تنسيقات بيانات PKI

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
تدوين ASN.1
ترميز BER/CER/DER
عملية تفريغ DER HEX
تشفير Base64
تشفير PEM
شهادات X.509 و CRLs
معايير PKCS
معلومات ذات صلة

المقدمة

يصف هذا وثيقة أكثر مفتاح عام بنية أساسية (PKI) معطيات تنسيق وتشفير.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تشفير المفتاح العام (المفاهيم الأساسية).
- البنية الأساسية للمفتاح العام (المفاهيم الأساسية).

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

أحلت cisco فني طرف إتفاق لمعلومة على وثيقة إتفاق.

تدوين ASN.1

الصيغة المجردة Abstract Syntax Notation One (ASN.1) هي لغة رسمية لتعريف أنواع البيانات وقيمها، وكيفية إستخدام هذه الأنواع والقيم من البيانات ودمجها في هياكل بيانات مختلفة. الهدف من المعيار هو تعريف الصياغة التجريدية للمعلومات دون تقييد كيفية تشفير المعلومات للإرسال.

فيما يلي مثال مقتبس من *X.509 RFC*:

```
{  (Version  ::=  INTEGER  {  v1(0), v2(1), v3(2
                CertificateSerialNumber ::= INTEGER
                        } Validity ::= SEQUENCE
                                ,notBefore Time
                                { notAfter Time
                            } Time ::= CHOICE
                           ,utcTime UTCTime
                { generalTime GeneralizedTime
```

ارجع إلى هذه المستندات من مواقع معايير الاتحاد الدولي للاتصالات (ITU-T):

- ASN.1 X.680: مواصفات التدوين الأساسي
- ASN.1 X.681: مواصفات كائن المعلومات
- ASN.1 X.682: مواصفات القيد
- ASN.1 X.683: وضع مواصفات ASN.1 في المعاملات

بحث عن توصيات ITU-T - للبحث عن **X.509** في **Rec. أو Standard** مع **Language** المعينة على **ASN.1**.

ترميز BER/CER/DER

وقد حدد الاتحاد الدولي للاتصالات - T طريقة قياسية لترميز هياكل البيانات الموصوفة في ASN.1 إلى بيانات ثنائية. يعرف X.690 قواعد الترميز الأساسية (BER) ومجموعتيه الفرعيتين، قواعد الترميز القانونية (CER) وقواعد الترميز المميزة (DER). كل الثلاثة مبنية على حقول بيانات **نوع-طول-قيمة** معبأة في هيكل هرمي، الذي بني من **SETs**، **Sequence**، و**OPTIONs**، مع هذه الاختلافات:

- يوفر BER طرق متعددة لتشفير نفس البيانات، والتي لا تناسب عمليات التشفير.
- وتوفر وحدة خفض الانبعاثات التخزينية ترميزا لا لبس فيه وتستخدم بيانات غير محدودة الطول، مع علامة نهاية البيانات في حالات محددة.
- يوفر نظام DER ترميزا لا لبس فيه ويستخدم علامات طول واضحة في حالات محددة.
- ومن بين هذه المجالات الثلاثة، فإن DER هو الذي تتم مواجهته عادة عند التعامل مع حمولات PKI والحمولات المشفرة.

على سبيل المثال: في DER، يتم تشفير قيمة 20 بت 1010 101100 1101 1110 على أنها :

- **العلامة**: bitstring) `0x03`)
- **الطول**: `0x04` (بايت)
- **القيمة**: `0x04De0`
- **تشفير DER الكامل**: `0x030404BCDE0`

البادئة 04 تعني أن ال 4 بت الأخيرة (تساوي التالي 0) من القيمة المشفرة يجب أن يتم تجاهلها لأن القيمة المشفرة لا تنتهي على حدود البايت.

ارجع إلى هذه المستندات من موقع معايير TU-T:

- قواعد الترميز X.690 ASN.1: مواصفات قواعد الترميز الأساسية (BER) وقواعد الترميز القانونية (CER) وقواعد الترميز المميزة (DER)

من موقع الويكيبيديا، ارجع إلى هذه الوثائق:

- قواعد التشفير الأساسية
- قواعد الترميز القانونية
- قواعد الترميز المميزة

عملية تفريغ DER HEX

يعرض IOS من Cisco وأجهزة الأمان المعدلة (ASA) وأجهزة أخرى محتوى DER كعملية **تفريغ سداسية عشرية** باستخدام الأمر **show running-config**. هنا هو المخرج:

```
crypto pki certificate chain root
                                certificate ca 01
3082017C A0030201 02020101 300D0609 2A864886 F70D0101 04050030 30820213
1D310C30 0A060355 040B1303 54414331 0D300B06 03550403 1304726F 6F74301E
170D3039 30373235 31313436 33325A17 0D313230 37323431 31343633 325A301D
...
```

