

JCATT ファイルフォーマット仕様書

RSA-PSS

2008年1月18日

独立行政法人 情報処理推進機構

目 次

1	はじめに	1
2	RSA-PSS	2
2.1	パラメータファイル (*.par)	4
2.2	リクエストファイル (*.req)	6
2.3	Facts ファイル (*.fax)	8
2.4	レスポンスファイル (*.rsp)	10
2.5	結果ファイル (*.out)	12

1 はじめに

暗号アルゴリズム試験ツール (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ponse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、試験対象暗号モジュール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ponse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

- [] で囲まれた“タグ”の次の行に値を記述する。
- タグは各ファイルフォーマットに記述した順番通りに記述すること。
- レスponseファイルにおいては【出力】と記述したタグが、試験対象モジュール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 RSA-PSS

RSA-PSS アルゴリズム試験のためのファイルフォーマットを記述する。各表において，試験方法に関する以下の略語を使用する。

- RGT: Random Generation Test

試験方法の詳細は，暗号アルゴリズム試験仕様書を参照のこと。

各表中，プライベート鍵識別子，公開鍵 e 識別子，擬似乱数生成関数識別子，マスク生成関数識別子は下表の通りである。

表 1: プライベート鍵識別子

識別子	対応するプライベート鍵
TYPE1	プライベート鍵は $(p, q, dP, dQ, qInv)$
TYPE2	プライベート鍵は (d, n)

表 2: 公開鍵 e 識別子

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

表 3: 擬似乱数生成関数識別子

識別子	対応する擬似乱数生成関数
M_PRNG_ANSIX942_ANNEXC1_SHA1	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
M_PRNG_FIPS186_APPENDIX31_SHA1	PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1
M_PRNG_FIPS186_REVISIED_APPENDIX31_SHA1	PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1
M_PRNG_ISO18031_HASH	Hash.DRBG
M_PRNG_ISO18031_CTR	CTR.DRBG
M_PRNG_ISO18031_OFB	OFB.DRBG

表 4: マスク生成関数 (MGF) 識別子

MGF 識別子	対応する MGF
M_MGF_ANSI944_SHA1	ANSI X9.44 SHA-1
M_MGF_ANSI944_SHA256	ANSI X9.44 SHA-256
M_MGF_ANSI944_SHA384	ANSI X9.44 SHA-384
M_MGF_ANSI944_SHA512	ANSI X9.44 SHA-512

擬似乱数生成関数のパラメータ

擬似乱数生成関数のパラメータは、タグ [Parameter of PRNG] の下に、4 行 (各パラメータにつき 1 行) で以下の順で 16 進表記で記述する。ただし、*resseed counter* は 10 進数表記で記述する。

- PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1

- 1 行目：空行
- 2 行目：*XSEED*
- 3 行目：空行
- 4 行目：空行

- ISO18031 HASH DRBG

- 1 行目：ハッシュ関数識別子 (下表を参照のこと)
- 2 行目：*C*
- 3 行目：*additional input*
- 4 行目：*resseed counter*

- ISO18031 OFB DRBG

- 1 行目：ブロック暗号識別子 (下表を参照のこと)
- 2 行目：*KEY*
- 3 行目：*additional input*
- 4 行目：*resseed counter*

表 5: ハッシュ関数識別子

ハッシュ関数識別子	対応するハッシュ関数
M_Hash_SHA1	SHA-1
M_Hash_SHA256	SHA-256
M_Hash_SHA384	SHA-384
M_Hash_SHA512	SHA-512

表 6: ブロック暗号識別子

ブロック暗号識別子	対応するブロック暗号
M_BlockCipher_TDES	3-key Triple DES
M_BlockCipher_AES	AES

2.1 パラメータファイル (*.par)

表 7: RSA-PSS パラメータファイル

機能	タグ	内容
(共通)	[Algorithm Name]	RSA-PSS
署名生成	[Function Name]	Sign
	[Bitlength of Modulus]	法 n のビット長
	[PRNG]	擬似乱数生成関数識別子 (このタグは試験 2 の場合のみ記述する.)
	[Parameter of PRNG]	擬似乱数生成関数パラメータ (このタグは試験 2 の場合のみ記述する.)
	[Hash]	ハッシュ関数識別子
	[MGF]	マスク生成関数識別子
	[Secret Key Type]	プライベート鍵識別子
	[Public Key Type]	公開鍵 e 識別子
	[Seed P]	ランダムな平文を生成するための擬似乱数生成関数用乱数シード
	[Bitlength of Seed P]	Seed P のビット長
	[Seed K]	鍵ペア生成のための擬似乱数生成用乱数シード
	[Bitlength of Seed K]	Seed K のビット長
	[Seed Salt]	$salt$ 生成のための擬似乱数生成用乱数シード. $salt$ とは, PKCS#1 v2.1 に記述されている EMSA-PSS エンコーディングにおけるオクテットストリングのことである.
	[Bitlength of Seed Salt] ¹	Seed Salt のビット長
	[Number of Signatures for RGT]	RGT で生成する署名の個数.
	[SaltFlag] ¹	$Salt$ の入力フラグ. 0: 指定なし, 1: 指定あり.
	[Bitlength of Salt]	$Salt$ のビット長
	[Bitlength of Plaintexts]	平文のビット長
	[Number of Plaintexts]	平文の数

