JCATT ファイルフォーマット仕様書

NIST SP800-56B に記載された KAS2

2018 年 8 月

独立行政法人情報処理推進機構

目次

1　はじめに

暗号アルゴリズム実装試験ツール (以下 JCATT と略記する) が使用する各種ファイルのフォーマット規則を記述する．JCATT が使用するファイルには次のようなものがある．

ファイルの種類

- パラメータファイル (*.par)
  試験項目の設定を記述する．JCATT を用いて作成する．
- リクエストファイル (*.req)
  暗号モジュール開発ベンダに対する要求を記述する．JCATT を用いて作成する．
- Facts ファイル (*.fax)
  テストベクタを記述する．JCATT を用いて作成する．
- レスポンスファイル (*.rsp)
  ベンダからの回答を記述する．リクエストファイルおよび本稿で指定するファイルフォーマットに基づいてベンダが作成する．
- 結果ファイル (*.out)
  試験結果を記述する．JCATT を用いて作成する．

これらのファイルの名前は，次の規則に従ってつけること．

ファイル名の規則

- 拡張子は，上記 ( ) 内に指定したものを使用すること．
- 拡張子以外の名前は，試験対象実装ごとに同じ名称をつけること．
  リクエストファイル (*.req) と Facts ファイル (*.fax) の生成時には，リクエストファイル (*.req) と Facts ファイル (*.fax) に対してパラメータファイル (*.par) と同じ名称を JCATT が自動的につける．
  試験実行時には，同じ名称のレスポンスファイル (*.rsp) と Facts ファイル (*.fax) に対して試験が行われる．また，試験実行時は，結果ファイル (*.out) に対して，Facts ファイル (*.fax) と同じ名称を JCATT が自動的につける．

ファイルフォーマット詳細は次章以降に記述する．各ファイルに共通の規則は次の通りである．

共通規則

- JCATT 互換ファイルフォーマットの選択時, [　　] で囲まれた “タグ” の次の行に値を記述する．
- CAVS 準互換ファイルフォーマットの選択時, 〈 タグ 〉=〈 値 〉 の形式で 1 行で記述する．
- ヘッダ部分については各行について [〈 タグ 〉=〈 値 〉] の形式で 1 行で記述する．
- レスポンスファイルにおいては，【出力】と記述したタグが，試験対象実装が出力するデータを記述する箇所である．
- 半角英数字を用いること．
- タグおよび値は大文字小文字の区別をするので，大文字小文字を含めて正確に記述すること．ただし，数値を 16 進数で記述する場合は，大文字小文字は区別しない．
- 一文字目が ♯(半角) で始まるコメント行を自由に書き込むことができる．
- 平文，暗号文，鍵などのデータの区切り文字は改行 (CR+LF または LF) とする．
- 平文，暗号文，署名，鍵などのデータは 16 進表記とする．
- ビット数，個数などの数値は 10 進表記とする．
- ACSII コードを使用すること．
- 各行には必ず改行を入れること (最後のデータと EOF との間にも改行を入れること)．

2　NIST SP800-56B に記載された KAS2

鍵確立手法 KAS2 in NIST SP 800-56B の暗号アルゴリズム実装試験のためのファイルフォーマットを記述する.

`Algorithm Name` は，KAS2_in_NIST_SP800_56B.

試験方法の詳細は，暗号アルゴリズム実装試験仕様書を参照のこと.

2.1　CAVS 準互換ファイルフォーマット

この章で取り扱うファイルフォーマットでは, 公開鍵指数の種別として, 表1に記載された表現, 鍵導出関数識別子として, 表2に記載された表現, Key Confirmation に使う MAC アルゴリズム識別子として, 表3に記載された表現を用いる.

表1　公開鍵指数の種別

識別子	対応する公開鍵 e
TYPE1	$e = 65,537$
TYPE2	e はランダム

表2　鍵導出関数識別子

鍵導出関数識別子	対応する鍵導出関数	
SP800_56B_5_5_1_KDFConcat_SHA1	NIST SP 800-56B	Concatenation based KDF with SHA-1
SP800_56B_5_5_1_KDFConcat_SHA224		Concatenation based KDF with SHA-224
SP800_56B_5_5_1_KDFConcat_SHA256		Concatenation based KDF with SHA-256
SP800_56B_5_5_1_KDFConcat_SHA384		Concatenation based KDF with SHA-384
SP800_56B_5_5_1_KDFConcat_SHA512		Concatenation based KDF with SHA-512
SP800_56B_5_5_1_KDFConcat_SHA512_224		Concatenation based KDF with SHA-512/224
SP800_56B_5_5_1_KDFConcat_SHA512_256		Concatenation based KDF with SHA-512/256
SP800_56B_5_5_1_KDFConcat_SHA3_256		Concatenation based KDF with SHA3-256
SP800_56B_5_5_1_KDFConcat_SHA3_384		Concatenation based KDF with SHA3-384
SP800_56B_5_5_1_KDFConcat_SHA3_512		Concatenation based KDF with SHA3-512
SP800_56B_5_5_1_KDFConcat_HMAC_SHA1		Concatenation based KDF with HMAC-SHA-1
SP800_56B_5_5_1_KDFConcat_HMAC_SHA224		Concatenation based KDF with HMAC-SHA-224
SP800_56B_5_5_1_KDFConcat_HMAC_SHA256		Concatenation based KDF with HMAC-SHA-256
SP800_56B_5_5_1_KDFConcat_HMAC_SHA384		Concatenation based KDF with HMAC-SHA-384
SP800_56B_5_5_1_KDFConcat_HMAC_SHA512		Concatenation based KDF with HMAC-SHA-512
SP800_56B_5_5_1_KDFConcat_HMAC_SHA512_224		Concatenation based KDF with HMAC-SHA-512/224
SP800_56B_5_5_1_KDFConcat_HMAC_SHA512_256		Concatenation based KDF with HMAC-SHA-512/256
SP800_56B_5_5_1_KDFConcat_HMAC_SHA3_256		Concatenation based KDF with HMAC-SHA3-256
SP800_56B_5_5_1_KDFConcat_HMAC_SHA3_384		Concatenation based KDF with HMAC-SHA3-384
SP800_56B_5_5_1_KDFConcat_HMAC_SHA3_512		Concatenation based KDF with HMAC-SHA3-512
SP800_56B_5_5_1_KDFASN1_SHA1		ASN.1 based KDF with SHA-1
SP800_56B_5_5_1_KDFASN1_SHA224		ASN.1 based KDF with SHA-224
SP800_56B_5_5_1_KDFASN1_SHA256		ASN.1 based KDF with SHA-256
SP800_56B_5_5_1_KDFASN1_SHA384		ASN.1 based KDF with SHA-384
SP800_56B_5_5_1_KDFASN1_SHA512		ASN.1 based KDF with SHA-512
SP800_56B_5_5_1_KDFASN1_SHA512_224		ASN.1 based KDF with SHA-512/224
SP800_56B_5_5_1_KDFASN1_SHA512_256		ASN.1 based KDF with SHA-512/256
SP800_56B_5_5_1_KDFASN1_SHA3_256		ASN.1 based KDF with SHA3-256
SP800_56B_5_5_1_KDFASN1_SHA3_384		ASN.1 based KDF with SHA3-384
SP800_56B_5_5_1_KDFASN1_SHA3_512		ASN.1 based KDF with SHA3-512
SP800_56B_5_5_1_KDFASN1_HMAC_SHA1		ASN.1 based KDF with HMAC-SHA-1
SP800_56B_5_5_1_KDFASN1_HMAC_SHA224		ASN.1 based KDF with HMAC-SHA-224
SP800_56B_5_5_1_KDFASN1_HMAC_SHA256		ASN.1 based KDF with HMAC-SHA-256
SP800_56B_5_5_1_KDFASN1_HMAC_SHA384		ASN.1 based KDF with HMAC-SHA-384
SP800_56B_5_5_1_KDFASN1_HMAC_SHA512		ASN.1 based KDF with HMAC-SHA-512
SP800_56B_5_5_1_KDFASN1_HMAC_SHA512_224		ASN.1 based KDF with HMAC-SHA-512/224
SP800_56B_5_5_1_KDFASN1_HMAC_SHA512_256		ASN.1 based KDF with HMAC-SHA-512/256
SP800_56B_5_5_1_KDFASN1_HMAC_SHA3_256		ASN.1 based KDF with HMAC-SHA3-256
SP800_56B_5_5_1_KDFASN1_HMAC_SHA3_384		ASN.1 based KDF with HMAC-SHA3-384
SP800_56B_5_5_1_KDFASN1_HMAC_SHA3_512		ASN.1 based KDF with HMAC-SHA3-512
ANS_X942_7_7_2_KDFConcat_SHA1	ANS X9.42-2001	Concatenation based KDF with SHA-1
ANS_X942_7_7_2_KDFConcat_SHA224		Concatenation based KDF with SHA-224
ANS_X942_7_7_2_KDFConcat_SHA256		Concatenation based KDF with SHA-256
ANS_X942_7_7_2_KDFConcat_SHA384		Concatenation based KDF with SHA-384
ANS_X942_7_7_2_KDFConcat_SHA512		Concatenation based KDF with SHA-512
ANS_X942_7_7_2_KDFASN1_SHA1		ASN.1 based KDF with SHA-1
ANS_X942_7_7_2_KDFASN1_SHA224		ASN.1 based KDF with SHA-224
ANS_X942_7_7_2_KDFASN1_SHA256		ASN.1 based KDF with SHA-256
ANS_X942_7_7_2_KDFASN1_SHA384		ASN.1 based KDF with SHA-384
ANS_X942_7_7_2_KDFASN1_SHA512		ASN.1 based KDF with SHA-512

2.1.1　パラメータファイル (*.par)

表3　MAC アルゴリズム識別子

MAC アルゴリズム識別子	対応する MAC アルゴリズム
HMAC_SHA1	HMAC-SHA-1
HMAC_SHA224	HMAC-SHA-224
HMAC_SHA256	HMAC-SHA-256
HMAC_SHA384	HMAC-SHA-384
HMAC_SHA512	HMAC-SHA-512
HMAC_SHA512_224	HMAC-SHA-512/224
HMAC_SHA512_256	HMAC-SHA-512/256
HMAC_SHA3_256	HMAC-SHA3-256
HMAC_SHA3_384	HMAC-SHA3-384
HMAC_SHA3_512	HMAC-SHA3-512
CMAC_AES128	CMAC-AES-128
CMAC_AES192	CMAC-AES-192
CMAC_AES256	CMAC-AES-256

表4　NIST SP800-56B に記載された KAS2 パラメータファイル

機能	タグ		内容	表記
鍵共有	ヘッダ	AlgorithmName	KAS2_in_NIST_SP800_56B	文字列
		TargetFunction	KeyAgreement	文字列
		TargetRole	IUT が担う役割 (Party_U, Party_V)	文字列
		TypeOfPublicKeyU	Party U の公開鍵指数の種別 (65537:TYPE1, random:TYPE2)	文字列
		TypeOfPrivateKeyU	Party U のプライベート鍵の種別 (CRT なし:TYPE2)	文字列
		BitLengthOfModulusPartyU	Party U の公開鍵の法 n のビット長	10 進
		TypeOfPublicKeyV	Party V の公開鍵指数の種別 (65537:TYPE1, random:TYPE2)	文字列
		TypeOfPrivateKeyV	Party V のプライベート鍵の種別 (CRT なし:TYPE2)	文字列
		BitLengthOfModulusPartyV	Party V の公開鍵の法 n のビット長	10 進
		KDF	(鍵導出関数識別子)	文字列
		BitLengthOfSaltForHMACbasedKDF	HMAC ベースの KDF を使用する場合, salt のビット長	10 進
		BitLengthOfOI	OtherInfo のビット長	10 進
		ID_U	Party U の Identifier	16 進
		ID_V	Party V の Identifier	16 進
		KeyConfirmationSupported	サポートする Key confirmation のタイプ (• Key Confirmation なし:NoKC, • unilateral key confirmation from party U to party V:Unilateral_U_to_V, • unilateral key confirmation from party V to party U:Unilateral_V_to_U, • bilateral key confirmation:Bilateral)	文字列
		SelectedTestMethod	暗号アルゴリズム実装試験仕様書—鍵確立手法—の選択された試験項目の番号	10 進
		BitLengthOfDKM	DKM のビット長	10 進
		NumberOfDKM	DKM の個数	10 進
		RatioOfInvalidData	鍵確立に失敗するデータの割合. (次の場合は省略: • TargetRole = Party_U かつ Unilateral key confirmation from party U to party V の選択時; • TargetRole = Party_V かつ Unilateral key confirmation from party V to party U の選択時は省略.)	浮動小数点
		NumberOfDKMForRGT	SelectedTestMethod = 1 の場合, random generation test における生成する DKM の個数	10 進
		NumberOfTestSubsets	SelectedTestMethod = 1 の場合, 試験の部分集合の数	10 進
		MACforKeyConfirmation	KeyConfirmationSupported ≠ NoKC の場合, Key confirmation に使う MAC アルゴリズム. それ以外は省略.	文字列
		BitLengthOfMacKey	KeyConfirmationSupported ≠ NoKC の場合, Key confirmation に使う MacKey のビット長. それ以外は省略.	10 進
		BitLengthOfMacTag	KeyConfirmationSupported ≠ NoKC の場合, Key confirmation に使う MacTag のビット長. それ以外は省略.	10 進

