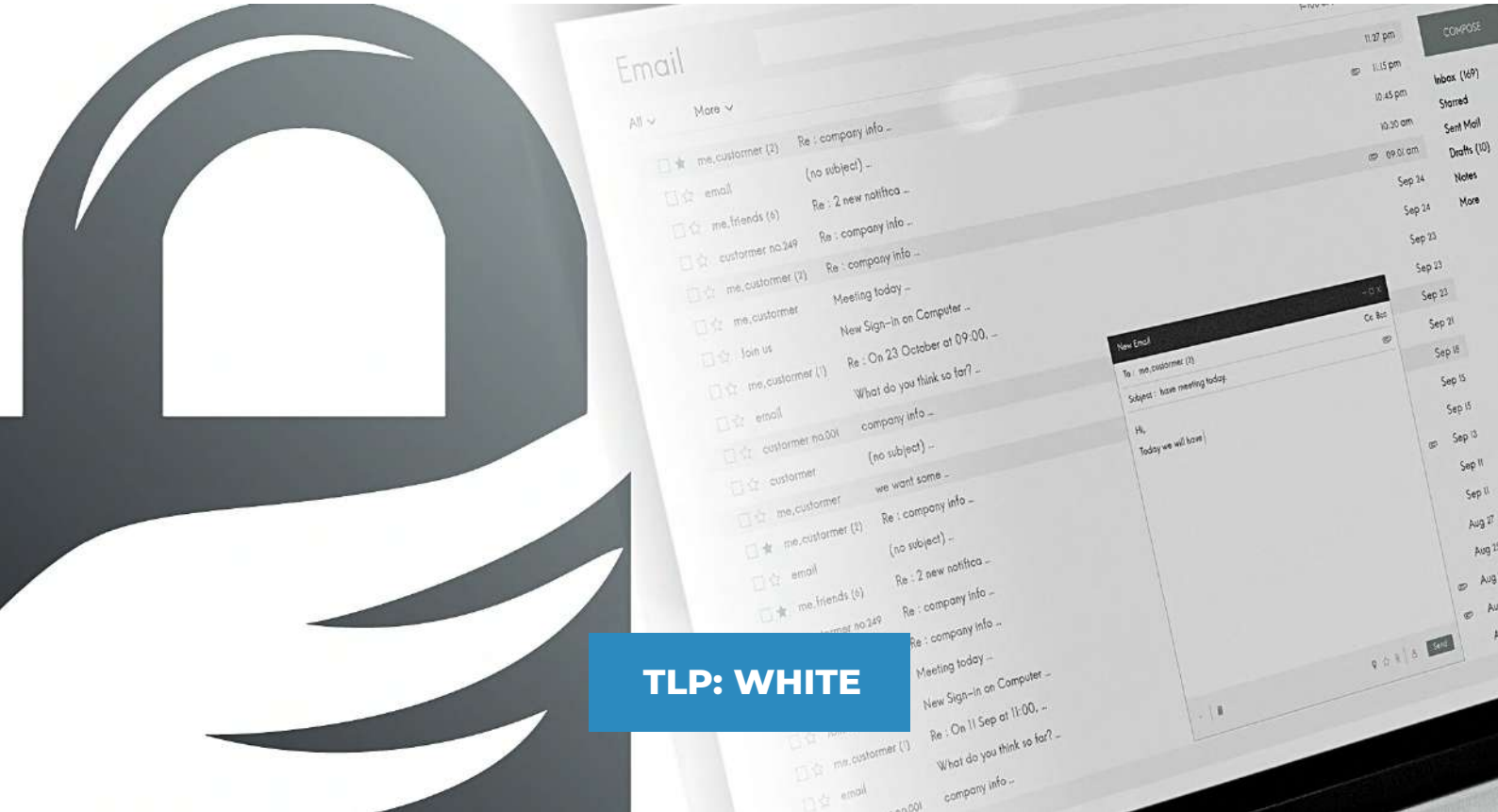
DIREKTORAT OPERASI KEAMANAN SIBER
NATIONAL CSIRT OF INDONESIA
Id-SIRTII/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE COORDINATION CENTER

PANDUAN PENGGUNAAN OPENPGP

MOZILLA THUNDERBIRD, ZIMBRA, DAN MICROSOFT OUTLOOK

DIREKTORAT OPERASI KEAMANAN SIBER

2022



TLP: WHITE

DAFTAR ISI

PRETTY GOOD PRIVACY (PGP)

Sejarah enkripsi End-to-End (E2E) bermula dari teknologi yang bernama Pretty Good Privacy (PGP) yang dikembangkan oleh Phil Zimmermann pada tahun 1991. PGP merupakan program komputer yang digunakan untuk melakukan pertukaran pesan rahasia melalui email. Pada awalnya kehadiran PGP menimbulkan pertentangan dari pemerintah Amerika Serikat karena diduga melanggar larangan mengenai ekspor alat kriptografi dengan alasan keamanan. Amerika Serikat bahkan melakukan penyelidikan terhadap Phil Zimmermann karena membagikan alat kriptografi kepada pengguna komputer di seluruh dunia.

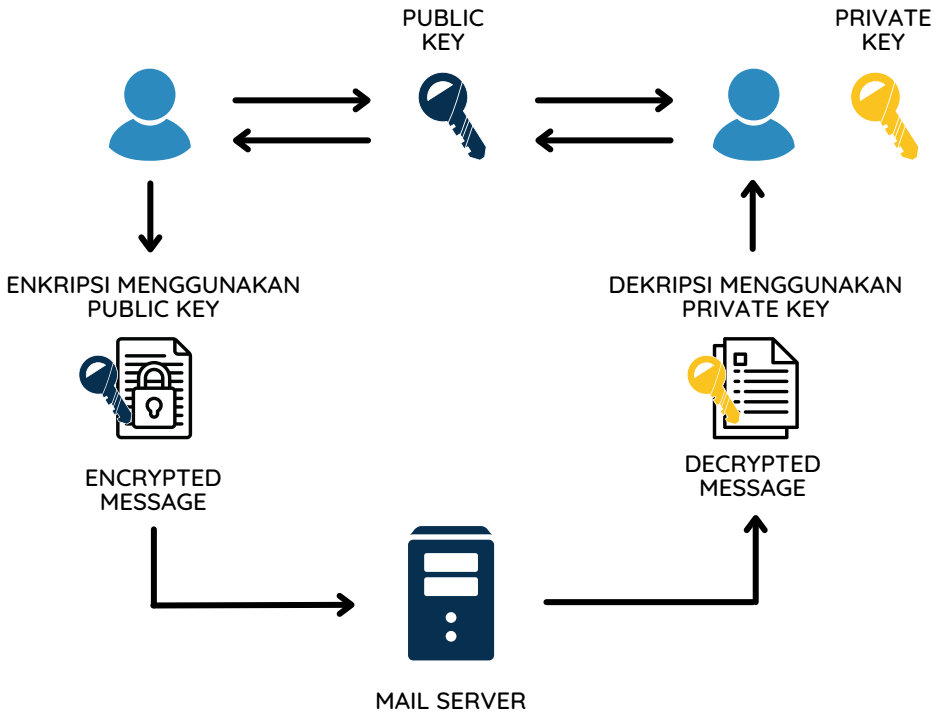
Kehadiran PGP membuat ahli teknologi mulai mengembangkan layanan enkripsi data yang aman untuk privasi pengguna, sepanjang tahun 1997 hingga 2011 muncul berbagai peningkatan PGP, salah satunya adalah OpenPGP. terdapat banyak versi dari software PGP yang telah diciptakan. Pada tahun 1997, Phil Zimmerman membuat proposal ke Internet Engineering Task Force (IETF) untuk pembuatan standar PGP open-source. Proposal tersebut kemudian diterima dan mengarah pada pembuatan protokol OpenPGP, yang hingga saat ini menjadi format standar untuk kunci dan pesan enkripsi.

SKEMA PENGGUNAAN OPENPGP

PGP menggunakan 2 kunci yaitu:

Private Key: Kunci yang hanya boleh dimiliki oleh user yang bersangkutan. Private key digunakan untuk melakukan dekripsi dan memberikan digital sign terhadap pesan yang akan dikirimkan.

