Nama :Tomy Ady Nurdiansyah

NIM :1310651104

Kelas :A reguler pagi

Keamanan Arsitektur dan Desain

Arsitektur keamanan merupakan salah satu komponen dari produk / sistem arsitektur secara keseluruhan dan dikembangkan untuk memberikan bimbingan selama desain produk / sistem.

Arsitektur keamanan adalah artefak desain yang menggambarkan bagaimana kontrol keamanan (= penanggulangan keamanan) diposisikan dan bagaimana mereka berhubungan dengan arsitektur sistem secara keseluruhan. Kontrol ini melayani tujuan untuk mempertahankan atribut kualitas sistem seperti kerahasiaan, integritas dan ketersediaan.

Sebuah kebijakan keamanan adalah pernyataan yang menjelaskan bagaimana entitas mengakses satu sama lain, operasi apa entitas yang berbeda dapat melaksanakan, apa tingkat perlindungan yang diperlukan untuk sistem atau produk perangkat lunak, dan tindakan apa yang harus diambil ketika persyaratan ini bukan aku.

Sebuah model keamanan menguraikan persyaratan yang diperlukan untuk benar mendukung dan menerapkan kebijakan keamanan tertentu.

1. Sistem Arsitektur Komputer
2. Sistem Arsitektur Keamanan
3. Keamanan Model
4. Keamanan Produk Metode Evaluasi dan Kriteria

- **Formal arsitektur:** konseptual memahami struktur dan perilaku dari entitas yang kompleks diperlukan sebelum mencoba untuk mengamankan itu. Arsitektur map komponen sistem, interaksi dan saling ketergantungan dalam satu model kohesif.
- **Arsitektur sistem:** Struktur perangkat keras dan komponen perangkat lunak sistem umum, dan bagaimana keamanan dapat diimplementasikan.
- **Model keamanan:** Representasi simbolik dari kebijakan yang memetakan tujuan para pembuat kebijakan untuk seperangkat aturan bahwa perangkat lunak dan sistem harus mengikuti dalam berbagai kondisi sistem.
- **Evaluasi sistem, sertifikasi dan akreditasi:** Metode yang digunakan untuk memeriksa bagian-bagian yang relevan keamanan dari sistem (misalnya, referensi memantau, kontrol

akses dan kernel perlindungan mekanisme), dan bagaimana sertifikasi dan akreditasi dikonfirmasi.

Arsitektur Formal

Pengembangan arsitektur formal dibahas dalam Keamanan Informasi Pemerintahan dan Manajemen Risiko domain dalam konteks program keamanan organisasi dan keamanan perusahaan kerangka . Dalam domain ini, jenis yang sama dari pendekatan arsitektur dieksplorasi tetapi dalam konteks arsitektur sistem.

Arsitektur adalah alat yang digunakan untuk konseptual memahami struktur dan perilaku entitas yang kompleks. Deskripsi arsitektur adalah penjelasan formal dan representasi dari suatu sistem, komponen yang membentuk sistem, interaksi dan saling ketergantungan antara komponen-komponen, dan hubungan dengan lingkungan.

Secara konseptual, arsitektur adalah pada tingkat tertinggi ketika datang ke proses keseluruhan pengembangan sistem.

Desain sistem

Pada tahap desain sistem, spesifikasi kebutuhan sistem dikumpulkan dan bahasa pemodelan yang digunakan untuk menetapkan bagaimana sistem akan mencapai tujuan desain (misalnya, fungsi yang diperlukan, kompatibilitas, toleransi kesalahan, diperpanjang, keamanan, kegunaan dan pemeliharaan). Bahasa pemodelan adalah grafis umum untuk memvisualisasikan sistem dari pandangan struktural statis dan pandangan perilaku dinamis. Hal ini membuat lebih mudah untuk memahami apa komponen dalam sistem harus mencapai individual, serta bagaimana mereka bekerja sama untuk mencapai yang lebih besar, tujuan arsitektur didirikan.Pada fase ini, model keamanan yang membantu membangun desain sistem untuk memenuhi tujuan arsitektur - seperti Bell-LaPadula, Biba , dan Clark-Wilson - diperkenalkan.

Ada standar berkembang yang menguraikan spesifikasi arsitektur sistem.Pertama Institute of Electrical and Electronics Engineers Inc (IEEE) datang dengan standar (1471) yang disebut *Praktek IEEE Direkomendasikan untuk Deskripsi Arsitektur Sistem Software-Intensif.* Ini diadopsi oleh Organisasi Internasional untuk Standardisasi (ISO) dan diterbitkan

pada tahun 2007 sebagai ISO / IEC 42010: 2007. Ia kemudian diperbarui dan berganti nama menjadi ISO / IEC / IEEE 42011, *Sistem dan rekayasa perangkat lunak - deskripsi Arsitektur*. Standar ini terus berkembang dan meningkatkan;tujuannya adalah untuk standarisasi internasional bagaimana arsitektur sistem terjadi bukan pengembang produk hanya "winging" dan datang dengan pendekatan milik mereka sendiri. Sebuah pendekatan disiplin untuk arsitektur sistem memungkinkan untuk kualitas yang lebih baik, interoperabilitas, diperpanjang, portabilitas dan keamanan.

