

Šifrovaný e-mail

Datum zpracování: 31. 10. 2023

Zpracovali: Knespl Daniel, Kohout Daniel, Koten Tomáš, Musilová Anežka



Zadání

1. S pomocí software **GPG**, **Thunderbird** a pluginu **Enigmail** zprovozněte funkce podpisu a šifrování pro e-maily.
2. Propojte software s existujícími účty.
3. Odešlete digitálně podepsaný e-mail bez šifrování.
4. Odešlete šifrovaný e-mail bez podpisu.
5. Odešlete šifrovaný a podepsaný e-mail.
6. Porovnejte jejich vnitřní strukturu a formát.
7. Proces dokumentujte screenshoty a kopiemi relevantních částí e-mailů.

Úlohu zpracovávejte ve 2 - 5členných týmech.

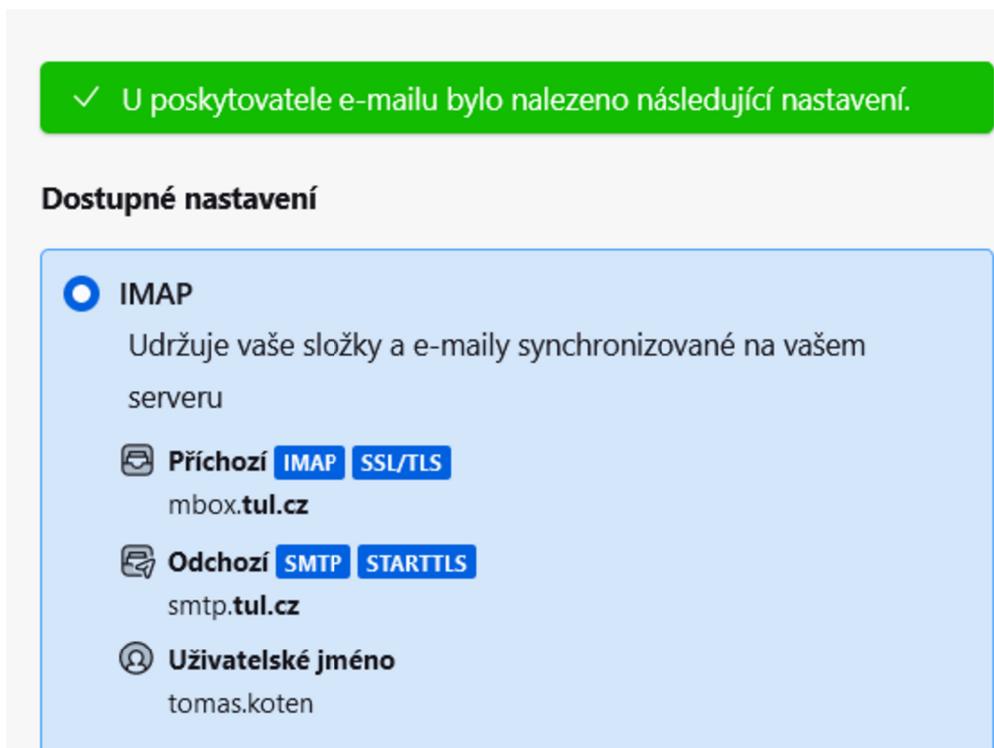
Pro zařízení s OS Android doporučuji aplikaci [K-9 Mail](#).



Postup

1. Thunderbird

- Nainstaloval jsem klienta Thunderbird a přihlásil se pod školním emailem.
- Ponechal jsem implicitní nastavení.



Obrázek 1: Nastavení Thunderbird

- Přešel jsem do **Nastavení → Nastavení účtu** a nastavil jsem *Text podpisu*

Text podpisu: Použít HTML (např. **tučně**)

S přáním hezkého dne,

Koten Tomáš

Obrázek 2: Nastavení podpisu



- Dále jsem přešel do **Nastavení** → **Nastavení účtu** → **Koncové šifrování** a zde jsem si nechal vytvořit osobní klíč OpenPGP

OpenPGP



Obrázek 3: Vytvoření osobního klíče

- Nastavil jsem platnost klíče na 2 měsíce

Vytvořit klíč OpenPGP

Identita Tomáš Koten <tomas.koten@tul.cz> - tomas.koten@tul.cz

Doba platnosti klíče

Určete dobu platnosti svého nově vytvořeného klíče. Dobu platnosti můžete později změnit a v případě potřeby ji prodloužit.