Public Key: Kunci yang boleh disebarkan ke user-user lain. Public key digunakan untuk mengenkripsi pesan yang ditujukan kepada pemilik private key.



Pada saat ini, OpenPGP telah banyak digunakan dan disediakan secara built-in pada email client (aplikasi email). Contoh email client yang memanfaatkan OpenPGP untuk menyediakan pengiriman email terenkripsi bagi penggunananya adalah Mozilla Thunderbird, Zimbra, dan Microsoft Outlook.

PENGGUNAAN OPENPGP PADA MOZILLA THUNDERBIRD

MOZILLA THUNDERBIRD

Mozilla Thunderbird adalah perangkat lunak email client yang dikembangkan oleh Mozilla Foundation. Pada 7 Desember 2004, versi 1.0 dirilis dan diunduh lebih dari 500.000 juta kali dalam 3 hari pertama. Pada saat ini mozila thunderbird versi terakhir adalah 91.5.1. Mulai pada versi 78.2.1 Mozilla Thunderbird telah mengintegrasikan OpenPGP langsung ke dalam aplikasi utama. Sehingga, Tidak diperlukan add-on untuk mengirimkan email terenkripsi.

INSTALASI

Untuk melakukan instalasi Mozilla Thunderbird dapat langsung mengunjungi web resmi dari Mozilla Thunderbird dan mengunduh file aplikasi sesuai dengan sistem operasi yang digunakan. Selain tersededia dalam berbagai sistem operasi, Mozilla Thunderbird juga tersedia dalam berbagai bahasa. Berikut merupakan tautan untuk mengunduh Mozilla Thunderbird :
https://www.thunderbird.net/en-US/thunderbird/all/

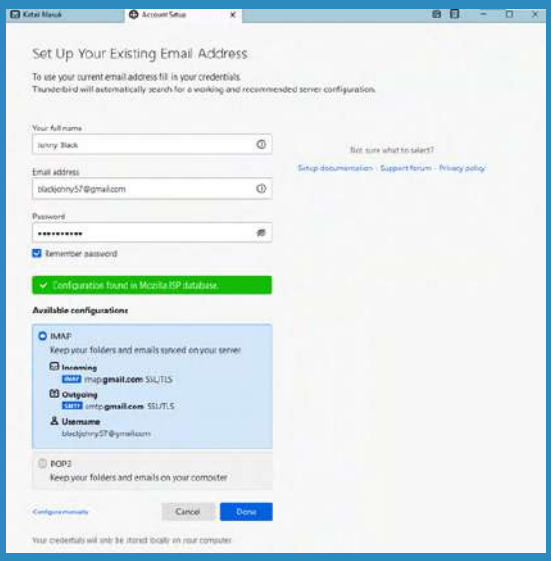
KONFIGURASI AKUN

Sebelum dapat menggunakan Mozilla Thunderbird lakukan konfigurasi akun dengan memasukkan email yang akan digunakan dan memilih protokol email yang digunakan atau didukung server email masing-masing. Terdapat beberapa langkah yang dilkukan pada tahap ini yaitu:

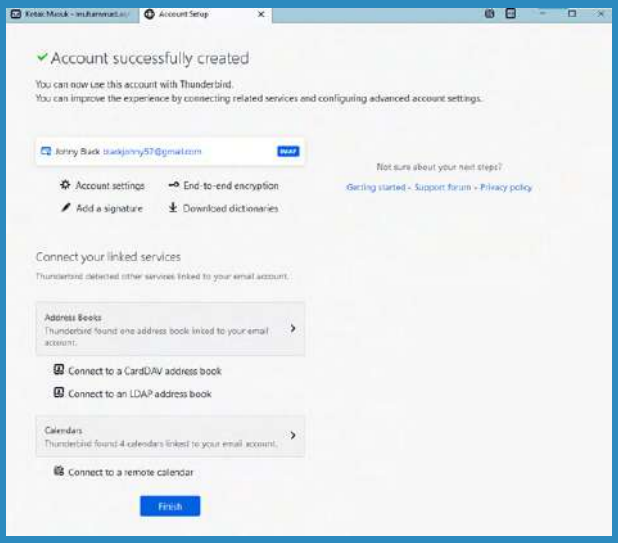
1. Mengisi Nama Pengguna
2. Masukkan alamat email yang akan digunakan
3. Masukkan password yang akan digunakan untuk login akun mozilla thunderbird

4. Pilih protokol email yang didukung server email masing-masing, lalu klik done

- IMAP : Email disimpan pada server
- POP3 : Email disimpan pada komputer secara lokal

