



Serial No. N5962

NAFO/FC Doc. 11/27
(ADOPTED)

33rd ANNUAL MEETING – SEPTEMBER 2011

Amendment to NAFO CEM Annex XIX

Introduction

Based on investigation performed by the Secretariat at the request of STACTIC regarding 'best practices' for HTTPs communication, it would seem appropriate to proceed to implement a system of security certificate management that accounts for the revocation of certificates using Certificate Revocation Lists (CRL), which is not currently the practice followed by the NAFO Secretariat. The consequence would be that :

1. All FMCs would be required to use certificates from a recognized Certificate Authority for VMS communication
2. The Secretariat would need to purchase a 3rd party-signed certificate, and distribute the public certificate to all inspection CPs and communicating FMCs
3. Update the current VMS software to accommodate the changes

Furthermore, it would seem necessary to update the text in NCEM Annex XIX (Provisions on security) para. 4.4. to reflect the need to ensure that public certificates more completely identify and validate the submitting party.

(amended text underlined):

Annex XIX - 4.4 Communication Security

Appropriate encryption protocols duly tested by the Secretariat and approved by the Fisheries Commission shall be applied to ensure confidentiality and authenticity. Key management policy shall be in place to support the use of cryptographic techniques. In particular, the integrity of the PKI (public key infrastructure) will be guaranteed by ensuring that digital certificates correctly identify and validate the party submitting the information.