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.

	Contraction of the second			
show:	<ab></ab>	~		
Field		Value	^	
Certificate Policies		[1]Certificate Po	lev:Policy Ide	
Enhanced Key Usage		Unknown Key Us	Unknown Key Usage (1.2.840	
CRL Distribution Points		[1]CRL Distributi	on Point: Dietz	
Subject Key Identifier		f0873f100ca451	38c694e834e	
Basic Constraints		Subject Type-E	Subject Type=End Entity, Pat	
Key Usage		Digital Signature	Non-Repudia	
Thumborint		52c4372d5007c2	3866bf6bc076	
F	URL=http://oi.pen	uri.co.id/Meterai-g1.crl		

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

1.11	
<u>ч</u>	
Value	-
[1]Certificate Policy:Policy Ide	
Unknown Key Usage (1.2.840	
[1]CRL Distribution Point: Distr	
f0873f100ca45138c694c834c	
Subject Type =End Entity, Pat	
Digital Signature, Non-Repudia	
52c4372d5007c2866bf6bc076	
on, Key Encipherment (e0)	
on, Key Encipherment (e0)	
	Value [1]Cortificate Policy/Policy Job Unknown Key Usage (1,2,649 [1]CBL Distribution Point: Cistr 506/971/000-451308;c594-8334c Sobject Type = Cind Entity, Pet Bigital Starature, Non-Recada 52: 4372/(5007c.2866hfbic/76

- 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.

eral Details Certification Path	General Details Certification Path
Certificate Information	Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.	Windows does not have enough information to verify this certificate.
Issued to: Peruri CA - G1	Issued to: Bayu Wicaksono
Issued by: Peruri CA - G1	Issued by: Peruri CA - G1
Valid from 06/11/2018 to 03/11/2028	Valid from 28/12/2018 to 28/12/2019
Install Certificate Issuer Statemen	Install Certificate Issuer Statement

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