Guidance for Relying Party

Change History

Date	*Version*	*Created by*	*Change description*
9 February 2024	1.0	Purnomo Wahyu Hidayat	Initial document
			-

Contents

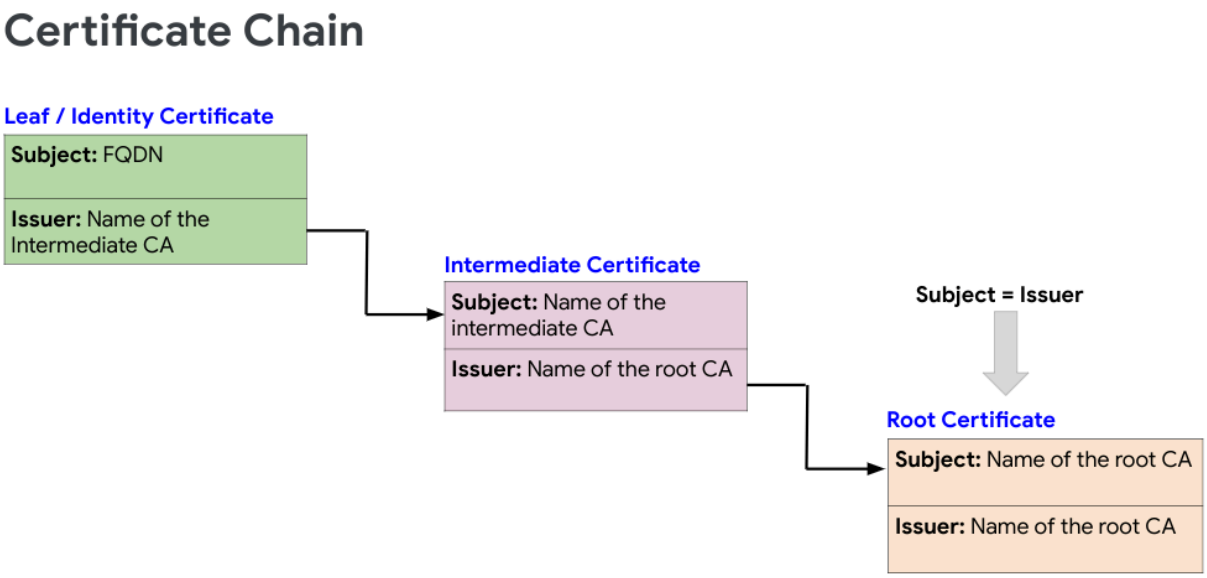
Overview

The purpose of this document is to explain about configuration that can be followed by a relying party to check the validity of a subscriber's digital certificate issued by VIDA. A relying party is an entity who, by using another's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the issuer of the certificate. It includes the entity who is relying on a document or transaction that is digitally signed with a certificate issued by VIDA. Relying party also relies on the validity of binding the Subscriber's name to a public key.

1. Verifying the certificate subject and issuer

a. Split the certificate chain into the following certificates
   - Entity certificate
   - Intermediate certificate
   - Root certificate

b. The following figure shows an example certificate chain:



c. Run the following OpenSSL command to get the Subject and Issuer for each certificate in the chain from entity to root and verify that they form a proper certificate chain:

openssl x509 -text -in ***certificate***

Where ***certificate*** is the name of the certificate.

d. Verify that the certificates in the chain adhere to the following guidelines
    - Subject of each certificate matches the Issuer of the preceding certificate in the chain (except for the Entity certificate).
    - Subject and Issuer are the same for the root certificate.

Sample output issuing :
openssl x509 -text -in issuer.pem | grep -E '(Subject|Issuer):'

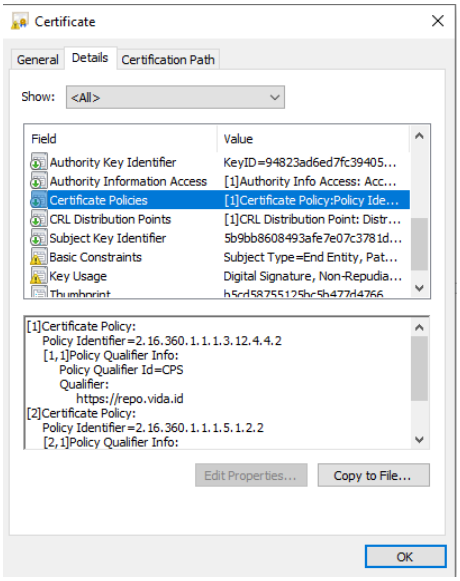
Rooted By Kominfo

Issuer: CN=Root CA Indonesia DS G1, O=Kementerian Komunikasi dan Informatika, C=ID
Subject: CN=VIDA Certificate Authority, OU=CA, O=PT Indonesia Digital Identity, L=Jakarta, ST=DKI Jakarta, C=ID