Arsitektur sistem

Arsitektur komputer mencakup semua bagian dari sistem komputer yang diperlukan untuk itu berfungsi, termasuk sistem operasi , memori chip , sirkuit logika, perangkat penyimpanan, perangkat input dan output , komponen keamanan, bus dan antarmuka jaringan. Hubungan timbal balik dan kerja internal dari semua bagian ini bisa sangat kompleks; membuat mereka bekerja sama dalam mode aman memerlukan metode yang rumit dan mekanisme. Semakin Anda memahami bagaimana potongan-potongan yang berbeda bekerja dan memproses data, semakin Anda akan memahami bagaimana kerentanan benar-benar terjadi dan bagaimana penanggulangan bekerja untuk menghambat dan menghalangi ancaman dari yang diperkenalkan, ditemukan dan dieksploitasi.

Model keamanan

Sebuah konsep penting dalam desain dan analisis sistem yang aman adalah model keamanan karena menggabungkan kebijakan keamanan harus ditegakkan dalam sistem. Sebuah model adalah representasi simbolis dari kebijakan; itu peta keinginan para pembuat kebijakan menjadi seperangkat aturan bahwa sistem komputer harus mengikuti dengan menetapkan struktur data eksplisit dan teknik yang diperlukan untuk menegakkan kebijakan keamanan. Sebuah model keamanan biasanya direpresentasikan dalam matematika dan analitis ide, yang kemudian dipetakan ke spesifikasi sistem dan dikembangkan oleh programmer melalui kode pemrograman.

Keamanan Dasar Teorema - yang menyatakan jika sistem menginisialisasi dalam keadaan aman dan semua negara transisi yang aman, maka setiap negara berikutnya akan aman tidak peduli apa input terjadi - ditutupi, serta empat model yang masing-masing memiliki unik fokus dan meminjamkan untuk digunakan dalam sistem tertentu untuk kebutuhan spesifik:

- Model Bell-LaPadula adalah model matematika pertama dari kebijakan keamanan bertingkat yang mendefinisikan konsep mode negara dan diperlukan aman dari akses. Ini memastikan bahwa informasi mengalir dengan cara yang tidak melanggar kebijakan sistem dan kerahasiaan terfokus.
- Model Biba adalah model transisi negara formal yang menggambarkan seperangkat aturan kontrol akses yang dirancang untuk memastikan integritas data.
- Model Clark-Wilson adalah model diterapkan untuk melindungi integritas data dan memastikan bahwa transaksi diformat dengan benar berlangsung.
- Model Non-Interferensi adalah model keamanan bertingkat resmi yang menyatakan bahwa perintah dan kegiatan yang dilakukan pada satu tingkat keamanan tidak harus dilihat oleh atau mempengaruhi subjek atau objek pada tingkat keamanan yang berbeda.

Mode keamanan, sementara itu, menggambarkan kondisi keamanan di mana fungsi sistem. Sistem dapat mendukung satu atau lebih mode keamanan, sehingga melayani satu atau lebih kelompok klasifikasi keamanan pengguna.Domain ini membahas empat mode dan juga memperkenalkan konsep jaminan kepercayaan. Tingkat kepercayaan didasarkan pada kinerja TCB.Konsep kepercayaan dan jaminan dikontraskan, dan efek merugikan dari kompleksitas pada jaminan juga mencatat.

Metode evaluasi sistem

Evaluasi jaminan meneliti bagian-bagian yang relevan keamanan dari sistem, termasuk dipercaya dasar komputasi, mekanisme kontrol akses , referensi memantau, kernel, dan mekanisme perlindungan. Hubungan dan interaksi antara komponen-komponen ini juga dievaluasi. Ada beberapa metode yang berbeda untuk mengevaluasi dan menetapkan tingkat jaminan ke sistem:

- Kriteria Trusted Evaluasi Sistem Komputer (TCSEC), juga disebut sebagaiUS Jeruk Book , menjelaskan kriteria khusus untuk beberapa daerah evaluasi (kebijakan keamanan, identifikasi, label, dokumentasi, akuntabilitas, jaminan siklus hidup dan perlindungan terus-menerus), dan proses formal evaluasi dilaksanakan oleh Pusat Keamanan Komputer Nasional , yang menghasilkan produk dievaluasi.

