draft-friel-acme-subdomains-02

Friel, Barnes	Cisco
Hollebeek	DigiCert
Richardson	Sandelman Software Works

Sub-domain certificates

- ACME (RFC 8555) allows an ACME server to issue certificates for a given identifier (e.g. a subdomain) without requiring a challenge to be explicitly fulfilled against that identifier
- An ACME server could issue a certificate for **sub.domain.com** where the ACME client has only fulfilled a challenge for **domain.com**
- An ACME server could issue certificates for a number of sub-domain certificates and only require a single challenge to be fulfilled against the parent domain

Sub-domains with pre-authorization

+	+ ient +	+ ACN +	+ ИЕ +	++ DNS ++
STE	 2 1: Pre-Authoriza 	tion d	 of paren 	t domain
	POST /newAuthz "domain.com"	>		
	201 authorization <	ns 		
	Publish DNS TXT "domain.com"			>
	 POST /challenge 	>	 Verify	
	 200 status=valid <			>
	 Delete DNS TXT "domain.com" 		 	>

C1	ient	++ ACME	++ DNS
+		++ !	++
STE	P 2: Place order f 	or subdomain	1
	POST /newOrder "sub.domain.com" 	>	
	201 status=ready <		
	POST /finalize CSR "sub.domain.	com"	
	 200 OK status=va <	lid 	
	POST /certificat		
	200 OK PKI "sub.domain. <	com"	

Updates since IETF106 / draft-01

- 1. Defines "basedomain" boolean field in authorization object to explicitly differentiate between parent or base domain authorizations and wildcard authorizations
- 2. Clarify that base domain authorizations may optionally be used with the pre-authorization workflow, but pre-authorization is not mandatory
- 3. Updated appendix to clarify that depending on the deployment use case, ACME server policy may conform to CA/Browser Forum Baselines, but subdomain certificates may be used in multiple other scenarios where CAB compliance is not required

Next steps

- Missing security considerations
- Adoption?