22. RFC 8230：Using RSA Algorithms with CBOR Object Signing and Encryption (COSE) Messages
RFC 8230：將 RSA 演算法與 CBOR 物件簽章和加密（COSE）訊息一起使用

網際網路工程任務組 (IETF)
Request for Comments: 8230
分類: 標準協定
ISSN: 2070-1721

M. Jones
Microsoft

2017 年 9 月

將 RSA 演算法與 CBOR 物件簽章和加密（COSE）訊息一起使用

摘要

CBOR 物件簽章和加密（COSE）規範使用簡明二進位物件表示（CBOR）定義加密訊息編碼。該規範定義了演算法編碼和表示形式，使 RSA 演算法能夠用於 COSE 消息。編碼被指定用於 RSA 概率簽章方案（RSASSA-PSS）簽章，RSA 加密方案 - 最佳非對稱加密填充（RSAES OAEP）加密和 RSA 密鑰。

本文的狀態

這是一份網際網路標準協定文件。

本文是網際網路工程任務組（IETF）的產品。 它代表了 IETF 社群的共識。 它已經過公眾審查，並已獲得網際網路工程指導小組（IESG）的批准發佈。 有關網際網路標準的更多資訊，請參見 RFC 7841 的第 2 節。

有關本文的當前狀態，任何勘誤以及如何提供回饋的資訊，請訪問 http://www.rfc-editor.org/info/rfc8230。

版權聲明

目錄

1. 前言 3
1.1. 要求符號和習慣用語 3
2. RSASSA-PSS簽章演算法 3
3. RSAES-OAEP密鑰加密演算法 4
4. RSA 密鑰 4
5. IANA 注意事項 6
5.1. COSE 演算法註冊 6
5.2. COSE 密鑰類型註冊 7
5.3. COSE密鑰類型參數註冊 7
6. 安全注意事項 9
6.1. 密鑰尺寸安全注意事項 9
6.2. RSASSA-PSSS 安全注意事項 10
6.3. RSAES-OAEP安全注意事項 10
7. 參考文獻 10
7.1. 規範性參考 11
7.2. 訊息參考 11
致謝 12
作者地址 12

1. 前言

CBOR 物件簽章和加密（COSE）[RFC8152]規範使用簡明二進位物件表示（CBOR）[RFC7049]定義加密訊息編碼。 該規範定義了演算法編碼和表示，使 RSA 演算法能夠用於 COSE 消息。

1.1. 需求符號和習慣用語

關鍵字"必須(MUST)"、"不得(MUST NOT)"，"必要(REQUIRED)"，"必須(SHALL)"，"不得(SHALL NOT)"，"應該(SHALL NOT)"，"不應該(SHOULD NOT)"，"建議(RECOMMENDED)"，"不建議(RECOMMENDED)"，"可以(MAY)"，"可選(OPTIONAL)"在本文中，只有當它們出現在所有大寫字母中時才會按照 BCP 14 [RFC2119] [RFC8174]中的描述進行解釋，如此處所示。

2. RSASSA-PSS 簽章演算法

RSASSA-PSS 簽章演算法在[RFC8017]中定義。

RSASSA-PSS 簽章演算法使用散列函數（h），遮罩生成函數（mgf）和鹽長度（sLen）進行參數化。 對於本說明書，遮罩生成功能固定為[RFC8017]中定義的 MGF1。 建議使用相同的散列函數來散列資料以及遮罩生成函數。本規範遵循此建議。salt 的長度與 hash 函數輸出的長度相同。
在創建或驗證簽章時，實現需要檢查密鑰類型是否為 “RSA”。

本文中指定的 RSASSA-PSS 演算法如下表所示。

Name	Value	Hash	Salt Length	Description
PS256	-37	SHA-256	32	RSASSA-PSS w/ SHA-256
PS384	-38	SHA-384	48	RSASSA-PSS w/ SHA-384
PS512	-39	SHA-512	64	RSASSA-PSS w/ SHA-512