注

- この 2 つのタグで試験 1, 2, 3 のいずれを行うかを識別する.
 試験 1 を行う場合: [Bitlength of Seed Salt] と [SaltFlag] が共に 0 の場合
 試験 2 を行う場合: [Bitlength of Seed Salt] が 0 でなく [SaltFlag] が 0 の場合
 試験 3 を行う場合: [Bitlength of Seed Salt] と [SaltFlag] が共に 0 でない場合
 それ以外の場合は, エラーとする.

表 8: RSA-PSS パラメータファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	RSA-PSS
署名検証	[Function Name]	Verification
	[Bitlength of Modulus]	署名生成と同じ
	[Hash]	
	[MGF]	
	[Secret Key Type]	
	[Public Key Type]	
	[Seed P]	
	[Bitlength of Seed P]	
	[Seed K]	
	[Bitlength of Seed K]	
	[Seed Salt]	
	[Bitlength of Seed Salt]	
	[Bitlength of Salt]	
	[Bitlength of Plaintexts]	
	[Number of Plaintexts]	
	[Rate of Fail Data]	署名検証が不合格になる割合
鍵ペア生成	[Function Name]	Key Generation
	[Bitlength of Modulus]	法 n のビット長
	[Secret Key Type]	プライベート鍵識別子
	[Public Key Type]	公開鍵 e 識別子
	[Number of Keys]	鍵の数

2.2 リクエストファイル (*.req)

表 9: RSA-PSS リクエストファイル

機能	タグ	内容
(共通)	[Algorithm Name]	RSA-PSS
署名生成	[Function Name]	Sign
	[Bitlength of Modulus]	法 n のビット長
	[PRNG]	擬似乱数生成関数識別子 (このタグは試験 2 の場合のみ記述する.)
	[Parameter of PRNG]	擬似乱数生成関数パラメータ (このタグは試験 2 の場合のみ記述する.)
	[Hash]	ハッシュ関数識別子
	[MGF]	マスク生成関数識別子
	[Secret Key Type]	プライベート鍵識別子
	[p] ¹	素数 p
	[q] ¹	素数 q
	[d] ¹	プライベート鍵 d
	[n] ¹	法 n
	[dP] ¹	$d \bmod p - 1$
	[dQ] ¹	$d \bmod q - 1$
	[qInv] ¹	$q^{-1} \bmod p$
	[Seed Salt]	<i>salt</i> 生成のための擬似乱数生成用乱数シード. <i>salt</i> とは, PKCS#1 v2.1 に記述されている EMSA-PSS エンコーディングにおけるオクテットストリングのことである.
	[Bitlength of Seed Salt]	Seed Salt のビット長
	[Bitlength of Plaintexts]	平文のビット長
	[SaltFlag]	<i>Salt</i> の入力フラグ. 0: 指定なし, 1: 指定あり.
	[Bitlength of Salt]	<i>Salt</i> のビット長
	[Number of Plaintexts]	平文の数
	[Plaintexts] ²	平文
	[Salts] ³	<i>salt</i>
	[Number of Signatures for RGT]	RGT で生成する署名の個数. このタグは試験 1 の場合のみ記述する.

注

1. プライベート鍵識別子に応じて, $([d],[n])$ の組または $([p],[q],[dP],[dQ],[qInv])$ の組いずれか一方を記述する.
2. [Number of Plaintexts] 個の平文を記述する.
3. 試験 3 の時のみ, [Number of Plaintexts] 個の *salt* を記述する.

