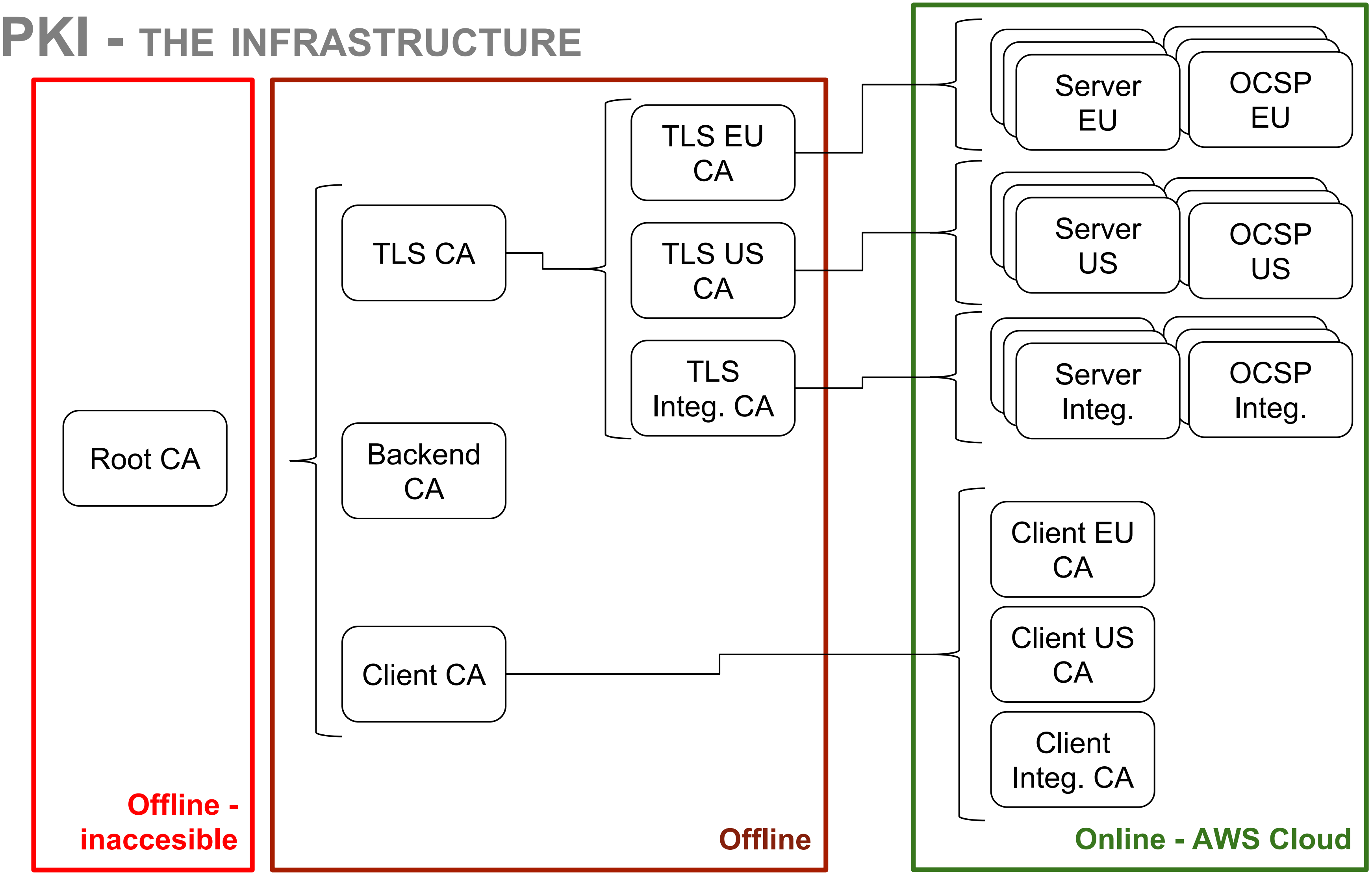
AMAN
digital.Media.Solutions

PKI Automation in the Cloud

Munich, May 2018

PKI - THE INFRASTRUCTURE



Challenges & Risks

Challenges:

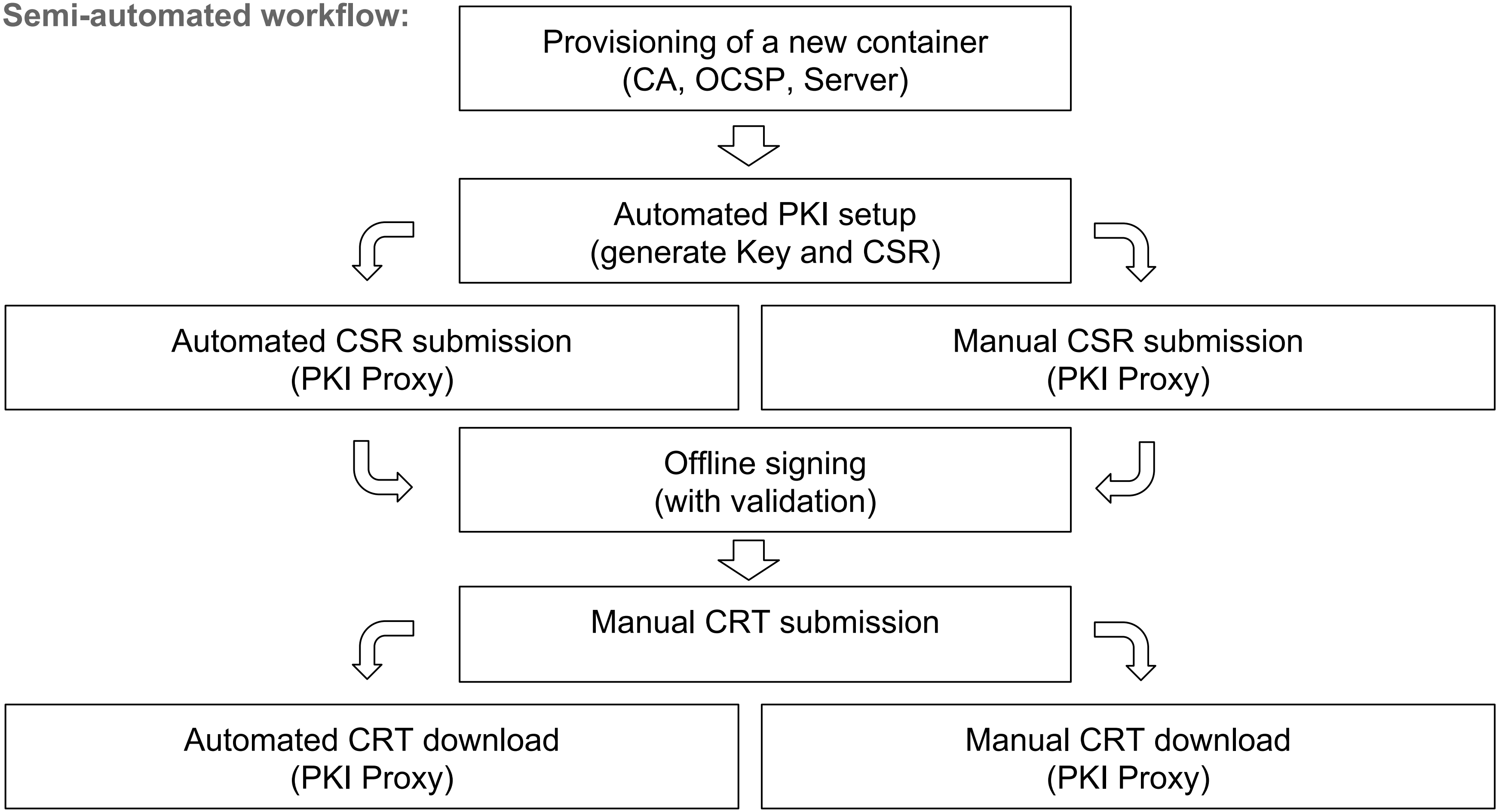
- Multiple environments
  - Multiple CAs
  - DN naming structure
  - Overview
- Multiple suppliers
- Scaling of instances
- CRL maintenance

Risks:

- Human factor
  - CSRs with wrong DNs
  - CSRs with identical keys
  - CRTs from wrong CA
  - CRTs from wrong CSR
- Response time
  - manual effort during scaling

Solution: Automation

Semi-automated workflow:



Provisioning of a new container
(CA, OCSP, Server)

Automated PKI setup
(generate Key and CSR)

Automated CSR submission
(PKI Proxy)

Manual CSR submission
(PKI Proxy)