Issuer: CN=VIDA Root Certificate Authority, OU=CA, O=PT Indonesia Digital Indentity, L=Jakarta, ST=DKI Jakarta, C=ID
Subject: CN=VIDA Sign Certificate Authority, OU=CA, O=PT Indonesia Digital Identity, L=Jakarta, ST=DKI Jakarta, C=ID

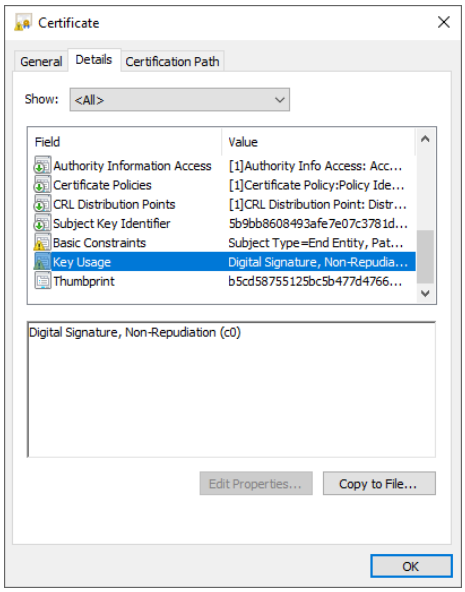
2. Checking Certificate Policies

Certificate policies can be found inside certificate subscribers section **Certificate Policies**



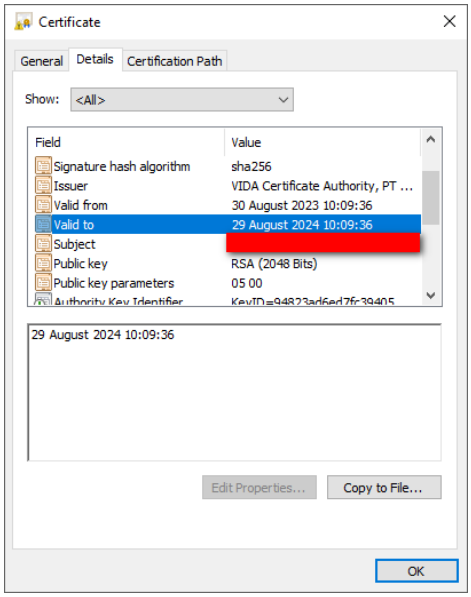
3. Checking Certificate Usage

Certificate usage can be found inside certificate subscribers section **Key Usage**



4. Checking Certificate Validity

Certificate usage can be found inside certificate subscribers section **Valid to**



5. Checking if the subscriber certificate is still valid using OCSP and CRL ?

5.1. OCSP

VIDA provides OCSP. OCSP (Online Certificate Status Protocol) that can be used by relying party to check the validity of certificates in real-time.

- OpenSSL

Using OpenSSL, you can connect to VIDA OCSP. You need to download certificates based on the provided link and follow the command below:

Request :

openssl ocsp -issuer <VIDAIssuingCA.cer> -CAfile <VIDARootCA.cer> -cert <UserCertificate.cer> -req_text -url <VIDA OCSP Url>

Response Valid Certificate :

OCSP Request Data:
  Version: 1 (0x0)
  Requestor List:
    Certificate ID:
      Hash Algorithm: sha1

Issuer Name Hash: 9563A04DCEAFD7545AA1EE4769272E3C51826CAB
Issuer Key Hash: 0F7EDF996A38958C8944F1AB8F7BA949EB6CCEA5
Serial Number: 76E32E3E1A1AFD9E0AD2E68EE3C00C19B0D9EB5E
Request Extensions:
OCSP Nonce:
04109D54DC61BB9DA354F25A5ADD3FEA6850
Response verify OK
UserCertificate.cer: good
This Update: Apr 28 05:40:38 2020 GMT

Response Revoke Certificate And Reason :

OCSP Request Data:
Version: 1 (0x0)
Requestor List:
Certificate ID:
Hash Algorithm: sha1
Issuer Name Hash: 9563A04DCEAFD7545AA1EE4769272E3C51826CAB
Issuer Key Hash: 0F7EDF996A38958C8944F1AB8F7BA949EB6CCEA5
Serial Number: 76E32E3E1A1AFD9E0AD2E68EE3C00C19B0D9EB5E
Request Extensions:
OCSP Nonce:
041087120733A04C1EBB9155BD1542C667AA
Response verify OK
UserCertificate.cer: revoked
This Update: Apr 28 05:41:56 2020 GMT
Reason: keyCompromise
Revocation Time: Apr 28 05:40:08 2020 GMT

Response Expired Certificate Or Not Issued By VIDA :

OCSP Request Data:
Version: 1 (0x0)
Requestor List:
Certificate ID:
Hash Algorithm: sha1
Issuer Name Hash: 9563A04DCEAFD7545AA1EE4769272E3C51826CAB
Issuer Key Hash: 0F7EDF996A38958C8944F1AB8F7BA949EB6CCEA5
Serial Number: 76E32E3E1A1AFD9E0AD2E68EE3C00C19B0D9EB5E
Request Extensions:
OCSP Nonce:
041087120733A04C1EBB9155BD1542C667AA
Response verify UNKNOWN
UserCertificate.cer: unknown