表 10: RSA-PSS リクエストファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	RSA-PSS
署名検証	[Function Name]	Verification
	[Bitlength of Modulus]	法 n のビット長
	[Hash]	ハッシュ関数識別子
	[MGF]	マスク生成関数識別子
	[n]	法 n
	[Bitlength of Salt]	$salt$ のビット長
	[Bitlength of Plaintexts]	平文のビット長
	[Number of Signatures]	署名, 平文の組の数
	[e] ¹	公開鍵 e
	[Signatures] ¹	署名
	[Plaintexts] ¹	平文
鍵ペア生成	[Function Name]	Key Generation
	[Bitlength of Modulus]	法 n のビット長
	[Secret Key Type]	プライベート鍵識別子
	[Public Key Type]	公開鍵 e 識別子
	[Number of Keys]	鍵の数

注

1. [Number of Signatures] 個の公開鍵 e , 署名および平文を記述する。

2.3 Facts ファイル (*.fax)

表 11: RSA-PSS Facts ファイル

機能	タグ	内容
(共通)	[Algorithm Name]	RSA-PSS
署名生成	[Function Name]	Sign
	[Bitlength of Modulus]	法 n のビット長
	[PRNG]	擬似乱数生成関数識別子 (このタグは試験 2 の場合のみ記述する.)
	[Parameter of PRNG]	擬似乱数生成関数パラメータ (このタグは試験 2 の場合のみ記述する.)
	[Hash]	ハッシュ関数識別子
	[MGF]	マスク生成関数識別子
	[Secret Key Type]	プライベート鍵識別子
	[Public Key Type]	公開鍵 e 識別子
	[p] ¹	素数 p
	[q] ¹	素数 q
	[d] ¹	プライベート鍵 d
	[n] ¹	法 n
	[dP] ¹	$d \bmod p - 1$
	[dQ] ¹	$d \bmod q - 1$
	[qInv] ¹	$q^{-1} \bmod p$
	[e]	公開鍵 e
	[Seed Salt]	<i>salt</i> 生成のための擬似乱数生成用乱数シード. <i>salt</i> とは, PKCS#1 v2.1 に記述されている EMSA-PSS エンコーディングにおけるオクテットストリングのことである.
	[Bitlength of Seed Salt]	Seed Salt のビット長
	[Bitlength of Plaintexts]	平文のビット長
	[SaltFlag]	<i>salt</i> の入力フラグ. 0: 指定なし, 1: 指定あり.
	[Bitlength of Salt]	<i>salt</i> のビット長
	[Number of Plaintexts]	平文の数
	[Plaintexts] ²	平文
	[Salts] ³	<i>salt</i>
	[Signatures] ²	署名
	[Number of Signatures for RGT]	RGT で生成する署名の個数. このタグは試験 1 の場合のみ記述する.

注

1. プライベート鍵識別子に応じて, $([d],[n])$ の組または $([p],[q],[n],[dP],[dQ],[qInv])$ の組いずれか一方を記述する.
2. [Number of Plaintexts] 個の平文および署名を記述する. ただし, 署名は試験 2 および 3 の時のみ記述する.
3. 試験 3 の時のみ, [Number of Plaintexts] 個の *salt* を記述する.

表 12: RSA-PSS Facts ファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	RSA-PSS
署名検証	[Function Name]	Verification
	[Bitlength of Modulus]	法 n のビット長
	[Hash]	ハッシュ関数識別子
	[MGF]	マスク生成関数識別子
	[Secret Key Type]	プライベート鍵識別子
	[Public Key Type]	公開鍵 e 識別子
	$[p]^1$	素数 p
	$[q]^1$	素数 q
	$[d]^1$	プライベート鍵 d
	$[n]^1$	法 n
	$[dP]^1$	$d \bmod p - 1$
	$[dQ]^1$	$d \bmod q - 1$
	$[qInv]^1$	$q^{-1} \bmod p$
	[Bitlength of Salt]	$salt$ のビット長
	[Bitlength of Plaintexts]	平文のビット長
	[Number of Signatures]	署名, 平文の組の数
	$[e]^2$	公開鍵 e
	[Signatures] ²	署名
	[Plaintexts] ²	平文
	[Results] ²	署名検証結果. 検証合格の時 0, 不合格の時 1 と記述する.
鍵ペア生成	[Function Name]	Key Generation
	[Bitlength of Modulus]	法 n のビット長
	[Secret Key Type]	プライベート鍵識別子
	[Public Key Type]	公開鍵 e 識別子
	[Number of Keys]	鍵の数

注

1. プライベート鍵識別子に応じて, $([d],[n])$ の組または $([p],[q],[n],[dP],[dQ],[qInv])$ の組いずれか一方を記述する.
2. [Number of Signatures] 個の公開鍵 e , 署名, 平文, および署名検証結果を記述する.

