

2. Handlungsschritt (20 Punkte)

Korrekturrand

Die MED GmbH gliedert sich in die Abteilungen Allgemeinmedizin und Sportmedizin. Zukünftig sollen die Abteilungen Naturheilverfahren und Arbeitsmedizin hinzukommen.

Sie planen den Einsatz von VLANs.

a) Nennen Sie vier Gründe, die für den Einsatz eines VLANs statt einer physikalischen Gesamtnetzwerkstruktur sprechen. (4 Punkte)

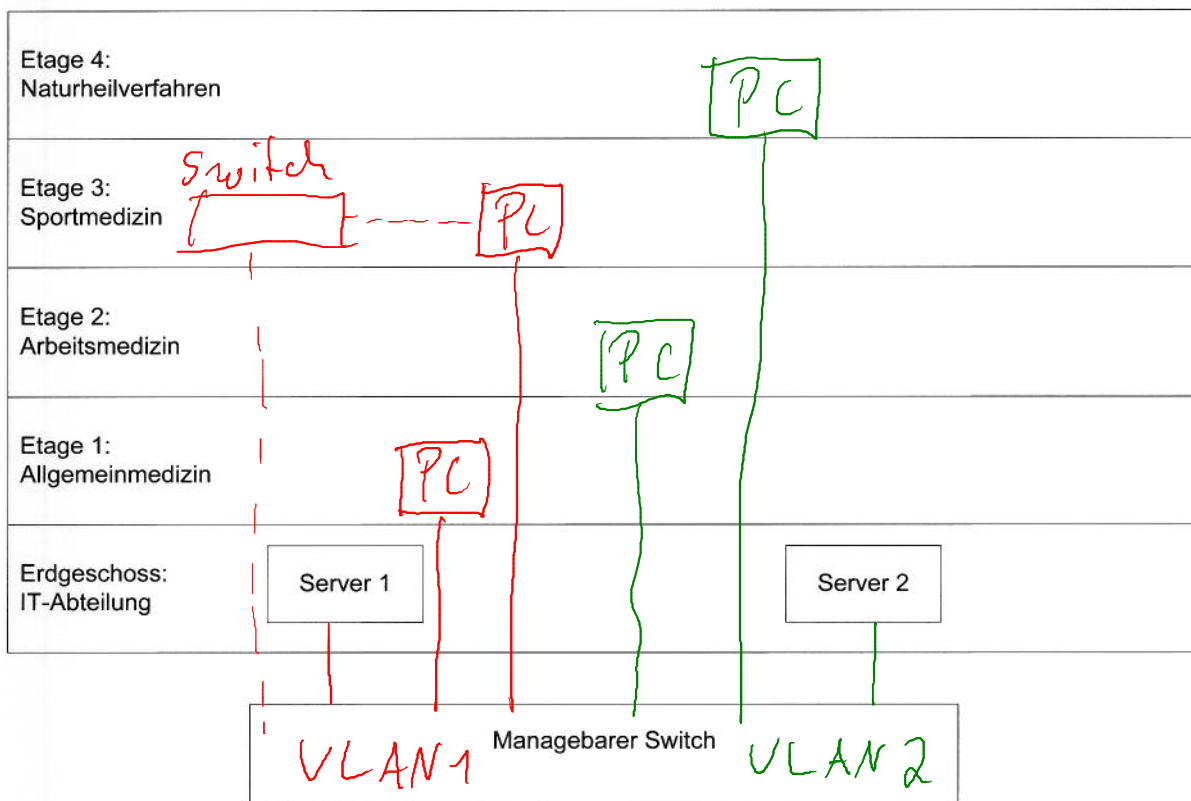
- erhöhte Sicherheit durch Trennung der Netze
- Vereinfachung bei Umstrukturierung
- Bessere Leistung des Netzwerks durch Reduzierung der Broadcastdomain
- Flexibilisierung / Unabhängigkeit von der vorhandenen Topologie
- Delegation der Netzwerkadministration
- Priorisierung des Netzwerkverkehrs

b) Jede Abteilung belegt eine Etage des Gebäudes. Die Abteilungen Allgemeinmedizin und Sportmedizin sollen an das VLAN 1, die beiden übrigen Abteilungen an das VLAN 2 angeschlossen werden.

