Legacy CMC API on SwissSign's new CA platform

Known differences and issues on the new Certificate Authority platform

Type	Topic	Description
Difference	**Trust Chain**	The new platform has a new trust chain (Intermediate CAs). Customers who use certificate pinning need to trust the new chain. It can be downloaded here https://www.swisssign.com/support/ca-prod.html
Difference	**CSR Format**	The new CA platform only accepts binary DER as CSR format, while the legacy CA platform accepts the PEM encoding as well.
Difference	**CSR Signature Algorithm**	The new CA platform accepts CSR with SHA224 and higher, while the legacy CA platform also accepts weaker ones like MD4, MD5 and SHA1.
Difference	**SDN of Email Silver**	The new CA platform requests CN attribute for SDN of S/MIME E-Mail ID Silver certificates, while the legacy CA platform requests Email attribute for SDN.

CMC API on different environments

The CMC API of the SwissSign legacy CA was implemented on SwissSign's new CA platform as well.

CA	Legacy CA		New CA	
Environment	STAGING	PROD	PRE-PROD	PROD
CMC URL	https://ra.swiss.signdemo.com/ws/cmc	https://ra.swisssign.net/ws/cmc	https://cmc.pre.swisssign.ch/ws/cmc	https://cmc.swisssign.ch/ws/cmc

To be able to access the CMC API your client certificate's serial numbers (40 digits HEX) to your MPKI needs to be authorized on the corresponding environment.

CMC API Use

- The API specification can be found here New CA: Technical Specification of CMC API

- Please do not forget to URL encode the parameters in the query string.

- Example call for PRE-PROD environment: https://cmc.pre.swisssign.ch/ws/cmc?**account=**MPKI50001016%20-%20Firma%20Muster%20AG&**product=**SwissSign%20EV%20SSL%20Gold%20Single-Domain&**ignore_unconsumed**=1

CA	Legacy CA		New CA	
Environment	STAGING	PROD	PRE-PROD	PROD
CMC URL	https://ra.swiss.**signdemo.com**/ws/cmc	https://ra.**swisssign.net**/ws/cmc	https://cmc.**pre**.swisssign.ch/ws/cmc	https://**cmc.swisssign.ch**/ws/cmc
account=	Staging account name i.e. accountname.ra	Prod account name i.e. accountname.ra	• assigned from sales office i.e. "MPKI5000005%20-%20Firma%20Muster%20AG"	• Migration customers: set to the same string as used on legacy CA i.e. "company.ra" • New customers: use the account name sent by e-mail i.e. "MPKI5000005%20-%20Firma%20Muster%20AG"
product=	Staging product name i.e. accountname-productname	Prod product name i.e. accountname-productname	• Pre-Prod product name as URL encoded name on the next table • same product name as you use on the legacy CA, i.e. accountname-productname	• Prod product name as URL encoded name on the next table • same product name as you use on the legacy CA, i.e. accountname-productname

CMC product names

Product	You can use these strings * being any account name string	Or the new URL encoded product names
SwissSign EV SSL Gold Single-Domain	*-ev-gold	SwissSign%20EV%20SSL%20Gold%20Single-Domain
SwissSign EV SSL Gold Multi-Domain	*-ev-gold-multi	SwissSign%20EV%20SSL%20Gold%20Multi-Domain
SwissSign OV SSL Gold Wildcard	*-gold-wild	SwissSign%20OV%20SSL%20Gold%20Wildcard
SwissSign OV SSL Gold Single-Domain	*-ssl-gold	SwissSign%20OV%20SSL%20Gold%20Single-Domain
SwissSign OV SSL Gold Multi-Domain	*-ssl-gold-multi	SwissSign%20OV%20SSL%20Gold%20Multi-Domain
SwissSign DV SSL Silver Single-Domain	*-ssl-silver	SwissSign%20DV%20SSL%20Silver%20Single-Domain
SwissSign DV SSL Silver Multi-Domain	no ssl-silver-multi product in legacy CA	SwissSign%20DV%20SSL%20Silver%20Multi-Domain
SwissSign DV SSL Silver Wildcard	*-silver-wild	SwissSign%20DV%20SSL%20Silver%20Wildcard
SwissSign Pro S/MIME E-Mail ID Gold	*-perso-org-gold	SwissSign%20Pro%20S%2FMIME%20E-Mail%20ID%20Gold
SwissSign Pro S/MIME E-Mail ID Gold with Auth.	*-perso-org-gold-auth	SwissSign%20Pro%20S%2FMIME%20E-Mail%20ID%20Gold%20with%20Auth
SwissSign Pro S/MIME E-Mail ID Gold RSASSA-PSS	*-perso-org-gold-rsassapss	SwissSign%20Pro%20S%2FMIME%20E-Mail%20ID%20Gold%20RSASSA-PSS
SwissSign Personal S/MIME E-Mail ID Silver	*-perso-silver-emailonly	SwissSign%20Personal%20S%2FMIME%20E-Mail%20ID%20Silver