Platnost klíče skončí za měsíců

Platnost klíče není omezená

Pokročilé nastavení

Určete pokročilá nastavení vašeho klíče OpenPGP.

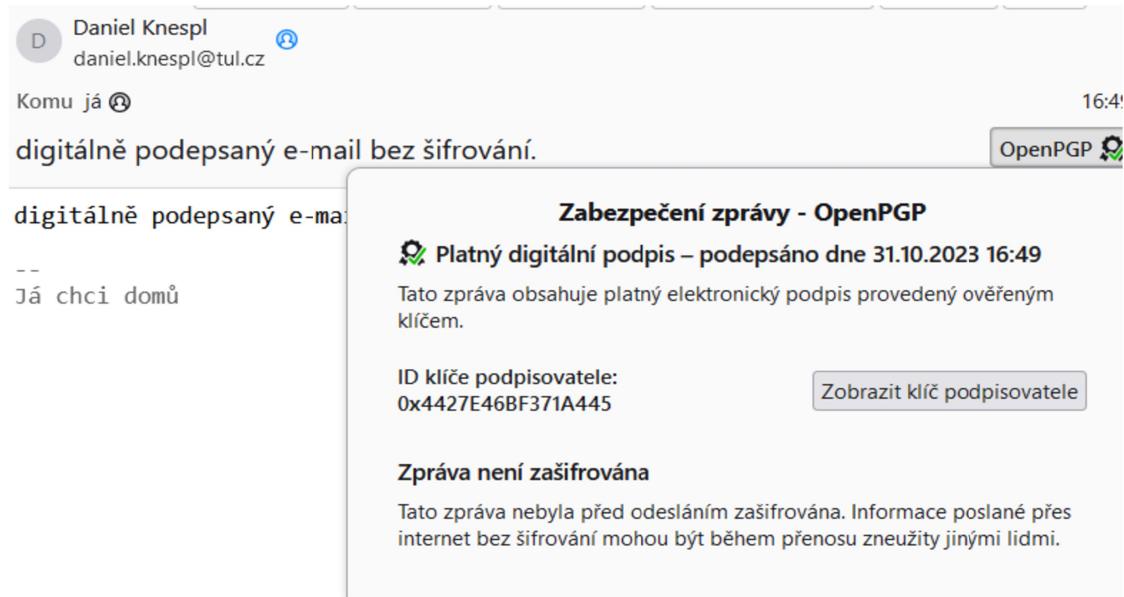
Typ klíče: RSA

Velikost klíče: 3072

Obrázek 4: Nastavení parametrů osobního klíče

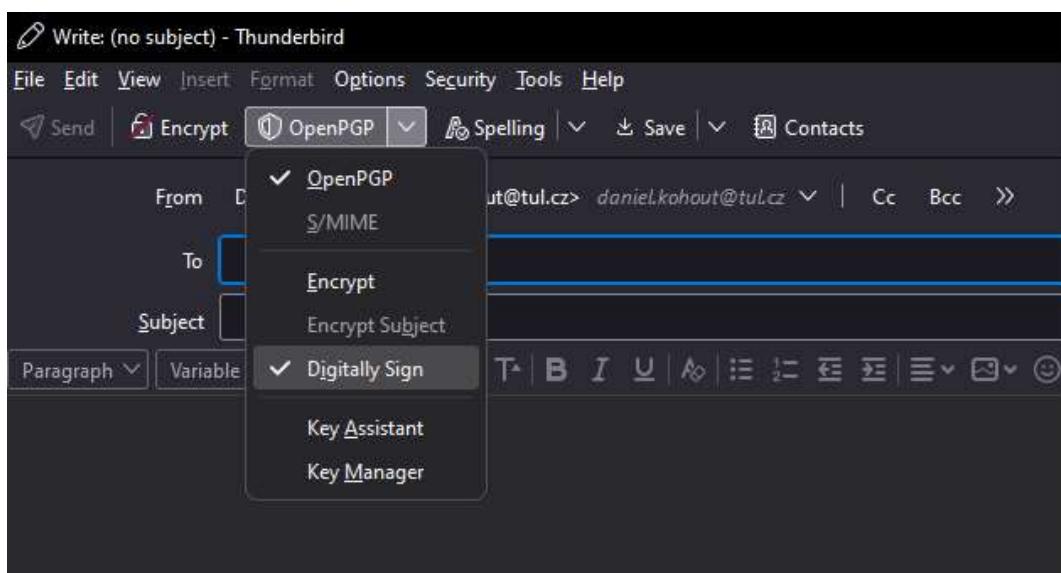


- Odeslal jsem kolegovi nezašifrovaný email s podpisem, aby mohl získat můj digitální podpis a nazpátek jsem dostal email s jeho digitálním podpisem.



