


# DER SCHLÜSSEL VOM SCHLÜSSEL VOM SCHLÜSSEL

Die Epa - technische Erklärung

Abstract orange line art in the bottom right corner, resembling a stylized map or a complex network of lines.



Vortrag: Authentifizierung, SAML, etc, wird nicht betrachtet  
Empfehlungen:

36c3: "Hacker hin oder her": Die elektronische Patientenakte kommt!

[media.ccc.de/v/36c3-10595-hacker\\_hin\\_oder\\_her\\_die\\_elektronische\\_patientenakte\\_kommt](https://media.ccc.de/v/36c3-10595-hacker_hin_oder_her_die_elektronische_patientenakte_kommt)

38c3: „Konnte bisher noch nie gehackt werden“: Die elektronische Patientenakte kommt - jetzt für alle!

[media.ccc.de/v/38c3-konnte-bisher-noch-nie-gehackt-werden-die-elektronische-patientenakte-kommt-jetzt-fr-alle](https://media.ccc.de/v/38c3-konnte-bisher-noch-nie-gehackt-werden-die-elektronische-patientenakte-kommt-jetzt-fr-alle)



1100 Seiten Spezifikation



zu schützende Dokument



## Meta Daten

- title, author, comments, creationTime, languageCode, mimeType, size
- u.a. für Suche und Exploration



## Policy-Dokumente

- Zugriffsregeln auf Dokument, Ersteller-Recht, ...
- Für jeden Versicherten, Vertreter, jede berechnigte Leistungserbringerinstitution ein Dokument
- wird im Frontend erzeugt