This Update: Apr 28 05:41:56 2020 GMT

In order to obtain VIDA CA Revocation Status using OCSP, visit the following sites:

VIDA ROOT CERTIFICATE AUTHORITY

- OCSP Service
- Port for OCSP Service – 80

VIDA SIGN CERTIFICATE AUTHORITY

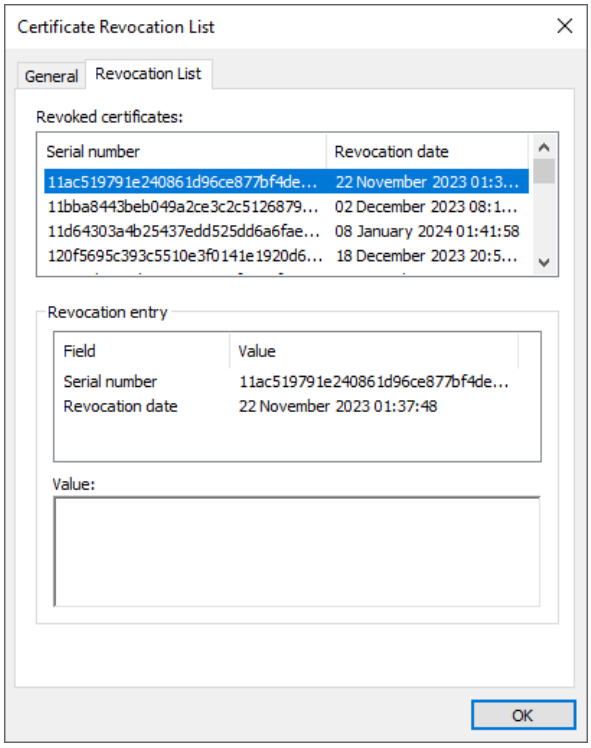
- OCSP Service
- Port for OCSP Service – 80

VIDA CERTIFICATE AUTHORITY

- OCSP Service
- Port for OCSP Service – 80

5.2. CRL

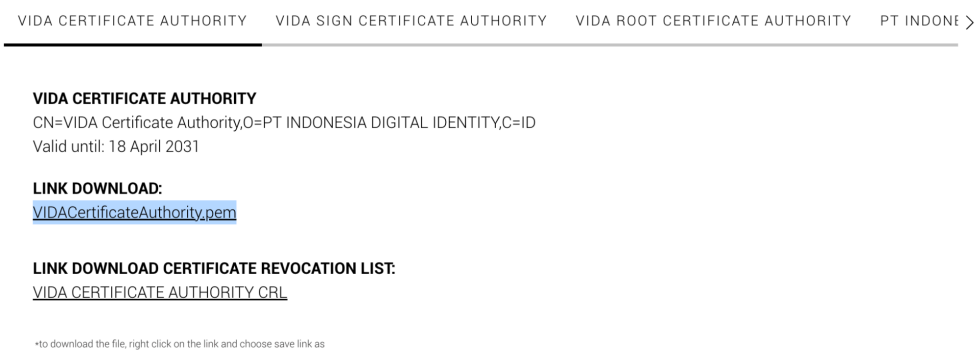
CRL is a list of digital certificates that have been revoked. Please note that expired certificates are not included in the CRL file.



Certificate is revoked if serial number certificate listed in CRL list.
You need to download CRL's based on the provided link and follow the command below:

In order to obtain VIDA CA certificates and the CRLs via https:

1. Visit VIDA repository page in https://repo.vida.id
2. Right click on the chosen link
3. Choose "Save Link As"



VIDA CA Certificates

VIDA ROOT CERTIFICATE AUTHORITY

CN=VIDA Root Certificate Authority,OU=CA,O=PT Indonesia Digital Indentity,L=Jakarta,ST=DKI Jakarta,C=ID
Valid until: 1 Januari 2038
Download

VIDA SIGN CERTIFICATE AUTHORITY

CN=VIDA Sign Certificate Authority,OU=CA,O=PT Indonesia Digital Identity,L=Jakarta,ST=DKI Jakarta,C=ID
Valid until: 26 Mei 2030
Download

VIDA CERTIFICATE AUTHORITY

CN=VIDA Certificate Authority,O=PT INDONESIA DIGITAL IDENTITY,C=ID
Valid until: 18 April 2031
Download

CRLs

- VIDA ROOT CERTIFICATE AUTHORITY
- VIDA SIGN CERTIFICATE AUTHORITY
- VIDA CERTIFICATE AUTHORITY

Regulatory Compliance

PT Indonesia Digital Identity - VIDA is an Certificate Authority (CA) in Indonesia that is rooted under Root CA Indonesia operated by Kemenkominfo based on SK Dirjen Aptika Kemenkominfo No.1 Year 2023. See more information in VIDA Repository