يمكن تحويل هذا النوع من تفريغ السداسي العشري مرة أخرى إلى DER بطرق مختلفة. على سبيل المثال، يمكنك إزالة حروف المسافة وانتقالها إلى **البرنامج xxd**:

```
cat ca.hex | tr -d ' ' | xxd -r -p -c 32 | openssl x509 -inform der -text -noout $
```

والطريقة السهلة الأخرى هي إستخدام نص بيرل :

```
usr/bin/perl/!#
  } (<>) foreach
;s/[^a-fA-F0-9]//g
;((_$ ,"*print join("", pack("H
{
```

```
perl hex2der.pl < hex-file.txt > der-file.der $
```

بالإضافة إلى ذلك، تعد هذه العملية طريقة مضغوطة لتحويل **مقالب الذاكرة**، حيث تم نسخ كل منها يدويا مسبقا إلى ملف مع امتداد **.hex**، من سطر أوامر **bash** كما هو موضح هنا:

```
for hex in *.hex; do
    "{b="${hex%.hex
  hex2der.pl < "$hex" > "$b".der
openssl x509 -inform der -in "$b".der > "$b".pem
openssl x509 -in "$b".pem -text -noout > "$b".txt
done
```

ينتج عن كل ملف:

- **file.hex** - الملف الأصلي (يجب أن يحتوي على أرقام سداسية عشرية فقط).
- **file.der** - شهادة بتنسيق DER (ثنائي).

- **file.pem** - ترخيص بتنسيق PEM (Base64 + رأس/تذييل).
- **file.txt** - إصدار الشهادة سهل الاستخدام ويمكن قراءته.

تشفير Base64

يمثل ترميز Base64 البيانات الثنائية ذات الأحرف القابلة للطباعة (`/A-ZA-z0-9+`) مثل **ترميز uencode**. في التحويل من البيانات الثنائية إلى Base64، يتم تشفير كل مجموعة 6 بت من البيانات الأصلية إلى حرف ASCII قابل للطباعة 8 بت مع جدول ترجمة. لذلك، زاد حجم البيانات بعد الترميز بنسبة 33 في المائة (البيانات أوقات 8 مقسومة على 6 وحدات بت، تساوي 1.333).

يتم إستخدام مخزن مؤقت سعة 24 بت لترجمة ثلاث (3) مجموعات من ثماني (8) وحدات بت إلى أربع (4) مجموعات من ست (6) وحدات بت. لذلك قد يلزم وجود (1) أو (2) بايت للحشو في نهاية تدفق بيانات الإدخال. يتم الإشارة إلى الإضافة في نهاية البيانات التي تم ترميزها في Base64، بواسطة علامة واحد يساوي (=) لكل مجموعة مكونة من ثمانية (8) وحدات بت مضافة إلى الإدخال أثناء الترميز.

ارجع إلى هذا المثال من ويكيبيديا.

راجع أحدث المعلومات في RFC 4648: عمليات تشفير البيانات Base16 و Base32 و Base64.

تشفير PEM

يعد "البريد المحسن للخصوصية" (PEM) بمثابة وحدة PKI قياسية كاملة ل Internet Engineering Task Force (IETF)) لتبادل الرسائل الآمنة. لم يعد يتم إستخدامه على نطاق واسع على هذا النحو، ولكن صياغة التضمين الخاصة به تم اقتراضها على نطاق واسع من أجل تنسيق البيانات المرتبطة بالبنية الأساسية للبنية الأساسية (PKI) المشفرة بواسطة Base64 واستبدالها.

يقوم PEM RFC 1421، القسم 4.4: آلية التضمين، بتعريف رسائل PEM كما هي محددة بواسطة حدود التضمين (EBs)، والتي تستند إلى RFC 934، بهذا التنسيق:

```
-----BEGIN PRIVACY-ENHANCED MESSAGE-----
Header: value
Header: value
...

Base64-encoded data
...
-----END PRIVACY-ENHANCED MESSAGE-----
```

في الممارسة العملية اليوم، عند توزيع البيانات بتنسيق PEM، يتم إستخدام تنسيق الحدود هذا:

```
-----BEGIN type-----
...
-----END type-----
```

يمكن أن يكون **الكتابة** مع مفاتيح أو شهادات أخرى مثل:

- RSA
-
-
-
- X509

ملاحظة: على الرغم من أن وحدات RFC لا تجعل هذا إلزاميا، فإن عدد الشرطات البادئة والزائدة (-) في شبكات

الإنترنت (EB) كبير ويجب أن يكون دائما خمسة (5). وإلا، فإن بعض التطبيقات، مثل OpenSSL، تقوم بحظر الإدخال. ومن ناحية أخرى، لا تتطلب التطبيقات الأخرى، مثل Cisco IOS، عناوين EB على الإطلاق.

