NIST Special Publication 800-135

Recommendation for Existing Application-Specific Key Derivation Functions

Quynh Dang

Computer Security Division
Information Technology Laboratory

C O M P U T E R S E C U R I T Y

December 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick Gallagher, Director

Abstract

Cryptographic keys are vital to the security of internet security applications and protocols. Many widely-used internet security protocols have their own application-specific Key Derivation Functions (KDFs) that are used to generate the cryptographic keys required for their cryptographic functions. This Recommendation provides security requirements for those KDFs.

KEY WORDS: Cryptographic key, shared secret, Diffie-Hellman (DH) key exchange, hash function, Key Derivation Function (KDF), Hash-based Key Derivation Function, Randomness Extraction, Key expansion, Pseudorandom Function (PRF), HMAC, ANS X9.42-2001, ANS X9.63-2001, IKE, SSH, TLS, SRTP, SNMP and TPM.

Acknowledgements

The author gratefully appreciates the comments and contributions of the many reviewers in various Federal agencies and the public. In particular, the author would like to thank Elaine Barker, William E. Burr, Lily Chen, Tim Polk and Hugo Krawczyk.

Table of Contents

1 Introduction 2

2 Authority 2

3 Glossary of Terms, Acronyms and Mathematical Symbols 3

3.1 Terms and Definitions 3

3.2 Acronyms 4

3.3 Symbols & Mathematical Operations 5

4 Extraction-then-Expansion (E-E) Key Derivation Procedure 6

4.1 Internet Key Exchange (IKE) 7

4.1.1 IKE version 1 (IKEv1) 8

4.1.2 IKE version 2 (IKEv2) 10

4.2 Key Derivation in Transport Layer Security (TLS) 10

4.2.1 Key Derivation in TLS versions 1.0 and 1.1 10

4.2.2 Key Derivation in TLS version 1.2 11

5 Other Existing Key Derivation Functions 12

5.1 Key Derivation Functions in American National Standards (ANS) X9.42-2001 and ANS X9.63-2001 12

5.2 Secure Shell (SSH) Key Derivation Function 13

5.3 The Secure Real-time Transport Protocol (SRTP) Key Derivation Function 15

5.4 Simple Network Management Protocol (SNMP) Key Derivation Function/Key Localization Function 16

5.5 Trusted Platform Module (TPM) Key Derivation Function 17

6 References 18

Recommendation for Application-Specific Key Derivation Functions

1 Introduction

This document specifies security requirements for existing application-specific key derivation functions in:

- American National Standard (ANS) X9.42-2001-Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography (ANS X9.42-2001) [ANS X9.42] (also in RFC 2631 [RFC 2631]),
- American National Standard (ANS) X9.63-2001-Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography (ANS X9.63-2001) [ANS X9.63] (also in RFC 3278 [RFC 3278]),
- Internet Key Exchange (IKE) (version 1: RFC 2409 [RFC 2409] and version 2: RFC 4306 [RFC 4306]),
- Secure Shell (SSH): RFC 4251 [RFC 4251],
- Transport Layer Security (TLS) version 1.0: RFC 2246 [RFC 2246], version 1.1: RFC 4346 [RFC 4346] and version 1.2: RFC 5246 [RFC 5246].
- The Secure Real-time Transport Protocol (SRTP): RFC 3711 [RFC 3711],
- User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMP): RFC 2574 [RFC 2574], and
- Trusted Platform Module (TPM) (Parts 1 [TPM Principles], 2 [TPM Structures] and 3 [TPM Commands]).

2 Authority

This publication has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems.

This Recommendation has been prepared for use by federal agencies. It may be used by non-governmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

Conformance testing for implementations of this Recommendation will be conducted within the framework of the Cryptographic Module Validation Program (CMVP) and the Cryptographic Algorithm Validation Program (CAVP). The requirements of this Recommendation are indicated by the word "**shall**." Some of these requirements may be out-of-scope for CMVP or CAVP validation testing, and thus are the responsibility of entities using, implementing, installing or configuring applications that incorporate this Recommendation.

3 Glossary of Terms, Acronyms and Mathematical Symbols

3.1 Terms and Definitions

Algorithm	A clearly specified mathematical process for computation; a set of rules that, if followed, will give a prescribed result.
Approved	FIPS-**approved** and/or NIST-**recommended**. An algorithm or technique that is either 1) specified in a FIPS or NIST Recommendation, 2) adopted in a FIPS or NIST Recommendation or 3) specified in a list of NIST-**approved** security functions.
Approved hash algorithms	Cryptographic hash algorithms specified in FIPS 180-3 [FIPS 180-3].
Block cipher	A family of functions and their inverse functions that is parameterized by cryptographic keys; the functions map bit strings of a fixed length to bit strings of the same length.
Cryptographic key (key)	A parameter used in conjunction with a cryptographic algorithm that determines the algorithm's operation in such a way that an entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot. Examples include: 1. The transformation of plaintext data into ciphertext data, 2. The transformation of ciphertext data into plaintext data,

