sPACE Attack: Spoofing eID's Password Authenticated Connection Establishment

A Critical Man-in-the-Middle Vulnerability in the German eID Scheme

The objective of this document is to highlight a vulnerability within the eID scheme ("Online-Ausweis-Funktion" [1]) of the German National Identity Card. This vulnerability compromises the hardware security, enabling an attacker to effectively carry out scalable Man-In-The-Middle attacks. The attack does not require remote code execution, physical access, or similar approaches and can be executed through apps uploaded to the official app stores. Such attacks compromise access to services that rely on eID security, including government services, eHealth platforms, and banking systems. Additionally, the attacker can extract the personal data stored in the eID. This attack requires no special privileges and can be executed remotely. Due to the nature of the vulnerability as a design flaw, implementing countermeasures may prove challenging or impractical. The vulnerability has the CVE ID CVE-2024-23674 and a CVSS rating of 9.7 (Critical).

A responsible disclosure process was conducted with the BSI (Bundesamt für Sicherheit in der Informationstechnik), during which the BSI acknowledged the presence of the vulnerability. Their defense centers on the user's responsibility for maintaining the security of their client devices. However, users typically exhibit poor security practices. In addition, this paper demonstrates that the attack remains successful even when all BSI recommendations are followed and client devices are updated.

I. INTRODUCTION

The German eID scheme, commonly referred to as the "Online-Ausweis-Funktion," is a digital identity system provided by the German government. Integrated as a component of the German National Identity Card, this functionality enables secure and user-friendly online authentication processes, as well as the generation of digital signatures for citizens.

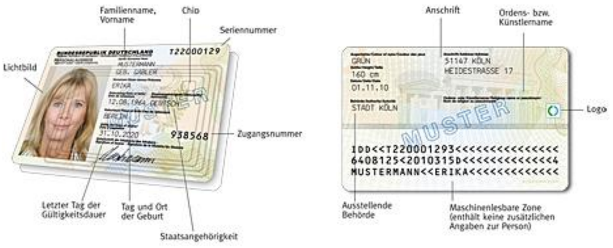


FIG. 1. The German National Identity Card

The German eID scheme consists of several integral components, each playing a distinctive role in ensuring secure digital identity verification. The key components are outlined below:

1. **National Identity Card (Personalausweis)**: Issued to German citizens, this physical identity card incorporates a contactless chip that securely stores personal information and cryptographic keys.

2. **eID (Online-Ausweis-Funktion)**: Embedded in the identity card's chip, the eID scheme facilitates online authentication and electronic signatures.

3. **Contactless Cryptographic Chip**: Secured against various types of attacks and certified at the highest security levels, this chip enables the Online-Ausweis-Funktion and can be accessed remotely using NFC technology.

4. **Secure PIN**: Citizens require a personal 6-digit PIN to access the Online-Ausweis-Funktion, serving as a

critical element in authenticating the cardholder.

5. **Reader Devices / Terminals**: These devices, categorized into security levels (”Basic Reader (Cat-B),” ”Standard Reader (Cat-S),” ”Comfort Reader (Cat-K)”), facilitate user interaction with the chip. Security levels vary, with Basic Readers lacking a separate PIN pad, while Standard and Comfort Readers feature dedicated PIN pads.

6. **eID Client**: The client application, such as the official AusweisApp [2], facilitates communication with the identity card. Typically, the eID client operates on the smartphone of the citizens.

7. **eID Server**: Responsible for reading data from the identity card, the server engages in mutual authentication with the chip. Access to the chip requires an ”Authorization Certificate” (”Berechtigungszertifikat”), as specified in the technical guideline BSI TR-03130 [3]. The eID server provides a web service endpoint for communication with the eID client, utilizing SOAP/PAOS messages known as the eCard API Framework (BSI TR-03112 [4]).

8. **Service Provider**: Organizations (e.g. an insurance) offering online services (e.g. electronic patient records / ePA) that necessitate identity verification interact with the eID system to authenticate citizens securely. Service Providers are identified through the authorization certificate. The German government maintains an official list of issued Authorization Certificates [5].

9. **Password Authenticated Connection Establishment (PACE)**: The PACE protocol is a security mechanism utilized in the eID scheme of the German National Identity Card. PACE is designed to secure the communication between the eID card and the local device utilizing the Secure PIN of the citizen. It ensures the confidentiality and integrity of the data exchanged.

10. **Application Protocol Data Unit (APDU)**: Defined by ISO/IEC 7816-4 [6], APDUs serve as the message format for communication with the smart card, facilitating the exchange of information.

The system is designed to be versatile and secure, allowing users to access various online services, including government portals, tax filing, health services, insurances, banking, and e-commerce platforms.

II. BACKGROUND

[**Hardware Security**] At the heart of the German eID scheme is a state-of-the-art chip designed according to the highest standards of hardware security. This secure element, integrated directly into the identity card, serves as the hardware factor for digital identity and cryptographic operations. The chip is equipped with security features that provide resilience against a spectrum of potential threats. The chip facilitates secure communication through the implementation of standardized protocols (”General Authentication Protocol”), using the Application Protocol Data Unit (APDU) format for secure data exchange between the card and the eID server.

The architectural overview of the eID system is explained in the ”German eID Whitepaper” [7]. One important aspect is the mutual authentication between the eID server and the chip. This essential security measure ensures an end-to-end encrypted channel to access the eID function:

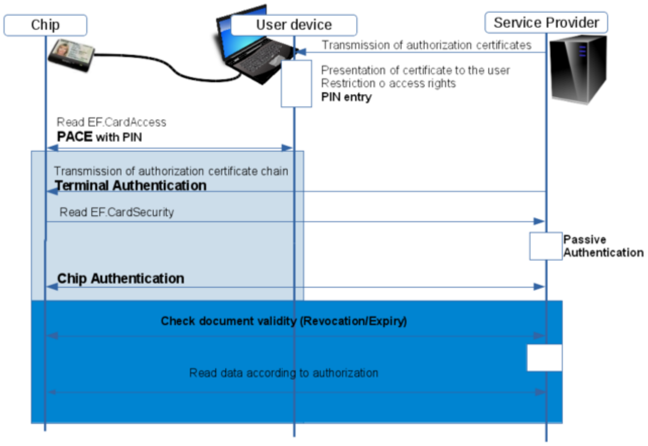

Chip
User device
Service Provider
Transmission of authorization certificates
Presentation of certificate to the user
Restriction o access rights
PIN entry
Read EF.CardAccess
PACE with PIN
Transmission of authorization certificate chain
Terminal Authentication
Read EF.CardSecurity
Passive Authentication
Chip Authentication
Check document validity (Revocation/Expiry)
Read data according to authorization

FIG. 2. Authentication mechanism

The architectural framework for the German eID is also illustrated in the ”German eID LoA Mapping” document [8]:

”The corresponding private keys are securely stored on the chip of the eID card (German ID card, residence permit or eID card for Union citizens) of the card holder. As part of the cryptographic protocols, a corresponding PIN of the card holder is required to unlock the chip of the eID card. Consequently, the German eID utilises two authentication factors from the different authentication factor categories “possession” (eID card) and “knowledge” (PIN).”

”The authentication mechanism of the German eID is based on a mutually authenticated and end-to-end-protected channel between the service provider and the chip of the eID card via a sequence of cryptographic protocols. This protects against attacks such as Man-in-the-Middle.”

”The PACE protocol verifies the PIN entered by the user and establishes a secure messaging channel (i.e. an encrypted and authenticated channel) with strong session keys between the card holder's local device (e.g. computer or card reader) and the chip of the German eID."

