Prüfungsamt
Fachbereich Wirtschaftswissenschaften

Professur/Chair:Deutsche Telekom Chair for Mobile Business & Multilateral Security

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Winter Semester 2012/13

Matrikelnummer: *Student ID:*

Bitte auch auf jedes Lösungsblatt oben rechts eintragen! *Please also record this on each page in the top right corner!*

Modulkürzel/ *Module Code*: INKO

Themensteller/*Lecturer:* Dr.Martin Reichenbach

Modultitel/*Module Title:* Information and Communication Technologies: Infrastructure, Technology and Business Models

Wichtig: **Durch Ihre Unterschrift in der Teilnehmerliste bestätigen Sie, folgende Prüfungsvorschriften zu beachten:**

- Sie haben den nachfolgenden Text gelesen und stimmen allen Punkten zu.
- Sie fühlen sich gesund und sind in der Lage, an der Prüfung teilzunehmen.
- Sie haben sich über die Vorschriften der PO, die Teilnahme an Klausurprüfungen betreffend, informiert.
- Sie haben zur Kenntnis genommen, dass Sie für die ordnungsgemäße Abgabe der Klausur vor Verlassen des Prüfungsraumes selbst verantwortlich sind. Dazu gehört, dass Sie auf Ihrem Platz bleiben, bis alle Klausuren eingesammelt sind, und den Prüfungsraum nicht verlassen, bevor die Klausuren gezählt und die Vollständigkeit festgestellt wurde.
- Es sind folgende Hilfsmittel erlaubt:

  _____
- Das Mitbringen eines Mobiltelefons oder anderer elektronischer Kommunikationsmedien in die Klausur ist verboten. Zuwiderhandeln gilt als Täuschungsversuch.
- Bitte lassen Sie ausreichend Korrekturrand, und schreiben Sie **nicht** mit Bleistift oder roter Tinte.

Im Falle einer **Erkrankung** während der Klausur beachten Sie bitte:

1. Vermerken Sie die Erkrankung in Ihrer Klausur (Unterschrift!) und informieren Sie die Aufsicht unverzüglich.
2. Geben Sie die Klausur und alle Prüfungsblätter ab und achten Sie darauf, daß die Abgabe in der Anwesenheitsliste vermerkt wird.
3. Falls Sie Hilfe benötigen, wenden Sie sich an die Aufsicht.
4. Gehen Sie **unmittelbar** zum Arzt und reichen Sie innerhalb von drei Arbeitstagen ein Attest, das Ihnen die Prüfungsunfähigkeit bescheinigt, beim Prüfungsamt ein.
5. Bei **wiederholter Erkrankung** im selben Studienabschnitt ist ein **amtsärztliches** Attest erforderlich, das die Prüfungsunfähigkeit bescheinigt:
   - Lassen Sie sich von der Aufsicht oder im Prüfungsamt ein Aufforderungsformular zur Vorstellung beim Amtsarzt geben.
   - Suchen Sie den Amtsarzt am selben Tag oder am nächsten Arbeitstag auf.

Important: **with your signature on the signature list you confirm to comply with the following examination requirements**

- You have read the follow text and agree to all points.
- You feel healthy and able to participate in the examination.
- You have informed yourself with the examination regulations regarding the participation of exams.
- You have taken notice that you are responsible to hand in your examination orderly before you leave the examination room. This includes that you remain quietly seated until all examinations have been counted and it is determined that all examinations have been submitted.
- The following resources and aids are allowed:

  _____
- Carrying mobile phones or other electronic communication devices during the exam is forbidden. Violating this rule will be counted as an attempt to cheat.
- Please leave sufficient space in the margin for marking, please do **not** write with a **pencil** or **red ink**.

In case you fall ill and become unfit for examination during the course of examination please note the following:

1. Please record this in writing including your signature on your examination documents and inform an invigilator immediately.
2. Submit your examination and all examination documents and ensure that the information is declared on the signature list.
3. In case you need help please inform an invigilator.
4. Please see a doctor immediatley on the day on which you discontinued the examination. Submit the required medical certificate which confirms your inability to participate in the examination to the examination office within 3 working days.
5. In case of **repeated illness** during the same official aera of study you are required to to submit a medical certificate from a public **health medical officer:**
   - Please collect the medical examination request form for the public health medical officer from an invigilator or the examination office.
   - Please go and see a public health medical officer on the same day or on the next working day.