	3. The computation of a digital signature from data, 4. The verification of a digital signature, 5. The computation of an authentication code from data, 6. The verification of an authentication code from data and a received authentication code.
Key agreement primitive	A DLC primitive specified in SP 800-56A [SP 800-56A] or an RSA Secret Value Encapsulation (RSASVE) operation specified in SP 800-56B [SP 800-56B].
Key derivation key	A key that is used as an input to a key derivation function or key expansion function to derive other keys.
Nonce	A time-varying value that has at most a negligible chance of repeating; for example, a random value that is generated anew for each use, a time-stamp, a sequence number, or some combination of these. It can be a secret or non-secret value.
Pre-shared key	A secret key that is established between communicating parties before a communication protocol starts.
Pseudorandom function (PRF)	A function that can be used to generate output from a random seed and a data variable, such that the output is computationally indistinguishable from truly random output.
Pseudorandom key	As used in this Recommendation, a binary string that is taken from the output of a PRF.
Secret keying material	The binary data that is used to form secret keys, such as AES encryption keys or HMAC keys.
Shall	This term is used to indicate a requirement that needs to be fulfilled to claim conformance to this Recommendation. Note that **shall** may be coupled with **not** to become **shall not.**
Shared secret	A secret value that has been computed using a key agreement algorithm.
Should	This term is used to indicate an important recommendation. Ignoring the recommendation could result in undesirable results. Note that **should** may be coupled with **not** to become **should not**.

3.2 Acronyms

ANS	American National Standard
CMAC	Block Cipher-based Message Authentication Code
DLC	Discrete Logarithm Cryptography

E-E	Extraction-then-Expansion
FIPS	Federal Information Processing Standard
HKDF	Hash-based Key Derivation Function
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IKEv1	IKE version 1
IKEv2	IKE version 2
KDF	Key Derivation Function
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
PRF	Pseudorandom Function
RFC	Request for Comments
SA	Security Association
SHA	Secure Hash Algorithm
SSH	Secure Shell
SP	Special Publication
TLS	Transport Layer Security
TPM	Trusted Platform Module

3.3 Symbols & Mathematical Operations

AES(k, input) A single AES encryption operation as specified in FIPS 197 [FIPS 197] with *k* and *input* being the AES encryption key and one 128-bit block of plaintext/data, respectively.

g^{xy} Diffie-Hellman (DH) key exchange value, also called a DH shared secret (in IKE version 1).

g^{ir} DH key exchange value, also called a DH shared secret (in IKE version 2).

|| Concatenation operation; for example, *a* || *b* means that string *b* is appended after string *a*.

0x0X 8-bit binary representation of the hexadecimal number *X*, for example, 0x02 = 00000010.

HASH	A cryptographic hash function, such as SHA-1.
HMAC-HASH	The HMAC algorithm using the hash function, HASH (e.g., HASH could be SHA-1). See FIPS 198-1 for the specification of the HMAC algorithm using one of the **approved** hash functions.
HMAC-PRF	The HMAC function being used as a PRF.
P_HASH	A function that uses the HMAC-HASH as the core function in its construction. The specification of this function is in RFCs 2246 and 5246.
$\lceil x \rceil$	The ceiling of x; the smallest integer $\geq x$. For example, $\lceil 5 \rceil = 5$ and $\lceil 5.2 \rceil = 6$.
$\lfloor x \rfloor$	The floor of x; the largest integer $\leq x$. For example, $\lfloor 5 \rfloor = 5$ and $\lfloor 6.9 \rfloor = 6$.
$\|x\|$	The length of the string x in bits.
$\oplus$	A bitwise logical operation such that $1 \oplus 1 = 0$, $1 \oplus 0 = 1$, $0 \oplus 0 = 0$, and $0 \oplus 1 = 1$. For example, given a string $A = 10$ and a string $B = 11$, then $A \oplus B = (1 \oplus 1) \| (0 \oplus 1) = 01$.
XOR	A *XOR* B is equivalent to A $\oplus$ *B*. See the definition of the bitwise logical operation $\oplus$ above.
Pre-shared-key	A secret key that has previously been established. See "pre-shared key" in Section 3.1 above.
SKEY	A session key in TPM.

4 Extraction-then-Expansion (E-E) Key Derivation Procedure

NIST has specified several key derivation functions (KDFs) in SP 800-56A, SP 800-56B and SP 800-108 [SP 800-108]. SP 800-56C [SP 800-56C] specifies an additional KDF that is an extraction-then-expansion (E-E) procedure, which has a different structure from the KDFs in SP 800-56A, SP 800-56B and SP 800-108. The procedure consists of two separate steps: a randomness extraction step and a key expansion step. The general specification of the E-E procedure is in SP 800-56C, which provides an additional method for deriving keys when performing a key establishment scheme as specified in SP 800-56A and SP 800-56B . Figure 1 below shows the relationship of the E-E procedure in SP 800-56C with the **approved** KDFs in SP 800-108. In Figure 1, the randomness extraction step outputs a key derivation key, which is then used as

input to the key expansion step. Any **approved** KDFs in SP 800-108 can be used as the key expansion step that derives keying material and can also be used to derive more keying material from the key expansion step's derived key(s)/keying material. The following sections discuss protocols that use the E-E procedure. Note that even though the KDFs in these protocols use the E-E procedure for key derivation, their specific randomness extraction and/or key expansion step(s) do not meet all specification of SP 800-56C. These KDFs are only **approved** for use within the limitations described in the corresponding sections later in this document.