[**Reader Levels**] The German eID system specifies different levels of readers, as outlined in BSI TR-03119 [9]:

1. **Basic Reader (Cat-B)**: Basic Readers (Cat-B) are suitable for home use and are typically integrated devices like smartphones or notebooks. Unlike other categories, the basic reader does not necessitate a "PIN pad (secure PIN entry) with PACE support." It is commonly utilized in low-security scenarios such as "age verification," "eTicketing," and "Internet shopping" (refer to BSI TR-03119 [9]).

2. **Standard Reader (Cat-S)**: Standard Readers (Cat-S) are physical smart card readers equipped with a PIN pad to ensure secure PIN entry. Designed as the "eID function on the Internet with increased security requirements" this category enhances security for various online interactions.

3. **Comfort Reader (Cat-K)**: The Comfort Reader is equipped with a PIN pad for secure PIN input and a display featuring 2 x 16 alpha-numeric characters. This category supports all functions of the eID card, including the qualified electronic signature.

According to BSI TR-03119 [9]: "Whereas the Basic Readers constitute the inexpensive variant, used especially for applications with limited security level dedicated to home users, the Standard and Comfort Reader devices are, in addition, construed for applications with extended security functions in terms of both function and safety."

The Standard Readers (see FIG. 3) Comfort Readers are physical devices connected via USB, which can pose challenges in terms of usability and cost. An example of such a device is the "cyberJack RFID standard (USB)" manufactured by REINER (refer to [10]).

The original design choice of the eID scheme appears robust in terms of security, suggesting the use of basic readers for low-security situations and standard or comfort readers for scenarios demanding substantial or high security. However, the challenge arises due to the lack of market adoption for physical readers. In practice, most German citizens rely on their smartphones to interact with the eID card, either directly when using the eID on the smartphone or as a reader for the AusweisApp on a laptop. Therefore, in practical terms, only basic readers are left today.

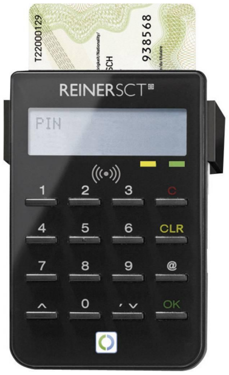


FIG. 3. Standard Reader: cyberJack RFID standard (USB)

III. THE VULNERABILITY

The design flaw in the German eID scheme manifests in two aspects: a) the insufficient decoupling of the two authentication factors (physical possession and knowledge/PIN), enabling an attacker to compromise both factors simultaneously, and b) the absence of mechanisms validating the endpoints between the eID server and the user's eID client, thereby leaving room for Man-in-the-Middle (MITM) attacks through spoofing.

The identified actors in this attack scenario include:

1. **Victim ("Alice")**: Alice is a German citizen and wants to utilize her eID for accessing an online service ("Service Provider A"). Alice follows all recommendations provided by the BSI to ensure that her client device is updated and has antivirus installed.

2. **Attacker ("Mallory")**: Mallory is a remote attacker who seeks unauthorized access to an online service ("Service Provider B"), impersonating Alice.

3. **Service Provider A**: Legitimate German online services utilizing the eID for secure access, such as banks, insurance providers, and eGovernment services, which Alice intends to access.

4. **Service Provider B**: Legitimate German online services using the eID for secure access, but Mallory aims to gain unauthorized entry by exploiting the identified design flaw.

The normal workflow for Alice is as follows:

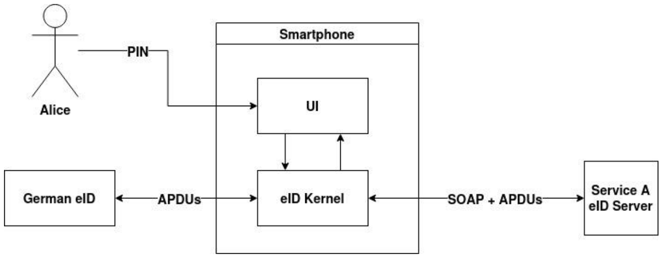


FIG. 4. Normal flow for the German eID

The details concerning the eID server have been omitted for the sake of simplicity.

Mallory's Man-in-the-Middle (MITM) attack would modify the flow as follows:

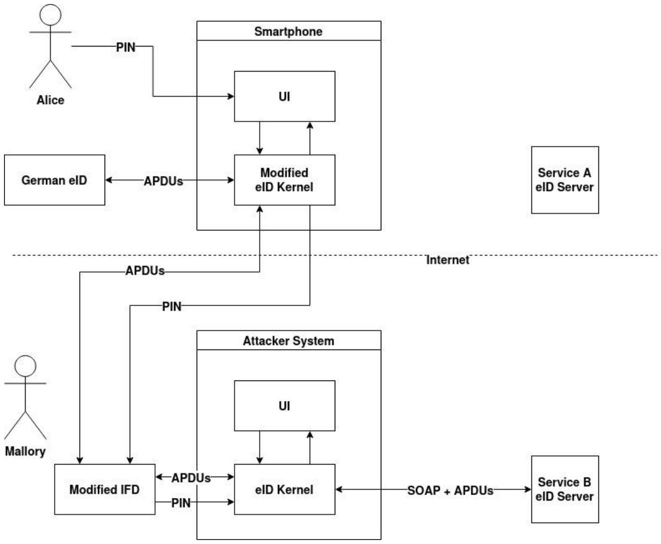


FIG. 5. MITM attack flow for the German eID

The attack involves placing a modified eID-Kernel on Alice's device, redirecting both the APDU and the PIN. Importantly, executing this operation does not require any special permissions on Alice's device, allowing for the manipulation of the Password Authenticated Connection Establishment (PACE) protocol in the eID, thereby coining the term "sPACE Attack" (Spoofing Password Authenticated Connection Establishment).

The attacks consists of the following steps:

1. **Preparation**: The attacker establishes a system (e.g. a server) capable of receiving incoming connections from Alice's client device.

2. **Placing the eID Kernel** The attacker either acquires or uses an authentic official app, then uploads an update that includes the modified eID kernel and enabled support for deeplinks from the eID system. This step does not require any special permissions or remote code execution. When Alice attempts to authenticate for Service Provider A, the app with the modified eID kernel is activated. It's important to emphasize that Alice has no possibility to prevent this, and the attack is effective even when the system is fully patched.

3. **Activation**: Upon Alice's initiation of identification for Service Provider A, a connection is established from Alice's device to Mallory's system. Once connected, Mallory starts identification for Service B. The eID server of Service Provider B initiates the General Authentication Protocol. Mallory intercepts this communication while placing the identification of Alice for Service Provider A on hold.

4. **APDU-Redirection**: The attacker redirects the APDU commands from Service Provider B to Alice's device, creating the illusion that the physical card is in the attacker's possession. This effectively compromises the first authentication factor, physical possession.

5. **PIN-Redirection**: Mallory intercepts the PIN on Alice's device through the modified eID-Kernel, transmitting it to the attacker's system. This action creates the appearance for Service Provider B that the PIN is in the attacker's possession, breaching the second authentication factor, knowledge. Mallory now gains access to Service Provider B in Alice's name.

6. **Finishing**: Mallory unpauses Alice's identification with Service Provider A. Alice seamlessly accesses Service A without reentering the PIN, preventing suspicion.

The outcome of the attack is that Alice successfully accesses Service Provider A without raising suspicion, while Mallory gains unauthorized access to Service Provider B in Alice's name. Importantly, Service Provider B lacks the means to detect the occurrence of the attack.

[**Why does the attack work?**] The German eID scheme lacks a secure PIN entry mechanism for basic readers, as highlighted in [9]. Considering that the physical chip is in proximity to the device where the PIN is entered, Mallory can exploit both the hardware factor (using APDU redirection) and the knowledge factor (by intercepting the PIN entry) in a single attack. Additionally, the eID system inadequately verifies the identity of the actors at both ends of the encrypted channel, allowing an attacker to impersonate Alice. Notably, the eID system lacks true end-to-end encryption, as the PIN entry occurs on an unsecured endpoint.