Ergänzen Sie den folgenden VLAN-Plan indem Sie

ba) in jede Etage einen PC einzeichnen und diesen jeweils mit der entsprechenden Netzwerkkomponente verbinden. (2 Punkte)

bb) die Server 1 und 2 mit der entsprechenden Netzwerkkomponente verbinden. Server 1 soll dem VLAN 1 und Server 2 dem VLAN 2 zugeordnet werden. (2 Punkte)



c) Nennen Sie die Schicht des OSI-7-Schichtenmodells, auf der die Netzwerkkomponenten arbeiten müssen, wenn die beiden Server zum Zweck einer Datensynchronisation verbunden werden. (2 Punkte)

Layer 3

d) Der geplante GBit-Ethernet-Switch unterstützt PoE.

Korrekturrand

Erläutern Sie die PoE-Funktion.

(2 Punkte)

Power over Ethernet, Netzwerkgeräte werden über das Ethernet-Kabel mit Strom versorgt

e) Die technische Dokumentation zu dem VLAN-Switch liegt in englischer Beschreibung vor (s. u.). Beantworten Sie dazu die folgenden Fragen in Deutsch.

ea) Wie viele Geräteadressen können von dem Switch gespeichert und verwaltet werden?

(2 Punkte)

8000 Adressen

eb) Wozu dient die effiziente Bandbreitenkontrolle?

(2 Punkte)

Priorisierung des Netzwerkverkehrs
z.B. IP-Telefonie

ec) Durch welches Merkmal des Switches wird erreicht, dass sich keine fremden Clients über den Switch unbefugten Zugriff zum Netzwerk verschaffen können?

(2 Punkte)

802.1x - Zugangskontrolle von Netzwerkteilnehmern, um unautorisierten Zugriff zu verhindern

ed) Wie viele VLANs werden unterstützt?

(2 Punkte)

256 VLANs

VLAN-SW001PoE

Fast-Ethernet switch which supports flexible PoE and Gigabit connections for performance networks

- 24 Fast-Ethernet and two combo ports for Gigabit connections
- PoE at all 24 ports (total power output: max. 185 W)
- QoS-port based, 802.1p or TOS/DiffServ
- 802.1x authentication at all ports

Performance- Efficiency- Security

- The backplane can handle data throughput at up to 8.8 Gbps. Speed is provided by very short latency times under 5µs as required by the switch to determine the output port for a certain input port. The switch stores and manages up to 8000 MAC addresses and it supports up to 256 active VLANs.
- Just as important as the rapid spanning tree algorithm is the efficient control of bandwidth. This ensures that important applications such as IP telephony are constantly provided with ample bandwidth to avoid interruptions to conversations. Conducting bandwidth control, the VLAN-SW001PoE prioritizes the data traffic according to predefined criteria (e.g. voice data or certain ports).
- The VLAN-SW001PoE gives you the assurance that rogue clients cannot use this switch to gain access to your network. Configuring 802.1x access control for all ports ensures that unauthorized devices plugged into a switch port cannot gain access to the network. The VLAN-SW001PoE also features rigorous defenses against attacks such as MAC flooding.

