# http(s)://trust-provider.com/products/!DecodeCSR

### **Version History**

1.00	Original ve	ersion.
1.01	Added:	"showFieldNames" and "showErrorCodes" parameters.
	Added:	Further documentation of the showXXXXX parameters (section 2).
	Changed:	"showErrorMessages=N" will now only hide the error messages; "showErrorCodes=N" should be used to hide the error codes.
	Changed:	"product" was incorrectly called "productID" in this document.
1.02	Added:	"countryNameType" parameter.
1.03	Added:	Note about decodeCSR.html utility.
1.04	Added:	"showKeySize" parameter.
	Changed:	Maximum Key Size is now 8192-bits.
1.05	Added:	Unicode support (UTF8String, non-ASCII BMPString, "responseFormat=0").
	Added:	Enterprise SSL, SGC and Legacy products.
1.06	Added:	"showSANDNSNames" parameter.
	Added:	Error code –40.
	Added:	Some more "product" values.
1.07	Added:	"showCSRHashes" parameter.
	Added:	Error code –1.
	Added:	SHA-1 and MD5 CSR Hash response lines.
	Changed:	CSR requirements (minimum key size, signature algorithm).
	Added:	"SECTIGO SSL" DV product range.
1.08	Added:	"showSignatureAlgorithm" parameter.
	Added:	"SECTIGO AMT SSL" product range.
	Changed:	CSRs may now contain ECC public keys and be signed using ECDSA.
1.09	Added:	"showCSRHashes2" parameter.

Note:  $\frac{https://secure.sectigo.com/utilities/decodeCSR.html}{https://secure.sectigo.com/utilities/decodeCSR.html} is a demonstration of DecodeCSR. It should work with any browser that supports XMLHTTP (Microsoft Internet Explorer 5+, Mozilla, etc).$ 

#### 1. Request

Required variables are in **bold**. Optional variables are in *italics*.

Variable Name (case insensitive)	Type	Max. Length		Allowe	ed Values		Description
csr	string	<b>32767</b> chars	present, sh	s may be in any order (altho		sses, if	Certificate Signing Request (Base-64 encoded, with or without theBEGIN xxxxx
			OID	<u>Description</u>	Supported ASN.1 Type(s)	Max. Length	and
			2.5.4.3	Common Name (MUST contain the Fully-Qualified Domain Name)	DirectoryString	64 chars	END xxxxx header and footer)
				ude these fields:		T	
			OID 2.5.4.10	Description Organization Name	Supported ASN.1 Type(s) DirectoryString	Max. Length 64 chars	
			2.5.4.11	Organizational Unit Name	DirectoryString	64 chars	
			2.5.4.18	Post Office Box	DirectoryString	40 chars	
			2.5.4.9	Street Address 1	DirectoryString	128 chars	
			2.5.4.9	Street Address 2	DirectoryString	128 chars	
			2.5.4.9	Street Address 3	DirectoryString	128 chars	
			2.5.4.7	Locality Name State or Province Name	DirectoryString DirectoryString	128 chars	
			2.5.4.17	Postal Code	DirectoryString	40 chars	
			2.5.4.6	Country Name (ISO-3166 2-char code)	PrintableString	2 chars	
			Subject Pi RSA: OIE ECC: OIE Attributes Any attri Signature md5Witt or sha12 or sha25 or sha25 or sha38 or sha51 or ecdsa- or ecdsa- or ecdsa- or ecdsa-	r fields MAY be present, bu ublic Key Info: D = rsaEncryption (PKCS# D = id-ecPublicKey (RFC32: butes MAY be present, but v Algorithm: hRSAEncryption (PKCS# VithRSAEncryption (PKCS 4WithRSAEncryption (PKCS 4WithRSAEncryption (PK 6WithRSAEncryption (PK 2WithRSAEncryption (PK withRSAEncryption (PK withRSAEncr	1); Size = <b>2048</b> to <b>8192</b> bi 279); Curve = <b>P-256</b> , <b>P-38</b> will be ignored. 1) S#1) CC\$#1) CC\$#1)		
responseFormat	integer		0 = UTF-8 1 = XML	3 text			If omitted, the default value is <b>0</b> .
showErrorCodes	char	1 char	Y or N.				If omitted, the default value is <b>Y</b> .
showErrorMessages	char	1 char	Y or N.				If omitted, the default value is <b>Y</b> .