By deploying an update to an existing app or persuading Alice to install a malicious app from the app store, this attack can be carried out without requiring any specific permissions on Alice's device. This remains effective even if the user adheres to all of the BSI's security recommendations.

[**What is Spoofing?**] Spoofing refers to a technique in which an attacker masquerades as something it is not, often with the intention of tricking individuals, systems, or devices into believing it is authentic or trustworthy. This type of impersonation can take various forms, such as IP spoofing, email spoofing, or app spoofing. In the context of cybersecurity, spoofing attacks aim to manipulate the identity or origin of data, messages, or interactions, leading to potential security breaches or unauthorized access.

Within the context of this vulnerability, spoofing is employed as a means to deceive the eID server by making the Mallory's system appear as if it were Alice's client device. Additionally, spoofing is utilized to mislead Alice into downloading a seemingly legitimate app from the app store, which, in reality, contains malicious elements.

IV. ALTERNATIVE WAYS OF PLACING THE EID KERNEL

In addition to the methods described under step 2. above, the attacker can use additional methods to place the modified eID kernel on Alice's device:

[**2a. Phishing**] Likely the most scalable method for deploying the modified eID-Kernel is through simple phishing. In this scenario, the attacker aims to convince Alice to download an app containing the modified eID-Kernel. Two approaches are feasible:

1. **Malicious Version of Existing App**: The attacker creates a malicious version of an existing app already incorporating the eID-Kernel (e.g., AusweisApp, banking apps, etc.). The attacker downloads the original app, substitutes the eID-Kernel with a modified version, and re-uploads the altered app under their own app store account. Numerous instances exist where this method has gone undetected by the app store review process. Examples of such cases can be found in [11] and [12]. This approach requires no special permissions on the client device. In the PoC, a fake version of the official "AusweisApp" labeled "Ausweis Plus" has been created (see Figure 6).

   Furthermore, the official AusweisApp uses a custom URI scheme ("eid://") for deep linking, disregarding the recommended approach using universal links. This enables the attacker to deploy a malicious app that responds to deeplinks intended for the official app.

   The situation is further exacerbated by Europe's Digital Market Act (DMA), which will enable sideloading of apps (refer to [13]).

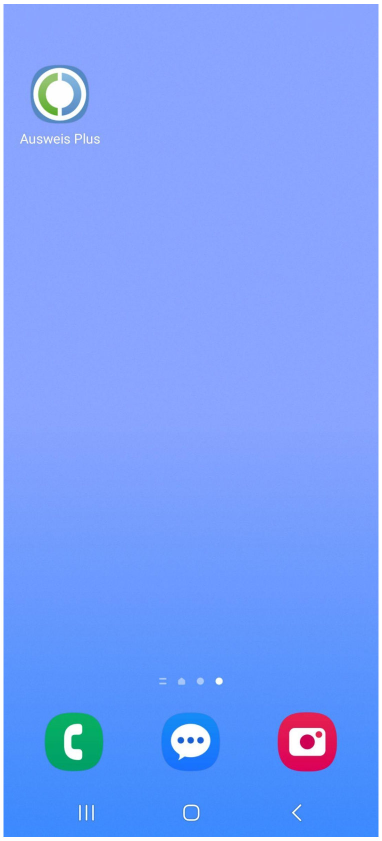


FIG. 6. Fake Ausweis Plus App

2. **Creation of a New App**: The attacker develops a new app and includes "eID Login" as part of its functionality. For instance, the attacker might create a new gambling app, requiring users to identify themselves using the eID for security reasons. Since this approach does not mimic any existing app, the likelihood of detection during the app store review process is minimal.

In both cases, Alice ends up with an app on her smartphone containing the modified eID-Kernel. For the execution of the PoC, the phishing approach involving a malicious version of AusweisApp has been used.

[**2b. Remote Exploit**] The next option, particularly suitable for targeted attacks directed at a specific individual (e.g., a politician), involves the attacker exploiting the client device directly. Various examples of such compromises, as detailed in [14] and [15], exist. The attacker possesses multiple options to await the next step:

1. The attacker may opt to wait in userspace until the eID client app is in operation, subsequently attaching

to the running process, akin to the methodology employed by tools such as Frida.

2. By altering the installed APK of the eID client app, the attacker can place the modified eID-Kernel.

3. Alternatively, the attacker may compromise the operating system itself, biding their time until the eID client app is initiated.

An illustrative example is the Pegasus malware (refer to [16]), renowned for its usage in targeting politicians, journalists, and other high-profile individuals. Such malware could be employed to specifically target the eID of exceptionally sensitive groups.

[**2c. Supply Chain Attack**] The final option available to the attacker involves executing a supply chain attack against one of the manufacturers of the eID client app. In this scenario, once the manufacturer is compromised, the build process for the app is altered to distribute the attacker's modified eID-Kernel. Successful instances of this method can be found in various examples, as outlined in [17] and [18]. Such an attack can compromise all users of that manufacturer at once.

V. PROOF OF CONCEPT

To validate the vulnerability, a proof of concept (PoC) of the attack has been successfully implemented. The PoC was utilized to execute a Man-in-the-Middle (MITM) attack against the author's own data. The PoC utilizes a customized version of the Governikus desktop software (refer to the source code [19]), featuring a modified IFD client responsible for receiving the compromised PIN and redirecting the APDUs as well as a modified eID kernel placed in the malicious app.

An overview of the steps involved is provided below:

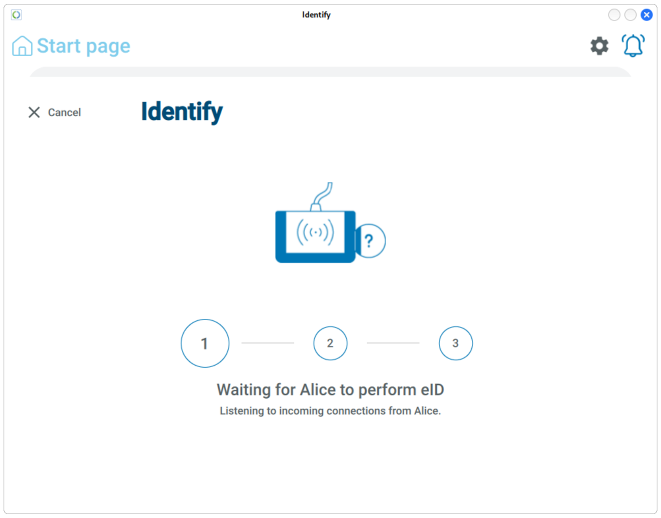
[**1. Preparation**] In the preparation phase, the attacker initiates a modified version of the Governikus desktop software. The software undergoes three critical modifications:

1. Introduction of a new command to receive the extracted PIN from the client device

2. Setting the PSK (Pre-Shared Key) to a fixed value

3. Launching the IFD mode at the start, awaiting an incoming connection from Alice.

Figure FIG. 7 shows the modified software in a waiting state for an incoming connection from Alice. The IFD connection is pre-configured with a static fingerprint/PSK, aligning with the certificate from Alice's client device.



