



Camera Notarială din Republica Moldova

Ghid de creare și utilizare a cheilor PGP (Pretty Good Privacy) in Roundcube

O cheie **PGP (Pretty Good Privacy)** este un set de date criptografice folosit pentru a asigura securitatea comunicațiilor digitale, în special a mesajelor electronice. Aceste chei sunt utilizate pentru două scopuri principale: semnarea digitală și criptarea.

1. Semnarea Digitală:

Prin semnarea digitală, deținătorul cheii atestă autenticitatea unui mesaj sau document digital.

Semnarea se face folosind cheia privată a utilizatorului și poate fi verificată de alți utilizatori cu ajutorul cheii publice corespunzătoare.

2. Criptarea:

Prin criptare, mesajele pot fi protejate împotriva interceptării sau citirii neautorizate.

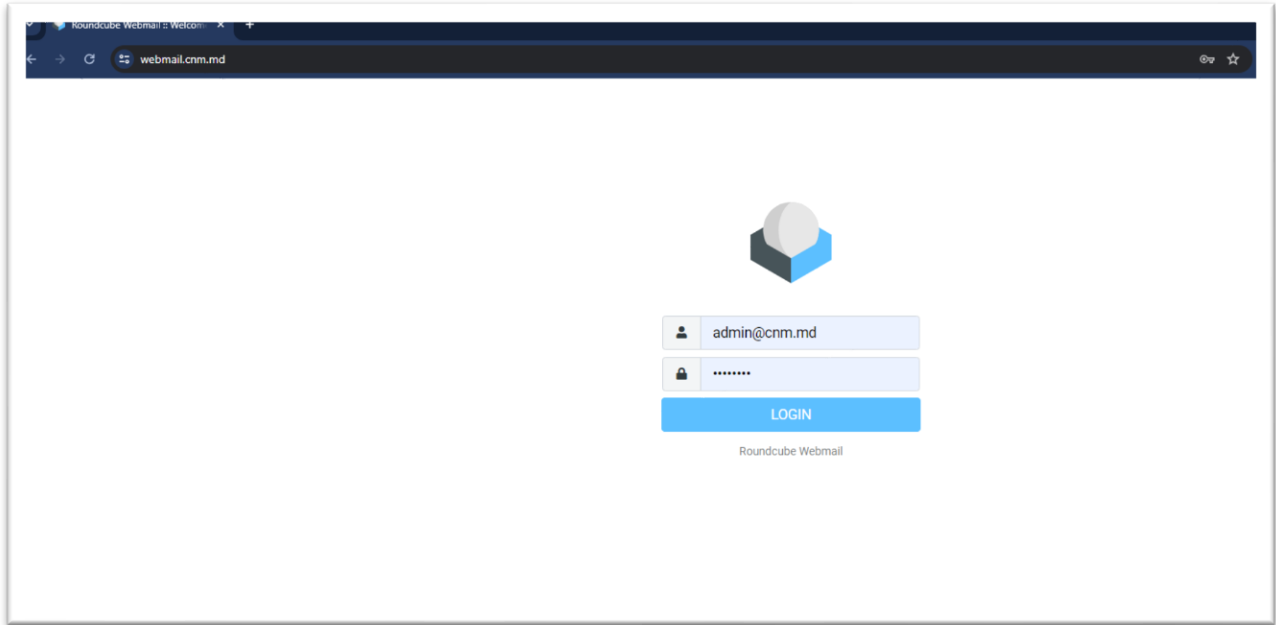
Mesajele criptate pot fi decriptate doar de către destinatarul legitim, care deține cheia privată corespunzătoare cheii publice folosite pentru criptare.