Obrázek 5: Digitálně podepsaný e-mail bez šifrování

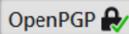
- Pro zašifrování je nutné zaškrtnout volbu **Encrypt** (Zašifrovat)
- Pro přidání digitální podpisu je nutné zaškrtnou volbu **Digitally Sign** (Elektronicky podepsat)



- Dále jsem dostal šifrovaný email bez podpisu

Daniel Knespl  daniel.knespl@tul.cz

Komu já  16:51

šifrovaný e-mail bez podpisu. 

šifrovaný e-mail bez pod

--
Já chci domů

Zabezpečení zprávy - OpenPGP

 Žádný elektronický podpis

Tato zpráva neobsahuje elektronický podpis odesílatele. Chybějící podpis znamená, že zprávu mohl odeslat kdokoliv, kdo zná danou e-mailovou adresu. Je také možné, že tato zpráva byla pozměněna během cesty sítí.

 **Zpráva je zašifrována**

Tato zpráva byla před odesláním zašifrována. Díky tomu je zajištěno, že si ji může přečíst jenom její adresát.

ID vašeho dešifrovacího klíče: 0xA21962ABDA2CC239 (ID podklíče: 0x2E2F05B89C0F6F1E)

[Zobrazit váš dešifrovací klíč](#)

Zpráva byla zašifrována pro vlastníky následujících klíčů:

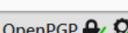
Daniel Knespl <daniel.knespl@tul.cz>
0x4427E46BF371A445 (0x88CB88196331808A)

Obrázek 6: Šifrovaný e-mail bez podpisu.

- Nakonec jsem dostal šifrovaný a podepsaný email

Daniel Knespl  daniel.knespl@tul.cz

Komu já  16:53

šifrovaný a podepsaný e-mail 

šifrovaný a podepsaný e-

--
Já chci domů

Zabezpečení zprávy - OpenPGP

 **Platný elektronický podpis**

Tato zpráva obsahuje platný elektronický podpis provedený ověřeným klíčem.

ID klíče podpisovatele: 0x4427E46BF371A445 [Zobrazit klíč podpisovatele](#)

 **Zpráva je zašifrována**

Tato zpráva byla před odesláním zašifrována. Díky tomu je zajištěno, že si ji může přečíst jenom její adresát.

ID vašeho dešifrovacího klíče: 0xA21962ABDA2CC239 (ID podklíče: 0x2E2F05B89C0F6F1E)

[Zobrazit váš dešifrovací klíč](#)

Zpráva byla zašifrována pro vlastníky následujících klíčů:

Daniel Knespl <daniel.knespl@tul.cz>
0x4427E46BF371A445 (0x88CB88196331808A)

Obrázek 7: Šifrovaný a podepsaný e-mail



2. Rozdíly ve zdrojovém kódu emailů

- Šifrovaný a podepsaný email byl velmi podobný šifrovanému emailu bez podpisu
 - Nalevo podepsaný email bez šifrování, napravo nepodepsaný email zašifrovaný
 - První zpráva aktivovala více příznaků pro odhalení spamu

Obrázek 8: X-Spam-Status

- Vpravo zvýrazněná fráze jen značí, že uživatelské jméno obsahuje nestandardní znaky jako jsou písmena s háčky a čárkami.

