EAP 1.01版證書指南

目錄

簡介 必要條件 需求 採用元件 慣例 伺服器證書 主題欄位 頒發者欄位 增強型金鑰使用欄位 根CA證書 主題和頒發者欄位 中繼CA憑證 主題欄位 頒發者欄位 使用者端憑證 頒發者欄位 增強型金鑰使用欄位 主題欄位 主題替代名稱欄位 電腦證書 主題和SAN欄位 頒發者欄位 附錄A — 通用證書擴展 附錄B — 證書格式轉換 附錄C — 證書有效期 相關資訊

<u>簡介</u>

本文檔澄清了與各種形式的可擴展身份驗證協定(EAP)相關的各種證書型別、格式和要求所伴隨的 一些混淆。本文討論的與EAP相關的五種證書型別是伺服器、根CA、中間CA、客戶端和電腦。這 些證書有不同的格式,並且根據涉及的EAP實施對每種證書可能有不同的要求。

<u>必要條件</u>

本文件沒有特定需求。

<u>採用元件</u>

本文件所述內容不限於特定軟體和硬體版本。

<u>慣例</u>

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

<u>伺服器證書</u>

伺服器證書安裝在RADIUS伺服器上,其在EAP中的主要用途是建立加密的傳輸層安全(TLS)隧道 ,以保護身份驗證資訊。使用EAP-MSCHAPv2時,伺服器證書將承擔輔助角色,該輔助角色將 RADIUS伺服器標識為身份驗證的可信實體。此輔助角色是通過使用Enhanced Key Usage(EKU)欄 位完成的。EKU欄位將證書標識為有效的伺服器證書,並驗證頒發證書的根CA是否為受信任的根 CA。這需要存在根<u>CA證書</u>。Cisco Secure ACS要求證書採用Base64編碼或DER編碼的二進位制 X.509 v3格式。

您可以使用提交到CA的ACS中的憑證簽署請求(CSR)建立此憑證。或者,也可以使用內部CA(如 Microsoft證書服務)證書建立表單剪下證書。必須注意的是,雖然您可以建立金鑰大小大於1024的 伺服器證書,但任何大於1024的金鑰都不適用於PEAP。即使身份驗證通過,客戶端也會掛起。

如果使用CSR建立證書,則會使用.cer、.pem或.txt格式建立證書。在極少數情況下,建立時沒有副 檔名。確保您的證書是純文字檔案檔案,其副檔名可以根據需要更改(ACS裝置使用.cer或.pem副 檔名)。此外,如果您使用CSR,則會在您指定的路徑中建立憑證的私密金鑰,該路徑可能包含也 可能不包含延伸模組且具有相關聯的密碼(在ACS上安裝時需要該密碼)。 無論副檔名如何,請確 保它是具有副檔名的純文字檔案檔案,您可以根據需要對其進行更改(ACS裝置使用.pvk或.pem副 檔名)。 如果沒有為私鑰指定路徑,ACS會將金鑰儲存在C:\Program Files \CiscoSecure ACS vx.x \CSAdmin \Logs目錄中,並在安裝證書時沒有為私鑰檔案指定路徑時在此目錄中查詢。

如果使用Microsoft證書服務證書提交表單建立證書,請確保將金鑰標籤為可匯出,以便可以在 ACS中安裝證書。以這種方式建立證書可顯著簡化安裝過程。您可以從證書服務Web介面直接將其 安裝到正確的Windows應用商店中,然後使用CN作為參考從儲存中安裝到ACS上。安裝在本地電腦 儲存中的證書也可以從Windows儲存匯出並輕鬆安裝在另一台電腦上。匯出此類證書時,需要將金 鑰標籤為可匯出並給定密碼。證書隨後以.pfx格式顯示,其中包括私鑰和伺服器證書。

在Windows證書儲存中正確安裝後,伺服器證書需要顯示在Certificates(Local Computer)> Personal > Certificates資料夾中,如本示例視窗所示。