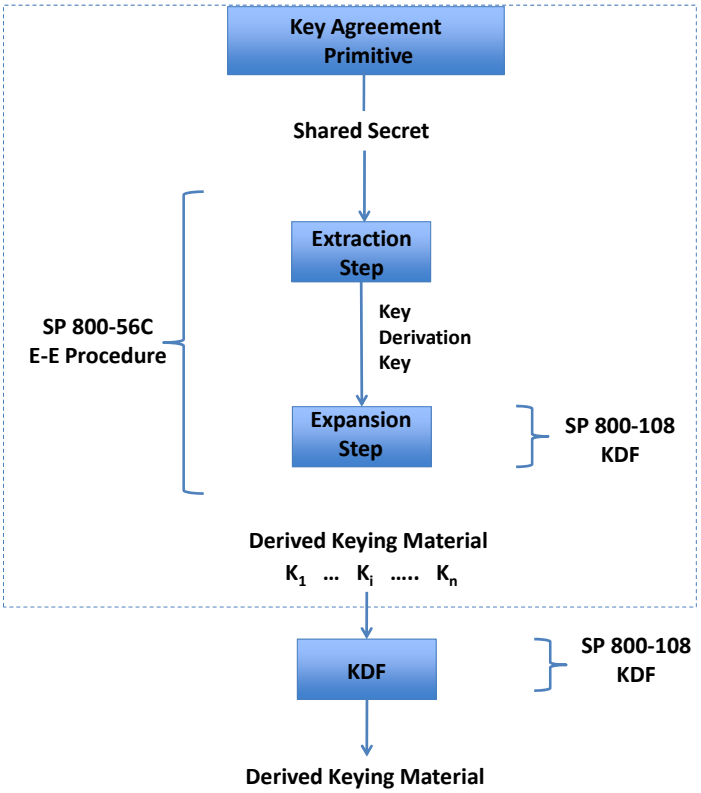


Figure 1: Key Derivation

4.1 Internet Key Exchange (IKE)

Versions 1 and 2 of the Internet Key Exchange (IKE) are specified in RFC 2409 and RFC 4306, respectively, and use HMAC-based Pseudorandom Functions (PRFs) in

their KDFs to generate keying material for their security associations (SAs). IKEv1[1] and IKEv2 specify multiple PRFs, including those based on HMAC and block ciphers. Only an **approved** hash function and HMAC function **shall** be used.

4.1.1 IKE version 1 (IKEv1)

In IKEv1, a string called *SKEYID* is derived from secret material known only to the communicating parties. An HMAC-PRF is used to produce the *SKEYID*. The secret material that is input to the HMAC function is either a Diffie-Hellman shared secret g^{xy}, secret nonces generated by both of the communicating parties, or a pre-shared key. In the protocol, the method used to generate *SKEYID* depends on the authentication method. One of the following three different functions is used as a randomness extraction step to produce the *SKEYID*:

1) When digital signatures are used for authentication, the function is:

   SKEYID = HMAC ($Ni_b \| Nr_b$, g^{xy}), where *Ni_b* and *Nr_b* are non-secret values.

2) When a public key algorithm encryption is used for authentication, the function is:

   SKEYID = HMAC (HASH ($Ni_b \| Nr_b$), CKY-I || CKY-R), where *Ni_b* and *Nr_b* are secret nonces, and CKY-I and CKY-R are non-secret values.

3) When a pre-shared key is used for authentication, the function is:

   SKEYID = HMAC (*pre-shared-key*, $Ni_b \| Nr_b$), where *Ni_b* and *Nr_b* are non-secret values.

Additional technical details for the variables in the functions are provided in RFC 2409.

The appropriate PRF (i.e., the HMAC functions 1-3 above) is executed only once to generate the *SKEYID*.

After the randomness extraction step above, the *SKEYID* is fed into a feedback function that performs the key expansion step and produces the necessary keying material. The resulting keying material is defined by the following equations:

$SKEYID_d = HMAC(SKEYID, g^{xy} \| CKY\text{-}I \| CKY\text{-}R \| 0)$

(*SKEYID_d* is used as the key derivation key to generate fresh keying material for new, negotiated security associations.)

$SKEYID_a = HMAC(SKEYID, SKEYID_d \| g^{xy} \| CKY\text{-}I \| CKY\text{-}R \| 1)$

(*SKEYID_a* is used as an HMAC key to authenticate the current security association's messages.)

$SKEYID_e = HMAC(SKEYID, SKEYID_a \| g^{xy} \| CKY\text{-}I \| CKY\text{-}R \| 2)$

[1] Note that IKEv1 is considered obsolete by the IETF and not recommended for new protocols.

(*SKEYID_e* is used as a key derivation key to derive a symmetric encryption key to provide confidentiality for the current SA's messages. More details about this function can be found in Appendix B of RFC 2409.)