3. Handlungsschritt (20 Punkte)

Korrekturrund

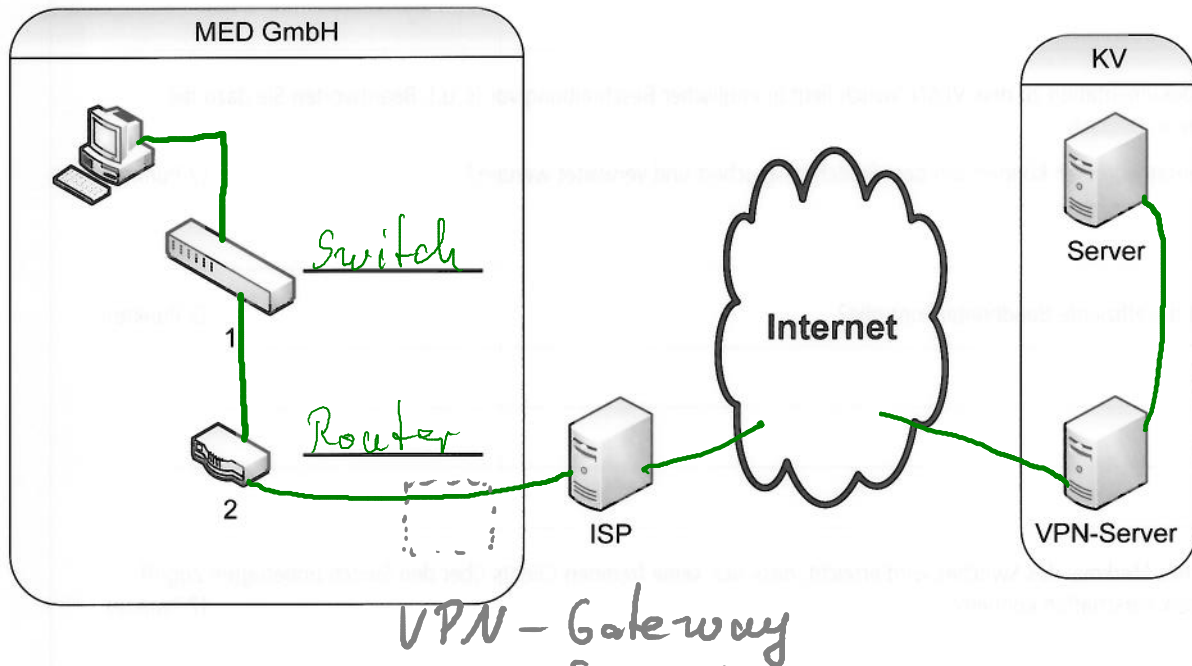
a) Die MED GmbH soll mit der Kassenärztlichen Vereinigung (KV) über ein „site to site“ VPN verbunden werden.

aa) In der folgenden Skizze sollen Sie die geplante VPN-Verbindung darstellen.

Vervollständigen Sie dazu die Skizze, indem Sie

- die Bezeichnungen für die mit 1 und 2 gekennzeichneten Komponenten eintragen.
- alle Verbindungen einzeichnen.

(3 Punkte)

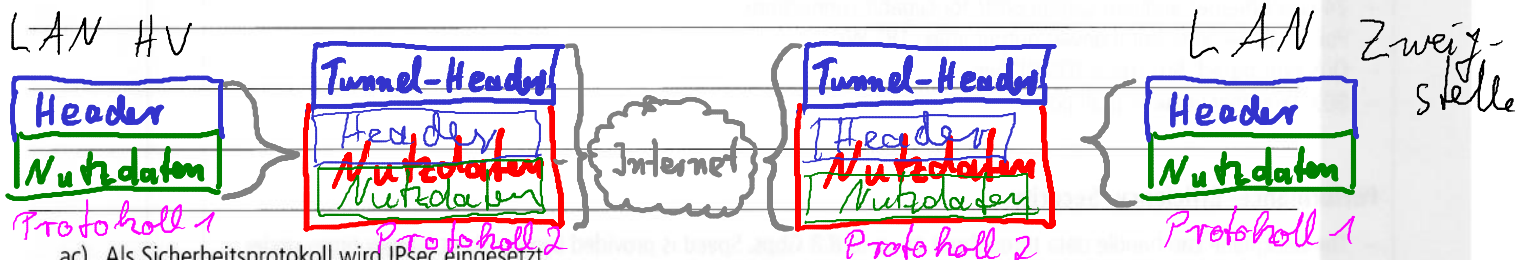
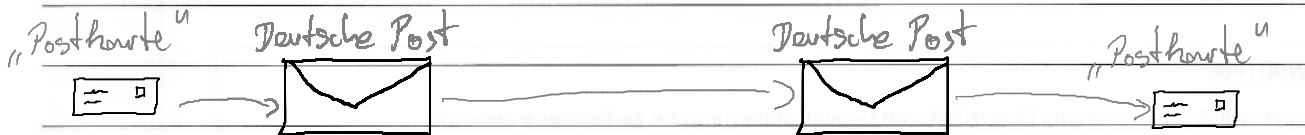


ab) Das VPN erzeugt einen sogenannten „Tunnel“.

Erläutern Sie stichwortartig den „Tunneling-Prozess“.

(4 Punkte)

Verkapselung der Daten oder des Protokolls
in ein anderes Protokoll



ac) Als Sicherheitsprotokoll wird IPsec eingesetzt.