自簽名證書是您建立的沒有根證書或CA中間參與的證書。它們在subject和issuer欄位中具有相同的 值,如根CA證書。大多數自簽名證書使用X.509 v1格式。因此,它們不適用於ACS。但是,自版本 3.3起,ACS能夠建立自己的自簽名證書,您可以將其用於EAP-TLS和PEAP。請勿使用大於1024的 金鑰大小來相容PEAP和EAP-TLS。如果您使用自簽名證書,則證書還以根CA證書的容量運行,並 且當您使用Microsoft EAP請求方時,必須安裝在客戶端的**證書(本地電腦)>受信任的根證書頒發** 機構>證書資料夾中。它會自動安裝在伺服器上的受信任根證書儲存中。但是,在ACS證書設定中 的證書信任清單中仍然必須信任它。如需詳細資訊,請參閱根CA憑證一節。

由於使用Microsoft EAP請求方時,自簽名證書用作伺服器證書的根CA證書,並且由於有效期不能 從預設的一年延長,因此Cisco建議您僅將這些證書用於EAP作為臨時措施,直到可以使用傳統 CA。

<u>主題欄位</u>

Subject欄位標識證書。CN值用於確定證書的「常規」頁籤中的「頒發給」欄位,並填充了您在 ACS「CSR」對話方塊的「證書主題」欄位中輸入的資訊,或填充了Microsoft證書服務中「名稱」 欄位的資訊。如果使用了從儲存安裝證書的選項,則CN值用於告知ACS需要在本地電腦證書儲存中 使用哪種證書。



<u>頒發者欄位</u>

Issuer欄位標識剪下證書的CA。使用此值可確定證書的「常規」頁籤中「頒發者」欄位的值。它將 用CA的名稱填充。

now: <all></all>	
Field	Value
E Version	V3
🚍 Serial number	48A6 7397 0000 0000 0012
🚍 Signature algorithm	sha1RSA
🚍 Issuer	Standalone31, SLC TAC, US
Valid from	Monday, July 19, 2004 11:33:
💳 Yalid to	Tuesday, July 19, 2005 11:43
💳 Subject	test, SLC TAC, US
🚍 Public key	R5A (1024 Bits)
IN = Standalone31) = SLC TAC I = US	

<u>增強型金鑰使用欄位</u>

Enhanced Key Usage欄位可識別憑證的預期用途,需列為「伺服器驗證」。 當您使用Microsoft的 PEAP和EAP-TLS請求方時,此欄位為必填欄位。使用Microsoft Certificate Services時,將在獨立 CA中配置,並且從「目標用途」下拉選單中選擇Server Authentication Certificate,在「企業CA」 中配置,並且從「證書模板」下拉選單中選擇Web Server。如果您使用具有Microsoft證書服務的 CSR來請求證書,則您沒有選擇使用獨立CA指定目標用途。因此,不存在EKU欄位。使用企業 CA,您將看到「目標用途」下拉選單。某些CA不使用EKU欄位建立證書,因此當您使用Microsoft EAP請求方時,它們無用。

how: <all></all>	
Field	Value
🚍 Issuer	Standalone31, SLC TAC, US
🔚 Valid from	Monday, July 19, 2004 11:33:
🗖 Valid to	Tuesday, July 19, 2005 11:43
Subject	test, SLC TAC, US
🗖 Public key	R5A (1024 Bits)
💽 Enhanced Key Usage	Server Authentication(1.3.6.1
💽 Subject Key Identifier	6c 61 ad e0 59 62 68 3a ae 65
Authority Key Identifier	KeyID=73 ed fb c2 bf c9 d1 3
berver Auchenticacion(1.5.6.1.5	.5,7,3,1)

<u>根CA證書</u>

根CA證書的用途之一是將伺服器證書(以及中間CA證書,如果適用)標識為ACS和Windows EAP-MSCHAPv2請求方的受信任證書。它必須位於ACS伺服器上的Windows中的受信任的根憑證授權庫 中,如果是EAP-MSCHAPv2,則位於客戶端電腦上。大多數第三方根CA證書都隨Windows一起安 裝,因此幾乎不費吹灰之力。如果使用Microsoft證書服務,並且證書伺服器與ACS位於同一電腦上 ,則自動安裝根CA證書。如果在Windows的受信任的根證書頒發機構儲存中找不到根CA證書,則 必須從CA獲取並安裝該證書。在Windows證書儲存中正確安裝後,根CA證書需要顯示在 Certificates(Local Computer)> Trusted Root Certification Authorities > Certificates資料夾中,如本 示例視窗所示。

