# Germany Is Rolling Out Nation-Scale Key Escrow And Nobody Is Talking About It

Jan Sebastian Götte[1]

Technical University of Darmstadt, Darmstadt, Germany, research@jaseg.de

**Abstract.** Germany is currently rolling out an opt-out, nation-scale database of the medical records of the majority of its population, with low-income people being disproportionally represented among its users. While there has been considerable criticism of the system coming from civil society, independent academic analysis of the system by the cryptography and information security community has been largely absent. In this paper, we aim to raise awareness of the system's existence and, based on the system's public specifications, highlight several concerning cryptographic engineering decisions. Our core observations is that the system's most sensitive long-term user keys are derived by a rudimentary, home-grown centralized key escrow mechanism. This mechanism relies on a per-use salt and only 256 bit of entropy, shared globally across millions of users. Furthermore, the system's specification mandates only level 3 compliance with the obsolete FIPS 140-2 security standard, which requires "hard, opaque potting", but lacks active tamper sensing. As a result, the system remains vulnerable to attacks by nation states and other well-funded adversaries.

**Keywords:** Physical Security· Tamper Resistance· Hardware Security Module (HSM)· Cryptography· Governance· Healthcare

## 1 Introduction

Beginning May 2025, after several delays, Germany has started the nation-scale rollout of its new electronic medical record system. The system aims to create a national database accessible to all healthcare providers that holds the complete electronic medical records of all publically insured people living in Germany. The system aims to replace paper-based workflows that are error-prone and lead to healthcare providers often only having access to a subset of patient's medical records. Data in scope for the system includes medical letters, laboratory results, and medical imaging files.

Due to Germany's mandatory health insurance laws, the system's user base encompasses the majority of all German residents. People who have replaced their public health insurance with private insurance as of now are not subject to the system. In Germany, by law private health insurance is only available to people from the top 10th percentile of household income. This means that the system disproportionally affects people who have low income, creating an equity

issue. While it is possible to opt out from the use of the system, the process of opting out is difficult. Additionally, the government and health insurance providers have publically depicted the system in a one-sidedly positive way, meaning that it is unlikely the majority of people subject to the system have a comprehensive understanding of the system's benefits and risks that would be necessary for an informed decision.

While there has been loud criticism of the system's security from civil society organizations such as digital rights nonprofit organization Chaos Computer Club (CCC) [16] and several severe security flaws have been demonstrated practically, this criticism has largely been ignored by the political structures in charge. We observe that despite this civil society outrage and the system's large scale, it has received little attention from the academic cryptography and information security community.

In this paper, we aim to point out some perplexing cryptographic engineering decisions in the system. In particular, we point out that the system's core per-user secrets are kept in a rudimentary key escrow system whose security is based on engineering assumptions, not on cryptographic principles. Furthermore, we observe that by specification, the individual user keys of the system are derived from a per-user cleartext salt based on a system-wide long-term secret with only 256 bits of entropy[1]. Finally, we note that according to specification, the only physical security requirement for the protection of this highly sensitive secret is a "hard, opaque potting material", with no tamper detection and response required.

We base our analysis on the system's publicly available standards in their latest version as of the writing of this paper in April 2025, describing version 3.0 of the healthcare record system [9, 11]. We note that the implementation might well deviate from these standards and be more secure–however, with the system's history of flaws, we believe this is unlikely to be the case. The reference implementation provided by the specification authority [13] follows the specified minimum requirements closely. As of now, there is no meaningful way for either the public or for researchers such as us to ascertain the concrete implementation security of the system.

## 2 The Design of ePA

ePA (short for *elektronische Patientenakte*, "electronic patient record"), is embedded into Germany's national public healthcare backend system "Telematikinfrastruktur" (TI). TI is a highly complex system, and a detailed description would exceed the limits of this paper. Briefly put, TI consists of a shared DMZ that parties like insurance providers and healthcare providers connect to through

[1] In previous versions of the standard [10, 12], there were two escrow services, with both keys used in layers to reduce the risk of a compromise of either one. The current standard only requires one escrow service, and drops the entropy requirement of the root keys from 512 bits to 256 bits. The apparent reason for the long-term nature of these keys is that they are updated manually.

a VPN. At the client location, usually an individual doctor's office or a hospital, this VPN connection is terminated by a specialized VPN appliance named "Konnektor" that simultaneously acts as a trusted component inside the client network hosting some software for purposes such as authentication. The Konnektor contains several smart cards that store keys used for authentication. Konnektor devices are offered by several vendors and healthcare providers like doctor's offices are indivudally responsible for purchasing and maintaining a Konnektor.