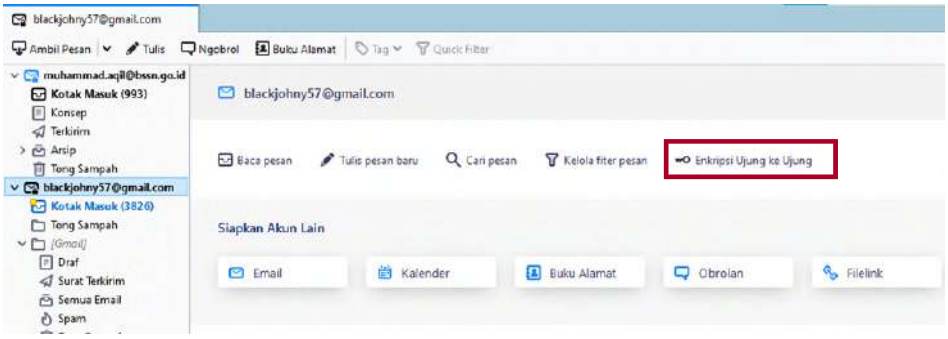


5. Klik Finish setelah berhasil melakukan proses konfigurasi akun



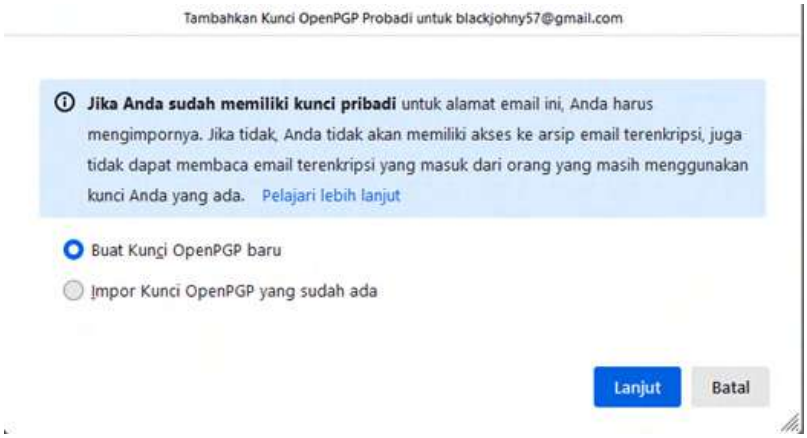
GENERATE KEY PAIR

1. Pada tampilan utama Klik pada “Enkripsi Ujung ke Ujung”

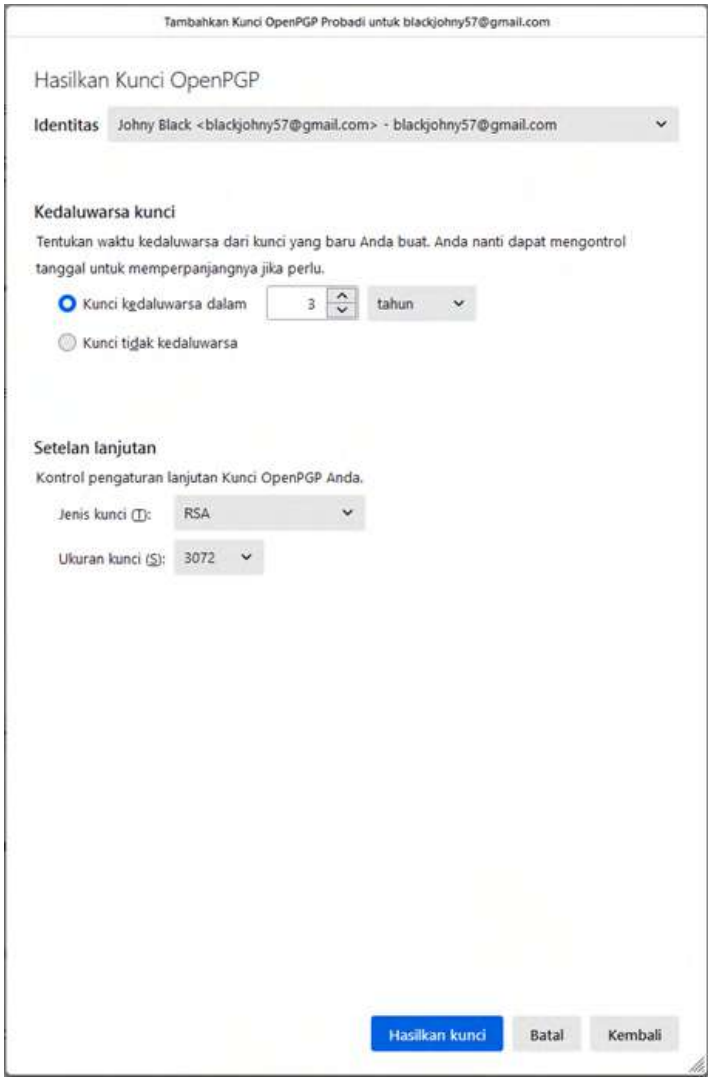


2. Klik pada “Tambahkan Kunci…”

3. Pilih **"Buat Kunci OpenPGP baru"** apabila belum memiliki pasangan kunci publik dan private, dan apabila telah memiliki pasangan kunci dapat dipilih **"Impor Kunci OpenPGP yang sudah ada"**



4. Atur masa berlaku kunci, dan algoritma enkripsi serta panjang kunci yang akan dibangkitkan. Secara default masa berlaku kunci diatur akan kadaluwarsa dalam 3 tahun, algoritma enkripsi menggunakan RSA, dan ukuran kunci adalah 3072. Apabila sudah diatur klik "Hasilkan Kunci"



PERTUKARAN KUNCI PUBLIK

Berkomunikasi menggunakan email terenkripsi dapat dilakukan ketika memiliki kunci publik orang yang akan dikirimi pesan terenkripsi. Mereka juga membutuhkan kunci publik kita untuk mengirim kembali pesan secara terenkripsi.

1. Buat pesan baru dengan klik “Tulis pesan baru” pada menu utama
2. Tulis pesan dan lampirkan kunci publik

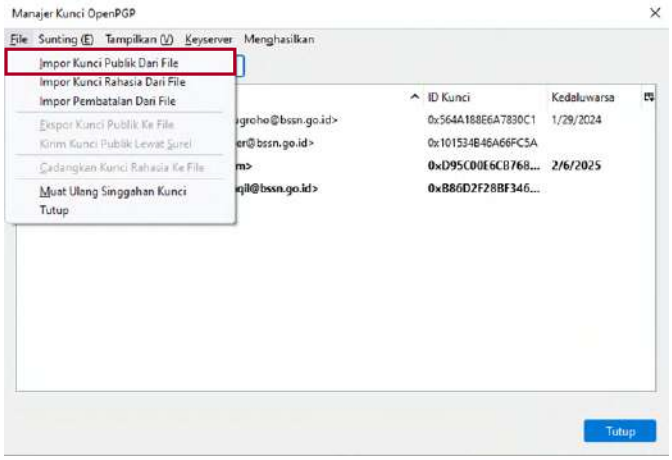
3. Kirim pesan ke penerima pesan

IMPORT PUBLIC KEY

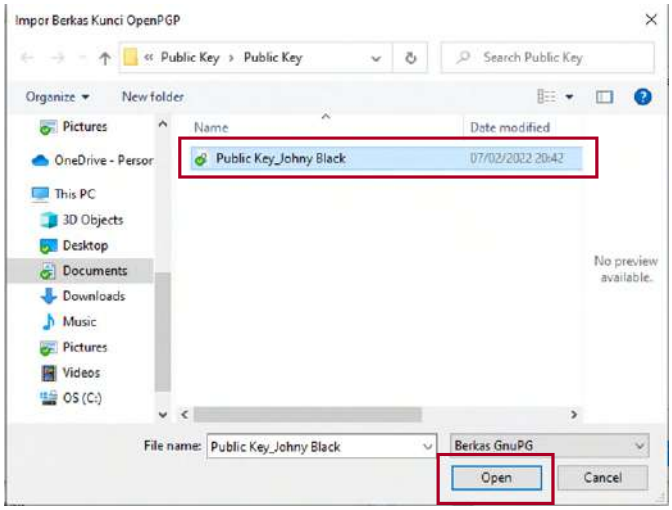
Pengirim pesan sebelum melakukan komunikasi rahasia harus memiliki kunci publik penerima pesan. Oleh karena itu, kedua belah pihak harus melakukan import pada email client masing-masing yang digunakan.

1. Buka pesan email berisi lampiran public key yang telah diterima
2. Unduh public key lalu klik “simpan” pada bagian lampiran email.

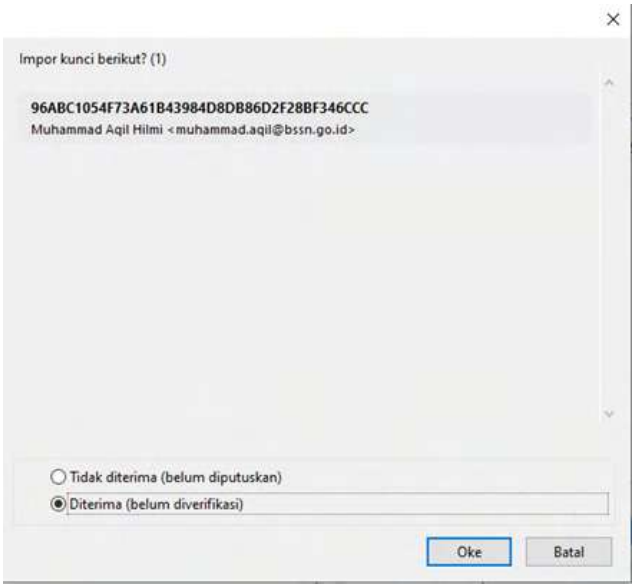
4. Pada tampilan utama, Klik “Enkripsi Ujung ke Ujung”
5. Klik pada “Manjer Kunci OpenPGP”
6. Pilih “File” lalu klik “Impor Kunci Publik Dari File”



7. Pilih file kunci publik yang telah diunduh sebelumnya, Klik “Open”.



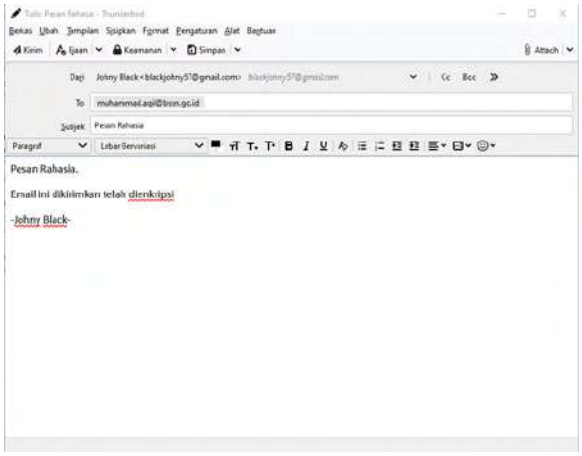
8. Klik Pilihan “Diterima (belum diverivikasi)” lalu klik “Oke”



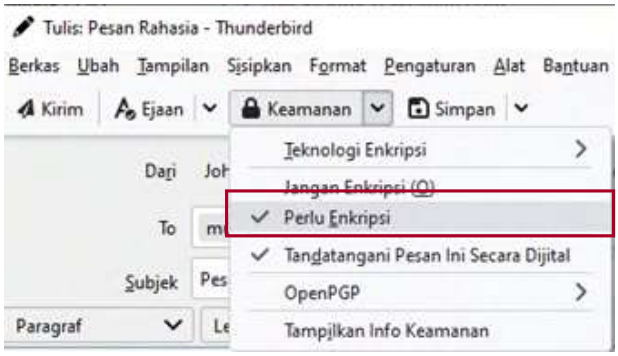
MENGIRIM PESAN TERENKRIPSI

Setelah melakukan pertukaran kunci dan melakukan import kunci publik. Kita dapat melakukan kirim terima email secara aman dengan enkripsi end-to-end.