O pereche de chei PGP constă din:

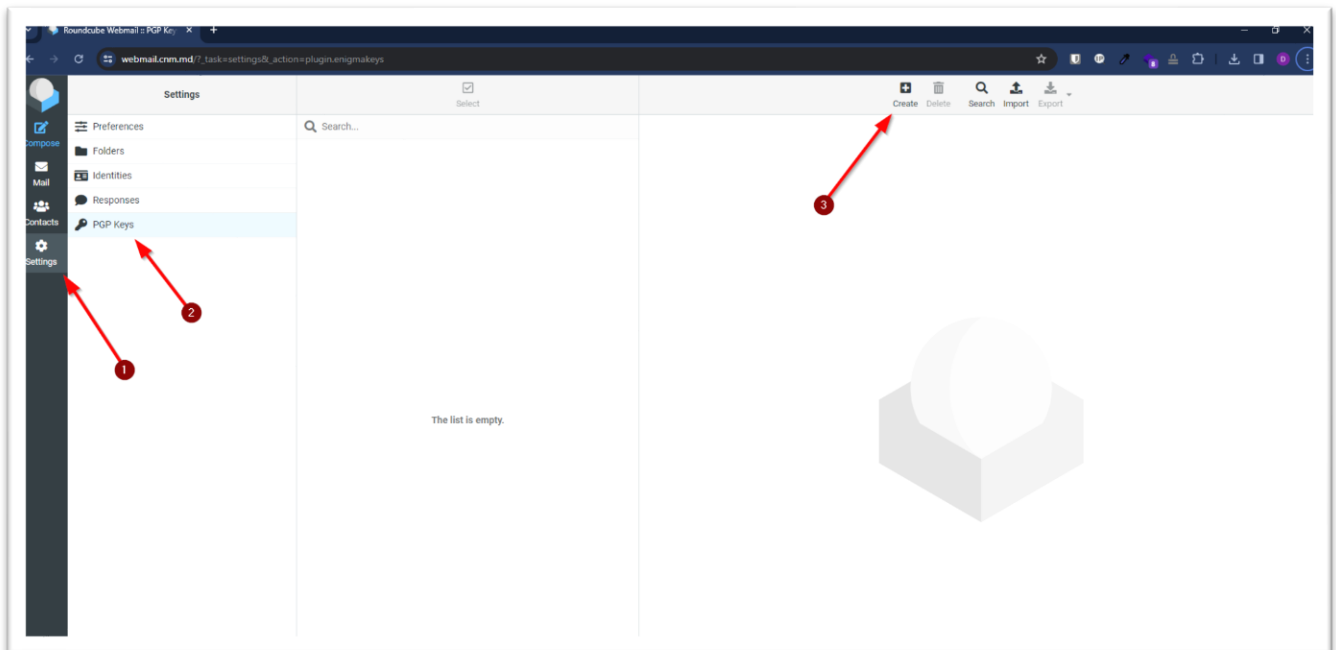
- **Cheia Publică (Public Key):** Aceasta este distribuită liber și poate fi partajată cu oricine. Este folosită pentru a verifica semnături digitale și pentru a cripta mesaje către deținătorul cheii private corespunzătoare.
- **Cheia Privată (Private Key):** Aceasta trebuie păstrată în secret. Este folosită pentru a semna digital mesaje și pentru a decripta mesaje primite criptate cu cheia publică corespunzătoare.