Nennen Sie drei Sicherheitsmechanismen, die das Protokoll IPsec bereitstellt.

(3 Punkte)

- Authentifizierung
- Verschlüsselung (Schlüsselaustausch + Verschlüsselung der Daten + Ent)
- Integritätsicherung der Daten

b) Ein RAID-System soll Sicherheit und hohe Verfügbarkeit von Patientendaten gewährleisten.

Korrekturrand

ba) Man unterscheidet Software-RAID und Hardware-RAID.

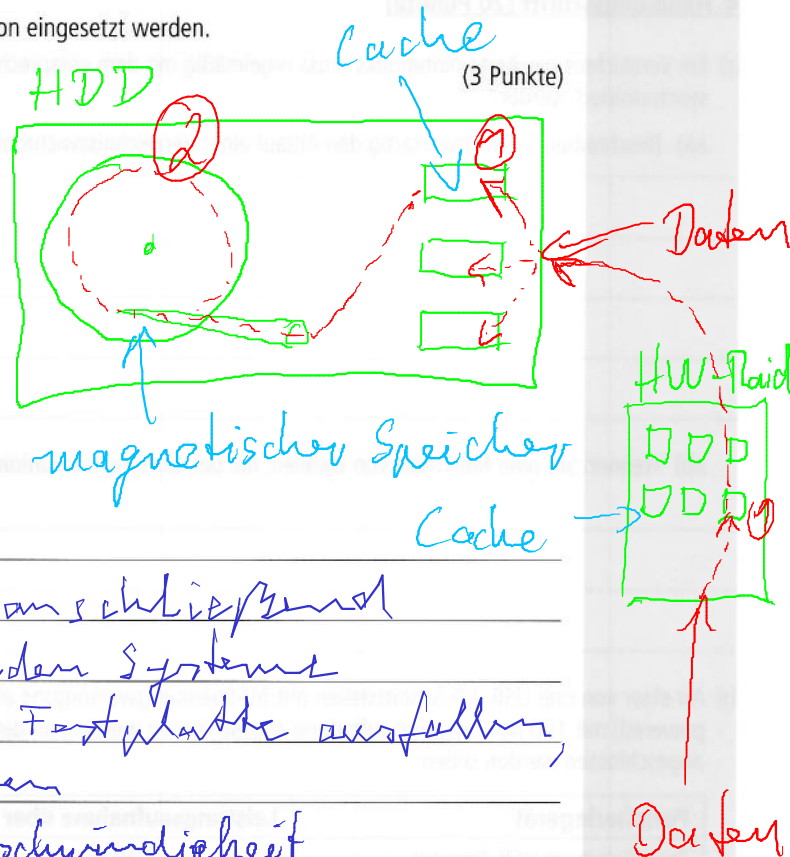
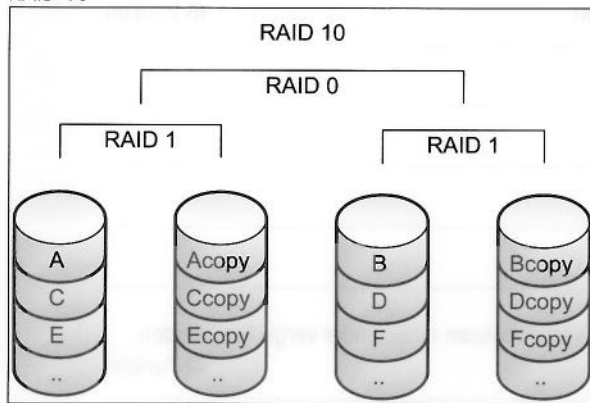
Vergleichen Sie die beiden RAID-Implementierungen, indem Sie die folgenden Vergleichskriterien jeweils mit „hoch“ oder „niedrig“ bewerten. (3 Punkte)

Vergleichskriterien	Software-RAID	Hardware-RAID
Kosten der Implementierung	niedrig	hoch
Performance	niedrig	hoch
CPU-Last am Host	hoch	niedrig

bb) In der MED GmbH soll nachfolgend abgebildete RAID-Kombination eingesetzt werden.