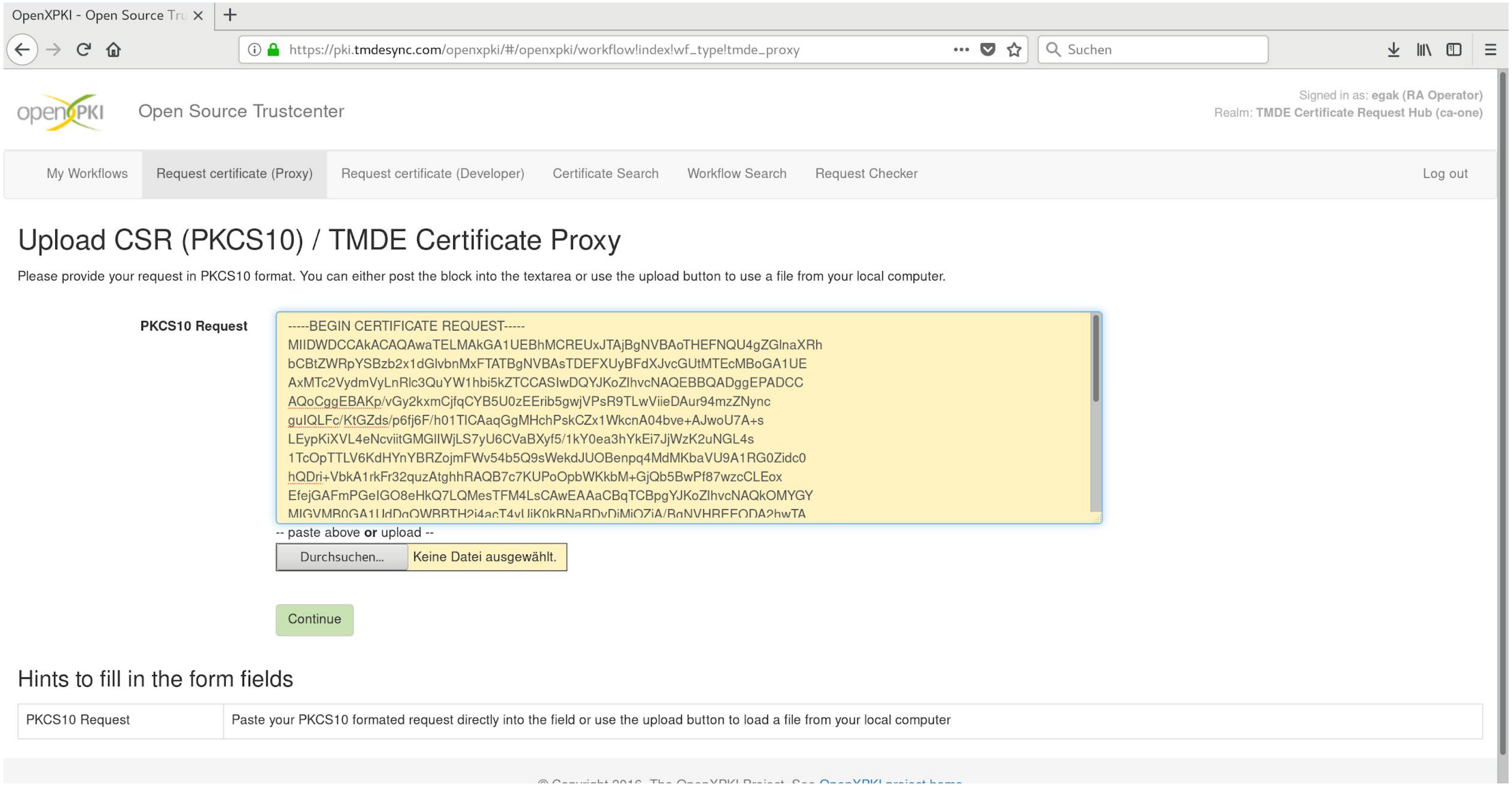
Offline signing
(with validation)

Manual CRT submission

Automated CRT download
(PKI Proxy)

Manual CRT download
(PKI Proxy)

Step-by-Step: Upload CSR



OpenXPKI - Open Source Tru
https://pki.tmdesync.com/openxpki/#/openxpki/workflow!index!wf_type!tmde_proxy
Suchen

Open Source Trustcenter

Signed in as: egak (RA Operator)
Realm: TMDE Certificate Request Hub (ca-one)

My Workflows
Request certificate (Proxy)
Request certificate (Developer)
Certificate Search
Workflow Search
Request Checker
Log out

Upload CSR (PKCS10) / TMDE Certificate Proxy

Please provide your request in PKCS10 format. You can either post the block into the textarea or use the upload button to use a file from your local computer.