Bitte für die Korrektur freilassen! / *Please leave blank for grading purposes!*

Ergebnis/*Result*:

Aufgabe/Question:	1	2	3	4	5	6	7	Summe/Sum
Punkte/Points:								

Punkte ***Points***	**Note** ***Grade***	**Unterschrift des Prüfers** ***Examinar's Signature***

Exercise 1: Authentication (15 Points)

a) Alice is a customer of the *Bank of Duckburg* and she regularly uses online banking. She receives an e-mail with the subject „Bank of Duckburg – Please update your personal information“. In the text of the e-mail she is informed that a system maintenance has been performed and that she should login to the online banking platform and enter 10 transaction numbers from her TAN-list. Below this text, there is a hyperlink with the title “Bank of Duckburg - Online Banking Portal - Login“. Alice clicks on this link. On the website that appears, Alice enters her login credentials and clicks on „Login“. A few seconds later, the browser automatically gets redirected to a page where she enters the TAN numbers.

With a high probability, to what kind of attack Alice has fallen victim. Name and describe two security measures that would secure her online banking system against such kind of attacks (**10 points** total, 2 for naming the attack, 2 for naming of the countermeasures and 2 for describing them each)?

Alice ist Kunden der D-Bank und nutzt regelmäßig Onlinebanking. Sie erhält eine Email mit dem Thema "D-Bank - Bitte aktualisieren Sie Ihre persönlichen Daten". Im Text der Email wird sie darüber informiert, dass aus Wartungsgründen ein Update durchgeführt wurde und sie sich anmelden sollte, um die Korrektheit ihrer persönlichen Daten zu überprüfen und 10 TAN-Nummern zur Sicherung Ihrer Transaktionen eingeben . Unter diesem Text ist ein Hyperlink sichtbar mit dem Titel "D-Bank - Online Banking Portal - Login". Alice klickt auf diesen Link, und auf der folgenden Webseite gibt sie ihren Nutzernamen und ihre Kennung ein. Ein paar Sekunden später wird der Browser automatisch auf eine Seite weitergeleitet, auf der sie die 10 TAN-Nummern eingeben soll.

Welcher Angriffsart ist Alice wahrscheinlich zum Opfer gefallen? Nennen und beschreiben Sie zwei Sicherheitsmaßnahmen, die Ihr Online Banking gegen solche Angriffe schützen könnten.

Attack: TAN Phishing.

Security Measures

Mobile TAN (sending SMS with TAN to mobile phone)

Photo-TAN (encrypting transaction details plus TAN on the banking server and showing it on the screen, the user scans it with a banking app on the smartphone, decrypts it, let customer confirm the transaction data, and enter the decrypted TAN into the browser)

c) What is a challenge-response technique? Describe shortly how it works and its main advantage. (5 **points**)

Was ist eine Challenge Response Technik? Beschreiben Sie kurz, wie sie funktioniert und zeigen sie ihren bedeutendsten Vorteil.

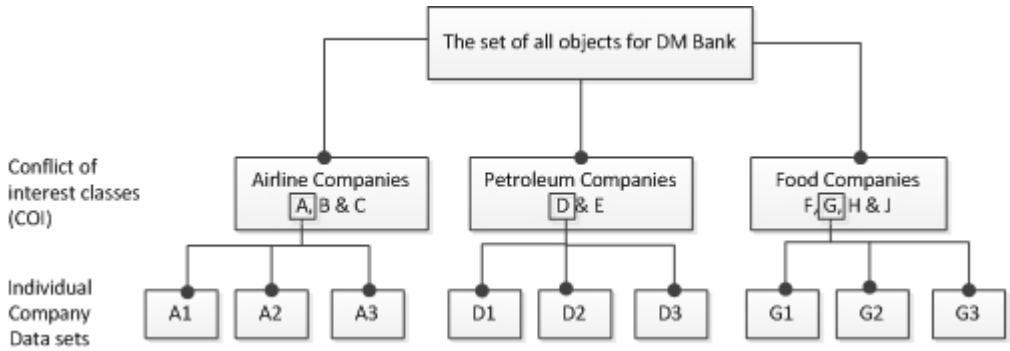
aus SS12

Exercise 2: Access Control (12 Points)

