2.0.0 Release Notes

- Release Notes
  - fbeta ePA-Service – Version 2.0.0.
  - Überblick
  - Features
    - 1. TLS Clientsystem → TI-Gateway Konnektor
  - Troubleshooting
- Release Notes (ENG)
  - fbeta ePA-Service – Version 2.0.0
  - Overview
  - Features
    - 1. TLS client system → TI Gateway Konnektor
  - Troubleshooting

Release Notes

fbeta ePA-Service – Version 2.0.0.

Release-Typ: Feature Release

Betroffene Komponenten: Konnektor/TLS, beginn TI 2.0

Überblick

Version 2.0.0 fokussiert sich auf die RISE-seitige Umstellung vom TIaaS-Client auf das TI-Gateway.

Der Fokus dieses Releases liegt insbesondere auf:

- Handling des Clients beim Kommunizieren mit dem Konnektor über den TI-Gateway,

---

Features

1. TLS Clientsystem → TI-Gateway Konnektor

Das TLS-Verhalten für Konnektor-Requests wurde entsprechend der Anforderung vom TI-Gateway angepasst.

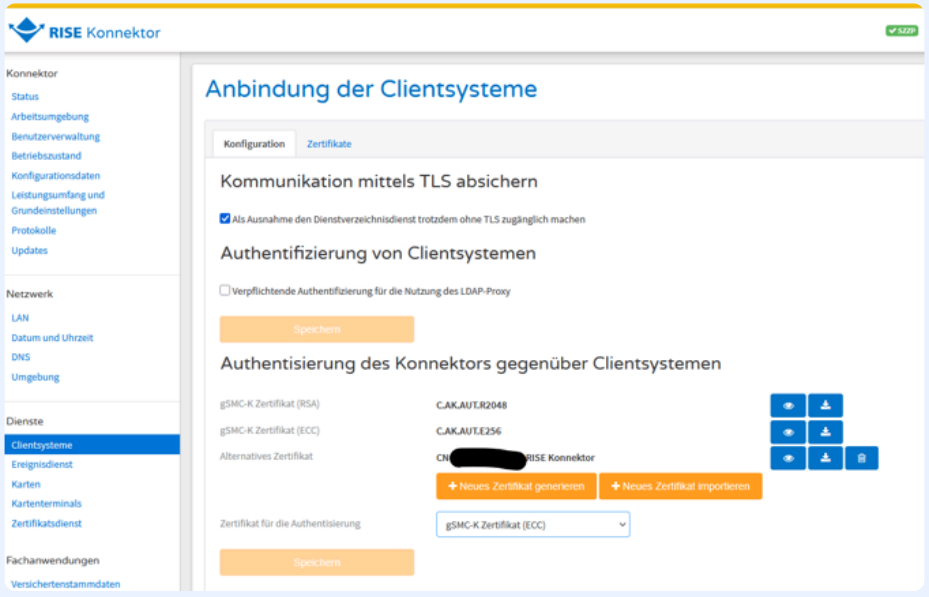
Neu in 2.0.0:

- `KONNEKTOR_TLS_MODE` : Diese neue Umgebungsvariable **MUSS** gesetzt sein. Sie bildet die Konfiguration ab, wie der Konnektor sich beim Client authentifiziert. Da der Konnektor diesbezüglich verschiedene Möglichkeiten bietet, ist es wichtig, diese Konfiguration gleich der Konfiguration im Konnektor zu setzen.
  - `smc_k` : Der TLS-Handshake wird mit dem gSMC-K-Zertifikat durchgeführt. Dies ist der empfohlene Modus für den Produktivbetrieb. Das smc_k-Zertifikat wird von der gematik ausgestellt und kann über den TI-Truststore validiert werden.

