KOMINFO	**Nomor**	**:**	**SINT/20240131/v1.4**
	Versi	**:**	**1.4**
	Tanggal	**:**	**31 Januari 2024**
	Hal	**:**	**24 Halaman**

Standar Interoperabilitas PSrE Indonesia (PSrE Instansi dan non-Instansi)

31 Januari 2024

Direktur Tata Kelola Aplikasi Informatika

merangkap sebagai Policy Authority

Balai Sertifikasi Elektronik

Ditandatangani secara elektronik
DIREKTUR TATA KELOLA APLIKASI INFORMATIKA

Aries Kusdaryono

Catatan :

- UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang diterbitkan **iOTENTIK/BSrE**

Lembar Catatan Review/Revisi

Tanggal	Rev	Uraian	Oleh
25 Juli 2022	1.0	Versi Awal, gabungan Standar Interoperabilitas Instansi versi 1.2 dan Standar Interoperabilitas Non Instansi versi 1.4 sekaligus memisahkan Bab terkait OID menjadi Dokumen Hierarki OID untuk IKP di Indonesia	Tim Tata Kelola Sertifikasi Elektronik
21 September 2022	1.1	Perbaikan minor terkait format penulisan	Tim Tata Kelola Sertifikasi Elektronik
16 Januari 2023	1.2	Perbaikan Bab II.3.3.1 tentang basic field validity OCSP responder	Tim Tata Kelola Sertifikasi Elektronik
4 Mei 2023	1.3	● Penambahan catatan pada Bab II.1.1 bagian subject sertifikat dan penambahan Lampiran I ● Perbaikan pada Bab II.1.2 bagian subject alternative name ● Koreksi terhadap OID CA Issuer URL pada Bab II.1.2 bagian authority info access	Tim Tata Kelola Sertifikasi Elektronik
31 Januari 2024	1.4	● Perbaikan ketentuan DN Sertifikat Pemilik dari PSrE non-Instansi pada Bab II.1.1 ● Menambahkan policy qualifier dari policy information PSrE Indonesia pada Bab II.1.2 ● Penambahan atribut dan OID pada Lampiran I	Tim Tata Kelola Sertifikasi Elektronik

Daftar Isi

I. Umum

I.1. Penjelasan Umum

Spesifikasi ini mendeskripsikan profil dari Sertifikat Elektronik (Sertifikat) berdasarkan ketentuan peraturan perundang-undangan terkait tata kelola penyelenggaraan sertifikasi elektronik.

I.2. Susunan dan Ruang Lingkup

Spesifikasi ini mematuhi standar internasional [RFC5280] serta menentukan profil Sertifikat untuk X.509 v3. Dokumen ini juga membatasi tujuan dan struktur isian dasar (basic field) dan isian ekstensi (extension field) pada Sertifikat.

I.3. Standar-Standar yang Terkait

1. [X500] ITU-T Recommendation X.500 (1997) | ISO/IEC 9594-1:1998, Information technology - Open Systems Interconnection - The Directory : Overview Of Concepts, Models and Services
2. [X501] ITU-T Recommendation X.501 (1997) | ISO/IEC 9594-2:1995, Information technology - Open Systems Interconnection - The Directory : Part 2 : Models
3. [X509] ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8:1998, Information technology - Open Systems Interconnection - The Directory : Authentication Framework
4. [RFC2119] IETF RFC 2119 (1997), Key Words for use in RFCs to Indicate Requirement Levels
5. [RFC3850] IETF RFC 3850 (2004), Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling
6. [RFC5280] IETF RFC 5280 (2008), Internet X.509 Public Key Infrastructure Certificate and CRL Profile
7. [RFC6818] IETF RFC 6818 (2013), Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

I.4. Kode Penggunaan

Sebagian istilah yang digunakan di dalam spesifikasi ini mematuhi *RFC 2119* atas status implementasi pada perangkat lunak PSrE Indonesia dan pengguna:

1. **Harus** atau ***Must/Mandatory*** **(simbol: M)**, wajib digunakan.
2. **Opsional** atau **Optional (simbol: O),** dapat digunakan secara opsional dengan mempertimbangkan kesesuaian situasi**.**
3. **Tidak Boleh** atau **Must Not (simbol: X),** tidak boleh digunakan**.**
4. **Tidak Diatur** atau **Not Stipulated (simbol: -),** tidak disebutkan ketentuannya di dalam spesifikasi ini**.**
5. **Kritikal** atau **Critical (simbol: C).**
6. **Tidak kritikal** atau ***Noncritical*** **(simbol: N)**.
7. **Disarankan** atau ***Recommended*** **(simbol: R)**, disarankan untuk digunakan dengan mempertimbangkan keamanan dan interoperabilitas.
8. **Tidak disarankan** atau ***Not Recommended*** **(simbol: NR)**, tidak disarankan untuk digunakan dengan mempertimbangkan keamanan dan interoperabilitas.

