JCATT ファイルフォーマット仕様書

NIST SP800-132 に記載された PBKDF

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 SP800-132 に記載された PBKDF

PBKDF in NIST SP 800-132 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，PBKDF_in_NIST_SP800_132.
各表において，試験方法に関する以下の略語を使用する．

- PRF: Pseudorandom Function

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, PRF 識別子として, 表1に記載された表現を用いる．

表1　PRF 識別子

PRF 識別子	対応する PRF
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`

2.1.1　パラメータファイル (*.par)

表2　NIST SP800-132 に記載された PBKDF パラメータファイル

機能	タグ		内容	表記
鍵導出関数	ヘッダ	`AlgorithmName`	PBKDF_in_NIST_SP800_132	文字列
		`PRF`	(PRF 識別子)	文字列
		`IterationCountC`	C の値	10 進
		`kLenDivisibleBy8`	8 の倍数の $kLen$ のサポートの有無 (有:True, 無:False)	文字列
		`BitLengthOfPasswordForpLenltB`	B 未満のパスワードのビット長	10 進
		`BitLengthOfPasswordForpLeneqB`	B に等しいパスワードのビット長	10 進
		`BitLengthOfPasswordForpLengtB`	B より大きいパスワードのビット長	10 進
		`BitLengthOfSaltForsLenlthLenMinus32`	$128 \leq \mathbf{len}(S) < (hLen - 32)$ なる Salt S のビット長の代表値	10 進
		`BitLengthOfSaltForsLeneqhLenMinus32`	$\mathbf{len}(S) = (hLen - 32)$ なる Salt S のビット長	10 進
		`BitLengthOfSaltForsLengthLenMinus32`	$\mathbf{len}(S) > (hLen - 32)$ なる Salt S のビット長の代表値	10 進
		`MinkLenDivisibleByhLen`	$hLen$ で割り切れる $kLen$ の, IUT がサポートする範囲の最小値	10 進
		`MaxkLenDivisibleByhLen`	$hLen$ で割り切れる $kLen$ の, IUT がサポートする範囲の最大値	10 進
		`MinkLenDivisibleBy8`	($hLen$ で割り切れない)8 の倍数の $kLen$ の, IUT がサポートする範囲の最小値	10 進
		`MaxkLenDivisibleBy8`	($hLen$ で割り切れない)8 の倍数の $kLen$ の, IUT がサポートする範囲の最大値	10 進
		`NumberOfTestSubsets`	試験の部分集合の数	10 進
		`NumberOfTrialsForEachTestSubset`	試験の各部分集合の中で, 導出する keying material の数	10 進

2.1.2 リクエストファイル (*.req)

