

Šifrovaný e-mail

Datum zpracování: 12. 11. 2023

Zpracovali: Kevin Daněk, Nepřiměřená dávka alkoholu

Zadání

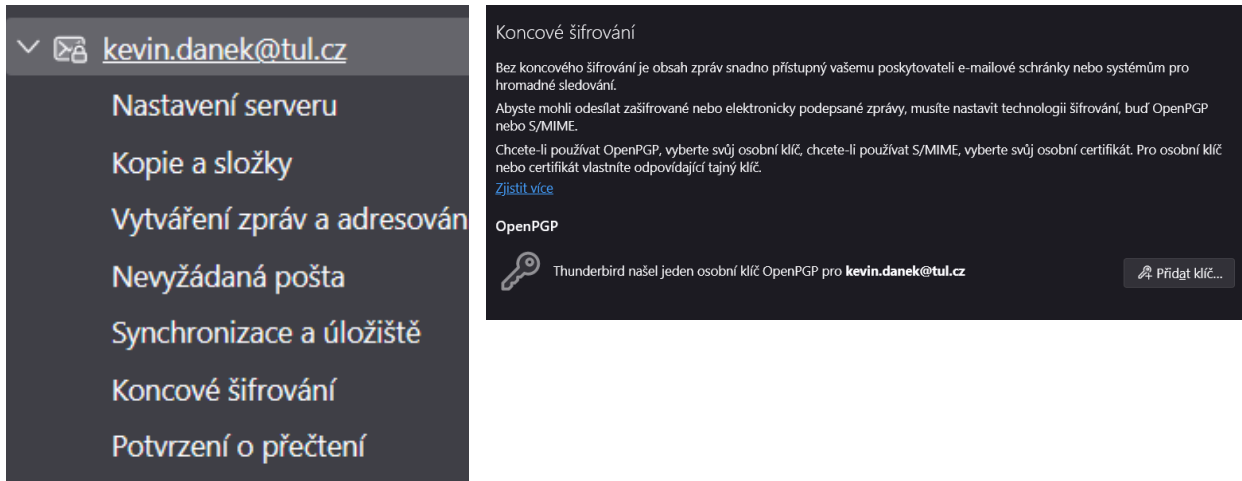
Ve virtuálním systému proveďte následující úkony.

1. S pomocí software **GPG** a **Thunderbird** 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.

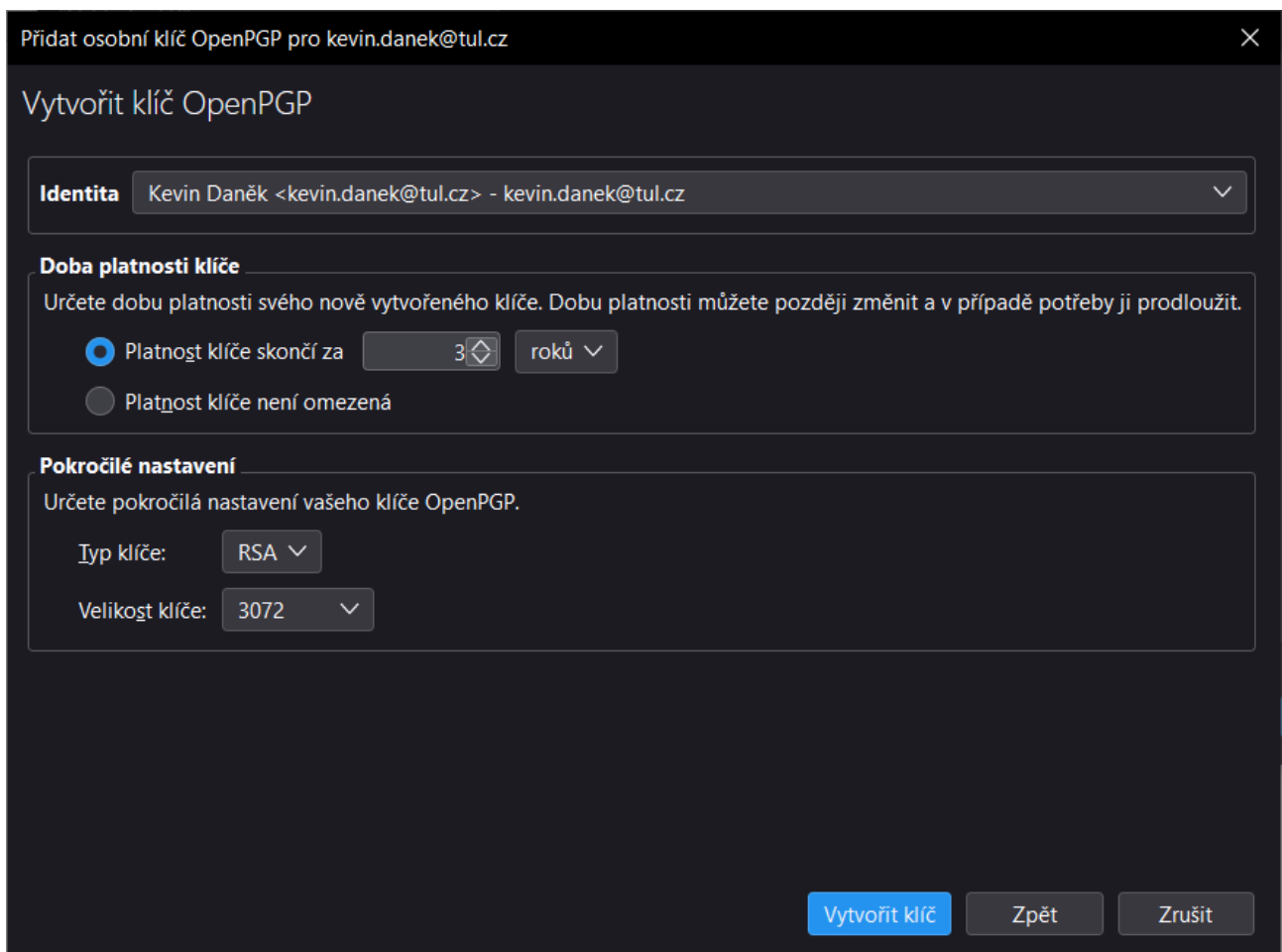
Elaborát do e-learningu nahrávejte ve **formátu PDF**.

