BEST PRACTICE PAPER

SICAM GridPass Registration Authority

SICAM GridPass is not only a combined Registration Authority and Certificate Authority but also a single Registration Authority which can be connected to an external Certificate Authority. This paper describes the possibilities, the technical background, and the configuration for this feature.

SIEMENS

Contents

PURPOSE

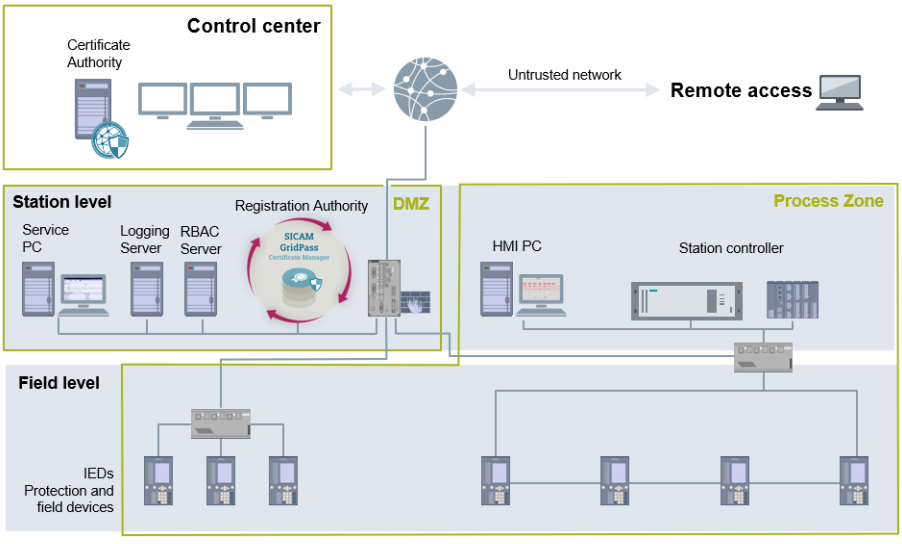
SICAM GridPass Registration Authority

In general, SICAM GridPass is an all-in-one Registration Authority (RA) and Certificate Authority (CA). But now you can use SICAM GridPass as a standalone Registration Authority to connect to an external Certificate Authority, like the workflow of requesting and receiving an identity card in your residents' registration office and the issuing of your identity card by an external authority (in Germany for example the “Bundesdruckerei”).

Topology of Registration Authority and Certificate Authority

In case a Certificate Authority (CA) is placed in your Control Center or office network backend you can use it now. Or in case you want not do deal with CA private keys you can use a CA service from external and can use the service now together with SICAM GridPass acting as Registration Authority (RA). A single SICAM GridPass RA or multiple SICAM GridPass RAs can be placed in your multiple substations and can receive Certificate Signing Requests (CSR) from any devices or systems in the substation and redirect it to the external CA. Or as an additional feature the SICAM GridPass RA applies directly a manual created CSR to the external CA.

Use SICAM GridPass as a Registration Authority and connect it to an inhouse Certificate Authority or external Certificate Authority service. Use a Certificate Authority service to avoid the protection and the backup of the Certificate Authority private key.



Trust relationship

Device and SICAM GridPass RA have a mutual trust relationship based on the TLS client- and server-certificates used for the EST connection. In case a new certificate on device side is necessary, the device generates a private/public key pair first and build a CSR which includes among other certificate things the public key and signs the CSR with the generated private key. This CSR is sent now over the EST connection to the SICAM GridPass RA. Only devices trusted by the SICAM GridPass RA can send a CSR to the SICAM GridPass RA.

In any cases the received CSR from the devices will be checked first by the SICAM GridPass RA comprising the proof-of-possession of the private key and the content of the CSR. The CSR will be adjusted by the SICAM GridPass RA if needed. This, from SICAM GridPass RA checked, adjusted and new from SICAM GridPass RA digital signed CSR will be forwarded to the external CA over the CMP enrollment protocol. In case the SICAM GridPass RA has a certificate based mutual trust relationship to the external CMP server the external CMP server will now forward the CSR to the external CA and the external CA will issue an external CA digital signed certificate with the CSR information plus additional information (e.g., the validity) and send it back over CMP to the SICAM GridPass RA.

Now the SICAM GridPass RA send the issued certificate back over the mutual authenticated EST connection to the device which has requested the certificate or offers a download over the Web-Browser to the authenticated SICAM GridPass RA user.

The CMP protocol can be used together with a TCP based connection based on http or https or can be used offline. In general https with mutual authentication is used. In case sending the CSR to the CMP server over https also here the certificate based mutual trust is in place for the https connection between SICAM GridPass RA and the CMP server.

The external CA which has issued the operational device certificates has to be trusted in the whole system using and trust these device certificates.