Pașii pentru crearea și utilizarea cheilor PGP

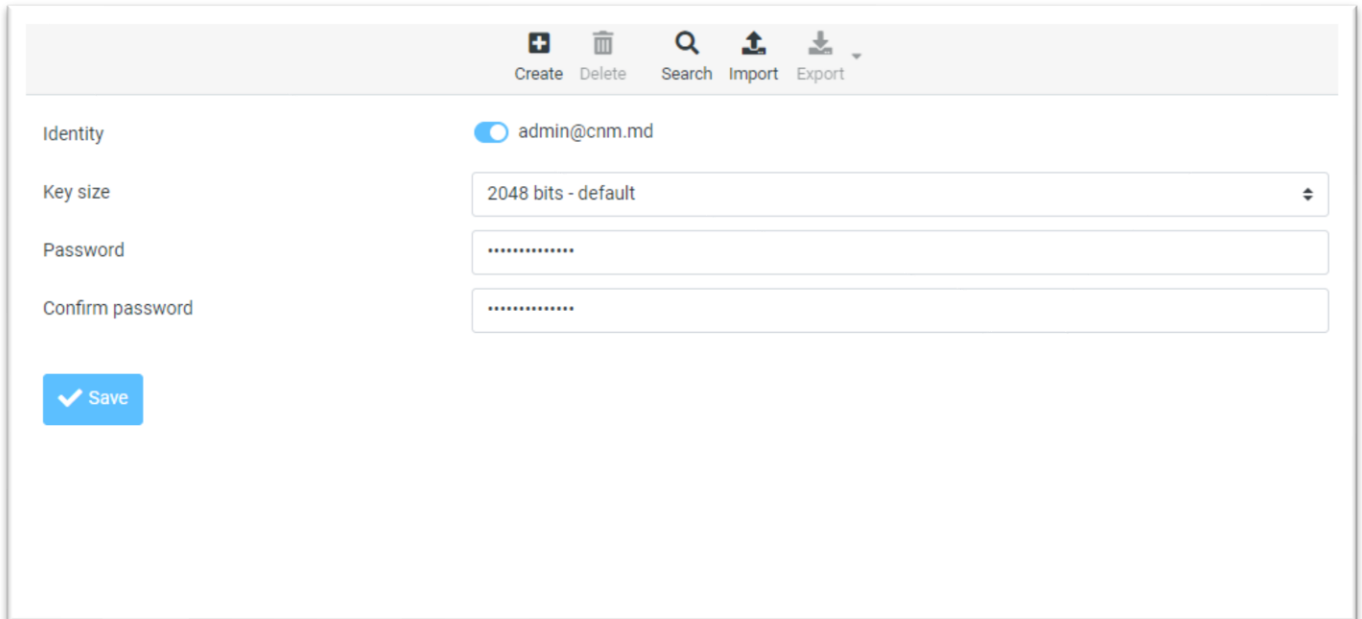
1. Accesam și ne logam pe interfața web a serviciului de poștă webmail.cnm.md



2. În secțiunea **Settings** găsim funcționalul **PGP Keys** și vom crea o cheie nouă:
Settings >> PGP Keys >> Create



3. La câmpul **Identity** vom marca bifa să fie activă pentru cutia poștală care o folosim, **Key size** lăsăm default, iar la câmpurile **Password** și **Confirm Password** vom introduce o parolă complexă care să includă: litere mari și mici ale alfabetului latin, cifre și simboluri (Exemplu de parolă: **4mUDU2@BPvkyr#**) iar la final salvăm modificările făcute accesând butonul **Save**



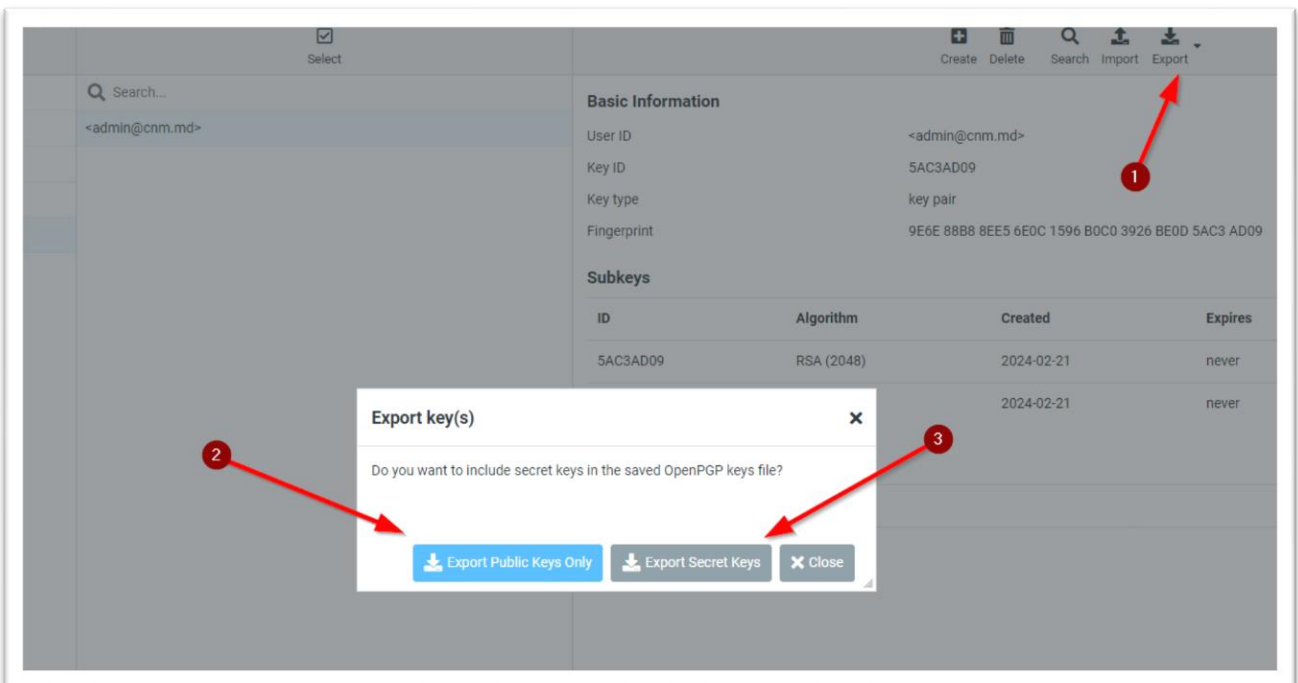
The screenshot shows a web interface for generating a key. At the top, there are icons for Create, Delete, Search, Import, and Export. Below these, the 'Identity' field is set to 'admin@cnm.md' with a toggle switch. The 'Key size' is set to '2048 bits - default'. There are two password input fields, one for 'Password' and one for 'Confirm password', both containing masked characters. A blue 'Save' button with a checkmark is located at the bottom left.