PKCS10 Request

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDWDCCAkACAQAwaTELMAkGA1UEBhMCREUxJTAjBgNVBAoTHEFNQU4gZGlnaXRh
bCBtZWRpYSBzb2x1dGlvbnMxFTATBgNVBAsTDEFXUyBFdXJvcGUtMTEcMBoGA1UE
AxMTc2VydmVyLnRlc3QuYW1hbi5kZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAKp/vGy2kxmCjfqCYB5U0zEErib5gwjVPsR9TLwViieDAur94mzZNync
guIQLFc/KtGZds/p6fj6F/h01TICAaqGgMHchPskCZx1WkcnA04bve+AJwoU7A+s
LEypKiXVL4eNcviitGMGlIWjLS7yU6CVaBXyf5/1kY0ea3hYkEi7JjWzK2uNGL4s
1TcOpTTLV6KdHYnYBRZojmFWv54b5Q9sWekdJUOBenpq4MdMKbaVU9A1RG0Zidc0
hQDri+VbkA1rkFr32quzAtghhRAQB7c7KUPoOpbWKkbM+GjQb5BwPf87wzcCLEox
EfejGAFmPGeIGO8eHkQ7LQMesTFM4LsCAwEAAaCBqTCBpgYJKoZIhvcNAQkOMYGY
MIGVMB0GA1UdDgQWBBTH2i4acT4vUiK0kBNaBDvDiMiOZiA/BgNVHREEODA2hwTA
```

-- paste above **or** upload --

Durchsuchen... Keine Datei ausgewählt.

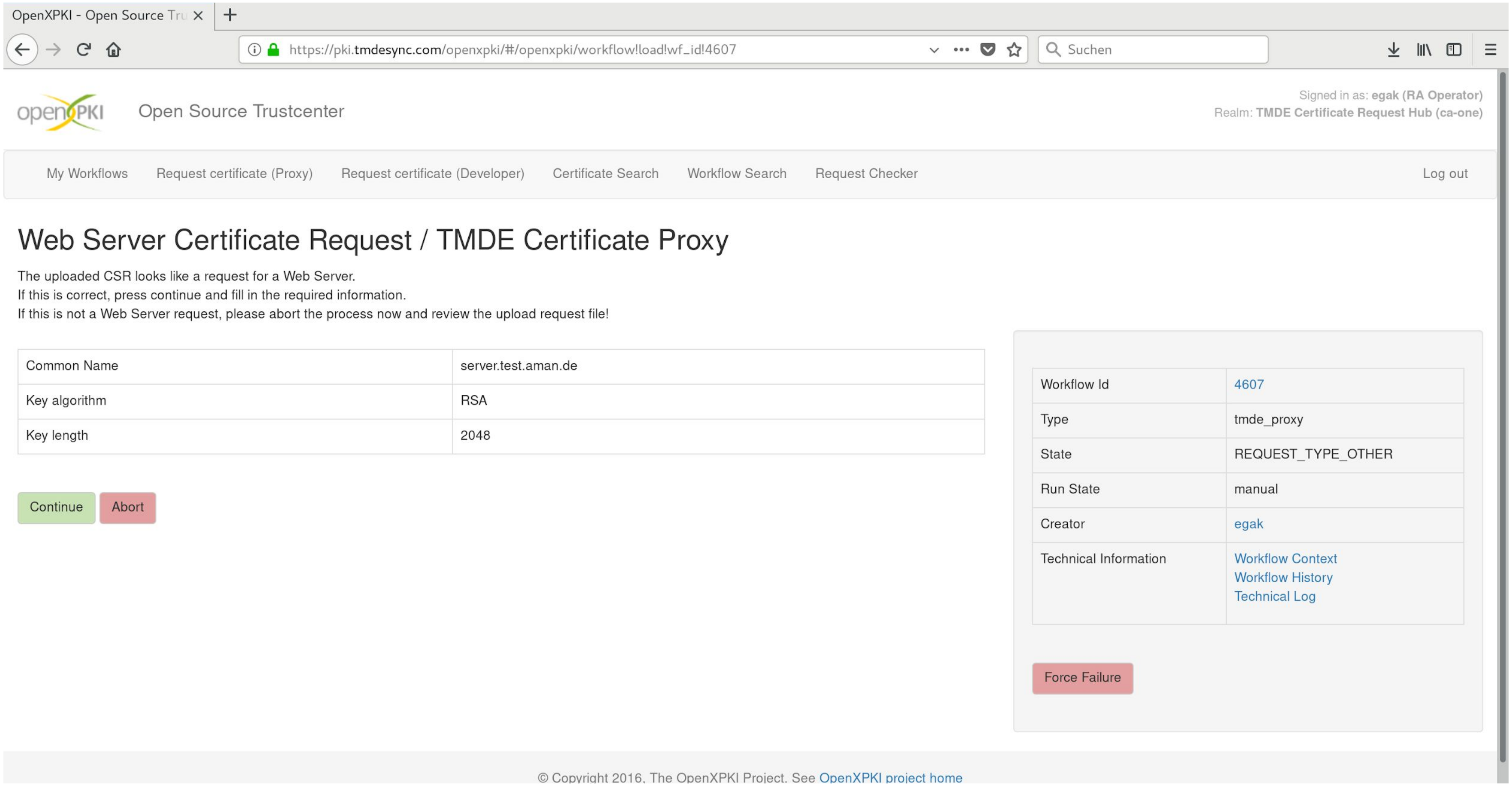
Continue

Hints to fill in the form fields

PKCS10 Request	Paste your PKCS10 formated request directly into the field or use the upload button to load a file from your local computer

© Copyright 2016, The OpenXPKI Project. See OpenXPKI project home

Step-by-Step: Uploaded CSR



OpenXPKI - Open Source Tru
https://pki.tmdesync.com/openxpki/#/openxpki/workflow!load!wf_id!4607
Suchen
openXPKI
Open Source Trustcenter
Signed in as: egak (RA Operator)
Realm: TMDE Certificate Request Hub (ca-one)
My Workflows
Request certificate (Proxy)
