



Dear Colleagues,

Thank you for your diligence and patience with the TMCH-CA renewal process this past February. Thanks to the work by all parties, this renewal was executed without incident.

With this renewal, we had planned for the TMCH-CA root certificate to be valid for 20 years. Unfortunately, due to circumstances beyond our control the TMCH-CA will need to be recertified much sooner than expected.

Recently we became aware of a decision by the manufacturer of our hardware security modules (HSMs) to cease production of the devices. Further, there is no successor product as they are exiting that line of business, and support for their current products will cease in March 2025[1].

The Keyper products we use were in part selected as they were the only viable device that met FIPS 140-2 Level 4 certification, the highest certification possible. They do not provide a function that would allow the private key to be exported and imported into an alternative vendor's device.

Given this information, we are commencing an analysis of the options available regarding HSMs for use with the TMCH-CA. At present, we have no further information or timelines regarding the next regeneration and recertification of the TMCH-CA root certificate.

For the time being, the TMCH-CA will continue to operate as is, and no actions are required on your part. Once we have a better knowledge of this situation and more information, we will provide it to you.

Thank you for your understanding, and we regret and apologize for this inconvenience.

If you have any questions, please contact [ICANN Global Support](#).

Technical Services  
Global Domains and Strategy  
Internet Corporation for Assigned Names and Numbers (ICANN)