4. În lista de certificate, găsim certificatul generat de noi și putem vedea toată informația despre dânsul.

Important: Descărcați Cheia Publică și Cheia Privată în calculatorul Dvs.

Pașii pentru descărcarea cheii publice: Export >> Export Selected >> Export Public Keys Only

Pașii pentru descărcarea cheii private: Export >> Export Selected >> Export Secret Keys



The screenshot shows the details of a certificate. The 'Basic Information' section includes User ID (<admin@cnm.md>), Key ID (5AC3AD09), Key type (key pair), and Fingerprint (9E6E 88B8 8EE5 6E0C 1596 B0C0 3926 BE0D 5AC3 AD09). The 'Subkeys' section is a table with columns for ID, Algorithm, Created, and Expires. A red arrow points to the 'Export' button in the top right. A dialog box titled 'Export key(s)' is open, asking 'Do you want to include secret keys in the saved OpenPGP keys file?'. The dialog has three buttons: 'Export Public Keys Only', 'Export Secret Keys', and 'Close'. Red arrows point to the 'Export Public Keys Only' and 'Export Secret Keys' buttons.

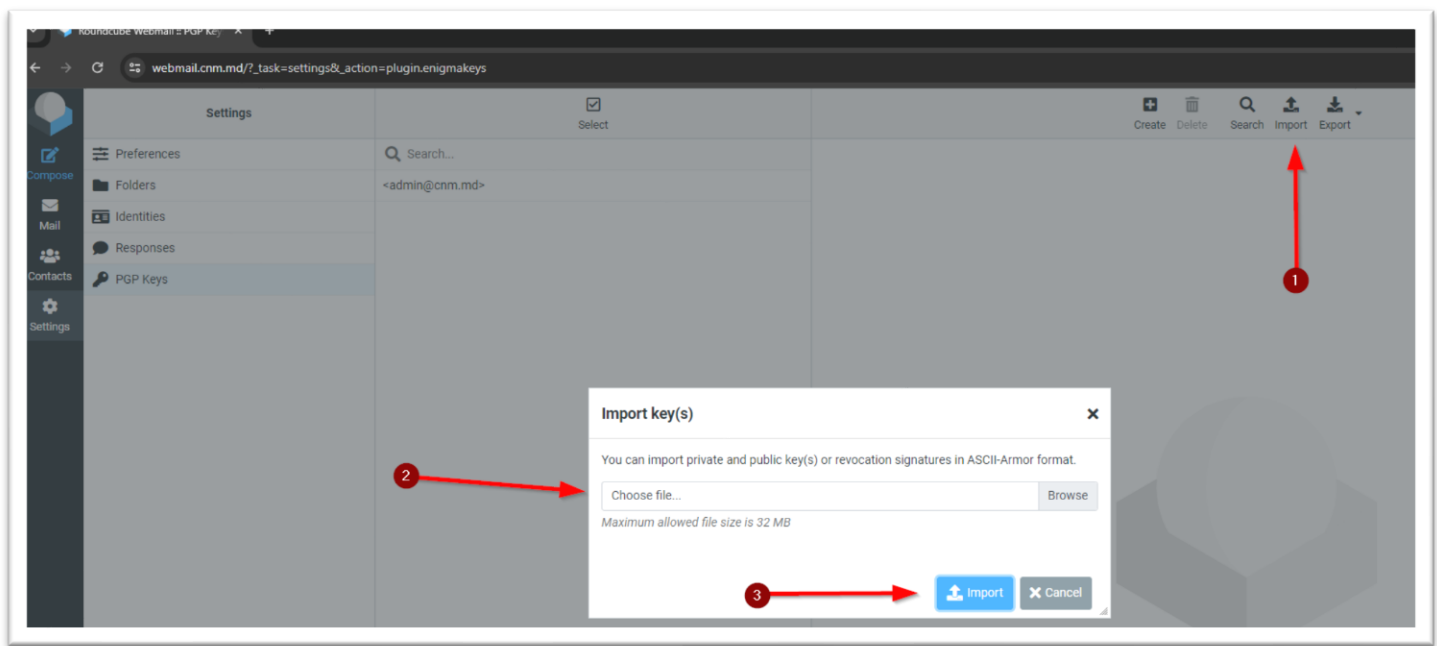
ID	Algorithm	Created	Expires
5AC3AD09	RSA (2048)	2024-02-21	never
		2024-02-21	never