zu schützende  
Dokument



dokumentenindividueller symmetrischer  
Dokumentenschlüssel



Dokumenten  
Chifftrat



Meta Daten



aktenspezifischer symmetrischer  
kontextschlüssel



Meta Dokumenten  
Chiffre



Policy-Dokumente



aktenspezifischer symmetrischer  
Kontextschlüssel



Policy Dokumenten  
Chiffirat



dokumentenindividueller symmetrischer Dokumentenschlüssel



aktenspezifischer symmetrischer Aktenschlüssel

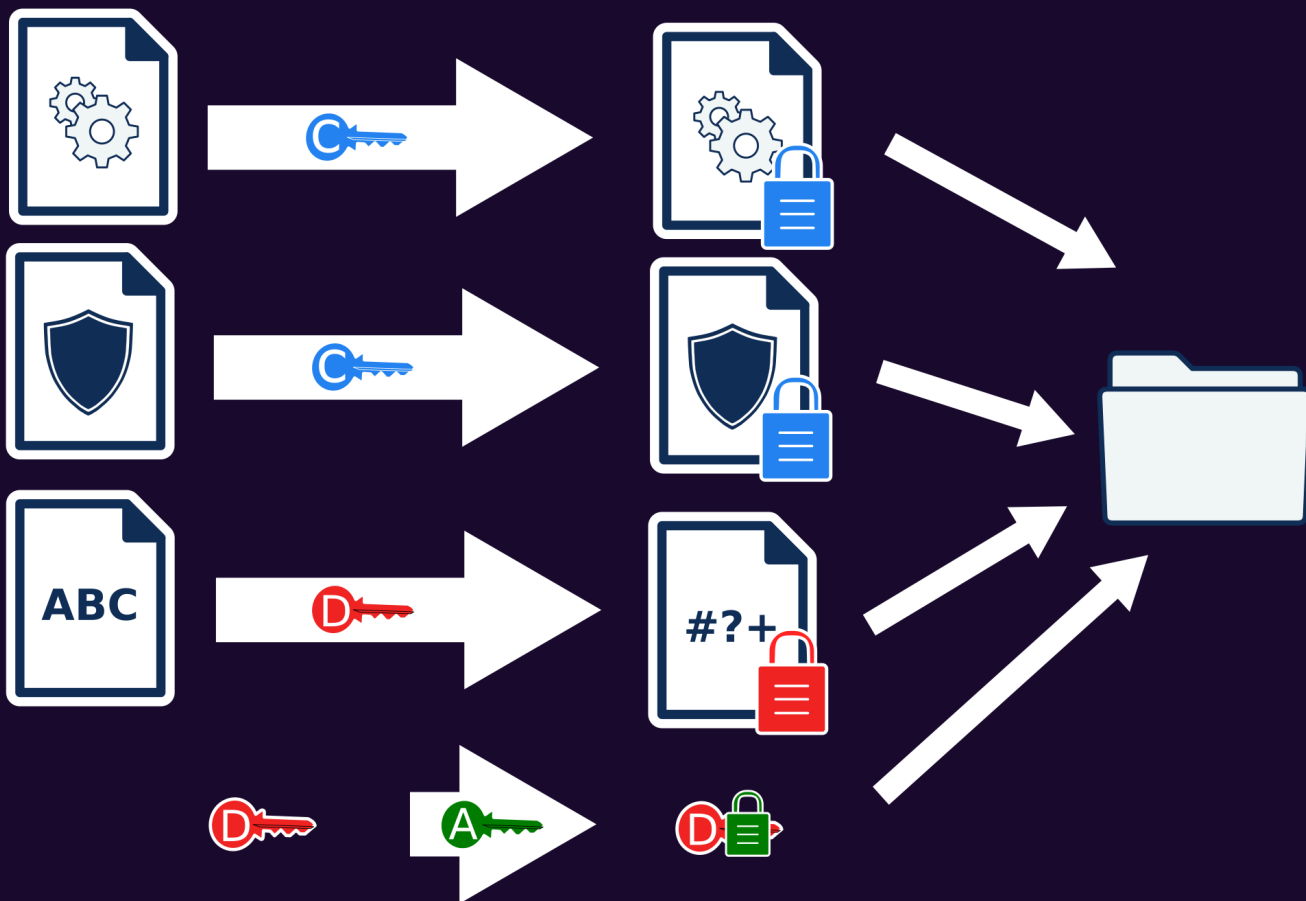


Dokumentenschlüssel Chiffre





Aktensystem



**AKTENWEITE SCHLÜSSEL**

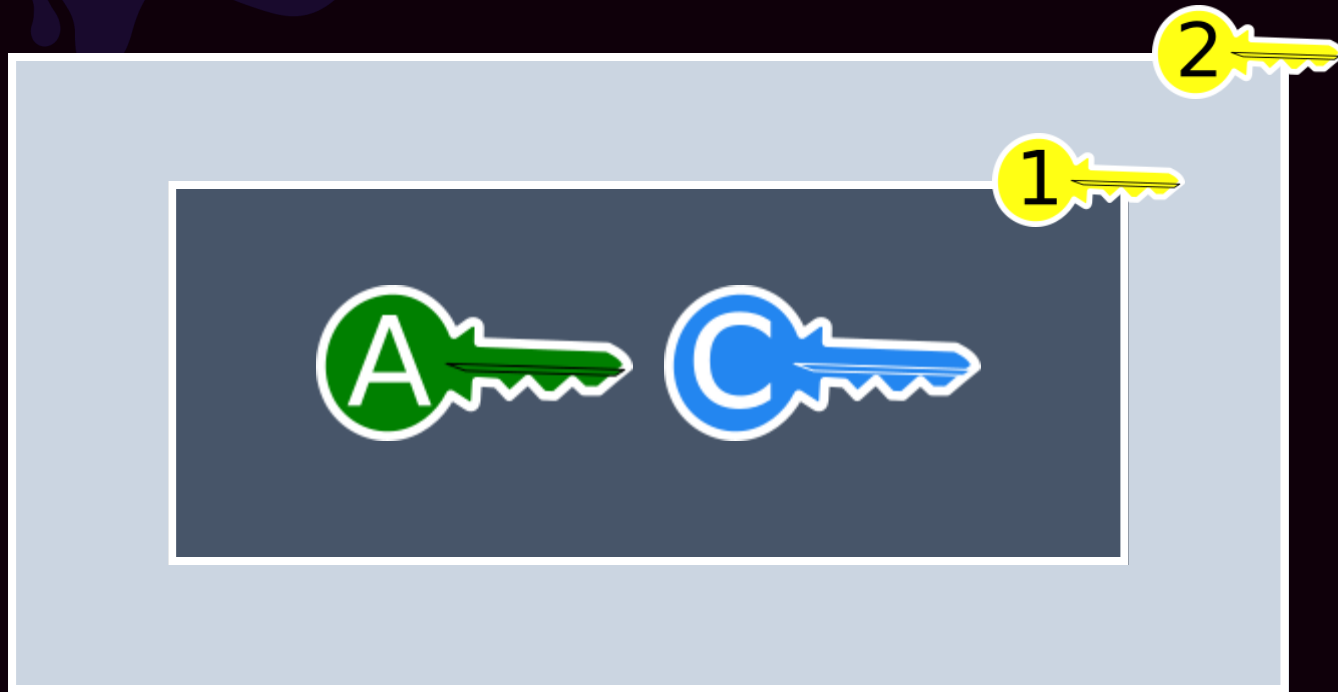
# AKTENWEITE SCHLÜSSEL



aktenspezifischer symmetrischer Aktenschlüssel



aktenspezifischer symmetrischer Kontextschlüssel



- clientseitig zweifach verschlüsselte Chiffre im "Zwiebelschalenprinzip" mittels AES-GCM
- mit Autorisierungsschlüssel 1 und 2