Waiting for Alice to perform eID

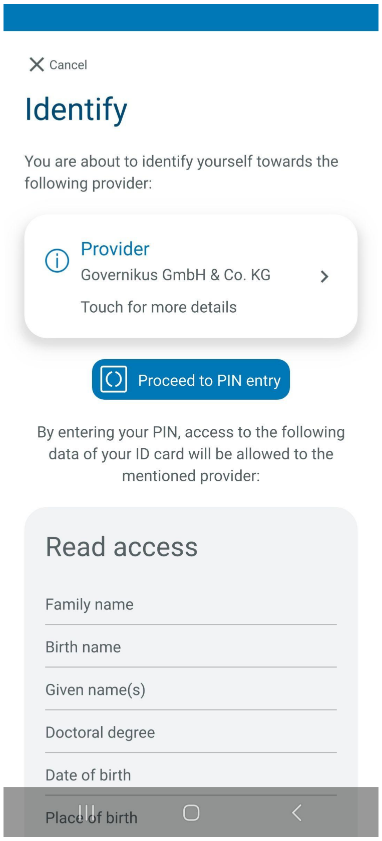
Listening to incoming connections from Alice.

FIG. 7. Waiting for Alice

[**2. Modified eID-Kernel**] The next step involves placing a modified eID-Kernel on Alice's device. The attacker either uses an existing app that is available in the official app store or acquires one that is for sale. In both cases apps with a high number of existing installations in Germany are preferable for the attacker. Subsequently, the attacker uploads an update to this app, including the modified eID kernel and a registration for the eid:// deeplinks.
Why does this method succeed? The German eID scheme employs a custom URI scheme for deeplinking ("eid://"). Despite being considered insecure and discouraged by Apple and Google, the BSI disregarded these security recommendations and opted to use this URI scheme. This choice allows for the interception of deeplinks on the mobile device, redirecting user interaction to the modified eID kernel.

[**3. Activation**] The attacker waits until Alice initiates an identification using the German eID. In this PoC Alice aims to retrieve the personal information from her eID ("See my personal data"). Once the identification process starts, the modified eID-Kernel on the client device is automatically activated. The modified eID client, featuring the same PSK as detailed in the "Preparation" phase, connects to the attacker's listening websocket. Detecting this connection, the attacker responds by initiating the eID identification for the targeted service ("Service Provider B") that they aim to access as Alice.

The modified app allows Alice to commence the standard identification process, including downloading the "Authorization Certificate" ("Berechtigungszertifikat") of Service Provider A. At this point, Alice encounters a screen indicating that she is connecting to Service


Cancel

Identify

You are about to identify yourself towards the following provider:

Provider
Governikus GmbH & Co. KG
Touch for more details

Proceed to PIN entry

By entering your PIN, access to the following data of your ID card will be allowed to the mentioned provider:

Read access

Family name

Birth name

Given name(s)

Doctoral degree

Date of birth

Place of birth

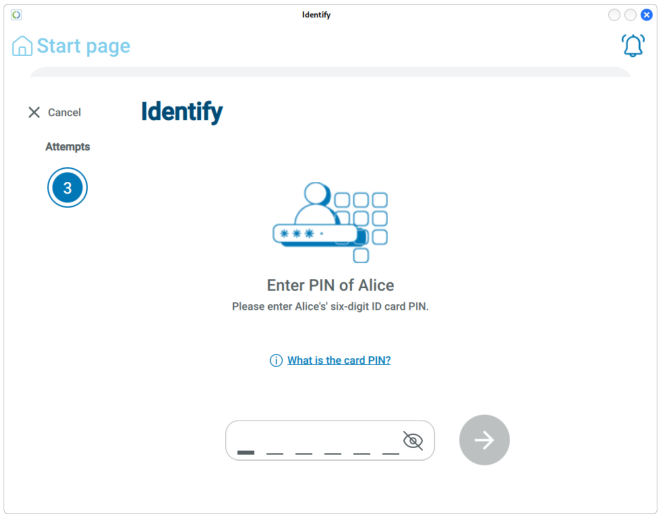
FIG. 8. Alice is shown the (wrong) certificate of Service Provider A

Provider A (refer to Figure FIG. 8). In this PoC, where Alice seeks access to her personal data, she is shown the official certificate of Governikus. As soon as Alice continues, the APDU-Redirection is triggered.

[**4. APDU-Redirection**] Service Provider B establishes communication with the attacker's system, transmitting the SOAP/APDU commands. The modified Governikus software on the attacker's system redirects these commands (APDUs) to Alice's client device. Subsequently, on Alice's device, the IFD service receives the APDUs and forwards them to the connected physical Identity Card.

Upon the initiation of the PACE protocol, the attacker requires Alice's PIN. Illustrated in figure FIG. 9, the attacker's software waits to receive the PIN from Alice.

[**5. PIN-Redirection**] The attacker triggers the PIN entry screen on Alice's device, as depicted in figure FIG. 10. As this aligns with the normal flow that Alice would expect, Alice enters her PIN without suspicion. The PIN is intercepted and transmitted through a specialized message on the IFD channel. Subsequently, the attacker receives the PIN (refer to figure FIG. 11) and inputs it for the PACE protocol. It is important to emphasize that a real attacker would likely automate this step.


Identify

Start page

Cancel

Identify

Attempts

3

Enter PIN of Alice

Please enter Alice's' six-digit ID card PIN.

What is the card PIN?

FIG. 9. Attacker waits for the PIN of Alice

The process continues with the exchange of APDUs between Alice's device and the attacker's system until the identification is successfully completed.

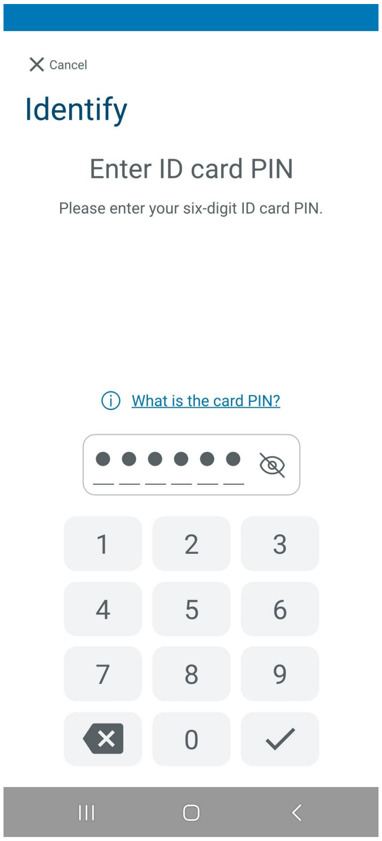
The attacker now possesses access to the target service as Alice.

[**6. Finishing**] Upon the completion of the attack, the original connection from Alice's device to Service Provider A is unpaused. The attacker utilizes the stored PIN obtained from the "PIN-Redirection" step for the PACE protocol. Consequently, the identification for Service Provider A does not demand additional user interaction from Alice, allowing her to seamlessly access the service. Illustrated in Figure FIG. 12, Alice successfully accesses the service to retrieve the data from her eID. The only potential distinction Alice might observe is a slightly prolonged readout from her eID, as two readouts are actually performed: one by the attacker for Service Provider B and the subsequent readout for Service Provider A.

VI. RESPONSIBLE DISCLOSURE AND BSI RESPONSE

After the discovery of the vulnerability, a responsible disclosure has been initiated with the BSI. A first version of this paper has been provided and a timeline of 45 days in line with the process defined by the BSI as detailed in the 'BSI CVD guideline for security researchers' has been set.

The BSI confirmed the vulnerability ("Yes, we agree that your described scenario enables an attacker to authenticate against a relying party using the eID of a victim through compromising the user space.").


