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.

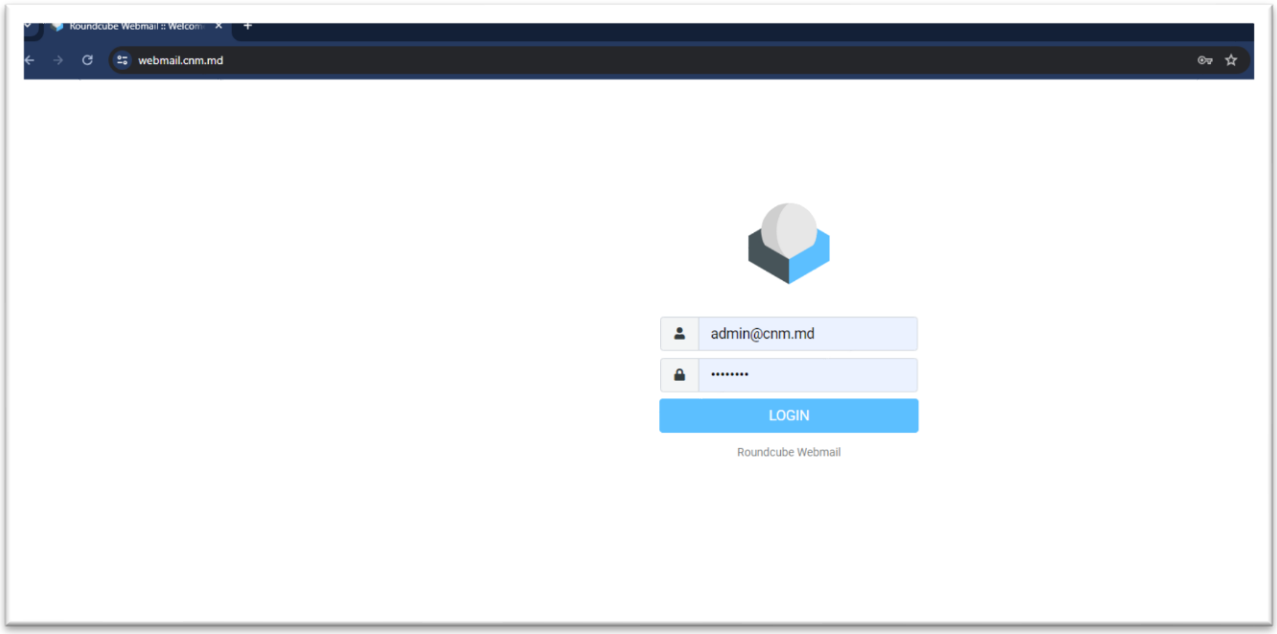
Mesajele criptate pot fi decriptate doar de către destinatarul legitim, care deține cheia privată corespunzătoare cheii publice folosite pentru criptare.

O pereche de chei PGP constă din:

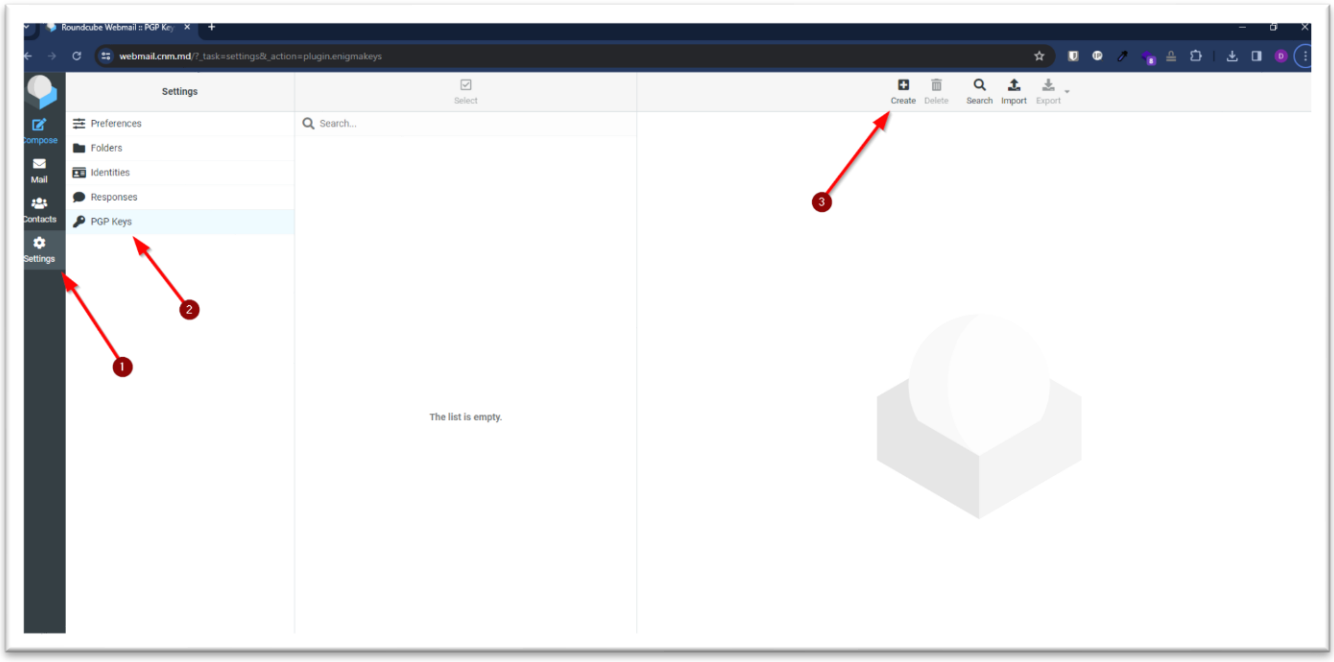
- **Cheia Publică (Public Key)**: Aceasta este distribuită liber și poate fi partajată cu oricine. Este folosită pentru a verifica semnături digitale și pentru a cripta mesaje către deținătorul cheii private corespunzătoare.
- **Cheia Privată (Private Key)**: Aceasta trebuie păstrată în secret. Este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

Pașii pentru crearea și utilizarea cheilor PGP

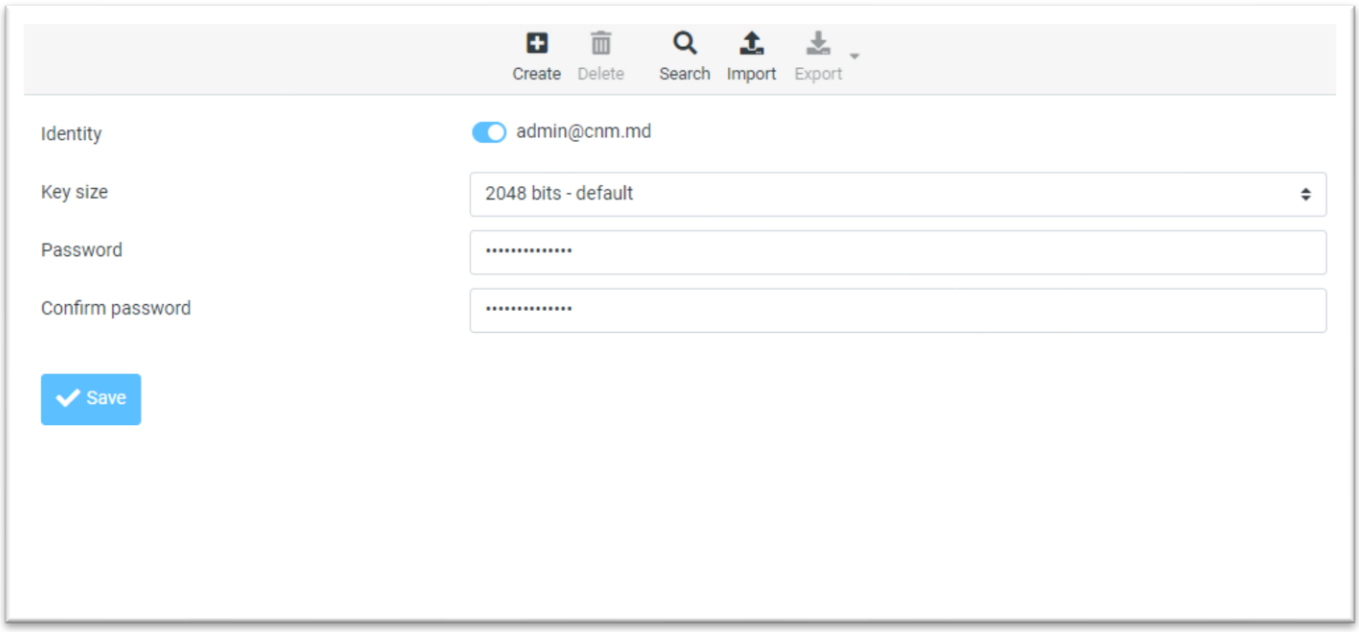
1. Accesam și ne logam pe interfața web a serviciului de poștă webmail.cnm.md



