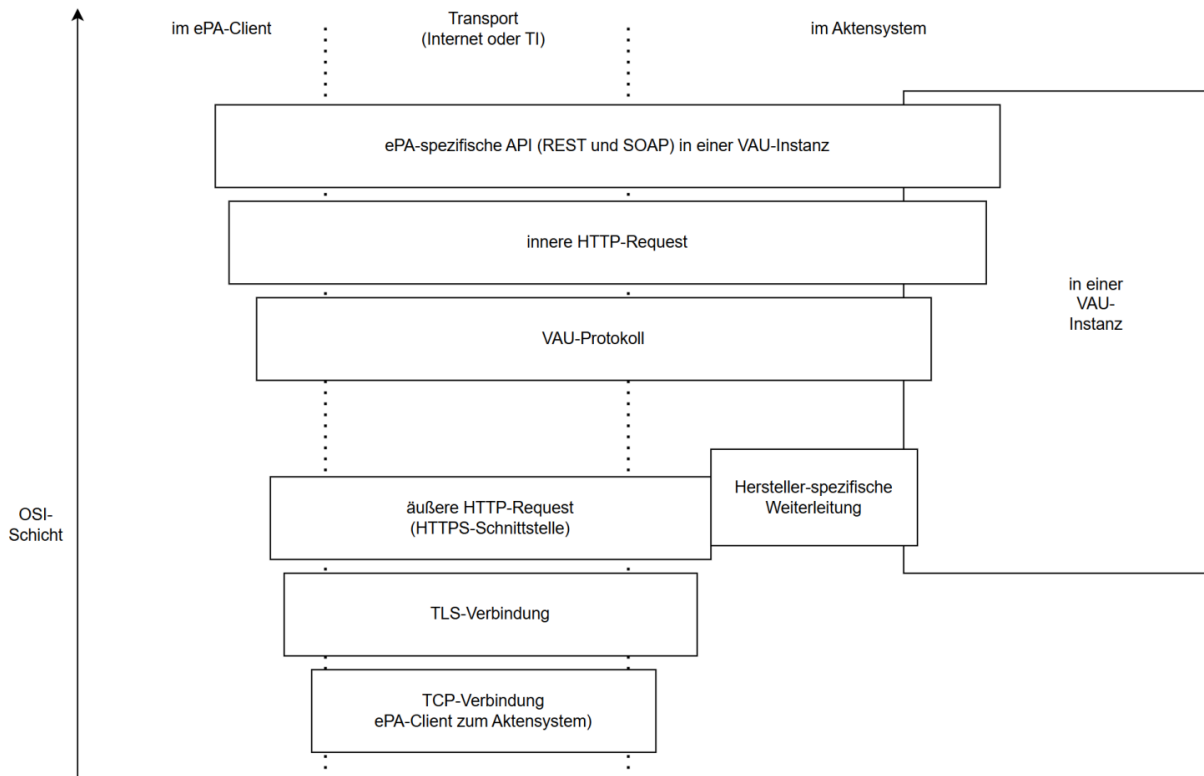


# TLS+VAU-Protokoll

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:	<a href="https://gemospec.gematik.de/docs/gemSpec/gemSpec_Krypt/latest/#7">https://gemospec.gematik.de/docs/gemSpec/gemSpec_Krypt/latest/#7</a>
Beispiel-Code für Aushandlung der symmetrischen VAU-Kanal-Schlüssel:	<a href="https://bitbucket.org/andreas_hallof/vau-protokoll/src/master/minimal/">https://bitbucket.org/andreas_hallof/vau-protokoll/src/master/minimal/</a>

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

---

Revision #4

Created 10 April 2025 15:27:57 by Admin

Updated 10 April 2025 21:44:57 by Admin