Request certificate (Developer)
Certificate Search
Workflow Search
Request Checker
Log out

Web Server Certificate Request / TMDE Certificate Proxy

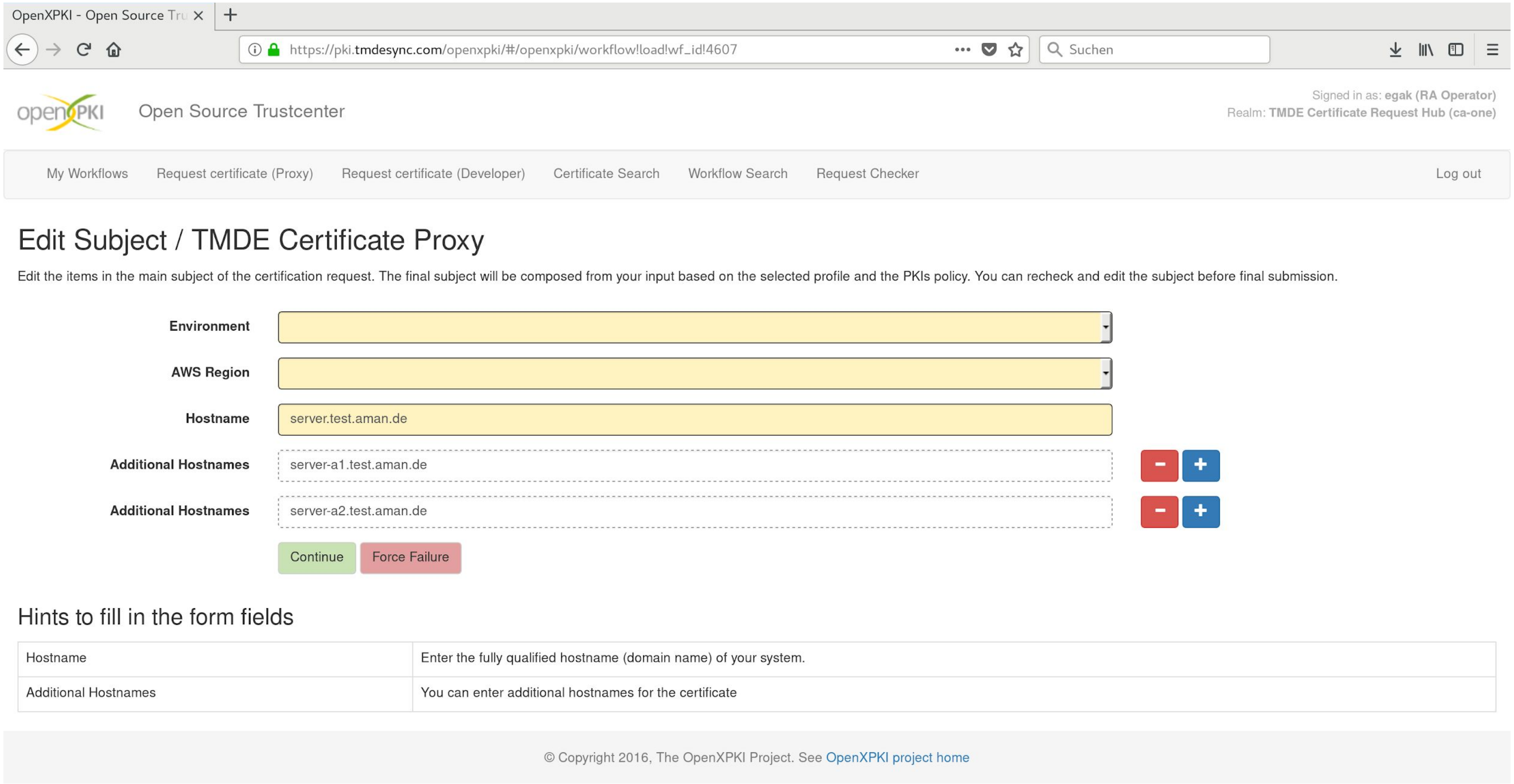
The uploaded CSR looks like a request for a Web Server.
If this is correct, press continue and fill in the required information.
If this is not a Web Server request, please abort the process now and review the upload request file!

Common Name	server.test.aman.de
Key algorithm	RSA
Key length	2048

Workflow Id	4607
Type	tmde_proxy
State	REQUEST_TYPE_OTHER
Run State	manual
Creator	egak
Technical Information	Workflow Context Workflow History Technical Log

© Copyright 2016, The OpenXPKI Project. See OpenXPKI project home

Step-by-Step: Add detail information



OpenXPKI - Open Source Tru
https://pki.tmdesync.com/openxpki/#/openxpki/workflow!load!wf_id!4607
Suchen
openXPKI
Open Source Trustcenter
Signed in as: egak (RA Operator)
Realm: TMDE Certificate Request Hub (ca-one)
My Workflows
Request certificate (Proxy)
Request certificate (Developer)
Certificate Search
Workflow Search
Request Checker
Log out

Edit Subject / TMDE Certificate Proxy

Edit the items in the main subject of the certification request. The final subject will be composed from your input based on the selected profile and the PKIs policy. You can recheck and edit the subject before final submission.

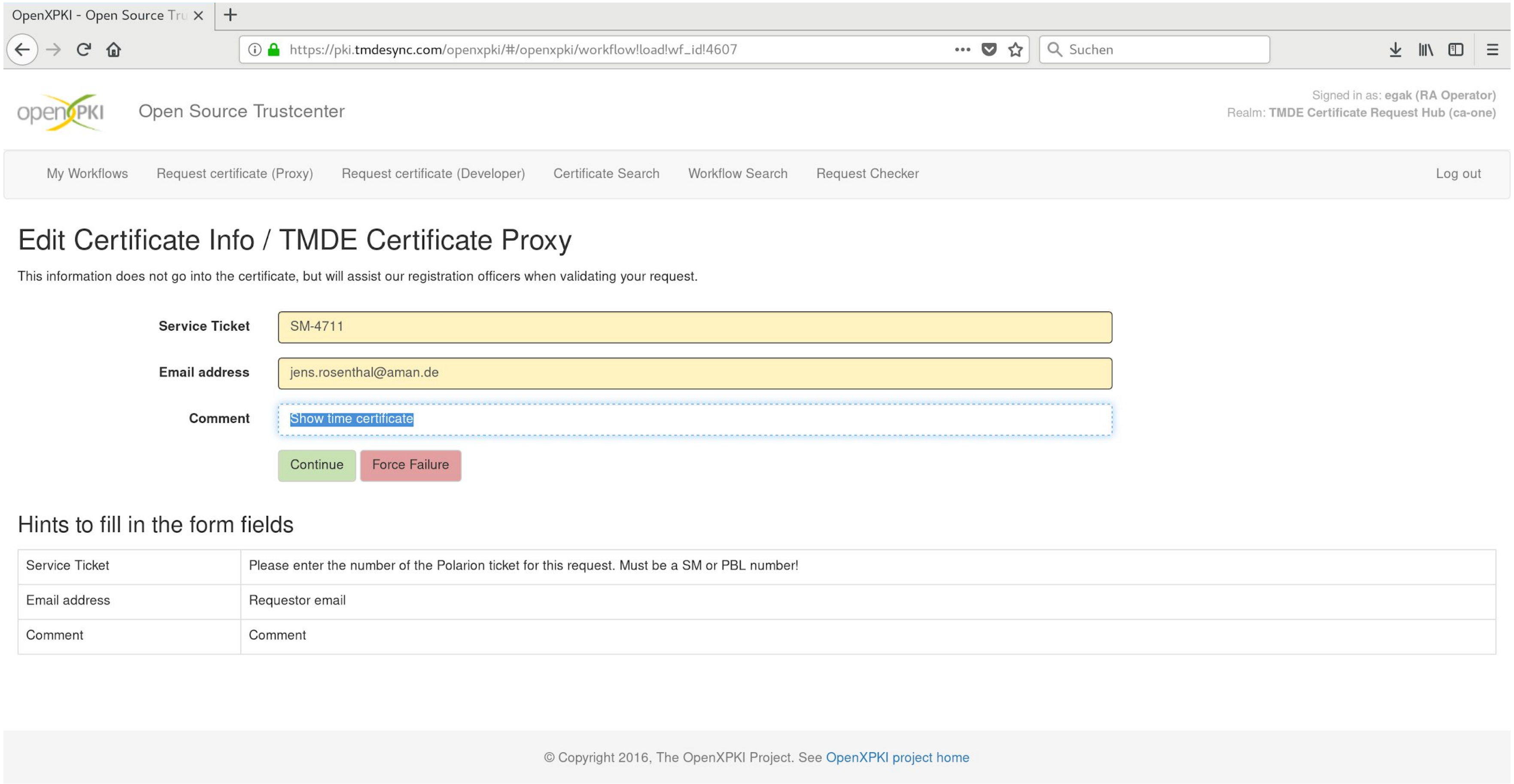