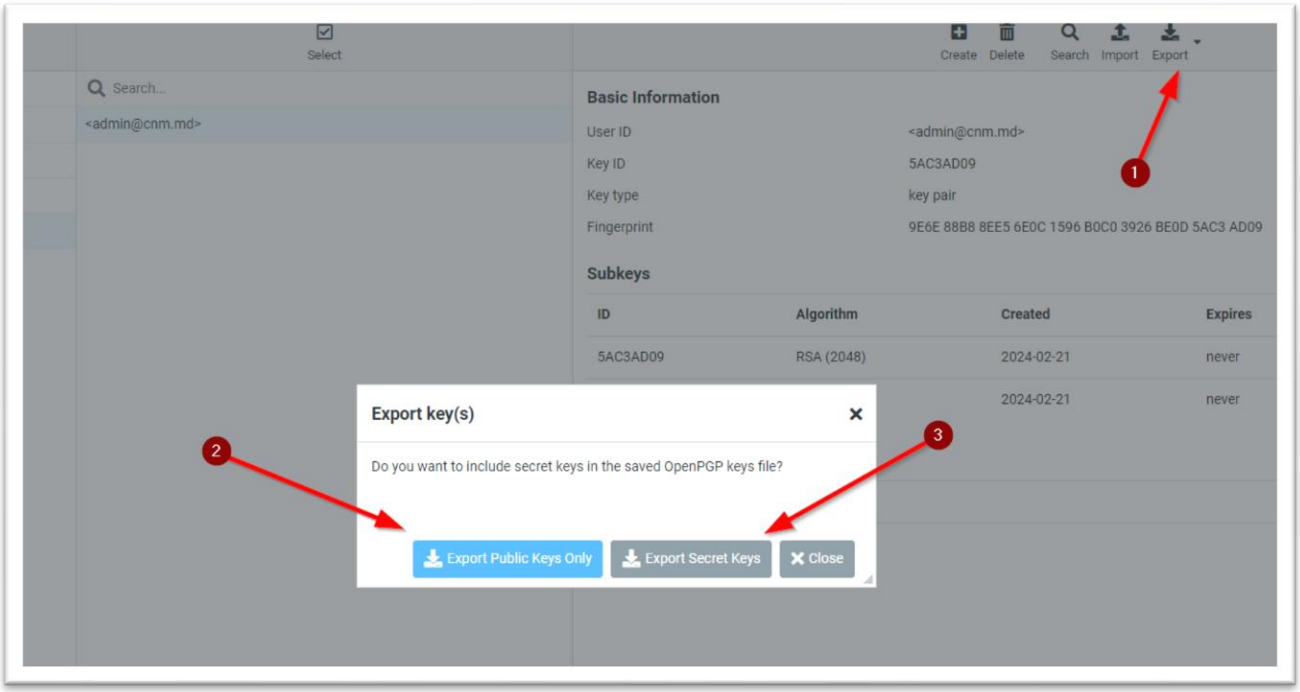
2. În secțiunea **Settings** găsim funcționalul **PGP Keys** și vom crea o cheie nouă:
   Settings >> PGP Keys >> Create



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



4. În lista de certificate, găsim certificatul generat de noi și putem vedea toată infromația 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

