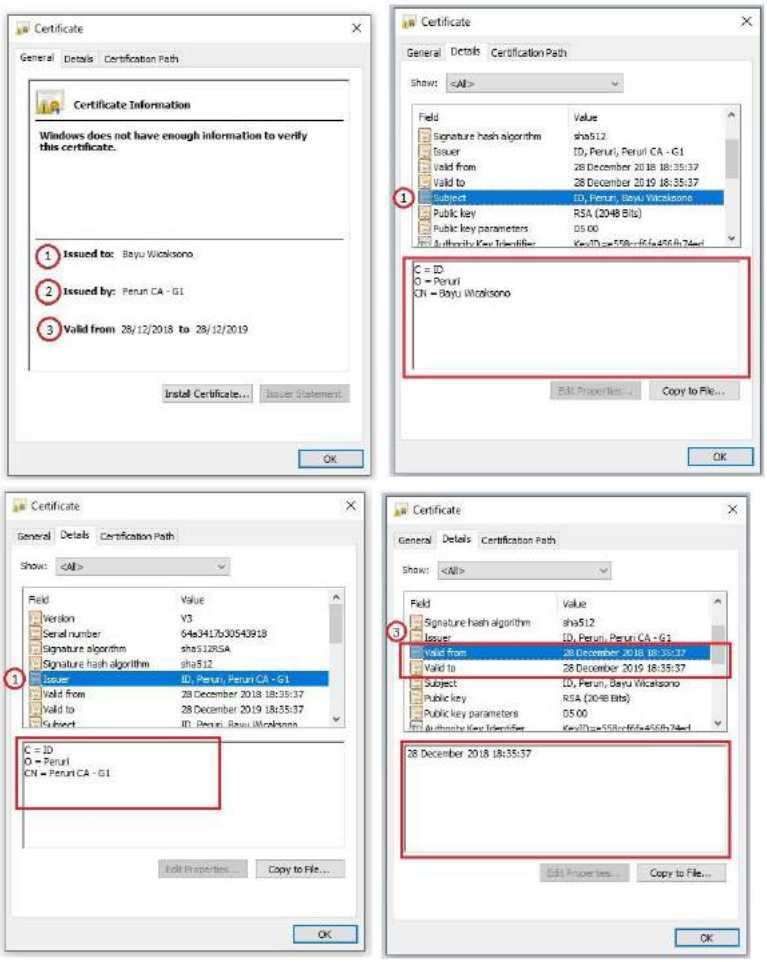
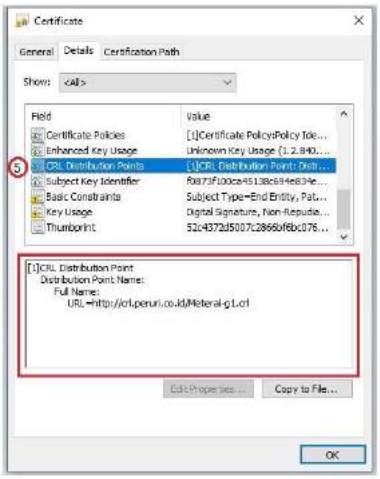
Cara melakukan verifikasi dan validasi keaslian sertifikat digital

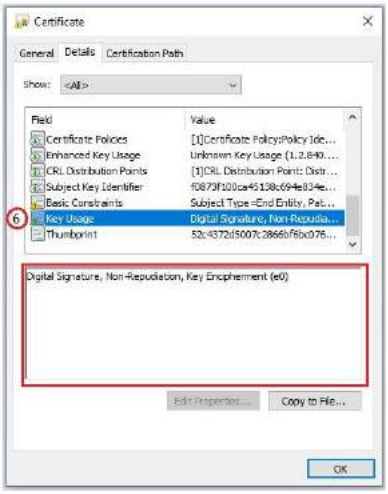
1. Download certificate di email, ubah extension .pem menjadi .crt
2. Buka certificate dengan double click.
3. Attribute pada X509 Certificate :
   a) Issued to / Subject, adalah pemilik dari certificate, contoh : Bayu Wicaksono.
   b) Issued by, adalah CA yang mengeluarkan certificate, contoh : Peruri CA - G1
   c) Valid From - To -, adalah Masa berlaku certificate.



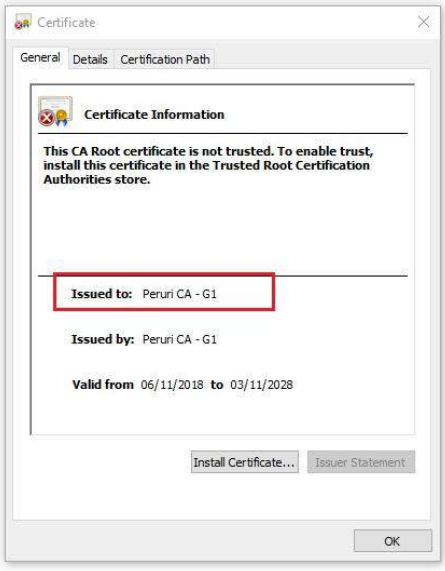
   d) Certificate Policy, berisi CPS yang dipublikasikan oleh CA.
   e) CRL Distribution Point, Certificate Revoke List dimana daftar certificate yang sudah dicabut.

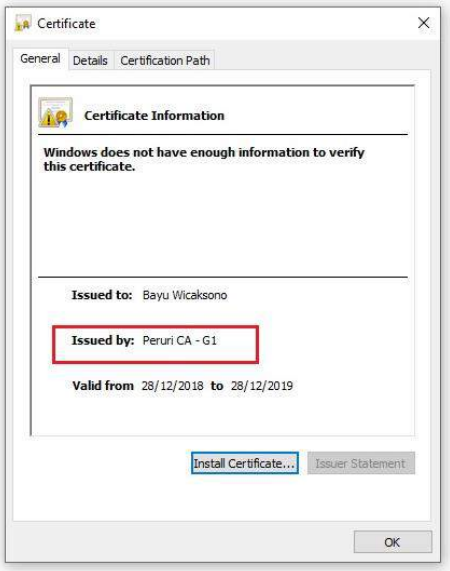


f) Key Usage, adalah peruntukan dari Certificate yang dikeluarkan, contoh nya untuk Digital Signature / Document Signing.



4. Download CA Certificate untuk melakukan verifikasi terhadap certificate yang telah di sign oleh CA.
5. Pastikan CA Certificate yang digunakan sesuai, dengan membandingkan Issued to dan Issued by.





6. Gunakan openSSL, lakukan command sebagai berikut :

openssl verify -verbose -CAfile <certificate ca> <certificate pemilik>

contoh :

openssl verify -verbose -CAfile CertificateCA.crt Pemilik.crt

Pemilik.crt: OK

7. Verifikasi Sample.crt berhasil dilakukan.

Catatan:

Setiap sertifikat dapat dilihat detailnya menggunakan pdf reder atau membuka file.crt pada Windows. Informasi yang perlu diperiksa di antaranya :

- Tanda tangan penerbit;
- Parameter kebijakan;
- Parameter penggunaan;
- Periode validitas;
- Informasi pencabutan atau pembekuan;
- Batas tanggung jawab penggunaan sertifikat