Tree Examples	IssedTo A	liss and Ey	Expisation Date:	Intended Purposes	Fige
Conseia Past	SecureSian RootC42	SecureSign RoolCA2	9(15/2020	Secure Enel, Server	Jap
Cartificates (Loca Cortration)	SecureSign RootCA3	Securation RootCA3	9/15/2020	Secure Ental, Server	30
R- Fersonal	SelfSigned	SelfSigned	6(24)2005	Serve: Authentication	-OW
E-📴 Trusted Root Certification Authorities	SERVICIOS DE CERTIFICACION~	SERVICIOS DE CERTIFICACION - A	3(9)2009	Secure Enal, Server	ÆF
L- Certficates	SIA Secure Client CA	SIA Secure Clenk CA	7/3/20:9	Secure Email, Server	Sec
🖻 🛅 Enterprise Frast	STA Secure Server CA	STA Becure Server CA	7)5(20.9	Secure Email, Server	300
E-Contermediate Certification Authorities	SJCA	SJCA	3/27/2006	<4lb	-OV
🕮 - 🦲 Trusted Publishers	Sonora Classil CA	Sonora Clarat CA	1/5/2021	Clent Authentication	Son
🗷 🔛 Untrusted Certificetes	Sonera Class2 CA	Sonera Class2 CA	4/5/2021	Server Authenticatio	Son
🗄 🧰 Ihrd-Arty Root Certification Authoritie	Pandaine31	9 and ime31	3/30/2006	cWla	<n <="" td=""></n>
🕀 🦲 Trusted People	I Sreto	2.reto	0/19/2040	500) s	dVA.
0 ACSCortStore	Swikskey Root CA	Swester Fact CA	12/31/2015	Secure Enal, Server	SWE
H- COULStore	Symante: Foot CA	Symantec Root CA	4/30/2011	-sAlla	-SVA
B-III Other People	IC Instuenter Class 1 CA	C TrustCenter Class 1 CA	1/1/2001	Secure Engl, Server	10
E-Certificace Enrolment Requests	TC TrustCenter Class 2 FA	TC TrustCenter Class 2 CA	14(20-1	Secure Final, Server	TC
E-C SPC	TC TrustCenter Cless 3 CA	TC TrustCenter Class D CA	1/1/2011	Secure Driel, Server	TC 2
E-terge Centricates - Content Oser	TC TrustCenter Class 4 CA	TC TrustCenter Class 4 CA	1/1/20:1	Secure Enal, Seiver	TC 1
information and the state of th	TC TrustCenter Time Stamping CA	"C TrustCenter Time Stemping CA	1/1/20:1	Time Stemping	TO
# C Enterreixe Drust:	Telekom-Control-Kommission Top 1	Telekom-Contro-Kommission Top-U	9/24/2005	Server Authenticatio	Aus
III Categoria Certification & therities	Thavte Persona Basir CA	Thavle Personal Basic CA	12(3)(2020	Clent Authentication	That
🗷 🦲 Active Dreitto Y Liser Object 📃	Thavte Persone Freemail CA	Therete Personal Freemail CA	12/31/2020	Clent Authentication	The
w 🦲 trusted -ublishers	Thaste Persona Prenium CA	Thatwise Personal Priemium CA	12/30/2020	Clent Authentication.	Ibe
🕸 🦲 Untrusted Certificates	Theaste Premium Server CA	Therefore Premum Server Co.	12/31/2020	Server Authenticatio	The
🗄 🧰 Third Norty Root Contification Authoritie	Thavte Server CA	Thankle Server CA	12/31/2020	Server Authenticath	Thew
distanti in Martin	4			······································	Constant in