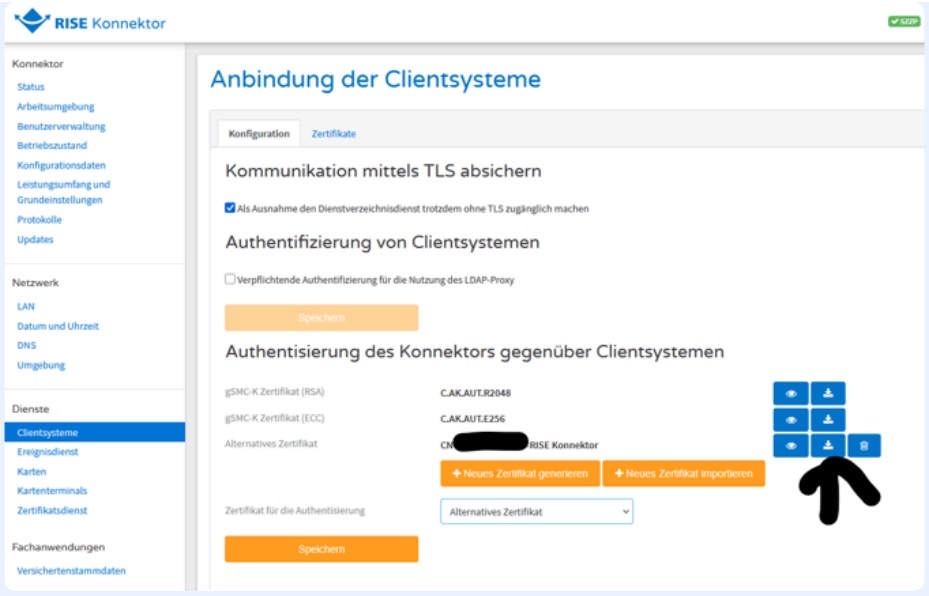
- `alternative` : Der TLS-Handshake wird mit einem alternativen Zertifikat durchgeführt. Dies wird typischerweise für Test- oder Entwicklungszwecke verwendet. Das alternative Zertifikat wird vom Konnektor selbst ausgestellt und wird nicht über den TI-Truststore validiert. Das Zertifikat muss in der Datei config/ssl/konnektor/cert.pem bereitgestellt werden.
- `insecure` : Der TLS-Handshake wird ohne Überprüfung des Konnektor-Zertifikats durchgeführt. Dies ist unsicher und wird für den Produktivbetrieb NICHT empfohlen.

Bezüglich `KONNEKTOR_TLS_MODE` : Wählen Sie den Modus so, dass er der Konfiguration des Konnektors entspricht.
Das bedeutet:

- Wenn Sie den `smc_k` -Modus gewählt haben, gehen Sie sicher, dass `“KonnektorUI > Dienste > Clientsysteme > Konfiguration > Authentisierung des Konnektors gegenüber Clientsystemen > Zertifikat für Authentisierung”` auf `“gSMC-K Zertifikat (ECC)”` gesetzt ist.



- Wenn Sie den `alternative` -Modus gewählt haben, gehen Sie sicher, dass `“KonnektorUI > Dienste > Clientsysteme > Konfiguration > Authentisierung des Konnektors gegenüber Clientsystemen > Zertifikat für Authentisierung”` auf `“Alternatives Zertifikat”` gesetzt ist.
  Laden Sie danach das “Alternative Zertifikat” herunter und speichern es als “cert.pem” im config-Ordner.



- Wenn Sie den `insecure`-Modus gewählt haben, sind keine weiteren Einstellungen nötig.

- Die Umgebungsvariablen `KONNEKTOR_JWS_URL` und `KONNEKTOR_ALLOW_INSECURE_TLS` werden nicht mehr benötigt und können aus der Konfigurationsdatei entfernt werden.