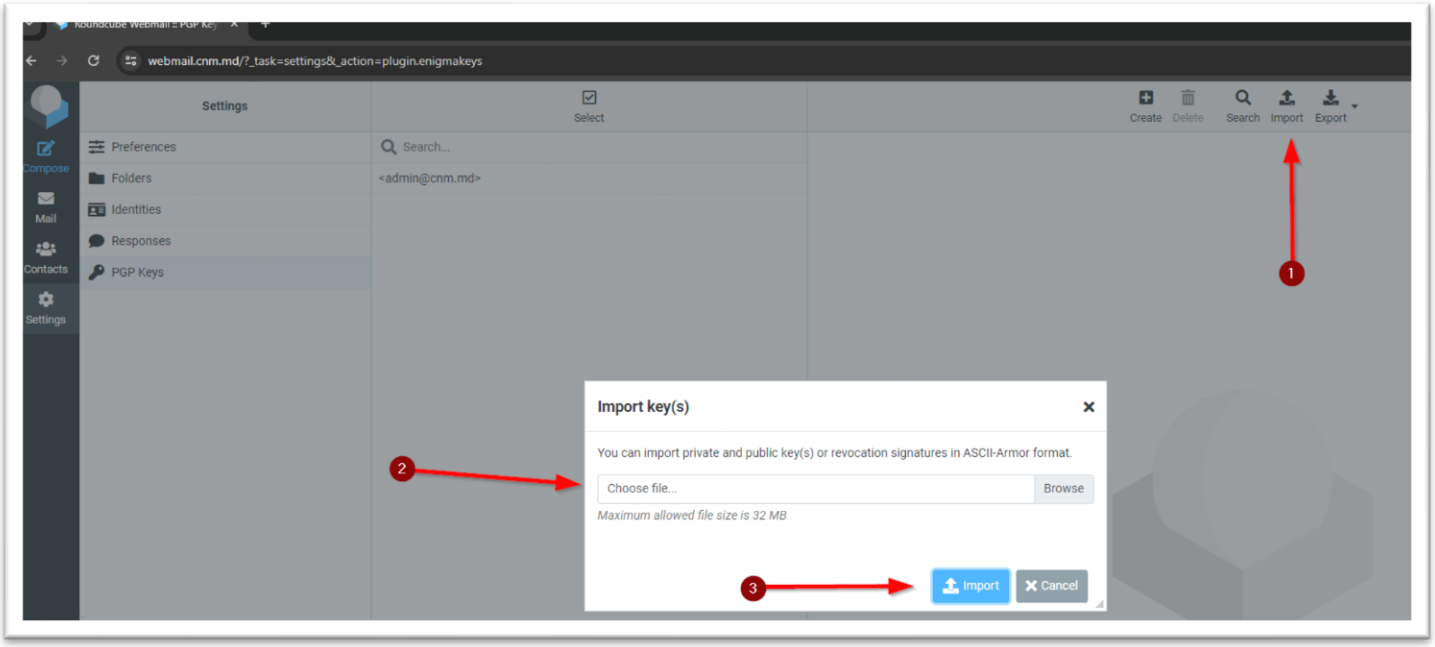


- **Cheia Publică (Public Key)**: ***Aceasta este distribuită liber și poate fi partajată cu oricine***. Este folosită pentru a verifica semnături digitale și pentru a cripta mesaje către deținătorul cheii private corespunzătoare.
- **Cheia Privată (Private Key)**: ***Aceasta trebuie păstrată în secret***.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

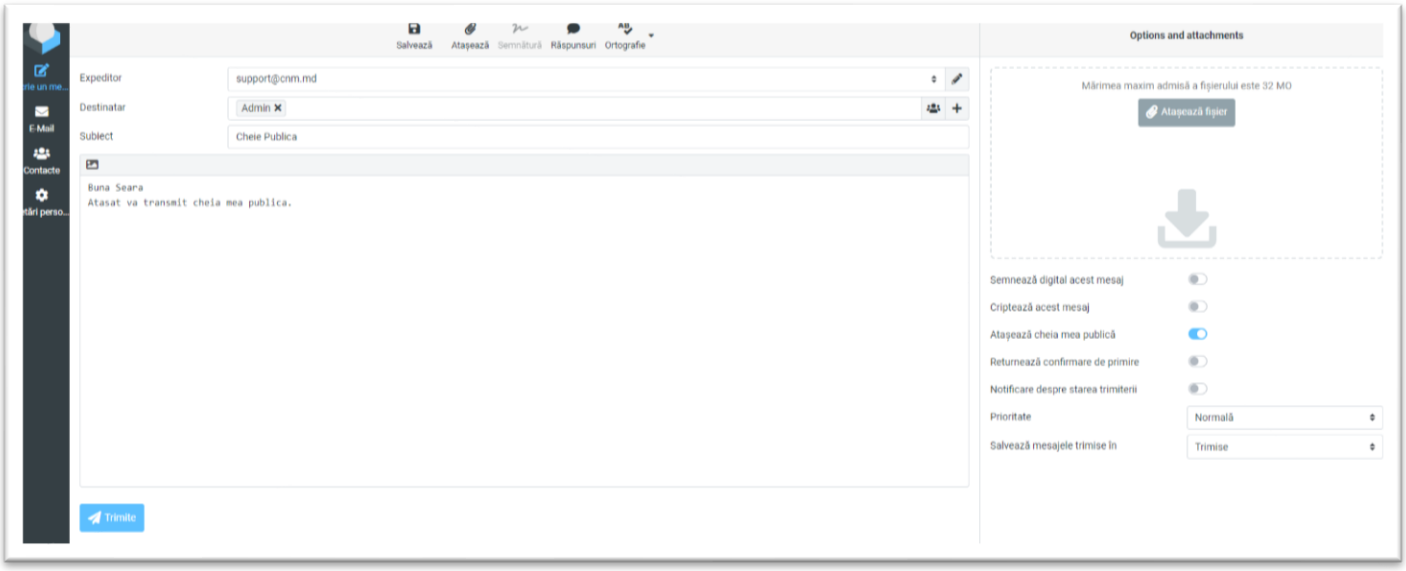
5. Pentru a trimite mesaje criptate altora sau pentru a le verifica semnăturile, aveți nevoie de cheile lor publice, deci este necesar sa solicitati Cheile Publice de la corespondentii Dvs, iar ulterior sa le importati in cutia Dvs. Postala. Avem 2 posibilitati sa importam Cheile Publice ale corespendentilor:

   - In cazul in care deja avem cheia publica a unuia din corespondenti salvata in calculator, trebuie sa o importam in cutia noastra postala:

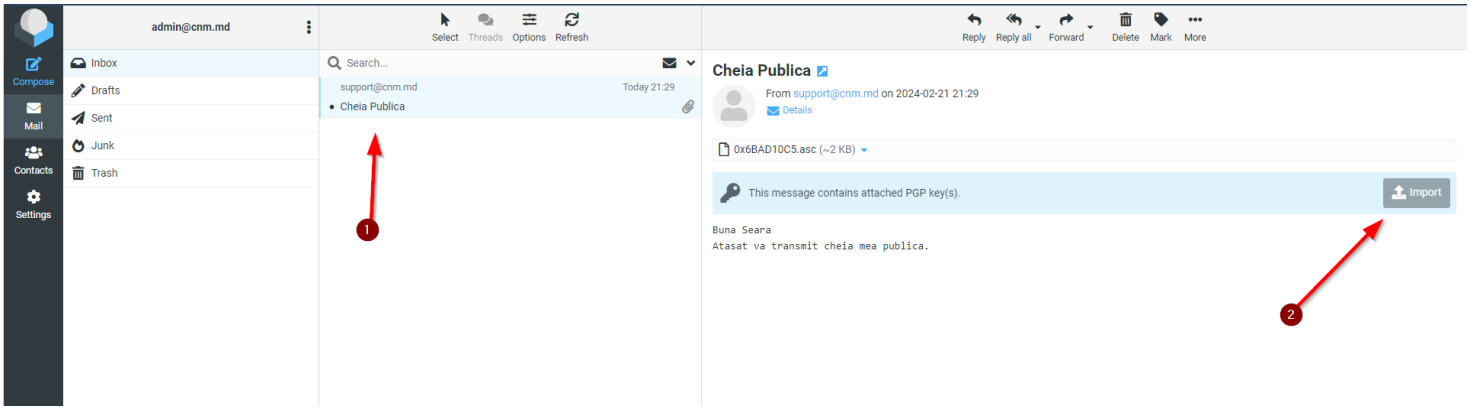
   Import >> Choose file (alegem fisierul de pe calculator) >> Import – dupa importare ve-ti avea cheia in lista cheilor publice din rubrica PGP Keys



   - Titularul cheii publice poate sa va transmita cheia printr-un mesaj obisnuit in care va bifa in meniul din partea dreapta optiunea **Ataseaza cheia mea publică,** deci de la utilizatorul support@cnm.md am transmis cheia publica catre admin@cnm.md