2.4 レスポンスファイル (*.rsp)

表 13: RSA-PSS レスポンスファイル

機能	タグ	内容
(共通)	[Algorithm Name]	RSA-PSS
署名生成	[Function Name]	Sign
	[Bitlength of Modulus]	法 n のビット長
	[PRNG]	擬似乱数生成関数識別子 (このタグは試験 2 の場合のみ記述する.)
	[Parameter of PRNG]	擬似乱数生成関数パラメータ (このタグは試験 2 の場合のみ記述する.)
	[Hash]	ハッシュ関数識別子
	[MGF]	マスク生成関数識別子
	[Secret Key Type]	プライベート鍵識別子
	[p] ¹	素数 p
	[q] ¹	素数 q
	[d] ¹	プライベート鍵 d
	[n] ¹	法 n
	[dP] ¹	$d \bmod p - 1$
	[dQ] ¹	$d \bmod q - 1$
	[qInv] ¹	$q^{-1} \bmod p$
	[Seed Salt]	<i>salt</i> 生成のための擬似乱数生成用乱数シード. <i>salt</i> とは, PKCS#1 v2.1 に記述されている EMSA-PSS エンコーディングにおけるオクテットストリングのことである.
	[Bitlength of Seed Salt]	Seed Salt のビット長
	[Bitlength of Plaintexts]	平文のビット長
	[SaltFlag]	<i>Salt</i> の入力フラグ. 0: 指定なし. 1: 指定あり.
	[Bitlength of Salt]	<i>salt</i> のビット長
	[Number of Plaintexts]	平文の数
	[Plaintexts] ²	平文
	[Salts] ³	<i>salt</i>
	[Signatures] ²	【出力】署名
	[Number of Signatures for RGT]	RGT で生成する署名の個数. このタグは試験 1 の場合のみ記述する.
	[Signatures for RGT] ⁴	【出力】RGT で生成された署名. このタグは試験 1 の場合のみ記述する.

注

1. プライベート鍵識別子に応じて, $([d],[n])$ の組または $([p],[q],[dP],[dQ],[qInv])$ の組いずれか一方を記述する.
2. [Number of Plaintexts] 個の平文および署名を記述する.
3. 試験 3 の時のみ, [Number of Plaintexts] 個の *salt* を記述する.
4. [Plaintexts] データの 1 番目の平文を用いて生成した署名を記述する.

表 14: RSA-PSS レスポンスファイル (続き)

機能	タグ	内容
(共通)	[Algorithm Name]	RSA-PSS
署名検証	[Function Name]	Verification
	[Bitlength of Modulus]	法 n のビット長
	[Hash]	ハッシュ関数識別子
	[MGF]	マスク生成関数識別子
	[n]	法 n
	[Bitlength of Salt]	$salt$ のビット長
	[Bitlength of Plaintexts]	平文のビット長
	[Number of Signatures]	署名, 平文の組の数
	[e] ¹	公開鍵 e
	[Signatures] ¹	署名
	[Plaintexts] ¹	平文
	[Results] ¹	【出力】署名検証結果．検証合格の時 0 , 不合格の時 1 と記述する．
鍵ペア生成	[Function Name]	Key Generation
	[Bitlength of Modulus]	法 n のビット長
	[Secret Key Type]	プライベート鍵識別子
	[Number of Keys]	鍵の数
	[p] ²	【出力】素数 p
	[q] ²	【出力】素数 q
	[d] ²	【出力】プライベート鍵 d
	[e] ²	【出力】公開鍵 e
	[n] ²	【出力】法 n
	[dP] ²	【出力】 $d \bmod p - 1$
	[dQ] ²	【出力】 $d \bmod q - 1$
	[qInv] ²	【出力】 $q^{-1} \bmod p$

注

1. [Number of Signatures] 個の公開鍵 e , 署名 , 平文 , および署名検証結果を記述する .
2. プライベート鍵のタイプに応じて , ($[p]$, $[q]$, $[d]$, $[e]$, $[n]$) の組または ($[p]$, $[q]$, $[dP]$, $[dQ]$, $[qInv]$, $[e]$, $[n]$) の組いずれか一方を [Number of Keys] 個記述する .

2.5 結果ファイル (*.out)

表 15: RSA-PSS 結果ファイル

タグ	内容
[Algorithm Name]	暗号名
[Function Name]	試験対象機能名
[Results]	試験結果

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タグ名と，そのタグ内の何番目 (No.，#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．
- 鍵ペア生成機能に対する試験において試験不合格の場合，下記のようにどの条件が合格 (ok) でどの条件が不合格 (NG) となったかも表示される．
NG(#1 : p is prime ?)
ok(#1 : q is prime ?)
例えば，ok(#1 : q is prime ?) は， q は素数であるという条件を満たしていることを示し，NG(#1 : p is prime ?) は， p は素数であるという条件を満たしていないことを示す．詳細は別紙の試験項目を記述した文書を参照のこと．