I.5. Singkatan

ASN.1 : *Abstract Syntax Notation One*
CA : *Certification Authority* (Penyelenggara Sertifikasi Elektronik/PSrE)
CPS : *Certification Practice Statement*
CRL : *Certificate Revocation List* (Daftar Pencabutan Sertifikat Elektronik)
DN : *Distinguished Name*
OID : *Object Identifier*
PSrE : Penyelenggara Sertifikasi Elektronik
SHA : *Secure Hash Algorithm*

II. Profil

II.1. Profil Sertifikat

II.1.1. Basic Field

Field	Type	M	PSrE Induk	PSrE Indonesia	Subscriber/Pemilik
Certificate (seq)					
tbsCertificate	TBSCertificate	**M**			
signatureAlgorithm	AlgorithmIdentifier	**M**			
AlgorithmIdentifier (seq)					
algorithm	OBJECT IDENTIFIER		1.2.840.113549.1.1.11 (SHA256WithRSAEncryption)	1.2.840.113549.1.1.11 (SHA256WithRSAEncryption) atau 1.2.840.113549.1.1.12 (SHA384WithRSAEncryption) atau 1.2.840.113549.1.1.13 (SHA512WithRSAEncryption)	1.2.840.113549.1.1.11 (SHA256withRSAEncryption) atau 1.2.840.113549.1.1.12 (SHA384withRSAEncryption) atau 1.2.840.113549.1.1.13 (SHA512withRSAEncryption)
parameters	ANY DEFINED BY algorithm OPTIONAL		NULL	NULL	NULL
signatureValue	BIT STRING	**M**	Tanda tangan PSrE Induk	Tanda tangan PSrE Induk	Tanda tangan PSrE Indonesia
TBSCertificate (seq)					
version	INTEGER{v1(0), v2(1), v3(3)}	**M**	Harus menggunakan versi 3	Harus menggunakan versi 3	Harus menggunakan versi 3
serialNumber	INTEGER	**M**	Serial number sertifikat	Serial number sertifikat	Serial number sertifikat

Field	Type	M	PSrE Induk	PSrE Indonesia	Subscriber/Pemilik
			disesuaikan dengan RFC 5280	disesuaikan dengan RFC 5280	disesuaikan dengan RFC 5280
signature	AlgorithmIdentifier	**M**			
AlgorithmIdentifier (seq)					
algorithm	OBJECT IDENTIFIER		1.2.840.113549.1.1.11 (sha256WithRSAEncryption)	1.2.840.113549.1.1.11 (SHA256WithRSAEncryption) atau 1.2.840.113549.1.1.12 (SHA384WithRSAEncryption) atau 1.2.840.113549.1.1.13 (SHA512WithRSAEncryption)	1.2.840.113549.1.1.11 (SHA256withRSAEncryption) atau 1.2.840.113549.1.1.12 (SHA384withRSAEncryption) atau 1.2.840.113549.1.1.13 (SHA512withRSAEncryption)
parameters	ANY DEFINED BY algorithm OPTIONAL		NULL	NULL	NULL
issuer	Name	**M**	**DN PSrE Induk** (CN=Root CA Indonesia DS {Issuance Number}, O=Kementerian Komunikasi dan Informatika, C=ID)	**DN PSrE Induk** (CN=Root CA Indonesia DS {Issuance Number}, O=Kementerian Komunikasi dan Informatika, C=ID)	**DN PSrE Indonesia** (CN=<Nama PSrE atau Merek Dagang>, O=<Nama Resmi Badan Usaha/Instansi>, C=ID)
validity	Validity	**M**	20 tahun	10 tahun	maksimal 2 tahun
Validity(seq)					
notBefore	UTCTime		Waktu mulai validitas	Waktu mulai validitas	Waktu mulai validitas
notAfter	UTCTime		Waktu validitas berakhir	Waktu validitas berakhir	Waktu validitas berakhir
subject	Name	**M**	**DN PSrE Induk** (CN=Root CA Indonesia DS {Issuance Number}, O=Kementerian Komunikasi	**DN PSrE Indonesia** (CN=<Nama PSrE atau Merek Dagang>, O=<Nama Resmi Badan Usaha/Instansi>, C=ID)	**Untuk PSrE Instansi minimal memuat:** **DN untuk Tanda Tangan Elektronik**