- Masyarakat Eropa meluncurkan Kriteria Teknologi Informasi Evaluasi Keamanan (ITSEC). ITSEC terlihat terutama pada fungsi dan jaminan sebagai dua daerah kategori yang luas dengan subpos. Perbedaan utama antara AS dan Eropa pendekatan harus dilakukan dengan skema rating mereka. Eropa ITSEC menerapkan sistem penilaian terpisah untuk fungsi keamanan dan jaminan sedangkan US TCSEC menggunakan sistem single-rating. Hubungan membingungkan antara dua dieksplorasi secara mendalam.
- Common Criteria standar evaluasi global yang memiliki asal-usul dalam upaya global independen, yang didasarkan pada standar AS dan mewakili standar pan-Eropa lainnya. Standar, yang didirikan pada tahun 1990, adalah standar kompromi global yang menggantikan kedua TCSEC dan ITSEC. Hal ini memperkenalkan konsep profil perlindungan, yang membutuhkan garis tertentu dunia nyata di industri.

Manfaat dari memiliki satu set yang diakui secara global dan diterima kriteria adalah membantu konsumen dengan mengurangi kompleksitas peringkat dan menghilangkan kebutuhan untuk memahami definisi dan arti dari peringkat yang berbeda dalam berbagai skema evaluasi. Hal ini juga membantu pedagang karena sekarang mereka dapat membangun satu set spesifik persyaratan untuk menjual produk mereka secara internasional daripada harus memenuhi beberapa penilaian yang berbeda.

Arsitektur sistem komputer yang penting dan terdiri dari banyak topik.Sistem ini harus:

- Pastikan memori yang benar terpisah dan dilindungi,
- Memastikan bahwa hanya berwenang akses objek pelajaran,
- Memastikan bahwa proses tidak dipercaya tidak dapat melakukan kegiatan yang akan menempatkan proses lain pada risiko,
- Mengontrol arus informasi, dan
- Tentukan domain sumber daya untuk setiap mata pelajaran.

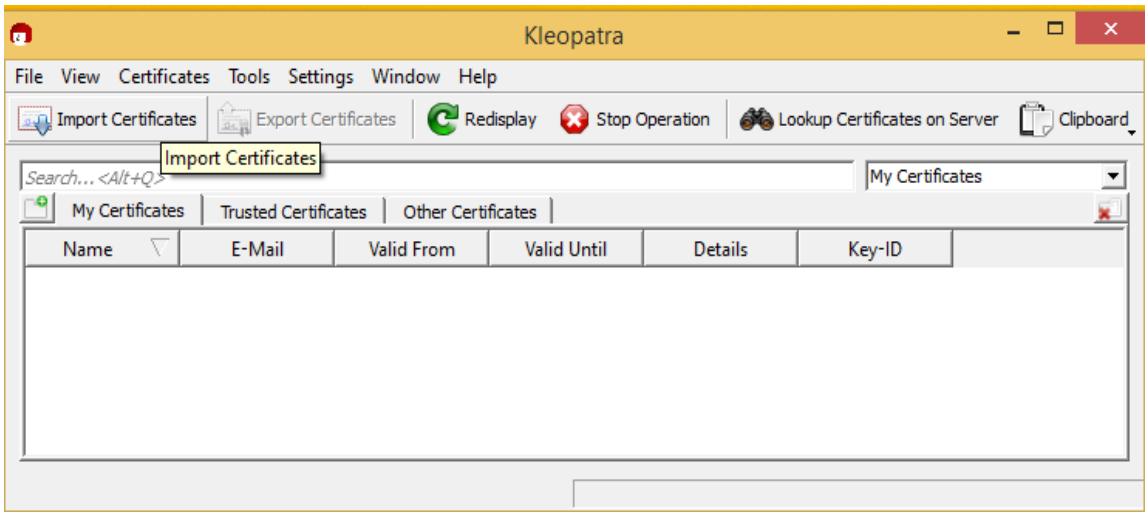
Sebuah sistem juga harus memastikan bahwa jika komputer mengalami jenis gangguan, tidak akan menghasilkan keadaan yang tidak aman. Banyak dari masalah ini dibahas dalam kebijakan keamanan sistem, dan model keamanan dibangun untuk mendukung persyaratan kebijakan ini. Setelah kebijakan keamanan, model dan arsitektur telah dikembangkan, sistem operasi komputer atau produk harus dibangun, diuji, dievaluasi dan dinilai.

Sementara sering diabaikan dalam pengelolaan keamanan perusahaan sehari-hari, arsitektur sistem komputer merupakan aspek penting untuk keamanan sistem secara keseluruhan, dan sama-sama penting untuk mengetahui untuk ujian CISSP.