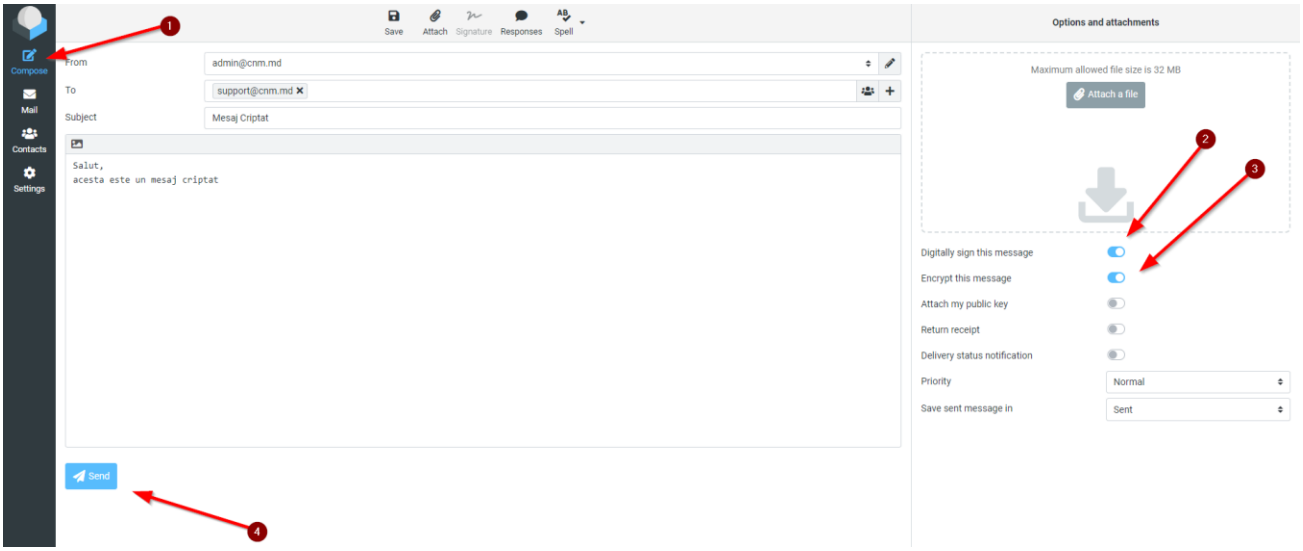


La deschiderea mesajului din cutia postala admin@cnm.md apasam butonul **Import,** iar ulterior gasim cheia importata in lista cheilor publice din rubrica PGP Keys