表3: NIST SP800-132 に記載された PBKDF 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
鍵導出関数	ヘッダ	AlgorithmName	PBKDF_in_NIST_SP800_132		文字列	[AlgorithmName = PBKDF_in_NIST_SP800_132]
		PRF	PRF 識別子		文字列	[PRF = HMAC_SHA512]
		IterationCountC	Iteration count C	C	10 進表記	[IterationCountC = 1000]
		kLendivisibleBy8	8 の倍数の $kLen$ のサポートの有無 (有:True, 無:False)		文字列	[kLendivisibleBy8 = True]
		BitLengthOfPasswordForpLenltB	B 未満の Password のビット長.		10 進表記	[BitLengthOfPasswordForpLenltB = 256]
		BitLengthOfPasswordForpLeneqB	B に等しい Password のビット長.		10 進表記	[BitLengthOfPasswordForpLeneqB = 1024]
		BitLengthOfPasswordForpLengtB	B より大きい Password のビット長.		10 進表記	[BitLengthOfPasswordForpLengtB = 2048]
		BitLengthOfSaltForsLenlthLenMinus32	$128 \leq \mathbf{len}(S) < (hLen - 32)$ なる Salt S を IUT がサポートする場合, そのビット長の代表値. サポートしない場合, 0.		10 進表記	[BitLengthOfSaltForsLenlthLenMinus32 = 128]
		BitLengthOfSaltForsLeneqhLenMinus32	$\mathbf{len}(S) = (hLen - 32)$ なる Salt S を IUT がサポートする場合, そのビット長.		10 進表記	[BitLengthOfSaltForsLeneqhLenMinus32 = 480]
		BitLengthOfSaltForsLengthLenMinus32	$\mathbf{len}(S) > (hLen - 32)$ なる Salt S を IUT がサポートする場合, そのビット長の代表値.		10 進表記	[BitLengthOfSaltForsLengthLenMinus32 = 512]
		MinkLenDivisibleByhLen	$hLen$ で割り切れる $kLen$ の, IUT がサポートする範囲の最小値		10 進表記	[MinkLenDivisibleByhLen = 512]
		MaxkLenDivisibleByhLen	$hLen$ で割り切れる $kLen$ の, IUT がサポートする範囲の最大値		10 進表記	[MaxkLenDivisibleByhLen = 2048]
		MinkLenDivisibleBy8	($hLen$ で割り切れない)8 の倍数の $kLen$ の, IUT がサポートする範囲の最小値		10 進表記	[MinkLenDivisibleBy8 = 112]
		MaxkLenDivisibleBy8	($hLen$ で割り切れない)8 の倍数の $kLen$ の, IUT がサポートする範囲の最大値		10 進表記	[MaxkLenDivisibleBy8 = 1280]
		NumberOfTestSubsets	試験の部分集合の数		10 進表記	[NumberOfTestSubsets = 12]
		NumberOfTrialsForEachTestSubset	試験の各部分集合の中で, 導出する master key の数		10 進表記	[NumberOfTrialsForEachTestSubset = 10]
	試験部分集合 *1 *2 *3	COUNT	0 以上 NumberOfTrialsForEachTestSubset 未満の整数		10 進表記	COUNT = 0
		kLen	導出する master key (mk) のビット長 ($kLen$)	$kLen$	10 進表記	kLen = 512
		Password	Password (P)	P	16 進表記	Password = 2f9a . . . 3664
		sLen	Salt S のビット長	$\mathbf{len}(S)$	10 進表記	sLen = 256
		Salt	Salt S	S	16 進表記	Salt = ?
		mk	master key (mk)	mk	16 進表記	mk = ?

*1 8 の倍数の $kLen$ のサポートの有無, IUT がサポートする $kLen$ の範囲, 及び IUT がサポートする $sLen$ の範囲の組みあわせに対応して, 最大 36 個の部分集合を記載する.