CMP can handle many trust relationships. Be careful with the possibility of variances of trust anchors. Decide before implementation which abstraction of trust relationship you need

It could be confusing because of so many trust relationships. Because CMP is defined to work also without a defined transport mechanism the security levels of trust are encapsulated. Certificates used for operation, used for CMP and used for the https connection to the CMP server can be issued from different CAs, no limitation is foreseen in the specifications for CMP. Therefore, for the enrollment different CAs can be used but not necessarily.

Technical realization RA/CA connection

The certificate enrollment between devices and RA is implemented by using EST published in [RFC7030] and used with the support of certificate based mutual authentication in SICAM GridPass.

The connection between the RA and CA works over the CMP lightweight profile. CMP is published in [RFC4210] and CRMF in [RFC4211], followed by a document specifying a transfer mechanism for CMP messages using HTTP [RFC6712]. CMP lightweight is a profiling to simplify the CMP variances.

CMP offers many variances of mechanisms to enroll a certificate. SICAM GridPass has a dedicated feature set to support CMP. Please check before implementation if the feature set is sufficient for your chosen external Certificate Authority

SICAM GridPass supports one variance to send the CSR to the CMP server. The CSR from RA to the CA for receiving an operational certificate is transmitted over a certificate based mutual authenticated https connection to the CMP server. Offline or http-based transmission is not supported. Additionally, this CSR is signed by a RA client certificate which is trusted by the CA. To accept an CA issued operational certificate on RA site the issuer of the CMP server certificate must be trusted also by the RA. No other variance is supported.

For the devices this works completely transparent because of using the EST protocol is used in the same way in case SICAM GridPass acts as an RA/CA in combination. Issuing certificates from an external CA is implemented for the automated certificate enrollment over EST and the manual certificate creation over the SICAM GridPass UI.

A revocation request over CMP protocol to the external CA is also supported.

Workflow

1. The device has a manual imported or during manufacturing phase imprinted certificate which is used for the mutual authenticated EST client connection to the SICAM GridPass RA.
    a. Additionally, the device has imported and trusted the CA certificate which has issued the SICAM GridPass RA EST server certificate.
    b. Additionally, the SICAM GridPass RA has imported and trusted the CA certificate which has issued the device EST client certificate.
2. The device generates a public/private key pair and a Certificate Signing Request (CSR) to request a certificate for e.g., to secure the IEC 61850-8-1 MMS connection according to IEC 62351-4. The device signs the CSR which includes the generated public key with the generated private key.
3. The device connects to the SICAM GridPass RA over EST which is a mutual authenticated TLS connection and sends the signed CSR to the SICAM GridPass RA.
4. SICAM GridPass RA checks the Proof of Possession (PoS) of the device private key with verifying the signature.
5. SICAM GridPass RA add optional parameters to the CSR and rebuild and signs the CSR conforming to the CMP standard.
6. SICAM GridPass RA connects to the CMP server of the external CA over https which is a mutual authenticated TLS connection and sends the SICAM GridPass signed CSR to the authenticated CMP server.
7. The CMP server forwards the CSR to the external CA which signs the CSR which results in a certificate.
8. The CMP server sends the certificate back over the https connection to SICAM GridPass RA. Afterwards SICAM GridPass RA send the certificate back to the device over the EST connection.
9. The device can use the certificate for the secured IEC 61850-8-1 connection.

Configuration

SICAM GridPass CMP configuration

Necessary key material, certificates, and CMP endpoint information
To use SICAM GridPass as Registration Authority (RA) normally you get the client certificates together with the private key from the Registration Authority as PKCS#12 containers. You need one key-pair for client authentication for the https connection to the external CA and one key pair for signing the Certificate Signing Requests (CSR) send over https to the CA which is supporting CMP.

Collect all necessary key material and certificates before starting the configuration because different stakeholders could be involved

Additionally, because of mutual authentication you will need the CA certificate from the CA which has issued the https server certificate and when validating signature-based protection of CMP response messages, also the CA certificate to trust while checking certificate chains during CMP server authentication. In case you have a trust chain of CA certificates you need the whole chain of the used CA certificates

For the later operation you also need the CA (chain) of the CA which is issuing the certificates in case this is different to the CA which has issued the https and CMP server certificate.

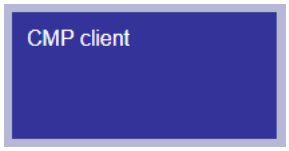
The CMP endpoint is represented by an URL which must be provided by the CA starting with https://....