Nastavení Šifrování a podpisu

Po nainstalování klienta Thunderbird a připojení účtů kevin.danek@tul.cz a kevin.danek@outlook.cz jsem jako první šel do nastavení, kde jsem našel záložku “Koncové šifrování”. V ní jsem našel správu klíču OpenPGP, která slouží k vytváření a přiřazování klíčů pro podpis a šifrování



Vytvoření klíče bylo přímočaré. V plovoucím okně se seznamem klíčů jsem zvolil možnost “Vytvořit” a vyplnil patřičné údaje, tj. platnost klíče a pro jaký účet má být vytvořen.





Poté již stačilo vytvořený klíč přiřadit k účtu a byl aktivní.

OpenPGP

 Thunderbird našel jeden osobní klíč OpenPGP pro **kevin.danek@tul.cz**

 Přidat klíč...

 Vaše současná konfigurace používá klíč s ID **0xC3D6AC4DBE383174** [Zjistit více](#)

☐ Žádný

Pro tuto identitu OpenPGP nepoužívat.

☒ **0xC3D6AC4DBE383174**

Datum konce platnosti: 11. 11. 2026

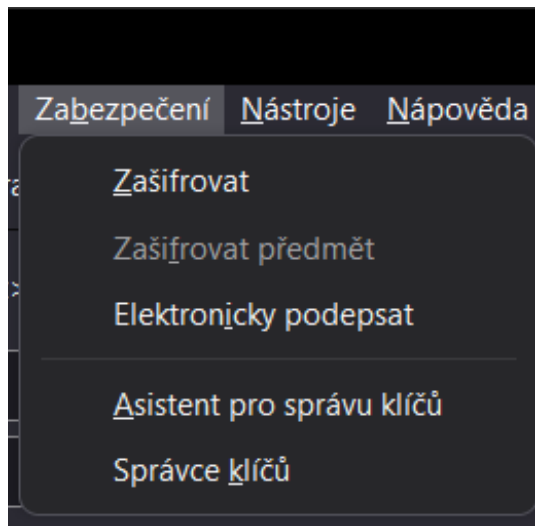
Zveřejnění veřejného klíče na serveru klíčů ho umožní druhým najít.