Cancel

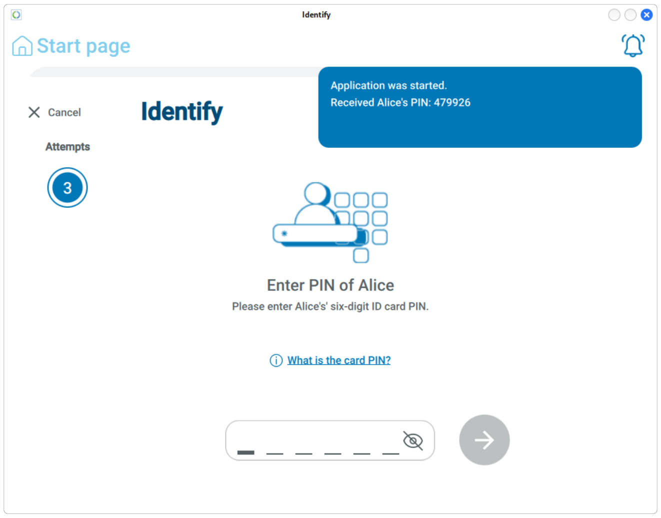
Identify

Enter ID card PIN

Please enter your six-digit ID card PIN.

What is the card PIN?

FIG. 10. Alice entering her PIN



Identify

Attempts

3

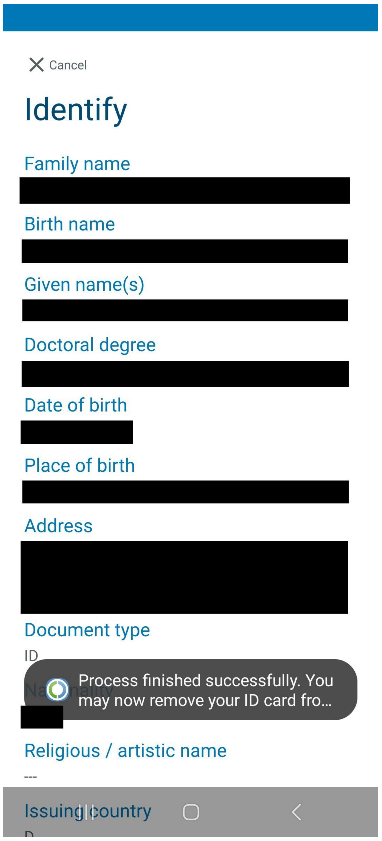
Application was started.
Received Alice's PIN: 479926

Enter PIN of Alice

Please enter Alice's' six-digit ID card PIN.

What is the card PIN?

FIG. 11. Attacker receives the PIN


Cancel

Identify

Family name
[redacted]

Birth name
[redacted]

Given name(s)
[redacted]

Doctoral degree
[redacted]

Date of birth
[redacted]

Place of birth
[redacted]

Address
[redacted]

Document type
ID

Process finished successfully. You may now remove your ID card fro...

[redacted]

Religious / artistic name

Issuing country
D

FIG. 12. Alice successfully accesses Services Provider A. NOTE: The author's personal data is removed from the screenshot.

However, their primary counterargument centers on placing the responsibility for client device security on the user, citing legal obligations for the citizen (”ensuring a secure operational environment at the client side is an obligation of the ID card owner per §27 (2) and (3) PAuswG.”). These obligations for citizens to ensure a secure operational environment include regular updates to the operating system, anti-virus programs, and firewalls (refer to [20]).

1. The reply essentially confirms that the German eID provides only client-side security when basic readers are used. The security level is determined by the weakest link, which, in this context, is the user's device. That other components of the system, such as the chip or the eID server, possess higher levels of security becomes irrelevant as an attacker will invariably target the weakest link in a system. For certain attack vectors, such as deeplinking and phishing, the security level can even be considered as falling below client-side security, as these vectors do not require compromising the user's device.

2. Assigning responsibility for security solely to users is an irresponsible approach. It is a well-established fact that users often face challenges in maintaining robust security practices. Relying on everyday citizens to consistently stay updated with the latest patches and anti-virus software is likely impractical. Notably, the BSI's security advice lacks guidance on phishing. Any security system, including the German eID, that places responsibility for security solely to users is fundamentally

flawed in its design.

3. The claim that users can prevent such an attack by following security advice is not correct. The research paper outlines various potential attack vectors, including the deeplink vulnerability, phishing, remote exploits, and supply chain attacks. Of these, only the remote exploit is effectively addressed by the BSI's security advice. Notably, the deeplink and phishing vectors are effective even if the operating system is updated, and antivirus programs and firewalls are in place. The proof of concept clearly demonstrated the effectiveness of the attack even on a fully updated system thereby proving the BSI's answer as incorrect. Shifting the responsibility for security to everyday citizens is not only irresponsible but also ineffective in preventing the attack.

Given that the eID is employed to safeguard highly sensitive systems with the potential for substantial financial gains through attacks, it seems inevitable that this vulnerability will be exploited at scale.

VII. POTENTIAL COUNTERMEASURES

The objective of this section is to outline potential countermeasures against the identified vulnerability. The countermeasures are first described individually, followed by an overview of the specific attack vectors against which each countermeasure might be effective.

[**C1: Use Secure PIN Entry**] As delineated in BSI TR-03119 [9], Basic Readers should be reserved for services with low security requirements (e.g., "age verification," "eTicketing," and "Internet shopping"). All other services should mandate the use of Standard or Comfort Readers. Any reader equipped with a physical PIN pad and a display is not suspectible to the described attack.

The BSI acknowledges that this countermeasure effectively mitigates the issue but adds, "However, enforcement of a specific card reader device by the service provider is neither possible nor feasible," leaving the feasibility of this countermeasure uncertain.

[**C2: Certification of BSI TR-03124**] BSI TR-03124 [21] emphasizes the need for secure PIN entry, especially for card readers without secure PIN entry (i.e., "basic readers"). The TR states "The eID-Client implements the following security relevant functionalities (...) PIN-Pad for card readers without secure PIN entry (i.e. a “basic reader”) (...) These functionalities MUST be suitably protected against manipulation.". While the TR serves as a technical specification, mandatory certification of the eID client ensures compliance with the standard, protecting against manipulation.

[**C3: User Security Training**] Recognizing that a portion of the attack can be executed through compromising the user's device, adherence to proper security hygiene practices, such as using antivirus software, regular system updates, and avoiding side-loading will help preventing the compromise.

The BSI agrees that "these measures are advised for all users of the eID function".

[**C4: Manufacturer Security Certification**] Given that a supply chain attack could compromise all users of a specific eID client manufacturer, enhancing security requirements for manufacturers and instituting a certification process to validate the implementation of these requirements will bolster resistance against supply chain attacks.

[**C5: Approved List of eID Clients**] Removed after discussion with the BSI.

[**C6: Client Side Security**] Recognizing that the vulnerability compromises the hardware security of the eID, shifting focus to client-side security measures becomes imperative. Implementing measures such as obfuscation, rooting detection, checksums, anti-debugging measures, and refraining from publishing the source code of eID clients as open source can make executing the attack more challenging.

These measures serve as a "band-aid" only and can be bypassed by a determined attacker. Nonetheless, their implementation is recommended, considering that the eID provides only client-side security, and these measures offer some level of security.

[**C7: Endpoint Verification**] Removed after discussion with the BSI.

[**C8: Decoupling of Authentication Factors**] Recognizing the inadequate decoupling of the two authentication factors (possession/knowledge), implementing measures to properly decouple these factors could potentially mitigate the vulnerability. For instance, requiring Alice to enter the PIN on a different device from where she uses the physical identity card, akin to certain banking apps, could enhance security.

The BSI adds, "However, this implementation does not allow the two factors to be decoupled," suggesting that this may not be a viable option.

[**C9: Deeplink Security**] Deep linking to the eID clients (and especially the official AusweisApp) should be secured against redirection by utilizing universal links instead of custom URL schemes.

The BSI states, ”The invocation mechanism of the eID-Client as specified in BSI TR-03124 deliberately ensures the possibility to redirect to an arbitrary eID-Client installed on the client system. Using Universal Links would break this interoperability.”

