Mapping Between
Functional Package for Secure Shell (SSH), Version 1.0, 13 May 2021
and
NIST SP 800-53 Revision 5

Important Caveats

- **Product vs. System.** The Common Criteria is designed for the evaluation of products; the Risk Management Framework (NIST SP 800-37 Revision 2, DOD 8510.01) and associated control/control interpretations (NIST SP 800-53 Revision 5, CNSSI № 1253) are used for the assessment and authorization of mission systems. **Products cannot satisfy controls outside of the system context**. Products may support a system satisfying particular controls, but typically satisfaction also requires the implementation of operational procedures; further, given that systems are typically the product of integration of multiple products configured to meet mission requirements, an overall system assessment is required to determine if the control is satisfied in the overall system context.
- **Granularity of SFRs vs controls.** It is important to remember that the Security Functional Requirements (SFRs) and the Security and Privacy Controls (Controls) are at completely different levels of abstractions. SFRs can be very low level, specifying internal characteristics and behaviors of given functions. Even when broader, SFRs are restricted to a specific product. Controls, on the other hand, are very high level, specifying both technical behavior and processes for the system writ large, broadly across the large number of devices, components and products that make up the system and achieve the overall mission. A low-level SFR may contribute in some small way towards the satisfaction of a control, but it rarely satisfies the control in isolation and should not be interpreted as doing so. More often, the combination of SFRs that define the security functionality of a product may serve to support just a single control, and looking at the finer level of detail may not be as useful, such as the low-level details of protocol implementations. When looking at these mappings, it is important to remember the differences in levels of abstraction; in particular, it is important not to read more into an SFR to Control mapping than a contribution of some level of support.
- **SA-4(7).** Perhaps it is needless to say, but satisfaction of any NIAP PP supports system satisfaction of SA-4(7), which is the implementation of CNSSP № 11.
- **SC-8.** The primary purpose of this functional package is to define SSH protocol requirements to ensure a proper and sufficiently secure baseline implementation of the protocol, generally in support of a trusted channel to a trusted external IT entity or trusted path to a remote user or administrator. Conformance to this package is therefore intended to satisfy SC-8 and SC-8(1) at a high level.
- **System context of supported controls.** For a conformant TOE to support these controls in the context of an information system, the selections and assignments completed in the TOE’s Security Target must be congruent with those made for the supported controls. For example, the TOE’s ability to generate audit records only supports AU-2 to the extent that the TOE’s audit records are included in the set of “organization-defined auditable events” assigned by that control. The security control assessor must compare the TOE’s functional claims to the behavior

required for the system to determine the extent to which the applicable controls are supported.

- **Functional Package.** This is a functional package, which is a specification of functional requirements that can be referenced by a Protection Profile and is not intended to be a complete specification for a security product or capability on its own. A TOE that conforms to this functional package must also conform to a Protection Profile that references this package as well. The security control mapping for that Protection Profile (and any PP-Modules that the TOE also claims) must also be considered to determine the extent to which a conformant TOE supports the implementation of organizational security controls.
- **Granularity of SFRs vs controls.** It is important to remember that the Security Functional Requirements (SFRs) and the Security and Privacy Controls (Controls) are at completely different levels of abstractions. SFRs can be very low level, specifying internal characteristics and behaviors of given functions. Even when broader, SFRs are restricted to a specific product. Controls, on the other hand, are very high level, specifying both technical behavior and processes for the system writ large, broadly across the large number of devices, components and products that make up the system and achieve the overall mission. A low-level SFR may contribute in some small way towards the satisfaction of a control, but it rarely satisfies the control in isolation and should not be interpreted as doing so. More often, the combination of SFRs that define the security functionality of a product may serve to support just a single control, and looking at the finer level of detail may not be as useful, such as the low-level details of protocol implementations. When looking at these mappings, it is important to remember the differences in levels of abstraction; in particular, it is important not to read more into an SFR to Control mapping than a contribution of some level of support.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
Mandatory Requirements (presented alphabetically)				
FCS_SSH_EXT.1	**SSH Protocol**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE uses SSH as a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
Optional Requirements (presented alphabetically)				
This package has no optional requirements.				
Objective Requirements (presented alphabetically)				
This package has no objective requirements.				
Implementation-Based Requirements (presented alphabetically)				
This package has no implementation-based requirements.				
Selection-Based Requirements (presented alphabetically)				
FCS_SSHC_EXT.1	**SSH Protocol - Client**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE uses SSH as a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
FCS_SSHS_EXT.1	**SSH Protocol - Server**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE uses SSH as a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.