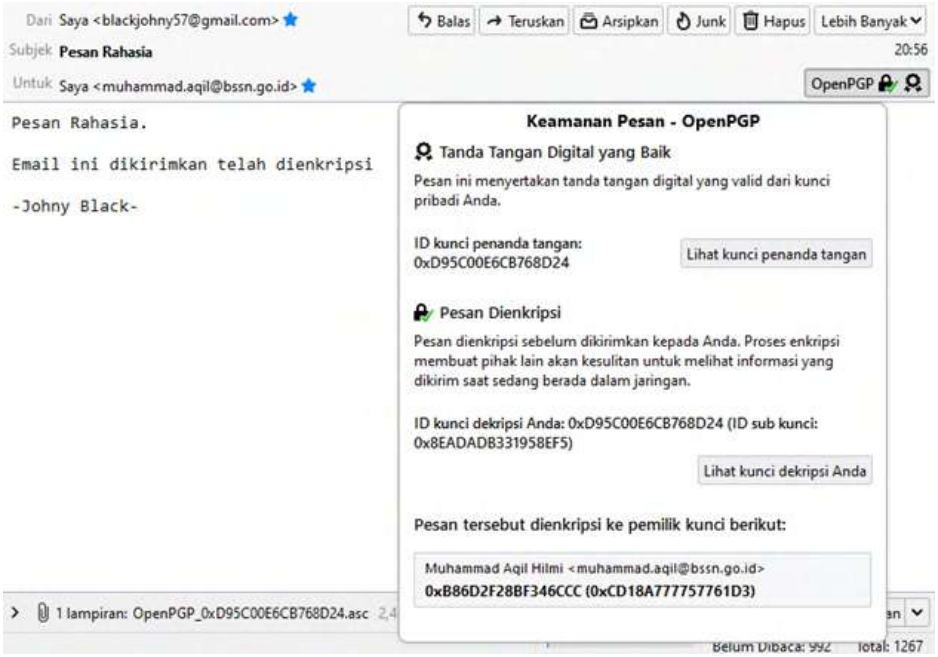
1. Buat pesan baru



2. Buka Tab "Keamanan" dan pilih "Perlu Enkripsi".



3. Kirim pesan
4. Penerima pesan akan mendapatkan pesan yang dikirimkan dan akan secara otomatis didekripsi oleh Mozilla Thunderbird dan langsung ditampilkan



PENGGUNAAN OPENPGP PADA ZIMBRA

ZIMBRA

Zimbra Mail Collaboration adalah produk dari Synacor yang dapat membagikan surat, dokumen, kalender, dan lain-lain kepada pengguna internal maupun eksternal secara aman. Zimbra Mail Collaboration memberikan kebebasan serta kemudahan para penggunanya untuk bekerja secara virtual dari mana saja dengan menggunakan perangkat tablet, ponsel, ataupun laptop. Server Zimbra Mail Collaboration juga menyediakan dukungan penuh lintas platform dengan integrasi pada sistem operasi utama seperti Windows, Mac, dan Linux desktop.

OpenPGP berbasis pada PGP (Pretty Good Privacy) merupakan tool untuk enkripsi email, hadir pada Zimbra dalam bentuk Zimlets atau Add on yang dibuat oleh Barry De Graaff.

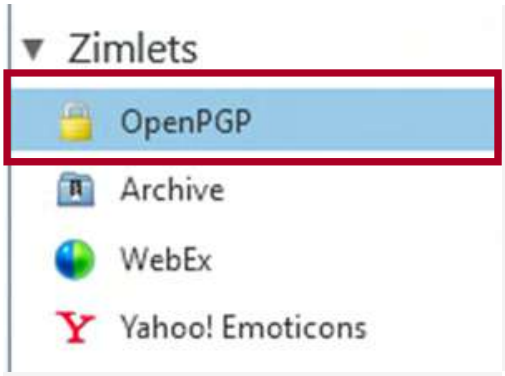
INSTALASI

Pada Zimbra Mail Server, OpenPGP dikemas dalam bentuk Zimlets atau Add-On tambahan. Zimlet hanya bekerja pada Zimbra versi 8.8.15, 9.0 dan diatasnya.

Install Zimbra OpenPGP Zimlet versi 2.7.7

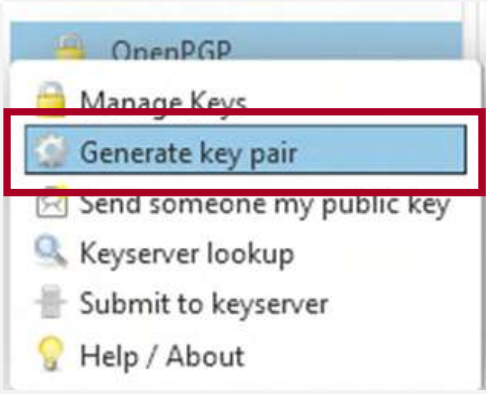
```
[root@myzimbra ~]# rm -Rf /opt/zimbra/zimlets-
deployed/_dev/tk_barrydegraaff_zimbra_openpgp/
[root@myzimbra ~]# su zimbra
[zimbra@myzimbra ~] wget https://github.com/Zimbra-Community/pgp-
zimlet/releases/download/2.7.7/tk_barrydegraaff_zimbra_openpgp.zip -O
/tmp/tk_barrydegraaff_zimbra_openpgp.zip
[zimbra@myzimbra ~] zmzimletctl deploy /tmp/tk_barrydegraaff_zimbra_openpgp.zip
[zimbra@myzimbra ~] zmmailboxdctl restart
```

GENERATE KEY PAIR

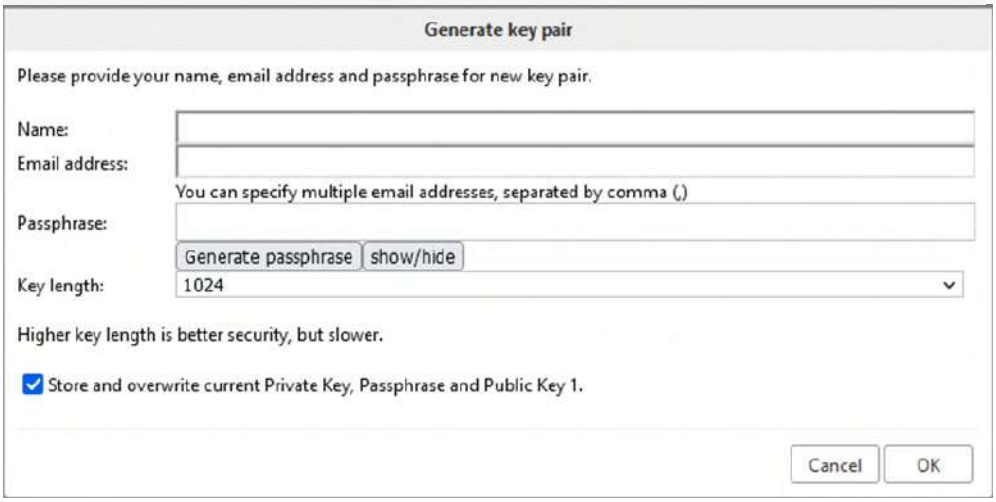


1. Login WebMail Zimbra
2. Buka tab openPGP yang terletak di bagian kiri bawah pada bagian Zimlets

3. Klik kanan pada openPGP dan pilih Generate key pair



4. Isi bagian name, Email address, passphrase, dan key length, default nya adalah 1024 namun anda dapat mengubahnya. Passphrase digunakan pada saat anda akan membuka email yang terenkripsi