After successfully graduating from your studies, you get a job at an investment bank. There you quickly realize that the security policy of the bank is based on the Chinese Wall model, which you have learnt during your studies. Consider the database of the investment house given below. It consists of companies’ records about

investment data. The following *Chinese Wall Model* shows the datasets for each company in the database and the conflict of interest (COI) classes.

Nach erfolgreich absolviertem BWL-Studium schaffen Sie den Direkteinstieg in eine Investmenbank. Dort finden Sie die Datenbank mit Kunden-/Unternehmensdaten in Bezug auf Investmentaktivitäten und Sie erkennen auf Anhieb, dass die Security Policy der Bank auf dem *Chinese Wall Modell* basiert, das sie bereits während ihres Studiums kennen gelernt haben. Das folgende Modell zeigt die Datensätze für jedes Unternehmen in der Datenbank und die Conflict of Interest Klassen (COI).



a) You receive your first tasks and access provisions. At this moment, are there any access restrictions to objects? Are there any objects, where you now have access to due to the Chinese Wall policy? (**3 Points**)

Sie stehen kurz vor ihrem ersten Arbeitsauftrag und Systemzugriff. Gibt es zum jetzigen Zeitpunkt Objekte, auf die Sie grundsätzlich wegen der Chinese Wall Policy zugreifen dürfen? Nennen Sie diese Objekte? (**3 Punkte**)

Yes, all, because there are no restrictions from other tasks so far.

b) Let us assume that you as your first task gain access to Airline Company A's data sets first; at this stage, you possess information concerning Airline Company A's data sets. Can you gain access to Petroleum Company D's data set? Justify your answer (**3 points**).
Nehmen Sie an, dass Sie ale ersten Arbeitsauftrag Zugriff auf die Daten der Airline A bekommen. Können Sie daraufhin auch auf Daten der Petroleum Firma D zugreifen? Begründen Sie ihre Antwort. (**3 Punkte**)
Ja, weil in einem anderen COI class.

c) What is the minimum number of analysts (including you) needed to access the data sets from all companies in the Petroleum and Food Companies Classes (**3 points**)?
Wieviele Analysten (inklusive Ihrer Person) müssten es sein, um die Datensätze aller Unternehmen der Klasse "Petroleum" und "Food" zugreifen zu können? (**3 Punkte**)
5

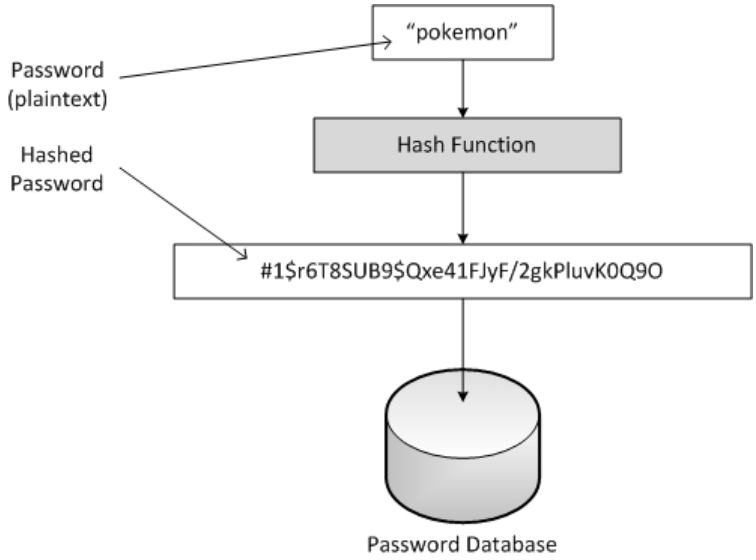
d) Let's assume now that besides Airline Company A, during your work you gain access also to Food Company G. Name all the companies' data sets in all COI classes, where you can get access (now or in the future) (**3 points**).
Nehmen wir an, dass Sie neben der Airline A während Ihrer Arbeitstätigkeit auch Zugriff auf die Nahrungsmittelfirma G erhalten. Nennen Sie alle Unternehmen in allen COI Klassen, auf die Sie jetzt

oder in Zukunft Zugriff hätten. (**3 Punkte**)
A1, A2, A3, G1, G2, G3

Exercise 3: Cryptography / Electronic Signatures (10 Points)