2.1.2 リクエストファイル (*.req)

表5: NIST SP800-56B に記載された KAS2 リクエストファイル

機能	分類	タグ	内容	暗号アルゴリズム実装試験仕様書 —鍵確立手法— 上の表記との対応	値の表記	例示
鍵共有	ヘッダ	AlgorithmName	KAS2_in_NIST_SP800_56B		文字列	[AlgorithmName = KAS2_in_NIST_SP800_56B]
		TargetFunction	KeyAgreement		文字列	[TargetFunction = KeyAgreement]
		TargetRole	IUT が担う役割 (Party_U, Party_V)		文字列	[TargetRole = Party_U]
		TypeOfPublicKeyU	Party U の公開鍵指数の種別 (65537:TYPE1, random:TYPE2)		文字列	[TypeOfPublicKeyU = TYPE1]
		TypeOfPrivateKeyU	Party U のプライベート鍵の種別 (CRT なし:TYPE2)		文字列	[TypeOfPrivateKeyU = TYPE2]
		BitLengthOfModulusPartyU	Party U の公開鍵の法 n のビット長		10 進表記	[BitLengthOfModulusPartyU = 3072]
		TypeOfPublicKeyV	Party V の公開鍵指数の種別 (65537:TYPE1, random:TYPE2)		文字列	[TypeOfPublicKeyV = TYPE1]
		TypeOfPrivateKeyV	Party V のプライベート鍵の種別 (CRT なし:TYPE2)		文字列	[TypeOfPrivateKeyV = TYPE2]
		BitLengthOfModulusPartyV	Party V の公開鍵の法 n のビット長		10 進表記	[BitLengthOfModulusPartyV = 3072]
		KDF	鍵導出関数識別子		文字列	[KDF = SP800_56B_5_5_1_KDFConcat_SHA1]
		BitLengthOfSaltForHMACbasedKDF	HMAC ベースの KDF を使用する場合, salt のビット長		10 進表記	[BitLengthOfSaltForHMACbasedKDF = 0]
		BitLengthOfOI	OtherInfo のビット長		10 進表記	[BitLengthOfOI = 384]
		ID_U	Party U の Identifier		16 進表記	[ID_U = a1b2c3d4e5]
		ID_V	Party V の Identifier		16 進表記	[ID_V = 4a434154546964]
		KeyConfirmationSupported	サポートする Key Confirmation のタイプ (• Key Confirmation なし:NoKC, • unilateral key confirmation from party U to party V:Unilateral_U_to_V, • unilateral key confirmation from party V to party U:Unilateral_V_to_U, • bilateral key confirmation:Bilateral)		文字列	[KeyConfirmationSupported = NoKC]
		SelectedTestMethod	暗号アルゴリズム実装試験仕様書—鍵確立手法—の選択された試験項目の番号 (試験 1:1, 試験 2:2, 試験 3:3)		10 進表記	[SelectedTestMethod = 1]
		BitLengthOfDKM	DKM のビット長	$KBits$	10 進表記	[BitLengthOfDKM = 320]
		NumberOfDKM	DKM の個数		10 進表記	[NumberOfDKM = 2048]
		RatioOfInvalidData	鍵確立に失敗するデータの割合. (次の場合は省略: • TargetRole = Party_U かつ Unilateral key confirmation from party U to party V の選択時; • TargetRole = Party_V かつ Unilateral key confirmation from party V to party U の選択時は省略.)		浮動小数点表記	[RatioOfInvalidData = 0.5]
		NumberOfDKMForRGT	KeyConfirmationSupported = NoKC の場合, random generation test において生成する DKM の個数. それ以外は省略		10 進表記	[NumberOfDKMForRGT = 2048]
		NumberOfTestSubsets	KeyConfirmationSupported = NoKC の場合, 試験の部分集合の数. それ以外は省略		10 進表記	[NumberOfTestSubsets = 2]
		MACforKeyConfirmation	KeyConfirmationSupported ≠ NoKC の場合, Key confirmation に使う MAC アルゴリズム. それ以外は省略.		文字列	[MACforKeyConfirmation = HMAC_SHA512]
		BitLengthOfMacKey	KeyConfirmationSupported ≠ NoKC の場合, Key confirmation に使う MacKey のビット長. それ以外は省略.		10 進表記	[BitLengthOfMacKey = 128]
		BitLengthOfMacTag	KeyConfirmationSupported ≠ NoKC の場合, Key confirmation に使う MacTag のビット長. それ以外は省略.		10 進表記	[BitLengthOfMacTag = 512]
Party U 試験 1 ヘッダ *1		nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = c26f . . . 4dfd
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		dU	Party U のプライベート鍵指数 d_U	d_U	16 進表記	dU = 0d0f . . . f1c1
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = bcde . . . dd5b
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
Party U 試験 1 本体 *2*3		COUNT	0 以上 NumberOfDKM 未満の整数又は 0 以上 NumberOfDKMForRGT 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CV	Party V が生成した暗号文	C_V	16 進表記	CV = 54ae . . . 1201
		CU	Party U が生成する暗号文	C_U	16 進表記	CU = ?
		DKM	Party U が導出した $DerivedKeyingMaterial$	$DerivedKeyingMaterial$ (DKM)	16 進表記	DKM = ?
		Result	鍵確立の成功又は失敗		文字列	Result = ?
Party U 試験 2 KAS2-Party_U-confirmation ヘッダ		nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = c26f . . . 4dfd
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		dU	Party U のプライベート鍵指数 d_U	d_U	16 進表記	dU = 0d0f . . . f1c1
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = bcde . . . dd5b
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
Party U 試験 2 KAS2-Party_U-confirmation 本体 *4		COUNT	0 以上 NumberOfDKM 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CV	Party V が生成した暗号文	C_V	16 進表記	CV = 1d10 . . . de15
		CU	Party U が生成する暗号文	C_U	16 進表記	CU = ?
		KeyData	Party U が導出する $KeyData$	$KeyData$	16 進表記	KeyData = ?
		MacTagU	Party U が計算した MacTag	$MacTag_U$	16 進表記	MacTagU = ?
Party U 試験 2 KAS2-Party_V-confirmation ヘッダ		nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = c26f . . . 4dfd
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		dU	Party U のプライベート鍵指数 d_U	d_U	16 進表記	dU = 0d0f . . . f1c1
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = bcde . . . dd5b
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
Party U 試験 2 KAS2-Party_V-confirmation 本体 *5		COUNT	0 以上 NumberOfDKM 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CU	Party U の暗号文	C_U	16 進表記	CU = 812a . . . 0814
		ZU	C_U の生成に使用した secret value Z_U	Z_U	16 進表記	ZU = 6065 . . . ad19
		CV	Party V が生成した暗号文	C_V	16 進表記	CV = 0ccb . . . ed0d
		MacDataV	MacDataV	$MacData_V$	16 進表記	MacDataV = 4b43 . . . 0814
		MacTagV	MacTagV	$MacTag_V$	16 進表記	MacTagV = 262c . . . 7c6d
		KeyData	Party U が導出する $KeyData$	$KeyData$	16 進表記	KeyData = ?
		Result	鍵確立の成功又は失敗		文字列	Result = ?
Party U 試験 3 ヘッダ		nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = c26f . . . 4dfd
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		dU	Party U のプライベート鍵指数 d_U	d_U	16 進表記	dU = 0d0f . . . f1c1
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = bcde . . . dd5b
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
Party U 試験 3 本体 *6		COUNT	0 以上 NumberOfDKM 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CU	Party U の暗号文	C_U	16 進表記	CU = 1d10 . . . de15
		ZU	C_U の生成に使用した secret value Z_U	Z_U	16 進表記	ZU = 457f . . . e64b
		CV	Party V が生成した暗号文	C_V	16 進表記	CV = 1d10 . . . de15
		MacDataU	MacDataU	$MacData_U$	16 進表記	MacDataU = 4b43 . . . a317
		MacDataV	MacDataV	$MacData_V$	16 進表記	MacDataV = 4b43 . . . 0345
		MacTagV	MacTagV	$MacTag_V$	16 進表記	MacTagV = 5610 . . . 9131
		KeyData	Party U が導出する $KeyData$	$KeyData$	16 進表記	KeyData = ?
		MacTagU	Party U が計算した MacTag	$MacTag_U$	16 進表記	MacTagU = ?
		Result	鍵確立の成功又は失敗		文字列	Result = ?
Party V 試験 1 ヘッダ *1		nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = bae1 . . . 56eb
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = 8a53 . . . 9fdf
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
		dV	Party V のプライベート鍵指数 d_V	d_V	16 進表記	dV = 3f27 . . . 546d
Party V 試験 1 本体 *7*8		COUNT	0 以上 NumberOfDKM 未満の整数又は 0 以上 NumberOfDKMForRGT 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CU	Party U が生成した暗号文	C_U	16 進表記	CU = 54ae . . . 1201
		CV	Party V が生成する暗号文	C_V	16 進表記	CV = ?

table continued on next page

continued from previous page

機能	分類	タグ	内容	暗号アルゴリズム実装試験仕様書 ―鍵確立手法― 上の表記との対応	値の表記	例示
		DKM	Party V が導出する $DerivedKeyingMaterial$	$DerivedKeyingMaterial$ (DKM)	16 進表記	DKM = ?
		Result	鍵確立の成功又は失敗		文字列	Result = ?
	Party V 試験 2 KAS2-Party_U-confirmation ヘッダ	nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = bae1 . . . 56eb
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = 8a53 . . . 9fdf
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
		dV	Party V のプライベート鍵指数 d_V	d_V	16 進表記	dV = 3f27 . . . 546d
	Party V 試験 2 KAS2-Party_U-confirmation 本体 *9	COUNT	0 以上 NumberOfDKM 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CU	Party U が生成した暗号文	C_U	16 進表記	CU = 1d10 . . . de15
		CV	Party V の暗号文	C_V	16 進表記	CV = 1d10 . . . de15
		ZV	C_V の生成に使用した secret value Z_V	Z_V	16 進表記	ZV = 457f . . . e64b
		MacDataU	MacDataV	$MacData_U$	16 進表記	MacDataU = 4b43 . . . de15
		MacTagU	MacTagU	$MacTag_U$	16 進表記	MacTagU = 9d6e . . . ae0d
		KeyData	Party V が導出する $KeyData$	$KeyData$	16 進表記	KeyData = ?
		Result	鍵確立の成功又は失敗		文字列	Result = ?
	Party V 試験 2 KAS2-Party_V-confirmation ヘッダ	nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = bae1 . . . 56eb
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = 8a53 . . . 9fdf
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
		dV	Party V のプライベート鍵指数 d_V	d_V	16 進表記	dV = 3f27 . . . 546d
	Party V 試験 2 KAS2-Party_V-confirmation 本体 *10	COUNT	0 以上 NumberOfDKM 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CU	Party U が生成した暗号文	C_U	16 進表記	CU = 1d10 . . . de15
		CV	Party V が生成する暗号文	C_V	16 進表記	CV = ?
		KeyData	Party V が導出する $KeyData$	$KeyData$	16 進表記	KeyData = ?
		MacTagV	Party V が計算した MacTag	$MacTag_V$	16 進表記	MacTagV = ?
	Party V 試験 3 ヘッダ	nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = bae1 . . . 56eb
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = 8a53 . . . 9fdf
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
		dV	Party V のプライベート鍵指数 d_V	d_V	16 進表記	dV = 3f27 . . . 546d
	Party U 試験 3 本体 *11	COUNT	0 以上 NumberOfDKM 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CU	Party U が生成した暗号文	C_U	16 進表記	CU = 1d10 . . . de15
		CV	Party V の暗号文	C_V	16 進表記	CV = 1d10 . . . de15
		ZV	C_V の生成に使用した secret value Z_V	Z_V	16 進表記	ZV = 457f . . . e64b
		MacDataU	MacDataU	$MacData_U$	16 進表記	MacDataU = 4b43 . . . de15
		MacTagU	MacTagU	$MacTag_U$	16 進表記	MacTagU = 9d6e . . . ae0d
		MacDataV	MacDataV	$MacData_V$	16 進表記	MacDataV = 4b43 . . . de15
		KeyData	Party V が計算した $KeyData$	$KeyData$	16 進表記	KeyData = ?
		MacTagV	Party V が計算した MacTag	$MacTag_V$	16 進表記	MacTagV = ?
		Result	鍵確立の成功又は失敗		文字列	Result = ?

