draft-friel-acme-integrations

ACME TEAP integration

Friel, Barnes cisco

Summary

- TEAP (RFC 7170) defines how a Peer can perform certificate enrolment by exchanging PKCS#10 / PKCS#7 payloads with a TEAP server
- TEAP does not define how the TEAP server interacts with the CA
- ACME "describes a protocol that a CA and an applicant can use to automate the process of ... certificate issuance."
- draft-friel-acme-integrations describes how a TEAP server can leverage ACME to integrate with a CA for automated certificate issuance
 - Equally applicable to TEAP-BRKSI (draft-lear-eap-teap-brski)
 - No changes required to existing ACME or TEAP drafts (probably)

draft-friel-acme-integrations Use Cases

- ACME issuance of sub-domain certificates
- Multiple client / device certificate integrations
 - 1. EST
 - RFC 7030 Enrollment over Secure Transport
 - 2. BRSKI
 - draft-ietf-anima-bootstrapping-keyinfra Bootstrapping Remote Key Infrastructures
 - **3. TEAP**
 - RFC 7170 Tunnel Extensible Authentication Protocol
 - 4. TEAP-BRSKI
 - draft-lear-eap-teap-brski Bootstrapping Key Infrastructure over EAP

TEAP -> ACME 1 of 3

• ACME domain authorization



TEAP -> ACME 2 of 3

• Peer establishes TEAP outer TLS tunnel

+	edge	+ TEAP-9	Server	ACME	++ DNS
		+		1	++
	STEP 2:	Establs	; h EAP Outer Tunnel		100 A
		25 000 25.			
	EAP-Request/				
	Type=Identity				
	<				
	EAP-Response/				
	Type=Identity			i	
		>			
	Type=TFAP.				
	TEAP Start,			i i	
	Authority-ID T	LV			
	<				
	FAP-Response/				
	Type=TEAP,			i	
	TLS(ClientHell	o)		l l	
		>			
	 FAP-Request/				
	Type=TEAP,			1	
	TLS(ServerHell	ο,		i	
	Certificate,				
	ServerKeyExcha	nge,			
	Certificatereq	uest, ∍)			
	<				
				į.	
	EAP-Response/				
	TUS(Contificate				
	ClientKevExcha	r, nge.			
	CertificateVer	ify,		i	
	ChangeCipherSp	ec,			
	Finished)				
		>			
	FAP-Request/				
	Type=TEAP,				
	TLS(ChangeCiphe	erSpec,			
	Finished),	TIN			
	{Crypto-Binding	g ILV,			
	<				
					į.
	EAP-Response/				
	Type=TEAP,	- TIV			
	Result TIV=Suco	s ILV, Sess}			
		>		i i	i i
	EAP-Request/				
	Request-Action	TLV:			
	Status=Failur	re,			
	Action=Proces	ss-TLV,			ļ
	TLV=PKCS#10}				
	<				
	1			1	1

TEAP -> ACME 3 of 3

• Peer enrols for certificate

++ Pledge	++ TEAP-Server	++ ACME	++ DNS
++	++	++	++
STEP 3:	Enroll for certificat	te	1
EAP-Response/ Type=TEAP, {PKCS#10 TLV: "pledgeid.doma:	in.com"}		
	POST /newOrd "pledgeid.do	der omain.com" >	
	201 status=r	ready	
	POST /final: PKCS#10 CSR pledgeid.do	ize omain.com" >	
	200 OK statu <	us=valid	
	POST /certit	ficate	
	 200 OK PEM "pledgeid.do	omain.com" 	
 EAP-Request/ Type=TEAP, {PKCS#7 TLV, Result TLV=Suc <	ccess}		
EAP-Response/ Type=TEAP, {Result TLV=Suc	:cess}		
 EAP-Success <			

Discussion

- Is this of broader interest?
- Do we need a backoff/retry mechanism in response to the Peer's PKCS#10 TLV?
- Are there channel binding issues not covered by <u>https://tools.ietf.org/html/rfc7170#section-3.8.2</u> "Certificate Provisioning within the Tunnel" ?
- Related drafts
 - draft-yusef-acme-3rd-party-device-attestation
 - draft-moriarty-acme-client