Field	Type	M	PSrE Induk	PSrE Indonesia	Subscriber/Pemilik
			dan Informatika, C=ID)		**Orang-perseorangan pegawai Instansi** (CN={Nama Orang}[1], O=Nama Instansi, C=ID) **DN untuk Segel Elektronik** (CN={Nama Instansi}, C=ID)
					Untuk PSrE non-Instansi minimal memuat: **DN untuk Tanda Tangan Elektronik** ● **Orang-perseorangan Pribadi** (CN={Nama Orang}[2], OU=Personal , C=ID) ● **Orang-perseorangan berafiliasi ke perusahaan** (CN={Nama orang}[3], O=Nama Badan Usaha, C=ID) Catatan: Dalam hal PSrE Indonesia menggabungkan DN untuk Tanda Tangan Elektronik orang-perseorangan Pribadi dan untuk orang-perseorangan berafiliasi ke perusahaan setelah mendapat persetujuan Kominfo, maka minimal memuat (CN={Nama Orang}[4],

[1] string of maximum 64 characters as stated in National ID (KTP) or birth certificate, without title
[2] string of maximum 64 characters as stated in National ID (KTP) or birth certificate, without title
[3] string of maximum 64 characters as stated in Deed of Establishment and its amendments (Akta Pendirian Perusahaan dan perubahannya)
[4] string of maximum 64 characters as stated in National ID (KTP) or birth certificate, without title

Field	Type	M	PSrE Induk	PSrE Indonesia	Subscriber/Pemilik
					OU=Personal , C=ID) Ketentuan DN digabungkan ini hanya berlaku sampai 31 Januari 2025. **DN untuk Segel Elektronik** (CN={Nama Badan Usaha}[3], C=ID) Catatan: Apabila perlu menambahkan atribut DN selain yang disebutkan di atas, cara penulisannya merujuk ke Lampiran I. Penulisan Email Address merujuk pada II.1.2 bagian SubjectAlternativeName.
`subjectPublicKeyInfo`	SubjectPublicKeyInfo	**M**			
SubjectPublicKeyInfo (seq)					
`algorithm`	AlgorithmIdentifier				
AlgorithmIdentifier (seq)					
`algorithm`	OBJECT IDENTIFIER		1.2.840.113549.1.1.1 (`rsaEncryption`) (Key Length: 4096)	1.2.840.113549.1.1.1 (`rsaEncryption`) (Key Length: 4096)	1.2.840.113549.1.1.1 (`rsaEncryption`) (Key Length: 2048) atau 1.2.840.10045.2.1, (ecPublicKey), 1.2.840.10045.3.1.7, (prime256v1)
`parameters`	ANY DEFINED BY algorithm		NULL	NULL	NULL

Field	Type	M	PSrE Induk	PSrE Indonesia	Subscriber/Pemilik
	OPTIONAL				
subjectPublicKey	BIT STRING		Kunci Publik Root CA	Kunci Publik PSrE Indonesia	Kunci Publik Subscriber
extensions	EXPLICIT Extensions	**M**			
Extensions (seq size (1...MAX))					
extension	EXTENSION				
EXTENSION (seq)					
extnID	OBJECT IDENTIFIER		OID dari extension	OID dari extension	OID dari extension
critical	BOOLEAN DEFAULT FALSE				
extnValue	OCTET STRING		Berisi nilai ASN.1 dari type ekstensi yang digunakan dengan menggunakan DER encoding	Berisi nilai ASN.1 dari type ekstensi yang digunakan dengan menggunakan DER encoding	Berisi nilai ASN.1 dari type ekstensi yang digunakan dengan menggunakan DER encoding

II.1.2. Standard Extension Field

Field	Type	OID	PSrE Induk			PSrE Indonesia			Subscriber/Pemilik		
			M	C	Information	M	C		M	C	
AuthorityKeyIdentifier (seq)		**2.5.29.35**	**O**	**N**		**M**	**N**		**M**	**N**	
keyIdentifier	OCTET STRING				Hash SHA-1 160 bit dari kunci publik PSrE Induk			Hash SHA-1 160 bit dari kunci publik PSrE Induk			Hash SHA-1 160 bit dari kunci publik PSrE Indonesia
authorityCertIssuer	GeneralNames										
authorityCertSerialNum	INTEGER										