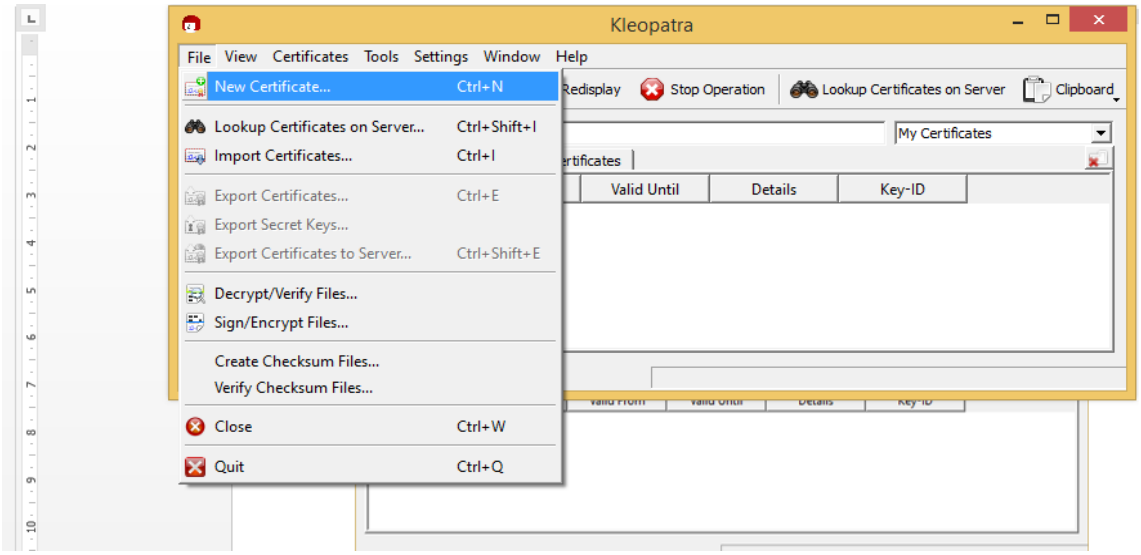
Tugas 2

Tutorial kleopatra

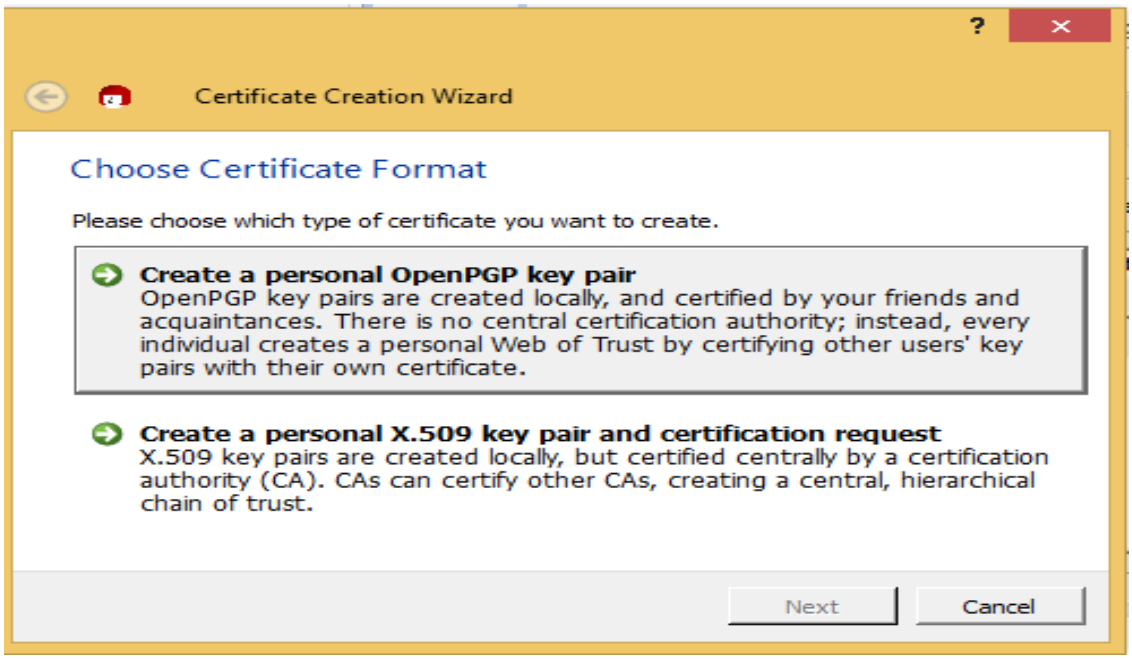
Buka kleopatra



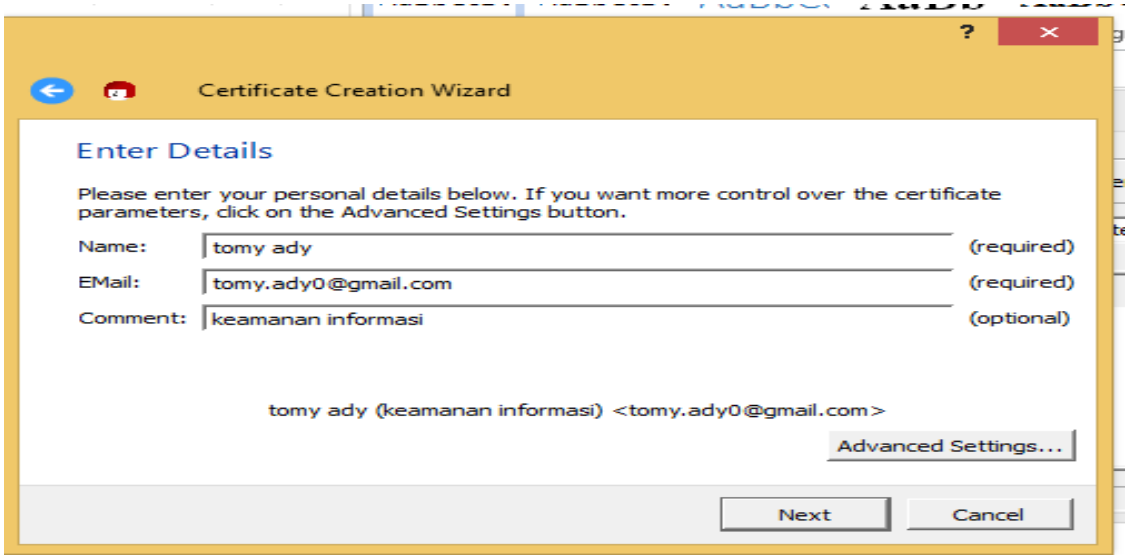
Pilih file klik new Certificate seperti dibawah ini:



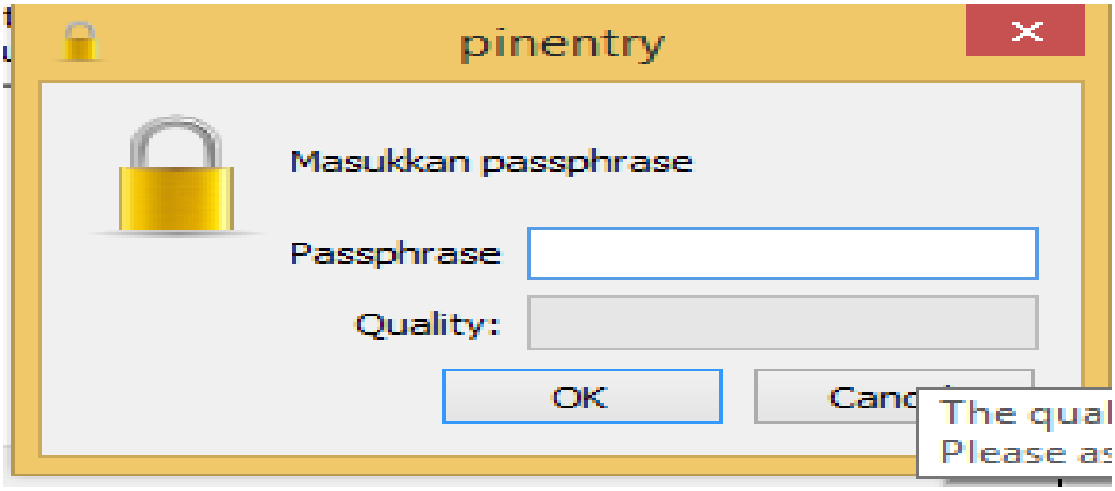
Kemudian pilih klik Create personal OpenPGP key pair



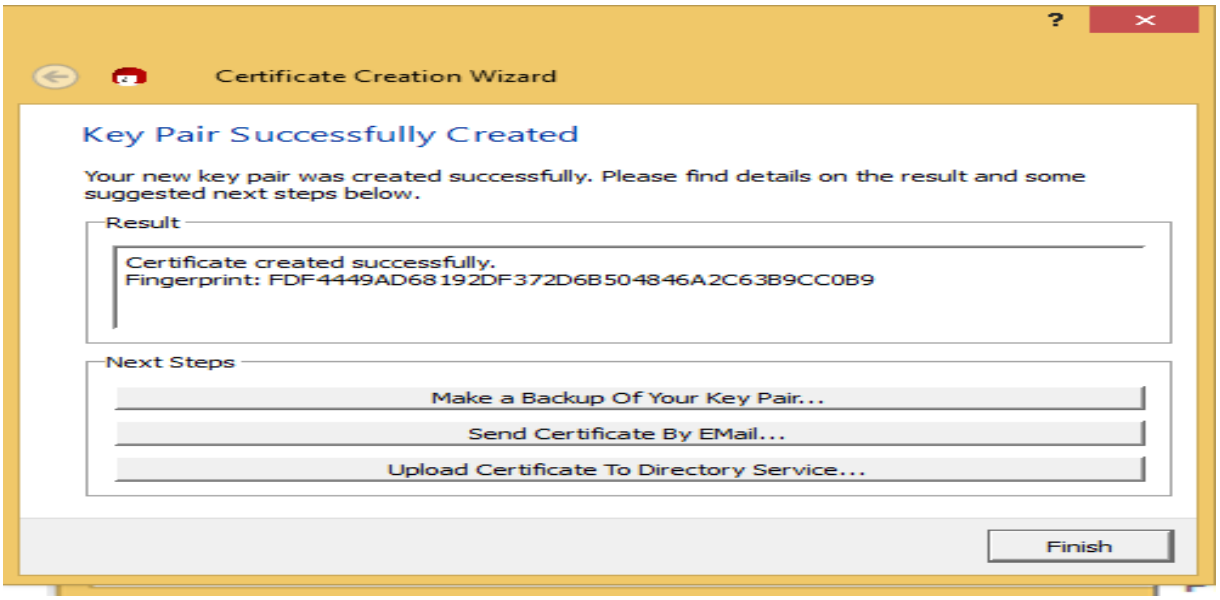
Tekan next kemudian isi Nama ,Email ,Komentar