*1 試験 1 の各部分集合に対して, 1 セットずつ, 本体の直前にヘッダが出力される. NumberOfTestSubsets = 2 の場合には, 計 2 セットのヘッダが出力されることになる.

*2 試験 1 の部分集合として, NumberOfDKM 組の各データを以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = 0 に対応する暗号文 C_V を記述する.
CU = ?                             ♯ i = 0 に対応する暗号文 C_U のプレースホルダ.
DKM = ?                            ♯ i = 0 に対応する DerivedKeyingMaterial (DKM) のプレースホルダ.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = 1 に対応する暗号文 C_V を記述する.
CU = ?                             ♯ i = 1 に対応する暗号文 C_U のプレースホルダ.
DKM = ?                            ♯ i = 1 に対応する DerivedKeyingMaterial (DKM) のプレースホルダ.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
CU = ?                             ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U のプレースホルダ.
DKM = ?                            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する DerivedKeyingMaterial (DKM) のプレースホルダ.
```

*3 NumberOfDKM 組のデータに引き続き, 試験 1 の部分集合として, NumberOfDKMForRGT 組の各データを以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = 0 に対応する暗号文 C_V を記述する.
CU = ?                             ♯ i = 0 に対応する暗号文 C_U のプレースホルダ.
DKM = ?                            ♯ i = 0 に対応する DerivedKeyingMaterial (DKM) のプレースホルダ.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = 1 に対応する暗号文 C_V を記述する.
CU = ?                             ♯ i = 1 に対応する暗号文 C_U のプレースホルダ.
DKM = ?                            ♯ i = 1 に対応する DerivedKeyingMaterial (DKM) のプレースホルダ.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
CU = ?                             ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U のプレースホルダ.
DKM = ?                            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する DerivedKeyingMaterial (DKM) のプレースホルダ.
```

*4 NumberOfDKM 個の各データの組を以下のように記述する.

```
COUNT = 0                              ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                     ♯ i = 0 に対応する暗号文 C_V を記述する.
CU = ?                                 ♯ i = 0 に対応する暗号文 C_U のプレースホルダ.
KeyData = ?                            ♯ i = 0 に対応する KeyData のプレースホルダ.
MacTagU = ?                            ♯ i = 0 に対応する MacTag_U のプレースホルダ.

COUNT = 1                              ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                     ♯ i = 1 に対応する暗号文 C_V を記述する.
CU = ?                                 ♯ i = 1 に対応する暗号文 C_U のプレースホルダ.
KeyData = ?                            ♯ i = 1 に対応する KeyData のプレースホルダ.
MacTagU = ?                            ♯ i = 1 に対応する MacTag_U のプレースホルダ.
⋮
COUNT = ⟨NumberOfDKM − 1⟩              ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                     ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
CU = ?                                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U のプレースホルダ.
KeyData = ?                            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する KeyData のプレースホルダ.
MacTagU = ?                            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する MacTag_U のプレースホルダ.
```

∗5 NumberOfDKM 個の各データの組を以下のように記述する.

```
COUNT = 0                              ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 812a ... 0814                     ♯ i = 0 に対応する暗号文 C_U を記述する.
ZU = 6065 ... ad19                     ♯ i = 0 に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
CV = 0ccb ... ed0d                     ♯ i = 0 に対応する暗号文 C_V を記述する.
MacDataV = 4b43 ... 0814               ♯ i = 0 に対応する, MacTag_V の生成に用いた MacData を記述する.
MacTagV = 262c ... 7c6d                ♯ i = 0 に対応する, MacTag_V を記述する.
KeyData = ?                            ♯ i = 0 に対応する, KeyData のプレースホルダ.
Result = ?                             ♯ i = 0 に対応する, 鍵確立の成功又は失敗のプレースホルダ.

COUNT = 1                              ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 812a ... 0814                     ♯ i = 1 に対応する暗号文 C_U を記述する.
ZU = 6065 ... ad19                     ♯ i = 1 に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
CV = 0ccb ... ed0d                     ♯ i = 1 に対応する暗号文 C_V を記述する.
MacDataV = 4b43 ... 0814               ♯ i = 1 に対応する, MacTag_V の生成に用いた MacData を記述する.
MacTagV = 262c ... 7c6d                ♯ i = 1 に対応する, MacTag_V を記述する.
KeyData = ?                            ♯ i = 1 に対応する, KeyData のプレースホルダ.
Result = ?                             ♯ i = 1 に対応する, 鍵確立の成功又は失敗のプレースホルダ.
⋮
COUNT = ⟨NumberOfDKM − 1⟩              ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 812a ... 0814                     ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
ZU = 6065 ... ad19                     ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
CV = 0ccb ... ed0d                     ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
MacDataV = 4b43 ... 0814               ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_V の生成に用いた MacData を記述する.
MacTagV = 262c ... 7c6d                ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_V を記述する.
KeyData = ?                            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, KeyData のプレースホルダ.
Result = ?                             ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, 鍵確立の成功又は失敗のプレースホルダ.
```

∗6 NumberOfDKM 個の各データの組を以下のように記述する.

```
COUNT = 0                              ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 812a ... 0814                     ♯ i = 0 に対応する暗号文 C_U を記述する.
ZU = 6065 ... ad19                     ♯ i = 0 に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
CV = 0ccb ... ed0d                     ♯ i = 0 に対応する暗号文 C_V を記述する.
MacDataU = 4b43 ... a317               ♯ i = 0 に対応する, MacTag_U の生成に用いる MacData_U を記述する.
MacDataV = 4b43 ... 0345               ♯ i = 0 に対応する, MacTag_V の生成に用いた MacData_V を記述する.
MacTagV = 5610 ... 9131                ♯ i = 0 に対応する, MacTag_V を記述する.
KeyData = ?                            ♯ i = 0 に対応する, KeyData のプレースホルダ.
MacTagU = ?                            ♯ i = 0 に対応する, MacTag_U のプレースホルダ.
Result = ?                             ♯ i = 0 に対応する, 鍵確立の成功又は失敗のプレースホルダ.

COUNT = 1                              ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 812a ... 0814                     ♯ i = 1 に対応する暗号文 C_U を記述する.
ZU = 6065 ... ad19                     ♯ i = 1 に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
CV = 0ccb ... ed0d                     ♯ i = 1 に対応する暗号文 C_V を記述する.
MacDataU = 4b43 ... a317               ♯ i = 1 に対応する, MacTag_U の生成に用いる MacData_U を記述する.
MacDataV = 4b43 ... 0345               ♯ i = 1 に対応する, MacTag_V の生成に用いた MacData_V を記述する.
MacTagV = 5610 ... 9131                ♯ i = 1 に対応する, MacTag_V を記述する.
KeyData = ?                            ♯ i = 1 に対応する, KeyData のプレースホルダ.
MacTagU = ?                            ♯ i = 1 に対応する, MacTag_U のプレースホルダ.
Result = ?                             ♯ i = 1 に対応する, 鍵確立の成功又は失敗のプレースホルダ.
⋮
COUNT = ⟨NumberOfDKM − 1⟩              ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 812a ... 0814                     ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
ZU = 6065 ... ad19                     ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
CV = 0ccb ... ed0d                     ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
MacDataU = 4b43 ... a317               ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_U の生成に用いる MacData_U を記述する.
MacDataV = 4b43 ... 0345               ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_V の生成に用いた MacData_V を記述する.
MacTagV = 5610 ... 9131                ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_V を記述する.
KeyData = ?                            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, KeyData のプレースホルダ.
MacTagU = ?                            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_U のプレースホルダ.
Result = ?                             ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, 鍵確立の成功又は失敗のプレースホルダ.
```

∗7 試験 1 の部分集合として, NumberOfDKM 組の各データを以下のように記述する.

```
COUNT = 0                              ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                     ♯ i = 0 に対応する暗号文 C_U を記述する.
CV = ?                                 ♯ i = 0 に対応する暗号文 C_V のプレースホルダ.
DKM = ?                                ♯ i = 0 に対応する DerivedKeyingMaterial (DKM) のプレースホルダ.

COUNT = 1                              ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                     ♯ i = 1 に対応する暗号文 C_U を記述する.
CV = ?                                 ♯ i = 1 に対応する暗号文 C_V のプレースホルダ.
DKM = ?                                ♯ i = 1 に対応する DerivedKeyingMaterial (DKM) のプレースホルダ.
⋮
COUNT = ⟨NumberOfDKM − 1⟩              ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                     ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
CV = ?                                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V のプレースホルダ.
DKM = ?                                ♯ i = ⟨NumberOfDKM − 1⟩ に対応する DerivedKeyingMaterial (DKM) のプレースホルダ.
```

∗8 NumberOfDKM 組のデータに引き続き, 試験 1 の部分集合として, NumberOfDKMForRGT 組の各データを以下のように記述する.

```
COUNT = 0                              ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                     ♯ i = 0 に対応する暗号文 C_U を記述する.
CV = ?                                 ♯ i = 0 に対応する暗号文 C_V のプレースホルダ.
DKM = ?                                ♯ i = 0 に対応する DerivedKeyingMaterial (DKM) のプレースホルダ.

COUNT = 1                              ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                     ♯ i = 1 に対応する暗号文 C_U を記述する.
CV = ?                                 ♯ i = 1 に対応する暗号文 C_V のプレースホルダ.
DKM = ?                                ♯ i = 1 に対応する DerivedKeyingMaterial (DKM) のプレースホルダ.
⋮
COUNT = ⟨NumberOfDKM − 1⟩              ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                     ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
CV = ?                                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V のプレースホルダ.
DKM = ?                                ♯ i = ⟨NumberOfDKM − 1⟩ に対応する DerivedKeyingMaterial (DKM) のプレースホルダ.
```

∗9 NumberOfDKM 個の各データの組を以下のように記述する.

```
COUNT = 0                              ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                     ♯ i = 0 に対応する暗号文 C_U を記述する.
CV = 812a ... 0814                     ♯ i = 0 に対応する暗号文 C_V を記述する.
ZV = 6065 ... ad19                     ♯ i = 0 に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
MacDataU = 4b43 ... 0814               ♯ i = 0 に対応する, MacTag_U の生成に用いた MacData を記述する.
MacTagU = 262c ... 7c6d                ♯ i = 0 に対応する, MacTag_U を記述する.
KeyData = ?                            ♯ i = 0 に対応する, KeyData のプレースホルダ.
Result = ?                             ♯ i = 0 に対応する, 鍵確立の成功又は失敗のプレースホルダ.

COUNT = 1                              ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                     ♯ i = 1 に対応する暗号文 C_U を記述する.
CV = 812a ... 0814                     ♯ i = 1 に対応する暗号文 C_V を記述する.
ZV = 6065 ... ad19                     ♯ i = 1 に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
MacDataU = 4b43 ... 0814               ♯ i = 1 に対応する, MacTag_U の生成に用いた MacData を記述する.
MacTagU = 262c ... 7c6d                ♯ i = 1 に対応する, MacTag_U を記述する.
KeyData = ?                            ♯ i = 1 に対応する, KeyData のプレースホルダ.
Result = ?                             ♯ i = 1 に対応する, 鍵確立の成功又は失敗のプレースホルダ.
⋮
COUNT = ⟨NumberOfDKM − 1⟩              ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                     ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
CV = 812a ... 0814                     ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
ZV = 6065 ... ad19                     ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
MacDataU = 4b43 ... 0814               ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_U の生成に用いた MacData を記述する.
MacTagU = 262c ... 7c6d                ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_U を記述する.
KeyData = ?                            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, KeyData のプレースホルダ.
Result = ?                             ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, 鍵確立の成功又は失敗のプレースホルダ.
```

∗10 NumberOfDKM 個の各データの組を以下のように記述する.

```
COUNT = 0                              ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                     ♯ i = 0 に対応する暗号文 C_U を記述する.
CV = ?                                 ♯ i = 0 に対応する暗号文 C_V のプレースホルダ.
KeyData = ?                            ♯ i = 0 に対応する KeyData のプレースホルダ.
MacTagV = ?                            ♯ i = 0 に対応する MacTag_V のプレースホルダ.

COUNT = 1                              ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                     ♯ i = 1 に対応する暗号文 C_U を記述する.
CV = ?                                 ♯ i = 1 に対応する暗号文 C_V のプレースホルダ.
KeyData = ?                            ♯ i = 1 に対応する KeyData のプレースホルダ.
MacTagV = ?                            ♯ i = 1 に対応する MacTag_V のプレースホルダ.
⋮
COUNT = ⟨NumberOfDKM − 1⟩              ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                     ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8    ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                     ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
CV = ?                                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V のプレースホルダ.
KeyData = ?                            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する KeyData のプレースホルダ.
MacTagV = ?                            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する MacTag_V のプレースホルダ.
```

