SSL Certificate Service

Product Announcement

Product Documentation

Contents

Product Announcement
Domain Validation Policy Update

Last updated : 2021-07-02 09:48:01

In order to comply with the requirements of CA/Browser Forum, the following changes will be introduced to domain validation policies, which will take effect from **December 1, 2021**.

From December 1, 2021, file validation supports only issuing the SSL certificate for the current validated domain, but not wildcard SSL certificates as well as its sub-domains.

Currently, Tencent Cloud's SSL Certificate Service only requires validating the primary domain (e.g., `dnspod.cn`), and will also issue SSL certificates for wildcard certificates (e.g., `*.dnspod.cn` or `*.sub.dnspod.cn`) and its sub-domains (e.g., `sub.dnspod.cn` or `sub2.sub1.dnspod.cn`).

But from December 1, 2021, if a domain is validated using file validation, the certificate can only be issued for the domain validated. For example, if the domain `dnspod.cn` is validated using file validation, an SSL certificate can only be issued for the `dnspod.cn` domain, but not `*.dnspod.cn` or `sub.dnspod.cn`.

Notice on Stopping the Issuance of 2-Year SSL Certificates by CAs Starting from September 1, 2020

Last updated : 2020-09-03 17:47:42

Due to the changes in Apple and Google's root store policies, as of September 1, 2020, newly issued SSL/TLS certificates with a validity period greater than 13 months (397 days) will be prohibited by policy and will not be trusted. Starting from September 1, 2020, global CAs will no longer issue 2-year SSL certificates. Tencent Cloud will also stop providing the 2-year SSL certificate purchase service from August 25, 2020. To purchase a 2-year SSL certificate, ensure that it is requested and issued before August 25, 2020.

FAQs:

What changes will the policy changes bring?

Due to the root store policy changes of Apple and Google, as of September 1, 2020, the validity periods of newly issued SSL/TLS certificates cannot exceed 13 months.

When will the policy changes take effect?

September 1, 2020.

I just bought a 2-year SSL certificate. Will it still be trusted after September 1, 2020?

Certificates issued before September 1, 2020 with a validity period longer than 397 days will not be affected by the policy changes.

What happens if I reprocess a 2-year certificate after the policy changes take effect?

If you reprocess a 2-year certificate after September 1, 2020, the validity period of the reissued certificate will be limited to 397 days.

⚠ Note :

Thank you for your support for Tencent Cloud. We will, as always, continue to provide you with professional HTTPS services.
If you encounter any problems while using our services, contact us for assistance by submitting a ticket.

Announcement on Stop Using the Symantec SSL Certificate Name After 30 April 2020

Last updated : 2020-06-01 17:17:55

DigiCert (formerly Symantec) noted that the Symantec logo would not be used on its SSL certificate after 30 April 2020.

Updates

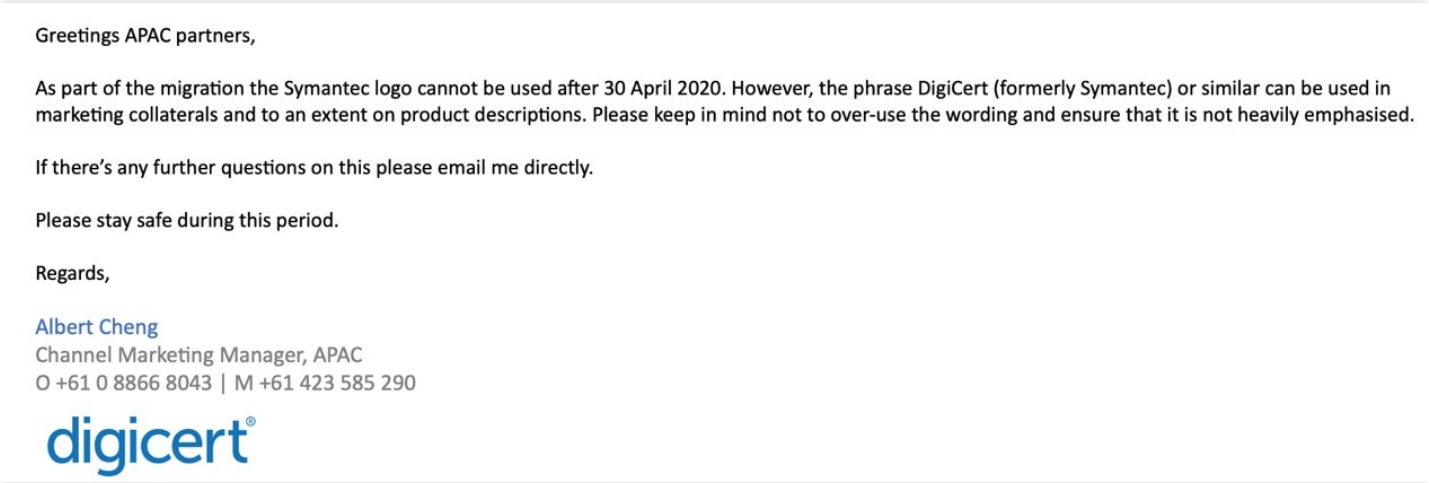
1. The Symantec SSL Certificate is renamed as DigiCert Secure Site SSL Certificate, as shown in the following figure.

2. Norton Secured Seal is also updated, as shown in the following figure.

- Renaming exerts no influence on certificate delivery and use.
- After renaming, the original product features and services remain unchanged. Moreover, DigiCert provides Secure Site Pro to support the post-quantum algorithm feature.

DigiCert Announcement

The following figure shows the announcement from DigiCert:



Greetings APAC partners,

As part of the migration the Symantec logo cannot be used after 30 April 2020. However, the phrase DigiCert (formerly Symantec) or similar can be used in marketing collaterals and to an extent on product descriptions. Please keep in mind not to over-use the wording and ensure that it is not heavily emphasised.

If there's any further questions on this please email me directly.

Please stay safe during this period.

Regards,

Albert Cheng
Channel Marketing Manager, APAC
O +61 0 8866 8043 | M +61 423 585 290

digicert®

- Thank you for your support for Tencent Cloud. We will, as always, continue to provide you with professional HTTPS service.
- If you have any problems when using our services, contact us by submitting a ticket.

Notice on DigiCert’s Certificate Revocation Due to Private Key Compromises

Last updated：2020-09-03 17:48:23

According to DigiCert's notice, DigiCert launched a private key compromise detection system in late April 2020. The system automatically detects private key compromises on project code hosting platforms such as GitHub and SourceForge. If the system detects compromised private keys, DigiCert will notify subscribers and revoke the corresponding certificates after 24 hours.
To protect your website and information security, please keep your certificate's private key safe. Do not upload your private key to public networks to avoid incidents such as certificate revocation or information leakage.

⚠ Note：

Thank you for your support for Tencent Cloud. We will, as always, continue to provide you with professional HTTPS services.
If you encounter any problems while using our services, contact us for assistance by submitting a ticket.