Field	Type	OID	PSrE Induk			PSrE Indonesia			Subscriber/Pemilik		
			M	C	Information	M	C		M	C	
ber											
SubjectKeyIdentifier		**2.5.29.14**	**M**	**N**		**M**	**N**		**M**	**N**	
subjectKeyIdentifier	OCTET STRING				Hash SHA-1 160 bit dari kunci publik PSrE Induk			Hash SHA-1 160 bit dari kunci publik PSrE Indonesia			Hash SHA-1 160 bit dari kunci publik Pemilik
KeyUsage		**2.5.29.15**	**M**	**C**		**M**	**C**		**M**	**C**	
keyUsage	BIT STRING				keyCertSign (5), cRLSign (6) Nilai key usage (00001100)			keyCertSign (5), cRLSign (6) Nilai key usage (00001100)			Sesuai dengan CPS dari PSrE Indonesia, namun sertifikat yang diterbitkan oleh PSrE Indonesia untuk Subscriber tidak boleh memiliki key usage cRLSign dan keyCertSign Catatan: sertifikat dengan keyUsage digitalSignature, nonRepudiation harus dipisahkan dari sertifikat dengan keyUsage keyEncipherment, dataEncipherment, encipherOnly, decipherOnly.
CertificatePolicies (seq size(1...MAX))		**2.5.29.32**	**X**	**-**		**M**	**C**		**M**	**C**	
policyInformation	PolicyInformation										

Field	Type	OID	PSrE Induk			PSrE Indonesia			Subscriber/Pemilik		
			M	C	Information	M	C		M	C	
PolicyInformation (seq)											
`policyIdentifier`	OBJECT IDENTIFIER							Memuat OID PSrE Instansi atau PSrE non-Instansi yang mengacu ke Bab III Dokumen Hierarki OID untuk IKP Indonesia.			Memuat OID yang mengacu ke Bab III pada Dokumen Hierarki OID untuk IKP Indonesia.
`policyQualifiers`	Sequence Size (1...MAX) PolicyQualifierInfo							Memuat url dari dokumen CPS PSrE Induk.			
SubjectAlternativeName		**2.5.29.17**									
`subjectAlternativeName`	GeneralNames		**O**	**N**		**O**	**N**		**O**	**N**	Apabila PSrE Indonesia menyimpan: 1. NIK Pemilik menggunakan informasi virtual ID (VID), sesuai ketentuan Subject Identification Method (SIM) pada RFC 4683, disimpan dalam bentuk otherName dari struktur GeneralName menggunakan SII Type=2.16.360

Field		OID	PSrE Induk			PSrE Indonesia			Subscriber/Pemilik		
			M	C	Information	M	C		M	C	
											.1.1.1.6.1 untuk tipe NIK. 2. Email address[5] Pemilik, sesuai RFC 5280 disimpan di Subject Alternative Name Extension dengan mengikuti ketentuan rfc822Name
IssuerAlternativeName		**2.5.29.18**	**X**	**-**		**O**	**N**		**O**	**N**	
`issuerAlternativeName`	GeneralNames										
BasicConstraint (seq)		**2.5.29.19**	**M**	**C**		**M**	**C**		**M**	**C**	
`cA`	BOOLEAN				true			true			false
`pathLenConstraint`	INTEGER							0			
NameConstraint		**2.5.29.30**	**X**	**-**		**X**	**-**		**X**	**-**	
`permittedSubtrees`	GeneralSubtrees										
`excludedSubtrees`	GeneralSubtrees										

[5] Penulisan Email address menggunakan atribut MAIL. Penggunaan atribut E untuk Email address sudah tidak disarankan.

