Commercial Solutions for Classified (CSfC) Selections for Client Virtualization Systems (VS)

Overview

Client Virtualization System (VS) products (i.e., Software Virtualization as defined in the Mobile Access (MA) Capability Package (CP)) used in Commercial Solutions for Classified (CSfC) solutions shall be validated by National Information Assurance Partnership (NIAP)/Common Criteria Evaluation and Validation Scheme (CCEVS) or Common Criteria Recognition Arrangement (CCRA) partnering schemes as complying with the current requirements of NIAP's Protection Profile for Virtualization Version 1.1 (PP_BASE_VIRTUALIZATION_V1.1), Protection Profile-Module for Client Virtualization Version 1.1 (MOD_CV_V1.1), Functional Package for TLS Version 1.1 (PKG_TLS_V1.1), and this validated compliance shall include the selectable requirements contained in this document.

Client VS can be implemented in different ways, threats and technology continuously progress, and Client VS continue to evolve, which may cause the below selections to change or become obsolete. The objectives of the below selections are to provide information to configure VS/Virtual Machine (VM) isolation and integrity, support the use of Commercial National Security Algorithm Suite (CNSA Suite) cryptography, and enable the use of Client VS in CSfC solutions.

Please provide comments on usability, applicability, and/or shortcomings to the CSfC Program (csfc@nsa.gov).

Notes

Note 1: The following selections apply to CSfC Client VS functionality. If needed, functionality and/or configurations outside the scope of a CSfC Client VS that conflict with the CSfC selections could be NIAP validated using a separate iteration of the Security Functional Requirement (SFR). The Security Target (ST) author should document that the iteration of the SFR should not be used to validate compliance with CSfC selections and the configuration is not part of the NIAP-certified evaluated configuration for CSfC Client VS Use Cases.

Note 2: PKG_TLS_V1.1 and the CSfC Selections for TLS are only required as prescribed by PP_BASE_VIRTUALIZATION_V1.1.

Note 3: The below SFRs/Selections contain some mandatory SFRs without Selections or modifications. The exclusion of other mandatory SFRs in the below Selections does not indicate that mandatory PP SFRs are not required (i.e., Compliance with the requirements as prescribed by the PP, Functional Packages, and outlined in the Overview Section above are required). Some mandatory SFRs are included in the below Selections to highlight some SFRs relevant to CSfC Client VS.

Document Conventions

The conventions used in descriptions of the document are as follows:

- Assignment completed within a selection in the PP: the completed assignment text is indicated with *italicized and underlined text* (i.e., CSfC mandatory completed assignments/selections unless otherwise indicated by the text "at least one of the following underlined selections")
- Assignment partially completed in the PP: indicated with *italicized text*
- Refinement text is indicated with ~~strikethroughs~~
- Additional clarifying text or CSfC specific language is indicated with `light blue Courier New Text`
- Links to sources, additional information, and email addresses are indicated with blue underlined text.

Protection Profile for Virtualization Version 1.0 Selections

FCS_CKM.1.1

`If asymmetric keys are generated,` the TSF shall generate asymmetric cryptographic keys in accordance with `at least one of the following` specified cryptographic key generation algorithm [**Selection**:

- *RSA schemes using cryptographic key sizes [2048-bit `and 3072-bits` or greater] that meet the following: [FIPS PUB 186-4, "Digital Signature Standard (DSS)",Appendix B.3] ,*
- *ECC schemes using ["NIST curves" P-256, P-384, and [selection: ~~P-521~~, no other curves] that meet the following: [FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4] ,*
- ~~*FFC schemes using cryptographic key sizes [2048-bit `and 3072-bits` or greater] that meet the following: [FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1]].*~~ ,
- ~~*FFC Schemes using Diffie-Hellman group 14 that meet the following: [RFC 3526]*~~,
- *FFC Schemes using safe primes that meet the following: ['NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes"]*

] ~~and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]~~.

FCS_CKM.2.1

`If cryptographic key establishment takes place,` the TSF shall ~~distribute cryptographic keys~~ perform cryptographic key establishment in accordance with `at least one of the following` specified cryptographic key establishment methods: [**Selection:**

- ~~*RSA-based key establishment schemes that meets the following: RSAESPKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography SpecificationsVersion 2.2"*~~,
- *Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair- Wise Key Establishment Schemes Using Discrete Logarithm Cryptography",*
- *Finite field-based key establishment schemes that meets the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair- Wise Key Establishment Schemes Using Discrete Logarithm Cryptography",*
- ~~*Key establishment scheme using Diffie-Hellman group 14 that meets the following: RFC 3526]*~~

] ~~that meets the following [assignment: list of standards]~~.

