## Präambel

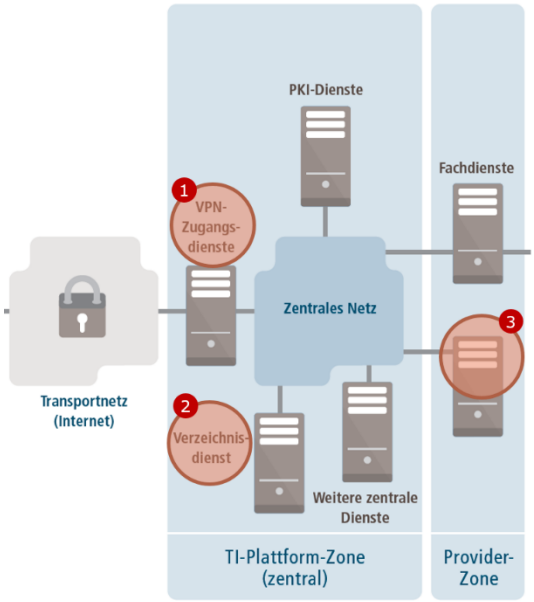
Die Telematikinfrastruktur ist die technische und organisatorische Informations-, Kommunikations- und Sicherheitsinfrastruktur des deutschen Gesundheitssystems. Sie vernetzt alle Akteure und Institutionen miteinander und ermöglicht dadurch einen sicheren und leistungsfähigen Datenaustausch untereinander.

Zur Stärkung der Ende-zu-Ende-Sicherheit der Telematikinfrastruktur (TI) und des öffentlichen Vertrauens haben unabhängige und neutrale Sicherheitsexperten eine sogenannte 360-Grad-Sicherheitsanalyse durchgeführt: Die gematik hatte hierfür mit SEQRED S. A. und SEC Consult Unternehmensberatung GmbH zwei international anerkannte Unternehmen im Bereich Cyber- und Applikationssicherheit beauftragt.

Die Prüfer versuchten, mit verschiedenen Methoden mögliche Schwachstellen aufzudecken. Die Widerstandskraft der TI und der gematik gegenüber Angriffen, das erfolgreiche Erkennen dieser Angriffe und eine zeitnahe zielgerichtete Reaktion standen bei dieser Sicherheitsanalyse im Fokus.

## Gegenstand der 360-Grad-Sicherheitsanalyse

Die folgende Abbildung stellt einen Überblick über die ausgewählten und zu prüfenden Angriffsziele im Rahmen der 360-Grad-Sicherheitsanalyse dar.




**Security Assessment**

PKI-Managementsystem

**Penetrationstests**

1. VPN-Zugangsdienst
2. Verzeichnisdienst

**Source Code Analyse**

3. Signaturdienst

**Red Team Testing**

Organisatorische Verwundbarkeit

Technische Schwachstellen

SEQRED hat die Sicherheitsbewertung (Security Assessment) für das PKI-Managementsystem durchgeführt; mit Public-Key-Infrastruktur (PKI) wird in der Kryptologie ein System bezeichnet, das digitale Zertifikate ausstellen, verteilen und prüfen kann. Im Mittelpunkt der Analyse stand die Rezension von Architektur, Konfiguration und dem sog. Assume Breach. Das „Assume-Breach-Paradigma" geht davon aus, dass trotz aufwendiger Sicherheitsvorkehrungen im Bereich der IT jedes Unternehmen einmal Opfer einer Cyber-Attacke wird.

Darüber hinaus wurden von SEQRED die Penetrationstests des Verzeichnisdienstes – sozusagen dem zentralen „Adressbuch" in der Telematikinfrastruktur – und der VPN-Zugangsdienste in Form von Black-Box-Tests durchgeführt: Für die Teilnahme in der Telematikinfrastruktur benötigen die Akteure einen dafür speziell zugelassenen

Zugangsdienst eines externen Anbieters und nutzen diesen über die verschlüsselte Verbindung eines virtuellen privaten Netzwerks (VPN). Der Black-Box-Test beschreibt eine Softwaretestmethode, bei der Tests anhand der bloßen Spezifikation entwickelt werden. Die Prüfer entwickeln hierbei also Tests, ohne die innere Funktionsweise des zu testenden Systems zu kennen.

SEC Consult hat eine teilweise Überprüfung der Quellcodes (partielles Source Code Review) des Signaturdienstes durchgeführt sowie ein Assessment – also eine Einschätzung – des zugrundeliegenden Software-Entwicklungsprozesses inklusive des Betriebs, basierend auf OWASP SAMM v2[1]. Zusätzlich war SEC Consult auch für die sog. Red Team Testings der gematik zuständig. Hierbei versetzen sich IT-Sicherheitsexperten in die Rolle eines tatsächlichen Hackers und versuchen, beispielsweise an sensible Daten eines Unternehmens heranzukommen.