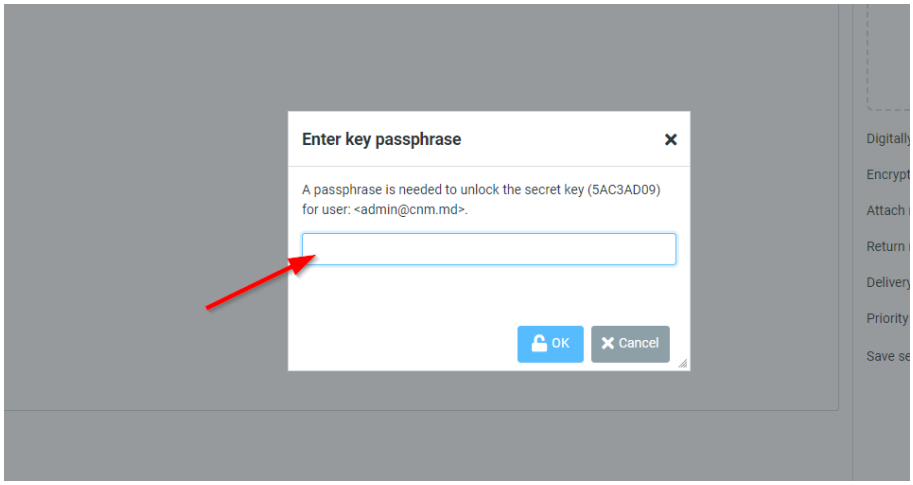


Criptarea și semnarea mesajelor

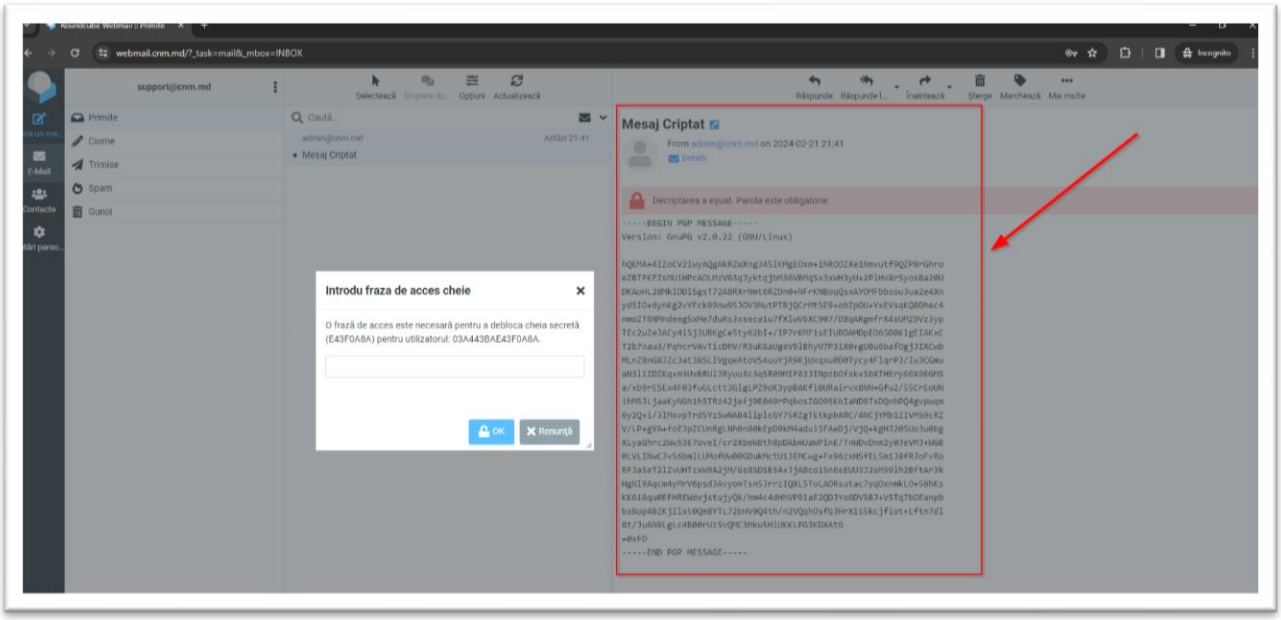
Compunerea mesajelor se face in mod obisnuit accesand butonul **Compose** din cutia Dvs postala, **pentru a semna si cripta mesajul**, din meniul din partea dreapta **vom pune bifele** la **Digitally sign this message si Encrypt this message** apoi butonul **Send**



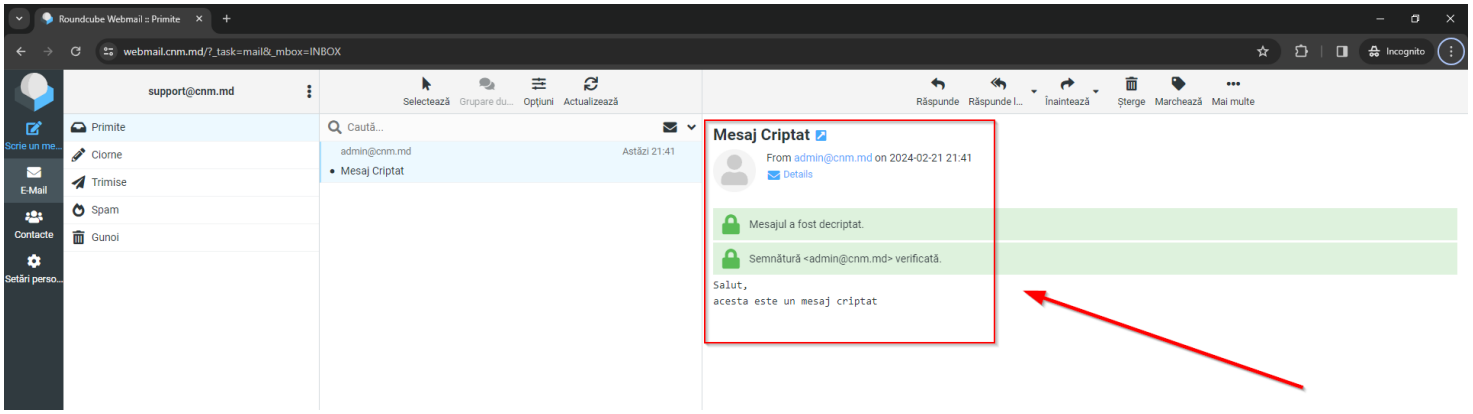
Dupa apasarea butonului de expediere, va fi necesar sa introduceti parola certificatului care a fost generate in punctul 3 din acest ghid si vom face click pe ok.



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**