Typically computer systems don't store passwords in plaintext (in their original form), because if the attacker can somehow get to where they're stored, he has access to all the passwords. A more secure way is to store a hash of the password, rather than the password itself. This is depicted in the figure below.

Typischerweise speichern Computer Passworte nicht im Klartext (in ihrer ursprünglichen Form), weil ein Angreifer, sobald er Zugriff auf diesen Rechner bekäme, dann auch Zugriff auf alle Passworte im Klartext hätte. Ein sicherer Weg ist es, einen "HASH" als Fingerabdruck des Passwortes zu speichern. Dieses Vorgehen sehen Sie im folgenden Bild.



a) Assess and decide whether this is more secure. How much more? Explain how someone who gets access to the database and retrieves the hash values could find out the passwords of the users (**4 points)**.

Bewerten und entscheiden Sie, ob dieses Vorgehen sicherer ist. Wieviel sicherer? Erklären Sie, warum/wie jemand mit Zugriff auf die Datenbank mit dem Hashwerten auch die ursprünglichen Passworte herausfinden könnte. (**4 Punkte**)
Es ist sicherer, das Geheimnis "Passswort "wird so nicht im Klartext gespeichert. Wenn aber jemand Zugriff auf die Hashwerte bekommt, kann er durch Brute Force und Dictionary Attacks aus den Hashwerten auf die zugrundeliegenden Passworte zurückschließen.

b) Due to which attack scenario, conducted using public key systems, does the need for certification emerge? Name and describe in detail, how such an attack would work (**6 points,** 2 points for naming, 4 for describing).

Welcher Angriff, der mittels öffentlicher Schlüssel durchgeführt werden kann, macht Zertifizierung notwendig? **Name and describe in detail, how such an attack would work** (**6 points,** 2 Punkte fürs Nennen, 4 Punkte fürs Beschreibung).

MitM-Angriffe, um die zu verhindern, wird eine Zertifizierung nötig.

.

See Lecture Slides.

Exercise 4: Cryptography / Electronic Signatures (10 Points)

a) Use the Vigenère Chiffre to decrypt the word “ZGCTRGZGKWV” by using the key “SEC” **(5 points).**

Verwenden Sie die Vigenère-Chiffre für die Entschlüsselung des Wortes “ZGCTRGZGKWV” und verwenden Sie dabei den Schlüssel “SEC” **(5 Punkte).**

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Z	G	C	T	R	G	Z	G	K	W	V
S	E	C	S	E	C	S	E	C	S	E
H	C	A	B	N	E	H	C	I	E	R

b) Which approach is used to bypass the inherent challenges/weaknesses of symmetric and asymmetric cryptography? Name the approach and describe a setup for a generic and secure Client Server Communication protocol. Use current symmetric and asymmetric cryptosystems to depict your solution. (**5 points**: 1 point for naming, 4 points for describing the example)

Welchen pragmatischen Ansatz wählen Designer von Sicherheitslösungen, um die logistischen Probleme der Verwendung symmetrischer und asymmetrischer Kryptografie zu umgehen? Nennen Sie den Ansatz und beschreiben Sie die Vorgehensweise anhand eines allgemein verwendbaren, sicheren Protokolls für Client-Server-Kommunikation anhand je eines gängigen symmetrischen und asymmetrischen Algorithmusses (5 **Punkte:** 1 Punkte fürs Nennen, 4 Punkte fürs Beispiel)..

Antwort: Hybridverfahren, die jeweiligen Nachteile ausschließen (Nachteile sichere Schlüsselverteilung bei Symm., Performance bei asymm. Kryptosystemen).