Beschreiben Sie stichpunktartig die Funktion des RAID-Systems. (3 Punkte)

RAID 10



- Festplatten als Raid 1, anschließend Raid 0 über diese beiden Systeme
- es darf pro Subraid 1 Festplatte ausfallen, insgesamt 2 Festplatten
- hohe Les- und Schreibgeschwindigkeit
- 50% der Bruttokapazität als Nettokapazität

bc) Erläutern Sie kurz zwei positive Eigenschaften dieser RAID-10-Kombination. (2 Punkte)

- sehr performant lesen + schreiben
- insgesamt 2 Festplatten können ausfallen, 1 Festplatte pro Subraid
- schnelle Rekonstruktion

Fortsetzung 3. Handlungsschritt →

Fortsetzung 3. Handlungsschritt

Korrekturrand

- bd) Berechnen Sie die zur Verfügung stehende Netto-Speicherkapazität des RAID-Systems mit folgender Formel, wenn jede der vier Festplatten eine Speicherkapazität von je 1 TB besitzt.

Formel: $C = n \cdot d / 2$

C = verfügbarer Speicherplatz

n = Anzahl der Laufwerke

d = Festplattenkapazität

(2 Punkte)

$$C = 4 \cdot \frac{1}{2} = 2 \text{ TB}$$

$$2 \text{ TB} \cdot \frac{1000^4 \text{ Byte}}{1 \text{ TB}} = \times \text{ Byte}$$

4. Handlungsschritt (20 Punkte)

- a) Ein Verzeichnis der Ärzte-Notebooks muss regelmäßig mit dem entsprechenden Verzeichnis eines Servers in der MED GmbH synchronisiert werden.

- aa) Beschreiben Sie stichwortartig den Ablauf einer Verzeichnissynchronisation.

(6 Punkte)

- Vergleich der Ordnerstruktur
- Vergleich der Dateien in den Ordnern (Zeitstempel, Größe, Checksum)
- fehlende Dateien übertragen | - Datei mit neuerer Version ersetzen

- ab) Nennen Sie zwei Merkmale von Dateien, die bei der Synchronisation von Verzeichnissen miteinander verglichen werden.

(2 Punkte)

- Zeitstempel
- Existenz
- Dateigröße

- b) An einer von drei USB 2.0-Schnittstellen mit 5V-Spannungsversorgung eines Ärzte-Notebooks soll ein passiver USB-Hub (bus powered) mit 100 mA Leistungsaufnahme angeschlossen werden, an den wiederum folgende Peripheriegeräte über USB angeschlossen werden sollen:

Peripheriegerät	Leistungsaufnahme über USB
Desinfizierbare USB-Tastatur	120 mA
USB-Maus	100 mA
USB-Stick für Bilddatenspeicherung	140 mA
Gesundheitskarten-Reader	60 mA

R : Widerstand $[\Omega]$
 $\uparrow$
 Ohm

- ba) Berechnen Sie die Leistung in Watt, die das Notebook an der USB-Schnittstelle bei gleichzeitigem Betrieb aller Peripheriegeräte bereitstellen müsste.

(3 Punkte)

$$P = \frac{(100 + 120 + 100 + 140 + 60) \text{ mA}}{1000} \cdot 5 \text{ V} = 2,6 \text{ A} \cdot \text{V}$$

Spannung [V] $\uparrow$ Umrechnungsfaktor von mA auf A

$$P = U \cdot I$$

Stromstärke [A]

$$P = U \cdot I \quad U = R \cdot I$$

$\frac{U}{R \cdot I}$

Dieses **Konzeptpapier** ist zur Eintragung von Nebenrechnungen und sonstigen Hilfsaufzeichnungen gedacht. Es muss vor Bearbeitung der Aufgaben dem Aufgabensatz entnommen werden. Bitte beachten Sie, dass Ihre Eintragungen **auf diesem Konzeptpapier** grundsätzlich nicht bewertet werden.



A series of horizontal lines for writing, spanning the width of the page below the header.

Handwriting practice lines consisting of 20 horizontal lines.

bb) Die Leistungsaufnahme aller Peripheriegeräte übersteigt die Leistung der Notebook-USB-Schnittstelle.

Korrekturrand

Nennen Sie eine Möglichkeit, wie trotzdem alle genannten Peripheriegeräte betrieben werden können.