∗11 NumberOfDKM 個の各データの組を以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                 ♯ i = 0 に対応する暗号文 C_U を記述する.
CV = 812a ... 0814                 ♯ i = 0 に対応する暗号文 C_V を記述する.
ZV = 6065 ... ad19                 ♯ i = 0 に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
MacDataU = 4b43 ... 0345           ♯ i = 0 に対応する, MacTag_U の生成に用いた MacData_U を記述する.
MacTagU = 5610 ... 9131            ♯ i = 0 に対応する, MacTag_U を記述する.
MacDataV = 4b43 ... a317           ♯ i = 0 に対応する, MacTag_V の生成に用いる MacData_V を記述する.
KeyData = ?                        ♯ i = 0 に対応する, KeyData のプレースホルダ.
MacTagV = ?                        ♯ i = 0 に対応する, MacTag_V のプレースホルダ.
Result = ?                         ♯ i = 0 に対応する, 鍵確立の成功又は失敗のプレースホルダ.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                 ♯ i = 1 に対応する暗号文 C_U を記述する.
CV = 812a ... 0814                 ♯ i = 1 に対応する暗号文 C_V を記述する.
ZV = 6065 ... ad19                 ♯ i = 1 に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
MacDataU = 4b43 ... 0345           ♯ i = 1 に対応する, MacTag_U の生成に用いた MacData_U を記述する.
MacTagU = 5610 ... 9131            ♯ i = 1 に対応する, MacTag_U を記述する.
MacDataV = 4b43 ... a317           ♯ i = 1 に対応する, MacTag_V の生成に用いる MacData_V を記述する.
KeyData = ?                        ♯ i = 1 に対応する, KeyData のプレースホルダ.
MacTagV = ?                        ♯ i = 1 に対応する, MacTag_V のプレースホルダ.
Result = ?                         ♯ i = 1 に対応する, 鍵確立の成功又は失敗のプレースホルダ.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
CV = 812a ... 0814                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
ZV = 6065 ... ad19                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
MacDataU = 4b43 ... 0345           ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_U の生成に用いた MacData_U を記述する.
MacTagU = 5610 ... 9131            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_U を記述する.
MacDataV = 4b43 ... a317           ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_V の生成に用いる MacData_V を記述する.
KeyData = ?                        ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, KeyData のプレースホルダ.
MacTagV = ?                        ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_V のプレースホルダ.
Result = ?                         ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, 鍵確立の成功又は失敗のプレースホルダ.
```

2.1.3 Facts ファイル (*.fax)

表6: NIST SP800-56B に記載された KAS2 Facts ファイル

機能	分類	タグ	内容	暗号アルゴリズム実装試験仕様書 ―鍵確立手法― 上の表記との対応	値の表記	例示
鍵共有	ヘッダ	AlgorithmName	KAS2_in_NIST_SP800_56B		文字列	[AlgorithmName = KAS2_in_NIST_SP800_56B]
		TargetFunction	KeyAgreement		文字列	[TargetFunction = KeyAgreement]
		TargetRole	IUT が担う役割 (Party_U, Party_V)		文字列	[TargetRole = Party_U]
		TypeOfPublicKeyU	Party U の公開鍵指数の種別 (65537:TYPE1, random:TYPE2)		文字列	[TypeOfPublicKeyU = TYPE1]
		TypeOfPrivateKeyU	Party U のプライベート鍵の種別 (CRT なし:TYPE2)		文字列	[TypeOfPrivateKeyU = TYPE2]
		BitLengthOfModulusPartyU	Party U の公開鍵の法 n のビット長		10 進表記	[BitLengthOfModulusPartyU = 3072]
		TypeOfPublicKeyV	Party V の公開鍵指数の種別 (65537:TYPE1, random:TYPE2)		文字列	[TypeOfPublicKeyV = TYPE1]
		TypeOfPrivateKeyV	Party V のプライベート鍵の種別 (CRT なし:TYPE2)		文字列	[TypeOfPrivateKeyV = TYPE2]
		BitLengthOfModulusPartyV	Party V の公開鍵の法 n のビット長		10 進表記	[BitLengthOfModulusPartyV = 3072]
		KDF	鍵導出関数識別子		文字列	[KDF = SP800_56B_5_5_1_KDFConcat_SHA1]
		BitLengthOfSaltForHMACbasedKDF	HMAC ベースの KDF を使用する場合, salt のビット長		10 進表記	[BitLengthOfSaltForHMACbasedKDF = 0]
		BitLengthOfOI	OtherInfo のビット長		10 進表記	[BitLengthOfOI = 384]
		ID_U	Party U の Identifier		16 進表記	[ID_U = a1b2c3d4e5]
		ID_V	Party V の Identifier		16 進表記	[ID_V = 4a434154546964]
		KeyConfirmationSupported	サポートする Key Confirmation のタイプ (• Key Confirmation なし:NoKC, • unilateral key confirmation from party U to party V:Unilateral_U_to_V, • unilateral key confirmation from party V to party U:Unilateral_V_to_U, • bilateral key confirmation:Bilateral)		文字列	[KeyConfirmationSupported = NoKC]
		SelectedTestMethod	暗号アルゴリズム実装試験仕様書―鍵確立手法―の選択された試験項目の番号 (試験 1:1, 試験 2:2, 試験 3:3)		10 進表記	[SelectedTestMethod = 1]
		BitLengthOfDKM	DKM のビット長	$KBits$	10 進表記	[BitLengthOfDKM = 320]
		NumberOfDKM	DKM の個数		10 進表記	[NumberOfDKM = 2048]
		RatioOfInvalidData	鍵確立に失敗するデータの割合. (次の場合は省略: • TargetRole = Party_U かつ Unilateral key confirmation from party U to party V の選択時; • TargetRole = Party_V かつ Unilateral key confirmation from party V to party U の選択時は省略.)		浮動小数点表記	[RatioOfInvalidData = 0.5]
		NumberOfDKMForRGT	KeyConfirmationSupported = NoKC の場合, random generation test において生成する DKM の個数. それ以外は省略		10 進表記	[NumberOfDKMForRGT = 2048]
		NumberOfTestSubsets	KeyConfirmationSupported = NoKC の場合, 試験の部分集合の数. それ以外は省略		10 進表記	[NumberOfTestSubsets = 2]
		MACforKeyConfirmation	KeyConfirmationSupported ≠ NoKC の場合, Key confirmation に使う MAC アルゴリズム. それ以外は省略.		文字列	[MACforKeyConfirmation = HMAC_SHA512]
		BitLengthOfMacKey	KeyConfirmationSupported ≠ NoKC の場合, Key confirmation に使う MacKey のビット長. それ以外は省略.		10 進表記	[BitLengthOfMacKey = 128]
		BitLengthOfMacTag	KeyConfirmationSupported ≠ NoKC の場合, Key confirmation に使う MacTag のビット長. それ以外は省略.		10 進表記	[BitLengthOfMacTag = 512]
	Party U 試験 1 ヘッダ *1	nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = 8f0a . . . b66f
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		dU	Party U のプライベート鍵指数 d_U	d_U	16 進表記	dU = 0491 . . . ed01
		pU	Party U の素数 p_U	p_U	16 進表記	pU = c24b . . . 71ef
		qU	Party U の素数 q_U	q_U	16 進表記	qU = bc78 . . . 8381
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = b2c9 . . . cf9f
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
		dV	Party V のプライベート鍵指数 d_V	d_V	16 進表記	dV = 11ef . . . 8be9
		pV	Party V の素数 p_V	p_V	16 進表記	pV = edd1 . . . 229d
		qV	Party V の素数 q_V	q_V	16 進表記	qV = c074 . . . 386b
	Party U 試験 1 本体 *2*3	COUNT	0 以上 NumberOfDKM 未満の整数又は 0 以上 NumberOfDKMForRGT 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CV	Party V が生成した暗号文	C_V	16 進表記	CV = 54ae . . . 1201
		ZV	Party V が C_V の生成に使用した secret value Z_V	Z_V	16 進表記	ZV = 0003 . . . e7f2
		Result	鍵確立の成功又は失敗 (C_V が仕様を満たさない場合:F, それ以外は P)		文字列	Result = P
	Party U 試験 2 KAS2-Party_U-confirmation ヘッダ	nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = 8f0a . . . b66f
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		dU	Party U のプライベート鍵指数 d_U	d_U	16 進表記	dU = 0491 . . . ed01
		pU	Party U の素数 p_U	p_U	16 進表記	pU = c24b . . . 71ef
		qU	Party U の素数 q_U	q_U	16 進表記	qU = bc78 . . . 8381
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = b2c9 . . . cf9f
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
		dV	Party V のプライベート鍵指数 d_V	d_V	16 進表記	dV = 11ef . . . 8be9
		pV	Party V の素数 p_V	p_V	16 進表記	pV = edd1 . . . 229d
		qV	Party V の素数 q_V	q_V	16 進表記	qV = c074 . . . 386b
	Party U 試験 2 KAS2-Party_U-confirmation 本体 *4	COUNT	0 以上 NumberOfDKM 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CV	Party V が生成した暗号文	C_V	16 進表記	CV = 1d10 . . . de15
		ZV	Party V が C_V の生成に使用した secret value Z_V	Z_V	16 進表記	ZV = 457f . . . e64b
	Party U 試験 2 KAS2-Party_V-confirmation ヘッダ	nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = 8f0a . . . b66f
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		dU	Party U のプライベート鍵指数 d_U	d_U	16 進表記	dU = 0491 . . . ed01
		pU	Party U の素数 p_U	p_U	16 進表記	pU = c24b . . . 71ef
		qU	Party U の素数 q_U	q_U	16 進表記	qU = bc78 . . . 8381
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = b2c9 . . . cf9f
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
		dV	Party V のプライベート鍵指数 d_V	d_V	16 進表記	dV = 11ef . . . 8be9
		pV	Party V の素数 p_V	p_V	16 進表記	pV = edd1 . . . 229d
		qV	Party V の素数 q_V	q_V	16 進表記	qV = c074 . . . 386b
	Party U 試験 2 KAS2-Party_V-confirmation 本体 *5	COUNT	0 以上 NumberOfDKM 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CU	Party U の暗号文	C_U	16 進表記	CU = 812a . . . 0814
		ZU	C_U の生成に使用した secret value Z_U	Z_U	16 進表記	ZU = 6065 . . . ad19
		CV	Party V が生成した暗号文	C_V	16 進表記	CV = 0ccb . . . ed0d
		ZV	C_V の生成に使用した secret value Z_V	Z_V	16 進表記	ZV = 457f . . . e64b
		MacDataV	MacDataV	$MacData_V$	16 進表記	MacDataV = 4b43 . . . 0814
		MacTagV	MacTagV	$MacTag_V$	16 進表記	MacTagV = 262c . . . 7c6d
		KeyData	Party U が導出した $KeyData$	$KeyData$	16 進表記	KeyData = 03bf . . . 7bd6
		Result	鍵確立の成功又は失敗 (成功:P, 失敗:F)		文字列	Result = P
	Party U 試験 3 ヘッダ	nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = 8f0a . . . b66f
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		dU	Party U のプライベート鍵指数 d_U	d_U	16 進表記	dU = 0491 . . . ed01
		pU	Party U の素数 p_U	p_U	16 進表記	pU = c24b . . . 71ef
		qU	Party U の素数 q_U	q_U	16 進表記	qU = bc78 . . . 8381
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = b2c9 . . . cf9f
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
		dV	Party V のプライベート鍵指数 d_V	d_V	16 進表記	dV = 11ef . . . 8be9
		pV	Party V の素数 p_V	p_V	16 進表記	pV = edd1 . . . 229d
		qV	Party V の素数 q_V	q_V	16 進表記	qV = c074 . . . 386b
	Party U 試験 3 本体 *6	COUNT	0 以上 NumberOfDKM 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CU	Party U の暗号文	C_U	16 進表記	CU = 1d10 . . . de15

table continued on next page

continued from previous page

機能	分類	タグ	内容	暗号アルゴリズム実装試験仕様書 ―鍵確立手法― 上の表記との対応	値の表記	例示
		ZU	C_U の生成に使用した secret value Z_U	Z_U	16 進表記	ZU = 457f . . . e64b
		CV	Party V が生成した暗号文	C_V	16 進表記	CV = 1d10 . . . de15
		ZV	C_V の生成に使用した secret value Z_V	Z_V	16 進表記	ZV = 457f . . . e64b
		MacDataU	MacDataU	$MacData_U$	16 進表記	MacDataU = 4b43 . . . a317
		MacDataV	MacDataV	$MacData_V$	16 進表記	MacDataV = 4b43 . . . 0345
		MacTagV	MacTagV	$MacTag_V$	16 進表記	MacTagV = 5610 . . . 9131
		KeyData	Party U が導出した $KeyData$	$KeyData$	16 進表記	KeyData = 6da2 . . . a130
		MacTagU	Party U が計算した MacTag	$MacTag_U$	16 進表記	MacTagU = ade5 . . . 26c9
		Result	鍵確立の成功又は失敗 (成功:P, 失敗:F)		文字列	Result = P
	Party V 試験 1 ヘッダ *1	nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = 8f0a . . . b66f
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		dU	Party U のプライベート鍵指数 d_U	d_U	16 進表記	dU = 0491 . . . ed01
		pU	Party U の素数 p_U	p_U	16 進表記	pU = c24b . . . 71ef
		qU	Party U の素数 q_U	q_U	16 進表記	qU = bc78 . . . 8381
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = b2c9 . . . cf9f
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
		dV	Party V のプライベート鍵指数 d_V	d_V	16 進表記	dV = 11ef . . . 8be9
		pV	Party V の素数 p_V	p_V	16 進表記	pV = edd1 . . . 229d
		qV	Party V の素数 q_V	q_V	16 進表記	qV = c074 . . . 386b
	Party V 試験 1 本体 *7*8	COUNT	0 以上 NumberOfDKM 未満の整数又は 0 以上 NumberOfDKMForRGT 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CU	Party U が生成した暗号文	C_U	16 進表記	CU = 54ae . . . 1201
		ZU	Party U が C_U の生成に使用した secret value Z_U	Z_U	16 進表記	ZU = 0003 . . . e7f2
		Result	鍵確立の成功又は失敗 (C_U が仕様を満たさない場合:F, それ以外は P)		文字列	Result = P
	Party V 試験 2 KAS2-Party_U-confirmation ヘッダ	nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = 8f0a . . . b66f
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		dU	Party U のプライベート鍵指数 d_U	d_U	16 進表記	dU = 0491 . . . ed01
		pU	Party U の素数 p_U	p_U	16 進表記	pU = c24b . . . 71ef
		qU	Party U の素数 q_U	q_U	16 進表記	qU = bc78 . . . 8381
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = b2c9 . . . cf9f
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
		dV	Party V のプライベート鍵指数 d_V	d_V	16 進表記	dV = 11ef . . . 8be9
		pV	Party V の素数 p_V	p_V	16 進表記	pV = edd1 . . . 229d
		qV	Party V の素数 q_V	q_V	16 進表記	qV = c074 . . . 386b
	Party V 試験 2 KAS2-Party_U-confirmation 本体 *9	COUNT	0 以上 NumberOfDKM 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CU	Party U が生成した暗号文	C_U	16 進表記	CU = 1d10 . . . de15
		ZU	C_U の生成に使用した secret value Z_U	Z_U	16 進表記	ZU = 457f . . . e64b
		CV	Party V の暗号文	C_V	16 進表記	CV = 1d10 . . . de15
		ZV	C_V の生成に使用した secret value Z_V	Z_V	16 進表記	ZV = 457f . . . e64b
		MacDataU	MacDataV	$MacData_U$	16 進表記	MacDataU = 4b43 . . . de15
		MacTagU	MacTagU	$MacTag_U$	16 進表記	MacTagU = 9d6e . . . ae0d
		KeyData	Party V が導出した $KeyData$	$KeyData$	16 進表記	KeyData = 03bf . . . 7bd6
		Result	鍵確立の成功又は失敗 (成功:P, 失敗:F)		文字列	Result = P
	Party V 試験 2 KAS2-Party_V-confirmation ヘッダ	nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = 8f0a . . . b66f
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		dU	Party U のプライベート鍵指数 d_U	d_U	16 進表記	dU = 0491 . . . ed01
		pU	Party U の素数 p_U	p_U	16 進表記	pU = c24b . . . 71ef
		qU	Party U の素数 q_U	q_U	16 進表記	qU = bc78 . . . 8381
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = b2c9 . . . cf9f
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
		dV	Party V のプライベート鍵指数 d_V	d_V	16 進表記	dV = 11ef . . . 8be9
		pV	Party V の素数 p_V	p_V	16 進表記	pV = edd1 . . . 229d
		qV	Party V の素数 q_V	q_V	16 進表記	qV = c074 . . . 386b
	Party V 試験 2 KAS2-Party_V-confirmation 本体 *10	COUNT	0 以上 NumberOfDKM 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CU	Party U が生成した暗号文	C_U	16 進表記	CU = 1d10 . . . de15
		ZU	Party U が C_U の生成に使用した secret value Z_U	Z_U	16 進表記	ZU = 457f . . . e64b
	Party V 試験 3 ヘッダ	nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = 8f0a . . . b66f
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		dU	Party U のプライベート鍵指数 d_U	d_U	16 進表記	dU = 0491 . . . ed01
		pU	Party U の素数 p_U	p_U	16 進表記	pU = c24b . . . 71ef
		qU	Party U の素数 q_U	q_U	16 進表記	qU = bc78 . . . 8381
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = b2c9 . . . cf9f
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
		dV	Party V のプライベート鍵指数 d_V	d_V	16 進表記	dV = 11ef . . . 8be9
		pV	Party V の素数 p_V	p_V	16 進表記	pV = edd1 . . . 229d
		qV	Party V の素数 q_V	q_V	16 進表記	qV = c074 . . . 386b
	Party U 試験 3 本体 *11	COUNT	0 以上 NumberOfDKM 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CU	Party U が生成した暗号文	C_U	16 進表記	CU = 1d10 . . . de15
		ZU	C_U の生成に使用した secret value Z_U	Z_U	16 進表記	ZU = 457f . . . e64b
		CV	Party V の暗号文	C_V	16 進表記	CV = 1d10 . . . de15
		ZV	C_V の生成に使用した secret value Z_V	Z_V	16 進表記	ZV = 457f . . . e64b
		MacDataU	MacDataU	$MacData_U$	16 進表記	MacDataU = 4b43 . . . de15
		MacTagU	MacTagU	$MacTag_U$	16 進表記	MacTagU = 9d6e . . . ae0d
		MacDataV	MacDataV	$MacData_V$	16 進表記	MacDataV = 4b43 . . . de15
		KeyData	Party V が導出した $KeyData$	$KeyData$	16 進表記	KeyData = 6da2 . . . a130
		MacTagV	Party V が計算した MacTag	$MacTag_V$	16 進表記	MacTagV = ade5 . . . 26c9
		Result	鍵確立の成功又は失敗 (成功:P, 失敗:F)		文字列	Result = P

*1 試験 1 の各部分集合に対して, 1 セットずつ, 本体の直前にヘッダが出力される. NumberOfTestSubsets = 2 の場合には, 計 2 セットのヘッダが出力されることになる.
*2 試験 1 の部分集合として, NumberOfDKM 組の各データを以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = 0 に対応する暗号文 C_V を記述する.
ZV = abf7 ... 52ba                 ♯ i = 0 に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
Result = P                         ♯ i = 0 に対応する, 鍵確立の成功又は失敗の期待値を記述する.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = 1 に対応する暗号文 C_V を記述する.
ZV = abf7 ... 52ba                 ♯ i = 1 に対応, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
Result = P                         ♯ i = 1 に対応する, 鍵確立の成功又は失敗の期待値を記述する.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
ZV = abf7 ... 52ba                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
Result = P                         ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, 鍵確立の成功又は失敗の期待値を記述する.
```