主題和頒發者欄位

Subject和Issuer欄位標識CA,並且需要完全相同。使用這些欄位填充證書的「常規」頁籤中的「頒 發給」和「頒發者」欄位。使用根CA的名稱填充。



<u>中繼CA憑證</u>

中間CA證書是用來標識從屬於根CA的CA的證書。某些伺服器證書(Verisign的無線證書)是使用 中間CA建立的。如果使用中間CA剪下的伺服器證書,則中間CA證書必須安裝在ACS伺服器上本地 電腦儲存的中間證書頒發機構區域中。此外,如果在客戶端上使用Microsoft EAP請求方,則建立中 間CA證書的根CA的根CA證書也必須位於ACS伺服器和客戶端上的相應儲存區中,以便可以建立信 任鏈。根CA證書和中間CA證書必須在ACS和客戶端上標籤為受信任。大多數中繼CA證書未隨 Windows一起安裝,因此您可能需要從供應商處獲取這些證書。在Windows證書儲存中正確安裝後 ,中間CA證書將顯示在Certificates(Local Computer)> Intermediate Certification Authorities > Certificates資料夾中,如本示例視窗所示。

Action Sew Eavorkes 👍 🔿 🔃					
166 Favorites	Essued To /	Issued Ey	ExpirationDate	Intended Purposes	Friend
Corsole Root Certificates (Loca Computer) Certificates (Loca Computer) Certificates (Loca Computer) Certificates (Loca Computer) Certificates (Loca Computer) Certificates Certification Authorities Certificate Revocation List Certificate Revocation List Certificate Revocation List Certificate Revocation List Certificate Certification Authorities Certificate Certification Authorities Certificate Certification Authorities Certificate Enrolment Requests Certificates - Carrent User Certificates - Carrent User	Gobellign Root CA GTE Cyber Trust Root Microsoft Windows Hardware Com Ints SUC Authority Root Agency Socure/Wet CA SOC Root Thavite Premium Server CA Thavite Server CA Unit - DATACory SoC VerSign Class 1 CA Individual Sul VerSign Class 2 CA - Individual Sul VerVal.vettsign Com/CFS Incorpibly	Root SGC Authority Root SGC Authority Microsoft Root Authority Root SGC Authority Class 1 Public Primary Cartification A Class 3 Public Primary Cartification A	1/20/201- 2/23/2006 12/31/2002 1/1/2009 12/31/2009 12/31/2009 7/16/200- 7/16/200- 6/24/2019 5/12/2006 1/5/2004 1/5/2004	1.0.5.1.4.1 911.10 1.3.5.1.4.1 911.10 Code Signing, Winds Server Authenticath 441» 1.3.5.1.4.1 911.10 1.3.5.1.4.1 911.10 1.3.5.1.4.1 911.10 441» 441» 2.16.840.1.113435	 Alvenic Alvenic

主題欄位

Subject欄位標識中間CA。此值用於確定證書的「常規」頁籤中的「頒發給」欄位。

Field	Value
Issuer	Class 3 Public Primary Certifica
Valid from	Wednesday, April 16, 1997 6:
Valid to	Wednesday, January 07, 200
Subject	www.verisign.com/CPS Incorp
Public key	RSA (1024 Bits) —
Basic Constraints	Subject Type=CA, Path Lengt
🕒 Key Usage	Certificate Signing, Off-line CR
NetscapeCertType	SSL CA, SMIME CA(06)
U = www.verisign.com/CPS U = VeriSign International S U = VeriSign, Inc.) = VeriSign Trust Network	Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign erver CA - Class 3

<u>頒發者欄位</u>

Issuer欄位標識剪下證書的CA。使用此值可確定證書的「常規」頁籤中「頒發者」欄位的值。它將 用CA的名稱填充。



使用者端憑證

「客戶端證書」用於在EAP-TLS中正面標識使用者。它們在構建TLS隧道方面不起作用,不用於加 密。通過三種方式之一完成陽性識別:

- CN(或名稱)Comparison 將證書中的CN與資料庫中的使用者名稱進行比較。有關此比較 型別的更多資訊包含在證書的Subject欄位的描述中。
- SAN Comparison 將證書中的SAN與資料庫中的使用者名稱進行比較。僅從ACS 3.2開始支援此比較。有關此比較型別的更多資訊包含在證書的「使用者可選名稱」欄位的描述中。
- Binary Comparison 將證書與資料庫中儲存的證書的二進位制副本進行比較(只有AD和LDAP可以做到這一點)。 如果使用證書二進位制比較,必須以二進位制格式儲存使用者證書。此外,對於通用LDAP和Active Directory,儲存證書的屬性必須是名為「usercertificate」的標準LDAP屬性。

