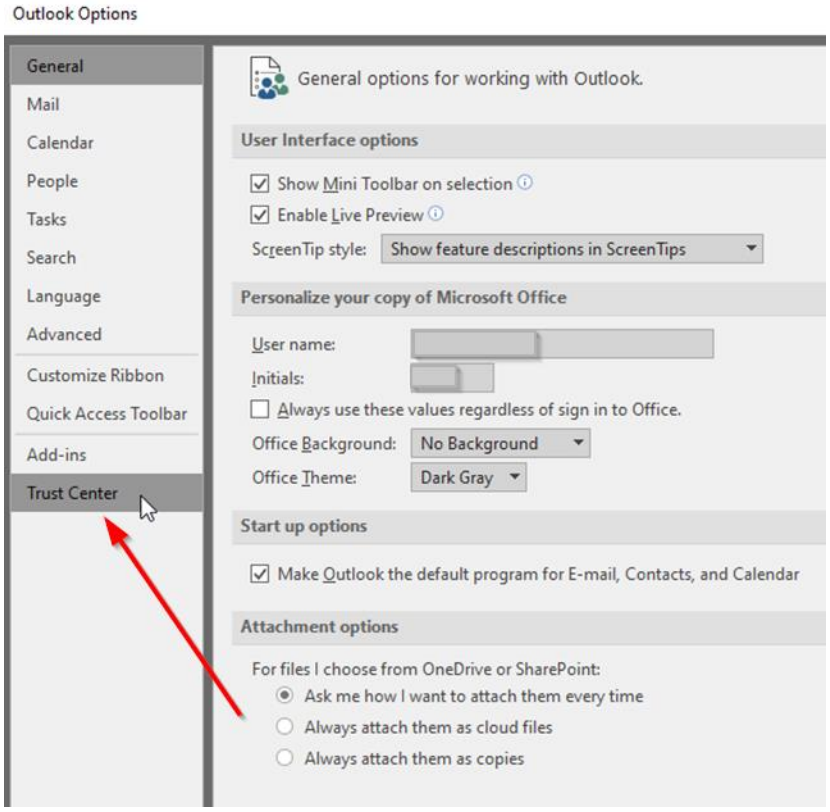



*Slika 1 - Meni traka sa alatima i opcija za dodavanje digitalnog potpisa*

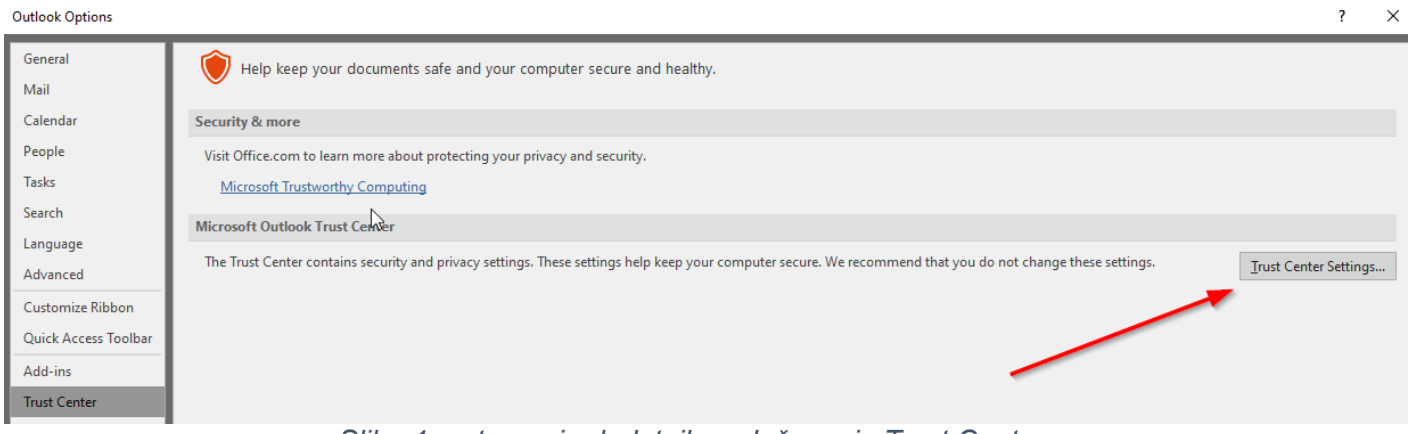



*Slika 2 - odabir dodatnih opcija*

2. Nakon što nam se otvori prozor sa dodatnim opcijama za podešavanje, sa liste na lijevoj strani biramo opciju **Trust Center/Centar povjerenja**. (Slika 3)
3. Za pristup opcijama za podešavanje digitalnog potpisa potrebno je još da se odabere dostupna opcija Trust Centre Settings/Postavke centra povjerenja. (Slika 4).