(2 Punkte)

- aktiver USB-Hub
- aufteilen auf mehrere USB-Schnittstellen

c) Die MED GmbH muss laut Gesetz medizinische Daten sichern. Sie sollen daher die MED GmbH zur Datensicherung beraten.

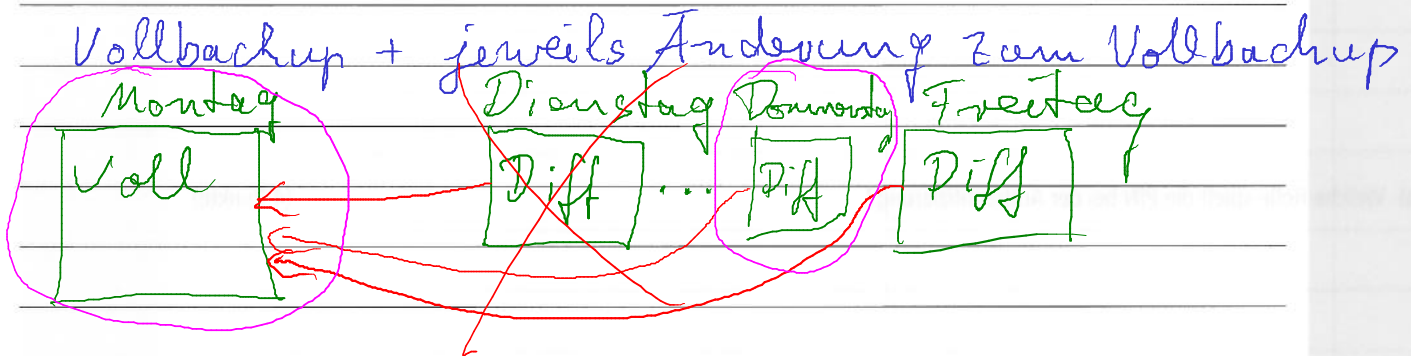
ca) Nennen Sie drei Ursachen für einen möglichen Datenverlust.

(3 Punkte)

- Hardwaredefekt
- Hackerangriff / Ransomware
- menschliches Versagen
- Softwarefehler
- Elementarschäden

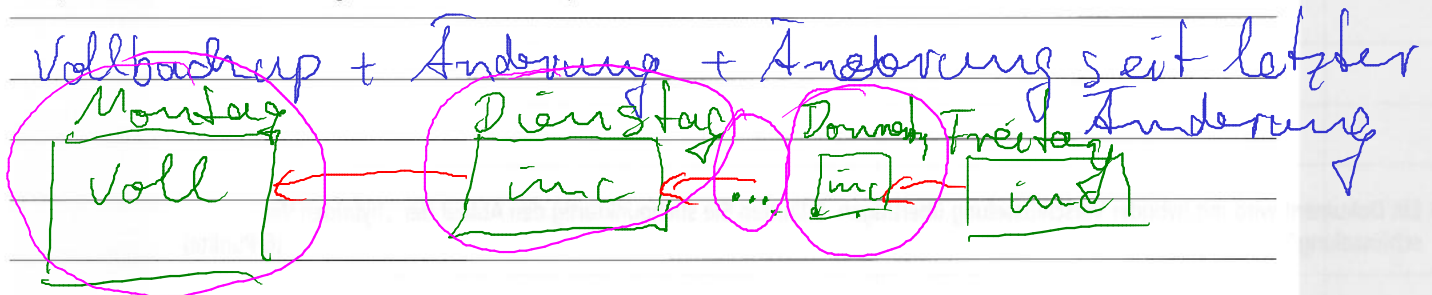
cb) Erläutern Sie stichwortartig differentielles Back-up.

(2 Punkte)



cc) Erläutern Sie stichwortartig inkrementelles Back-up.

(2 Punkte)



In der MED GmbH soll zukünftig auch die Gesundheitskarte zum Einsatz kommen. In diesem Zusammenhang sollen Sie den Ärzten untenstehende Fragen zu Datensicherheit und Datenschutz beantworten, die die Ärzte zu folgendem Text haben.

Die elektronische Gesundheitskarte

Wie werden Gesundheitsdaten in Zukunft geschützt?

...