showFieldNames	char	1 char	Y or N.	If omitted, the default
showEmptyFields	char	1 char	Y or N.	value is <b>Y</b> .  If omitted, the default
showCN	char	1 char	Y or N.	value is <b>Y</b> .  If omitted, the default
showAddress	char	1 char	Y or N.	value is Y.  If omitted, the default
showPublicKey	char	1 char	Y or N.	value is <b>Y</b> .  If omitted, the default value is <b>N</b> .
showKeySize	char	1 char	Y or N.	If omitted, the default value is N.
showSANDNSNames	char	1 char	Y or N. Only relevant for the Multi-Domain SSL and Unified Communications Certificate products.	If omitted, the default value is N.
showCSR	char	1 char	Y or N.	If omitted, the default value is <b>N</b> .
showCSRHashes	char	1 char	Y or N.	If omitted, the default value is N.
showCSRHashes2	char	1 char	Y or N.	If omitted, the default value is <b>N</b> .
showSignatureAlgorithm	char	1 char	Y or N.	If omitted, the default value is <b>N</b> .
product	integer		DV SSL Certificates: 488 = SectigoSSL DV 489 = SectigoSSL Wildcard DV 492 = SectigoSSL SSL Unified Communications Certificate DV  EV SSL Certificates: 337 = SectigoSSL EV Certificate 338 = EV SGC SSL Certificate 410 = SectigoSSL EV Multi-Domain EV Certificate  OV SSL Certificates: 43 = Trial SSL Certificate 44 = Intranet SSL Certificate 24 = InstantSSL Certificate 34 = InstantSSL Certificate 34 = InstantSSL Pro Certificate 35 = PremiumSSL Certificate 36 = PremiumSSL Wildcard Certificate 316 = PremiumSSL Legacy Certificate 317 = SGC SSL Certificate 322 = PremiumSSL Legacy Wildcard Certificate 323 = SGC SSL Wildcard Certificate 62 = EliteSSL Certificate 63 = GoldSSL Certificate 64 = PlatinumSSL Legacy Certificate 65 = PlatinumSSL Legacy Certificate 319 = PlatinumSSL Legacy Wildcard Certificate 319 = PlatinumSSL SGC Certificate 325 = PlatinumSSL SGC Certificate 335 = Multi-Domain SSL Certificate 336 = Unified Communications Certificate  AMT SSL Certificates: 510 = AMT SSL Wildcard Certificate 511 = AMT SSL Wildcard Certificate 512 = AMT SSL Wildcard Certificate	Product for which this CSR will be used. If omitted, product-specific checks are not performed.
countryNameType	string	7 chars	TWOCHAR or FULL.	If omitted, the default value is <b>TWOCHAR</b> .

The Request may be submitted via HTTP GET or POST. We recommend the use of POST wherever possible.

# 2. Response

Line	Possible Value(s)			
Mime-Type	text/plain			
Number Of Error Codes/Messages	0, 1, 2, etc			
Error Code & Error Message 1	See section 3			
Error Code & Error Message n				
Common Name	CN=xxxxx			
Organizational Unit Name	OU=xxxxx			
Organization Name	O=xxxxx			
Post Office Box	POB <sub>0</sub> x=xxxxx			
Street Address 1	STREET=xxxxx			
Street Address 2	STREET=xxxxx			
Street Address 3	STREET=xxxxx			
Locality Name	L=xxxxx			
State or Province Name	S=xxxx			
Postal Code	PostalCode=xxxxx			
Country Name	C=xxxxx			
Email Address	Email=xxxxx			
Telephone Number	Phone=xxxxx			
Public Key	Public Key=xxxxx			
Key Size (in bits)	Key Size=xxxxx			
Subject Alternative Name dnsName(s)	dnsName(s)=xxxxx,yyyy,zzzzz,etc,etc			
MD5 Hash of DER-encoded CSR	md5=xxxxx			
SHA-1 Hash of DER-encoded CSR	sha1=xxxxx			
SHA-256 Hash of DER-encoded CSR	sha256=xxxxx			
CSR Signature Algorithm	sigalg=xxxxx			
<blank line=""></blank>				
CSR (multiple lines)	The "csr" request variable, except: - any characters before the "BEGIN " header (if present) are removed leading/trailing spaces are removed.			