*Slika 3 - odabir opcije za dodavanje digitalnog potpisa*



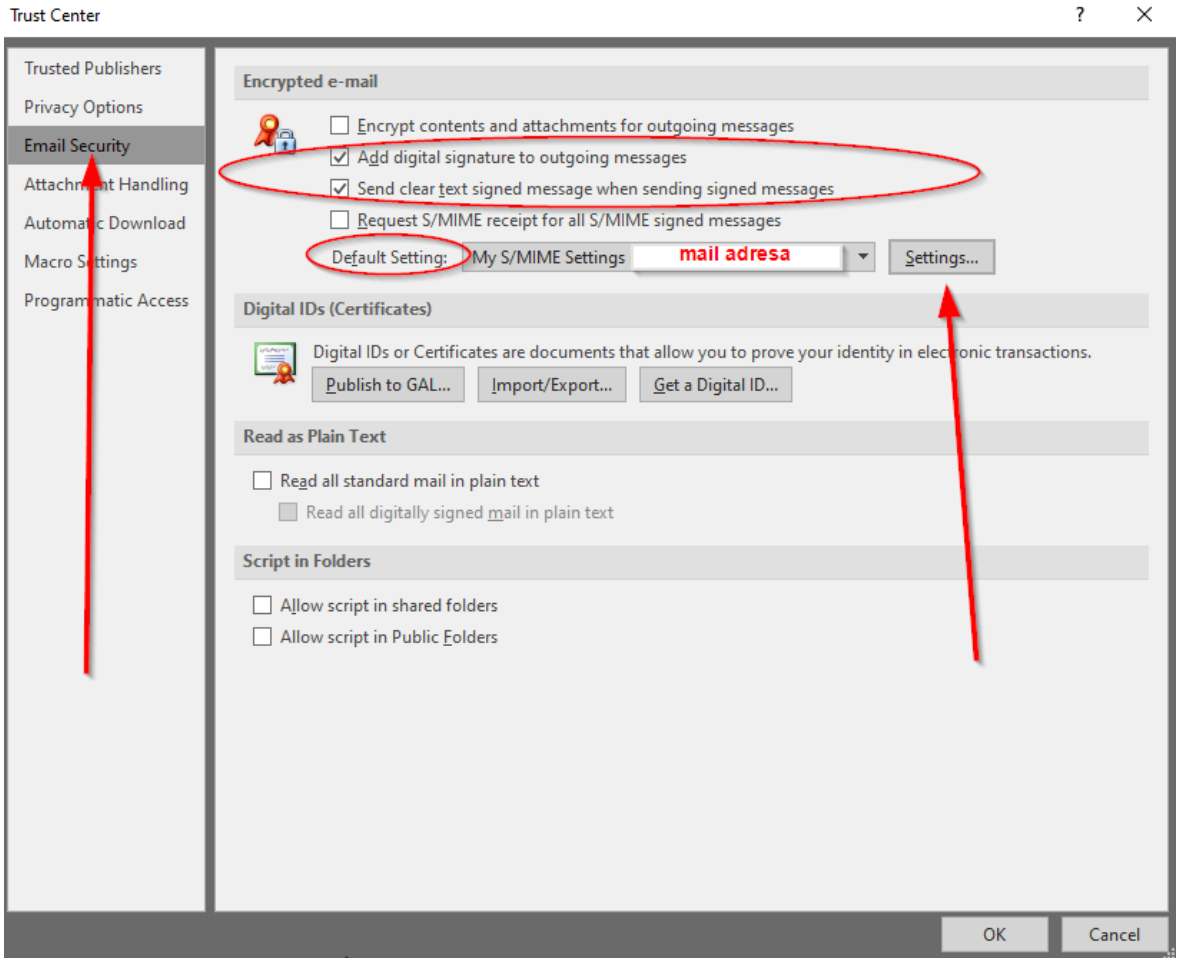

*Slika 4 – otvaranje dodatnih podešavanja Trust Center-a*

4. Završetkom prethodnog koraka otvara nam se prozor u kojem možemo podešavati postavke *Trust Center-a*. Od ponuđenih opcija na lijevoj strani potrebno je odabrati i označiti opciju **Email Security**. Označavanjem/odabirom ove opcije, sa desne strane nam se pojavljuju opcije za podešavanja sigurnosti e-maila, a između ostalog i one koje se tiču digitalnog potpisa.