表 1：RSASSA-PSS 算法值

3．RSAES-OAEP 密鑰加密演算法

RSAES-OAEP 是一種非對稱式密鑰密碼編譯演算法。 RSAEA-OAEP 的定義可以在[RFC8017]的第 7.1 節中找到。 使用遮罩生成函數（mgf），散列函數（h）和編碼參數（P）來參數化該演算法。 對於本節中定義的演算法標識符：

o mgf 始終設置為[RFC8017]中定義的 MGF1，並使用與 h 相同的散列函數。

o P 始終設置為空的八位元字串。

下表總結了剩餘的值。

Name	Value	Hash	Description
RSAES-OAEP w/ RFC 8017 default parameters	-40	SHA-1	RSAES-OAEP w/ SHA-1
RSAES-OAEP w/ SHA-256	-41	SHA-256	RSAES-OAEP w/ SHA-256
RSAES-OAEP w/ SHA-512	-42	SHA-512	RSAES-OAEP w/ SHA-512

Table 2: RSAES-OAEP 演算法值

密鑰的類型必須為 “RSA”。

4．RSA 密鑰

密鑰類型由 COSE_Key 物件的“kty”成員標識。 此規範在下表中為此成員定義了一個值。

Name	Value	Description
RSA	3	RSA Key

Table 3: 密鑰類型值

本文定義了 RSA 密鑰的公共和私有部分的密鑰結構。 RSA 公開密鑰和 RSA 私密密鑰一起形成 RSA 密鑰對。

該檔還支援所謂的“多品質”RSA 密鑰，其中模數可能具有兩個以上的素因數。 多品質 RSA 的好處是解密和簽章原語的計算成

本較低。 有關多素數如何影響 RSA 密碼系統安全性的討論，請參閱[MultiPrimeRSA]。

本文遵循[RFC8017]的命名規則，用於命名 RSA 公開密鑰或私密密鑰的欄位，並且相應的欄位具有相同的語義。RSA 密鑰欄位的要求如下：

o 對於所有的密鑰， “kty”必須存在，且值必須為 3。

o 對於公開密鑰，必須存在欄位'n'和'e'。 下表中定義的所有其他欄位必須不存在。

o 對於具有兩個素數的私密密鑰，欄位'other'，'r_i'，'d_i'和't_i'必須不存在; 所有其他領域必須存在。

o 對於具有兩個以上素數的私密密鑰，必須存在所有欄位。 對於第三到第 n 個素數，每個素數都表示為包含欄位'r_i'，'d_i'和't_i'的地圖。 欄位'other'是這些地圖的陣列。

o 所有數位關鍵參數都使用 CBOR 位元組字串類型（主要類型 2）以無符號大端表示形式編碼為八位元組序列。八位元組序列必須使用表示該值所需的最小八位元組數。 例如，值 32,768 表示為 CBOR 位元組序列 0b010_00010,0x80 0x00（主要類型 2，長度的附加資訊 2）。

下表提供了標籤值以及與每個標籤相關的類型的摘要。

Key Type	Name	Label	CBOR Type	Description
3	n	-1	bstr	the RSA modulus n
3	e	-2	bstr	the RSA public exponent e
3	d	-3	bstr	the RSA private exponent d
3	p	-4	bstr	the prime factor p of n
3	q	-5	bstr	the prime factor q of n
3	dP	-6	bstr	dP is d mod (p - 1)
3	dQ	-7	bstr	dQ is d mod (q - 1)
3	qInv	-8	bstr	qInv is the CRT coefficient q^(-1) mod p
3	other	-9	array	other prime infos, an array
3	r_i	-10	bstr	a prime factor r_i of n, where i >= 3
3	d_i	-11	bstr	d_i = d mod (r_i - 1)
3	t_i	-12	bstr	the CRT coefficient t_i = (r_1 * r_2 * ... * r_(i-1))^(-1) mod r_i

Table 4: RSA 密鑰參數

5. IANA 注意事項

5.1. COSE 演算法註冊

IANA 已在 IANA“COSE 演算法”註冊表[IANA.COSE]中註冊了以下值。

- Name: PS256
- Value: -37
- Description: RSASSA-PSS w/ SHA-256
- Reference: Section 2 of this document
- Recommended: Yes