Every person enrolled in the system as well as every healthcare professional providing services under it is issued an ID card that contains a smart card that contains keys used to authenticate towards the central infrastructure. The primary use of these smart cards up to now is that when someone visits a healthcare provider, they will insert their ID card into a terminal so the healthcare provider can automatically fetch their personal information such as name, birth date, address and enrollment status from their insurance provider.

ePA is implemented inside the TI system. Its centralized services are accessed by healthcare providers through the TI's VPN. Patient records are encrypted and decrypted inside TI's backend systems. Smart cards authenticate parties and hardware devices to each other. Each insurance provider picks one of several implementations of ePA's server-side infrastructure to run for its clients. Currently, there are two approved implementations of this server-side infrastructure.

With the current version of the specificatoin, the overall architecture of ePA heavily relies on Trusted Execution Environments (TEEs). Data processing on the server side is done in plaintext inside TEEs, with some cryptographic key management delegated to a Hardware Security Module. While attacks on the TEEs are considered in the system, the HSMs are assumed to be perfectly secure, and the system does not include mitigations for a compromised HSM. The primary motivation for plaintext processing seems to be to enable large-scale data analysis for research purposes without requiring consent or cooperation of the people whose records are being processed.

The primary services offered by the server side are authentication services, key escrow, and a database storing the encrypted records themselves. Records are symmetrically encrypted with keys that are derived from system-wide secrets inside an HSM. The primary motivation behind the use of a key escrow service seems to be to enable the creation of a duplicate patient ID smartcard in case a person looses theirs. While the current version of the standard is unclear on the exact mechanism of key derivation, in previous versions of the standard, the escrow service's root key, a random salt, and the healthcare ID number of the person owning the record was used in SHA256-HKDF. The specification requires that a new root key is generated once a year, but as far as we can tell, record key rollover is not done automatically but is only meant to be done when the *user* requests it, and old root keys must be retained forever to ensure old records can be accessed.

## 3 Related Work

The state-owned company specifying the system commissioned several security assessments of the system relating to the key escrow service. Fischlin [7] focuses on the cryptographic dimension of the key escrow service used in an older version of the standard, and is now obsolete. Slany [18] approaches the system at a higher level, and focuses on the cryptography of the inner protocol layers spoken between the system's components. Industry research organization Fraunhofer SIT was comissioned for a structured, theoretical assessment of attack paths to the system [8]. We are not currently aware of independent academic security research on the system.

The design and operation of the system have been independently described in detail by civil society activists, who have demonstrated several successful attacks on the system. Tschirsich, Brodowski, and Zilch [19] demonstrated how they could trivially acquire each of the smartcards as well as the Konnektor necessary for accessing the system. Tschirsich and Kastl [20] summarize the history of attacks demonstrated on the system and show multiple practical attacks on various parts of the system's implementation.

## 4 Concerning Cryptographic Engineering Choices

In this paper, we aim to highlight some of the design choices in the system that we believe stray from current best practice. This is by no means an exhaustive list, and is only meant to underscore why we believe the system deserves more scrutiny.

### 4.1 Use of Key Escrow

First, the system's general approach of using a key escrow service instead of securely storing the keys inside the system's already existing smart card infrastructure is concerning, given that this key escrow service poses a centralized security risk. The system's designers made this decision since it was deemed important that access to an encrypted record can be restored quickly after an insurance ID card is lost, without requiring the cooperation of the healthcare providers holding the primary copies of the person's medical records.

While key escrow services have been a topic of political debate in decades past, in the cryptographic community, consensus generally is that they are a bad idea since they pose a centralized target for attack, and increase attack surface [3, 4, 5].

### 4.2 Cryptographic Design

The system's overall cryptographic design is intentionally kept simple. The standard explicitly mentions that symmetric primitives have been preferred over asymmetric primitives in the core key escrow functions due to the risk of an

attack on asymmetric primitives in the long term. Notably, other advanced cryptographic techniques such as secret sharing schemes, oblivious pseudo-random functions, or multiparty computation that could help with the security and privacy of the key escrow service by reducing trust placed in any single component of the service are also absent while the system relies extensively on the engineering-based security guarantees of TEEs and HSMs. Given that the ePA system trusts its HSMs as unconditionally secure, it is unclear what purpose the manual yearly root key renewal serves, especially absent an automatic way to roll over the wrapped record keys.

