Requirements for protection of software emailed to NIST

1. Scope

A number of NIST's evaluation programs require the sending of libraries, executables and data to NIST. This document establishes exact specifications for the cryptographic protection of such materials. Particularly, it gives procedures for the provider of the software to sign the material to protect integrity and to support NIST in authenticating the sender. In addition this document gives the mechanism by which the material can be encrypted for confidentiality.

By encrypting the submissions, we ensure privacy; by signing the submission, we ensure authenticity (the software actually belongs to the submitter).

2. Submission of software to NIST

NIST requires that all software submitted by the participants be signed and encrypted. Two keys pairs are needed:

- Signing is done with the software provider's private key, and
- Encryption is done with NIST's public key, which is published on the NFIQ2.0 website.

NIST will validate all submitted materials using the participant's public key, and the authenticity of that key will be verified using the key's fingerprint. This fingerprint must be submitted to NIST in writing, normally by writing it on the signed participation agreement.

All cryptographic operations (signing and encrypting) shall be performed with software that implements the OpenPGP standard, as described in Internet RFC 4880. The freely available Gnu Privacy Guard (GPG) software, available at www.gnupg.org, is one such implementation.

The steps below show how to create a public/private key pair and fingerprint using the GPG software.

Participant generates their own key		
1	Generate your key pair	gpg --gen-key <press Enter for the default key type, DSA and Elgamal> <Choose a key size of 2048> <Choose a non-expiring key> <Press 'y'> <Enter Real Name> <Enter email address; this is the key identity> <Enter an optional comment> <Press 'O' to continue> <Enter a passphrase for the secret (private) key> Once the pair is generated, the key must be exported in the proper format to be sent to NIST. It is crucial that the applicant protect the private key by choosing a strong password that is not shared.
2	Export your public key	gpg --armor --output fornfiq2.gpg --export <email> where <email> is the address used in step 1 above; this address is the key identity. The public key will be saved into the file named 'fornfiq2.gpg'.
3	Email your public key	The file containing the public key must be sent to the NFIQ2 Liaison, nfiq2@nist.gov.
4	Write your public key fingerprint on the participation agreement	gpg --fingerprint <email> Where the <email> address is the same as in step 1. The key fingerprint will be shown in the output as a set of hex digits. The fingerprint must be copied onto the paper participant agreement sent to NIST.

Participant imports NIST's public key. The next series of step show how the participant will import the NFIQ2 public key, and authenticate that key using the key fingerprint. The NFIQ2 public key will be sent to each participant after receiving the signed agreement.		
1	Import NIST's NFIQ2's public key, contained in a file called public_nfiq2.gpg, for example	gpg --import public_nfiq2.gpg The output should be similar to: gpg: key 150CA80B: "ElhamTabassi <nfiq2@nist.gov>" imported . The key can be cut-and-pasted from http://www.nist.gov/itl/iad/ig/development_nfiq_2.cfm
2	Authenticate the NFIQ2 key	gpg --fingerprint nfiq2@nist.gov The key fingerprint will be shown in the output as a set of hex digits. These digits must be the same as our NFIQ2 public key fingerprint, which is posted on NFIQ2 website. If the fingerprints do not match, contact NIST and do not use the NFIQ2 key for encrypting.
3	Optionally, the participant may want to assign a level of trust to the NFIQ2 public key.	gpg --edit-key nfiq2@nist.gov <Enter 'trust' at the Command prompt> <Choose a trust level; 3 is a good choice> <Enter 'y' to approve the trust selection, if asked> <Enter 'q' to quit>
Sending software to NIST By following the above series of steps, the keys have been generated and exchanged between NIST and the participant. From this point forward, all software submissions MUST be signed and encrypted. In addition, general email communication can be encrypted and signed, if desired.		
1	Encrypt and sign the file to be submitted to NIST	gpg --default-key <email> --output <filename>.gpg --encrypt --recipient irex@nist.gov --sign <filename> <email> is the key identity chosen when the key pair was created <filename> is the file to be submitted to NIST <Enter the passphrase chosen for the private key> The result shall be emailed to nfiq2@nist.gov

NIST accepts no responsibility for unencrypted materials sent to NIST.