FAQ: MIGRATION EXERCISE SHA1 to SHA2

RELEASED: 23rd April, 2019 (Version 4)

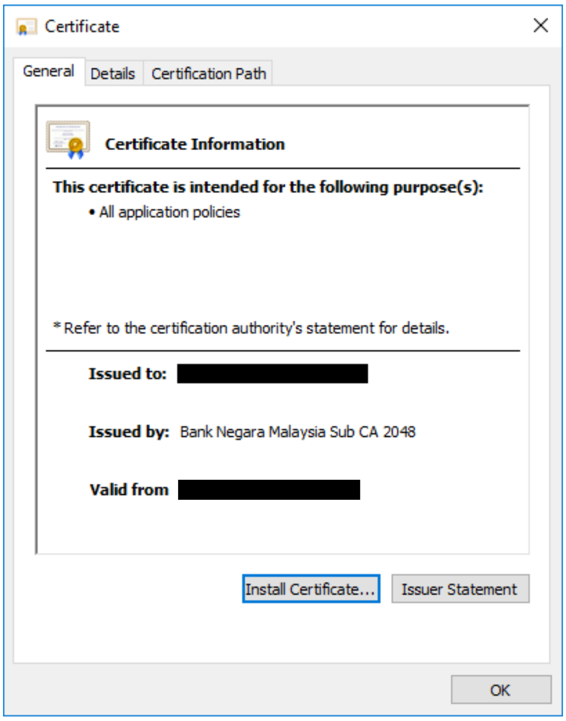
1. WHY I NEED TO REPLACE MY CERTIFICATE?

SHA-1 has been in use among commercial certification authorities (CAs) since the late 1990s but has been deprecated since November 2013. Recent advances in cryptographic attacks upon SHA-1 have led to the decision that the industry must prohibit continued issuance of SHA-1, but also transition to SHA-2 certificates, which are exponentially more secure. With SHA-2 certificates now available and widely supported by browsers and servers, and the technical deadline for replacement fast approaching, organizations need to maintain their migration path and process to ensure that there are no service disruptions or compromises of their security posture.

Further to the above Microsoft, Google and Mozilla have already started phasing out trust for SHA-1 SSL Certificates as of January 2017. In basic terms, SHA is a component of digital certificates used to ensure that data has not been modified. SHA-2 is the technical successor to SHA-1 and provides greater security than SHA-1. As computing power increases, SHA-1 will be able to be decrypted more easily and susceptible to exploitation by criminals and hackers. Administrators who have not yet replaced their SHA-1 certificates with SHA-2 certificates should start making the transition now as the risks associated SHA-1 are greater than previously expected.

The new replacement certificate from us will be using the SHA-2 signature algorithm. To facilitate this transition, please reach our Customer Care Team via email at customercare@posdigicert.com.my or via phone at 03 – 8800 8008 to initiate your Certificate Replacement.

Below is the sample of affected SHA1 certificate that needs to be migrated to SHA2:



Certificate Information

This certificate is intended for the following purpose(s):

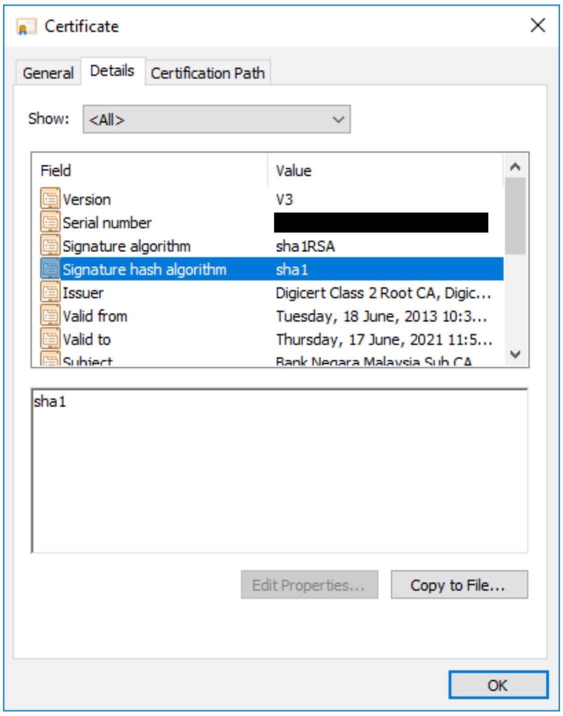
- All application policies

* Refer to the certification authority's statement for details.