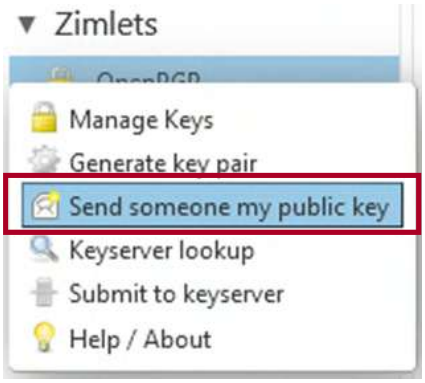


5. Setelah selesai anda akan mendapatkan Private Key dan Publik Key, simpan kunci tersebut di tempat yang aman.

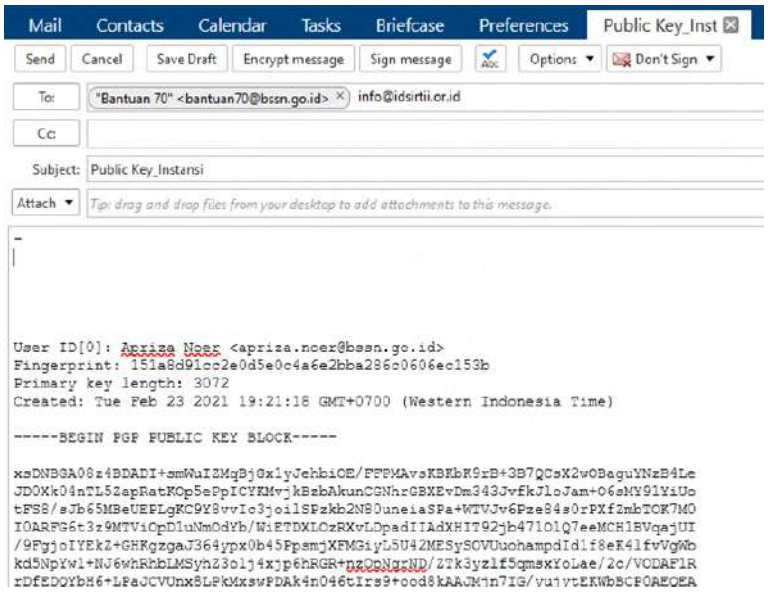
MEMBAGIKAN DAN IMPORT PUBLIC KEY

Agar dapat mengirimkan pesan dalam bentuk enkripsi dan diterima oleh user yang telah ditentukan diperlukan pertukaran Public Key antara pengirim dan penerima.

1. Klik kanan pada openPGP dan pilih Send someone my public key



2. Public Key akan dikirimkan sebagai email kepada penerima

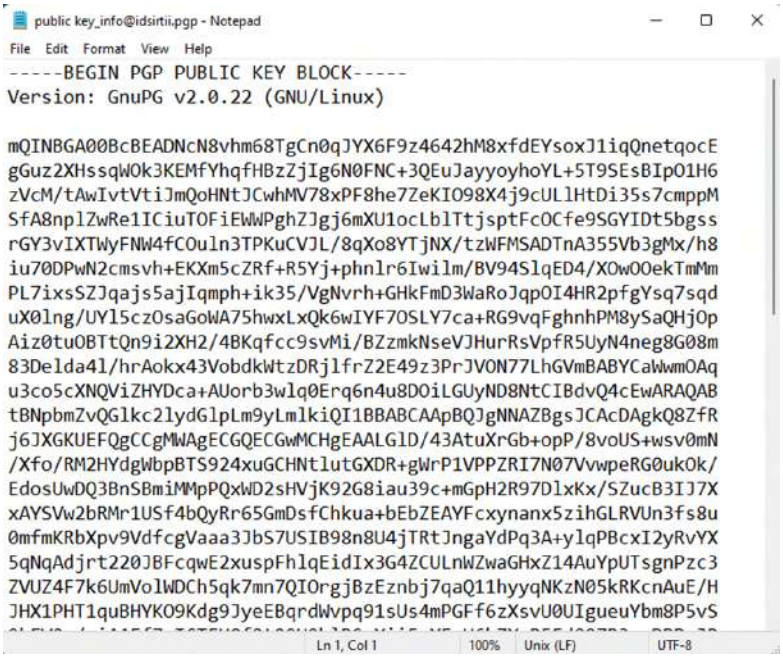


3. Setelah Public Key terkirim, pada email penerima dapat melakukan import public key tersebut dengan mengklik import public key

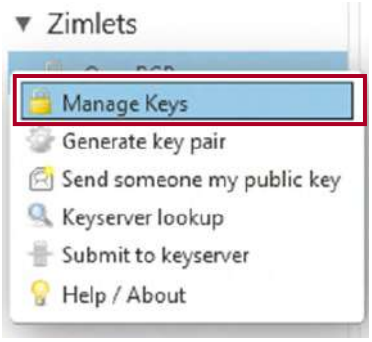
4. Tekan ok untuk melakukan import public key

Jika public key diterima tidak melalui email, sehingga tidak muncul pilihan import secara langsung dapat dilakukan import sebagai berikut:

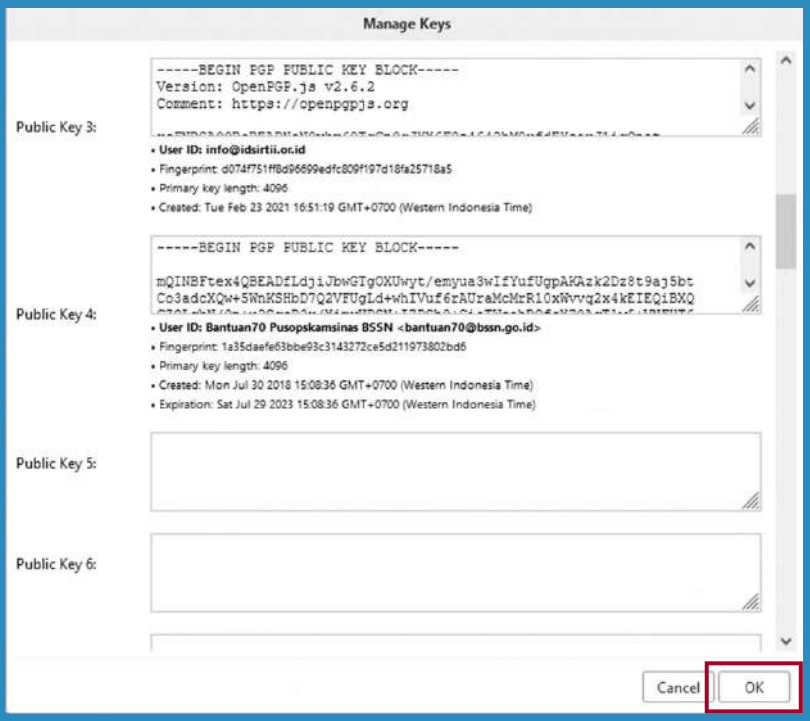
1. Buka file public key menggunakan notepad ataupun text editor yang lain kemudian copy isinya.



2. Klik kanan pada openPGP kemudian pilih Manage Keys



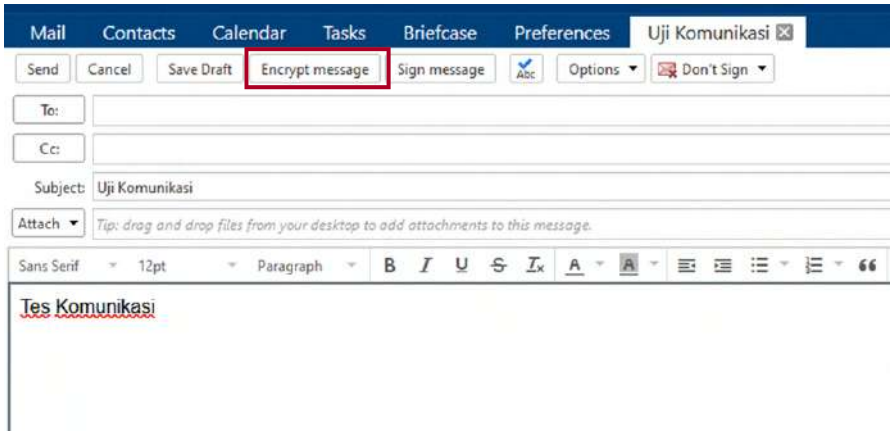
3. Paste public key yang sudah dicopy sebelumnya ke dalam kolom yang tersedia. Pilih kolom Public Key selain kolom Public Key 1. Kemudian klik OK untuk menyimpan