The argument against using Universal Links, as presented by the BSI, is not aligned with security best practices recommended by Apple and Google. As demonstrated in the proof of concept, the current practice of allowing custom URI schemes poses significant security risks, making it important to adopt more secure alternatives like Universal Links. Furthermore, the idea of redirecting to an ”arbitrary” eID client seems unsupported by reality, given that most services exclusively support a single eID client. Embracing Universal Links would therefore not compromise interoperability while significantly enhancing security in line with security best practices.

[**C10: Additional Authentication**] Relying parties, particularly those with substantial or high security requirements, should not solely depend on the eID for their sign-up or authentication processes.

Following discussions with the BSI, it has become evident that there may currently be no effective countermeasures against this vulnerability. Consequently, relying parties are advised to implement additional authentication methods alongside the eID to improve security. Potential additional measures include:

- Username / Password
- SMS OTP
- Authenticator Apps
- Physical letters
- Biometrics

For instance, in the case of insurance companies, many (though not all) electronic patient records services necessitate additional authentication steps beyond the eID. Users typically authenticate with a username and password before employing the eID. This layered approach enhances security.

On the other hand, BundID appears to be exclusively linked to the eID as an authentication method. In this scenario, if an attacker successfully compromises the eID, they would gain access to the victim's BundID. To mitigate this risk, BundID should consider introducing additional authentication requirements, as mentioned above.

[**C11: Notification of User**] Users should receive prompt notifications through an appropriate communication channel whenever their eID is used for sign-up or authentication. This communication approach ensures that users are informed of any eID-related activities, allowing them to detect potential attacks and enabling containment of possible damage. This practice aligns with established security best practices, where services routinely send login notifications to users for awareness.

[**Attack Vector Mapping**] This section provides an overview of how the countermeasures contribute to mitigating various attack vectors outlined in this paper. The attack vectors are:

1. AV1: Deeplink Attack
2. AV2: Phishing
3. AV3: Remote Exploit
4. AV4: Supply Chain Attack

The ensuing table shows the efficacy of each countermeasure against specific attack vectors:

Countermeasure	AV1	AV2	AV3	AV4
C1: Use Secure PIN Entry	✓	✓	✓	✓
C2: Certification of BSI TR-03124			✓	
C3: User Security Training			✓	
C4: Manufacturer Certification				✓
C6: Client Side Security			✓	
C8: Authentication Factors	✓	✓	✓	✓
C9: Deeplink Security	✓	✓		
C10: Additional Authentication	✓	✓	✓	✓
C11: Notification of User	✓	✓	✓	✓

VIII. CONCLUSION

This paper has shown the existence of a vulnerability in the German eID scheme, posing a significant risk to all services relying on the eID, especially those handling sensitive data such as insurances, banks, and government services. While the BSI acknowledges the vulnerability, it places the responsibility on users for maintaining client device security. Contrary to this, the paper demonstrates that even with a perfectly secure client device, the attack remains effective.

The attack does not rely on remote code execution, physical access, or similar requirements. The only prerequisite is that the user has an app on their smartphone, which is uploaded to the app store by a malicious actor.

The available countermeasures have been discussed, showing only limited viable options. At present, the author recommends:

1. C6 Client Side Security: Although acting as a temporary solution, this measure could enhance security to some extent.

2. C9 Deeplink Security: Implementing this countermeasure is highly recommended, as it would contribute

significantly to security and there appears to be no compelling reason not to do so.

3. C10 Additional Authentication: Given that other countermeasures do not effectively address the vulnerability, combining the eID with additional authentication measures appears to be the most viable option to attain the required security level.

Unfortunately, beyond these recommendations, there seem to be limited alternatives to mitigate this vulnerability, outside of discontinuing the use of eID for substantial or high security use cases.

IX. AUTHOR INFO

Note from the author:

"I am a private security researcher who has previously utilized the eID system. The details of how the eID guards against Man-in-the-Middle attacks, particularly when the PIN is entered on a smartphone, sparked my curiosity. Upon researching the details and implementing a PoC, I was surprised by the ease with which the system could be compromised and the far-reaching implications for the security and data privacy of German citizens.

My goal is to raise awareness regarding this vulnerability and to support with possible countermeasures. I adhere to the official 'BSI CVD guideline for security researchers', following responsible disclosure procedures to the concerned entities and the BSI. Full disclosure is planned after the recommended 45-day waiting period.

Given my commitment to privacy, I opt to remain anonymous. Furthermore, instances are documented where security researchers aiming to raise awareness about vulnerabilities within government systems, have encountered legal action instead of efforts to address the identified security issues. In addition, the existence of the vulnerability is independent of my identity.

For communication, you can reach me at 0xCtrlAlt@proton.me or you can subscribe to my blog at https://ctrlalt.medium.com/. Please note that I may answer some of the question I receive in additional blog posts at the address mentioned before. My PGP fingerprint is 8A9D D1DF CA47 494C 35EF DC26 53B2 F3B1 88D6 E7D4."

Appendix A: CVSS Calculation

The following is an estimate of the CVSS (Common Vulnerability Scoring System) score according to CVSS Version 3.1 (refer to [22]). CVSS, as defined by FIRST (see https://www.first.org/cvss/v3.1/specification-document), includes several key definitions:

Vulnerable Component: "That is, they represent characteristics of the thing that is vulnerable, which we refer to formally as the vulnerable component." In the context of this vulnerability, it applies to the eID scheme.

Impacted Component: "The Impact metrics reflect the direct consequence of a successful exploit and represent the consequence to the thing that suffers the impact, which we refer to formally as the impacted component." In the context of this vulnerability, this refers to the service relying on the eID for authentication or identification. In the PoC, the "Impacted Component" was the eID itself (as I used the vulnerability to read personal information from the chip). HOWEVER, in most cases, the "Impacted Component" will be a different entity. Consider the case of the electronic patient records: Here, the impacted component that "suffers the impact" is the electronic patient record service of the user.

It's vital to note that the CVSS score should not be and was not calculated based on the PoC attack but on a worst-case scenario (e.g., accessing the ePA, accessing BundID, etc.) that can be exploited using this vulnerability. This aligns with CVSS guidelines: "The Base Score reflects the severity of a vulnerability according to its intrinsic characteristics, which are constant over time and assume the reasonable worst-case impact across different deployed environments.". The catalog of providers accessible through the eID (see https://www.ausweisapp.bund.de/en/list-of-providers) includes some exceptionally sensitive services.

Considering the definitions outlined above:

1. **Attack Vector (AV)**: The research paper outlines four distinct attack vectors (deeplink vulnerability, phishing, remote exploit, and supply chain attack). The AV metric varies for these attack vectors, and the most dangerous one should be considered, which is the deeplink vulnerability vector. Given that this vulnerability is remotely

exploitable (e.g., through the app store), the attack vector is classified as "Network (AV:N)"

2. **Attack Complexity (AC)**: According to 2.1.2 of the CVSS guideline (see the link above), "Importantly, the assessment of this metric excludes any requirements for user interaction in order to exploit the vulnerability." There are no additional "conditions beyond the attacker's control that must exist in order to exploit the vulnerability." The following statement is true: "An attacker can expect repeatable success when attacking the vulnerable component," resulting in a value of "Low (AC:L)".

3. **Privileges Required (PR)**: The attacker is unauthorized before initiating the attack, leading to "None (PR:N)" for privileges required.

4. **User Interaction (UI)**: This attack necessitates at least one user actions such as holding the eID to the smartphone. Consequently, user interaction is "Required (UI:R)".