無論使用哪種比較方法,相應欄位(CN或SAN)中的資訊都必須與資料庫用於身份驗證的名稱相匹 配。AD在混合模式下使用NetBios名稱進行身份驗證,在本機模式下使用UPN。

本節討論使用Microsoft證書服務生成客戶端證書。EAP-TLS需要唯一的客戶端證書才能對每個使用 者進行身份驗證。必須在每台電腦上為每個使用者安裝證書。正確安裝後,憑證位於Certificates -Current User > Personal > Certificates資料夾中,如本範例視窗所示。

Tal ansale Roorly entiticates - Linnent Resrute	isonal) i embrates				
avuu den Panutes 🖶 🔿 🖬 🖬	1 × 10 × 27 3 2				
Tree Faverites	Lound To 🔺	Issued By	Espiration Date	Intended Purposes	Friend
Corado Root Certificates (Loca Cimputer) Certificates - Current User Certificates - Current User Certificates III - Certificates IIII - Certificates IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		Standal(mess)	112212005	Uent Authentication	(M)DS
Personal abore contains 1 certificate			U.		A

<u>頒發者欄位</u>

Issuer欄位標識削減證書的CA。使用此值可確定證書的「常規」頁籤中「頒發者」欄位的值。這將 使用CA的名稱填充。

Field Value Serial number 2E48 0C22 0000 0000 0 Signature algorithm sha1RSA Issuer SPORKSENTCA, Booga Valid from Thursday, July 22, 200 Valid to Friday, July 22, 2005 7 Subject CiscoBoy, Users, Booga Public key RSA (1024 Bits) Key Usage Digital Signature, Key E IN = SPORKSENTCA SPORKSENTCA C = Booga OC = local	ow: Zôlls	-
Field Value Serial number 2E48 0C22 0000 0000 0 Signature algorithm sha1RSA Issuer SPORKSENTCA, Booga, Valid from Thursday, July 22, 2005 7 Valid to Friday, July 22, 2005 7 Subject CiscoBoy, Users, Booga Public key RSA (1024 Bits) Key Usage Digital Signature, Key E N = SPORKSENTCA Signature, Key E	uw: Isais	
Serial number 2E48 0C22 0000 0000 0 Signature algorithm sha1RSA Issuer SPORKSENTCA, Booga, Valid from Thursday, July 22, 2005 7 Valid to Friday, July 22, 2005 7 Subject CiscoBoy, Users, Booga Public key RSA (1024 Bits) N = SPORKSENTCA Digital Signature, Key E N = SPORKSENTCA Signature algorithm C = Booga Signature algorithm	Pield	Value
Signature algorithm sha1RSA Issuer SPORKSENTCA, Booga, Valid from Thursday, July 22, 200 Valid to Friday, July 22, 2005 7 Subject CiscoBoy, Users, Booga Public key RSA (1024 Bits) Key Usage Digital Signature, Key E IN = SPORKSENTCA SPORKSENTCA C = Booga SPORKSENTCA	Serial number	2E48 0C22 0000 0000 000A
Issuer SPORKSENTCA, Booga, Valid from Thursday, July 22, 2005 7 Valid to Friday, July 22, 2005 7 Subject CiscoBoy, Users, Booga Public key RSA (1024 Bits) Key Usage Digital Signature, Key E N = SPORKSENTCA C = Booga C = local C = local	Signature algorithm	sha1RSA
Valid from Thursday, July 22, 200 Valid to Friday, July 22, 2005 7 Subject CiscoBoy, Users, Booga Public key RSA (1024 Bits) Key Usage Digital Signature, Key E N = SPORKSENTCA C = Booga C = local	Issuer	SPORKSENTCA, Booga, local
Valid to Friday, July 22, 2005 7 Subject CiscoBoy, Users, Booga Public key RSA (1024 Bits) Key Usage Digital Signature, Key E N = SPORKSENTCA C = Booga C = local C = local	Valid from	Thursday, July 22, 2004 7:23:
Subject CiscoBoy, Users, Booga Public key RSA (1024 Bits) Key Usage Digital Signature, Key E N = SPORKSENTCA C = Booga C = local	Valid to	Friday, July 22, 2005 7:23:21
Public key RSA (1024 Bits) Key Usage Digital Signature, Key E N = SPORKSENTCA C = Booga C = local	Subject	CiscoBoy, Users, Booga, local
E Key Usage Digital Signature, Key E N = SPORKSENTCA C = Booga C = local	Public key	RSA (1024 Bits)
N = SPORKSENTCA C = Booga C = local	🕃 Key Usage	Digital Signature, Key Encipher 🛓
Edit Properties	N = SPORKSENTCA C = Booga C = local	Edit Properties ⊆opy to File