CKY-I and *CKY-R* are non-secret values. The technical details of these variables are provided in RFC 2409. Figure 2 below shows the feedback function that produces the *SKEYID_d, SKEYID_a* and *SKEYID_e* above. This function conforms to the specification of the key expansion step in SP 800-56C.

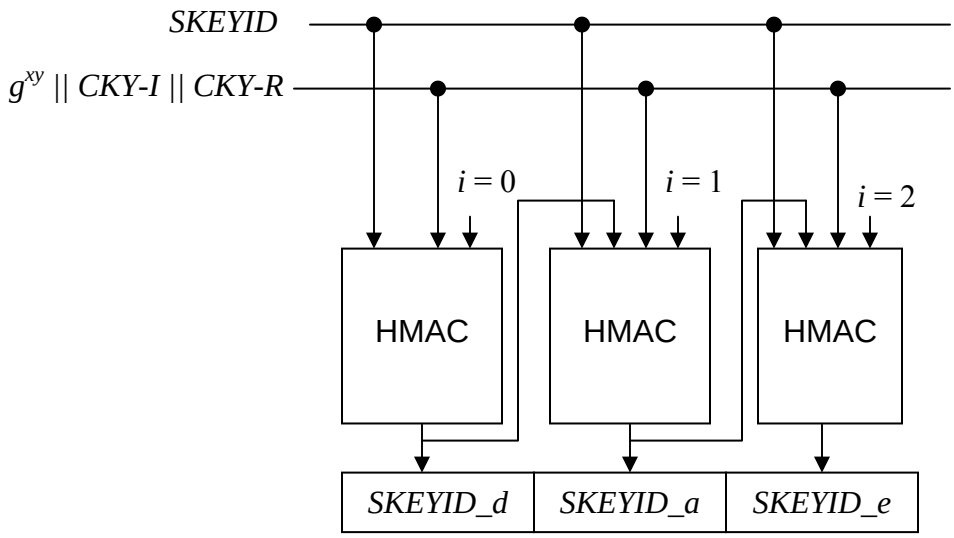


Figure 2: Key expansion Step in IKEv1

Note that both *SKEYID* and the Diffie-Hellman shared secret g^{xy} are secret values and are used as inputs to the HMAC in the key expansion step. Also note that all three resulting keys (i.e., *SKEYID_d*, *SKEYID_a* and *SKEYID_e*) are pseudorandom keys.

The IKEv1[2] KDFs are **approved** when the following conditions are satisfied:

(1) The IKEv1 KDFs are performed in the context of the IKEv1 protocol.

(2) The PRF is an HMAC-based PRF.

(3) The HMAC and HASH are NIST-**approved** algorithms and are used as specified in FIPSs 198-1 [FIPS 198-1] and 180-3, respectively.

[2] Note that when the function (randomness extraction step) used to produce the *SKEYID* is *SKEYID* = HMAC (*Ni_b* || *Nr_b*, g^{xy}) as described earlier in this section, the IKEv1 KDF is compliant with the current specification of SP 800-56C.

4.1.2 IKE version 2 (IKEv2)

In IKEv2, an HMAC is used as a randomness extraction step to extract randomness from a Diffie-Hellman shared secret (g^{ir}) and to uniformly distribute the randomness across the output (*SKEYSEED*). The function to produce *SKEYSEED* is:

$$SKEYSEED = \text{HMAC}\ (Ni \parallel Nr,\ g^{ir}).$$

Ni and *Nr* are nonces generated by the protocol initiator and responder, respectively; see RFC 4306 for more details. This function acts as the randomness extraction step of the E-E KDF. After the *SKEYSEED* is generated, a key expansion step is used to derive keys for the security association (SA). *SKEYSEED* is the key derivation key for the key expansion step. The string of concatenated non-secret attributes: *Ni* || *Nr* || *SPIi* || *SPIr*[3] is the fixed input message *P* field in SP 800-56C. Information about these non-secret attributes can be found in RFC 4306. The specification of the key expansion step can be found in Sections 2.13 and 2.14 of the RFC. Note that as shown in Figure 1, the keying material generated by this key expansion step is the output of the E-E procedure.

One of the seven secret keys derived from the *SKEYSEED* is called *SK_d***.** It is used as the key derivation key to derive new keys for child SA(s) using another KDF that is functionally the same as the key expansion step, but with a different set of attributes.

One of the attributes is an optional new Diffie-Hellman shared secret established during the creation of the child SA. Details of this function can be found in Sections 2.17 and 2.18 of RFC 4306.

The IKEv2 KDFs, which are compliant with SP 800-56C, are **approved** when used with an **approved** HMAC function using an **approved** hash function; see FIPSs 198-1 and 180-3, respectively**.** These KDFs are included here for completeness.

4.2 Key Derivation in Transport Layer Security (TLS)

In TLS, after a cipher suite negotiation is completed, a Diffie-Hellman (DH) key agreement or RSA key transport scheme is used to generate a pre-master secret. When RSA key transport is used, the pre-master secret is a random value generated by the client. When the DH key agreement scheme is used, the pre-master secret is the shared secret generated by the key agreement scheme.