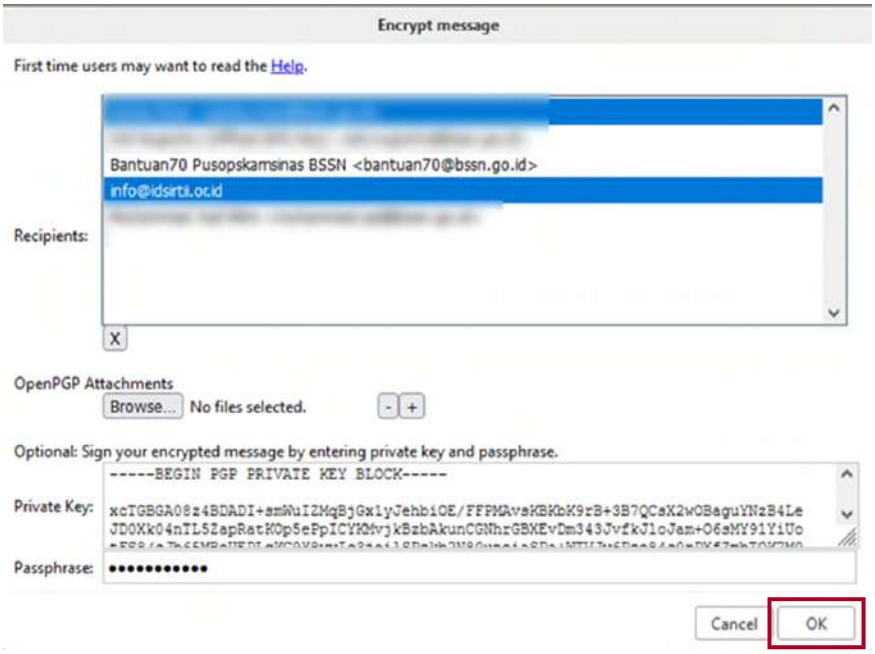
UJI COBA MENGIRIM PESAN TERENKRIPSI

Sebelum melakukan uji coba, pastikan pengirim dan penerima sudah memiliki Public Key masing-masing

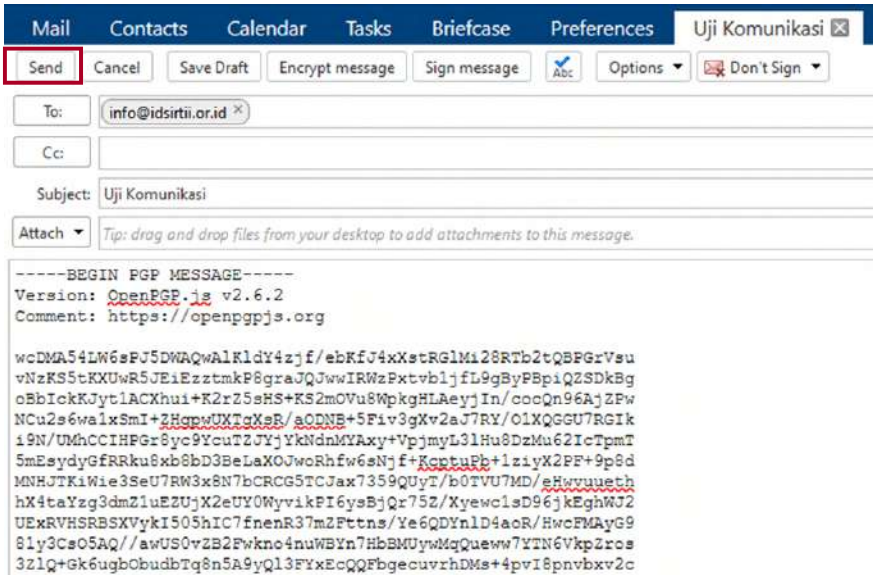
1. Buat email baru lalu klik Encrypt Message



2. Pilih penerima email, lalu klik OK jika telah selesai



3. Email akan terenkripsi seperti berikut, Klik send untuk mengirim email terenkripsi



4. Penerima akan menerima email dan terdapat tanda tangan (signature) pada email

PENGGUNAAN OPENPGP PADA OUTLOOK

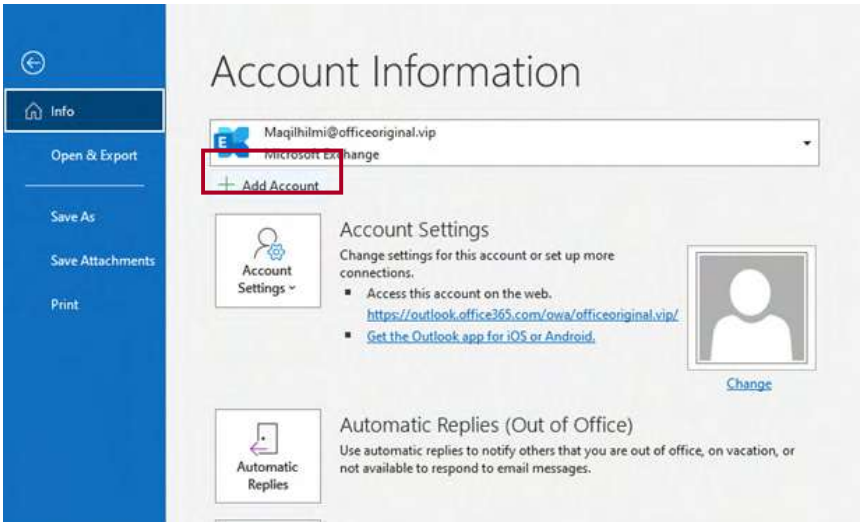
MICROSOFT OUTLOOK

Microsoft Outlook adalah salah satu aplikasi yang memiliki fungsi utama untuk mengirim, menerima, maupun membaca pesan email yang masuk. Namun selain itu, Microsoft Outlook ini memiliki fungsi lain yang bisa dimaanfaatkan. Fungsi lain tersebut adalah membuat jadwal kerja, kalender, dan catatan. Disamping itu Microsoft Outlook juga dapat digunakan untuk melakukan kirim terima email secara aman dengan terenkripsi.

MEMBUAT DAN MENAMBAHKAN AKUN MICROSOFT OUTLOOK

Pada Microsoft Outlook menyediakan pengguna untuk dapat menggunakan lebih dari satu akun. Pengguna dapat menambahkan email dengan membuat akun baru dengan cara sebagai berikut :

1. Klik pada tab “File”
2. Kemudian klik “Add Account”



3. Isikan Email, dan Password Email yang akan digunakan

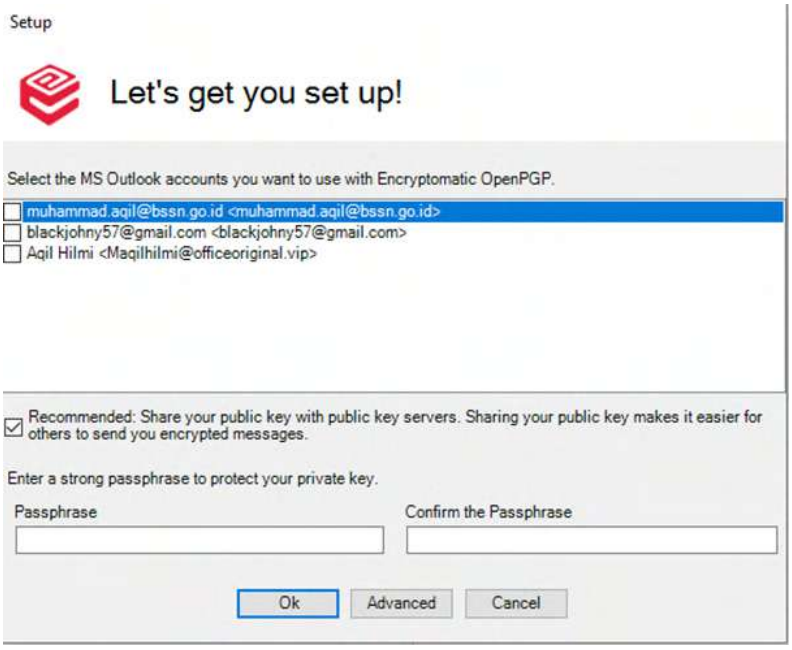
Kirim terima email terenkripsi menggunakan Microsoft Outlook membutuhkan tool tambahan atau add-on yang harus terpasang terlebih dahulu pada perangkat yang akan digunakan. Salah satu add-on yang dapat digunakan adalah Encryptomatic.