Date: Tue, 31 Oct 2023 16:40:22 +0100
MIME-Version: 1.0
User-Agent: Mozilla Thunderbird
Content-Language: cs
To: daniel.kohout@tul.cz
From: Daniel Knespl <daniel.knespl@tul.cz>
Subject: gigachad
Autocrypt: add=daniel.knespl@tul.cz; keydata=
xsDNBVGBH3gBDACn/1tBa99mpca11EfYmz0dHRjXZ/0KmB0z9Gykk0iLDwqY9B0c7/a0c3Z8
Date: Tue, 31 Oct 2023 16:41:54 +0100
MIME-Version: 1.0
User-Agent: Mozilla Thunderbird
Content-Language: cs
To: daniel.kohout@tul.cz
From: =?UTF-8?B?TXzaIvxds0hLCB8bmXFVmth?= <anezka.musilova@tul.cz>
Subject: ...
Content-Type: multipart/encrypted;
protocol="application/pgp-encrypted";
boundary="-----9KwIW9ad91TH1lvhrAuMNIas"

Obrázek 9: Zakódované jméno

- Nalevo informace o digitálním podpisu, napravo informace o zašifrování

Content-Type: multipart/signed; micalg=pgp-sha256;
protocol="application/pgp-signature";
boundary="-----1Egn9ZHryjQd79yPMIXXXZ11"

this is an OpenPGP/MIME signed message (RFC 4880 and 3156)
-----1Egn9ZHryjQd79yPMIXXXZ11
Content-Type: multipart/mixed; boundary="-----0d9xehx5F1dc4HnOCLeL0UyV"
Content-Type: protected-data; boundary="-----v1"
From: Daniel Knespel <daniel.knespel@tul.cz>
To: Tomas.Koten@tul.cz
Message-ID: <dad4f233_48f-4ed5_b914_431f8e67076a@tul.cz>
Subject: =?UTF-8?B?ZGlnaXR0b3JlZG9k?X?B?Y?W7DvS11W1hahw?y?W6TMuhahw?y?=?
=?UTF-8?B?R?h?w?S?w?R?y?<

-----0d9xehx5F1dc4HnOCLeL0UyV
Content-Type: multipart/mixed; boundary="-----x0D2zCrxR7xGtR0pJpk4wKV"

-----xg0D2zCrxR7xGtR0pJpk4wKV
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: base64

/G1naXDoexu1sgC9k/XB7Y?W7DvS11W1hahw?y?W6TMuhahw?y?B?D?w?/D?S?4?C?p?k?1?S?9?
D?Q?K?w?G?Y?h?ja?S?B?2?3?r?w?K?D?0?
-----xg0D2zCrxR7xGtR0pJpk4wKV
Content-Type: application/pgp-keys; name="OpenPGP_0x4427E46BF371A445.asc"
Content-Disposition: attachment; filename="OpenPGP_0x4427E46BF371A445.asc"
Content-Description: OpenPGP public key
Content-Transfer-Encoding: quoted-printable

Subject: ...
Content-Type: multipart/encrypted;
protocol="application/pgp_encrypted";
boundary="-----jgrrwu10atkfu3hctpnvdgq0"

This is an OpenPGP/MIME encrypted message (RFC 4889 and 3156)
-----jgrrwu10atkfu3hctpnvdgq0
Content-Type: application/pgp-encrypted
Content-Description: PGP/MIME version identification

Version: 1

-----jgrrwu10atkfu3hctpnvdgq0
Content-Type: application/octet-stream; name="encrypted.asc"
Content-Description: OpenPGP encrypted message
Content-Disposition: inline; filename="encrypted.asc"

-----BEGIN PGP MESSAGE-----

waDMA4j1LBjJMYCKA9w8DWLrxJy41kdVzOyL9k20tGHfJiYeyph+HuJuLyR4udUz
Dw73CkX70Q1hpgp1TA13vsbu8g0xQvHob1bhGu10NkXjghOz0pkqk0dxYh1YFI
Pw08qoe62hInNj8Xjz5gEN424QMPt1zIh2r70706b6FSR1ax1OpzDmR9v0oxd
VcfV8k18Vt1K1YVG7msqf5{Wqf1wqj9eB9Cn1xhuWjyvdm13t5Uyqgj7b+rGn
Dz04C1QEDJ1i18tWxoyg9ee1SHS172t8yDx8z//JsuPnKUm/J2b13ckrqQ1hgdA
3tMhYxaoCf1Z9r1Ma1yq9ckJcdG65hsvTQjP5uKq2KADq
10qGBCgk7rFfeUfglyPj70L9UfJ9JtDj0e1zRax3uGH0JLb0gE9Z5yEsqPwUer7bC
wxDMyA9vbi3B2eAqWpAcHr17Mz6uVH5m0c57T{KzqfBj7chcEv3jUtkhYR9456x
ruk//Cxs9t6r1vZpc2shdeqa999mz+uqcPl4f196o0PxVWt8Gx//zvcd0xhky0Kc
F21mWbkhEx//58HtP51CYKWDL8059nRhaQwLp3vdh0g8r3fRDUs3Wf1bxp
-----END PGP MESSAGE-----