If showErrorCodes is N and showErrorMessages is N, the "Number of Error Codes/Messages" line is completely omitted from the response.

If showErrorCodes is N, the "Error Code" portions of the "Error Code & Error Message x" lines are completely omitted from the response.

If showErrorMessages is N, the "Error Message" portions of the "Error Code & Error Message x" lines are completely omitted from the response.

If showFieldNames is N, the lines from "Common Name" to "Public Key" only contain "xxxxx" (see Possible Values in the above table). In other words, "CN=", "OU=", "O=", etc, are omitted.

If showEmptyFields is N, then any lines from "Common Name" to "Telephone Number" where "xxxxx" (see Possible Values in the above table) is empty are completely omitted.

If showFieldNames is N and showEmptyFields is N, it will be very difficult to determine which line in the response relates to which of the attributes from "Common Name" to "Public Key".

If showCN is N, the "Common Name" line is completely omitted.

If showAddress is N, the lines from "Organizational Unit Name" to "Telephone Number" are completely omitted.

If showPublicKey is N (the default), the "Public Key" line is completely omitted.

If showKeySize is N (the default), the "Key Size" line is completely omitted.

If showSANDNSNames is N (the default), the "Subject Alternative Name dnsName(s)" line is completely omitted.

If showCSRHashes and showCSRHashes2 are both N (the default), the "md5" and "sha1" lines are completely omitted.

If showCSRHashes2 is N (the default), the "sha256" line is completely omitted.

If showSignatureAlgorithm is N (the default), the "sigalg" line is completely omitted.

If showCSR is N (the default), the <Blank Line> and "CSR" line(s) are completely omitted.

If countryNameType is TWOCHAR (the default), "xxxxx" in the "C=xxxxx" line will use the ISO-3166 two character country code (e.g. US, GB, ES, etc).

If countryNameType is FULL, "xxxxx" in the "C=xxxxx" line will use the ISO-3166 full country name (e.g. United States, United Kingdom, Spain, etc).

#### 3. Error Codes & Messages

Each "Error Code & Error Message" line is of the format <*Error Code*><*SPACE*><*Error Message*> (depending on the values of *showErrorCodes* and *showErrorMessages*). Below are the possible "Error Code & Error Message" lines:

-1 Request was not made over https and "showCSRHashes=Y" was specified!					
-2 "xxxxx" is an unrecognised argument!					
-3 The "xxxxx" argument is missing!					
-4 The value of the "xxxxx" argument is invalid!					
-5 The Common Name (Domain Name) may not contain a *					
-6 The Common Name (Domain Name) must contain ONE *					
-7 "xx" is not a valid ISO-3166 country code!					
-8 The CSR is missing a required field!					
-10 The CSR cannot be decoded!					
-11 The CSR uses an unsupported algorithm!					
-12 The CSR has an invalid signature!					
-13 The CSR uses an unsupported key size!					
-14 An unknown error occurred!					
-18 The Common Name (Server Name) may not be a Fully-Qualified Domain Name!					
-19 The Common Name (Server Name) may not be an Internet-accessible IP Address!					
-23 The Common Name (Domain Name) should not include the http:// part!					
-24 The Common Name (Domain Name) should not include the https:// part!					
-25 The Common Name (Domain Name) may only contain the following characters: AZ az 09					
-40 The CSR uses a key that is believed to have been compromised!					
-41 The CSR uses an invalid key!					