∗3 NumberOfDKM 組のデータに引き続き, 試験 1 の部分集合として, NumberOfDKMForRGT 組の各データを以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = 0 に対応する暗号文 C_V を記述する.
ZV = abf7 ... 52ba                 ♯ i = 0 に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
Result = P                         ♯ i = 0 に対応する, 鍵確立の成功又は失敗の期待値を記述する.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = 1 に対応する暗号文 C_V を記述する.
ZV = abf7 ... 52ba                 ♯ i = 1 に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
Result = P                         ♯ i = 1 に対応する, 鍵確立の成功又は失敗の期待値を記述する.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
ZV = abf7 ... 52ba                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
Result = P                         ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, 鍵確立の成功又は失敗の期待値を記述する.
```

∗4 NumberOfDKM 個の各データの組を以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = 0 に対応する暗号文 C_V を記述する.
ZV = 457f ... e64b                 ♯ i = 0 に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = 1 に対応する暗号文 C_V を記述する.
ZV = 457f ... e64b                 ♯ i = 1 に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
ZV = 457f ... e64b                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
```

∗5 NumberOfDKM 個の各データの組を以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 812a ... 0814                 ♯ i = 0 に対応する暗号文 C_U を記述する.
ZU = 6065 ... ad19                 ♯ i = 0 に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = 0 に対応する暗号文 C_V を記述する.
ZV = 3bb8 ... cd3b                 ♯ i = 0 に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
MacDataV = 4b43 ... 0814           ♯ i = 0 に対応する, MacTag_V の生成に用いた MacData を記述する.
MacTagV = 262c ... 7c6d            ♯ i = 0 に対応する, MacTag_V を記述する.
KeyData = 985a ... 6ea2            ♯ i = 0 に対応する, KeyData の期待値を記述する.
Result = P                         ♯ i = 0 に対応する, 鍵確立の成功又は失敗の期待値を記述する.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 812a ... 0814                 ♯ i = 1 に対応する暗号文 C_U を記述する.
ZU = 6065 ... ad19                 ♯ i = 1 に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = 1 に対応する暗号文 C_V を記述する.
ZV = 3bb8 ... cd3b                 ♯ i = 1 に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
MacDataV = 4b43 ... 0814           ♯ i = 1 に対応する, MacTag_V の生成に用いた MacData を記述する.
MacTagV = 262c ... 7c6d            ♯ i = 1 に対応する, MacTag_V を記述する.
KeyData = 985a ... 6ea2            ♯ i = 1 に対応する, KeyData の期待値を記述する.
Result = P                         ♯ i = 1 に対応する, 鍵確立の成功又は失敗の期待値を記述する.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 812a ... 0814                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
ZU = 6065 ... ad19                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
ZV = 3bb8 ... cd3b                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
MacDataV = 4b43 ... 0814           ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_V の生成に用いた MacData を記述する.
MacTagV = 262c ... 7c6d            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_V を記述する.
KeyData = 985a ... 6ea2            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, KeyData の期待値を記述する.
Result = P                         ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, 鍵確立の成功又は失敗の期待値を記述する.
```

∗6 NumberOfDKM 個の各データの組を以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 812a ... 0814                 ♯ i = 0 に対応する暗号文 C_U を記述する.
ZU = 6065 ... ad19                 ♯ i = 0 に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = 0 に対応する暗号文 C_V を記述する.
ZV = 3bb8 ... cd3b                 ♯ i = 0 に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
MacDataU = 4b43 ... a317           ♯ i = 0 に対応する, MacTag_U の生成に用いる MacData_U を記述する.
MacDataV = 4b43 ... 0345           ♯ i = 0 に対応する, MacTag_V の生成に用いた MacData_V を記述する.
MacTagV = 5610 ... 9131            ♯ i = 0 に対応する, MacTag_V を記述する.
KeyData = 985a ... 6ea2            ♯ i = 0 に対応する, KeyData の期待値を記述する.
MacTagU = b376 ... ce24            ♯ i = 0 に対応する, MacTag_U の期待値を記述する.
Result = P                         ♯ i = 0 に対応する, 鍵確立の成功又は失敗の期待値を記述する.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 812a ... 0814                 ♯ i = 1 に対応する暗号文 C_U を記述する.
ZU = 6065 ... ad19                 ♯ i = 1 に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = 1 に対応する暗号文 C_V を記述する.
ZV = 3bb8 ... cd3b                 ♯ i = 1 に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
MacDataU = 4b43 ... a317           ♯ i = 1 に対応する, MacTag_U の生成に用いる MacData_U を記述する.
MacDataV = 4b43 ... 0345           ♯ i = 1 に対応する, MacTag_V の生成に用いた MacData_V を記述する.
MacTagV = 5610 ... 9131            ♯ i = 1 に対応する, MacTag_V を記述する.
KeyData = 985a ... 6ea2            ♯ i = 1 に対応する, KeyData の期待値を記述する.
MacTagU = b376 ... ce24            ♯ i = 1 に対応する, MacTag_U の期待値を記述する.
Result = P                         ♯ i = 1 に対応する, 鍵確立の成功又は失敗の期待値を記述する.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 812a ... 0814                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
ZU = 6065 ... ad19                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
ZV = 3bb8 ... cd3b                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
MacDataU = 4b43 ... a317           ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_U の生成に用いる MacData_U を記述する.
MacDataV = 4b43 ... 0345           ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_V の生成に用いた MacData_V を記述する.
MacTagV = 5610 ... 9131            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_V を記述する.
KeyData = 985a ... 6ea2            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, KeyData の期待値を記述する.
MacTagU = b376 ... ce24            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_U の期待値を記述する.
Result = P                         ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, 鍵確立の成功又は失敗の期待値を記述する.
```