## Prüfergebnisse

### Security Assessment des PKI-Managementsystems

Die beauftragten Prüfer haben keine kritischen Sicherheitsprobleme identifiziert, bei denen das PKI-Managementsystem den direkten Angriffen ausgesetzt sein könnte.

Wörtlich kam SEQRED zusammenfassend zu dem Ergebnis: *„Seqred consultants did not identify any critical security issues, which may expose PKI System to the direct attacks.*"

Es wurde allerdings festgestellt, dass in einigen Bereichen Abweichungen gegenüber Best Practices bestehen, die von dem Anbieter behandelt werden müssen, aber aus Sicht der Prüfer einem produktiven Einsatz nicht im Wege stehen.

### Penetrationstests des Verzeichnisdienstes und der VPN-Zugangsdienste

Der Test zeigte keine sicherheitskritischen Schwachstellen. In Anbetracht der im Verlauf der Tests festgestellten Schwachstellen und Fehler kam SEQRED zu dem Schluss: *„… that the security status of the application is at a high level.*" D. h. die Prüfer stuften den Sicherheitsstatus der Anwendungen auf einem hohen Niveau ein.

- Die spezifizierten Anforderungen der gematik werden durch die externen Anbieter überwiegend eingehalten, und es wurden keine schwerwiegenden Schwachstellen gefunden.
- Die Prüfer konnten auf keinem der getesteten Server eine Codeausführung erreichen. Es wurden lediglich geringfügige Konfigurationsprobleme festgestellt, die die Telematikinfrastruktur jedoch keinen direkten Angriffen aussetzt.

### Source Code Review des Signaturdienstes

SEC Consult stellt in seinem Review fest: *„Das Code Review identifizierte mehrere Schwachstellen im Rahmen des beauftragten Zeitraums vom 28.9.2020 bis 14.10.2020.*" Unter anderem wurde eine kritische Schwachstelle identifiziert, die es einem Angreifer erlaubt hätte, die Authentifizierung des Signaturdienstes zu umgehen. Diese Schwachstelle

[1] Das „Software Assurance Maturity Model" (OWASP SAMM) - hier in der Version 2 – ist ein Rahmenwerk des „Open Web Application Security Project (OWASP)", mit dem Unternehmen nicht nur den Reifegrad ihrer Softwareentwicklungsprozesse hinsichtlich der Sicherheit messen, sondern sie auch schrittweise verbessern können.

wurde umgehend vom Anbieter behoben, und die gesetzten Maßnahmen wurden danach von SEC Consult erneut geprüft und als tauglich bewertet.

- Das Assessment nach OWASP SAMM v2 ergab in den meisten analysierten Bereichen einen angemessenen Prozess-Reifegrad. SEC Consult kommt dabei zu der Bewertung: *„Auf der Reifegrad-Skala von 0 bis 3 erreicht der dem Signaturdienst zugrundeliegende Entwicklungsprozess einen Gesamt-Reifegrad von 2,35*."
- Wesentliche Stärken wurden in den Bereichen Governance (Führung), Design und Betrieb deutlich. Durch die sehr strengen Vorgaben der gematik in Bezug auf Sicherheitsanforderungen und Sicherheitsarchitektur sowie der regelmäßigen Gutachten und Audits durch unabhängige Dritte wird ein hohes Niveau des Prozessreifegrades in Bezug auf die Spezifikation relevanter Vorgaben sowie deren Überprüfung erreicht.

**Fazit**

Die 360-Grad-Sicherheitsanalyse hat die Erwartung der gematik erfüllt und die Ende-zu-Ende-Sicherheit der Telematikinfrastruktur grundsätzlich bestätigt. Für identifizierte Schwachstellen wurden in Abstimmung mit den Anbietern Maßnahmen zur umgehenden bzw. zeitnahen Bereinigung vereinbart und bereits teilweise bereits umgesetzt.

Die Telematikinfrastruktur erlebt derzeit bedeutende Veränderungen. Die ersten medizinischen Anwendungen werden bundesweit eingeführt. Die gematik wird auch 2021 wieder eine 360-Grad-Sicherheitsanalyse mit dem Untersuchungsschwerpunkt elektronische Patientenakte beauftragen und über die Ergebnisse informieren.

Die Untersuchung der elektronischen Patientenakte umfasst dabei auch den Schlüsselgenerierungsdienst. Dieser wurde in der Entwicklungsphase zunächst auf der Ebene der Spezifikationen wissenschaftlich untersucht. Die gematik hat hierzu bereits das Gutachten der TU Graz veröffentlicht. Die Analysen in diesem Jahr werden neben der Überprüfung der korrekten Implementierung auch die theoretische Analyse zur kryptographischen Sicherheit der zugrundeliegenden Sicherheitsprotokolle (des Schlüsselgenerierungsdienstes und der Vertrauenswürdigen Ausführungsumgebung) einschließen.