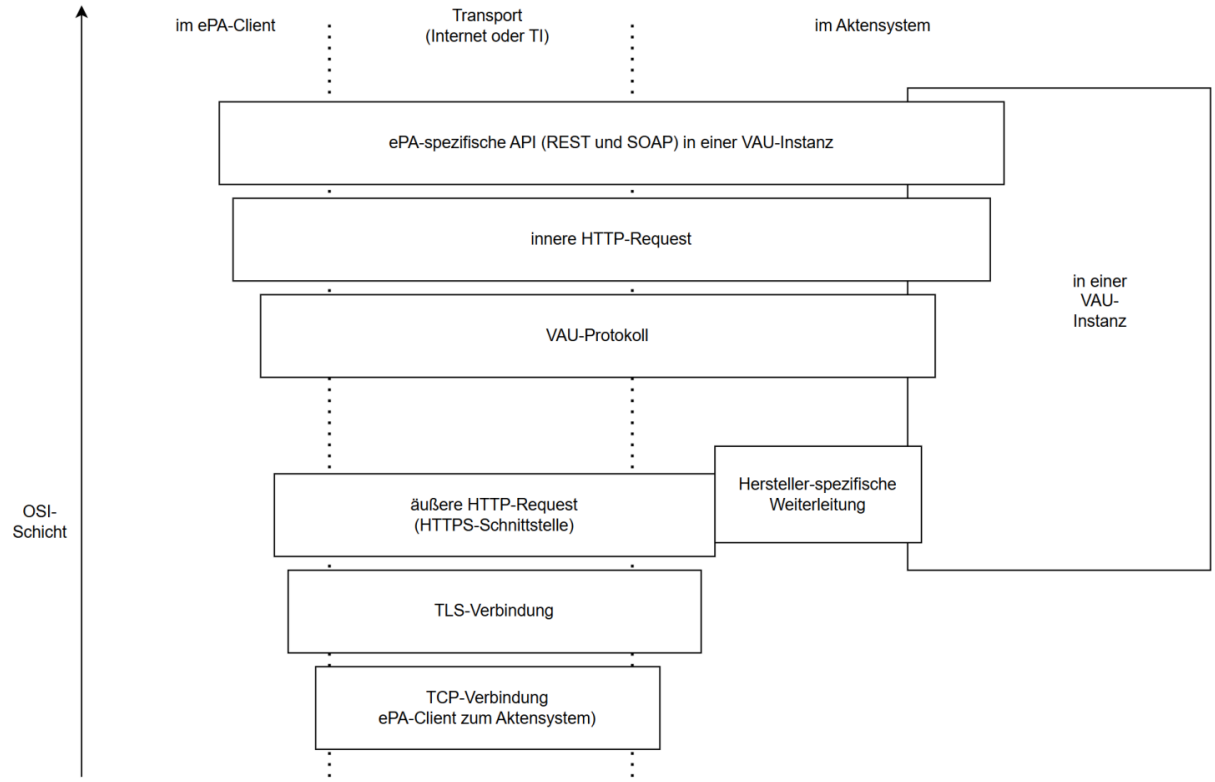
TLS+VAU-Protokoll

Bei ePA wird bei den Kommunikationen zwei Sicherungsschichten (TLS+VAU-Protokoll) parallel verwendet.



Zunächst gibt es eine TLS-Schicht, die die Grundlage einer HTTPS-Schnittstelle ist. Auf der TLS-Ebene gibt es ein TLS-Server-Zertifikat aus der TI-PKI.

Über diese HTTPS-Schnittstelle werden "äußere HTTP-Request" vom Client an den Server (VST, FDZ, ePA-AS) gesendet.

In diesen äußeren Requests sind VAU-Protokoll-Nachrichten verpackt. Eine zentrale Grundlage des VAU-Protokolls stellt das VAU-Protokoll-Server-Zertifikat -- wieder aus der Komponenten-PKI der TI.

VAU-Protokoll:

Spezifikation:	https://gemspec.gematik.de/docs/gemSpec/gemSpec_Kryp t/latest/#7
Beispiel-Code für Aushandlung der symmetrischen VAU-Kanal-Schlüssel:	https://bitbucket.org/andreas_hallof/vau-protokoll/src/master/minimal/

Beispiel-Code in python	https://bitbucket.org/andreas_hallof/vau-protokoll/src/master/
Beispiel-Code für Java:	https://github.com/gematik/lib-vau
Beispiel-Code in C#:	https://github.com/gematik/lib-vau-csharp
Beispiel-Code in Go:	https://github.com/gematik/zero-lab/tree/vau/pkg/libvau

Revision #4
Created 10 April 2025 15:27:57 by Admin
Updated 10 April 2025 21:44:57 by Admin