- **Cheia Publică (Public Key):** *Aceasta este distribuită liber și poate fi partajată cu oricine.* Este folosită pentru a verifica semnături digitale și pentru a cripta mesaje către deținătorul cheii private corespunzătoare.
- **Cheia Privată (Private Key):** *Aceasta trebuie păstrată în secret.* Este folosită pentru a semna digital mesaje și pentru a decripta mesaje primite criptate cu cheia publică corespunzătoare.

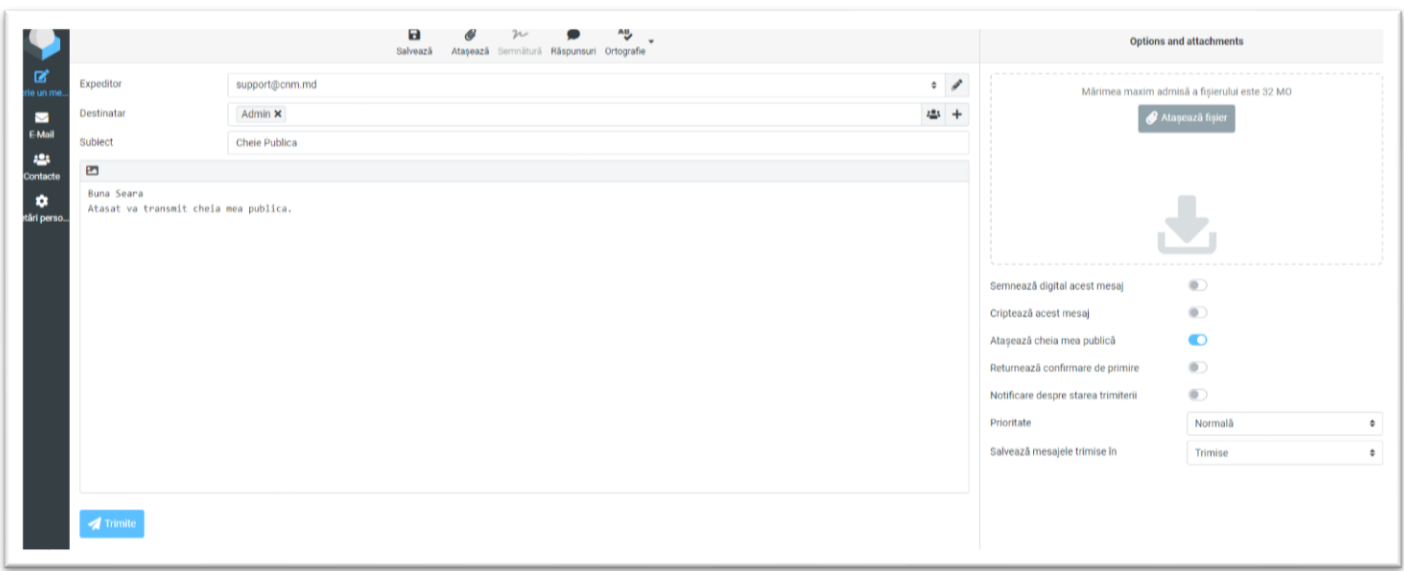
5. Pentru a trimite mesaje criptate altora sau pentru a le verifica semnăturile, aveți nevoie de cheile lor publice, deci este necesar să solicitați Cheile Publice de la corespondenții Dvs, iar ulterior să le importați în cutia Dvs. Postală. Avem 2 posibilități să importăm Cheile Publice ale corespondenților:

- În cazul în care deja avem cheia publică a unuia din corespondenți salvată în calculator, trebuie să o importăm în cutia noastră postală:

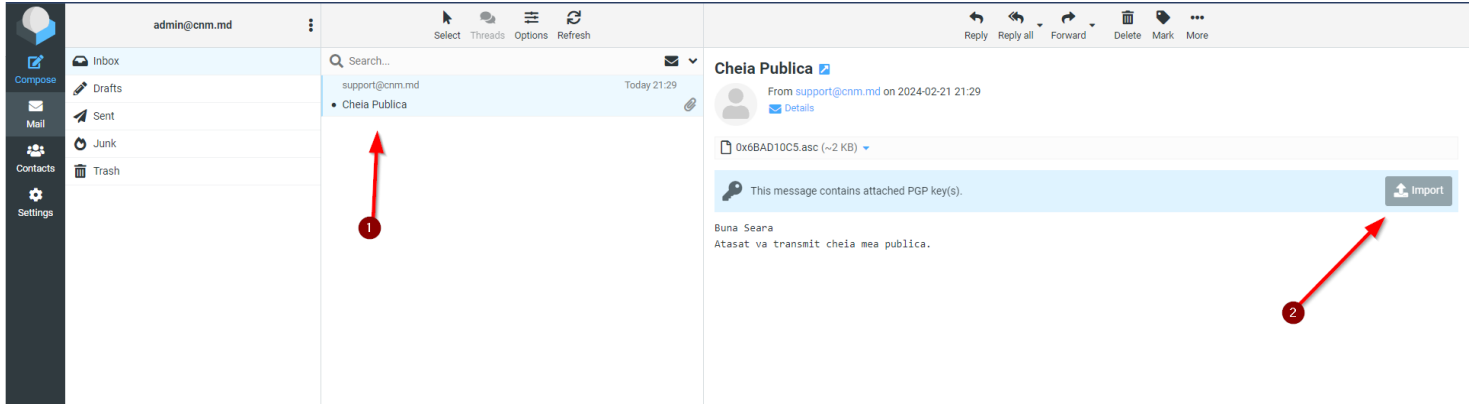
Import >> Choose file (alegem fisierul de pe calculator) >> Import – după importare veți avea cheia în lista cheilor publice din rubrica PGP Keys



- Titularul cheii publice poate să transmită cheia printr-un mesaj obișnuit în care să bifeze în meniul din partea dreaptă opțiunea **Atasează cheia mea publică**, deci de la utilizatorul support@cnm.md am transmis cheia publică către admin@cnm.md