Field		Type	OID	PSrE Induk			PSrE Indonesia			Subscriber/Pemilik		
				M	C	Information	M	C		M	C	
ExtendedKeyUsage (seq size (1...MAX))			**2.5.29.37**	**X**	**-**		**X**	**-**		**O**	**N**	Dapat dilihat pada RFC 5280 Section 4.2.1.12 ekstensi ExtendedKeyUsage tidak boleh memuat anyExtendedKeyUsage
keyPurposeId		Object Identifier										
CRLDistributionPoints (seq size (1...MAX))			**2.5.29.31**	**X**	**-**		**M**	**N**		**M**	**N**	
	DistributionPoint (seq)											
	distributionPoint	DistributionPointName							Mengacu ke RFC 5280 Diisi dengan alamat CRL yang memuat URL yang dapat dipakai oleh Pengandal untuk memeriksa status Sertifikat			Mengacu ke RFC 5280 Section 4.2.1.13 Diisi dengan alamat CRL yang memuat URL yang dapat dipakai oleh Pengandal untuk memeriksa status Sertifikat
	reasons	ReasonFlags										
	cRLIssuer	GeneralNames										Issuer CRL harus sama dengan PSrE, maka field ini harus dikosongkan
FreshestCRL			**2.5.29.46**	**X**	**-**		**O**	**N**		**O**	**N**	
freshestCRL		CRLDistributionPoi										

Field		Type	OID	PSrE Induk			PSrE Indonesia			Subscriber/Pemilik		
				M	C	Information	M	C		M	C	
		nt										
AuthorityInfoAccess (seq size (1..MAX))			**2.5.29.1**									
	AccessDescription (seq)											
	accessMethod	OBJECT IDENTIFIER		**X**	-		**X**	**-**		**M**	**N**	1.3.6.1.5.5.7.48.1
	accessLocation	GeneralName										OCSP URL
	AccessDescription (seq)											
	accessMethod	OBJECT IDENTIFIER		**X**	-		**X**	-		**M**	**N**	1.3.6.1.5.5.7.48.2
	accessLocation	GeneralName		**X**	-		**X**	-				ca Issuer URL

II.2. Profil CRL (Certificate Revocation List)

II.2.1. CRL Profile

Field	*ASN.1 Type*	*Note*	*M*
version	Integer	1 (version2)	**M**
issuer	Name		**M**
thisUpdate	UTCTime	Issuing date	**M**
nextUpdate	UTCTime	According CA's policy	**M**

revokedCertificates			**M**
userCertificate	Integer		**M**
revocationDate	UTCTime		**M**
crlEntryExtension	Extensions		**O**
crlExtensions			**M**

II.2.2. CRL Extension Field

Field	*ASN.1 Type*	*Note*	*C*	*M*
authorityKeyIdentifier			N	M
issuerAltName	otherName		N	O
cRLNumber	Integer		C	M
issuingDistributionPoint			C	O

II.3. Profil OCSP

Panduan Layanan OCSP:

1. PSrE Indonesia harus mendukung kapabilitas OCSP memakai metode GET atau POST untuk Sertifikat yang diterbitkan di bawah hierarki PSrE Induk.
2. PSrE Indonesia harus mengoperasikan kapabilitas OCSP yang menyediakan waktu respon sepuluh detik atau kurang di bawah kondisi operasi normal.
3. Respon OCSP harus ditandatangani oleh OCSP Responder yang sertifikatnya ditandatangani oleh PSrE Indonesia (Berinduk) yang menerbitkan Sertifikat yang statusnya sedang diperiksa.
4. Bila OCSP Responder menerima suatu permintaan status bagi sebuah Sertifikat yang belum pernah diterbitkan, responder TIDAK BOLEH menjawab dengan status “good”. PSrE Indonesia HARUS memantau responder atas permintaan-permintaan seperti itu sebagai bagian dari prosedur respon keamanan.
5. Sebagai bagian dari inisiatif interoperabilitas, Sertifikat yang diterbitkan oleh PSrE Indonesia harus memiliki `accessLocation` yang menunjuk ke OCSP Responder milik PSrE Indonesia.
6. Proses *end-to-end* harus diotomatisasi untuk penyediaan OCSP ke Pihak Pengandal. Tidak boleh ada intervensi manual kecuali ketika muncul

masalah.
7. OCSP harus menerima permintaan OCSP yang ditandatangani maupun tidak ditandatangani.
8. OCSP harus memberikan respon yang real time untuk status Sertifikat.
9. OCSP Responder harus bisa mendukung *nonce extension* dalam permintaan dan respon.
10. CPS PSrE harus mencerminkan persyaratan di atas dan ruang lingkup audit CA harus termasuk operasi layanan OCSP.
11. Rincian profil request dan respon ke dan dari OCSP responder mengacu kepada RFC 6960.