Troubleshooting

Bei Verbindungsproblemen in 2.0.0 prüfen Sie insbesondere:

- ob `KONNEKTOR_TLS_MODE` den Konfigurationen auf der Konnektor-UI entspricht (siehe `“Features > 1. TLS Clientsystem → TI-Gateway Konnektor”` above)
- Vollständigkeit der `config/.env`.
  - .env.template:

```
# RU (RU REF) , RT (RU DEV) or PROD
EPA_ENVIRONMENT = 'RT'

USER_AGENT = 'usrAgent/1.1.0'
# The url or ip address of the Konnektor to connect to.
# This is typically provided by your Konnektor / TI-as-a-Service provider or can be f
KONNEKTOR_URL = 'https://1.2.3.4'

# password for the konnektor '.p12' certificate
KONNEKTOR_CERT_PW = 'xxxx'

# Sets the mode in which the TLS handshake is performed on the connector.
# NOTE: Depending on how the configuration is set in the connector UI, different mode
# OPTIONS:
# - "smc_k": The TLS handshake is performed using the gSMC-K certificate. This is the
#            The smc_k certificate is issued by the gematik an can be validated by th
# - "alternative": The TLS handshake is performed using an alternative certificate. T
#                  The alternative certificate is issued by the Konnektor itself and
# - "insecure": The TLS handshake is performed without verifying the Konnektor's cert
KONNEKTOR_TLS_MODE = "smc_k"



# --- DiGA-specific variables (used when SMC-B has DiGA professionOID) ---
# Construct the Author string from the following variables
DIGA_NAME = ''
DIGA_MANUFACTURER = ''
```

```
SW_ADDITION_1 = '' # optional
SW_ADDITION_2 = '' # optional
SW_ADDITION_3 = '' # optional

#Alternatively, the entire Author string can also be used
#AUTHOR =


MANDANT_ID = ''
CLIENT_SYSTEM_ID = ''
WORKPLACE_ID = ''
USER_ID = '' # optional


LOG_LEVEL = 'INFO'
# Timeout for HTTPS requests in seconds
HTTPS_TIMEOUT = 30

# Mapping of provider numbers to service endpoints
# See: https://gemspec.gematik.de/docs/gemSpec/gemSpec_Aktensystem_ePAfueralle/latest
RECORD_PROVIDER_1 = 'IBM'
RECORD_PROVIDER_2 = 'Bitmarck Technik'

# Redis configuration
REDIS_HOST = 'redis'
REDIS_PORT = "6379"
REDIS_PASSWORD = ""
REDIS_DB = "0"

# Uvicorn Worker
UVICORN_WORKERS = "1"


# Optional: Enable a minimal UI to test API calls from a browser with basic auth
# UI_ENABLED = "True"
# Optionally pre-fill InsurantId suggestions used by the UI (Comma-separated list)
# UI_INSURANT_IDS = 'X110596703,X110580673,X110683834,X110618636,X110631746,X11053669
```

Release Notes (ENG)

fbeta ePA-Service – Version 2.0.0

Release type: Feature Release

Affected components: Konnektor/TLS, beginning TI 2.0

Overview

Version 2.0.0 focuses on the RISE-side migration from the TIaaS client to the TI Gateway.

The focus of this release is particularly on:

- Handling the client when communicating with the Konnektor via the TI Gateway.

