PRE-PROD Manual

Contents

Procedure to onboard the PRE-PROD environment

The PRE-PROD environment is used by partners and customers to test API and UI functionallity of SwissSign's new CA.

The environment is used in the context of...

- Testing the new CA before migrating from the old one
- Testing a new release of the new CA before its deployment to PROD
- Testing the integration of the MPKI (via ACME, RestAPI or CMC) into the environment of a new customer

Please provide the following to get an own PRE-PROD MPKI

- General email address for general notifications (i.e. info@company.ch)
- List of email addresses of operators
- For legacy CA and other customers using the CMC interface: serial numbers (40 digits HEX) of AutoRAO client certificate which shall be authorized to access the CMC API on the new CA.

Please note that every MPKI operator (registration authority operators) will need to onboard a SwissID digital identity to access the registration authority user interface (RA UI).

Differences between PRE-PROD and PROD

Feature on environment	PRE-PROD SwissSign CA	PROD SwissSign CA
Trusted in root stores of Google, Apple, Microsoft etc.	**NO**	**YES** Our new productive CA uses new Issuing CAs. Make sure to import the new trust chains in case you do certificate pinning. You can download the trust chains from here https://www.swisssign.com/support/ca-prod.html
Certificate attributes	Same dummy attributes for everybody Firma Muster AG Mustergasse 12 8000 Zürich Switzerland Commerce register CH-123.456.789	Your own from the order
Certificate attribute validation	Non validated dummy attributes	Yes, depending on the choosen MPKI type
Allowed algorithms for signing Certificate Signing Requests (CSRs)	As PROD (see right column)	Allowed are • sha-2 and • sha-3 hash-algorithms combined with RSA. These signatures might be PKCS1-v1_5 or PSS based. For details see below.

Signature Algorithm	The signature algorithm used when issuing the certificate			
	sha224	sha224/PSS/MfG1	sha3-224	sha3-224/PSS/MfG1
	sha256	sha256/PSS/MfG1	sha3-256	sha3-256/PSS/MfG1
	sha384	sha2384/PSS/MfG1	sha3-384	sha3-384/PSS/MfG1
	sha512	sha2512/PSS/MfG1	sha3-512	sha3-512/PSS/MfG1

Feature on environment	PRE-PROD SwissSign CA	PROD SwissSign CA
CSR extension	As PROD (see right column)	Only PEM (no cer, crt, p7b, p7c)
Operator access	List of email addresses of the operators must be specified when PRE-PROD MPKI is ordered	List of email addresses of the operators must be specified when MPKI is ordered
Costs	free of charge	apply
MPKI settings	• Type = EV (which includes OV and DV) • General email address = as specified during order • Notifications setting = set to client rao & certificate owner • Auto-enrollment = on • Publication in S/MIME LDAP = on	As specified in order
Possible change requests via sales@swisssign.com	• ~~Upgrade~~ • ~~Downgrade to OV or DV~~ • Change notification setting • Change auto-enrollment setting • Change publication setting	• Upgrade • Downgrade • Change notification setting • Change auto-enrollment seeting • Change publication setting
Certificate products	Every MPKI product is available.	Every MPKI product of the choosen MPKI type (DV/OV/EV)
CRL	TLS DV 2022 -1: http://crl.pre.swisssign.ch/cdp-53f70c9a-5d06-47e3-abbc-b647e17872f7 TLS OV 2022 -1: http://crl.pre.swisssign.ch/cdp-0fb9a4a8-da4d-4266-816c-0b46345e188b	TLS DV 2022 -1: http://crl.swisssign.ch/cdp-679723b2-8641-4642-8500-f6d2ff37e6ba TLS OV 2022 -1: http://crl.swisssign.ch/cdp-96b62f5a-6b73-4da4-87f7-ce4002c1cd34