Environment	
AWS Region	
Hostname	server.test.aman.de
Additional Hostnames	server-a1.test.aman.de
Additional Hostnames	server-a2.test.aman.de

Hints to fill in the form fields

Hostname	Enter the fully qualified hostname (domain name) of your system.
Additional Hostnames	You can enter additional hostnames for the certificate

© Copyright 2016, The OpenXPKI Project. See OpenXPKI project home

Step-by-Step: Add validation information


OpenXPKI - Open Source Tru
https://pki.tmdesync.com/openxpki/#/openxpki/workflow!load!wf_id!4607
Suchen
openXPKI
Open Source Trustcenter
Signed in as: egak (RA Operator)
Realm: TMDE Certificate Request Hub (ca-one)
My Workflows
Request certificate (Proxy)
Request certificate (Developer)
Certificate Search
Workflow Search
Request Checker
Log out
Continue
Force Failure

Edit Certificate Info / TMDE Certificate Proxy

This information does not go into the certificate, but will assist our registration officers when validating your request.

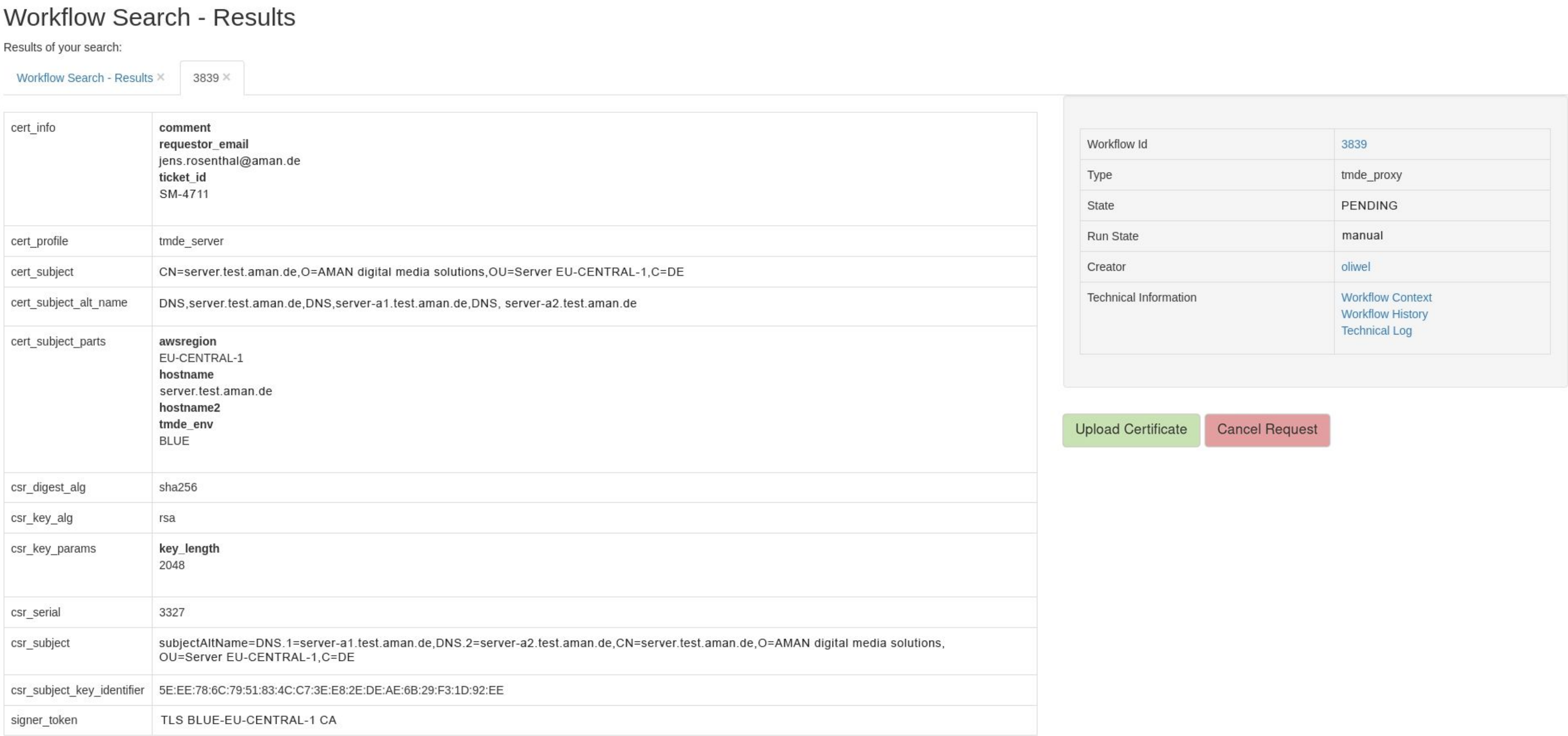
Service Ticket	SM-4711
Email address	jens.rosenthal@aman.de
Comment	Show time certificate

Hints to fill in the form fields

Service Ticket	Please enter the number of the Polarion ticket for this request. Must be a SM or PBL number!
Email address	Requestor email
Comment	Comment

© Copyright 2016, The OpenXPKI Project. See OpenXPKI project home

Step-by-Step: Validate and Sign CSR