*2 NumberOfTrialsForEachTestSubset 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.
kLen = 512                                 ♯ i = 0 に対応する kLen を記述する.
Password = e571 ... 519f                   ♯ i = 0 に対応する Password を記述する.
sLen = 256                                 ♯ i = 0 に対応する Salt S のビット長を記述する.
Salt = ?                                   ♯ i = 0 に対応する Salt S のプレースホルダ.
mk = ?                                     ♯ i = 0 に対応する master key mk 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.
kLen = 512                                 ♯ i = 1 に対応する kLen を記述する.
Password = 9f15 ... 4d17                   ♯ i = 1 に対応する Password を記述する.
sLen = 256                                 ♯ i = 1 に対応する Salt S のビット長を記述する.
Salt = ?                                   ♯ i = 1 に対応する Salt S のプレースホルダ.
mk = ?                                     ♯ i = 1 に対応する master key mk のプレースホルダ.
⋮
COUNT = ⟨NumberOfTrialsForEachTestSubset − 1⟩   ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ のデータの組について記述する.
kLen = 512                                 ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する kLen を記述する.
Password = dc6f ... c8f2                   ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する Password を記述する.
sLen = 256                                 ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する Salt S のビット長を記述する.
Salt = ?                                   ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する Salt S のプレースホルダ.
mk = ?                                     ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する master key mk のプレースホルダ.
```

2.1.3 Facts ファイル (*.fax)

表4: NIST SP800-132 に記載された PBKDF 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
鍵導出関数	ヘッダ	AlgorithmName	PBKDF_in_NIST_SP800_132		文字列	[AlgorithmName = PBKDF_in_NIST_SP800_132]
		PRF	PRF 識別子		文字列	[PRF = HMAC_SHA512]
		IterationCountC	Iteration count C	C	10 進表記	[IterationCountC = 1000]
		kLendivisibleBy8	8 の倍数の $kLen$ のサポートの有無 (有:True, 無:False)		文字列	[kLendivisibleBy8 = True]
		BitLengthOfPasswordForpLenltB	B 未満の Password のビット長.		10 進表記	[BitLengthOfPasswordForpLenltB = 256]
		BitLengthOfPasswordForpLeneqB	B に等しい Password のビット長.		10 進表記	[BitLengthOfPasswordForpLeneqB = 1024]
		BitLengthOfPasswordForpLengtB	B より大きい Password のビット長.		10 進表記	[BitLengthOfPasswordForpLengtB = 2048]
		BitLengthOfSaltForsLenlthLenMinus32	$128 \leq \mathbf{len}(S) < (hLen - 32)$ なる Salt S を IUT がサポートする場合, そのビット長の代表値. サポートしない場合, 0.		10 進表記	[BitLengthOfSaltForsLenlthLenMinus32 = 128]
		BitLengthOfSaltForsLeneqhLenMinus32	$\mathbf{len}(S) = (hLen - 32)$ なる Salt S を IUT がサポートする場合, そのビット長.		10 進表記	[BitLengthOfSaltForsLeneqhLenMinus32 = 480]
		BitLengthOfSaltForsLengthLenMinus32	$\mathbf{len}(S) > (hLen - 32)$ なる Salt S を IUT がサポートする場合, そのビット長の代表値.		10 進表記	[BitLengthOfSaltForsLengthLenMinus32 = 512]
		MinkLenDivisibleByhLen	$hLen$ で割り切れる $kLen$ の, IUT がサポートする範囲の最小値		10 進表記	[MinkLenDivisibleByhLen = 512]
		MaxkLenDivisibleByhLen	$hLen$ で割り切れる $kLen$ の, IUT がサポートする範囲の最大値		10 進表記	[MaxkLenDivisibleByhLen = 2048]
		MinkLenDivisibleBy8	($hLen$ で割り切れない)8 の倍数の $kLen$ の, IUT がサポートする範囲の最小値		10 進表記	[MinkLenDivisibleBy8 = 112]
		MaxkLenDivisibleBy8	($hLen$ で割り切れない)8 の倍数の $kLen$ の, IUT がサポートする範囲の最大値		10 進表記	[MaxkLenDivisibleBy8 = 1280]
		NumberOfTestSubsets	試験の部分集合の数		10 進表記	[NumberOfTestSubsets = 12]
		NumberOfTrialsForEachTestSubset	試験の各部分集合の中で, 導出する master key の数		10 進表記	[NumberOfTrialsForEachTestSubset = 10]
	試験部分集合 *1 *2 *3	COUNT	0 以上 NumberOfTrialsForEachTestSubset 未満の整数		10 進表記	COUNT = 0
		kLen	導出する master key (mk) のビット長 ($kLen$)	$kLen$	10 進表記	kLen = 512
		Password	Password (P)	P	16 進表記	Password = 2f9a . . . 3664
		sLen	Salt S のビット長	$\mathbf{len}(S)$	10 進表記	sLen = 256

*1 8 の倍数の $kLen$ のサポートの有無, IUT がサポートする $kLen$ の範囲, 及び IUT がサポートする $sLen$ の範囲の組みあわせに対応して, 最大 36 個の部分集合を記載する.

*2 NumberOfTrialsForEachTestSubset 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.
kLen = 512                                 ♯ i = 0 に対応する kLen を記述する.
Password = e571 ... 519f                   ♯ i = 0 に対応する Password を記述する.
sLen = 256                                 ♯ i = 0 に対応する Salt S のビット長を記述する.

COUNT = 1                                  ♯ i = 1 のデータの組について記述する.
kLen = 512                                 ♯ i = 1 に対応する kLen を記述する.
Password = 9f15 ... 4d17                   ♯ i = 1 に対応する Password を記述する.
sLen = 256                                 ♯ i = 1 に対応する Salt S のビット長を記述する.
⋮
COUNT = ⟨NumberOfTrialsForEachTestSubset − 1⟩   ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ のデータの組について記述する.
kLen = 512                                 ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する kLen を記述する.
Password = dc6f ... c8f2                   ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する Password を記述する.
sLen = 256                                 ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する Salt S のビット長を記述する.
```

2.1.4 レスポンスファイル (*.rsp)