Publikovat



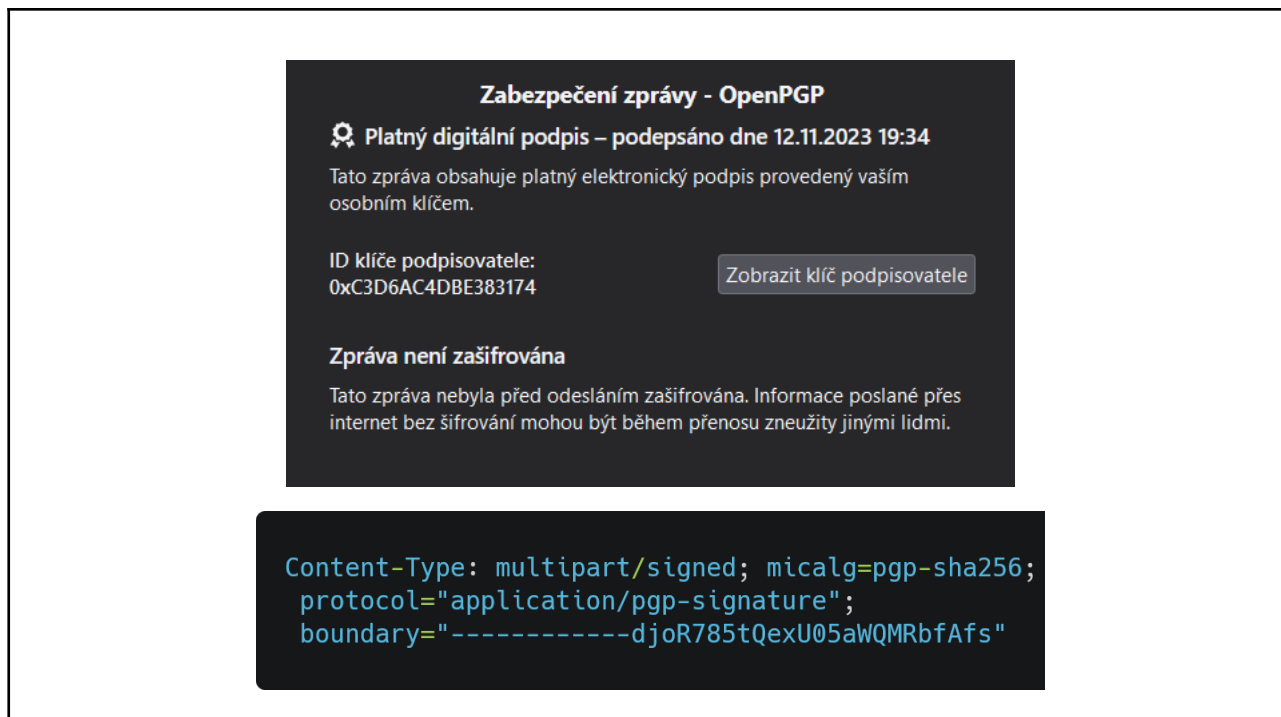
Obsah zpráv

V klientu Thunderbird lze možnosti digitálního podpisu a šifrování zvolit v záložce “Zabezpečení” při psaní zprávy.



Podepsaný e-mail

Podíváme-li se na hlavičku Content-Type, tak nám napoví, že e-mail je podepsaný - této informace využívá i klient Thunderbird, který ji zobrazí v plovoucím okně naproti předmětu zprávy.



Pokud ve zdrojovém kódu zprávy zabrouzdáme trochu níže, můžeme si všimnout sekce s jejím obsahem. Tento obsah je, jak už napovídají i hlavičky tohoto bloku, zakódován v Base64, což není úplně ideální, pokud si nepřejeme, aby ho někdo četl.



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

```
QWhvaiwNCnRvaGxIGplIGVtYWlsLCBrdGVyw70gamUgcG9kZXBzYW7DvSwgYWxlIG5lxaFp  
ZnJvdmFuw70uDQoNCg==
```