Obrázek 10: Informace o typu emailu



- Email s digitálním podpisem je zakončen **PUBLIC KEY** blokem a **PGP SIGNATURE**
- Zašifrovaný email končí blokem **PGP MESSAGE**

```
tHaIZExbd4E5L9/06+mb+4WSpullerB26M28mUICXGc1XSpdVr+8R0X0Ey54Jbv
jhBQaQ8JqoGMnRyREUBsQ7q/OzhBa7R4LHMm6XAbu2hGPxW6w/g38ZMCMNUAO
0E0o07KtG/3rEPu0b66v0WV4+Zhu5PMqz+8F7CMtTz9o2c1aEOKvkaeo
9gKwubTkdwXspIAg7kDnsz1M95d7q9NE5bmcmlkf5in9Lz1A/rstfhp9ov6E0Ihy
mR3kx66d351Vzsf5Ks60KJqBw/jmp9W//LqSwtsb45G0e0v0jzfFkmAuBvUfctb
jYEqd4RkbjFB4d2iTP1r0zTP8o1lNAR+hNvVfYFEmWmz1dKn5ed+M5/B/CgEuctb
czVOUM75/XrVmsn1u96GRY1+2F
=3DLsW0
-----END PGP PUBLIC KEY BLOCK-----
-----END PGP PUBLIC KEY BLOCK-----
-----xg0DZC1rxR7xGIR0pjk4wKV-
-----0d9xehx5F1dc4HMNoCL0LUuy-
-----1EGn0ZHrYjxdA29yPMIxZTi
Content-Type: application/pgp-signature; name="OpenPGP_signature.asc"
Content-Disposition: OpenPGP digital signature
Content-Description: attachment; filename="OpenPGP_signature.asc"
-----BEGIN PGP SIGNATURE-----
wsD5DAA0DCAAj1iCqZP0r0K4ehZdrj1nRcFka/NopCEUAmVDTFYT AwAAAAAAAGk0KRCFka/NopCkH
ygV//21.0800uCARNoV7/DW1nAe5B1Z16NLjcejV10V3H6TCz1X1DXRGTTPSdQzv7WrQk8xt
1Bm0d8gnz1vAFmB0M6629Ytr5Amog6nqQa/n3cWV9P4JwpcSF88HD15dh47r1ngKho2aR/c1
sHNYsq0c7RxZBpNe38/atNTbtrj3B811wmABy54wBouk1WmccZ5xkfd1d45JWH171S/De+Dy+Y6
wZlkgd415xbBaTTE76VB13651pKR8A7DNe8N201sc/g5Fx1z31PH3102UP+TJ8VpDz10rn9R
0t5n5dF7VaqAg8kpl1JpVewomk4N0uNa0gg99v0tVjg4Yp07uL8d6kP/otAGCHIAg87xh6B9
OaCojYXTsvk9Pxl+MgL3a2zHExhSi0wsvDv9vsmkUwsgE558v8XkU42AvYkRcrFTB916jHsvq
1LrY5U1jRfp1KGthcason/rbfmfvGyikdks1B8sUqwcb12dM5jZT9K6ruu
=xc/
-----END PGP SIGNATURE-----
-----BEGIN PGP MESSAGE-----
wCDMA4j1iBljMYCKAQv8Dwtrx7Y41kd2Vz0y9k20tGhf1W1Yevph+hEujuYr4UdUz jeEEv0Ybhz
w73CzCz709h1gpm1TA1jvshu8g0x0f0Qa1bGu1OrNk1xjgZ0pQqkodxhV1Yf1D5bckQ1ha
Pw00q00e/62niuJ8Xjz5qEM4240M9tPzamzTh/z0P7db6fFSR1ax1QyPzdm9r+yooXh9k8t3v160
VcfBkvt8/vzFkVvCz9qsf1LGGOT/waHyd99rcn+whuWtsYdm23Ksuhvgg5E7b1r+rc0n1AWEHTY8