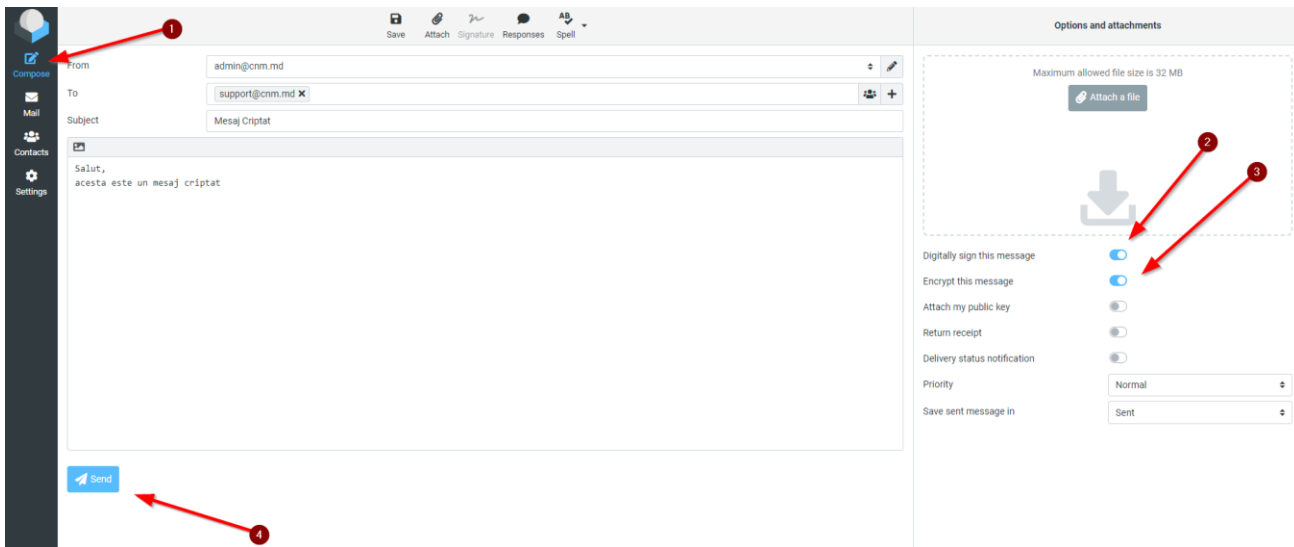


La deschiderea mesajului din cutia postala admin@cnm.md apasam butonul **Import**, iar ulterior gasim cheia importata in lista cheilor publice din rubrica PGP Keys

