Checklist on Encryption and Other "Information Security" Functions

See Instruction Sheet

1. Does your product perform "cryptography", or otherwise contain any parts or components that are capable of performing any of the following "information security" functions?
(Mark with an "X" all that apply)

a. □ encryption

b. □ decryption only (no encryption)

c. □ key management / public key infrastructure (PKI)

d. □ authentication (e.g., password protection, digital signatures)

e. □ copy protection

f. □ anti-virus protection

g. □ other (please explain) : ________________________________

h. □ NONE / NOT APPLICABLE

2. For items with encryption, decryption and/or key management functions (1.a, 1.b, 1.c above):

a. What symmetric algorithms and key lengths (e.g., 56-bit DES, 112 / 168-bit Triple-DES, 128 / 256-bit AES / Rijndael) are implemented or supported?

b. What asymmetric algorithms and key lengths (e.g., 512-bit RSA / Diffie-Hellman, 1024 / 2048-bit RSA / Diffie-Hellman) are implemented or supported?

c. What encryption protocols (e.g., SSL, SSH, IPSEC or PKCS standards) are implemented or supported?

d. What type of data is encrypted?

3. For products that contain an "encryption component", can this encryption component be easily used by another product, or else accessed / re-transferred by the end-user for cryptographic use?