FCS_COP.1/Hash

If the TSF performs cryptographic hashing services, the TSF shall perform [*cryptographic hashing*] services in accordance with a specified cryptographic algorithm [**Selection**: ~~*SHA-1*~~, *SHA-256*, *SHA-384*, *SHA-512*, *SHA-3-224*, *SHA-3-256*, *SHA-3-384*, *SHA-3-512*] and message digest sizes [**Selection**: *160, 256, 384, 512 bits*] that meet the following: [**Selection**: FIPS PUB 180-4"Secure Hash Standard", ISO/IEC 10118-3:2018].

FCS_COP.1/Sig

If the TSF performs cryptographic signature services, the TSF shall perform [*cryptographic signature services (generation and verification)*] in accordance with at least one of the following a specified cryptographic algorithm: [**Selection**:

- RSA schemes using cryptographic key sizes *[2048-bit and 3072 bits or greater*] *that meet the following: [FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 4]*,
- *ECDSA schemes using ["NIST curves" P-256, P-384, and [*Selection*: ~~P-521~~, no other curves]] that meet the following: [FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5]*

].

FCS_COP.1/ KeyedHash

If the TSF performs keyed-hash message authentication, the TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [**Selection**: *HMAC-SHA-1*, ~~*HMAC-SHA-256*~~, *HMAC-SHA-384*, *HMAC-SHA-512*, *SHA-3-224*, *SHA-3-256*, *SHA-3-384*, *SHA-3-512*] and cryptographic key sizes [**Assignment**: *key size(s) in bits ≥ the message digest size(s)*] and message digest sizes [**Selection**: *160, 256, 384, 512 bits*] that meet the following: [***FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code," and FIPS Pub 180-4, "Secure Hash Standard"***].

FCS_COP.1/UDE

If the TSF performs encryption and decryption, the TSF shall perform [*encryption and decryption*] in accordance with at least one of the following underlined specified cryptographic algorithms [**Selection:**

- *AES Key Wrap (KW) (as defined in NIST SP 800-38F),*
- *AES Key Wrap with Padding (KWP) (as defined in NIST SP 800-38F),*
- *AES-GCM (as defined in NIST SP 800-38D),*
- *AES-CCM (as defined in NIST SP 800-38C),*
- *AES-XTS (as defined in NIST SP 800-38E) mode,*
- *AES-CCMP-256 (as defined in NIST SP800-38C and IEEE 802.11ac-2013),*
- *AES-GCMP-256 (as defined in NIST SP800-38D and IEEE 802.11ac-2013),*
- *AES-CCMP (as defined in FIPS PUB 197, NIST SP 800-38C and IEEE*
- *802.11-2012),*
- *AES-CBC (as defined in FIPS PUB 197, and NIST SP 800-38A) mode,*
- *AES-CTR (as defined in NIST SP 800-38A) mode*

] and cryptographic key sizes [**Selection**: *128-bit key sizes*, *256-bit key sizes*].

FCS_ENT_EXT.1.1

The TSF shall provide a mechanism to make available to VMs entropy that meets FCS_RBG_EXT.1 through at least one of the following [**Selection:** *Hypercall interface, virtual device interface, passthrough access to hardware entropy source*].

FCS_ENT_EXT.1.2

The TSF shall provide independent entropy across multiple VMs.

FCS_RBG_EXT.1.1
The TSF shall perform all deterministic random bit generation services in accordance with NIST Special Publication 800-90A using `at least one of the following` [**Selection:** *Hash_DRBG (`SHA-384`, `SHA-512`), HMAC_DRBG (`SHA-384`, `SHA-512`), CTR_DRBG (`AES-256`)*].

`Application Note:` `The objective of the CSfC specific language for DRBG algorithms is to ensure compatibility with the CSfC CPs by selecting compliant algorithms that provide the required security strength.`

FCS_RBG_EXT.1.2
The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [**Selection**: *a software-based noise source*, *a hardware-based noise source*] with a minimum of [Selection: ~~*128 bits*~~, ~~*192 bits*~~, *256 bits*] of entropy at least equal to the greatest security strength, according to NIST SP 800-57, of the keys and hashes that it will generate.

