Historische Entwicklung VAU-Protokoll

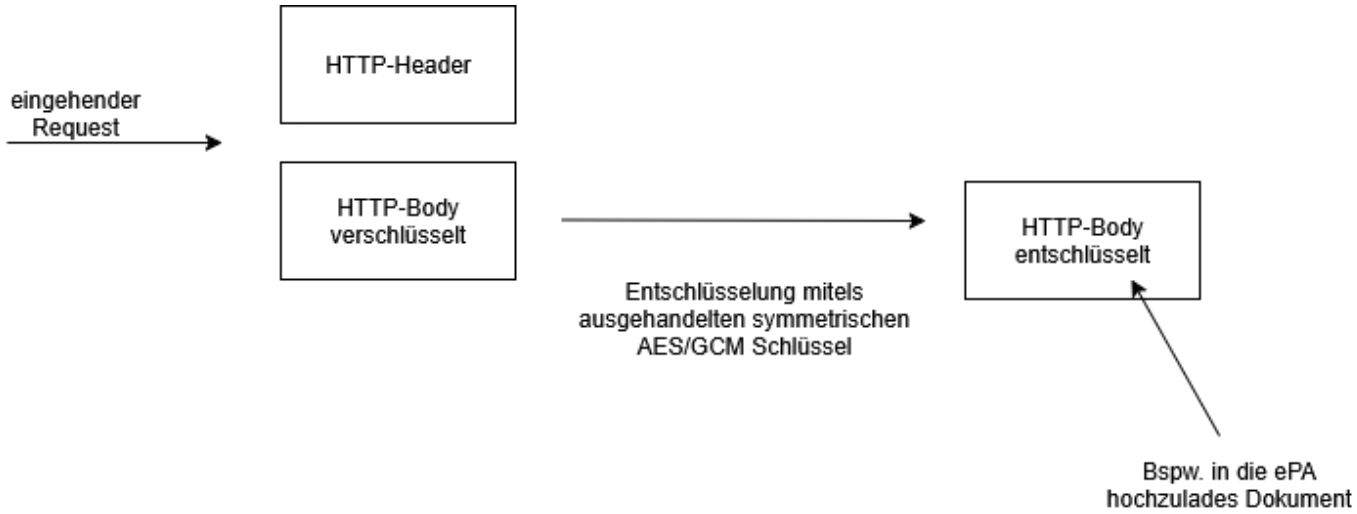
VAU-Protokoll Version 1.0

Im Jahr 2018 für erste ePA-Version (= Version 1.0) spezifiziert als zusätzliche Sicherungsschicht da TLS vor den VAU-Instanzen (Anwendungslogik) terminiert.

Für die Sicherung (authentisierte symmetrische Verschlüsselung mittels AES/GCM) muss mindestens ein symmetrischer Schlüssel frisch erzeugt werden. (Forward-Secrecy). -> Schlüsselaushandlung in einer Verbindungsinitialisierung mit dem Client.

(Hinweis: mit asymmetrischen kryptographischen Verfahren können nur sehr kleine Datenmengen verschlüsselt werden. -> man muss irgendwie zu symmetrischen Schlüsseln kommen.)

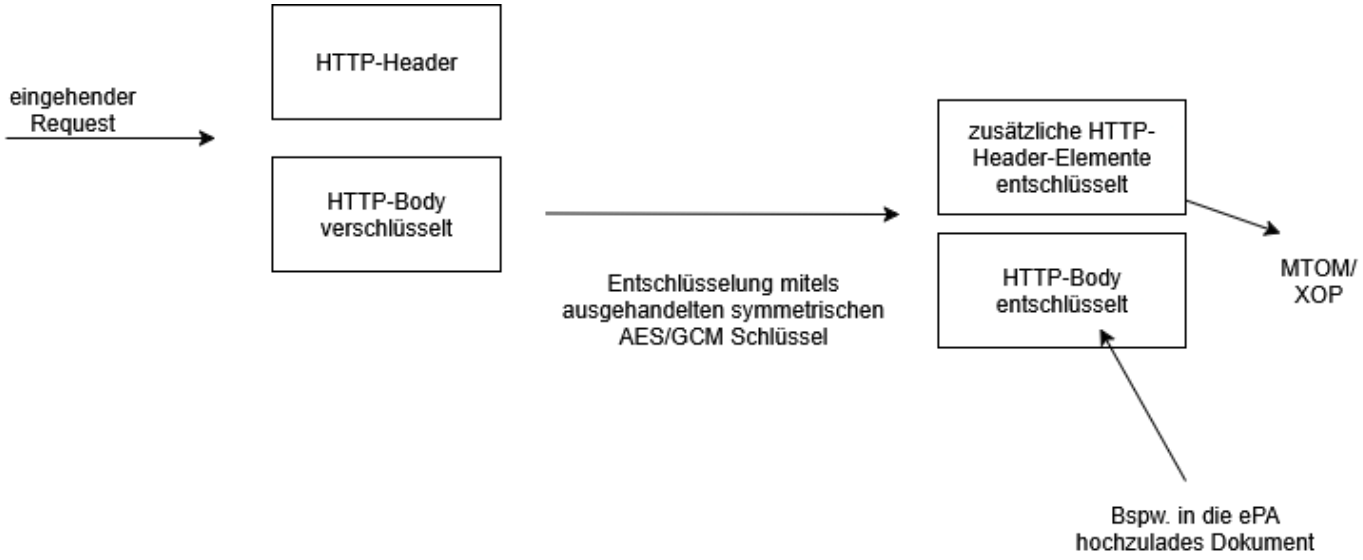
Nur die "Dokumente" (in SOAP-Container eingebettete Objekte) im HTTP-Body wurde verschlüsselt. Da 1-zu-1 Beziehung wurde der HTTP-Body = SOAP-Container = medizinisches Dokument verschlüsselt.