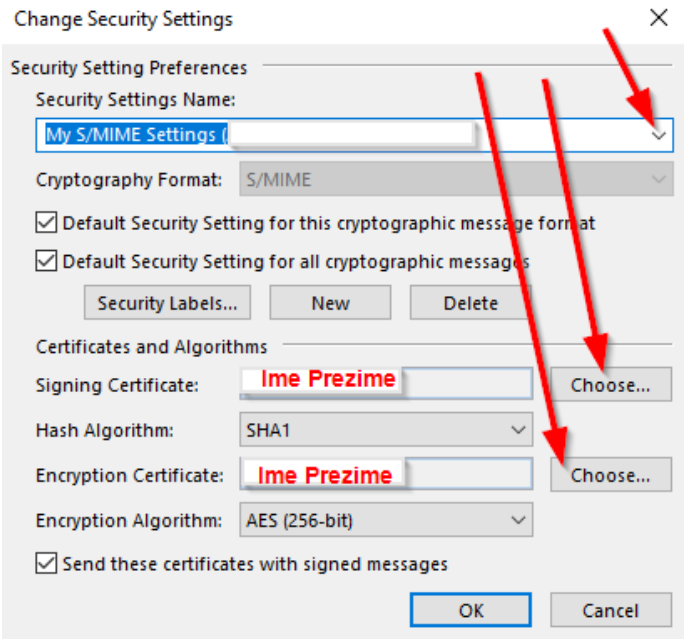
U dijelu *Encrypted e-mail/Enkriptovani e-mail*, ukoliko nam je token priključen na računar i isti ga prepoznaje, u dijelu **Default settings/Početne postavke** možemo vidjeti da li je već „učitan“ naš, potrebni certifikat. U polju za vrijednost (padajući meni) isti bi trebao biti prikazan na način da je prikazana, tj navedena e-mail adresa koja je upisana u sam certifikat. Ova adresa mora potpuno odgovarati našoj adresi, sa koje i šaljemo mailove.

Ukoliko imamo više dostupnih certifikata sa padajućeg menija možemo odabrati onaj odgovarajući. Za dodatna podešavanja vezno za certifikate koji će se koristiti za digitalno potpisivanje možemo kliknuti na opciju **Settings.../Postavke...** kada nam se otvori dodatni prozor sa dostupnim opcijama. U okviru ovih postavki možemo pregledati, promijeniti, odabrati koji certifikati se koriste za potpisivanje, za enkripciju podataka. (Slika 6)

U dijelu *Encrypted e-mail/Enkriptovani e-mail* pri samom vrhu imamo i nekoliko dostupnih opcija koje možemo uključiti ili isključiti. Za potrebe ovog uputstva posebno se osvrćemo na drugu dostupnu opciju *Add digital signature to outgoing messages*. Uključivanjem ove opcije podešavamo da se dodavanje digitalnog potpisa, tj potpisivanje odnosi na sve poslane mailove automatski. Ukoliko to želimo onda je potrebno da zakačimo kvadratić ispred ove opcije. (Slika 5)