FDP_HBI_EXT.1.1
The TSF shall use [~~Selection: no mechanism~~, [**Assignment**: *list of platform-provided, hardware-based mechanisms*]] to constrain a Guest VM's direct access to the following physical devices: [~~Selection: no devices~~, [**Assignment:** *Ethernet ports*, *all wireless devices*, *physical devices to which the VMM allows Guest VMs physical access*]].

FDP_VMS_EXT.1.1
The VS shall provide the following mechanisms for transferring data between Guest VMs: [Selection:

- ~~no mechanism~~,
- *virtual networking*,
- [A**ssignment**: *other inter-VM data sharing mechanisms*]

].

FDP_VMS_EXT.1.2
The TSF shall by default enforce a policy prohibiting sharing of data between Guest VMs.

FDP_VMS_EXT.1.3
The TSF shall allow Administrators to configure the mechanisms selected in FDP_VMS_EXT.1.1 to enable and disable the transfer of data between Guest VMs.

FDP_VMS_EXT.1.4
The VS shall ensure that no Guest VM is able to read or transfer data to or from another Guest VM except through the mechanisms listed in FDP_VMS_EXT.1.1.

FIA_AFL_EXT.1.1
The TSF shall detect when [**Selection**:

- *[Assignment: 10]*
- *an administrator configurable positive integer within a [**Assignment**: range of acceptable values]*

] unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely using a [Selection: *username and password*, *username and PIN*].

FIA_AFL_EXT.1.2
When the defined number of unsuccessful authentication attempts has been met, the TSF shall: [**Selection**: *prevent the offending Administrator from successfully establishing remote session using any authentication method that involves a password or PIN until* [***Assignment****: action to unlock*] *is taken by an Administrator, prevent the offending Administrator from successfully establishing remote session using any authentication method that involves a password or PIN until an Administrator defined time period has elapsed*].

FIA_UIA_EXT.1.1
The TSF shall require Administrators to be successfully identified and authenticated using one of the methods in FIA_UAU.5 before allowing any TSF-mediated management function to be performed by that Administrator.

FMT_SMO_EXT.1.1
The TSF shall support the configuration of separate management and operational networks through `at least one of the following underlined selections` [**Selection**: *separate physical networks, separate logical networks, trusted channels as defined in FTP_ITC_EXT.1, data encryption using an algorithm specified in FCS_COP.1/UDE*].

FPT_EEM_EXT.1.1
The TSF shall take advantage of execution environment-based vulnerability mitigation mechanisms supported by the Platform such as: [Selection:

- *Address space randomization*,
- *Memory execution protection (e.g., DEP)*,
- *Stack buffer overflow protection*,
- *Heap corruption detection*,
- [**Assignment:** *other mechanisms*],
- ~~*No mechanisms*~~].

FPT_RDM_EXT.1.2
The TSF shall enforce the following rules when [Assignment: *virtual or physical removable media and/or virtual or physical removable media devices*] are switched between information domains, then `at least one of the following` [**Selection:**

- *the Administrator has granted explicit access for the media or device to be connected to the receiving domain,*
- ~~*the media in a device that is being transferred is ejected prior to the receiving domain being allowed access to the device*~~,
- ~~*the user of the receiving domain expressly authorizes the connection*~~,
- *the device or media that is being transferred is prevented from being accessed by the receiving domain*

].

FPT_TUD_EXT.1.3
The TSF shall provide means to authenticate firmware/software updates to the TOE using a [**Selection**: *digital signature mechanism using certificates, digital signature mechanism not using certificates, published hash*] prior to installing those updates.

FCS_HTTPS_EXT.1.1
`If TLS as a client is used,` the TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2
If TLS as a client is used, the TSF shall implement HTTPS using TLS.

FIA_X509_EXT.1.1
If the selection for FTP_ITC_EXT.1 includes "IPsec," "TLS," or "TLS/HTTPS" or if FPT_TUD_EXT.1.3 is "digital signature mechanism", the TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation
- The certificate path must terminate with a trusted certificate
- The TOE shall validate a certificate path by ensuring the presence of the basicConstraints extension, that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met.
- The TSF shall validate that any CA certificate includes caSigning purpose in the key usage field
- The TSF shall validate revocation status of the certificate using at least one of the following [**Selection:** *OCSP as specified in RFC6960, a CRL as specified in RFC5759, an ~~OCSP TLS Status Request Extension (OCSP stapling) as specified in RFC 6066~~, ~~OCSP TLS Multi-Certificate Status Request Extension (i.e., OCSP Multi-Stapling) as specified in RFC 6961~~*].
- The TSF shall validate the extendedKeyUsage field according to the following rules::
    - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing Purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
    - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
    - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the EKU field.
    - OCSP certificates presented for OCSP responses shall have the OCSP Signing Purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the EKU field..