<u>增強型金鑰使用欄位</u>

Enhanced Key Usage欄位會識別憑證的預期用途,並需要包含使用者端驗證。當您使用 Microsoft的PEAP和EAP-TLS請求方時,此欄位為必填欄位。使用Microsoft證書服務時,當您從 目標用途」下拉選單中選擇Client Authentication Certificate時,會在獨立CA中配置此服務;當您從 「證書模板」下拉選單中選擇User時,會在企業CA中配置此服務。如果您使用具有Microsoft證書服 務的CSR來請求證書,則您沒有選擇使用獨立CA指定目標用途。因此,不存在EKU欄位。使用企業 CA,您將看到「目標用途」下拉選單。某些CA不使用EKU欄位建立證書。當您使用Microsoft EAP請求方時,它們毫無用處。

Field	Value	
Authority Key Identifier CRL Distribution Points Authority Information Access	KeyID=6e 70 3c ae 4c 71 af 2 [1]CRL Distribution Point: Distr [1]Authority Info Access: Acc	
Enhanced Key Usage Subject Alternative Name Thumbprint algorithm Thumbprint	Encrypting File System(1.3.6 Other Name:Principal Name=C sha1 17EB A9F1 4031 6C1F 50AF 9	
incrypting File System(1.3.6.1.4.1 iecure Email(1.3.6.1.5.5.7.3.4) lient Authentication(1.3.6.1.5.5.7	.311.10.3.4) 7.3.2)	- 3

主題欄位

此欄位用於CN比較。將列出的第一個CN與資料庫進行比較以查詢匹配項。如果找到匹配項,則身 份驗證成功。如果您使用獨立CA,則CN中會填充您在證書提交表單中Name欄位輸入的任何內容。 如果您使用企業CA,則CN會自動填充在Active Directory使用者和電腦控制檯中列出的帳戶名稱 (這不一定與UPN或NetBios名稱匹配)。

how: <all></all>		
Field	Value	
Issuer	SPORKSENTCA, Booga, local	
🔁 Valid from	Thursday, July 22, 2004 7:23:	
🚍 Valid to	Friday, July 22, 2005 7:23:21	
🚍 Subject	CiscoBoy, Users, Booga, local	-
Public key	RSA (1024 Bits)	
💽 Key Usage	Digital Signature, Key Encipher	
SMIME Capabilities	[1]SMIME Capability: Object I	
	20713000219928090301	
IN = Ciscoboy IN = Users DC = Booga DC = local		
	(

主題替代名稱欄位

Subject Alternative Name欄位用於SAN比較。將列出的SAN與資料庫進行比較以查詢匹配項。如果 找到匹配項,則身份驗證成功。如果您使用企業CA,則SAN會自動填充Active Directory登入名 @domain(UPN)。 獨立CA不包括SAN欄位,因此不能使用SAN比較。

how: <all></all>	
Field	Value
Authority Key Identifier CRL Distribution Points Authority Information Access	KeyID=6e 70 3c ae 4c 71 af 2 [1]CRL Distribution Point: Distr [1]Authority Info Access: Acc
🔂 Enhanced Key Usage	Encrypting File System(1.3.6
Thumbprint algorithm	sha1 17EB A9F1 4031 6C1F 50AF 9
Other Name: Principal Name=CiscoBoy@Boog	ja.local