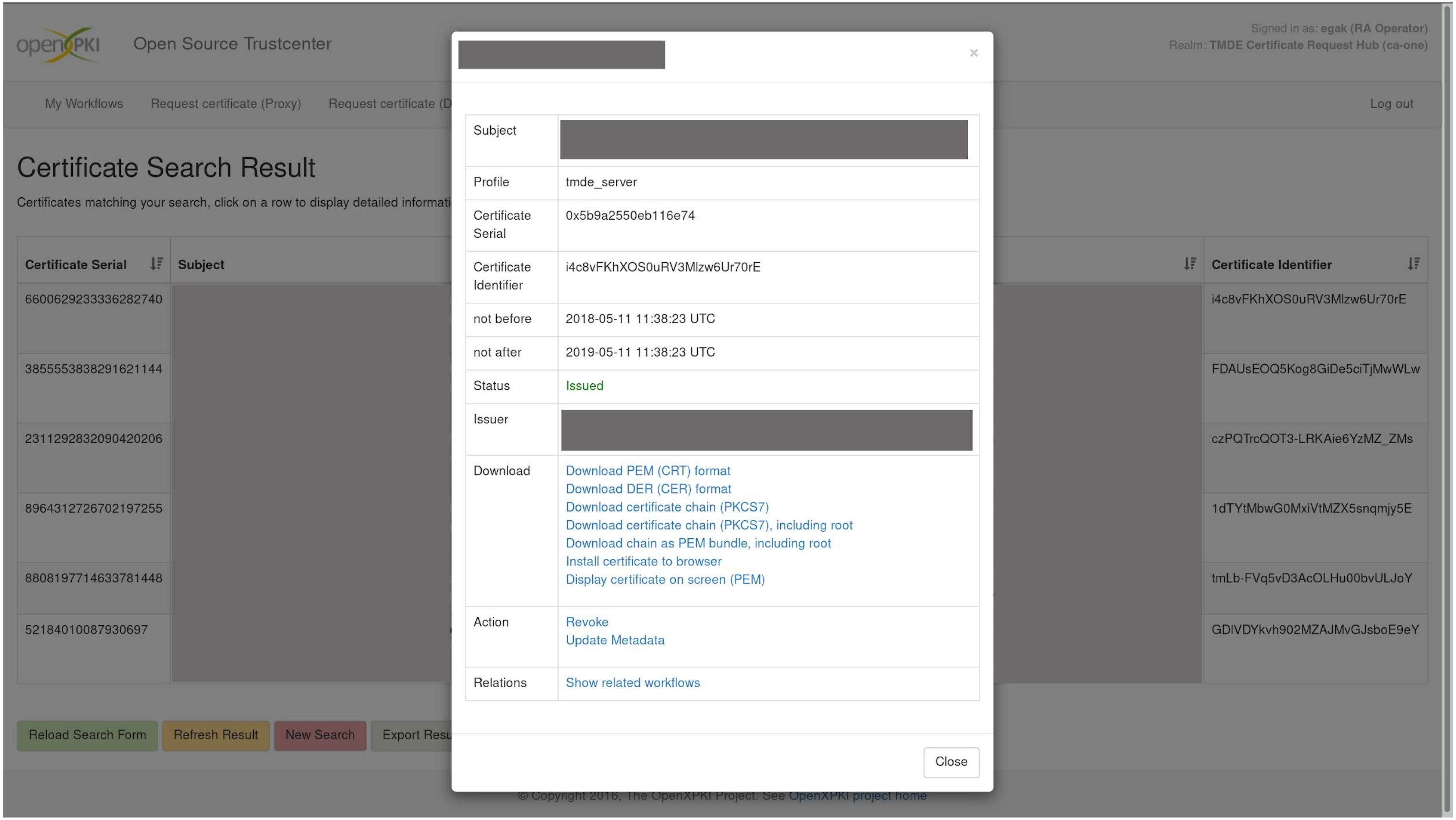
Workflow Search - Results

Results of your search:

cert_info	**comment** **requestor_email** jens.rosenthal@aman.de **ticket_id** SM-4711
cert_profile	tmde_server
cert_subject	CN=server.test.aman.de,O=AMAN digital media solutions,OU=Server EU-CENTRAL-1,C=DE
cert_subject_alt_name	DNS,server.test.aman.de,DNS,server-a1.test.aman.de,DNS, server-a2.test.aman.de
cert_subject_parts	**awsregion** EU-CENTRAL-1 **hostname** server.test.aman.de **hostname2** **tmde_env** BLUE
csr_digest_alg	sha256
csr_key_alg	rsa
csr_key_params	**key_length** 2048
csr_serial	3327
csr_subject	subjectAltName=DNS.1=server-a1.test.aman.de,DNS.2=server-a2.test.aman.de,CN=server.test.aman.de,O=AMAN digital media solutions, OU=Server EU-CENTRAL-1,C=DE
csr_subject_key_identifier	5E:EE:78:6C:79:51:83:4C:C7:3E:E8:2E:DE:AE:6B:29:F3:1D:92:EE
signer_token	TLS BLUE-EU-CENTRAL-1 CA

Workflow Id	3839
Type	tmde_proxy
State	PENDING
Run State	manual
Creator	oliwel
Technical Information	Workflow Context Workflow History Technical Log

Step-by-Step: Download signed CRT



openXPKI Open Source Trustcenter

Signed in as: **egak (RA Operator)**
Realm: **TMDE Certificate Request Hub (ca-one)**

Certificate Search Result

Certificates matching your search, click on a row to display detailed informati

Certificate Serial	Subject	Certificate Identifier