# SCHLÜSSELGENERIERUNGSDIENST 1 & 2

- generiert AES-256-Bit-Schlüssel für eine Entität
- Die zwei SGD sind technisch, organisatorisch und wirtschaftlich unabhängig voneinander
- Schlüsselableitung auf Grundlage von geheimen SGD-spezifischen Ableitungsschlüsseln (Masterkeys) und Ableitungsvektoren
- Deterministisch

AES-256(SHA-256(Vector), Masterkeys)

# ABLAUF ERSTMALIGE GENERIERUNG

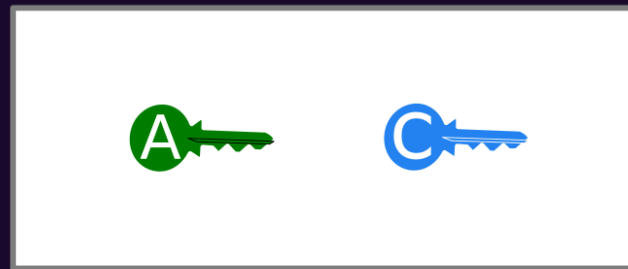
Request:  
r1:[KVN R]



SEED = [256-Bit-RND-in-Hexform];  
VEKTOR = r1:[SEED]:[KVN R]:[NAME\_OF\_CURRENT\_MASTERKEY]  
KEY = AES-256(SHA-256(VEKTOR),MASTERKEY)

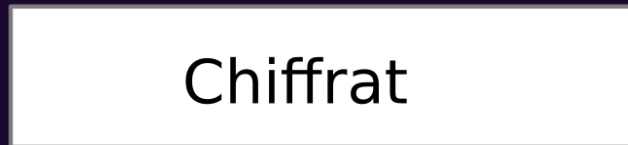


Response:  
AES-256-Bit-Schlüssel-in-Hexform und Vektor



SGD1

Vektor



SGD2

Vektor



Einlagerung in  
Komponente Autorisierung



# ABLAUF ZUKÜNFTIGE ABLEITUNG

Request:

r1:[SEED]:[KVNDR]:[NAME\_OF\_CURRENT\_MASTERKEY]



KEY = AES-256(SHA-256(VEKTOR),MASTERKEY)



Response:

AES-256-Bit-Schlüssel-in-Hexform und Vektor

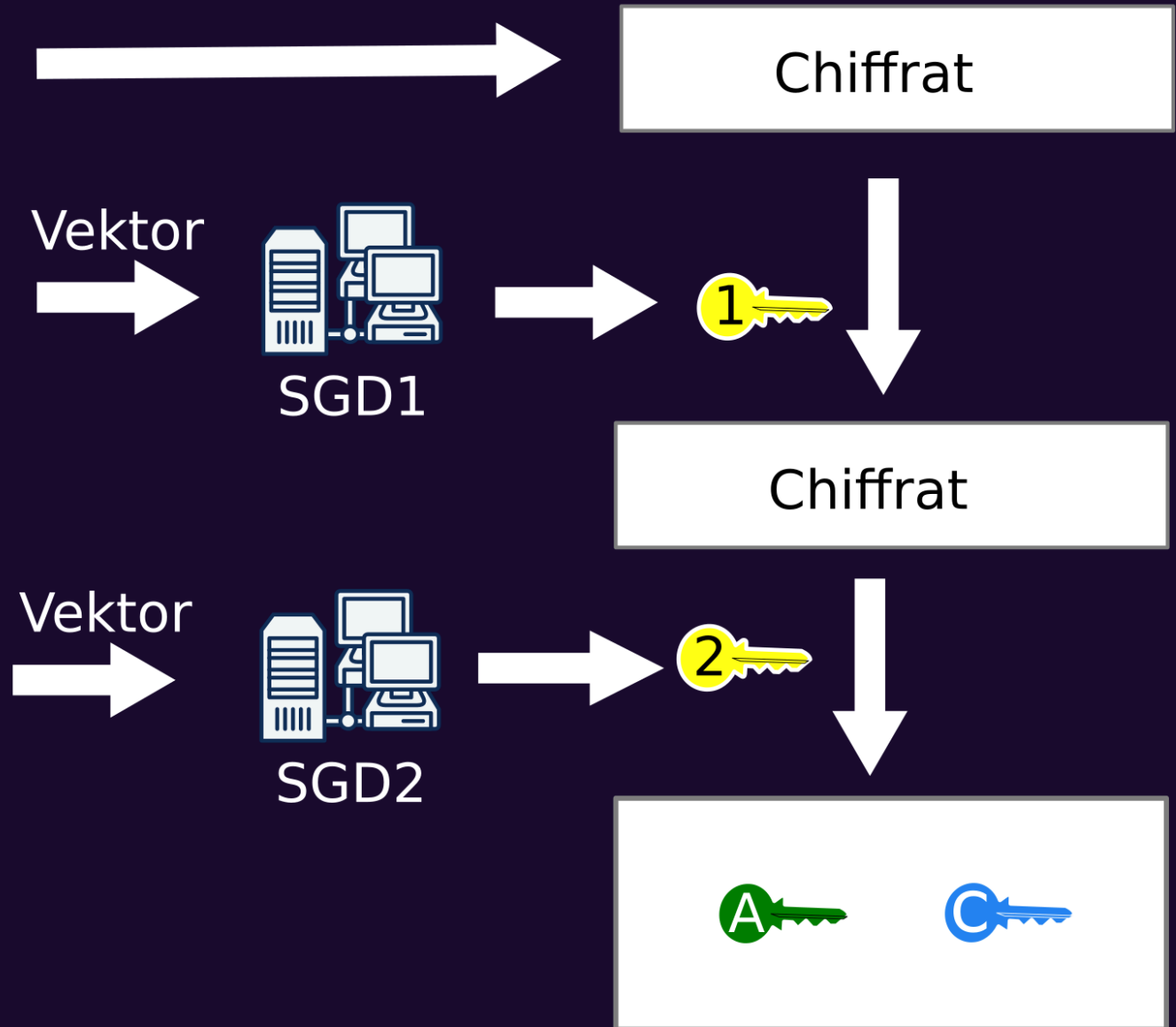
# FREITABE FÜR LEISTUNGSERBRINGER

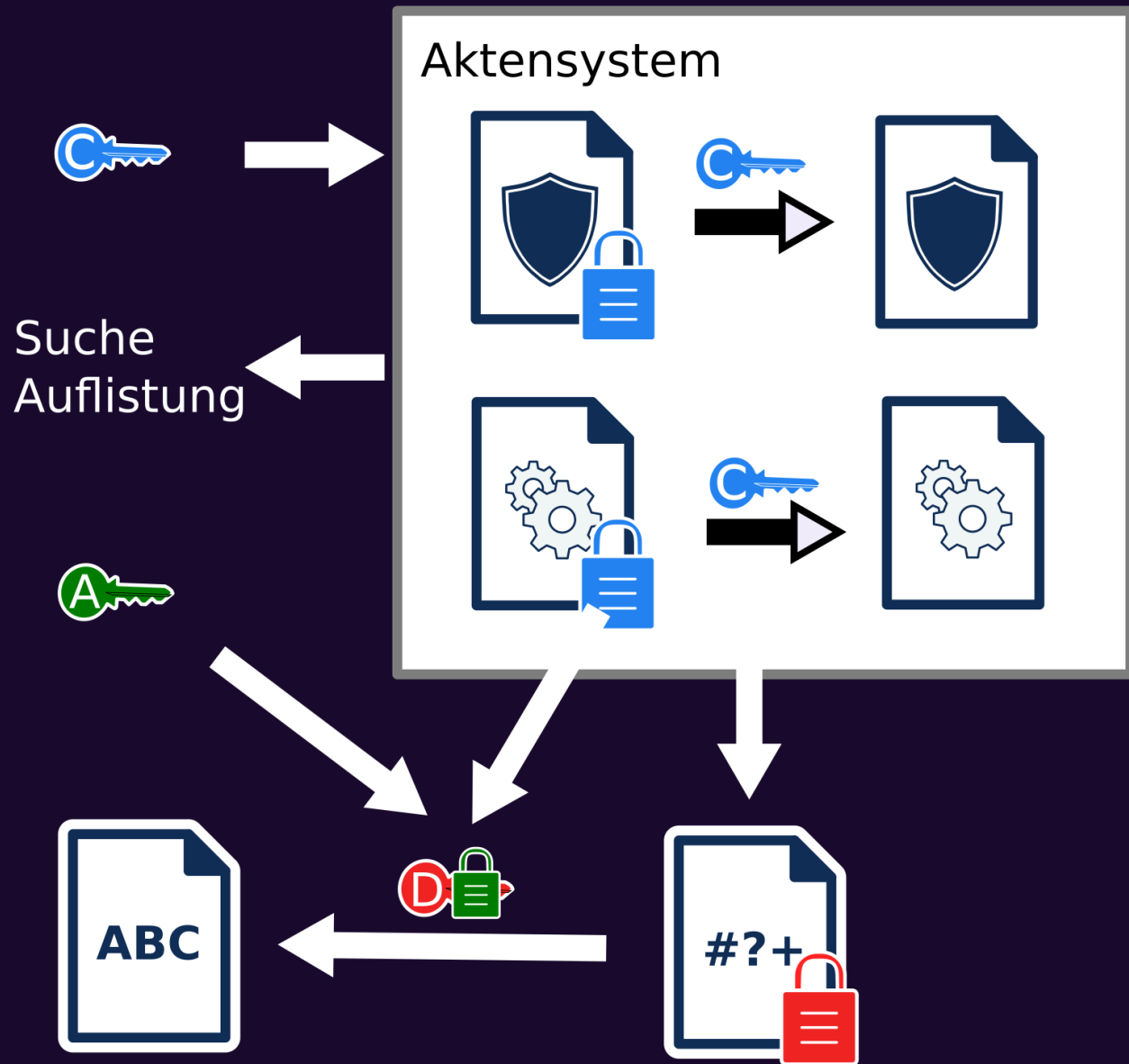
Vektor: r1:[SEED]:[KVNR]:[Telematik-ID]:[NAME\_OF\_CURRENT\_MASTERKEY]

- Autorisierungsschlüssel 1 & 2 für Berechtigten an SGDs anfragen
- Akten- und Kontextschlüssel für Berechtigten verschlüsseln
- Chiffre und Ableitungsvektoren in "Komponente Autorisierung" ablegen

Abruf Abruf

# Komponente Autorisierung





# VERTRAUENSWÜRDIGE AUSFÜHRUNGSUMGEBUNG - VAU

- Geschützte Nutzer-Session individuelle, nicht einsehbare umgebung im Aktensystem
- Nutzer überträgt über verschlüsselten und authentisierten Datenkanal Kontextschlüssel in diese
- in VAU werden Kontext informationen entschlüsselt, zum Beispiel für Suche

# UMSCHLÜSSELUNG

- Dabei werden Akten- und Kontextschlüssel ausgetausch
- Muss clientseitig passieren
- Alle Dokumentenschlüssel werden mit alten Schlüssel entschlüsselt und mit neuen Aktenschlüssel wieder verschlüsselt
- Dokumente Dokumentenschlüssel bleiben gleich

## FAZIT

- keine Daten an den Komponenten im Klartext gespeichert
- Aktenschlüssel liegt nur im Client und nur temporär im Klartext vor
- Aufteilung des Schlüsselmaterials gegen Missbrauch



# THANKS

[falk-m.de](https://falk-m.de)

[print view](#)