A consequence of the systems' simple cryptographic design is that the system trusts its components to a large degree. For instance, the system leaks a person's insurance ID number to the key escrow HSM every time record keys are requested. Along with the timing and frequency of these requests, this leaks information on the person's condition to the key escrow service in an identifiable way.

### 4.3 A Realistic Attacker Model

We observe that the system as a whole does not appear to be designed to defend against well-resourced adversaries. The series of practical attacks that have been demonstrated on the system confirm this impression. In Tschirsich and Kastl [20] summarize a series of successful attacks. Attacks include social engineering resulting in access to copies of smartcards enabling accessing patient records, using misconfigured Konnektor VPN appliances with their LAN DMZ and authentication interface exposed on the public internet, circumventing video-based authentication processes resulting in duplicate file keys being provided, classis SQL injection on a backend service maintaining an authentication database, accessing all national patient records through brute-force enumeration of weak identifiers, and several more.

We believe that a system like this must be designed to withstand well-resourced adversaries such as enemy secret services, since the medical data stored in such as information on chronic illness, sexually transmittable disease or severe food allergies has intelligence value. Repeated breaches of national digital infrastructure such as the 2015 breach of the US Office of Personnel Management [6] or the 2024 compromise of US telecommunications wiretapping systems [17] demonstrate that such state-sponsored attacks on national digital infrastructure are a realistic concern. A possible scenario in the ePA system would be an enemy secret service gaining access to one of the HSMs storing the systems' root secrets, extracting the root secret by an advanced physical attack, then being able to decrypt captured encrypted health records at will. Similarly, a nation-state adversary might have access to an exploit allowing the compromise of the system's TEEs, which would enable the extraction of any patient records being processed in plaintext inside these TEEs.

### 4.4 Physical Security

Physical security has received some consideration in the system's specification. First, smart cards are used extensively for authentication. Second, Hardware Security Modules are used in key locations of the system to process some cryptographic secrets. The core of the system's key escrow service is implemented inside an HSM. However, it is notable that the actual security level required for this HSM is only FIPS 140-2 level 3 [1]. Not only has FIPS 140-2 been superseded by FIPS 140-3 since 2019 [2], its security level 3 mostly provides logical separation of cryptographic functions from other logic and is not very meaningful in the context of physical attacks. The only physical requirement of FIPS 140-2 level 3 is that the HSM has a hard, opaque coating. This coating is specified to be tamper-evident, but notably no active tamper detection or response features are required by this standard. In contrast to the newer FIPS 140-3 standard and the related ISO/IEC 19790 [14] as well as ISO/IEC 24759 [15] standards, FIPS 140-2 does not make any particular requirements regarding resistance to side-channel attacks. The lack of tamper response, unspecified resistance to side-channel attacks and the fact that the ePA specification only requires the long-lived key escrow root key inside the HSM to have 256 bits of entropy lead to an unsatisfactory overall constellation.

## 5 Conclusion

In conclusion, we observe that in Germany's ePA national medical record database, despite the decade-long standardization and implementation process, several cryptographic compromises ended up in the system's final deployment. Even assuming that nation-scale key escrow is a good idea, the implementation of this key escrow system seems to stray from current best practice. The system uses a secret key with only 256 bits of entropy to derive highly sensitive secret keys for potentially tens of millions of people sharing an insurance provider. The cryptographic design of this escrow system is unsophisticated, ignoring the past three decades in cryptographic developments particularly in multiparty computation (MPC) and other secret sharing techniques in favor of an engineering approach. In the engineering dimension, the system's physical security is only held to the basic level 3 of the obsolete FIPS 140-2 standard, which is considerably less secure than an average credit card payment terminal. The system's root keys are only protected by a "hard, opaque potting material" and no tamper detection and response is required. We estimate that the system poses an attractive and soft target to nation-state adversaries. The system's shortcomings are made more severe by the fact that the system disproportionally affects the lives of people with low income.