Feature on environment	PRE-PROD SwissSign CA	PROD SwissSign CA
	TLS EV 2022 -1: http://crl.pre.swisssign.ch/cdp-a9921ee3-3299-482b-9d98-0b4473913837 S/MIME LCP 2022 - 1: http://crl.pre.swisssign.ch/cdp-6d345011-0540-4e39-b486-e8f2b2cc2e73 S/MIME NCP 2022 - 1: http://crl.pre.swisssign.ch/cdp-80ab789b-5958-4583-9cce-f2afceec8dae S/MIME NCP extended 2022 - 1: http://crl.pre.swisssign.ch/cdp-77a2a9e3-39a3-42ea-b0cb-b06ecb93d357	TLS EV 2022 -1: http://crl.swisssign.ch/cdp-9fdd910e-b9ff-4b2f-be38-2e93708c1b36 S/MIME LCP 2021 - 1: http://crl.swisssign.ch/cdp-d5057ba0-ce09-4d1d-8cc9-a60fa4c49c0 S/MIME NCP 2021 - 1: http://crl.swisssign.ch/cdp-5639ce88-5da9-408f-b25d-685d1e3e020a S/MIME NCP extended 2021 - 1: http://crl.swisssign.ch/cdp-26ab0cd6-f539-4f93-be04-39250cd56682
OCSP	http://ocsp.pre.swisssign.ch/sign/ocs-192cba97-3391-4237-8fad-b3973d0170ce	http://ocsp.swisssign.ch/sign/ocs-aaccced5-66e8-4069-9b1b-fd29ab73efec
AIA	TLS DV 2022 -1: http://aia.pre.swisssign.ch/air-fb17306a-7317-46ba-9593-4df04980894d TLS OV 2022 -1: http://aia.pre.swisssign.ch/air-7ec57c41-4c1a-4887-b351-9b5139a193b5 TLS EV 2022 -1: http://aia.pre.swisssign.ch/air-58900678-c0dd-4e1a-8d45-f050d9cf4c27 S/MIME LCP 2022 – 1:	TLS DV 2022 -1: http://aia.swisssign.ch/air-1b863385- f4a9-47fa-88a5-2a5abfd4a167 TLS OV 2022 -1: http://aia.swisssign.ch/air-0f2bf9a5-dd37- 48c9-a85b-12acdcb8be45 TLS EV 2022 -1: http://aia.swisssign.ch/air-20350159-813d- 4532-b988-8519eca57650 S/MIME LCP 2021 – 1:

Feature on environment	PRE-PROD SwissSign CA	PROD SwissSign CA
	http://aia.pre.swisssign.ch/air-4520af42-659c-4335-aecd-32b0fe203bf6 S/MIME NCP 2022 - 1: http://aia.pre.swisssign.ch/air-5df5f13c-0f97-4865-885b-e29eba202d2e S/MIME NCP extended 2022 - 1: http://aia.pre.swisssign.ch/air-09cbe36f-0480-42f5-b33a-8b8d8b7f032c	http://aia.swisssign.ch/air-79b46fac-4cd2- 4d42-9fe0-9cd078d13d8c S/MIME NCP 2021 - 1: http://aia.swisssign.ch/air-9c868187-6fca- 4313-aa5b-ce5fec83132f S/MIME NCP extended 2021 - 1: http://aia.swisssign.ch/air-d8cd150b-23a8- 4989-a18e-b683fdb5bb85
LDAP	ldaps://directory.pre.swisssign.ch	ldaps://directory.swisssign.ch
CT log integration	yes (Google Test Logs)	yes (multiple)
Validations	• domain validation • public suffix • embargo list • CAA check in DNS record	• domain validation • public suffix • embargo list • CAA check in DNS record
New CA interfaces	**PRE-PROD**	**PROD**
RA UI https://www.swisssign.com/en/support/mpki-setup/operator-documents.html	• https://ra.pre.swisssign.ch • Login with real SwissIDs (no test accounts)	• https://ra.swisssign.ch • Login with real SwissIDs (no test accounts)
RA API https://github.com/SwissSign-AG/RaApi contains • README.md describing the getting started	• Endpoint: https://api.ra.pre.swisssign.ch • API token can be retrieved from the RA UI	• Endpoint: https://api.ra.swisssign.ch • API token can be retrieved from the RA UI

Feature on environment	PRE-PROD SwissSign CA	PROD SwissSign CA
• api.json OpenAPI spec file for Swagger UI • Example scripts and clients		
ACME API ACME Schnittstelle Quick Start Guide (PDF)	• Endpoint: https://acme.pre.swisssign.ch/v1/ • Find registration-links in the ACME menu of the RA UI	• Endpoint: https://acme.swisssign.ch/v1/ • Find registration-links in the ACME menu of the RA UI
Legacy CMC API	• Endpoint: https://cmc.pre.swisssign.ch/ws/cmc • See doc "Legacy CMC API on SwissSigns new CA platform" for more information	• Endpoint: https://cmc.swisssign.ch/ws/cmc • See doc "Legacy CMC API on SwissSigns new CA platform" for more information

Additional help links

- MPKI support: https://www.swisssign.com/support/mpki-setup.html
- General support: https://www.swisssign.com/support/dokumentationen.html