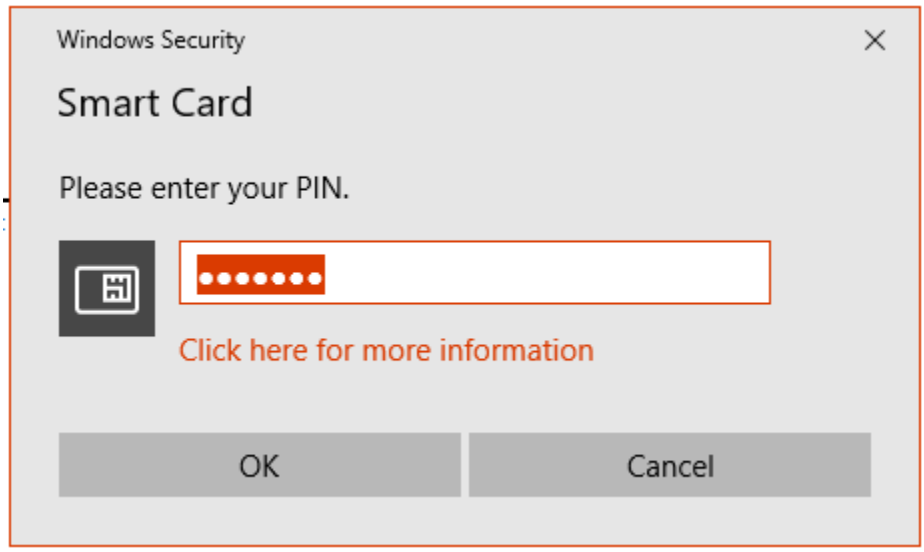

*Slika 5 - Linija za potpis u dokumentu*




*Slika 6 - prozor za promjenu sigurnosnih postavki*

5. Kada završimo podešavanja klikom na OK potvrđujemo ista. Dodatnim klikom na OK zatvaramo prozor sa podešavanjima te se vraćamo na početni prozor.

6. Ukoliko je zakačena opcija za automatko potpisivanje svih odlaznih poruka, iz koraka 4 (slika 5 – *Add digital signature to outgoing messages*, a što je tema ovog dijela uputstva, neophodno za okončanje potpisivanje e-mailova digitalnim potpisom jeste da izvršimo i autorizaciju, odnosno da unesemo PIN svog tokena u predviđeno polje, te potvrdimo klikom na OK. Naravno preduslov je da je token uključen u računar i vidljiv/dostupan samom operativnom sistemu računara. (Slika 7)