INSTALASI ENCRYPTOMATIC

Aplikasi Encryptomatic dapat diunduh melalui web resminya. Unduh installer aplikasi, lalu lakukan instalasi. Lakukan instalasi dengan menjalankan installer aplikasi dengan hak Administrator. Berikut merupakan tautan untuk mengunduh aplikasi tersebut https://www.encryptomatic.com/openpgp/

KONFIGURASI DAN GENERATE PASANGAN KUNCI

Setelah melakukan instalasi, buka Microsoft Outlook. Encryptomatic akan menampilkan tampilan konfigurasi OpenPGP.



1. Pilih akun email untuk penggunaan OpenPGP.
2. Encryptomatic menyediakan pilihan untuk melakukan publikasi kunci publik pada server kunci publik. Apabila tidak mengkehendaki hal tersebut dapat menghilangkan chechlist begitu juga sebaliknya
3. Isikan passphrase untuk melindungi private key yang akan dibangkitkan
4. Klik “Ok”

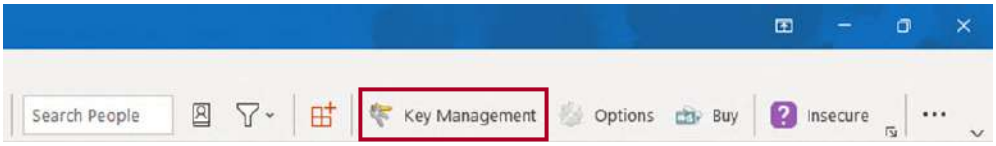
MEMBAGIKAN PUBLIC KEY

Agar dapat mengirimkan pesan dalam bentuk enkripsi dan diterima oleh user yang telah ditentukan diperlukan pertukaran Public Key antara pengirim dan penerima.

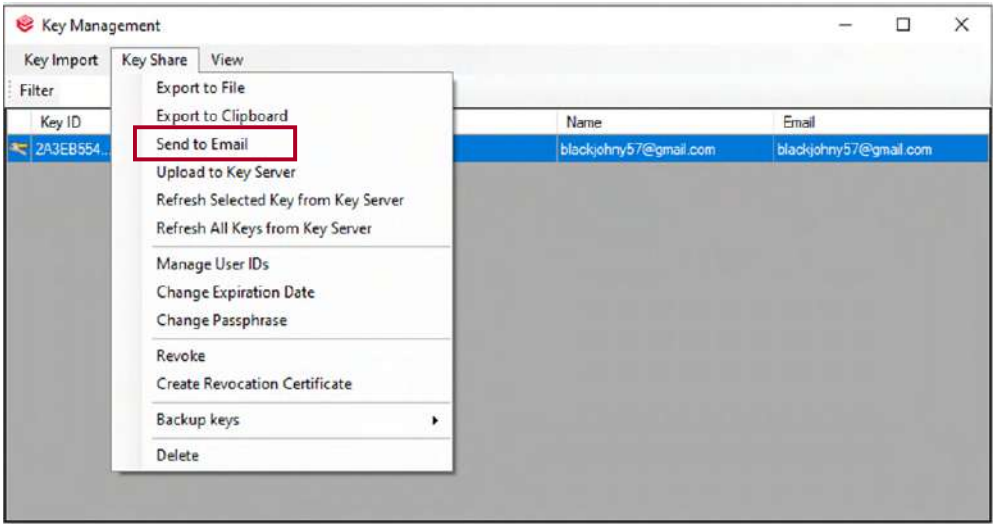
MEMBAGIKAN PUBLIC KEY

Agar dapat mengirimkan pesan dalam bentuk enkripsi dan diterima oleh user yang telah ditentukan diperlukan pertukaran Public Key antara pengirim dan penerima.

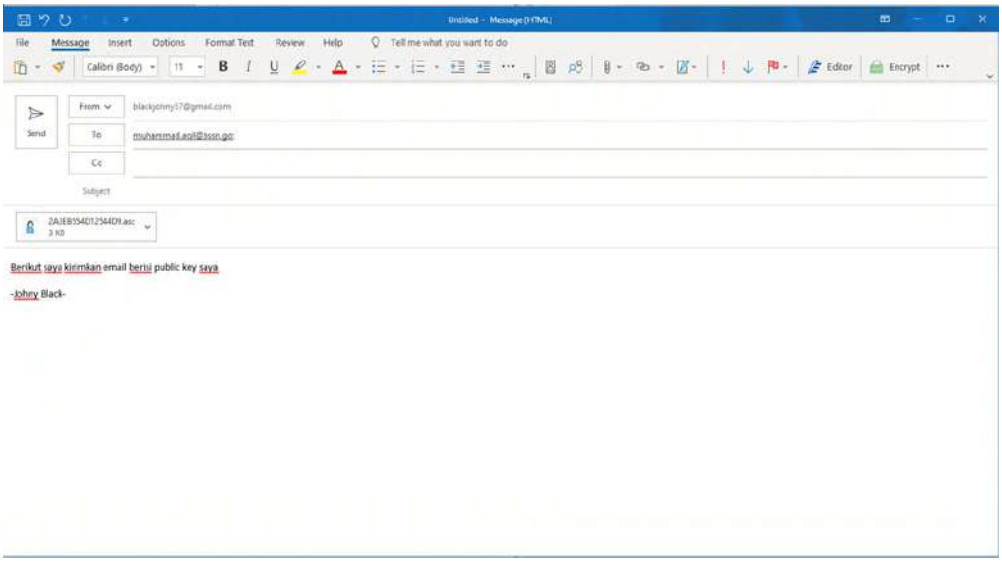
1. Pada bagian atas kanan, Klik “Key Management”



2. Pilih tab “Key Share” kemudian Klik “Send to Email”



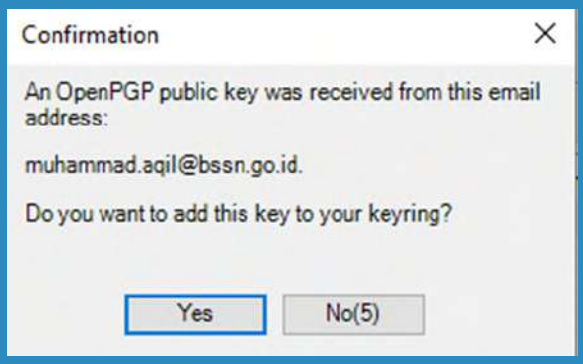
3. Buat email baru, secara otomatis public key sudah terlampir dalam email.



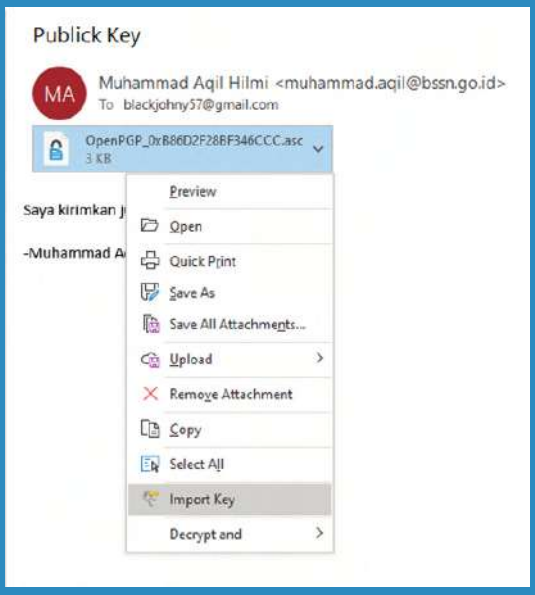
4. Kirimkan email tersebut

IMPORT PUBLIC KEY

- Apabila kita menerima email yang telah dilampirkan file public key oleh pengirim, maka akan muncul pop-up atau tampilan dimana kita dapat langsung menyimpan public key.