- Name: PS384
- Value: -38
- Description: RSASSA-PSS w/ SHA-384
- Reference: Section 2 of this document
- Recommended: Yes

- Name: PS512
- Value: -39
- Description: RSASSA-PSS w/ SHA-512
- Reference: Section 2 of this document
- Recommended: Yes

- Name: RSAES-OAEP w/ RFC 8017 default parameters
- Value: -40
- Description: RSAES-OAEP w/ SHA-1
- Reference: Section 3 of this document
- Recommended: Yes

- Name: RSAES-OAEP w/ SHA-256
- Value: -41
- Description: RSAES-OAEP w/ SHA-256
- Reference: Section 3 of this document
- Recommended: Yes

- Name: RSAES-OAEP w/ SHA-512
- Value: -42
- Description: RSAES-OAEP w/ SHA-512

- Reference: Section 3 of this document
- Recommended: Yes

5.2. COSE 密鑰類型註冊

IANA 已在 IANA“COSE 密鑰類型”註冊表[IANA.COSE]中註冊以下值。

- Name: RSA
- Value: 3
- Description: RSA Key
- Reference: Section 4 of this document

5.3. COSE 密鑰類型參數註冊

IANA 已在 IANA“COSE 密鑰類型參數”註冊表[IANA.COSE]中註冊了以下值。

- Key Type: 3
- Name: n
- Label: -1
- CBOR Type: bstr
- Description: the RSA modulus n
- Reference: Section 4 of this document

- Key Type: 3
- Name: e
- Label: -2
- CBOR Type: bstr
- Description: the RSA public exponent e
- Reference: Section 4 of this document

- Key Type: 3
- Name: d
- Label: -3
- CBOR Type: bstr
- Description: the RSA private exponent d
- Reference: Section 4 of this document

- Key Type: 3
- Name: p
- Label: -4
- CBOR Type: bstr
- Description: the prime factor p of n
- Reference: Section 4 of this document
- Key Type: 3
- Name: q
- Label: -5
- CBOR Type: bstr
- Description: the prime factor q of n
- Reference: Section 4 of this document

- Key Type: 3
- Name: dP
- Label: -6
- CBOR Type: bstr
- Description: dP is d mod (p - 1)
- Reference: Section 4 of this document

- Key Type: 3
- Name: dQ
- Label: -7
- CBOR Type: bstr
- Description: dQ is d mod (q - 1)
- Reference: Section 4 of this document

- Key Type: 3
- Name: qInv
- Label: -8
- CBOR Type: bstr
- Description: qInv is the CRT coefficient q^(-1) mod p
- Reference: Section 4 of this document

- Key Type: 3
- Name: other
- Label: -9
- CBOR Type: array
- Description: other prime infos, an array
- Reference: Section 4 of this document

- Key Type: 3
- Name: r_i
- Label: -10
- CBOR Type: bstr
- Description: a prime factor r_i of n, where i >= 3
- Reference: Section 4 of this document

- Key Type: 3
- Name: d_i
- Label: -11
- CBOR Type: bstr
- Description: d_i = d mod (r_i - 1)
- Reference: Section 4 of this document

- Key Type: 3
- Name: t_i
- Label: -12
- CBOR Type: bstr
- Description: the CRT coefficient t_i = (r_1 * r_2 * ... * r_(i-1))^(-1) mod r_i
- Reference: Section 4 of this document

6. 安全注意事項

6.1. 密鑰尺寸安全注意事項

這些演算法必須使用 2048 位元或更大的密鑰尺寸。 該密鑰尺寸大致對應於 128 位元對稱加密演算法所提供的相同強度。實現應該能夠加密和解密，模數在 2048 到 16K 位之間。 應用可以對模數的長度施加額外的限制。