Features

1. TLS client system → TI Gateway Konnektor

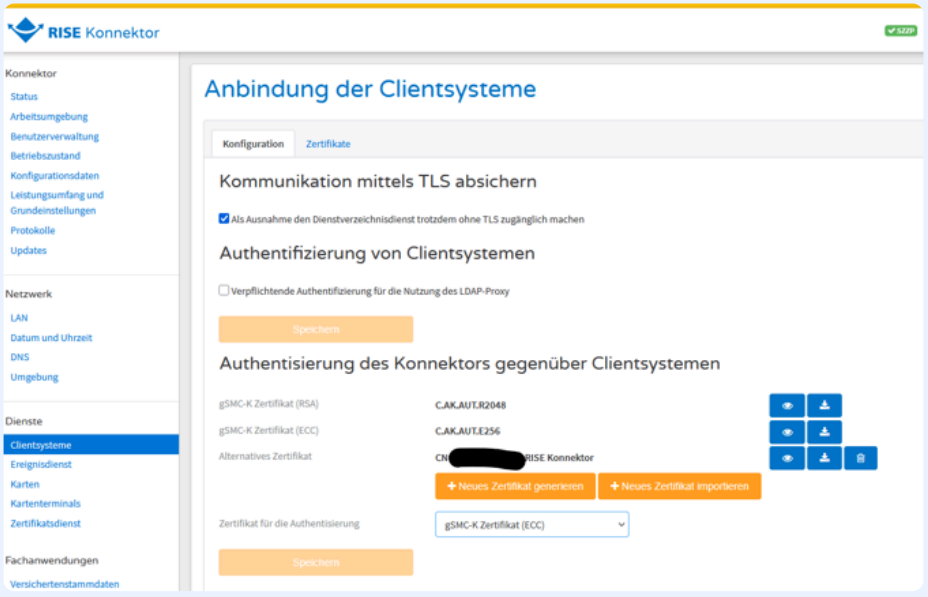
The TLS behavior for Konnektor requests has been adjusted according to the TI Gateway requirements.

New in 2.0.0:

- `KONNEKTOR_TLS_MODE`: This new environment variable **MUST** be set. It represents the configuration for how the Konnektor authenticates itself to the client. Since the Konnektor offers several options in this regard, it is important to set this configuration to match the configuration in the Konnektor.
  - `smc_k`: The TLS handshake is performed using the gSMC-K certificate. This is the recommended mode for production use. The smc_k certificate is issued by gematik and can be validated via the TI truststore.
  - `alternative`: The TLS handshake is performed using an alternative certificate. This is typically used for testing or development purposes. The alternative certificate is issued by the Konnektor itself and is not validated via the TI truststore. The certificate must be provided in the file config/ssl/konnektor/cert.pem.
  - `insecure`: The TLS handshake is performed without verifying the Konnektor certificate. This is insecure and is NOT recommended for production use.

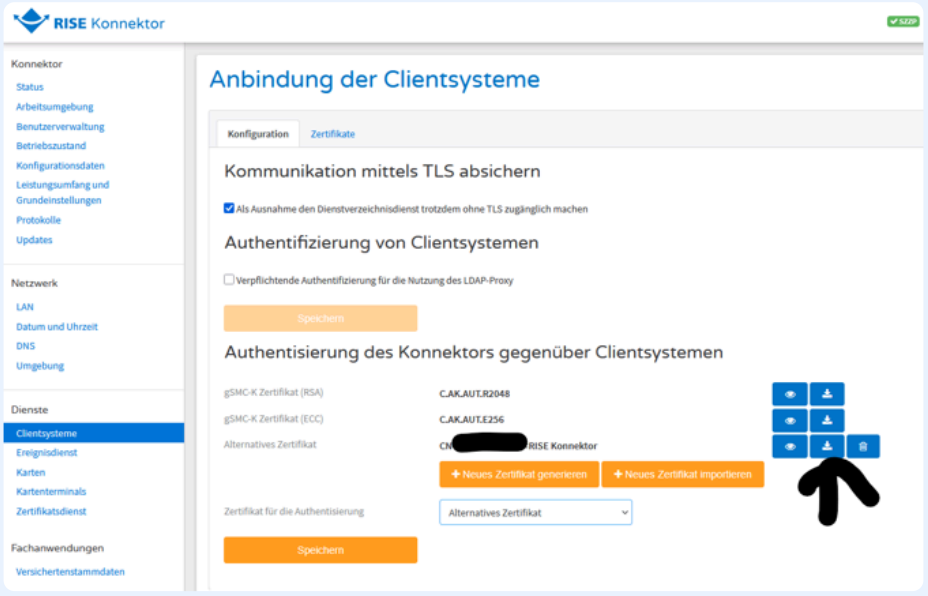
Regarding `KONNEKTOR_TLS_MODE`: Choose the mode so that it matches the Konnektor configuration.
This means:

- If you selected `smc_k` mode, make sure that `"KonnektorUI > Services > Client systems > Configuration > Authentication of the Konnektor to client systems > Certificate for authentication"` is set to `"gSMC-K certificate (ECC)"`.