使用電腦身份驗證時,電腦證書在EAP-TLS中使用,以主動識別電腦。只有當您配置Microsoft Enterprise CA進行證書自動註冊並將電腦加入域時,才能訪問這些證書。當您使用電腦的Active Directory憑證並將其安裝在本地電腦儲存中時,將自動建立證書。配置自動註冊之前已是域成員的 電腦將在下次Windows重新啟動時收到證書。電腦證書安裝在證書(本地電腦)MMC管理單元的**證 書(Certificates)>個人>證書**資料夾中,與伺服器證書一樣。由於無法匯出私鑰,因此無法在任何其 他電腦上安裝這些證書。

<u>主題和SAN欄位</u>

Subject和SAN欄位標識電腦。該值由電腦的完全限定名稱填充,並用於確定證書的「常規」頁籤中的「頒發給」欄位,對於「主題」和「SAN」欄位都相同。

I SALS	
Held	Value
Subject	regis.Booga.lccal
E Fublc key	PSA (1024 Bits)
💽 Key Usage	Digital Signature, Key Encipher
SMIME Capablities	[I]SMIME Capability: Object I
Enhanced Key Usage	Client Authentication(1.3.6.1
Certificate Template	Machine
Subject Key Identifier	5r 3d be fr 55 1b 35 3r 06 1e
_N = regis.300ga local	

<u>頒發者欄位</u>

Issuer欄位標識剪下證書的CA。使用此值可確定證書的「常規」頁籤中「頒發者」欄位的值。它將 用CA的名稱填充。

how: CAIS	
ried	Value 🔺
🚍 Signature algorithm	shalRSA
- İssuer	SPCRIKSENTCA, Booga, local
Vaid from	Tuesday, July 27, 2004 6:10
vald to	Wednesday, July 27, 2005 6
5ubject	regis.Eooga local
Public Key	FSP (1024 Ets)
💽 Key Usage	Digital Signature, Key Encohert
IN = SPCRKSENTCA IC = Eooga	
,c – loca	

<u> 附錄A — 通用證書擴展</u>

.csr — 這實際上不是證書,而是證書簽名請求。它是採用以下格式的純文字檔案檔案:

----BEGIN CERTIFICATE REQUEST----MIIBtDCCAR0CAQIwDzENMAsGA1UEAxMETW9yazCBnzANBgkqhkiG9w0BAQEFAAOB jQAwgYkCgYEAu3duNPToM711jadL1hMWTMT12yzDn2btVQsWHjdS9FARBOpVIuQe BAMCBkAwDQYJKoZIhvcNAQEFBQADgYEAkvHoMkTY0mhHwavsDey8IN7DsN0Io6vP tyjWnoKzHycO6NHt3k7f55Ch/nQ6ONSGBs02uYpjUUPJPq1hGBY4VEcV39zdPNs8 uPCuex/LZ4sOqgmd6WOxup3rEI01fJnqjpd7fwbX9Jr3Awc1gFsXS0Kg3WnjJD4i ILII9Vhw89s=

----END CERTIFICATE REQUEST----

.pvk — 此擴展表示私鑰,儘管此擴展不保證內容實際是私鑰。內容必須是採用以下格式的純文字檔 案: ----BEGIN RSA PRIVATE KEY----Proc-Type: 4,ENCRYPTED DEK-Info: DES-EDE3-CBC,751DA1C8E250B96B

YyLE3zsDTY1+Kq+6gAUF+YCO452KHmQJQn7AKxMnDqHeQrAePReL/zuxHiKsBjrN h2FGzV17bBVnBQZ/Ci/j92HYeQ2VZD8wB61YFsWV/30kYeyPYRctweteKFfgpFHi /ES9B0bWzrpFS1E1+I2L6o1dwnUkmMBIC1j1WNV3Xo+/5NFei1mdlgRMRtzR85Ub 4hUWzWCsRSFEcHEcNcsfxkach9stzkIMWB6d7RyvWyqNfb62702MhMhA9T01LYri NdM/Tsdz3Kfc7AXiNMvti5R0mSV89d6epLLE69PTWZLNxasCsCybhNt/ya/z7y1S oE4iBAwdZ9jCyuBB9viLBqps39zfiYrRTDkDXiVH3oIWKBbM30Ew3apgLFZiVRqZ 07xaX7oQyy4tQfo4UNnhPTX3kiMBA6t6UJvs6VIHsIIXYEY1HbL6bA== ----END RSA PRIVATE KEY----