Issued to: [redacted]

Issued by: Bank Negara Malaysia Sub CA 2048

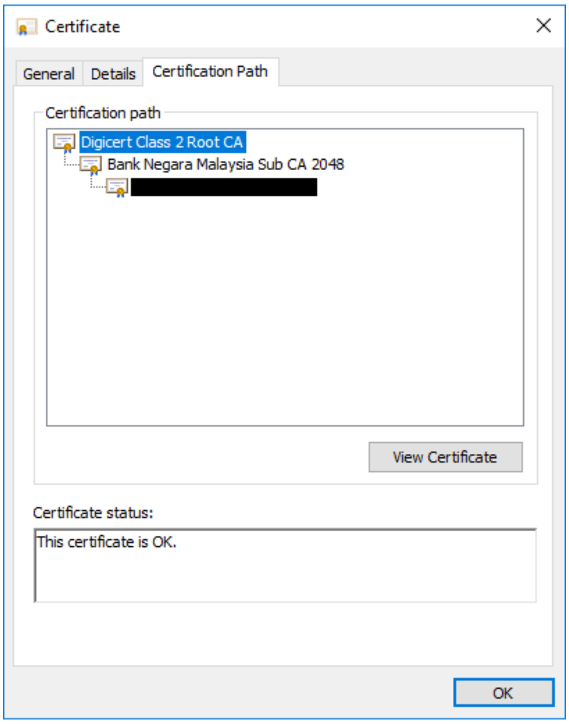
Valid from [redacted]



Show: <All>

Field	Value
Version	V3
Serial number	[redacted]
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	Digicert Class 2 Root CA, Digic...
Valid from	Tuesday, 18 June, 2013 10:3...
Valid to	Thursday, 17 June, 2021 11:5...
Subject	Bank Negara Malaysia Sub CA

sha1



Certification path

Digicert Class 2 Root CA
Bank Negara Malaysia Sub CA 2048
[redacted]

Certificate status:

This certificate is OK.

2. WHAT WILL HAPPEN IF I DON’T REPLACE THE CERTIFICATE?

a) Your website will be not accessible due to the security restrictions from the major web browsers.

b) Application owners who have restricted the SHA1 certificates will result in users not being able to perform signing, authentication or submit their reports.

c) Your organisation’s daily operations which are dependent on the usage of existing certificates will be interrupted.

3. WHO IS AFFECTED?

All users who are currently using the certificates below:

Pos Digicert Root Certificate

- Pos Digicert Class 1 Root CA
- Pos Digicert Class 2 Root CA

Pos Digicert Intermediate Certificate

- Class 1 2048 - Digisign ID
- Class 2 2048 - Bank Negara Malaysia
- Class 2 2048 - Digisign ID Basic
- Class 2 2048 - Bank Muamalat Malaysia Berhad
- Class 2 2048 - Digisign ID Enhanced
- Class 2 2048 - Digisign iVest CA
- Class 2 2048 - Digisign iVest CA Enhanced
- Class 2 2048 - Malaysia Premier CA
- Class 2 NCSA

4. DO I HAVE TO INCUR ANY REPLACEMENT COST?

Yes. The pricing is similar to your current product package. Please contact our Sales Team at sales@posdigicert.com.my to get the latest quotation on our products and services.

5. WHAT ARE THE REQUIRED DOCUMENTS?

For new and existing SHA-1 users you will need to complete both the ***Individual Certificate Application Form*** *and* ***Certificate Replacement Form - SHA1 to SHA2 Migration.*** The forms be downloaded at https://www.posdigicert.com.my/downloadpage/form. Please submit the required replacement form and CSR (if applicable) to applications@posdigicert.com.my.

8. SALIENT POINTS

What Users Need to Do?

1. Check on the readiness of their application with the application owners on whether it's SHA-2 ready.
2. For contingency purposes you may need to maintain both SHA-1 and SHA-2 certificates. You may check with your application owners on this as well.
3. Download new SHA-2 (G3) root certificate into their computers.
4. Migrate to SHA-2 user certificates by purchasing them with Pos Digicert.

Certificate Issuance

- SHA-1 certificates will only be issued up to 31 December 2018.
- Starting 1st January 2019 onwards, only SHA-2 certificates will be issued.
- Starting 1st April 2019, all existing SHA-1 certificates will be revoked by phases by Pos Digicert.

END

POS DIGICERT SDN BHD

With over a decade of experience, Pos Digicert strives to offer world-class security solution technologies to help application service providers enhance their effectiveness and capabilities in addressing security challenges. Pos Digicert will continue to build on its core strength and move forward in making its mark as a trusted and reliable electronic identity and security services provider.

Disclaimer: While care has been taken to ensure that information contained in the Pos Digicert's publications is true and correct at the time of publication, changes in circumstances after the time of publication may impact on the accuracy of this information. Pos Digicert makes no representation regarding the completeness, accuracy, or timeliness of any information and data posted in this document will be error-free

For more information, please visit our website at https://www.posdigicert.com.my or call our Customer Care at 03 – 8800 8008.

© 2019 Copyright: Pos Digicert Sdn Bhd