- If you selected `alternative` mode, make sure that `"KonnektorUI > Services > Client systems > Configuration > Authentication of the`

`Konnektor to client systems > Certificate for authentication"` is set to `"Alternative certificate"`.
Afterwards, download the "Alternative certificate" and save it as "cert.pem" in the config folder.



- If you selected `insecure` mode, no further settings are required.

- The environment variables `KONNEKTOR_JWS_URL` and `KONNEKTOR_ALLOW_INSECURE_TLS` are no longer used and can be removed from the configuration file.

Troubleshooting

In case of connectivity issues in 2.0.0 please check:

- that `KONNEKTOR_TLS_MODE` equals configurations in Konnektor-UI (see `"Features > 1. TLS client system → TI Gateway Konnektor"` above)
- that everything is included in `config/.env`.
  - .env.template:

```
# RU (RU REF) , RT (RU DEV) or PROD
EPA_ENVIRONMENT = 'RT'

USER_AGENT = 'usrAgent/1.1.0'
# The url or ip address of the Konnektor to connect to.
# This is typically provided by your Konnektor / TI-as-a-Service provider or can be f
KONNEKTOR_URL = 'https://1.2.3.4'

# password for the konnektor '.p12' certificate
KONNEKTOR_CERT_PW = 'xxxx'

# Sets the mode in which the TLS handshake is performed on the connector.
# NOTE: Depending on how the configuration is set in the connector UI, different mode
# OPTIONS:
# - "smc_k": The TLS handshake is performed using the gSMC-K certificate. This is the
#            The smc_k certificate is issued by the gematik an can be validated by th
# - "alternative": The TLS handshake is performed using an alternative certificate. T
```

```
#                  The alternative certificate is issued by the Konnektor itself and
# - "insecure": The TLS handshake is performed without verifying the Konnektor's cert
KONNEKTOR_TLS_MODE = "smc_k"


# --- DiGA-specific variables (used when SMC-B has DiGA professionOID) ---
# Construct the Author string from the following variables
DIGA_NAME = ''
DIGA_MANUFACTURER = ''
SW_ADDITION_1 = '' # optional
SW_ADDITION_2 = '' # optional
SW_ADDITION_3 = '' # optional


#Alternatively, the entire Author string can also be used
#AUTHOR =

MANDANT_ID = ''
CLIENT_SYSTEM_ID = ''
WORKPLACE_ID = ''
USER_ID = '' # optional


LOG_LEVEL = 'INFO'
# Timeout for HTTPS requests in seconds
HTTPS_TIMEOUT = 30

# Mapping of provider numbers to service endpoints
# See: https://gemspec.gematik.de/docs/gemSpec/gemSpec_Aktensystem_ePAfueralle/latest
RECORD_PROVIDER_1 = 'IBM'
RECORD_PROVIDER_2 = 'Bitmarck Technik'

# Redis configuration
REDIS_HOST = 'redis'
REDIS_PORT = "6379"
REDIS_PASSWORD = ""
REDIS_DB = "0"

# Uvicorn Worker
UVICORN_WORKERS = "1"


# Optional: Enable a minimal UI to test API calls from a browser with basic auth
# UI_ENABLED = "True"
# Optionally pre-fill InsurantId suggestions used by the UI (Comma-separated list)
# UI_INSURANT_IDS = 'X110596703,X110580673,X110683834,X110618636,X110631746,X11053669
```