DxGz1C1EDJ1iET8wxy9g6ee1SIS7272Bx/dsx/Z/JSuPMKUW/jb13ckrqcQ1h+gd0uJvP8m3Ey
3NmYca0Cf1zr9My1aay6k1Jdc66h5V7QjPsu97159f81YC2mK7r6+h90uKaq7KAQd1cT11Ca37
j0qGBCgkT17rFeuGwyPj70l9f1uADTj0e+rAX3wGJ1Q1m0G0e0Z5EyS4pPu0r+r7Cm6MhNv4dRT
wcdMAYavb1b1c028e0wApchHr174NzouHsmgs7Fk2qfBfjhecv3jUtk1YH9456xu0w80n1KxCT
Ruk//cXk9t66E1Vzcpzshdkeq99MSae+q-E4f196w0PQzVhL8sG/AzV1cdXksy0KctswlgFuza
F21AmVbXeX/28Hr1Tp51cykXvD1.88S0Qqdn1aw06z+tp3vd0xsg0R3fR013fC13DpxGm1t82ut
jxlobUnJz6jWxIP3M4d1ybhYz1zW1y319wamjnw/DwDfV8E//iCyp1492zPNg7rnhMu5cgHkZvk
1SQPDfj44+iu5/Fe0UvbzVhDe5z+bpl1V89PcdtGmGw1+w1uKTCs26uG7qPQvT12)f1o8N1N
wdp10s8C13A7CRs10yxpibp+110PG0Kg1s2kVnxvc1dy772FmcSAZNPV0QyXsrhueEV
ea1A-TkcuHnZkg1oL0gB61x4Ry1m2z2n+4e+x1u1185zDvpppq10Hsz/qkfhnyym6RPGFPY1
0sg1AYK0883jadoqg7X/+5T19hacraRACfSA4e4x0Yq10K0Y1TGBtHAAwHQTofFn9c8tQo
Rw272f13fd12d+jVf2m7z1UcUc1Djyv/qe-hvEwk1Lkn1p9t2zddg+9uYh2d6CngdMsVdcbz7
jFkYmo1+Aexg1H08r1hPxasHpx/yjdr1aQlMw2DoxGgtk/hbx1L1uccgpbpu28raXa7t3px02
BE0Mme91wCoC/01AdeiPtboeU1i3h0o1lxQlWrayd+hzzyqG0U1p2zG0Gk1gd+0ZFHusP43kIH
RCC1A1j7VxIYEjH6j1w1v1/fw1gxu0wn/7zLkk0oAktdxwM12V13gF48qwm/01w1cmkjp1u
px8Z2Hd0+u2B7oF9/09n/AUEfvmPvtvCwH+sp13k1gPF3PfRfP0Qy+s+5An169u9uKNe+dgih/tr
x0/3GtDE1/Cm0cB4Evg1QyGoPzQetqQHNGpxxxQztsfu3wI0sulr2g/0MqP46aAazYeYfRp
n1531FFC4ee0cZHxHpa0ikw5f00G5gchb0V0M1p1lN+ttg/8UlmwQ+Xo2bLJmgy0IKNCB0l1uifY
o11t612Chw91eBXK0tmh+3xxB1LkmD7hsp0q1+ox00AY+2rDrzV5hM1dSLLef5/HcytW1xh9PE
U0gqbrkrD9wkrF1m0y1L99y7x4hV1+ke1Ln0ksp12yfneBrz9B5871CD0grs1r/zgykvhn
DYYXw0o/SLl0+rF6qt4rayB0p+51BwO3x1j51jEmIZ08ogBS1+0EeTkw==

-----END PGP MESSAGE-----
```

Obrázek 11: Rozdíl konečných bloků



Závěr

Instalace a nastavení softwaru Thunderbird byla jednoduchá. Software obsahoval vše potřebné, takže nebylo nutné něco doinstalovávat. Nastavení zašifrování emailu či přidání digitálního podpisu bylo také přímočaré. Jedinou podmínkou bylo získat od kolegy nezašifrovaný email, který obsahoval jeho klíč a následující komunikace již mohla být zašifrována.

