ICTA
INFORMATION & COMMUNICATION TECHNOLOGIES AUTHORITY

CONTROLLER OF CERTIFICATION AUTHORITIES (CCA)

Level 12, The Celicourt 6, Sir Celicourt Antelme Street Port Louis Mauritius
Tel.: (230) 211 5333/4 Fax: (230) 211 9444 email: info@cca.mu

CCA
CONTROLLER OF CERTIFICATION AUTHORITIES OF MAURITIUS

THE CCA DIRECTIVE 1 of 2020

Ref: ICTA/CCA/CCAD/1/2020 02 June 2020

The Information and Communication Technologies Authority in the exercise of its function as the Controller of Certification Authorities and in pursuance of Section 18 (1) (z) of the Information and Communication Technologies Act 2001 (as amended), Section 37 of the Electronic Transactions Act 2000 (as amended) and Regulation 3 (3) of the Electronic Transactions (Certification Authorities) Regulations 2010, hereby issues the following Directive.

1. Short title and Commencement

   a) This Directive shall be called "The CCA Directive 1 of 2020 - (CCAD 1 of 2020)"

   b) The CCA Directive 1 of 2020 shall come into effect on 02 June 2020.

2. Scope and objective

   This Directive pertains to security measures for the management and operation of licensed, recognised and approved Certification Authorities (CAs). The purpose of the OCSP is to ensure the online verification of the validity of the digital certificates issued to licensed/recognised/approved CAs.

Mr Dick Christophe Ng Sui Wa
Chairman

Mr Jerome Louis
Officer in Charge

To: All Licensed, Recognised and Approved Certification Authorities

ICTA
INFORMATION & COMMUNICATION TECHNOLOGIES AUTHORITY

CONTROLLER OF CERTIFICATION AUTHORITIES (CCA)

Level 12, The Celicourt 6, Sir Celicourt Antelme Street Port Louis Mauritius
Tel.: (230) 211 5333/4 Fax: (230) 211 9444 email: info@cca.mu

CCA
CONTROLLER OF CERTIFICATION AUTHORITIES OF MAURITIUS

Directive 1 of 2020

1. All Certification Authorities (CAs) licensed/recognised/approved by the Controller of Certification Authorities of Mauritius (CCA) shall establish both an Online Certificate Status Protocol (OCSP) Service and a Certificate Revocation List (CRL) service to enable relying-party application software to determine the status of an identified Certificate in an online mode.

2. The CAs should operate their OCSP and CRL services as per the requirements set out in this document as follows:

    a. The CA shall support the generation and publishing of a CRL.

    b. The CA shall include the Uniform Resource Identifier (URI) of the published CRL to the CRL Distribution Point extension in CA issued certificates.

    c. OCSP and CRL revoked certificates shall be synchronised at all times.

    d. The use of OCSP stapling is mandatory for performance and security reasons, therefore, when supported by an end user server, the CA shall add the OCSP "Must-Staple" extension to issued certificates.

    e. OCSP responses must be signed by an OCSP Responder whose certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

    f. The end to end process must be automated for providing OCSP response to a Relying Party.

3. All CAs licensed/recognised/approved by the CCA Mauritius should modify their Certificate Practice Statement (CPS) to reflect the above requirements and the scope of the CA audit should include OCSP service operations.