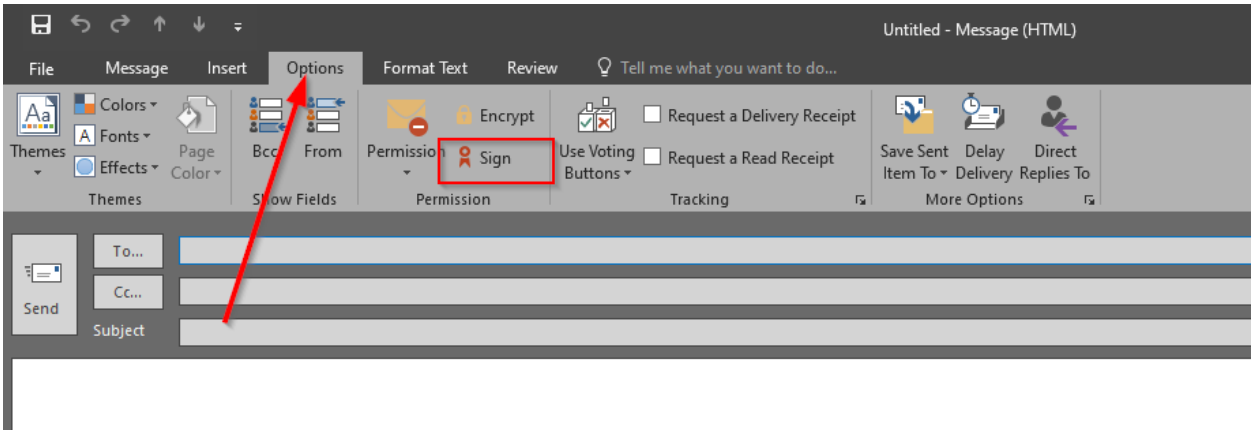



*Slika 7 - autorizacija tokena i certifikata unosom PIN-a*

# 2 Dodavanje digitalnog potpisa na odlazne e-mailove u Microsoft Outlook po potrebi

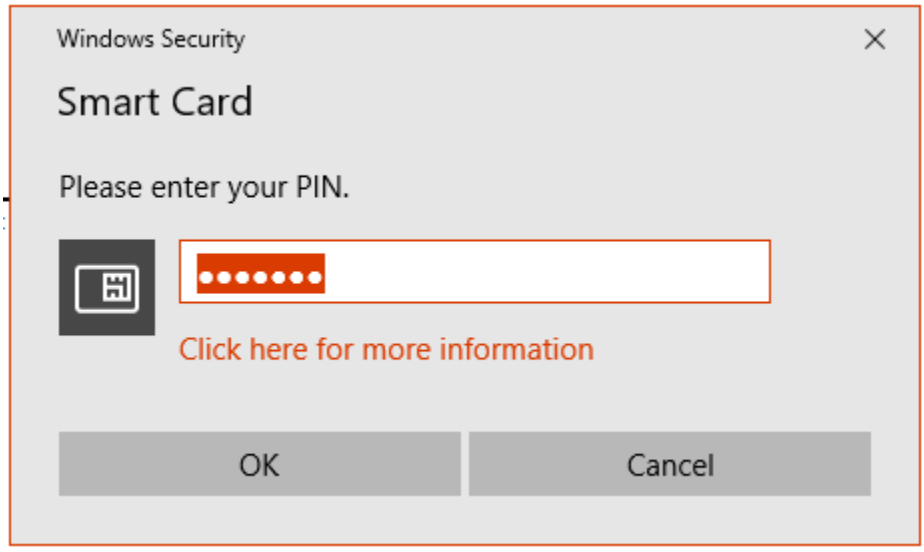
Ukoliko želimo selektivnu primjenu digitalnog potpisa na odlazne mailove, odnosno ne želimo da potpisujemo sve odlazne mailove već odabrane, možemo to uraditi prateći korake u nastavku. Koraci u nastavku nastavljaju se iza koraka 1 – 4 iz prethodnog dijela ovog upustva. Jedina razlika je u koraku 4, kada opciju za dodavanje automatskog digitalnog potpisa na sve odlazne mailove ostavljamo ne zakačenu. U tom slučaju potpis možemo primijeniti samo na željene odlazne mailove.

1. Klikom na **New Email/Novi Email** otvaramo prozor za kreiranje novog maila. Bitno je napomenuti da se kreiranje novog maila treba izvršavati u zasebnom iskačućem prozoru, sa svim dostupnim opcijama iz trake sa alatima.
2. Nakon što popunimo sve potrebno, uključujući adresu osoba kojima šaljemo mail, temu, određeni sadržaj, eventualne priloge, sa trake sa alatima biramo meni **Options/Opcije**. U dijelu *Permission/Permisije* primijetićemo opciju **Sign/Potpiši**. Klikom na ovu opciju i označavanjem iste uključujemo potpisivanje premeten email poruke digitalnim potpisom. Znači sve poruke na kojima prije slanja zakačimo/označimo navedenu opciju biće potpisane digitalnim potpisom. (Slika 8)




*Slika 8 - ručno potpisivanje emaila digitalnim certifikatom*

3. Neophodno za okončanje potpisivanje e-mailova digitalnim potpisom jeste da izvršimo i autorizaciju, odnosno da unesemo PIN svog tokena u predviđeno polje, te potvrdimo klikom na OK. Naravno preduslov je da je token uključen u računar i vidljiv/dostupan samom operativnom sistemu računara. (Slika 9)




*Slika 9 - autorizacija tokena i certifikata unosom PIN-a*

# 3 Dodatne informacije i napomene

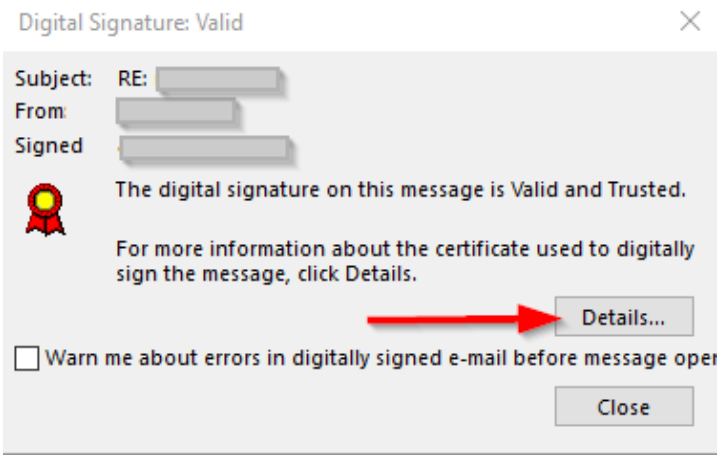
U slučajevima kada nam je uključeno automatsko potpisivanje digitalnim potpisom svih odlaznih poruka, a kada ne želimo da se na određenu to ne primijeni, moguće je ručno isključivanje potpisivanja digialnim potpisom te određene poruke. Ovo se radi na isti način kao i ručno uključivanje potpisivanja, s tim da ćemo primijetiti da je opcija **Sign/Potpiši** u *Preferences/Preferencije* dijelu *Options/Opcije* menija ovaj put već označena. Stoga je za isključivanje potpisivanja, a za razliku od ručnog dodavanja, sada potrebno ovu opciju isključiti.