.cer — 這是一個表示證書的通用擴展。伺服器、根CA和中間CA證書可以採用此格式。它通常是一 個副檔名的純文字檔案檔案,您可以根據需要進行更改,可以是DER格式或Base 64格式。可以將 此格式匯入Windows證書儲存區。

.pem — 此副檔名為Privacy Enhanced Mail。此擴展通常用於UNIX、Linux、BSD等。它通常用於 伺服器證書和私鑰,通常是一個副檔名為.pem到.cer的純文字檔案檔案,您可以根據需要對其進行 更改,以便將其匯入到Windows證書儲存區。

.cer和.pem檔案的內部內容通常類似於以下輸出:

----BEGIN CERTIFICATE----

MIIDhTCCAy+gAwIBAgIKSKZzlwAAAAAAEjANBgkqhkiG9w0BAQUFADA2MQswCQYD VQQGEwJVUzEQMA4GA1UEChMHU0xDIFRBQzEVMBMGA1UEAxMMU3RhbmRhbG9uZTMx MB4XDTA0MDcxOTE3MzMyNVoXDTA1MDcxOTE3NDMyNVowLjELMAkGA1UEBhMCVVMx AAQAGBvkDy7BaMBJgFRuS+QU8o2XfH5aAQiCcyKu/jK6mMt64QyCy9k= ----END CERTIFICATE----

.pfx — 此副檔名表示個人資訊交換。此格式是一種方法,可用於將證書捆綁到單個檔案中。例如 ,您可以將伺服器證書及其關聯的私鑰和根CA證書捆綁到一個檔案中,並輕鬆將該檔案匯入適當的 Windows證書儲存區。最常用於伺服器和客戶端證書。很遺憾,如果包含根CA證書,則根CA證書 始終安裝在當前使用者儲存而不是本地電腦儲存中,即使指定了本地電腦儲存進行安裝。

.p12 -通常只有客戶端證書才會顯示此格式。可以將此格式匯入Windows證書儲存區。

.p7b — 這是將多個證書儲存在一個檔案中的另一種格式。可以將此格式匯入Windows證書儲存區。

<u>附錄B — 證書格式轉換</u>

在大多數情況下,當您更改副檔名(例如,從.pem更改為.cer)時會發生證書轉換,因為證書通常 採用純文字檔案格式。有時,證書不是純文字檔案格式,您必須使用<u>OpenSSL</u>等工具對其進行轉 換。例如,ACS解決方案引擎無法安裝.pfx格式的證書。因此,必須將憑證和私鑰轉換為可用格式 。以下是OpenSSL的基本命令語法:

openssl pkcs12 -in c:\certs \test.pfx -out c:\certs \test.pem

系統將提示您輸入匯入密碼和PEM密碼短語。這些密碼必須相同,並且是在匯出.pfx時指定的私鑰 密碼。輸出是一個.pem檔案,該檔案包含.pfx中的所有證書和私鑰。此檔案可在ACS中同時稱為證 書和私鑰檔案,安裝時不會出現問題。

<u> 附錄C — 證書有效期</u>

憑證僅在其有效期期間內可用。根CA證書的有效期是在建立根CA時確定的,可以變化。中間CA證書的有效期在建立CA時確定,並且不能超過其從屬的根CA的有效期。使用Microsoft證書服務,伺服器、客戶端和電腦證書的有效期將自動設定為一年。只有當您按照<u>Microsoft知識庫文章254632</u>對Windows登錄檔進行駭客攻擊時,才能更改此值,並且此值不能超過根CA的有效期。ACS生成的自簽名證書的有效期始終為一年,在當前版本中無法更改。

相關資訊

- RADIUS 支援頁面
- <u>要求建議 (RFC)</u>
- <u>技術支援 Cisco Systems</u>