Hauptfunktionen

Die Prozessor-Chipkarte hat zwei Hauptfunktionen. Erstens fungiert sie als Authentifizierungswerkzeug. Dazu legt jeder Karteninhaber vor Erstverwendung eine persönliche Identifikationsnummer (PIN) nach Wahl fest. Die eigene PIN wird in verschlüsselter Form auf der Karte gespeichert.

...

Die zweite Funktion der Prozessorkarte ist die Durchführung der kryptografischen Verschlüsselungen aller Gesundheitsdaten des Versicherten. Einmal verschlüsselt, sind die Daten geschützt, unabhängig davon, wo sie sich gerade befinden. Alle Verschlüsselungen, die mit der Karte ausgeführt werden, sind vom Typ hybride Verschlüsselung.

...

Der geheime Schlüssel

Dass die gesundheitsrelevanten Informationen eines Versicherten geheim bleiben, steht und fällt mit der Geheimhaltung des privaten Schlüssels der elektronischen Gesundheitskarte. Deshalb hat man alle notwendigen Maßnahmen angewandt, um den Schutz des privaten Schlüssels des Patienten zu gewährleisten.

...

Komplexer Schlüssel

Der Schlüssel wird so komplex wie möglich gewählt: Seine Länge beträgt im Moment 2.048 Bit.

...

aa) Was wird als Authentifizierung bezeichnet?

(2 Punkt)

Nachweis der Identität

ab) Welche Rolle spielt die PIN bei der Authentifizierung?

(4 Punkte)

- Persönliche Identifikationsnummer
- ein Teil / Merkmal der 2FA, darf nur dem Patienten bekannt sein

b) Ein Dokument wird mit hybrider Verschlüsselung übertragen. Erläutern Sie stichpunktartig den Ablauf der „hybriden Verschlüsselung“.

(6 Punkte)

- Daten werden mit symmetrischen Verfahren verschlüsselt
- Der symmetrische Schlüssel wird mit dem öffentlichen (asymmetrischen) Schlüssel des Empfängers verschlüsselt
- verschlüsselte Daten + verschlüsselter symmetrischer Schlüssel werden übertragen
- Empfänger kann mit privatem Schlüssel den sym. Schlüssel entschlüsseln

- c) Sie sollen die symmetrische Ver- und Entschlüsselung mit einem 8 Bit-Schlüssel unter Verwendung des XOR-Operators demonstrieren. Verwenden Sie hierzu den nachstehend abgebildeten Auszug aus der ASCII-Tabelle.

Korrekturrand

ca) Verschlüsseln Sie in folgender Tabelle den Buchstaben „H“.

(4 Punkte)

Ausgangsinformation			Schlüssel	Verschlüsselte Informationen		
Zeichen	ASCII-hex	ASCII-bin	0000 1010	ASCII-bin	ASCII-hex	Zeichen
H	48	0100 1000 ~~0000 1010~~ 0100 0010	0000 1010	0100 0010 4 2	42	B

cb) Entschlüsseln Sie in folgender Tabelle den Buchstaben „z“.

(4 Punkte)

Ausgangsinformation			Schlüssel	Verschlüsselte Informationen		
Zeichen	ASCII-hex	ASCII-bin	0000 1010	ASCII-bin	ASCII-hex	Zeichen
s	73	0111 0011	0000 1010	0111 1001 ~~0000 1010~~ 0111 0011 7 3	7A	z

ASCII-Tabelle (Auszug)

Zeichen	ASCII-hex	Zeichen	ASCII-hex	Zeichen	ASCII-hex	Zeichen	ASCII-hex
A	41	N	4E	a	61	n	6E
B	42	O	4F	b	62	o	6F
C	43	P	50	c	63	p	70
D	44	Q	51	d	64	q	71
E	45	R	52	e	65	r	72
F	46	S	53	f	66	s	73
G	47	T	54	g	67	t	74
H	48	U	55	h	68	u	75
I	49	V	56	i	69	v	76
J	4A	W	57	j	6A	w	77
K	4B	X	58	k	6B	x	78
L	4C	Y	59	l	6C	y	79
M	4D	Z	5A	m	6D	z	7A

OR

A	B	A ∨ B
0	0	0
0	1	1
1	0	1
1	1	1

XOR

A	B	A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

AND, OR,
XOR, NAND
NOT