II.3.1. OCSP Request

Field	Type	M	OCSP Request
OCSPRequest (seq)			
`tbsRequest`	TBSRequest	**M**	
`optionalSignature`	EXPLICIT Signature OPTIONAL	**O**	
TBSRequest (seq)			
`version`	Integer	**M**	Harus menggunakan v1(0)
`requestorName`	EXPLICIT GeneralName OPTIONAL	**O**	GeneralName requestor OCSP
`requestList`	SEQUENCE OF Request	**M**	
Request(seq)			
`reqCert`	CertID	**M**	
CertID (seq)			
`hashAlgorithm`	OBJECT IDENTIFIER	**M**	
`issuerNameHash`	OCTET STRING	**M**	Hash of issuer's DN
`issuerKeyHash`	OCTET STRING	**M**	Hash of issuer's public key

	serialNumber	CertificateSerialNumber	**M**	CertificateSerialNumber
	singleRequestExtensions	EXPLICIT Extensions OPTIONAL	**O**	NULL
requestExtensions		EXPLICIT Extensions OPTIONAL	**O**	
Signature (seq)			**O**	
signatureAlgorithm		OBJECT IDENTIFIER	**M**	1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
signature		BIT STRING	**M**	Tanda tangan Pemilik
certs		EXPLICIT SEQUENCE OF Certificate	**M**	certificate Pemilik

II.3.2. OCSP Response

Field	Type	M	OCSP Response
OCSPResponse (seq)			
responseStatus	Enumerated	**M**	successful (0), -- Response has valid confirmations malformedRequest (1), -- Illegal confirmation request internalError (2), -- Internal error in issuer tryLater (3), -- Try again later sigRequired (5), -- Must sign the request unauthorized (6) -- Request unauthorized
responseBytes	[0] EXPLICIT ResponseBytes OPTIONAL	**O**	
ResponseBytes (seq)			

	responseType	OBJECT IDENTIFIER	**M**	id-pkix-ocsp 1
	response	OCTET STRING	**M**	he value for response SHALL be the DER encoding of **BasicOCSPResponse**
BasicOCSPResponse (seq)				
tbsResponseData		ResponseData	**M**	
	ResponseData(seq)			
	version	EXPLICIT Version DEFAULT v1	**M**	Harus menggunakan v1(0)
	responderID	ResponderID		CHOICE := byName : Name byKey : KeyHash KeyHash ::= OCTET STRING -- SHA-1 hash of responder's public key
	producedAt	GeneralizedTime	**M**	
	responses	SEQUENCE OF SingleResponse	**M**	
		SingleResponse (seq)		
		certID	CertID	**M**
		certStatus	CertStatus	**M**	CHOICE := good : Good revoked : RevokedInfo unknown : Unknown
		thisUpdate	GeneralizedTime	**M**	
		nextUpdate	EXPLICIT GeneralizedTime OPTIONAL	**O**	
		singleExtensions	EXPLICIT Extensions OPTIONAL	**O**	

	responseExtensions	EXPLICIT Extensions OPTIONAL	**O**	
signatureAlgorithm		AlgorithmIdentifier	**O**	GeneralName requestor OCSP
signature		BIT STRING	**M**	
certs		EXPLICIT SEQUENCE OF Certificate OPTIONAL	**O**	

II.3.3. OCSP Responder Certificate Profile

II.3.3.1. Basic Field

Field		Type	M	OCSP Certificate
Certificate (seq)				
tbsCertificate		TBSCertificate	**M**	
signatureAlgorithm, memiliki subfield:		AlgorithmIdentifier	**M**	
	AlgorithmIdentifier (seq)			
	algorithm	OBJECT IDENTIFIER		1.2.840.113549.1.1.11 (sha256WithRSAEncryption)
	parameters	ANY DEFINED BY algorithm OPTIONAL		NULL
signatureValue		BIT STRING	**M**	Tanda tangan PSrE Indonesia penerbit Sertifikat
TBSCertificate (seq)				
version		INTEGER{v1(0), v2(1), v3(2)}	**M**	Harus menggunakan versi 3
serialNumber		INTEGER	**M**	Serial number sertifikat
signature, memiliki subfield:		AlgorithmIdentifier	**M**	