Također, ukoliko šaljemo više mailova u kraćem vremenskom periodu, pri čemu ne zatvaramo Outlook aplikaciju niti isključujemo token iz računara, autorizaciju unosom PIN-a sistem će tražiti samo za prvi poslani mail. Ostali će biti potpisani bez dodatne autorizacije obzirom da sistem istu pamti kraći vremenski period.

Na sličan način kao i potpisivanje, moguće je uključiti i enkripciju podataka prilikom slanja. Opcije za uključivanje enkripcije vidljive su na slikama priloženim u ovom uputstvu. Međutim, bitno je napomenuti da za enkripciju podataka i namjena certifikata mora biti takva, odnosno certifikat na tokenu koji podjecujemo mora imati namjenu i za enkripciju podataka.

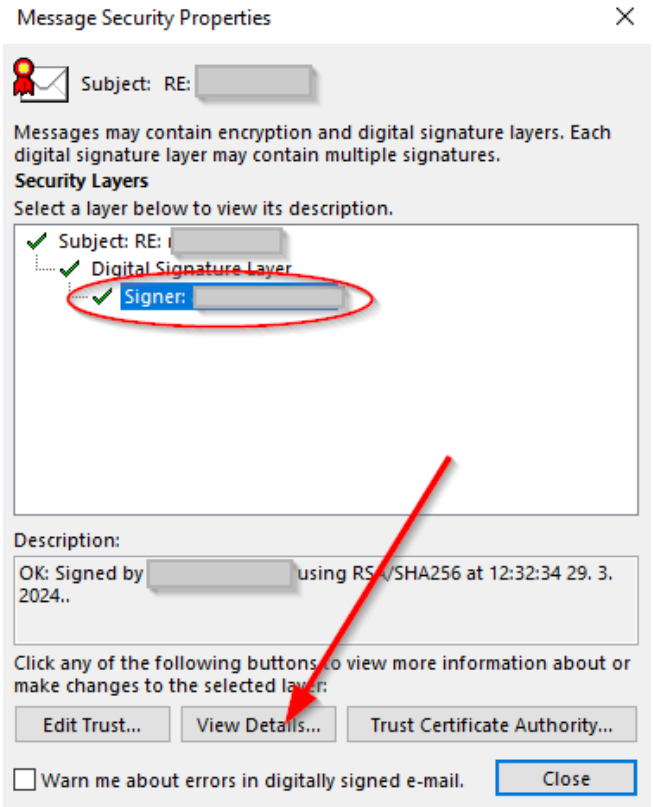
Kod email poruka potpisanih digitalnim potpisom, bez obzira da li se radi o odlaznim ili dolaznim porukama, može se utvrditi identitet potpisnika, kao i provjera o samom certifikatu. U okviru outlook aplikacije u pregledu poruka (*inbox* za dolazne, *sent items* za odlazne) poruke koje su digitalno potpisane isticu se simbolom  . Stoga ih je lako razlikovati od ostalih poruka koje nisu digtalno potpisane i koje nemaju prikazan navedeni simbol. Utvrđivanje potpisnika, provjeru certifikata i slično radimo na način da željenu poruku otvorimo u novom prozoru. Ispod osnovnih podataka o pošiljaocu poruke poput imena, prezimena, loga/slike, adrese sa koje je poslano i na koju se šalje, kod digitalno potpisanih poruka imamo i **Signed By/Potpisano od** statusnu liniju. Na istoj je navedena adresa sa koje se šalje poruka (a kako smo ranije navodili ona mora odgovarati adresi navedenoj u samom certifikatu), dok sa desne strane imamo ponovo prikazan gore navedeni simbol.