4.2.1 Key Derivation in TLS versions 1.0 and 1.1

In TLS versions 1.0 and 1.1 (TLS 1.0 and 1.1), the pre-master secret is input into an HMAC-MD5/HMAC-SHA-1 PRF[4] with some non-secret values to produce a master secret; the PRF acts as the randomness extraction step in an E-E KDF. The master

---

[3] *Ni* and *Nr* are nonces created by the initiator and responder, respectively. *SPIi* and *SPIr* are security parameter indexes (SPIs) of the initiator and responder respectively.

[4] The HMAC-MD5/HMAC-SHA-1 PRF uses HMAC-MD5 and HMAC-SHA-1 as the core functions in its construction, as specified in RFC 2246, Section 5.

secret is then input into the HMAC-MD5/HMAC-SHA1 PRF with other non-secret values to derive keying material for the negotiated cryptographic functions; in this case, the PRF acts as the key expansion step in the E-E KDF.

The HMAC-MD5/HMAC-SHA1 PRF contains two functions: P_MD5 and P_SHA1, which use MD5-HMAC and SHA-1-HMAC as the core functions, respectively. The specifications of P_MD5 and P_SHA-1 are in Section 5 of RFC 2246 (the function called P_hash in the RFC). The P_HASH function (P_MD5 or P_SHA-1) uses the double-pipeline iteration mode and HMAC-PRF specified in SP 800-108.

The outputs from both P_MD5 and P_SHA-1 are *XOR*ed together to produce the PRF output. This PRF is used as both a randomness extraction step to generate the master secret and as a key expansion step to derive keying material for the protocol from the master secret.

The TLS 1.0 and 1.1 KDF is **approved** when the following conditions are satisfied:

(1) The TLS 1.0 and 1.1 KDF is performed in the context of the TLS protocol.

(2) SHA-1 and HMAC are as specified in FIPSs 180-3 and 198-1, respectively.

Note that MD5 and HMAC-MD5 **shall not** be used as a general hash function or HMAC function, respectively.

4.2.2 Key Derivation in TLS version 1.2

In TLS version 1.2 (TLS 1.2), the pre-master secret is input into an HMAC-SHA-256 PRF[5] with some non-secret values to produce a master secret; the PRF acts as the randomness extraction step in an E-E KDF. The master secret is then input into the HMAC-SHA-256 PRF with some other non-secret values to derive keying material for the negotiated cryptographic functions; in this case, the PRF acts as the key expansion step in the E-E KDF.

The HMAC-SHA-256 PRF is P_SHA256. This PRF is used instead of the PRF in TLS 1.0 and 1.1 which is (P_MD5 ⊕ P_SHA-1).

In TLS 1.2, in addition to P_SHA256, any P_HASH with a stronger hash function, such as SHA-384 or SHA-512 (in FIPS 180-3), can be used as the PRF.

The TLS 1.2 KDF is an **approved** KDF when the following conditions are satisfied:

(1) The TLS 1.2 KDF is performed in the context of the TLS protocol.

(2) HMAC is as specified in FIPS 198-1.

(3) P_HASH uses either SHA-256, SHA-384 or SHA-512.

[5] The HMAC-SHA-256 PRF uses HMAC-SHA-256 as the core function in its construction, as specified in RFC 5246, Section 5.

5 Other Existing Key Derivation Functions

In this section, several application-specific KDFs that are not specified in SP 800-56A, SP 800-56B, SP 800-56C or SP 800-108, are considered. They do not follow the extraction-then-expansion procedure in SP 800-56C or may not meet all the specification requirements in either SP 800-56A, SP 800-56B or SP 800-108. The following figure illustrates the application of these KDFs.

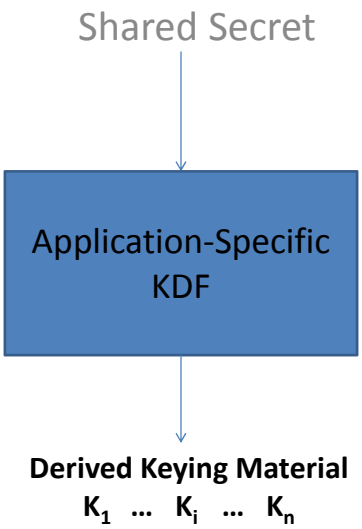


Figure 3: Application-Specific KDF.

5.1 Key Derivation Functions in American National Standards (ANS) X9.42-2001 and ANS X9.63-2001

There are two hash-based KDFs specified in ANS X9.42-2001 and one hash-based KDF specified in ANS X9.63-2001. These hash-based KDF specifications are similar to (but not the same as) the specifications of the hash-based KDFs specified in SPs 800-56A and B. A shared secret that is generated during a key agreement scheme and other non-secret values are used as input to the hash-based KDF to produce the derived keying material for the application. A counter value is pre-pended to the shared secret in the input to the hash-based KDFs in SPs 800-56A and B, but it is appended to the shared secret in the input to the hash-based KDFs in ANS X9.42-2001 and ANS X9.63-2001. Also, the identifiers of the communicating parties are required in the input to the hash-based KDFs in SPs 800-56A and B, but optional in ASN X9.42-2001 and ASN X9.63-2001.