∗7 試験 1 の部分集合として, NumberOfDKM 組の各データを以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                 ♯ i = 0 に対応する暗号文 C_U を記述する.
ZU = abf7 ... 52ba                 ♯ i = 0 に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
Result = P                         ♯ i = 0 に対応する, 鍵確立の成功又は失敗の期待値を記述する.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                 ♯ i = 1 に対応する暗号文 C_U を記述する.
ZU = abf7 ... 52ba                 ♯ i = 1 に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
Result = P                         ♯ i = 1 に対応する, 鍵確立の成功又は失敗の期待値を記述する.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
ZU = abf7 ... 52ba                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
Result = P                         ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, 鍵確立の成功又は失敗の期待値を記述する.
```

∗8 NumberOfDKM 組のデータに引き続き, 試験 1 の部分集合として, NumberOfDKMForRGT 組の各データを以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                 ♯ i = 0 に対応する暗号文 C_U を記述する.
ZU = abf7 ... 52ba                 ♯ i = 0 に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
Result = P                         ♯ i = 0 に対応する, 鍵確立の成功又は失敗の期待値を記述する.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                 ♯ i = 1 に対応する暗号文 C_U を記述する.
ZU = abf7 ... 52ba                 ♯ i = 1 に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
Result = P                         ♯ i = 1 に対応する, 鍵確立の成功又は失敗の期待値を記述する.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
ZU = abf7 ... 52ba                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
Result = P                         ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, 鍵確立の成功又は失敗の期待値を記述する.
```

∗9 NumberOfDKM 個の各データの組を以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                 ♯ i = 0 に対応する暗号文 C_U を記述する.
ZU = 3bb8 ... cd3b                 ♯ i = 0 に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
CV = 812a ... 0814                 ♯ i = 0 に対応する暗号文 C_V を記述する.
ZV = 6065 ... ad19                 ♯ i = 0 に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
MacDataU = 4b43 ... 0814           ♯ i = 0 に対応する, MacTag_U の生成に用いた MacData を記述する.
MacTagU = 262c ... 7c6d            ♯ i = 0 に対応する, MacTag_U を記述する.
KeyData = 985a ... 6ea2            ♯ i = 0 に対応する, KeyData の期待値を記述する.
Result = P                         ♯ i = 0 に対応する, 鍵確立の成功又は失敗の期待値を記述する.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                 ♯ i = 1 に対応する暗号文 C_U を記述する.
ZU = 3bb8 ... cd3b                 ♯ i = 1 に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
CV = 812a ... 0814                 ♯ i = 1 に対応する暗号文 C_V を記述する.
ZV = 6065 ... ad19                 ♯ i = 1 に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
MacDataU = 4b43 ... 0814           ♯ i = 1 に対応する, MacTag_U の生成に用いた MacData を記述する.
MacTagU = 262c ... 7c6d            ♯ i = 1 に対応する, MacTag_U を記述する.
KeyData = 985a ... 6ea2            ♯ i = 1 に対応する, KeyData の期待値を記述する.
Result = P                         ♯ i = 1 に対応する, 鍵確立の成功又は失敗の期待値を記述する.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
ZU = 3bb8 ... cd3b                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
CV = 812a ... 0814                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
ZV = 6065 ... ad19                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
MacDataU = 4b43 ... 0814           ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_U の生成に用いた MacData を記述する.
MacTagU = 262c ... 7c6d            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_U を記述する.
KeyData = 985a ... 6ea2            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, KeyData の期待値を記述する.
Result = P                         ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, 鍵確立の成功又は失敗の期待値を記述する.
```

∗10 NumberOfDKM 個の各データの組を以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                 ♯ i = 0 に対応する暗号文 C_U を記述する.
ZU = 457f ... e64b                 ♯ i = 0 に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                 ♯ i = 1 に対応する暗号文 C_U を記述する.
ZU = 457f ... e64b                 ♯ i = 1 に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
ZU = 457f ... e64b                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
```

∗11 NumberOfDKM 個の各データの組を以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                 ♯ i = 0 に対応する暗号文 C_U を記述する.
ZU = 3bb8 ... cd3b                 ♯ i = 0 に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
CV = 812a ... 0814                 ♯ i = 0 に対応する暗号文 C_V を記述する.
ZV = 6065 ... ad19                 ♯ i = 0 に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
MacDataU = 4b43 ... 0345           ♯ i = 0 に対応する, MacTag_U の生成に用いた MacData_U を記述する.
MacTagU = 5610 ... 9131            ♯ i = 0 に対応する, MacTag_U を記述する.
MacDataV = 4b43 ... a317           ♯ i = 0 に対応する, MacTag_V の生成に用いる MacData_V を記述する.
KeyData = 985a ... 6ea2            ♯ i = 0 に対応する, KeyData の期待値を記述する.
MacTagV = d0b8 ... e55a            ♯ i = 0 に対応する, MacTag_V の期待値を記述する.
Result = P                         ♯ i = 0 に対応する, 鍵確立の成功又は失敗の期待値を記述する.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                 ♯ i = 1 に対応する暗号文 C_U を記述する.
ZU = 3bb8 ... cd3b                 ♯ i = 1 に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
CV = 812a ... 0814                 ♯ i = 1 に対応する暗号文 C_V を記述する.
ZV = 6065 ... ad19                 ♯ i = 1 に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
MacDataU = 4b43 ... 0345           ♯ i = 1 に対応する, MacTag_U の生成に用いた MacData_U を記述する.
MacTagU = 5610 ... 9131            ♯ i = 1 に対応する, MacTag_U を記述する.
MacDataV = 4b43 ... a317           ♯ i = 1 に対応する, MacTag_V の生成に用いる MacData_V を記述する.
KeyData = 985a ... 6ea2            ♯ i = 1 に対応する, KeyData の期待値を記述する.
MacTagV = d0b8 ... e55a            ♯ i = 1 に対応する, MacTag_V の期待値を記述する.
Result = P                         ♯ i = 1 に対応する, 鍵確立の成功又は失敗の期待値を記述する.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
ZU = 3bb8 ... cd3b                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, Party U が暗号文 C_U の生成に用いた secret value Z_U を記述する.
CV = 812a ... 0814                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
ZV = 6065 ... ad19                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, Party V が暗号文 C_V の生成に用いた secret value Z_V を記述する.
MacDataU = 4b43 ... 0345           ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_U の生成に用いた MacData_U を記述する.
MacTagU = 5610 ... 9131            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_U を記述する.
MacDataV = 4b43 ... a317           ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_V の生成に用いる MacData_V を記述する.
KeyData = 985a ... 6ea2            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, KeyData の期待値を記述する.
MacTagV = d0b8 ... e55a            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_V の期待値を記述する.
Result = P                         ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, 鍵確立の成功又は失敗の期待値を記述する.
```

2.1.4 レスポンスファイル (*.rsp)

表7: NIST SP800-56B に記載された KAS2 レスポンスファイル

機能	分類	タグ	内容	暗号アルゴリズム実装試験仕様書 ―鍵確立手法― 上の表記との対応	値の表記	例示
鍵共有	ヘッダ	AlgorithmName	KAS2_in_NIST_SP800_56B		文字列	[AlgorithmName = KAS2_in_NIST_SP800_56B]
		TargetFunction	KeyAgreement		文字列	[TargetFunction = KeyAgreement]
		TargetRole	IUT が担う役割 (Party_U, Party_V)		文字列	[TargetRole = Party_U]
		TypeOfPublicKeyU	Party U の公開鍵指数の種別 (65537:TYPE1, random:TYPE2)		文字列	[TypeOfPublicKeyU = TYPE1]
		TypeOfPrivateKeyU	Party U のプライベート鍵の種別 (CRT なし:TYPE2)		文字列	[TypeOfPrivateKeyU = TYPE2]
		BitLengthOfModulusPartyU	Party U の公開鍵の法 n のビット長		10 進表記	[BitLengthOfModulusPartyU = 3072]
		TypeOfPublicKeyV	Party V の公開鍵指数の種別 (65537:TYPE1, random:TYPE2)		文字列	[TypeOfPublicKeyV = TYPE1]
		TypeOfPrivateKeyV	Party V のプライベート鍵の種別 (CRT なし:TYPE2)		文字列	[TypeOfPrivateKeyV = TYPE2]
		BitLengthOfModulusPartyV	Party V の公開鍵の法 n のビット長		10 進表記	[BitLengthOfModulusPartyV = 3072]
		KDF	鍵導出関数識別子		文字列	[KDF = SP800_56B_5_5_1_KDFConcat_SHA1]
		BitLengthOfSaltForHMACbasedKDF	HMAC ベースの KDF を使用する場合, salt のビット長		10 進表記	[BitLengthOfSaltForHMACbasedKDF = 0]
		BitLengthOfOI	OtherInfo のビット長		10 進表記	[BitLengthOfOI = 384]
		ID_U	Party U の Identifier		16 進表記	[ID_U = a1b2c3d4e5]
		ID_V	Party V の Identifier		16 進表記	[ID_V = 4a434154546964]
		KeyConfirmationSupported	サポートする Key Confirmation のタイプ (• Key Confirmation なし:NoKC, • unilateral key confirmation from party U to party V:Unilateral_U_to_V, • unilateral key confirmation from party V to party U:Unilateral_V_to_U, • bilateral key confirmation:Bilateral)		文字列	[KeyConfirmationSupported = NoKC]
		SelectedTestMethod	暗号アルゴリズム実装試験仕様書―鍵確立手法―の選択された試験項目の番号 (試験 1:1, 試験 2:2, 試験 3:3)		10 進表記	[SelectedTestMethod = 1]
		BitLengthOfDKM	DKM のビット長	$KBits$	10 進表記	[BitLengthOfDKM = 320]
		NumberOfDKM	DKM の個数		10 進表記	[NumberOfDKM = 2048]
		RatioOfInvalidData	鍵確立に失敗するデータの割合. (次の場合は省略: • TargetRole = Party_U かつ Unilateral key confirmation from party U to party V の選択時; • TargetRole = Party_V かつ Unilateral key confirmation from party V to party U の選択時は省略.)		浮動小数点表記	[RatioOfInvalidData = 0.5]
		NumberOfDKMForRGT	KeyConfirmationSupported = NoKC の場合, random generation test において生成する DKM の個数. それ以外は省略		10 進表記	[NumberOfDKMForRGT = 2048]
		NumberOfTestSubsets	KeyConfirmationSupported = NoKC の場合, 試験の部分集合の数. それ以外は省略		10 進表記	[NumberOfTestSubsets = 2]
		MACforKeyConfirmation	KeyConfirmationSupported ≠ NoKC の場合, Key confirmation に使う MAC アルゴリズム. それ以外は省略.		文字列	[MACforKeyConfirmation = HMAC_SHA512]
		BitLengthOfMacKey	KeyConfirmationSupported ≠ NoKC の場合, Key confirmation に使う MacKey のビット長. それ以外は省略.		10 進表記	[BitLengthOfMacKey = 128]
		BitLengthOfMacTag	KeyConfirmationSupported ≠ NoKC の場合, Key confirmation に使う MacTag のビット長. それ以外は省略.		10 進表記	[BitLengthOfMacTag = 512]
	Party U 試験 1 ヘッダ *1	nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = c26f . . . 4dfd
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		dU	Party U のプライベート鍵指数 d_U	d_U	16 進表記	dU = 0d0f . . . f1c1
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = bcde . . . dd5b
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
	Party U 試験 1 本体 *2*3	COUNT	0 以上 NumberOfDKM 未満の整数又は 0 以上 NumberOfDKMForRGT 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CV	Party V が生成した暗号文	C_V	16 進表記	CV = 54ae . . . 1201
		CU	【出力】Party U が生成した暗号文	C_U	16 進表記	CU = abf7 . . . 52ba
		DKM	【出力】Party U が導出した $DerivedKeyingMaterial$	$DerivedKeyingMaterial$ (DKM)	16 進表記	DKM = 4c61 . . . af35
		Result	【出力】鍵確立の成功又は失敗		文字列	Result = P
	Party U 試験 2 KAS2-Party_U-confirmation ヘッダ	nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = c26f . . . 4dfd
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		dU	Party U のプライベート鍵指数 d_U	d_U	16 進表記	dU = 0d0f . . . f1c1
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = bcde . . . dd5b
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
	Party U 試験 2 KAS2-Party_U-confirmation 本体 *4	COUNT	0 以上 NumberOfDKM 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CV	Party V が生成した暗号文	C_V	16 進表記	CV = 1d10 . . . de15
		CU	【出力】Party U が生成した暗号文	C_U	16 進表記	CU = 12df . . . 7d46
		KeyData	【出力】Party U が導出した $KeyData$	$KeyData$	16 進表記	KeyData = b0a7 . . . c0a8
		MacTagU	【出力】Party U が計算した MacTag	$MacTag_U$	16 進表記	MacTagU = b376 . . . ce24
	Party U 試験 2 KAS2-Party_V-confirmation ヘッダ	nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = c26f . . . 4dfd
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		dU	Party U のプライベート鍵指数 d_U	d_U	16 進表記	dU = 0d0f . . . f1c1
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = bcde . . . dd5b
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
	Party U 試験 2 KAS2-Party_V-confirmation 本体 *5	COUNT	0 以上 NumberOfDKM 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CU	Party U の暗号文	C_U	16 進表記	CU = 812a . . . 0814
		CV	Party V が生成した暗号文	C_V	16 進表記	CV = 0ccb . . . ed0d
		MacDataV	MacDataV	$MacData_V$	16 進表記	MacDataV = 4b43 . . . 0814
		MacTagV	MacTagV	$MacTag_V$	16 進表記	MacTagV = 262c . . . 7c6d
		KeyData	【出力】Party U が導出した $KeyData$	$KeyData$	16 進表記	KeyData = 985a . . . 6ea2
		Result	【出力】鍵確立の成功又は失敗		文字列	Result = P
	Party U 試験 3 ヘッダ	nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = c26f . . . 4dfd
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		dU	Party U のプライベート鍵指数 d_U	d_U	16 進表記	dU = 0d0f . . . f1c1
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = bcde . . . dd5b
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
	Party U 試験 3 本体 *6	COUNT	0 以上 NumberOfDKM 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CU	Party U の暗号文	C_U	16 進表記	CU = 1d10 . . . de15
		CV	Party V が生成した暗号文	C_V	16 進表記	CV = 1d10 . . . de15
		MacDataU	MacDataU	$MacData_U$	16 進表記	MacDataU = 4b43 . . . a317
		MacDataV	MacDataV	$MacData_V$	16 進表記	MacDataV = 4b43 . . . 0345
		MacTagV	MacTagV	$MacTag_V$	16 進表記	MacTagV = 5610 . . . 9131
		KeyData	【出力】Party U が導出した $KeyData$	$KeyData$	16 進表記	KeyData = 6da2 . . . a130
		MacTagU	【出力】Party U が計算した MacTag	$MacTag_U$	16 進表記	MacTagU = ade5 . . . 26c9
		Result	【出力】鍵確立の成功又は失敗		文字列	Result = P
	Party V 試験 1 ヘッダ *1	nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = bae1 . . . 56eb
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = 8a53 . . . 9fdf
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
		dV	Party V のプライベート鍵指数 d_V	d_V	16 進表記	dV = 3f27 . . . 546d
	Party V 試験 1 本体 *7*8	COUNT	0 以上 NumberOfDKM 未満の整数又は 0 以上 NumberOfDKMForRGT 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 . . . 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 . . . aee8
		CU	Party U が生成した暗号文	C_U	16 進表記	CU = 54ae . . . 1201
		CV	【出力】Party V が生成する暗号文	C_V	16 進表記	CV = 0ccb . . . ed0d

table continued on next page

continued from previous page

機能	分類	タグ	内容	暗号アルゴリズム実装試験仕様書 ―鍵確立手法― 上の表記との対応	値の表記	例示
		DKM	【出力】Party V が導出した $DerivedKeyingMaterial$	$DerivedKeyingMaterial$ (DKM)	16 進表記	DKM = 9797 ... 08aa
		Result	【出力】鍵確立の成功又は失敗		文字列	Result = P
	Party V 試験 2 KAS2-Party_U-confirmation ヘッダ	nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = bae1 ... 56eb
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = 8a53 ... 9fdf
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
		dV	Party V のプライベート鍵指数 d_V	d_V	16 進表記	dV = 3f27 ... 546d
	Party V 試験 2 KAS2-Party_U-confirmation 本体 *9	COUNT	0 以上 NumberOfDKM 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 ... 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 ... aee8
		CU	Party U が生成した暗号文	C_U	16 進表記	CU = 1d10 ... de15
		CV	Party V の暗号文	C_V	16 進表記	CV = 1d10 ... de15
		MacDataU	MacDataV	$MacData_U$	16 進表記	MacDataU = 4b43 ... de15
		MacTagU	MacTagU	$MacTag_U$	16 進表記	MacTagU = 9d6e ... ae0d
		KeyData	【出力】Party V が導出した $KeyData$	$KeyData$	16 進表記	KeyData = 985a ... 6ea2
		Result	【出力】鍵確立の成功又は失敗		文字列	Result = P
	Party V 試験 2 KAS2-Party_V-confirmation ヘッダ	nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = bae1 ... 56eb
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = 8a53 ... 9fdf
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
		dV	Party V のプライベート鍵指数 d_V	d_V	16 進表記	dV = 3f27 ... 546d
	Party V 試験 2 KAS2-Party_V-confirmation 本体 *10	COUNT	0 以上 NumberOfDKM 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 ... 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 ... aee8
		CU	Party U が生成した暗号文	C_U	16 進表記	CU = 1d10 ... de15
		CV	【出力】Party V が生成した暗号文	C_V	16 進表記	CV = 0ccb ... ed0d
		KeyData	【出力】Party V が導出した $KeyData$	$KeyData$	16 進表記	KeyData = 985a ... 6ea2
		MacTagV	【出力】Party V が計算した MacTag	$MacTag_V$	16 進表記	MacTagV = d0b8 ... e55a
	Party V 試験 3 ヘッダ	nU	Party U の公開鍵の法 n_U	n_U	16 進表記	nU = bae1 ... 56eb
		eU	Party U の公開鍵指数 e_U	e_U	16 進表記	eU = 010001
		nV	Party V の公開鍵の法 n_V	n_V	16 進表記	nV = 8a53 ... 9fdf
		eV	Party V の公開鍵指数 e_V	e_V	16 進表記	eV = 010001
		dV	Party V のプライベート鍵指数 d_V	d_V	16 進表記	dV = 3f27 ... 546d
	Party U 試験 3 本体 *11	COUNT	0 以上 NumberOfDKM 未満の整数		10 進表記	COUNT = 0
		OI	OtherInfo	$OtherInfo$	16 進表記	OI = a1b2 ... 0e21
		SaltForHMACbasedKDF	HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt. それ以外は省略.	$salt$	16 進表記	SaltForHMACbasedKDF = eb22 ... aee8
		CU	Party U が生成した暗号文	C_U	16 進表記	CU = 1d10 ... de15
		CV	Party V の暗号文	C_V	16 進表記	CV = 1d10 ... de15
		MacDataU	MacDataU	$MacData_U$	16 進表記	MacDataU = 4b43 ... de15
		MacTagU	MacTagU	$MacTag_U$	16 進表記	MacTagU = 9d6e ... ae0d
		MacDataV	MacDataV	$MacData_V$	16 進表記	MacDataV = 4b43 ... de15
		KeyData	【出力】Party V が導出した $KeyData$	$KeyData$	16 進表記	KeyData = 6da2 ... a130
		MacTagV	【出力】Party V が計算した MacTag	$MacTag_V$	16 進表記	MacTagV = ade5 ... 26c9
		Result	【出力】鍵確立の成功又は失敗 (成功:P, 失敗:F)		文字列	Result = P

*1 試験 1 の各部分集合に対して, 1 セットずつ, 本体の直前にヘッダが出力される. NumberOfTestSubsets = 2 の場合には, 計 2 セットのヘッダが出力されることになる.

*2 試験 1 の部分集合として, NumberOfDKM 組の各データを以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = 0 に対応する暗号文 C_V を記述する.
CU = abf7 ... 52ba                 ♯ i = 0 に対応して, IUT が生成した暗号文 C_U.
DKM = 4c61 ... af35                ♯ i = 0 に対応して, IUT が導出した DerivedKeyingMaterial (DKM).
Result = P                         ♯ i = 0 に対応して, IUT が計算した鍵確立の成功又は失敗.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = 1 に対応する暗号文 C_V を記述する.
CU = abf7 ... 52ba                 ♯ i = 1 に対応して, IUT が生成した暗号文 C_U.
DKM = 4c61 ... af35                ♯ i = 1 に対応して, IUT が導出した DerivedKeyingMaterial (DKM).
Result = P                         ♯ i = 1 に対応して, IUT が計算した鍵確立の成功又は失敗.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
CU = abf7 ... 52ba                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が生成した暗号文 C_U.
DKM = 4c61 ... af35                ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が導出した DerivedKeyingMaterial (DKM).
Result = P                         ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が計算した鍵確立の成功又は失敗.
```