除了需要擔心太小而無法提供所需安全性的密鑰之外，還存在太大的密鑰問題。使用過大的密鑰或奇怪的密鑰安裝了拒絕服務攻擊。 這有可能使用這些密鑰消耗資源。 強烈建議在開始加密操作之前檢查密鑰長度。

有兩種合理的方法可以解決這種攻擊。首先，在驗證密鑰是由接收方信任的一方控制之前，密鑰不應用於加密操作。這種方法意味著在做出關於密鑰的信任決定之前不會進行加密，這是[RFC7515]附錄 D 第 4 項中描述的過程。其次，應用程式可以對密鑰施加最大長度和最小長度要求。這限制了使用過大密鑰所消耗的資源。

6.2. RSASSA-PSSS 安全注意事項

可以針對 RSASSA-PSS [HASHID]安裝理論雜湊替換攻擊。但是，對所有操作一致地使用相同散列函數的要求是對其的有效緩解。與橢圓曲線數位簽章演算法（ECDSA）不同，散列函數輸出不會被截斷，因此始終對完整散列值進行簽章。RSASSA-PSS 的內部填充結構意味著需要在兩個散列函數之間進行多次衝突，以便在基於更改散列函數的情況下成功生成偽造。這種可能性極小。

6.3. RSAES-OAEP 安全注意事項

包含使用[RFC8017]附錄 A.2.1 中指定的默認參數的 RSAES-OAEP 版本，因為這是最廣泛實現的一組 OAEP 參數選擇。（這些預設參數是 SHA-1 雜湊函數和帶有 SHA-1 遮罩生成函數的 MGF1。）

與 RSAES-OAEP 一起使用的密鑰必須遵循[RFC8017]第 7.1 節中的約束。此外，不得使用具有低私密密鑰指數值的密鑰，如“RSA 密碼系統上的二十年攻擊”[Boneh99]的第 3 節中所述。

7. 參考文獻

7.1. 規範性參考

[Boneh99] Boneh, D., "Twenty Years of Attacks on the RSA Cryptosystem", Notices of the American Mathematical Society (AMS), Vol. 46, No. 2, pp. 203-213, 1999, <http://www.ams.org/notices/199902/boneh.pdf>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <https://www.rfc-editor.org/info/rfc7049>.

[RFC7515] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", RFC 7515, DOI 10.17487/RFC7515, May 2015, <https://www.rfc-editor.org/info/rfc7515>.

[RFC8017] Moriarty, K., Ed., Kaliski, B., Jonsson, J., and A. Rusch, "PKCS #1: RSA Cryptography Specifications Version 2.2", RFC 8017, DOI 10.17487/RFC8017, November 2016, <https://www.rfc-editor.org/info/rfc8017>.

[RFC8152] Schaad, J., "CBOR Object Signing and Encryption (COSE)", RFC 8152, DOI 10.17487/RFC8152, July 2017, <https://www.rfc-editor.org/info/rfc8152>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

7.2. 訊息參考

[HASHID] Kaliski, B., "On Hash Function Firewalls in Signature Schemes", Lecture Notes in Computer Science (LNCS), Volume 2271, pp. 1-16, DOI 10.1007/3-540-45760-7_1, February 2002, <https://rd.springer.com/chapter/10.1007/3-540-45760-7_1>.

[IANA.COSE] IANA, "CBOR Object Signing and Encryption (COSE)", <http://www.iana.org/assignments/cose>.

[MultiPrimeRSA] Hinek, M. and D. Cheriton, "On the Security of Multi-prime RSA", June 2006, <http://cacr.uwaterloo.ca/techreports/2006/cacr2006-16.pdf>.

致謝

該規範包含了 Jim Schaad 和 Brian Campbell 撰寫的“ CBOR 編碼消息語法”（2015 年 9 月）中的文本。感謝 Ben Campbell，Roni Even，Steve Kent，Kathleen Moriarty，Eric Rescorla，Adam Roach，Rich Salz 和 Jim Schaad 對規範的評論。

作者地址

Michael B. Jones
Microsoft

Email: mbj@microsoft.com
URI: http://self-issued.info/