The hash-based KDFs in ANS X9.42-2001 and ANS X9.63-2001 are **approved** when the following conditions are satisfied:

(1) Each of the hash-based KDFs is performed in the context of an ANS X9.42-2001 or ANS X9.63-2001 key agreement scheme.

(2) The hash function is one of the hash functions specified in FIPS 180-3.

(3) The hash function deployed in the hash-based KDF meets the security strength(s) required by the cryptographic function(s) for which the keying material is being generated. The security strengths of **approved** hash functions used in KDFs can be found in SP 800-57 [SP 800-57].

Note that any KDF that meets the specification of either the ANS X9.42-2001 or ANS X9.63-2001 hash-based KDF and is used in a scheme specified in one of these two Standards is **approved** when conditions (2) and (3) above are met. For example, the KDF specified in Section 2.1.2 (Generation of Keying Material) of RFC 2631 and the KDF (specified in [SEC1]) used in RFC 3278 are **approved**.

5.2 Secure Shell (SSH) Key Derivation Function

SSH is a protocol used between clients and servers for secure remote login and other secure network services over an insecure network or the Internet. The Internet Engineering Task Force (IETF) governs the SSH protocol (see RFC 4251). The SSH protocol consists of three major components: the Transport Layer Protocol (RFC 4253 [RFC 4253]), the User Authentication Protocol (RFC 4252 [RFC 4252]) and the Connection Protocol (RFC 4254 [RFC 4254]). The Transport Layer Protocol provides server authentication, confidentiality, and integrity.

Output from a key exchange[6] (see Section 7.2 of RFC 4253) in the Transport Layer Protocol is a shared secret, "*K*", and a hash value, "*H*". In the protocol, *K*, *H* and a specific set of other non-secret values are input to a hash function-based KDF to derive keying material. Different KDFs produce keying material for different cryptographic functions; however, the KDFs are similar (see below). The specifications for the KDFs in the Transport Layer Protocol can be found in Section 7.2 of RFC 4253.

The following is a description of the KDF used to derive a key, where *HASH* denotes a hash function, such as SHA-1 as specified in FIPS 180-3. The key to be derived is denoted by *KEY***,** and the length of *KEY* is denoted by *L*. The length of the hash function output is denoted by *HASH_Length*.

$$N = \lceil (L / Hash_Length) \rceil$$

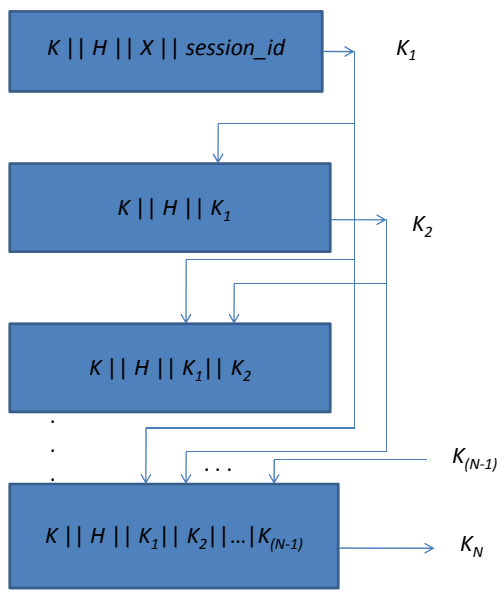
X is a character, such as A, B, C, D, E or F, depending on the type of key desired.

[6] The key exchange method specified for the protocol is one of the key agreement primitives described in SP 800-56A.

K_1 = HASH (K || H || X || *session_id*), where *session_id*[7] is a unique identifier for a SSH connection.
K_2 = HASH (K || H || K_1)
K_3 = HASH (K || H || K_1 || K_2)
……
K_N = HASH (K || H || K_1 || K_2 ||…|| $K_{(N-1)}$)

KEY = the L left most bits of (K_1 || K_2 ||…. K_N)

Figure **4** below shows the accumulative and feedback operation of the KDF.



KEY = L left most bits of (K_1 || K_2 ||…$K_{(N-1)}$|| K_N)

Figure 4: SSH KDF

Each box in Figure 4 represents a hash function computation. The variables in the box are input to the hash function. The arrow (→) indicates an output from the hash function.

---

[7] *session_id* is actually *H* from the first key exchange and remains unchanged for the whole connection. However, *K* and *H* will be changed when a key re-exchange is performed, see Section 9 of RFC 4253.

The SSH KDFs are **approved** when the following conditions are satisfied:

(1) They are performed in the context of the SSH protocol.

(2) The hash function is one of the hash functions specified in FIPS 180-3.

(3) The hash function deployed in the KDFs meets the security strength(s) required by the cryptographic function(s) for which the keying material is being generated. The security strengths of **approved** hash functions used in KDFs can be found in SP 800-57.