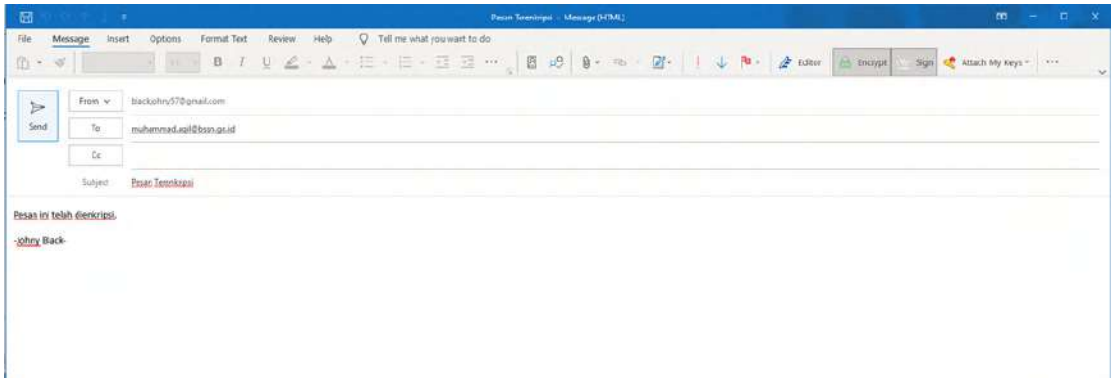
- Atau dapat juga melakukan import secara manual dengan cara membuka email yang dikirimkan, kemudian klik pada lampiran kunci publik dan pilih “Import Key”



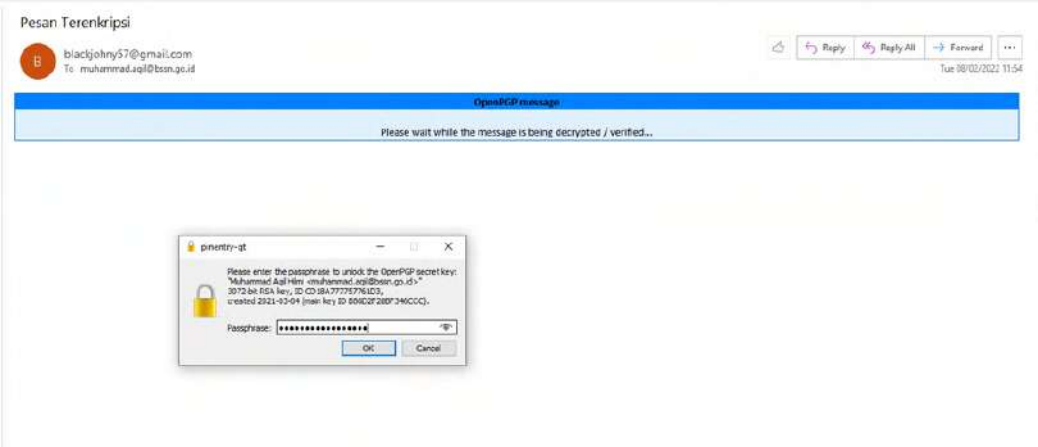
MENGIRIM PESAN TERENKRIPSI

Setelah melakukan pertukaran kunci dan melakukan import kunci publik. Kita dapat melakukan kirim terima email secara aman dengan enkripsi end-to-end.

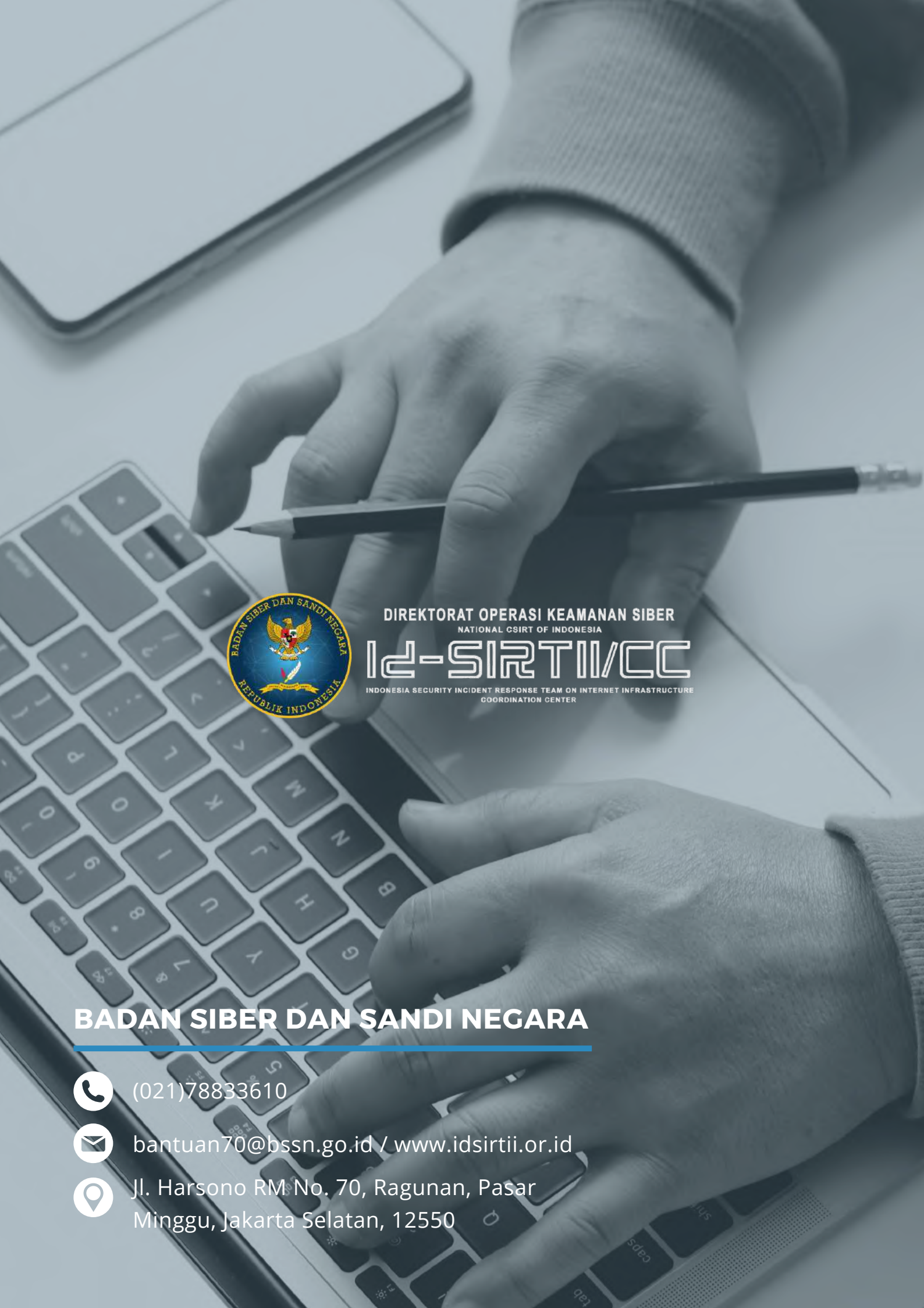
1. Buat pesan baru dengan klik pada “New Email”
2. Setelah pesan baru dibuat, lalu pilih “Encrypt” dan “Sign” untuk mengenkripsi dan menandatangani pesan.



3. Ketika pesan terenkripsi, akan diminta passphrase yang tadi telah dibangkitkan.
4. Pesan Terenkripsi berhasil dikirim
5. Penerima pesan memerlukan passphrase untuk mendekripsi pesan terenkripsi yang dikirimkan



6. Pesan berhasil diterima dan telah terdekripsi



DIREKTORAT OPERASI KEAMANAN SIBER
NATIONAL CSIRT OF INDONESIA
Id-SIRTII/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE COORDINATION CENTER

BADAN SIBER DAN SANDI NEGARA

(021)78833610

bantuan70@bssn.go.id / www.idsirtii.or.id

Jl. Harsono RM No. 70, Ragunan, Pasar Minggu, Jakarta Selatan, 12550