U ovom slučaju, kada nam je poruka otvorena u novom, zasebnom prozoru, bez obzira da li se radi o dolaznim ili odlaznim porukama, može se dvostrukim klikom na simbol, koji potvrđuje da su poruke digitalno potpisane, doći do dodatnih informacija o samom poptisniku, kao i do validnosti certifikata. Do dodatnih informacija o samom certifikatu može se doći klikom na Details.../Detalji... dugme. (Slika 10)



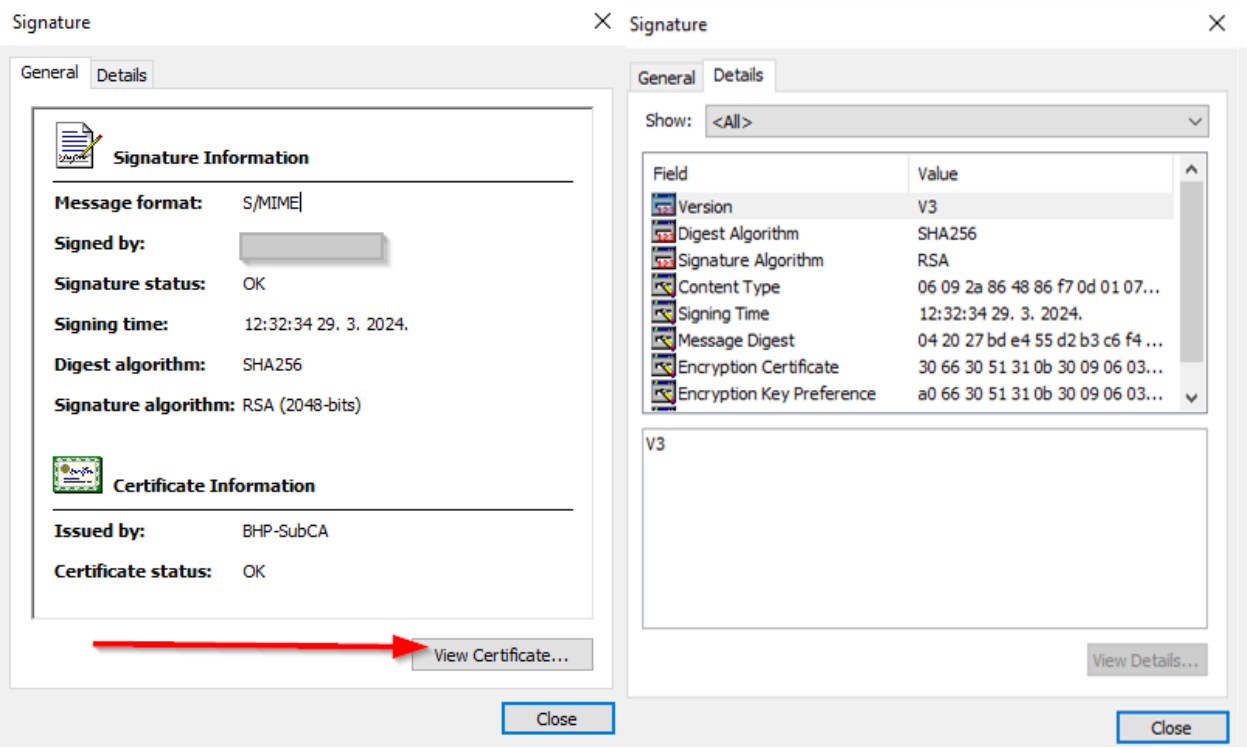

*Slika 10 - informacije o potpisniku, validnosti certifikata i samom certifikatu*

U okviru prozora za odlike sigurnosti potpisane poruke, koji nam se otvori možemo dobiti dodatne informacije o samom potpisniku, poput informacija o protkolu koji se koristio za potpisivanje, datumu kada je isto izvršeno. Također, označavanjem prvo same linije u kojoj je naveden potpisnik, te zatim klikom na **View Details.../Pogledaj detalje...** možemo doći do informacija o samom digitalnom potpisu koji je korišten za potpisivanje. (slika 11)