5. **Scope (S)**: Here the worst-case scenario has to be considered according to the CVSS guidelines. Consider the electronic patient records: The attacker exploits the vulnerability to access the electronic patient records of the user. In this case, there are two "security authorities" and two "security scopes" (see 2.2). The first security authority is the eID scheme and system. The second security authority is the attacked insurance company and its systems. As mentioned earlier: The Vulnerable Component is different from the Impacted Component. According to the CVSS guidelines, a scope change occurs "If a vulnerability in a vulnerable component can affect a component which is in a different security scope than the vulnerable component"). Therefore, the value is "Changed (S:C)".

   Note: The eID and the relying service can solely be considered as one security scope if the eID is exclusively used by that one relying service. Reiterating from section 2.2 of the CVSS guideline: "The security scope of a component encompasses other components that provide functionality SOLELY to that component, even if these other components have their own security authority.". As the eID is clearly used by many different relying services those are different security authorities.

6. **Confidentiality Impact (C)**: Consider the electronic patient records: the attacker can access information from a user's ePA using the vulnerability. These records involve highly confidential data (refer to CVSS guidelines: "the disclosed information presents a direct, serious impact."). Furthermore, using the deeplink vulnerability, the attacker can target many users simultaneously (all who download the app). Consequently, the confidentiality for the worst-case scenario, as mandated by CVSS guidelines, is "High (C:H)".

7. **Integrity Impact (I)**: Revisit the worst-case scenario: An external service relies on the eID for authentication (e.g., a bank). After a successful exploit, the attacker can leverage the acquired privileges to modify or delete settings, financial information, personal information etc., on the relying service. According to the NIST definition of integrity (see https://csrc.nist.gov/glossary/term/integrity: "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity."), the integrity of the relying service is clearly compromised. Given the highly sensitive nature of systems using the eID for authentication, it is evident that "malicious modification would present a direct, serious consequence to the impacted component." As per CVSS guidelines, this results in "High (I:H)".

8. **Availability Impact (A)**: It is possible to "fully deny access to resources in the impacted component" for some of the affected components. Some relying services allow the attacker to close the account, thereby denying access to the actual user. Therefore, in line with the above rationale and considering the worst-case scenario per CVSS guidelines, this would result in "High (A:H)".

9. **Confidentiality Requirement (CR)**: Considering that the eID protects highly critical services, the additional impact on confidentiality is high (e.g., accessing Alice's electronic patient records). Thus, the confidentiality requirement is "High (CR:H)".

10. **Integrity Requirement (IR)**: As the eID shields highly critical services, the additional impact on integrity is high (e.g., manipulating government services for Alice). Therefore, the integrity requirement is "High (CI:H)".

11. **Availability Requirement (AR)**: For the most likely attack vector of phishing the attacker cannot impact the availability of the eID. Therefore the availability requirement is not defined "Not Defined (AR:X)"

The corresponding CVSS 3.1 vector is ”AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H/CR:X/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:H/MI:H/MA:H”, resulting in a calculated CVSS score of 9.7 (Critical). The corresponding CWE is ”CWE-290: Authentication Bypass by Spoofing”.

Appendix B: CEM Attack Potential

The assessment of the attack potential, following Annex B.4 of the CEM v3.1 (Common Methodology for Information Technology Security Evaluation, see [23]), for the phishing approach is detailed below:

1. **Elapsed Time**: The development of the attack is estimated to range between one and two weeks. Consequently, the Elapsed Time is denoted as ”less than two weeks,” yielding a value of 2.

2. **Specialist Expertise**: Executing the attack demands some knowledge about the eID. Therefore, an ”Expert” is considered capable of executing the attack, resulting in a value of 6.

3. **Knowledge of TOE**: The attack relies solely on ”Public” information related to the Target of Evaluation (TOE), such as open-source code and technical specifications published by the BSI. Hence, the value is 0.

4. **Window of opportunity**: Given the attack’s undetectable nature and its potential for unlimited retries, the window of opportunity is classified as ”Unnecessary/unlimited.” Therefore, the value is 0.

5. **Equipment**: The attack is carried out using only a ”standard” laptop. Consequently, the value is 0.

The overall score sums up to 2 + 6 + 0 + 0 + 0 = 8. As a result, the attack potential is categorized as ”Basic.

Appendix C: Analysis by the BSI

> ”Your paper is well written and technically correct in nearly every aspect. Other publications addressing similar issues are known since 2010.”

Summary of BSI’s reply: The analysis notes that similar issues have been addressed in publications, probably refering to other publications by the Chaos Computer Club in 2010, showing vulnerabilities related to phishing the PIN.

In response: The difference of this new research lies in its demonstration that both the PIN AND the physical factor (the card) can be simultaneously targeted, showcasing undetectable attacks without the need for phishing the victim. This extends beyond the 2010 findings.

Interesting fact: In 2010, the BSI responded to the publication by stating that it was not a concern, assuming citizens would use standard or comfort readers for secure transactions. In today’s environment, where users predominantly utilize basic readers, this assumption is no longer applicable.

> ”The described attack however does not qualify as a Monster-in-the-Middle attack, because it needs manipulation of or within the user space or the app space respectively. A Monster-in-the-Middle attack is explicitly prevented by the security measurements of the German eID function, notably the TLS session binding and the entanglement of the TLS certificates with the authorization certificate.”

Summary of BSI’s reply: The described attack is not categorized as a Monster-in-the-Middle (MITM) attack since it requires manipulation in the user space, and MITM attacks are explicitly prevented by the security measures of the German eID function.

In response:

1. The classification of whether this is a MITM attack is a matter of semantics. What’s crucial to consider is the potential risk to individuals, such as Aunt Annie, whose patient records could be stolen from her insurance due to the vulnerability. Aunt Annie likely does not care about the matter of semantics.

2. The assertion that the security mechanism prevents MITM attacks is incorrect. The security mechanism establishes an end-to-end encrypted channel between the chip and the eID server, not between the user space and the eID server. Therefore, the ability to compromise the end-to-end encryption (in this case, through spoofing) from the user's device qualifies as a MITM attack. As demonstrated in the proof of concept, the session binding does not prevent the attack.

3. The BSI's own technical documentation states, ”The authentication mechanism of the German eID is based on a mutually authenticated and end-to-end-protected channel between the service provider and the CHIP of the eID card via a sequence of cryptographic protocols. This protects against attacks such as Man-in-the-Middle.” This statement emphasizes that any attacker situated between the chip and the eID server has to be considered a Man-in-the-Middle attack.

> ”As you pointed out correctly, it is possible to use the German eID with any eID-Client software that conforms to the specifications. This is not a design flaw, but deliberately designed that way. The German eID infrastructure is an open eco system, where eID-Clients (or Apps integrating an eID-Client) may be freely chosen by the user operating the client and eID-Server may be freely chosen by the service provider operating the Webservice. It is strongly advised though, to only use products with a conformity certification according to BSI TR-03124 or BSI TR-03130 respectively.”

Summary of BSI's reply: The eID scheme is an open ecosystem and users are ”strongly advised” to only use products with a conformity certification according to BSI TR-03124 or BSI TR-03130.

In response:

1. Requiring everyday citizens to assess ”conformity certifications” is completely unrealistic.

2. Upon examining the list of services, each service provider is using a single eID client, leaving citizens with no choice of eID clients.

3. The vulnerability exists irrespective of whether the eID client is certified or not. The proof of concept targeted the Governikus eID client, which is certified, directly contradicting the BSI's assessment.

> ”This enables users to choose which organisation/implementation they trust (including to NOT trust the official implementation) and also opens up the possibility to build their own clients. Be it from the existing open source code of the official AusweisApp or from other projects, like e.g. Open eCard App or even from scratch.”

Summary of BSI's reply: Ordinary citizens are expected to review the source code of the eID client implementations and should build their own eID clients.

In response: I am really at a loss for words here.