	AlgorithmIdentifier (seq)			
	algorithm	OBJECT IDENTIFIER		RSA algorithm identifier (1.2.840.113549.1.1.11)
	parameters	ANY DEFINED BY algorithm OPTIONAL		NULL
issuer		Name	**M**	DN CA Issuer
validity, memiliki subfield:		Validity	**M**	3 tahun
	Validity(seq)			
	notBefore	UTCTime		Waktu mulai validitas
	notAfter	UTCTime		Waktu validitas berakhir
subject		Name	**M**	DN Pemilik Sertifikat (CN={Nama OCSP Responder}, OU=OCSP Responder, O=Nama Legal PSrE, C=ID)
subjectPublicKeyInfo, memiliki subfield:		SubjectPublicKeyInfo	**M**	
	SubjectPublicKeyInfo (seq)			
	algorithm	AlgorithmIdentifier		
		AlgorithmIdentifier (seq)		
		algorithm	OBJECT IDENTIFIER	1.2.840.113549.1.1.1 (rsaEncryption) (Key Length: 2048)
		parameters	ANY DEFINED BY algorithm OPTIONAL	NULL
	subjectPublicKey	BIT STRING		Kunci Publik End Entity
extensions, memiliki subfield:		EXPLICIT Extensions	**M**	
	Extensions (seq size (1...MAX))			
	extension	EXTENSION		

		EXTENSION (seq)			
		extnID	OBJECT IDENTIFIER		OID dari extension
		critical	BOOLEAN DEFAULT FALSE		
		extnValue	OCTET STRING		Berisi nilai ASN.1 dari type ekstensi yang digunakan dengan menggunakan DER encoding

II.3.3.2. Standard Extension Field

Field	Type	OID	OCSP Certificate		
			M	C	
AuthorityKeyIdentifier (seq)		**2.5.29.35**	**M**	**N**	
keyIdentifier	OCTET STRING				SHA-1 160 bit
authorityCertIssuer	GeneralNames				
authorityCertSerialNumber	INTEGER				
SubjectKeyIdentifier		**2.5.29.14**	**M**	**N**	
subjectKeyIdentifier	OCTET STRING				SHA-1 160 bit
KeyUsage		**2.5.29.15**	**M**	**C**	
keyUsage	BIT STRING				digitalSignature
CertificatePolicies (seq size(1...MAX))		**2.5.29.32**	**M**	**C**	
policyInformation, memiliki subfield:	PolicyInformation				
PolicyInformation (seq)					
policyIdentifier	OBJECT IDENTIFIER				

	policyQualifiers	Sequence Size (1...MAX) PolicyQualifierInfo				
SubjectAlternativeName			**2.5.29.17**	**X**	**-**	
subjectAlternativeName		GeneralNames				
IssuerAlternativeName			**2.5.29.18**	**O**	**N**	
issuerAlternativeName		GeneralNames				
BasicConstraint (seq)			**2.5.29.19**	**M**	**C**	
cA		BOOLEAN				false
pathLenConstraint		INTEGER				
NameConstraint			**2.5.29.30**	**X**	**-**	
permittedSubtrees		GeneralSubtrees				
excludedSubtrees		GeneralSubtrees				
ExtendedKeyUsage (seq size (1...MAX))			**2.5.29.37**	**O**	**N**	
keyPurposeId		Object Identifier				1.3.6.1.5.5.7.3 (OCSP Signing)
FreshestCRL			**2.5.29.46**	**X**	**-**	
freshestCRL		CRLDistributionPoint				
AuthorityInfoAccess (seq size (1..MAX)), memiliki subfield:			**2.5.29.1**			
	AccessDescription (seq)					
	accessMethod	OBJECT IDENTIFIER		**X**	**-**	
	accessLocation	GeneralName				

III. Panduan Implementasi Certificate Path Validation

Objektif & Ruang Lingkup

Bagian ini membahas panduan implementasi *Certificate Path Validation*. Algoritme implementasi ini tercantum di dalam RFC 5280 bagian 6.

LAMPIRAN I:

Penulisan Atribut pada DN

Atribut	Keterangan	OID
UID or USERID	User identifier	0.9.2342.19200300.100.1.1
T	Title	2.5.4.12
DC	Domain component	1.3.6.1.4.1.311.1.1.3.1.3
STREET	Street / First line of address	2.5.4.9
L	Locality name	2.5.4.7
ST (or SP or S)	State or Province name	2.5.4.8
PC	Postal code / zip code	2.5.4.17
DNQ	Distinguished name qualifier	2.5.4.46
Description	Description	2.5.14.13