VAU-Protokoll Version 1.1

Im Jahr 2019 Erkenntnis: bei bestimmen SOAP-Kodierungen („SOAP Message Transmission Optimization Mechanism (MTOM)“/ „XML-binary Optimized Packaging (XOP)“-Kodierung) findet eine (aus Sicht VAU-Protokoll 1.0) ungünstige Verknüpfung zwischen HTTP-Body und HTTP-Header statt. Deshalb mussten nun auch Teile des HTTP-Headers in die Sicherung durch das VAU-Protokoll inkludiert

werden.

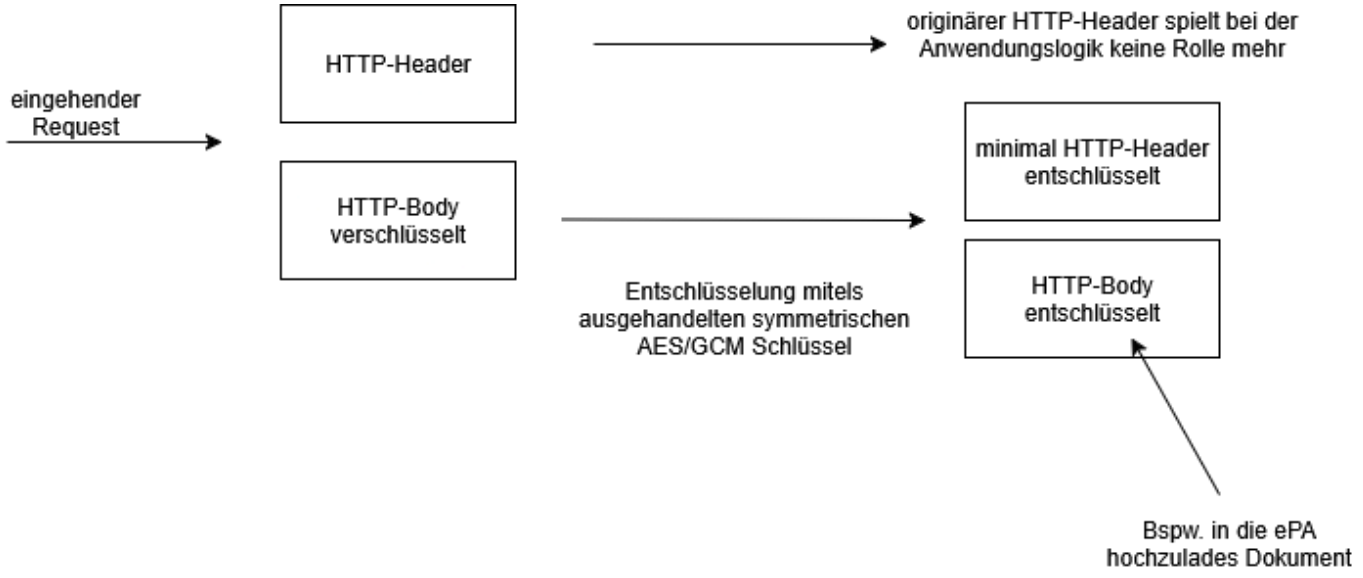


VAU-Protokoll Version für ePA für alle

Im Jahr 2023, Notwendigkeit der Änderung:

- Änderung der Authentisierungsmethode (OAuth2/OIDC)
- PQC-Sicherheit mit einbringen

Mit den Erfahrungen der Notwendigkeit der Anpassung von Version 1.0 nach 1.1 wird nun komplett ein minimaler HTTP-Header mit inkludiert. Es gibt also eine vollständigen HTTP-konformen inneren HTTP-Request / -Response.



Revision #4
Created 24 July 2025 07:03:09 by Admin

Updated 15 February 2026 10:21:25 by Admin