> ”When using a Basic Reader (Cat-B) without a secure PIN-entry and a dedicated display, input of the PIN and presentation of the authorization certificate as well as the requested data groups are bound to the security of the client device. This especially applies to Smartphones.
>
> If the user space on the client device is compromised (e.g. by installing a malicious eID-Client or other software, that may grab user input and/or block, change or overlay screen output) privacy of the PIN may be compromised as well as the security features of the eID-client regarding the service providers authorization.”

Summary of BSI's reply: Yes, the eID can actually be compromised completely by compromising the user space, as it is ”bound to the security of the client device.”

In response: This reply acknowledges that the eID scheme when using a Basic Reader (Cat-B) without a secure PIN-entry and a dedicated display relies on client-side security and does not provide hardware security. This aligns with the proof of concept, which has demonstrated exactly that. The next question is, what are the implications of this? Client-side security is insufficient for many use cases that currently rely on the eID for authentication.

My question to the BSI: ”Can we agree that the vulnerability enables the practical exploitation of a relying service (e.g., accessing their BundID) purely through compromising the user space of the victim, as elaborated in the research paper? If not, could you provide specific reasons for disagreement?”
”Yes, we agree that your described scenario enables an attacker to authenticate against a relying party using the eID of a victim through compromising the user space.”

In response: Agreed. Once more, the key question is: What are the implications of this?

”However we do not agree that this would imply the services of the relying parties are vulnerable their selves. From the point of view of the relying party, there is no exploitation or compromise of their systems as the authentication happened with a genuine eID and by using the correct protocols.”

Summary of BSI's reply: The services of relying parties are not compromised themselves as it's a genuine eID and the correct protocls are used.

In response: The actual systems (e.g., servers) of relying parties are, of course, not compromised. However, the response is also inaccurate. If an attacker can retrieve electronic patient records from an insurance company, the only valid conclusion is that the service of the insurance has been compromised. The method an attacker employs, whether it involves the ”correct protocols” or not, is irrelevant.

”User binding of an eID (that includes ensuring sole control) always depends on the cooperation and caution of the user.

Protection (i.e. confidentiality) of the PIN and ensuring a secure operational environment at the client side is an obligation of the ID card owner per §27 (2) and (3) PAuswG. This includes “using only technical systems and components, that are evaluated as secure by the Federal Office for Information Security.”

Summary of BSI's reply: The BSI acknowledges the vulnerability. However, their primary counterargument centers on placing the responsibility for client device security squarely on the user, citing legal obligations for the citizen.

In response:

1. Assigning responsibility for security solely to users is an irresponsible approach. It is a well-established fact that users often face challenges in maintaining robust security practices. Relying on everyday citizens to consistently stay updated with the latest patches and anti-virus software is likely impractical. Notably, the BSI's security advice lacks guidance on phishing, a significant and dangerous attack vector. Any security system, including the German eID, that places responsibility for security solely to users is fundamentally flawed in its design.

2. The claim that users can prevent such an attack by following security advice is not correct. The research paper outlines various potential attack vectors, including the deeplink vulnerability, phishing, remote exploits, and supply chain attacks. Of these, only the remote exploit is effectively addressed by the BSI's security advice. Notably, the deeplink and phishing vectors are effective even if the operating system is updated, and antivirus programs and firewalls are in place. The proof of concept, clearly demonstrated the effectiveness of the attack even on a fully updates system thereby proving the BSI's answer as incorrect. Shifting the responsibility for security to everyday citizens is not only irresponsible but also ineffective in preventing the attack.

”As long as a genuine AusweisApp is installed at least on the reading device, the attack would also be prevented.”

In response: This statement is not correct. Please refer to the proof of concept for a demonstration where a user was deceived into installing an additional app with eID functionality. Even with the genuine AusweisApp installed from the official app store, the attack was still successful. It is important to note that for none of the attack vectors does it matter whether the official AusweisApp is installed or not, except for the deeplinking attack on Android, where an app chooser would be displayed if two apps are installed which register the same deeplink.

Appendix D: Bibliography

[1] Bundesministerium des Innern und für Heimat. Personalausweisportal, . URL https://www.personalausweisportal.de/.

[2] Governikus GmbH & Co. KG. Ausweisapp, . URL https://www.ausweisapp.bund.de/.

[3] Bundesamt für Sicherheit in der Informationstechnik. Bsi tr-03130, . URL https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03130/tr-03130.html.

[4] Bundesamt für Sicherheit in der Informationstechnik. Bsi tr-03112, . URL https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03112/tr-03112.html.

[5] Bundesverwaltungsamt. Liste der diensteanbieter mit berechtigung. URL https://download.gsb.bund.de/VfB/npavfb.pdf.

[6] Wikipedia. Iso/iec 7816, . URL https://en.wikipedia.org/wiki/ISO/IEC_7816.

[7] Bundesamt für Sicherheit in der Informationstechnik. German eid whitepaper, . URL https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German_eID_Whitepaper_v1-4.pdf?__blob=publicationFile&v=2.

[8] Bundesamt für Sicherheit in der Informationstechnik. German eid loa mapping, . URL https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/EIDAS/German_eID_LoA_Mapping_v1-4.pdf?__blob=publicationFile&v=2.

[9] Bundesamt für Sicherheit in der Informationstechnik. Bsi tr-03119, . URL https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03119/BSI-TR-03119_V1_pdf.pdf?__blob=publicationFile&v=2.

[10] REINER Kartengeräte GmbH und Co. KG. cyberjack rfid standard (usb). URL https://shop.reiner-sct.com/chipkartenleser-fuer-die-sicherheitsklasse-3/cyberjack-rfid-standard-usb.

[11] Bleepingcomputer. Apt36 youtube clone. URL https://www.bleepingcomputer.com/news/security/apt36-state-hackers-infect-android-devices-using-youtube-app-clones/.

[12] Techradar. Google play store trojans. URL https://www.techradar.com/news/google-play-store-littered-with-dangerous-trojans.

[13] TechCrunch. Apple will reportedly allow sideloading apps with ios 17. URL https://techcrunch.com/2022/12/14/apple-will-reportedly-allow-sideloading-apps-with-ios-17/.

[14] Ars. 4 vulnerabilities under attack give hackers full control of android devices. URL https://arstechnica.com/gadgets/2021/05/hackers-have-been-exploiting-4-critical-android-vulnerabilities/.

[15] Lookout. Rooting malware makes a comeback: Lookout discovers global campaign. URL https://www.lookout.com/threat-intelligence/article/lookout-discovers-global-rooting-malware-campaign.

[16] Wikipedia. Pegasus (spyware), . URL https://en.wikipedia.org/wiki/Pegasus_(spyware).

[17] securityaffairs. 3cx supply chain attack allowed targeting cryptocurrency companies. URL https://securityaffairs.com/144411/apt/3cx-supply-chain-attack-cryptocurrency.html.

[18] arstechnica. 18,000 organizations downloaded backdoor planted by cozy bear hackers. URL https://arstechnica.com/information-technology/2020/12/18000-organizations-downloaded-backdoor-planted-by-cozy-bear-hackers/.

[19] Governikus GmbH & Co. KG. Ausweisapp2 source code, . URL https://github.com/Governikus/AusweisApp2.

[20] Bundesministerium des Innern und für Heimat. Your contribution to enhance security, . URL https://www.personalausweisportal.de/Webs/PA/EN/citizens/security-and-data-protection/security-advice/security-advice-node.html.

[21] Bundesamt für Sicherheit in der Informationstechnik. Bsi tr-03124, . URL https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03124/TR-03124_node.html.

[22] NIST. Vulnerability metrics. URL https://nvd.nist.gov/vuln-metrics/cvss.

[23] Common Criteria. Common methodology for information technology security evaluation. URL https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R2.pdf.