5.3 The Secure Real-time Transport Protocol (SRTP) Key Derivation Function

The SRTP is specified in RFC 3711. The protocol is intended to provide confidentiality, message authentication, and replay protection to the Real-time Transport Protocol (RTP) traffic and to the control traffic for RTP: the Real-time Transport Control Protocol (RTCP) (RFC 3550 [RFC 3550]). Session encryption keys (for a confidentiality service), cipher/encryption salts and authentication keys (for message authentication) in the SRTP are derived from a single master key, called *k_master*, using a KDF. Note that *k_master* is used as a key derivation key when input to the KDF. Details of the KDF can be found in Sections 4.3, 5.3 and 7.1 of RFC 3711.

Denote the cryptographic key (encryption key, cipher salt or authentication key (HMAC key), etc…) to be derived as K. The length of K is denoted by L. Below is a description of the KDF.

master_salt: a random non-secret value.

kdr: the key derivation rate. *kdr* is a number from the set $\{0, 1, 2^1, 2^2, 2^3 \ldots, 2^{24}\}$, represented as a 48-bit value.

index: an integer. See RFC 3711 for technical details about "*index*".

A function, *DIV*, is defined as followed:

a and x are non-negative integers.

$a \; DIV \; x = \lfloor a/x \rfloor$ when $x > 0$, or 0 when $x = 0$. ($a \; DIV \; x$) is represented by a 48-bit value in this KDF.

label: an 8-bit value represented by two hexadecimal numbers from the set of {0x01, 0x02, 0x03, 0x04, 0x05, 0x06}. In the future, this set might also include any or all of the values 0x06, 0x07,…,0xff.

$$key_id = label \,||\, (index \;\; DIV \; kdr)$$

$$input = (key_id \oplus master_salt) \| 0x0000,$$

where *key_id* and *master_salt* are right-aligned. One or more zeros is/are pre-pended to the shorter of the two strings before the (*key_id* ⊕ *master_salt*) operation is performed. After *key_id* and *master_salt* are *XOR*ed together, the result is then appended with 16 zero bits to form the *input*, a 128-bit value.

The *input* is used as input to AES-128 to produce a session encryption key, cipher salt or authentication key, with *k_master* being the encryption key. Note that AES-192 and AES-256 may also be used in the KDF. When AES-192 or AES-256 is used, the *k_master* is 192 or 256 bits, respectively. Specific specifications for the KDF when using either AES-192 or AES-256 are under development; see http://tools.ietf.org/html/draft-ietf-avt-srtp-big-aes-04.

$m = \lceil L/128 \rceil$ (*128* is the bit length of the AES output, and $m \geq 1$)

$Derived_keying_1 = \mathrm{AES}(k_master, input)$

$Derived_keying_2 = \mathrm{AES}(k_master, input + 1)$

.

.

.

$Derived_keying_m = \mathrm{AES}(k_master, input + (m - 1))$

K = the L leftmost bits of

$(Derived_keying_1 \| Derived_keying_2 \| \ldots \| Derived_keying_m)$.

The SRTP KDF is **approved** when the following conditions are satisfied:

(1) The KDF is performed in the context of the SRTP protocol.
(2) The AES encryption operation is as specified in FIPS 197.

5.4 Simple Network Management Protocol (SNMP) Key Derivation Function/Key Localization Function

The User-based Security Model (USM) for SNMP version 3 (SNMPv3) (RFC 2571 [RFC 2571]) is specified in RFC 2574. In this security model, a key localization function (i.e., a key derivation function) is used with a secret password when a user needs to share a different secret key with each authoritative SNMP engine[8]. Two key localization functions are specified in this model. Each uses an MD5 or SHA-1 hash function to generate different secret keys to share with each authoritative SNMP engine. The inputs to the key localization function are the password and the *snmpEngineID*, which is unique for each authoritative SNMP engine. If the hash function is collision resistant, then by using different *snmpEngineID*s, the key

[8] One of the SNMP engines involved in each communication is designated to be the authoritative SNMP engine, see RFC 2574 Section 1.5.1 for details.

localization function will produce different keys. Below is the description of the key localization function with SHA-1.

Denote *engineLength* and *passwordlen* to be the lengths (in bytes) of an *snmpEngineID* and a *password*, respectively.

Let $N = \lceil 1024 / passwordlen \rceil$.

Expanded_password = the leftmost 1024 bytes of the string of *N* repetitions of the *password*.

Derived_password = SHA-1 (*Expanded_password*). The *Derived_password* is the output of hashing the *Expanded_password* by SHA-1.

Let *Shared_key* to be the key that the user shares with the authoritative SNMP engine with ID *snmpEngineID.* The *Shared_key* is generated as follow:

Shared_key = SHA-1(*Derived_password* || *snmpEngineID* || *Derived_password*).

The USM KDF is **approved** when the following conditions are satisfied:

(1) It is performed in the context of the SNMP protocol.

(2) SHA-1 (as specified in FIPS 180-3) is used in the key localization function.

5.5 Trusted Platform Module (TPM) Key Derivation Function

Version 1.2 of the Trusted Platform Module is specified in the TPM Main Specification Parts 1, 2 and 3 ([TPM Principles], [TPM Structures] and [TPM Commands], respectively). It uses a SHA-1 HMAC-based Pseudorandom Function (PRF) in its KDF to generate keying material for transport sessions between the TPM and an application running on another processor.

