Key Agreement Scheme (KAS) guidance related to SP800-140Br1 and associated tables

(last updated May 16, 2025)

IG D.F Key Agreement Methods specifies approved and allowed key agreement schemes (KAS) that can be used as part of a module's approved services. Below is supplemental guidance on when to claim "KAS-full" as a Security Function Implementation (SFI) within a module validation and how to fill in the MIS tables.

KAS-full is claimed:

1. The module implements at least one of the asymmetric key agreement schemes (KAS) from item 2 below such that:
    a. **Module SSP established and used internally:** A KAS is used to establish (i.e., agree on) a module key/SSP that is used by the module for cryptographic protection. For example, the module is a network switch that uses KAS to establish a key that is used to protect (encrypt/decrypt) network traffic. It may be possible for the module to output the agreed upon key/SSP at a later time (e.g., for backup), but this is separate from and in addition to using it for cryptographic protection that is applied within the module boundary.

    b. **Party U or Party V**: The module performs and controls all necessary steps as either Party U or Party V per the claimed KAS specified in SP 800-56Arev3 or SP 800-56Brev2.

    c. **SSC + KDF**: The key agreement scheme's Shared Secret Computation (SSC) and Key Derivation Function (KDF) (and optional Key Confirmation - KC) are implemented together in an approved manner fully controlled by the module (i.e., it is NOT the responsibility of the operator to piece things together correctly).

    d. **Assurances**: The module implements the assurances / checks as required by SP 800-56Brev2 or SP 800-56Arev3, depending on the scheme selected and if the module is designated as Party U or Party V.

    e. **Test Report** (at minimum):

        I. **AS09.10** applies.

        II. **Section 10** self-tests implemented per IG D.F Scenario 1/2 Path (2).

2. ***Approved*** **or** ***allowed*** **key agreement schemes (KAS):**
    a. Approved: **IG D.F Scenario 1 Path (2)** SP 800-56Brev2 RSA based (IFC) – either end-to-end or split.

    b. Approved: **IG D.F Scenario 2 Path (2)** SP 800-56Arev3 ECC or FFC based – either end-to-end or split.

    c. Allowed: **IG D.F Scenario 3** (i.e., IG C.A Resolution 1) - using Brainpool curves within an otherwise approved IG D.F Scenario 2 Path (2) ECC scheme.

MIS Table Descriptions (see link)

Table 10 *Security Function Implementations* (SFI): Include KAS-Full claims as follows (extracted from the MIS Table Descriptions):

- Column Information
    - Name – Unique for every entry and include "KAS" (e.g., KAS1, KAS-ECC, or KAS-FFC).
    - Type – "KAS-Full".
    - [no change] Description – how this is used
    - SF Properties – Name/Value pairs
        - [if IG D.F Scenario 1 or 2] Name: "IG"; Value: "IG D.F Scenario <1 or 2>, path (2), <end-to-end or split>"
        - [if IG D.F Scenario 3] Name: "IG"; Value: "IG D.F Scenario 3 based on Scenario 2, path (2), <end-to-end or split>"
        - Name: "Key confirmation"; Value: "<yes or no>"
        - Name: "Key derivation"; Value: "IG 2.4.B SP 800-135rev1 CVL" and/or "KDA (separately tested)" and/or "KDA (tested as part KAS certificate)"
        - Name: "Caveat"; Value: "Key establishment methodology provides between <N> and <M> bits of security strength" (see IG D.B)
    - [no change] Algorithms – the set of tested algorithms that comprise the implementation to include prerequisites.
        - Per IG D.F Scenario 3, if Brainpool curves supported, the corresponding algorithms will be shown in the non-approved but allowed table and referenced by this Algorithms column.
    - [no change] Algorithm Properties – If a subset of the available capabilities are used, specify.

Table 24 *SSPs* captures the KAS SSPs, including, at minimum:

- [PSP] Public key(s) in a key pair
- [CSP] Private key(s) in a key pair
- [PSP] SP 800-56Arev3 domain parameters
- [CSP] Approved MAC algorithm key ("MacKey") and "MacData" for key confirmation (if employed)
- [CSP] Shared secret
- [CSP] Key derivation function keys (e.g., underlying MAC keys and/or KDF-specific secret parameters such as K_{DK} in SP 800-56Crev2 Two-Step, and IKEv2's "SKEYSEED" in SP 800-135rev1), as applicable
- [CSP] Shared secret key that is established (i.e., agreed upon)

KAS-full is NOT claimed:

1. **"KAS" as a service (i.e., no establishment):** The module offers as a service to an external operator (e.g., calling application) CAVP-tested KAS algorithms specified in item 2 above without establishing a module key/SSP used by the module for cryptographic protection. E.g., as common in software library validations or some single chip validations, the module

may offer KAS IFC-basic as a service (or several sub-routines) that receives as inputs all keying material necessary to output the agreed-upon key (i.e., “DerivedKeyingMaterial” in SP 800-56 standards).

   - **MIS Tables -** same as section above, except for the **Table 10 SFI table**:
     - Type – “KAS-SSC/KDF”.
   - **MIS Tables -** same as section above, except for:
     - the **Table 10 (SFI)**
       - Type – “KAS-SSC/KDF”.
     - the **Table 24 SSPs** (minimum SSPs):
       - [CSP] Shared secret key that is generated by the KAS service and passed back to the calling application.

2. **“KAS-SSC” as a service (i.e., no establishment):** The module offers as a service to an external operator (e.g., calling application) CAVP-tested KAS SSC that map to IG D.F Scenario 1 path (1) or IG D.F Scenario 2 path (1) without establishing a module key/SSP used by the module for cryptographic protection. E.g., module offers KAS1 IFC SSC as a service that receives as inputs all keying material necessary to compute and output the shared secret without applying a KDF/KDA (which may be a separate module service).

3. In either of the scenarios above:
   - **Security Policy (Section 2.7 Algorithm Specific Information) must state**: “The module does not establish SSPs using an approved key agreement scheme (KAS). However, it does offer some or all of the underlying KAS cryptographic functionality to be used by an external operator/application as part of an approved KAS.”
   - **Assurances**: See IG D.F Additional Comment #5 for relevant guidance.