Posledním významným blokem je část s PGP podpisem, který jednoznačně popisuje majitele původní zprávy.

```
-----djoR785tQexU05aWQMRbfAfs
Content-Type: application/pgp-signature; name="OpenPGP_signature.asc"
Content-Description: OpenPGP digital signature
Content-Disposition: attachment; filename="OpenPGP_signature.asc"

-----BEGIN PGP SIGNATURE-----

wsD5BAABCAAjFiEEw82y8UCVu4wFgwWVw9asTb44MXQFAMVRGsoFAwAAAAACGkQw9asTb44MXRn
zAwAufu1ly0Bh+/i5TC1xNPoyBeDibK+13WyzXbMcPEASkPVAA55WxG4A8xUMqbRXMXtqpt4SV/v
+SDMbgED0b8QC5cv38+tuaDMyu8hGfl9QLtVrhrIbhyEwhDf/9GZoQi6GeCFk5MMpw6JZBK2cBut
4hlQVEtaWDix0ljv3zwme9K3Gj5T1SMwwryzSxW/SBJolBghJyZ8xKxZRVr7DQ8QVhbXzk1dow7Z
mi7jbCRiPmY9EmLtS7StWxQjTGUxXjVnF6aWxC1XBH1FoEzRaTMqMuF3BPb1ygKNFCmE9odPoJ5K
Kw+hZnkjDpSvyotM289UdQ0BwqoAEImF9+aCsLqV3jCNDEZuSIxG7FUL7GnyvV/g1XztDu9+sKbn
mXNs3RkenlI7xPGrwKuufGZuDTIuF97lvYQgiG4gnq70WrV/GrKrXgySl+ruw60QfnSRHnSkYGyV
U0NTEbH14VJPZZ/P3iTf1SjFzegEMaEuK2n5MZ9b2udrfx2LocaBDItMSUu/
=3Glh
-----END PGP SIGNATURE-----

-----djoR785tQexU05aWQMRbfAfs--
```




Šifrovaný e-mail

Hned na první pohled si můžeme všimnout změny typu obsahu v globální hlavičce Content-Type. Kromě toho také z obsahu zprávy zmizelo tělo se zakódovanou zprávou v Base64.

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 sítě.

 **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: 0xC3D6AC4DBE383174 (ID podklíče: 0xE506D98F6E6FEAF2)

[Zobrazit váš dešifrovací klíč](#)

Zpráva byla zašifrována pro vlastníky následujících klíčů:

Kevin Daněk <kevin.danek@outlook.cz>
0xDF4900393C8746CC (0x42EBC1626B4C15BF)

```
Content-Type: multipart/encrypted;  
protocol="application/pgp-encrypted";  
boundary="-----JWSCQX0hbmRWh6gjTiZmb0g3"
```

Trochu níže můžeme najít skutečný obsah, včetně informací o klíči, který byl použit k zašifrování.

```
-----JWSCQX0hbmRWh6gjTiZmb0g3  
Content-Type: application/pgp-encrypted  
Content-Description: PGP/MIME version identification  
  
Version: 1  
  
-----JWSCQX0hbmRWh6gjTiZmb0g3  
Content-Type: application/octet-stream; name="encrypted.asc"  
Content-Description: OpenPGP encrypted message  
Content-Disposition: inline; filename="encrypted.asc"  
  
-----BEGIN PGP MESSAGE-----  
...  
-----END PGP MESSAGE-----  
  
-----JWSCQX0hbmRWh6gjTiZmb0g3--
```



Šifrovaný a podepsaný e-mail

Pokud k šifrování přidáme ještě podpis, ve zdrojovém kódu to nelze na první pohled poznat. Jediné, čeho si lze všimnout, je, že obsah PGP zprávy je delší. To je způsobeno tím, že i informace o podpisu e-mailu je šifrována.

Zabezpečení zprávy - OpenPGP

Platný elektronický podpis

Tato zpráva obsahuje platný elektronický podpis provedený vaším osobním klíčem.

ID klíče podpisovatele: 0xC3D6AC4DBE383174 [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: 0xC3D6AC4DBE383174 (ID podklíče: 0xE506D98F6E6FEAF2) [Zobrazit váš dešifrovací klíč](#)

Zpráva byla zašifrována pro vlastníky následujících klíčů:

Kevin Daněk <kevin.danek@outlook.cz>
0xDF4900393C8746CC (0x42EBC1626B4C15BF)

```
Content-Type: multipart/encrypted;  
protocol="application/pgp-encrypted";  
boundary="-----pNcRGsxvddHA9FhFzf1ZZwC"
```



Závěr

Nastavení podpisu i šifrování bylo v konečném důsledku jednodušší, než jsem čekal. Je to možná způsobeno tím, že Thunderbird má skvělou abstrakci nad správou klíčů a certifikátů, které by jinak potřebovali práci s utilitami jako je ssh-keygen. Certifikát, který není vydán certifikační autoritou, je teda trochu o ničem, ale minimálně digitální podpis, který lze jedním kliknutím zveřejnit na keys.openpgp.org, je věc, která přidá na důvěryhodnosti zpráv a rozhodně ji chci využívat do budoucna.