*3 NumberOfDKM 組のデータに引き続き, 試験 1 の部分集合として, NumberOfDKMForRGT 組の各データを以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = 0 に対応する暗号文 C_V を記述する.
CU = abf7 ... 52ba                 ♯ i = 0 に対応して, IUT が生成した暗号文 C_U.
DKM = 4c61 ... af35                ♯ i = 0 に対応して, IUT が導出した DerivedKeyingMaterial (DKM).
Result = P                         ♯ i = 0 に対応して, IUT が計算した鍵確立の成功又は失敗.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = 1 に対応する暗号文 C_V を記述する.
CU = abf7 ... 52ba                 ♯ i = 1 に対応して, IUT が生成した暗号文 C_U.
DKM = 4c61 ... af35                ♯ i = 1 に対応して, IUT が導出した DerivedKeyingMaterial (DKM).
Result = P                         ♯ i = 1 に対応して, IUT が計算した鍵確立の成功又は失敗.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
CU = abf7 ... 52ba                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が生成した暗号文 C_U.
DKM = 4c61 ... af35                ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が導出した DerivedKeyingMaterial (DKM).
Result = P                         ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が計算した鍵確立の成功又は失敗.
```

*4 NumberOfDKM 個の各データの組を以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = 0 に対応する暗号文 C_V を記述する.
CU = 12df ... 7d46                 ♯ i = 0 に対応して, IUT が生成した暗号文 C_U.
KeyData = b0a7 ... c0a8            ♯ i = 0 に対応して, IUT が導出した KeyData.
MacTagU = b376 ... ce24            ♯ i = 0 に対応して, IUT が計算した MacTag_U.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = 1 に対応する暗号文 C_V を記述する.
CU = 12df ... 7d46                 ♯ i = 1 に対応して, IUT が生成した暗号文 C_U.
KeyData = 985a ... 6ea2            ♯ i = 1 に対応して, IUT が導出した KeyData.
MacTagU = b376 ... ce24            ♯ i = 1 に対応して, IUT が計算した MacTag_U.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CV = 54ae ... 1201                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
CU = 12df ... 7d46                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が生成した暗号文 C_U.
KeyData = 985a ... 6ea2            ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が導出した KeyData.
MacTagU = b376 ... ce24            ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が計算した MacTag_U.
```

∗5 NumberOfDKM 個の各データの組を以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 812a ... 0814                 ♯ i = 0 に対応する暗号文 C_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = 0 に対応する暗号文 C_V を記述する.
MacDataV = 4b43 ... 0814           ♯ i = 0 に対応する, MacTag_V の生成に用いた MacData を記述する.
MacTagV = 262c ... 7c6d            ♯ i = 0 に対応する, MacTag_V を記述する.
KeyData = 985a ... 6ea2            ♯ i = 0 に対応して, IUT が導出した KeyData.
Result = P                         ♯ i = 0 に対応して, IUT が計算した鍵確立の成功又は失敗.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 812a ... 0814                 ♯ i = 1 に対応する暗号文 C_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = 1 に対応する暗号文 C_V を記述する.
MacDataV = 4b43 ... 0814           ♯ i = 1 に対応する, MacTag_V の生成に用いた MacData を記述する.
MacTagV = 262c ... 7c6d            ♯ i = 1 に対応する, MacTag_V を記述する.
KeyData = 985a ... 6ea2            ♯ i = 1 に対応して, IUT が導出した KeyData.
Result = P                         ♯ i = 1 に対応して, IUT が計算した鍵確立の成功又は失敗.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 812a ... 0814                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
MacDataV = 4b43 ... 0814           ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_V の生成に用いた MacData を記述する.
MacTagV = 262c ... 7c6d            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_V を記述する.
KeyData = 985a ... 6ea2            ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が導出した KeyData.
Result = P                         ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が計算した鍵確立の成功又は失敗.
```

∗6 NumberOfDKM 個の各データの組を以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 812a ... 0814                 ♯ i = 0 に対応する暗号文 C_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = 0 に対応する暗号文 C_V を記述する.
MacDataU = 4b43 ... a317           ♯ i = 0 に対応する, MacTag_U の生成に用いる MacData_U を記述する.
MacDataV = 4b43 ... 0345           ♯ i = 0 に対応する, MacTag_V の生成に用いた MacData_V を記述する.
MacTagV = 5610 ... 9131            ♯ i = 0 に対応する, MacTag_V を記述する.
KeyData = 985a ... 6ea2            ♯ i = 0 に対応して, IUT が導出した KeyData.
MacTagU = b376 ... ce24            ♯ i = 0 に対応して, IUT が計算した MacTag_U.
Result = P                         ♯ i = 0 に対応して, IUT が計算した鍵確立の成功又は失敗.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 812a ... 0814                 ♯ i = 1 に対応する暗号文 C_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = 1 に対応する暗号文 C_V を記述する.
MacDataU = 4b43 ... a317           ♯ i = 1 に対応する, MacTag_U の生成に用いる MacData_U を記述する.
MacDataV = 4b43 ... 0345           ♯ i = 1 に対応する, MacTag_V の生成に用いた MacData_V を記述する.
MacTagV = 5610 ... 9131            ♯ i = 1 に対応する, MacTag_V を記述する.
KeyData = 985a ... 6ea2            ♯ i = 1 に対応して, IUT が導出した KeyData.
MacTagU = b376 ... ce24            ♯ i = 1 に対応して, IUT が計算した MacTag_U.
Result = P                         ♯ i = 1 に対応して, IUT が計算した鍵確立の成功又は失敗.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 812a ... 0814                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
MacDataU = 4b43 ... a317           ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_U の生成に用いる MacData_U を記述する.
MacDataV = 4b43 ... 0345           ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_V の生成に用いた MacData_V を記述する.
MacTagV = 5610 ... 9131            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_V を記述する.
KeyData = 985a ... 6ea2            ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が導出した KeyData.
MacTagU = b376 ... ce24            ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が計算した MacTag_U.
Result = P                         ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が計算した鍵確立の成功又は失敗.
```

∗7 試験 1 の部分集合として, NumberOfDKM 組の各データを以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                 ♯ i = 0 に対応する暗号文 C_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = 0 に対応して, IUT が生成した暗号文 C_V.
DKM = 9797 ... 08aa                ♯ i = 0 に対応して, IUT が導出した DerivedKeyingMaterial (DKM).