表5: NIST SP800-132 に記載された PBKDF 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
鍵導出関数	ヘッダ	AlgorithmName	PBKDF_in_NIST_SP800_132		文字列	[AlgorithmName = PBKDF_in_NIST_SP800_132]
		PRF	PRF 識別子		文字列	[PRF = HMAC_SHA512]
		IterationCountC	Iteration count C	C	10 進表記	[IterationCountC = 1000]
		kLendivisibleBy8	8 の倍数の $kLen$ のサポートの有無 (有:True, 無:False)		文字列	[kLendivisibleBy8 = True]
		BitLengthOfPasswordForpLenltB	B 未満の Password のビット長.		10 進表記	[BitLengthOfPasswordForpLenltB = 256]
		BitLengthOfPasswordForpLeneqB	B に等しい Password のビット長.		10 進表記	[BitLengthOfPasswordForpLeneqB = 1024]
		BitLengthOfPasswordForpLengtB	B より大きい Password のビット長.		10 進表記	[BitLengthOfPasswordForpLengtB = 2048]
		BitLengthOfSaltForsLenlthLenMinus32	$128 \leq \mathbf{len}(S) < (hLen - 32)$ なる Salt S を IUT がサポートする場合, そのビット長の代表値. サポートしない場合, 0.		10 進表記	[BitLengthOfSaltForsLenlthLenMinus32 = 128]
		BitLengthOfSaltForsLeneqhLenMinus32	$\mathbf{len}(S) = (hLen - 32)$ なる Salt S を IUT がサポートする場合, そのビット長.		10 進表記	[BitLengthOfSaltForsLeneqhLenMinus32 = 480]
		BitLengthOfSaltForsLengthLenMinus32	$\mathbf{len}(S) > (hLen - 32)$ なる Salt S を IUT がサポートする場合, そのビット長の代表値.		10 進表記	[BitLengthOfSaltForsLengthLenMinus32 = 512]
		MinkLenDivisibleByhLen	$hLen$ で割り切れる $kLen$ の, IUT がサポートする範囲の最小値		10 進表記	[MinkLenDivisibleByhLen = 512]
		MaxkLenDivisibleByhLen	$hLen$ で割り切れる $kLen$ の, IUT がサポートする範囲の最大値		10 進表記	[MaxkLenDivisibleByhLen = 2048]
		MinkLenDivisibleBy8	($hLen$ で割り切れない)8 の倍数の $kLen$ の, IUT がサポートする範囲の最小値		10 進表記	[MinkLenDivisibleBy8 = 112]
		MaxkLenDivisibleBy8	($hLen$ で割り切れない)8 の倍数の $kLen$ の, IUT がサポートする範囲の最大値		10 進表記	[MaxkLenDivisibleBy8 = 1280]
		NumberOfTestSubsets	試験の部分集合の数		10 進表記	[NumberOfTestSubsets = 12]
		NumberOfTrialsForEachTestSubset	試験の各部分集合の中で, 導出する master key の数		10 進表記	[NumberOfTrialsForEachTestSubset = 10]
	試験部分集合 *1 *2 *3	COUNT	0 以上 NumberOfTrialsForEachTestSubset 未満の整数		10 進表記	COUNT = 0
		kLen	導出する master key (mk) のビット長 ($kLen$)	$kLen$	10 進表記	kLen = 512
		Password	Password (P)	P	16 進表記	Password = 2f9a . . . 3664
		sLen	Salt S のビット長	$\mathbf{len}(S)$	10 進表記	sLen = 256
		Salt	【出力】Salt S	S	16 進表記	Salt = c457 . . . 5816
		mk	【出力】master key (mk)	mk	16 進表記	mk = 19ab . . . ded1

*1 8 の倍数の $kLen$ のサポートの有無, IUT がサポートする $kLen$ の範囲, 及び IUT がサポートする $sLen$ の範囲の組みあわせに対応して, 最大 36 個の部分集合を記載する.

*2 NumberOfTrialsForEachTestSubset 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.
kLen = 512                                 ♯ i = 0 に対応する kLen を記述する.
Password = e571 ... 519f                   ♯ i = 0 に対応する Password を記述する.
sLen = 256                                 ♯ i = 0 に対応する Salt S のビット長を記述する.
Salt = c457 ... 5816                       ♯ i = 0 に対応する, ベンダーが指定した Salt S の値を記述する.
mk = 19ab ... ded1                         ♯ i = 0 に対応して, IUT が導出した master key mk.