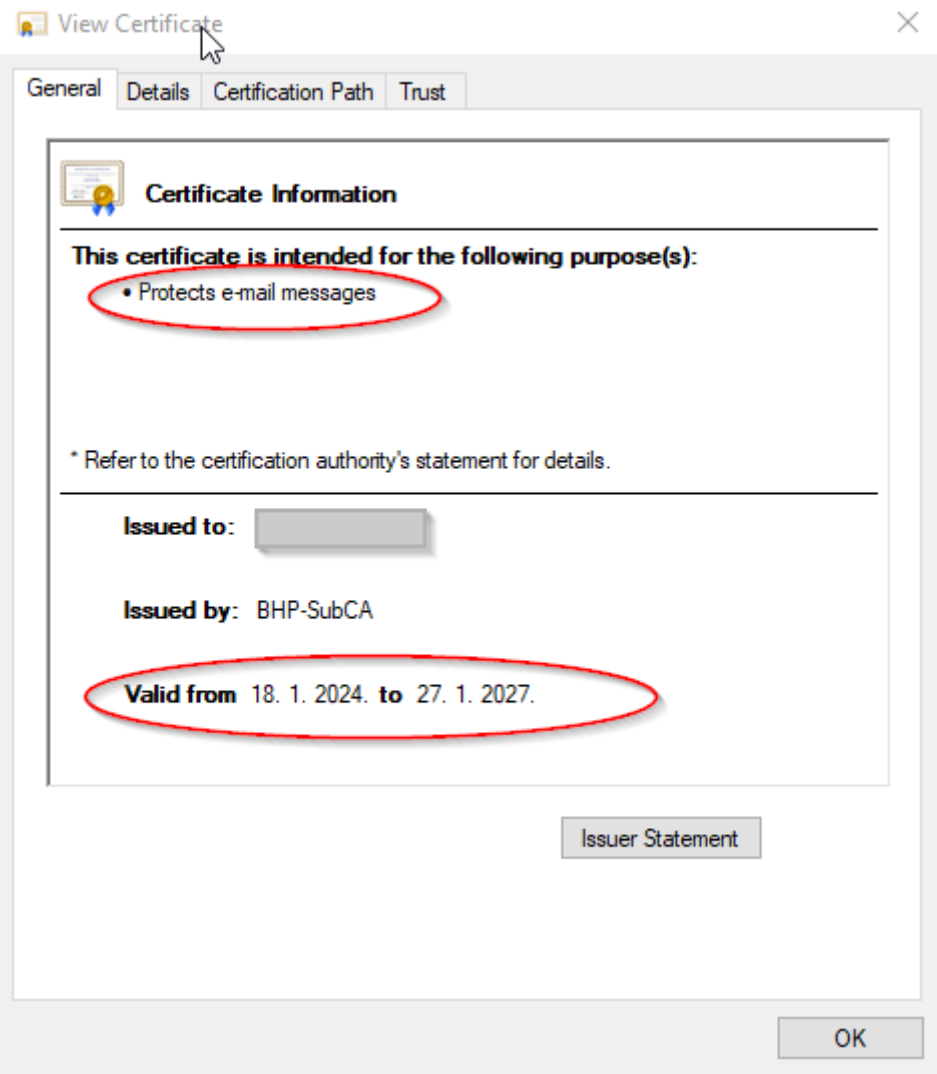

*Slika 11 - prozor sa odlikama sigurnosti poruke*

U novootvorenom prozoru ponovo imamo dodatnih informacija o samom potpisniku, o certifikatima, vremenu potpisivanja i slično. Ovaj put klikom na opciju **View Certificate... /Pogledaj certifikat...** na *General* tabu možemo doći do samog nivoa certifikata i detalja o istom (slika 12).




*Slika 12 - Detalji o potpisu*

U prozoru sa informacijama o samo certifikatu moguće je provjeriti i validirati sve relevantne informacije o samom certifikatu koji je korišten za digitalni potpis. Za potrebe ovog uputstva zadržaćemo se samo na General tabu, odnosno osnovnim infomacijama. Upravo ovdje su vjerovatno i najbitnije informacije poput svrhe izdavanja certifikata, zatim osobe kojoj je isti i izdat čime faktički potvrđujemo/utvrđujemo identitet potpisnika. Osim toga, možemo vidjeti i koji je to izdavaoc certifiktata, te i samu validnost izdanog certifikata.Dodatne informacije nalaze se i na ostalim tabovima. (slika 13).




*Slika 13 - detalji o certifikatu korištenom za digitalni potpis*