Take also the SICAM GridPass manual beside this configuration information. This document describes only the CMP specific things

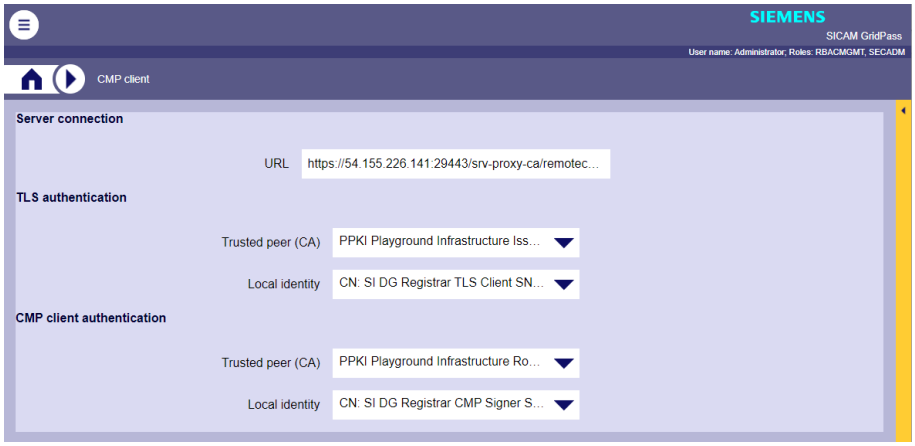
Presetting's in the SICAM GridPass User Interface to use CMP

At first import all necessary key material as mentioned above. Import your PKCS#12 certificate and key containers under the "Certificates" section and all received CA certificates under the "Certification authorities" section.

Afterwards, in the "CMP client" menu

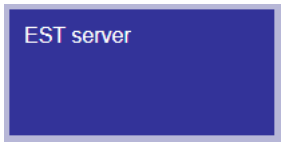


- enter the URL received by the CA provider under the "Server connection" section,
- select in the "TLS authentication" section the CA certificate which has issued the https server certificates and select the imported client certificate, which is used for the https client authentication,
- in the "CMP client authentication" section select the Root-CA certificate which is used for CMP server authentication and the client certificate which is signing the CSR over CMP.



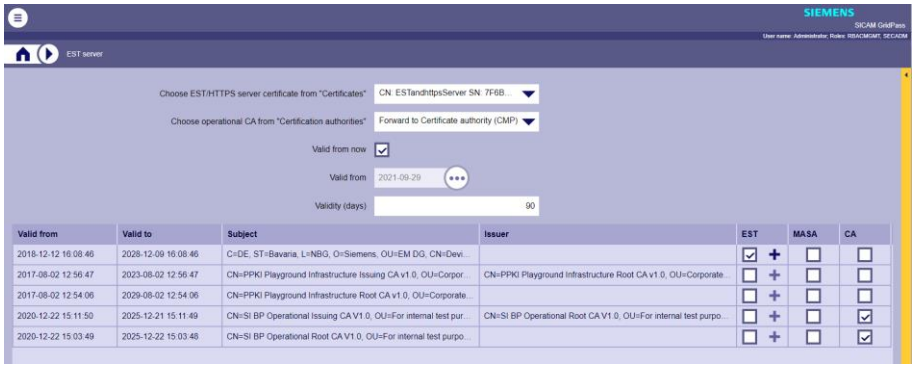
Settings in the SICAM GridPass User Interface to operate with an external CA over CMP

In the “EST server” menu

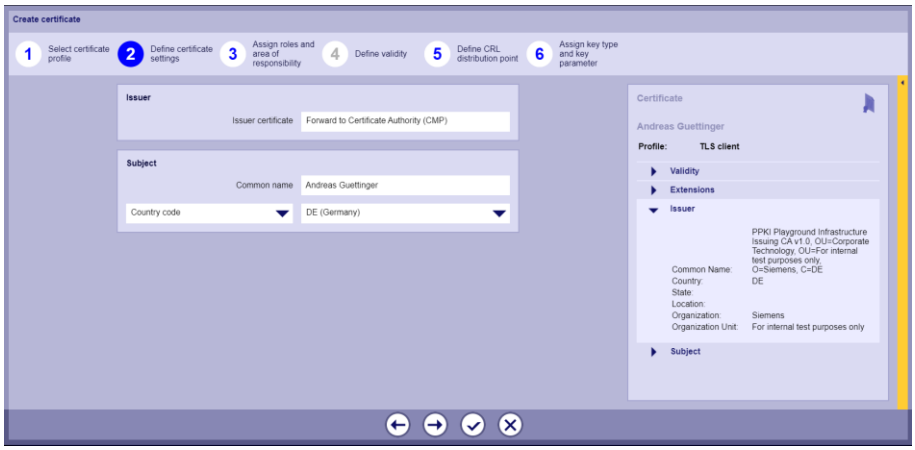


- choose for the operational CA „Forward to Certificate authority (CMP)”
- select all CAs in the CA checkbox section for distribution over the EST protocol to the certificate signing requester (e.g., SICAM A8000). Especially the CA (chain) which has issued the certificate.

Think about your secured process communication and Role Based Access Control which trust anchors must be available in your substation. Select these trust anchors here to distribute via EST



In case of a manual certificate request over the wizard, choose „Forward to Certificate authority (CMP)” for the Issuer certificate



Published by and copyright © 2021:

Siemens AG
Smart Infrastructure
Digital Grid
Humboldtstr. 59
90459 Nuremberg
Germany
www.siemens.com/gridsecurity

For more information,
please contact our
Customer Support Center.
Phone: +49 180 524 84 37
(Charges depending on the provider)
E-mail: support.energy@siemens.com