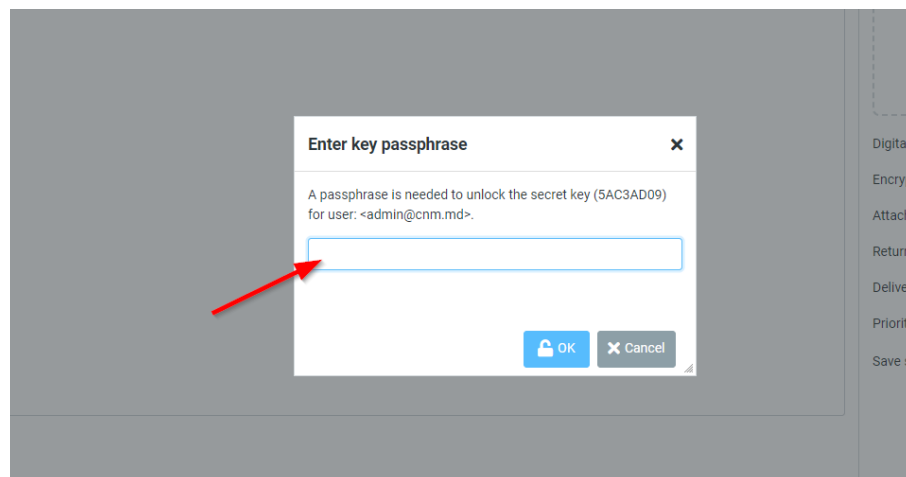


Criptarea și semnarea mesajelor

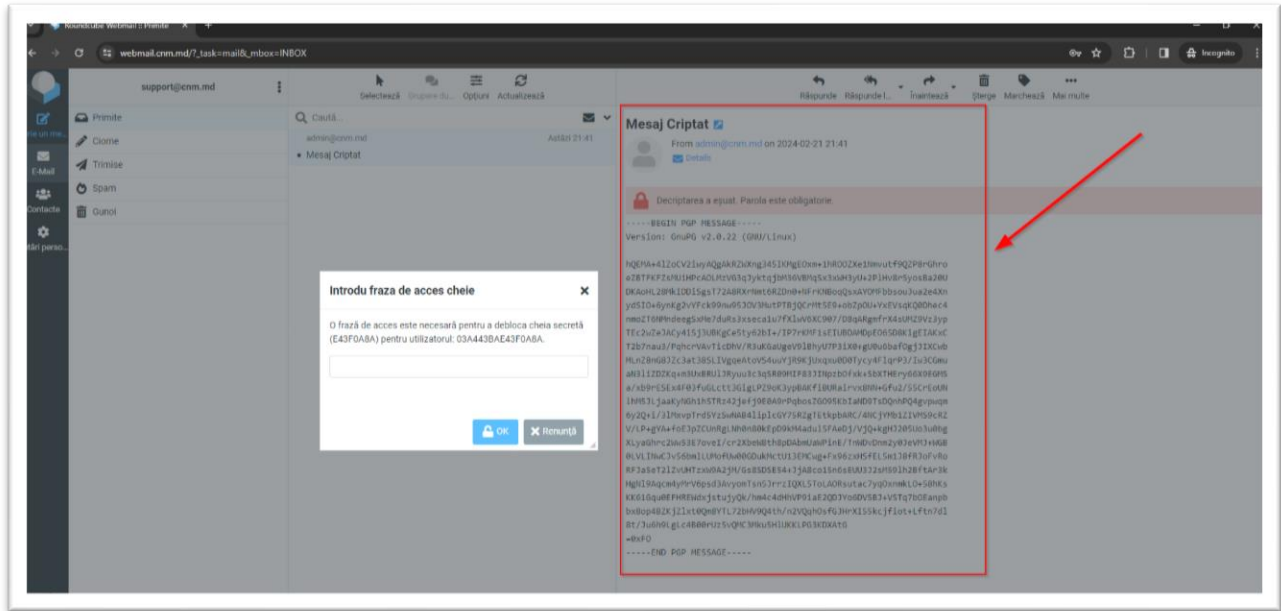
Compunerea mesajelor se face in mod obisnuit accesand butonul **Compose** din cutia Dvs postala, **pentru a semna si cripta mesajul**, din meniul din partea dreapta **vom pune bifele la Digitally sign this message si Encrypt this message** apoi butonul **Send**



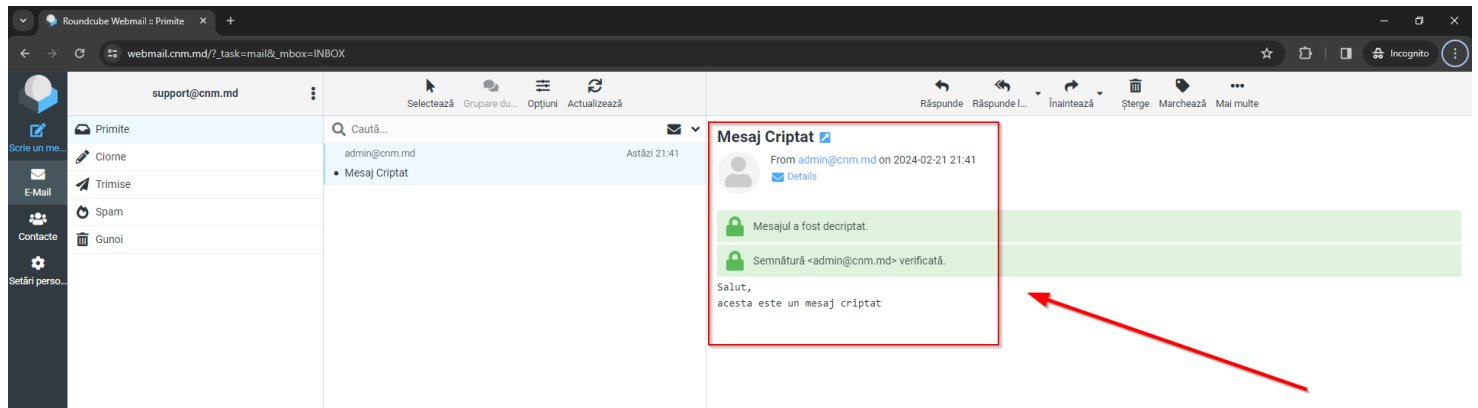
Dupa apasarea butonului de expediere, va fi necesar sa introduceti parola certificatului care a fost generate in punctul 3 din acest ghid si vom face click pe ok.



Citirea mesajului primit de la admin@cnm.md catre support@cnm.md, se va face la fel prin introducerea parolei setate la punctul 3. Mesajul din partea dreapta din prima poza de mai jos este criptat si nu poate fi citit de nimeni.



Dupa introducerea parolei, mesajul va fi disponibil pentru citire



Pentru transmiterea in regim obisnuit a mesajelor, nu se vor aplica bifele **Semneaza digital acest mesaj** si **Cripteaza acest mesaj**