راجع أحدث RFCs هذه للحصول على مزيد من المعلومات:

- المعيار RFC 1421: تطبيق PEM الجزء الأول: إجراءات تشفير الرسائل والمصادقة
- المعيار RFC 1422: إدارة المفاتيح القائمة على الشهادة (PEM) الجزء الثاني: إدارة المفاتيح القائمة على الشهادة
- المعيار RFC 1423: وحدات توسعة المنافذ (PEM) الجزء الثالث: الخوارزميات والأوضاع والمعرفات
- المعيار RFC 1424: تطبيق PEM الجزء الرابع: إصدار الشهادات الرئيسية والخدمات ذات الصلة

شهادات X.509 و CRLs

X.509 هي مجموعة فرعية من X.500، وهي مواصفات ITU موسعة حول اتصال الأنظمة المفتوحة. وهو يتناول على وجه التحديد الشهادات والمفاتيح العامة، وقد قامت الهيئة بتكييفه كمعيار على الإنترنت. يوفر X.509 بنية وبناء جملة، يتم التعبير عنهما في RFC بتدوين ASN.1، لتخزين معلومات الشهادة وقوائم إبطال الشهادات.

في X.509 PKI، يصدر المرجع المصدق شهادة تربط مفتاح عام، على سبيل المثال: مفتاح Rivest-Shamir-Adleman (RSA) أو مفتاح خوارزمية التوقيع الرقمي (DSA) باسم مميز معين (DN)، أو باسم بديل مثل عنوان البريد الإلكتروني أو اسم المجال المؤهل بالكامل (FQDN). تتبع شبكة DN البنية الواردة في معايير X.500. فيما يلي مثال:

```
CN=الاسم الشائع، L=الموقع، OU=Organization-unit، O=Organization، C=البلد
```

وبسبب تعريف ASN.1، يمكن تشفير بيانات X.509 إلى DER من أجل إستبدالها في شكل ثنائي، وتحويلها إختياريا إلى Base64/PEM لوسائل اتصال تستند إلى نص، مثل لصق النسخ على وحدة طرفية.

- ارجع إلى مستند معايير ITU-T هذا X.509 Open Systems Interconnection - الدليل: أطر شهادات السمات والمفتاح العام.
- راجع ملف تعريف قائمة إلغاء الشهادة (CRL) وشهادة X.509 وفقا لمعيار RFC 5280 للحصول على مزيد من المعلومات.

معايير PKCS

إن معايير التشفير باستخدام المفاتيح العامة (PKCS) عبارة عن مواصفات مستمدة من مختبرات RSA تطورت جزئيا إلى معايير صناعية. وتتناول تلك المواضيع التي غالبا ما تصادف هذه المواضيع؛ غير أن هذه المواضيع لا تتناول جميعها أشكال البيانات.

RFC 3347) **PKCS#1**) - يغطي جوانب التنفيذ للتشفير المستند إلى خوارزمية RSA (بدايات التشفير، أنظمة التشفير/التوقيع، بناء جملة ASN.1).

RFC 2898) **PKCS#5**) - يغطي اشتقاق المفتاح المستند إلى كلمة المرور.

RFC 2315) **PKCS#7**) وRFC 3852 **S/MIME** - يحدد صياغة رسالة لإرسال البيانات الموقعة والمشفرة والشهادات ذات الصلة. يستخدم غالبا كحاوية لشهادات X.509.

PKCS#8 - يحدد صياغة الرسالة لنقل أزواج مفاتيح RSA المشفرة أو النصوص غير المشفرة.

RFC 2985) **PKCS#9**) - يحدد فئات كائن إضافية وسمات هوية.

RFC 2986) **PKCS#10**) - يحدد صياغة رسالة لطلبات توقيع الشهادة (CSRs). يتم إرسال CSR من قبل كيان إلى

CA ويحتوي على المعلومات التي سيتم توقيعها من CA، مثل معلومات المفتاح العام والهوية والسمات الإضافية.

PKCS#12 - يحدد حاوية لتعبئة بيانات PKI ذات الصلة (بشكل نموذجي، **زوج مفاتيح الكيان + شهادة الكيان + شهادات CA الجذر والمتوسط**) ضمن ملف واحد. إنه تطور تنسيق Microsoft Personal Information Exchange (PFX)).

ارجع إلى هذه الموارد:
- مقال على بي كي سي
- صفحة مختبرات RSA على PKCS

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).