To protect the integrity of communications, a session key, *SKEY*, is derived from a secret authorization value, *Auth*, that is a secret key shared between the TPM and the application. An HMAC-PRF is used to produce the *SKEY* as follows:

> *SKEY* = HMAC (*Auth*, *Nonce_even* || *Nonce_odd*), where *Nonce_even* and *Nonce_odd* are non-secret values created by the random number generators on the TPM and the application, respectively.

Additional technical details for the variables in the functions are provided in Part 3 of the TPM Main Specification.

SKEY is used as an HMAC key to provide data integrity for communications during the session. Further keys may be derived from *SKEY* to provide encryption of parts of the session.

The TPM KDF is **approved** when the following conditions are satisfied:

(1) The TPM KDF is performed in the context of a TPM session (i.e. performed between a TPM and an application with a shared authorization value.)

(2) HMAC and SHA-1 are used as specified in FIPS 198-1 and 180-3, respectively.

Note that the KDF is a particular instance of the feedback mode as specified in Section 5.2 of SP 800-108, with an empty initial value (IV).

6 References

[ANS X9.42] NIST ANS X9.42-2001, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography, 2001.

[ANS X9.63] ANS X9.63-2001, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2001.

[FIPS 180-3] Federal Information Processing Standard 180-3, Secure Hash Standard (SHS), October 2008.

[FIPS 197] Federal Information Processing Standard 197, Advanced Encryption Standard (AES), November 2001.

[FIPS 198-1] Federal Information Processing Standard 198-1, The Keyed-Hash Message Authentication Code (HMAC), July 2008.

[RFC 2246] T. Dierks and C. Allen, The TLS Protocol Version 1.0, RFC 2246, January 1999.

[RFC 2409] D. Harkins and D. Carrel, The Internet Key Exchange (IKE), RFC 2409, November 1998.

[RFC 2571] D. Harrington, R. Presuhn and B. Wijnen, An Architecture for Describing SNMP Management Frameworks, RFC 2571, April 1999.

[RFC 2574] U. Blumenthal and B. Wijnen, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), RFC 2574, April 1999.

[RFC 2631] E. Rescorla, “Diffie-Hellman Key Agreement Method”, RFC 2631, June 1999.

[RFC 3278] S. Blake-Wilson, D. Brown and P. Lambert, Use of Elliptic Curve Cryptography (ECC) Algorithms in

Cryptographic Message Syntax (CMS), RFC 3278, April 2002.

[RFC 3550] H. Schulzrinne, S. Casner, R. Frederick and V. Jacobson, RTP: A Transport Protocol for Real-Time Applications, RFC 3550, July 2003.

[RFC 3711] M. Baugher, D. McGrew, M. Naslund, E. Carrara and K. Norrman, The Secure Real-time Transport Protocol (SRTP), RFC 3711, March 2004.

[RFC 4251] Y. Ylonen and C. Lonvick (Ed.), The Secure Shell (SSH) Protocol Achitecture, RFC 4251, January 2006.

[RFC 4252] T. Ylonen and C. Lonvick, The Secure Shell (SSH) Authentication Protocol, RFC 4252, January 2006.

[RFC 4253] T. Ylonen and C. Lonvick (Ed.), The Secure Shell (SSH) Transport Layer Protocol, RFC 4253, January 2006.

[RFC 4254] T. Ylonen and C. Lonvick, The Secure Shell (SSH) Connection Protocol, RFC 4254, January 2006.

[RFC 4306] C. Kaufman (Ed.), Internet Key Exchange (IKEv2) Protocol, RFC 4306, December 2005.

[RFC 4346] T. Dierks and E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.1, RFC 4346, April 2006.

[RFC 5246] T. Dierks and E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.2, RFC 5246, August 2008.

[SEC1] SECG, "Elliptic Curve Cryptography", Standards for Efficient Cryptography Group, 2000. www.secg.org/collateral/sec1.pdf.

[SP 800-56A] E. Barker, D. Johnson and M. Smid, “Recommendations for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), National Institute of Standards and Technology, NIST Special Publication 800-56A, March 2007.

[SP 800-56B] E. Barker, L. Chen, A. Regenscheid and M. Smid, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography”,

	National Institute of Standards and Technology, NIST Special Publication 800-56B, August 2009.
[SP 800-56C]	L. Chen, "Recommendation for Key Derivation through Extraction-then-Expansion", NIST SP 800 56C (Draft), September 2010.
[SP 800-57]	E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, "Recommendation for Key Management-Part 1: General (Revised), National Institute of Standards and Technology, NIST Special Publication 800-57, March 2007.
[SP 800-108]	L. Chen, "Recommendation for Key Derivation Using Pseudorandom Functions", National Institute of Standards and Technology (Revised)", NIST Special Publication 800-108, October 2009.
[TPM Principles]	TPM Main Specification Part 1 – Design Principles, July 2007.
[TPM Structures]	TPM Main Specification Part 2 – TPM Structures, July 2007.
[TPM Commands]	TPM Main Specification Part 3 – Commands, July 2007.