## References


1. (US) National Institute of Standards and Technology, Security Requirements for Cryptographic Modules, U.S. Department of Commerce. (2002). https://csrc.nist.gov/pubs/fips/140-2/upd2/final (visited on 04/08/2025). https://doi.org/10.6028/NIST.FIPS.140-2
2. (US) National Institute of Standards and Technology, Security Requirements for Cryptographic Modules, U.S. Department of Commerce. (2019). https://csrc.nist.gov/pubs/fips/140-3/final (visited on 05/15/2025). https://doi.org/10.6028/NIST.FIPS.140-3
3. Abelson, H., Anderson, R., Bellovin, S.M., Benalob, J., Blaze, M., Diffie, W., Gilmore, J., Neumann, P.G., Rivest, R.L., Schiller, J.I., Schneier, B.: The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption. World Wide Web J. **2**(3), 241–257 (1997)
4. Abelson, H., Anderson, R., Bellovin, S.M., Benaloh, J., Blaze, M., Diffie, W.", Gilmore, J., Green, M., Landau, S., Neumann, P.G., Rivest, R.L., Schiller, J.I., Schneier, B., Specter, M.A., Weitzner, D.J.: Keys under Doormats. Commun. ACM **58**(10), 24–26 (2015). https://doi.org/10.1145/2814825
5. Anderson, R.: Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley (2020)
6. Barrett, D., Yadron, D., Paletta, D.: U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say, Wall Street Journal. (2015). http://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888 (visited on 05/15/2025)
7. Fischlin, M.: Kryptographische Analyse Spezifikation Schlüsselgenerierungsdienst ePA, Technische Universität Darmstadt. (2021). https://www.gematik.de/media/erezept/SGD_Analyse_2021.pdf (visited on 05/15/2025)
8. Fraunhofer SIT, Abschlussbericht Sicherheitsanalyse Des Gesamtsystems ePA Für Alle, (2024). https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Abschlussbericht_Sicherheitsanalyse_ePA_fuer_alle_Fraunhofer_SIT.pdf (visited on 05/16/2025)
9. gematik, Spezifikation Aktensystem ePA für alle v1.4.1, (2025). https://gemspec.gematik.de/docs/gemSpec/gemSpec_Aktensystem_ePAfueralle/latest/ (visited on 05/16/2025)
10. gematik, Spezifikation Schlüsselgenerierungsdienst ePA v1.6.0, (2023). https://gemspec.gematik.de/downloads/gemSpec/gemSpec_SGD_ePA/gemSpec_SGD_ePA_V1.6.0.pdf (visited on 05/26/2025)
11. gematik, Übergreifende Spezifikation Verwendung Kryptographischer Algorithmen in Der Telematikinfrastruktur v2.28.1, (2024). https://gemspec.gematik.de/downloads/gemSpec/gemSpec_Krypt/gemSpec_Krypt_V2.28.1.html (visited on 05/16/2025)
12. gematik, Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur v2.40.0, (2025). https://gemspec.gematik.de/downloads/gemSpec/gemSpec_Krypt/gemSpec_Krypt_V2.40.0.pdf
13. Github Repository: eRP-FD/Vau-Hsm, https://github.com/eRP-FD/vau-hsm/tree/master (visited on 05/16/2025)
14. ISO/IEC 19790:2025, ISO. https://www.iso.org/standard/82423.html (visited on 05/15/2025)
15. ISO/IEC 24759:2025, ISO. https://www.iso.org/standard/82424.html (visited on 04/08/2025)

16. Koch, M.-C.: More and More Experts Warn against Electronic Patient Records, heise online. (2025). https://www.heise.de/en/news/More-and-more-experts-warn-against-electronic-patient-records-10235907.html (visited on 05/26/2025)
17. Menn, J.: Chinese Government Hackers Penetrate U.S. Internet Providers to Spy, The Washington Post. (2024). https://www.washingtonpost.com/technology/2024/08/27/chinese-government-hackers-penetrate-us-internet-providers-spy/ (visited on 05/15/2025)
18. Slany, W.: Sicherheitsanalyse zur Sicherheit der kritischen Komponenten der elektronischen Patientenakte nach §291a SGB V, (2020). https://www.gematik.de/media/gematik/Medien/Newsroom/Presse/Dokumente/Sicherheitsanalyse_TU_Graz_zur_ePA_mit_Vorwort_der_gematik.pdf (visited on 05/15/2025)
19. Tschirsich, M., Brodowski, c.-D.m.C., Zilch, D.A.: "Hacker Hin Oder Her": Die Elektronische Patientenakte Kommt!, (01:00:00 +0100). https://media.ccc.de/v/36c3-10595-hacker_hin_oder_her_die_elektronische_patientenakte_kommt (visited on 05/15/2025)
20. Tschirsich, M., Kastl, B.: „Konnte Bisher Noch Nie Gehackt Werden“: Die Elektronische Patientenakte Kommt - Jetzt Für Alle!, (00:00:00 +0100). https://media.ccc.de/v/38c3-konnte-bisher-noch-nie-gehackt-werden-die-elektronische-patientenakte-kommt-jetzt-fr-alle (visited on 05/15/2025)