Digital Signature Verification Statement

- **Digital Signatures**

Digital Signatures is an electronic representation of signatory's intent of signature and protects the integrity of data. Just like a traditional hard copy document signing recipient would be able to trust that it comes from the stated signatory.

Signature generation and validation is done using a private key and the corresponding public key. The signatory uses his/her private key and a hash function to generate a hash value that represents the entire data. This hash value is encrypted and sent to the intended recipient.

The recipient would then need to use the corresponding public key to decrypt the hash value. The recipient will run the hash function on the data to derive the hash value and compare it with the received and decrypted hash value. When the value matches it proves the integrity of the data and comes from the signatory. (**FIPS 186-3: Digital Signature Standard, June 2009**)

- **Digital Signature applications**

A digital signature algorithm allows an entity to authenticate the integrity of a signed data and the identity of the signatory. The recipient of a signed message can use a digital signature as evidence in demonstrating to a third party that the signature was, in fact, generated by the claimed signatory. This is known as non-repudiation, since the signatory cannot easily repudiate the signature at a later time. A digital signature algorithm is intended for use in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications that require data integrity assurance and data origin authentication. (**FIPS 186-3: Digital Signature Standard, June 2009**)

Certificate Revocation List (CRL)

A CRL is a time stamped list identifying revoked certificates which is signed by Netrust CA and is available in a public repository. Each revoked certificate is identified in a CRL by its certificate serial number. When a certificate-using system uses a certificate (e.g., for verifying a remote user's digital signature), that system not only checks the certificate signature and validity but also acquires a most recently-issued CRL and checks that the certificate serial number is not on that CRL list. An entry is added to the CRL as part of the next update following notification of revocation. An entry **MUST NOT** be removed from the CRL until it appears on one regularly scheduled CRL issued beyond the revoked certificate's validity period. Hence ONLY expired certificates are removed from the CRL. **(RFC3280: X.509 Public Key Infrastructure Certificate and Certificate Revocation List, page 12)**

- **Digital Signature and Certificate Revocation**

Digital signing can be invalid in the event compromised certificates (resigned or terminated employees) is being used for digital signing, Therefore in practice digital signature verification is also checked against certificate revocation list (CRL). In the event of a certificate compromise, the certificate will be revoked and published in the CRL. The validation will register that the certificate has been revoked prior to the digital signing timestamps and fails to validation. All digital signing done after the certificate is revoked shall fail validation. However existing signatures done before revocation will be able to validate successfully. (**FIPS 186-3.3: Digital Signature Verification and Validation**)

Digital Signature and Certificate Validity

It is important to note that verification of digital signatures also includes checking of signatures timestamps against its certificate validity period. This serves to protect against invalid digital signing done before or after the validity period of non-revoked certificate. Likewise validation of digital signature after its certificate expiry will always return a warning invalid digital signature message "Certificate has expired". However this warning message does not invalidate the authenticity and validity of the digital signature that were valid throughout its certificate validity. This is important for digitally signed documents and data kept for long periods of time beyond its certificate expiry.

Netrust recommends the following practices for digitally signed archived documents.

- Validation of signed documents with expired certificates to omit certificate validity checks and certificate revocation checks.
- Valid signed documents kept longer than its certificate expiry is archived and marked as permanently valid digitally signed documents.