FIA_X509_EXT.2.1
If the selection for FTP_ITC_EXT.1 includes "IPsec," "SSH", "TLS," or "TLS/HTTPS" or if FPT_TUD_EXT.1.3 is "digital signature mechanism using certificates", the TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [**Selection:** *IPsec, TLS, HTTPS, SSH, code signing for system software updates,* [***Assignment***: *other uses*]].

FIA_X509_EXT.2.2
When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall do at least one of the following [**Selection:** *allow the administrator to choose whether to accept the certificate in these cases, ~~accept the certificate~~, not accept the certificate*].

FPT_GVI_EXT.1.1
The TSF shall verify the integrity of Guest VMs through the following mechanisms: [**Assignment:** *integrity check via a Virtual Trusted Platform Module (vTPM), list of Guest VM integrity mechanisms*].

FPT_DDI_EXT.1.1
If the TOE has wireless devices and the wireless devices aren't disabled at the lowest level possible (e.g., hardware connection removed, disabled at a level below the hypervisor), the TSF shall ensure that device drivers for physical devices are isolated from the VMM and all other domains.

FPT_ML_EXT.1.1
The TSF shall support a measured launch of the Virtualization System. Measured components of the Virtualization system shall include the static executable image of the Hypervisor and: [**Selection**:

- *Static executable images of the Management Subsystem*,
- [***Assignment**: list of (static images of) Service VMs*],
- [***Assignment**: list of configuration files*]]
- *no other components*

].

FPT_ML_EXT.1.2
The TSF shall make the measurements selected in FPT_ML_EXT.1.1 available to the Management Subsystem.

Functional Package for TLS Version 1.1 Selections

FCS_TLS_EXT.1.1
If TLS as a client is used, the product shall implement [Selection:

- *TLS as a client*
- ~~*TLS as a server*~~,
- ~~*DTLS as a client*~~,
- ~~*DTLS as a server*~~

].

FCS_TLSC_EXT.1.1

If TLS as a client is used, the product shall implement TLS 1.2 (RFC 5246) and [Selection: ~~*TLS 1.1 (RFC 4346)*~~, *no earlier TLS versions*] as a client that supports at least one of the following cipher suites [**Selection:**

- ~~*TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246,*~~
- ~~*TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,*~~
- ~~*TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246,*~~
- ~~*TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,*~~
- ~~*TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,*~~
- ~~*TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246,*~~
- *TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,*
- ~~*TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,*~~
- ~~*TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,*~~
- ~~*TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*~~,
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,*
- ~~*TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,*~~
- ~~*TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,*~~
- ~~*TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*~~,
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*

] and also supports functionality for [Selection:

- *mutual authentication*
- ~~*session renegotiation,*~~
- ~~*none*~~

].

FCS_TLSC_EXT.1.2

If TLS as a client is used, the product shall verify that the presented identifier matches the reference identifier according to RFC 6125.

FCS_TLSC_EXT.1.3

If TLS as a client is used, the product shall not establish a trusted channel if the server certificate is invalid [**Selection:**

- *with no exceptions* or
- *except when override is authorized*

].

FCS_TLSC_EXT.2.1

If TLS as a client is used, the product shall support mutual authentication using X.509v3 certificates.

FCS_TLSC_EXT.3.1

If TLS as a client is used, the product shall present the signature_algorithms extension in the Client Hello with the supported_signature_algorithms value containing the following hash algorithms: [**Selection**: ~~*SHA256*~~, *SHA384*, *SHA512*] and no other hash algorithms.

FCS_TLSC_EXT.5.1

If TLS as a client is used, the product shall present the Supported Groups Extension in the Client Hello with at least one of the following underlined supported groups [**Selection:**

- ~~*secp256r1*~~,
- *secp384r1*,
- ~~*secp521r1*~~,
- ~~*ffdhe2048(256)*~~,
- *ffdhe3072(257)*,
- *ffdhe4096(258)*,
- ~~*ffdhe6144(259)*~~,
- ~~*ffdhe8192(260)*~~

].