6600629233336282740	[redacted]	i4c8vFKhXOS0uRV3Mlzw6Ur70rE
3855553838291621144	[redacted]	FDAUsEOQ5Kog8GiDe5ciTjMwWLw
2311292832090420206	[redacted]	czPQTrcQOT3-LRKAie6YzMZ_ZMs
8964312726702197255	[redacted]	1dTYtMbwG0MxiVtMZX5snqmjy5E
8808197714633781448	[redacted]	tmLb-FVq5vD3AcOLHu00bvULJoY
52184010087930697	[redacted]	GDlVDYkvh902MZAJMvGJsboE9eY

[redacted]

Subject	[redacted]
Profile	tmde_server
Certificate Serial	0x5b9a2550eb116e74
Certificate Identifier	i4c8vFKhXOS0uRV3Mlzw6Ur70rE
not before	2018-05-11 11:38:23 UTC
not after	2019-05-11 11:38:23 UTC
Status	Issued
Issuer	[redacted]
Download	Download PEM (CRT) format Download DER (CER) format Download certificate chain (PKCS7) Download certificate chain (PKCS7), including root Download chain as PEM bundle, including root Install certificate to browser Display certificate on screen (PEM)
Action	Revoke Update Metadata
Relations	Show related workflows

© Copyright 2016, The OpenXPKI Project. See OpenXPKI project home

Solution: Automation

Benefits:

- Validation
  - of DNs in CSRs
  - of signed CRTs
- Assistance
  - automated assignment of signing CAs
  - automated assignment of certificate purpose
  - documentation
  - overview
- Self-Service
  - semi automated process
  - authentication / authorization
  - faster

QUESTIONS?

Time for questions

JENS ROSENTHAL
Software Architect
AMAN digital media solutions
www.aman.de / jens.rosenthal@aman.de