COUNT = 1                                  ♯ i = 1 のデータの組について記述する.
kLen = 512                                 ♯ i = 1 に対応する kLen を記述する.
Password = 9f15 ... 4d17                   ♯ i = 1 に対応する Password を記述する.
sLen = 256                                 ♯ i = 1 に対応する Salt S のビット長を記述する.
Salt = c457 ... 5816                       ♯ i = 1 に対応する, ベンダーが指定した Salt S の値を記述する.
mk = 19ab ... ded1                         ♯ i = 1 に対応して, IUT が導出した master key mk.
⋮
COUNT = ⟨NumberOfTrialsForEachTestSubset − 1⟩   ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ のデータの組について記述する.
kLen = 512                                 ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する kLen を記述する.
Password = dc6f ... c8f2                   ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する Password を記述する.
sLen = 256                                 ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する Salt S のビット長を記述する.
Salt = c457 ... 5816                       ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応する, ベンダーが指定した Salt S の値を記述する.
mk = 19ab ... ded1                         ♯ i = ⟨NumberOfTrialsForEachTestSubset − 1⟩ に対応して, IUT が導出した master key mk.
```

2.1.5 結果ファイル (*.out)

表6: NIST SP800-132 に記載された PBKDF 結果ファイル

機能	分類	タグ	内容	値の表記	例示
鍵導出関数	ヘッダ	AlgorithmName	PBKDF_in_NIST_SP800_132	文字列	[AlgorithmName = PBKDF_in_NIST_SP800_132]
		PRF	PRF 識別子	文字列	[PRF = HMAC_SHA512]
		IterationCountC	Iteration count C	10 進表記	[IterationCountC = 1000]
		kLendivisibleBy8	8 の倍数の $kLen$ のサポートの有無 (有:True, 無:False)	文字列	[kLendivisibleBy8 = True]
		BitLengthOfPasswordForpLenltB	B 未満の Password のビット長.	10 進表記	[BitLengthOfPasswordForpLenltB = 256]
		BitLengthOfPasswordForpLeneqB	B に等しい Password のビット長.	10 進表記	[BitLengthOfPasswordForpLeneqB = 1024]
		BitLengthOfPasswordForpLengtB	B より大きい Password のビット長.	10 進表記	[BitLengthOfPasswordForpLengtB = 2048]
		BitLengthOfSaltForsLenlthLenMinus32	$128 \leq \mathbf{len}(S) < (hLen - 32)$ なる Salt S を IUT がサポートする場合, そのビット長の代表値. サポートしない場合, 0.	10 進表記	[BitLengthOfSaltForsLenlthLenMinus32 = 128]
		BitLengthOfSaltForsLeneqhLenMinus32	$\mathbf{len}(S) = (hLen - 32)$ なる Salt S を IUT がサポートする場合, そのビット長.	10 進表記	[BitLengthOfSaltForsLeneqhLenMinus32 = 480]
		BitLengthOfSaltForsLengthLenMinus32	$\mathbf{len}(S) > (hLen - 32)$ なる Salt S を IUT がサポートする場合, そのビット長の代表値.	10 進表記	[BitLengthOfSaltForsLengthLenMinus32 = 512]
		MinkLenDivisibleByhLen	$hLen$ で割り切れる $kLen$ の, IUT がサポートする範囲の最小値	10 進表記	[MinkLenDivisibleByhLen = 512]
		MaxkLenDivisibleByhLen	$hLen$ で割り切れる $kLen$ の, IUT がサポートする範囲の最大値	10 進表記	[MaxkLenDivisibleByhLen = 2048]
		MinkLenDivisibleBy8	($hLen$ で割り切れない)8 の倍数の $kLen$ の, IUT がサポートする範囲の最小値	0 進表記	[MinkLenDivisibleBy8 = 112]
		MaxkLenDivisibleBy8	($hLen$ で割り切れない)8 の倍数の $kLen$ の, IUT がサポートする範囲の最大値	10 進表記	[MaxkLenDivisibleBy8 = 1280]
		NumberOfTestSubsets	試験の部分集合の数	10 進表記	[NumberOfTestSubsets = 12]
		NumberOfTrialsForEachTestSubset	試験の各部分集合の中で, 導出する master key の数	10 進表記	[NumberOfTrialsForEachTestSubset = 10]
		⟨ 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．