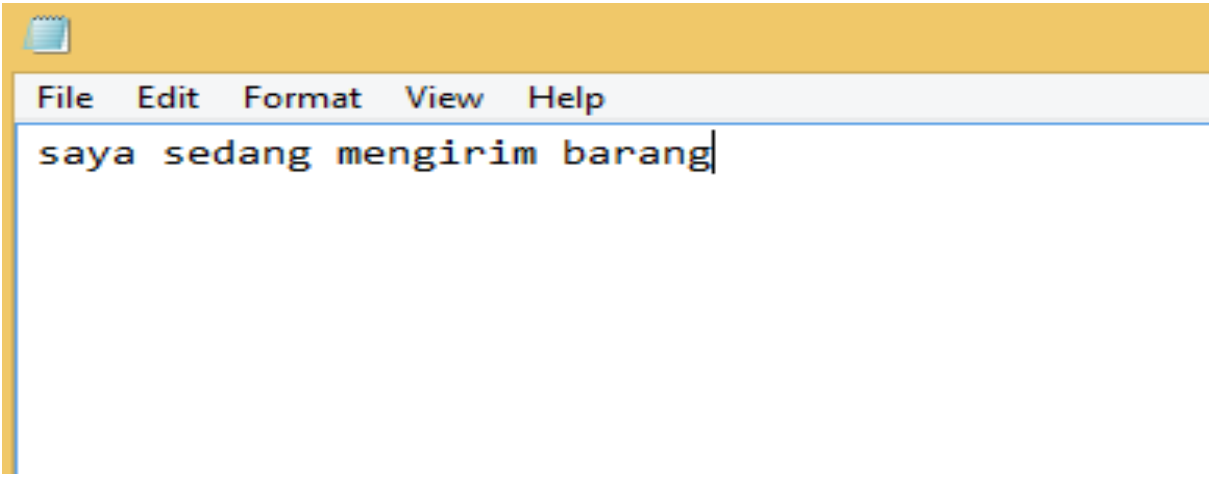
Kemudian tekan next masukkan pasword sesuka anda sampai 100%:



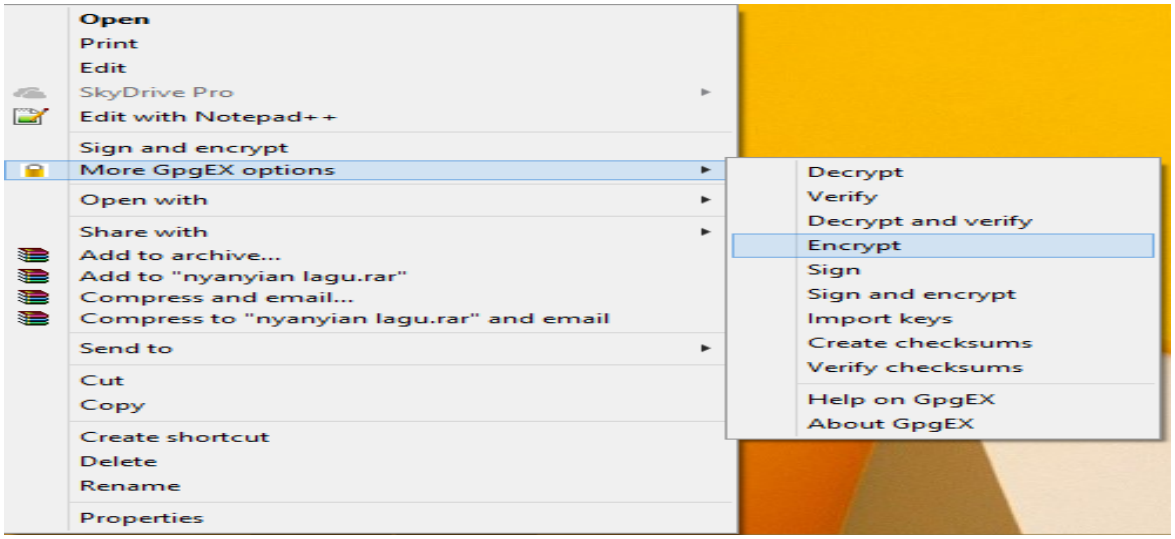
Kemudian klik finish



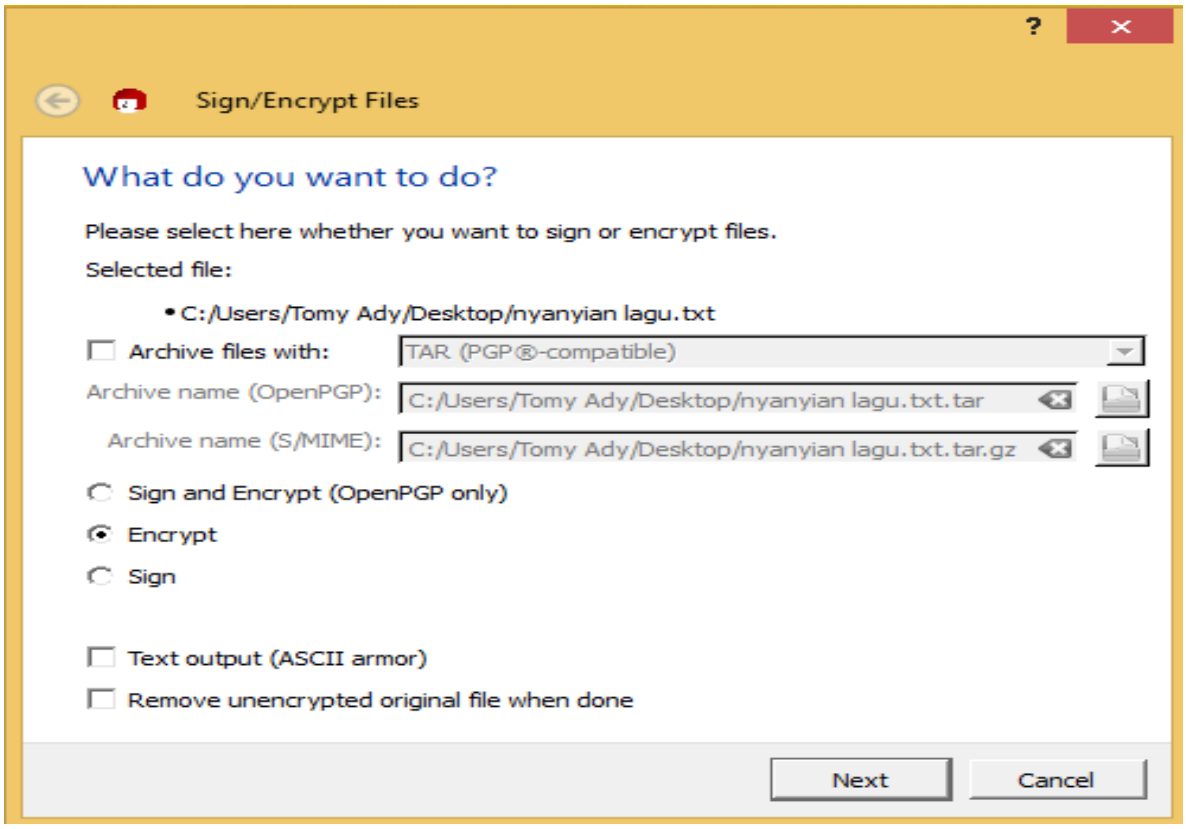
Buka notepad kemudian tuliskan sebuah data yang sedang diamankan kemudian simpan file ke documen/dekstop:



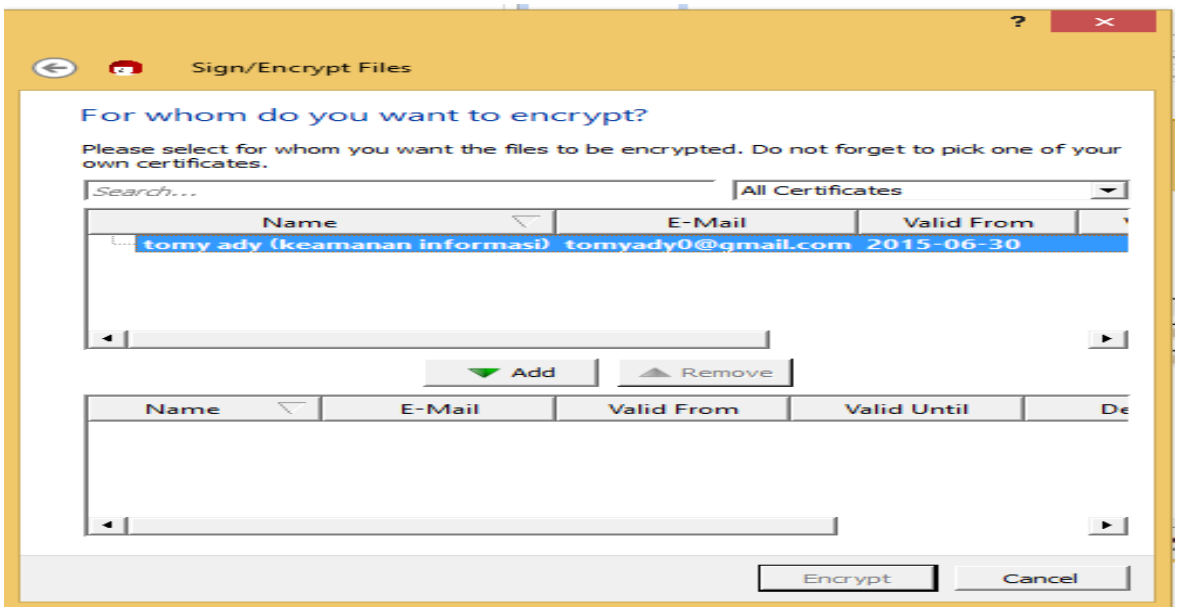
Kemudian klik kanan notepad yang sudah disimpan ,pilih klik More GpgEX options pilih klik encrypt seperti dibawah ini:



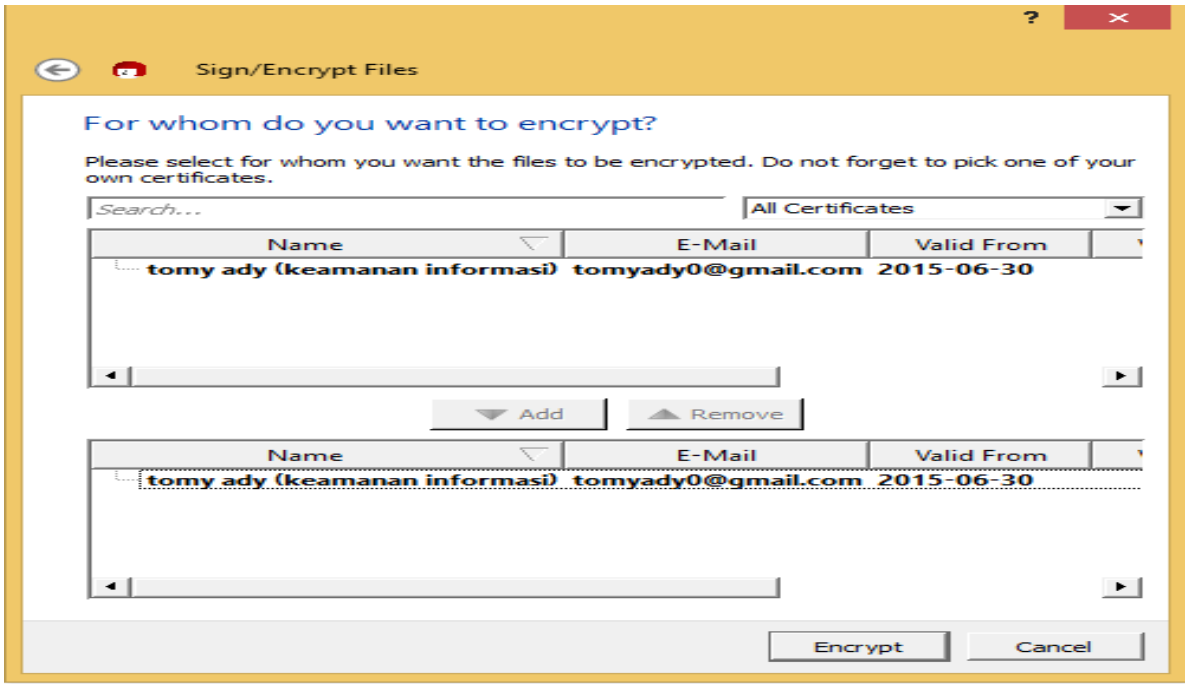
Jika muncul dibawah seperti ini tekan next :



Tekan nama email kemudian klik add ,klik encrypt seperti dibawah ini:



Jika sudah muncul email yang ada dibawah kemudian tekan encrypt ,selesaii ,data berhasil diamankan:



Jika ingin mebuka data kembali file yang berisi GPG dihapus kemudian file notepad yang berisi data tersebut dibuka dengan mengklik kanan pilih klik More GpgEX options kemudian klik desrypt data berhasil dibuka kembali .