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                 ♯ i = 1 に対応する暗号文 C_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = 1 に対応して, IUT が生成した暗号文 C_V.
DKM = 9797 ... 08aa                ♯ i = 1 に対応して, IUT が導出した DerivedKeyingMaterial (DKM).
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が生成した暗号文 C_V.
DKM = 9797 ... 08aa                ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が導出した DerivedKeyingMaterial (DKM).
```

∗8 NumberOfDKM 組のデータに引き続き, 試験 1 の部分集合として, NumberOfDKMForRGT 組の各データを以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                 ♯ i = 0 に対応する暗号文 C_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = 0 に対応して, IUT が生成した暗号文 C_V.
DKM = 9797 ... 08aa                ♯ i = 0 に対応して, IUT が導出した DerivedKeyingMaterial (DKM).

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                 ♯ i = 1 に対応する暗号文 C_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = 1 に対応して, IUT が生成した暗号文 C_V.
DKM = 9797 ... 08aa                ♯ i = 1 に対応して, IUT が導出した DerivedKeyingMaterial (DKM).
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が生成した暗号文 C_V.
DKM = 9797 ... 08aa                ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が導出した DerivedKeyingMaterial (DKM).
```

∗9 NumberOfDKM 個の各データの組を以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                 ♯ i = 0 に対応する暗号文 C_U を記述する.
CV = 812a ... 0814                 ♯ i = 0 に対応する暗号文 C_V を記述する.
MacDataU = 4b43 ... 0814           ♯ i = 0 に対応する, MacTag_U の生成に用いた MacData を記述する.
MacTagU = 262c ... 7c6d            ♯ i = 0 に対応する, MacTag_U を記述する.
KeyData = 985a ... 6ea2            ♯ i = 0 に対応して, IUT が導出した KeyData.
Result = P                         ♯ i = 0 に対応して, IUT が計算した鍵確立の成功又は失敗.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                 ♯ i = 1 に対応する暗号文 C_U を記述する.
CV = 812a ... 0814                 ♯ i = 1 に対応する暗号文 C_V を記述する.
MacDataU = 4b43 ... 0814           ♯ i = 1 に対応する, MacTag_U の生成に用いた MacData を記述する.
MacTagU = 262c ... 7c6d            ♯ i = 1 に対応する, MacTag_U を記述する.
KeyData = 985a ... 6ea2            ♯ i = 1 に対応して, IUT が導出した KeyData.
Result = P                         ♯ i = 1 に対応して, IUT が計算した鍵確立の成功又は失敗.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
CV = 812a ... 0814                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
MacDataU = 4b43 ... 0814           ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_U の生成に用いた MacData を記述する.
MacTagU = 262c ... 7c6d            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_U を記述する.
KeyData = 985a ... 6ea2            ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が導出した KeyData.
Result = P                         ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が計算した鍵確立の成功又は失敗.
```

∗10 NumberOfDKM 個の各データの組を以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                 ♯ i = 0 に対応する暗号文 C_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = 0 に対応して, IUT が生成した暗号文 C_V.
KeyData = 985a ... 6ea2            ♯ i = 0 に対応して, IUT が導出した KeyData.
MacTagV = d0b8 ... e55a            ♯ i = 0 に対応して, IUT が計算した MacTag_V.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                 ♯ i = 1 に対応する暗号文 C_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = 1 に対応して, IUT が生成した暗号文 C_V.
KeyData = 985a ... 6ea2            ♯ i = 1 に対応して, IUT が導出した KeyData.
MacTagV = d0b8 ... e55a            ♯ i = 1 に対応して, IUT が計算した MacTag_V.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 54ae ... 1201                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
CV = 0ccb ... ed0d                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が生成した暗号文 C_V.
KeyData = 985a ... 6ea2            ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が導出した KeyData.
MacTagV = d0b8 ... e55a            ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が計算した MacTag_V.
```

∗11 NumberOfDKM 個の各データの組を以下のように記述する.

```
COUNT = 0                          ♯ i = 0 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 0 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                 ♯ i = 0 に対応する暗号文 C_U を記述する.
CV = 812a ... 0814                 ♯ i = 0 に対応する暗号文 C_V を記述する.
MacDataU = 4b43 ... 0345           ♯ i = 0 に対応する, MacTag_U の生成に用いた MacData_U を記述する.
MacTagU = 5610 ... 9131            ♯ i = 0 に対応する, MacTag_U を記述する.
MacDataV = 4b43 ... a317           ♯ i = 0 に対応する, MacTag_V の生成に用いる MacData_V を記述する.
KeyData = 985a ... 6ea2            ♯ i = 0 に対応して, IUT が導出した KeyData.
MacTagV = d0b8 ... e55a            ♯ i = 0 に対応して, IUT が計算した MacTag_V.
Result = P                         ♯ i = 0 に対応して, IUT が計算した鍵確立の成功又は失敗.

COUNT = 1                          ♯ i = 1 のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = 1 に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                 ♯ i = 1 に対応する暗号文 C_U を記述する.
CV = 812a ... 0814                 ♯ i = 1 に対応する暗号文 C_V を記述する.
MacDataU = 4b43 ... 0345           ♯ i = 1 に対応する, MacTag_U の生成に用いた MacData_U を記述する.
MacTagU = 5610 ... 9131            ♯ i = 1 に対応する, MacTag_U を記述する.
MacDataV = 4b43 ... a317           ♯ i = 1 に対応する, MacTag_V の生成に用いる MacData_V を記述する.
KeyData = 985a ... 6ea2            ♯ i = 1 に対応して, IUT が導出した KeyData.
MacTagV = d0b8 ... e55a            ♯ i = 1 に対応して, IUT が計算した MacTag_V.
Result = P                         ♯ i = 1 に対応して, IUT が計算した鍵確立の成功又は失敗.
⋮
COUNT = ⟨NumberOfDKM − 1⟩          ♯ i = ⟨NumberOfDKM − 1⟩ のデータの組について記述する.
OI = a1b2 ... 0e21                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する OtherInfo を記述する.
SaltForHMACbasedKDF = eb22 ... aee8  ♯ HMAC を用いる鍵導出関数の選択時, HMAC の鍵として用いられる salt を記述する. それ以外は省略.
CU = 0ccb ... ed0d                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_U を記述する.
CV = 812a ... 0814                 ♯ i = ⟨NumberOfDKM − 1⟩ に対応する暗号文 C_V を記述する.
MacDataU = 4b43 ... 0345           ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_U の生成に用いた MacData_U を記述する.
MacTagU = 5610 ... 9131            ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_U を記述する.
MacDataV = 4b43 ... a317           ♯ i = ⟨NumberOfDKM − 1⟩ に対応する, MacTag_V の生成に用いる MacData_V を記述する.
KeyData = 985a ... 6ea2            ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が導出した KeyData.
MacTagV = d0b8 ... e55a            ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が計算した MacTag_V.
Result = P                         ♯ i = ⟨NumberOfDKM − 1⟩ に対応して, IUT が計算した鍵確立の成功又は失敗.
```

2.1.5 結果ファイル (*.out)

表8: NIST SP800-56B に記載された KAS2 結果ファイル

機能	分類	タグ	内容	値の表記	例示
鍵共有	ヘッダ	AlgorithmName	KAS2_in_NIST_SP800_56B	文字列	[AlgorithmName = KAS2_in_NIST_SP800_56B]
		TargetFunction	KeyAgreement	文字列	[TargetFunction = KeyAgreement]
		TargetRole	IUT が担う役割 (Party_U, Party_V)	文字列	[TargetRole = Party_U]
		TypeOfPublicKeyU	Party U の公開鍵指数の種別 (65537:TYPE1, random:TYPE2)	文字列	[TypeOfPublicKeyU = TYPE1]
		TypeOfPrivateKeyU	Party U のプライベート鍵の種別 (CRT なし:TYPE2)	文字列	[TypeOfPrivateKeyU = TYPE2]
		BitLengthOfModulusPartyU	Party U の公開鍵の法 n のビット長	10 進表記	[BitLengthOfModulusPartyU = 3072]
		TypeOfPublicKeyV	Party V の公開鍵指数の種別 (65537:TYPE1, random:TYPE2)	文字列	[TypeOfPublicKeyV = TYPE1]
		TypeOfPrivateKeyV	Party V のプライベート鍵の種別 (CRT なし:TYPE2)	文字列	[TypeOfPrivateKeyV = TYPE2]
		BitLengthOfModulusPartyV	Party V の公開鍵の法 n のビット長	10 進表記	[BitLengthOfModulusPartyV = 3072]
		KDF	鍵導出関数識別子	文字列	[KDF = SP800_56B_5_5_1_KDFConcat_SHA1]
		BitLengthOfSaltForHMACbasedKDF	HMAC ベースの KDF を使用する場合, salt のビット長	10 進表記	[BitLengthOfSaltForHMACbasedKDF = 0]
		BitLengthOfOI	OtherInfo のビット長	10 進表記	[BitLengthOfOI = 384]
		ID_U	Party U の Identifier	16 進表記	[ID_U = a1b2c3d4e5]
		ID_V	Party V の Identifier	16 進表記	[ID_V = 4a434154546964]
		KeyConfirmationSupported	サポートする Key Confirmation のタイプ (• Key Confirmation なし:NoKC, • unilateral key confirmation from party U to party V:Unilateral_U_to_V, • unilateral key confirmation from party V to party U:Unilateral_V_to_U, • bilateral key confirmation:Bilateral)	文字列	[KeyConfirmationSupported = NoKC]
		SelectedTestMethod	暗号アルゴリズム実装試験仕様書—鍵確立手法—の選択された試験項目の番号 (試験 1:1, 試験 2:2, 試験 3:3)	10 進表記	[SelectedTestMethod = 1]
		BitLengthOfDKM	DKM のビット長	10 進表記	[BitLengthOfDKM = 320]
		NumberOfDKM	DKM の個数	10 進表記	[NumberOfDKM = 2048]
		RatioOfInvalidData	鍵確立に失敗するデータの割合. (次の場合は省略: • TargetRole = Party_U かつ Unilateral key confirmation from party U to party V の選択時; • TargetRole = Party_V かつ Unilateral key confirmation from party V to party U の選択時は省略.)	浮動小数点表記	[RatioOfInvalidData = 0.5]
		NumberOfDKMForRGT	KeyConfirmationSupported = NoKC の場合, random generation test において生成する DKM の個数. それ以外は省略	10 進表記	[NumberOfDKMForRGT = 2048]
		NumberOfTestSubsets	KeyConfirmationSupported = NoKC の場合, 試験の部分集合の数. それ以外は省略	10 進表記	[NumberOfTestSubsets = 2]
		MACforKeyConfirmation	KeyConfirmationSupported ≠ NoKC の場合, Key confirmation に使う MAC アルゴリズム. それ以外は省略.	文字列	[MACforKeyConfirmation = HMAC_SHA512]
		BitLengthOfMacKey	KeyConfirmationSupported ≠ NoKC の場合, Key confirmation に使う MacKey のビット長. それ以外は省略.	10 進表記	[BitLengthOfMacKey = 128]
		BitLengthOfMacTag	KeyConfirmationSupported ≠ NoKC の場合, Key confirmation に使う MacTag のビット長. それ以外は省略.	10 進表記	[BitLengthOfMacTag = 512]
		⟨ Results ⟩	OK 又は NG	文字列	OK

注

- 試験合格の場合，⟨ Results ⟩ に OK と表示される．
- 試験不合格の場合，⟨ Results ⟩ に何らかの形式で NG と表示される．また，⟨ Results ⟩ には，レスポンスファイル内の不合格となったデータが記述されている何番目 (COUNT，# 等の記号で番号を表す) のデータが不合格となったかが表示される．不合格となったデータが記述されているタグ名は，前記のレスポンスファイル仕様に【出力】と記述したタグである．ただし，【出力】と記述したタグが 1 つしかない場合，タグ名は省略することがある．