Symmetrisch: AES, Triple DES; Asymmetrisch: RSA, Elliptic Curve

Antwort: 1) Schlüsselerzeugung symm. 2) Verschlüsselung der Nachrichten mit symm

Schlüssel 3) Anforderung Public Key des Empfängers 4) Schlüsselverteilung des symm.

Keys per asymm. Krypto, d.h. Versenden des mit dem Symm. Schlüssel verschlüsselten

Nachricht PLUS des mit dem Public Keys des Empfänger verschlüsselten Symm.Keys an

Empfänger 5) Der Empfänger entschlüsselt das Paket mit seinem Privaten Schlüsselteil, er-

hält so den Symmetrischen Schlüssel zur Entschlüsselung der ursprünglichen Nachricht.

Exercise 5: Data Protection & Privacy (9 Points)

a) Different „Privacy Enhancing Technologies (PET)“ were introduced in the lecture. Name and describe three exemplary threats from the current News, against which these PETs are suitable to secure your Privacy and Identy (**9 points**; 1 point for naming, 2 for describing per threat).

Sie haben ein Semester lang regelmäßig die Vorlesung Informations- und Kommunikationssicherheit besucht. Jetzt beschließen Sie, Ihre eigene Identität und Privatsphäre im Internet besser zu schützen. Gegen welche Bedrohungen helfen diese Techniken. Nennen Sie exemplarisch 3 z.B. In den Medien aktuell kommunizierten Bedrohungen, gegen die man sich mit den in der Vorlesung vorgestellten Privacy Enhancing Technologies. Schützen kann.

PRISM (Programm zur Überwachung und Auswertrung von elektronischen Medien und elektronisch gespeicherten Daten, ermöglicht eine umfassende Überwachung von Personen die digital kommunizieren, u.a. Durch Zugriff auf ihre live geführte Kommunikation

Tempora (im Rahmen des Programmes werden Internetknotenpunkte und transatlantische Datenverbindungen angezapft und die Daten gespeichert. Emails, Einträge in Soziale netzwerke, sowie Telefongespräche.

Xkeystore (Ausspähen des Google-Suchverhaltens, Speicherung der Verbindungdaten und zT de Kommunikationsinhalte).

Exercise 4: Identity Management (10 Points)

a) The categorization of Identity Management Systems can be based on the three-tier model introduced by Durand (Tier 1-3 Identities). Name these three tiers (**2 points**) and give a brief description what factor distinguishes the three identity tiers from each other? (**4 points)** Describe, based on this factor, how the three tiers are different from each other. **(4 Points)**
Der Klassifizierung von Identitätsmanagementsystemen liegen die verschiedenen Schichten der Identität nach Durand zugrunde („Tier 1-3 Identities"). Nennen und beschreiben Sie diese kurz. (2 Punkte) In Bezug auf welchen Faktor unterscheiden sich die verschiedenen Schichten der Identität voneinander? (4 Punkte) Erläutern Sie anhand dieses Faktors, wie sich die Schichten voneinander abgrenzen. (4 Punkte)

1) Tier 1: True („My") Identity / Tier 2: Assigned („Our") Identity / Tier3: Abstracted („Their") Identity (2 Points)
2) Kontrolle (2 Points)
3) Tier 1 Identity wird komplett vom Individuum kontrolliert. Die Tier 2 Identität kann nur zum Teil vom Individuum kontrolliert werden (die Attribute der Tier 2 Identität sind dem Individuum allerdings bekannt). Die Tier 3 Identität kann nicht vom Individuum kontrolliert werden (das Vorhandensein einer Tier 3 Identität kann, muss aber nicht zwingend, dem Individuum bekannt sein). (4 Punkte)

Exercise 5: Biometrics (8 Points)

a) Given a biometric system with a *False Acceptance Rate (FAR)* of 0,05. With 50 authentication attempts, what is the probability that a person gets falsely accepted at least one time? Gegeben sei ein biometrisches Authentifikationssystem mit einer False Acceptance Rate (FAR) von 0,05. Wie hoch ist die Wahrscheinlichkeit bei 50 Authentifizierungsversuchen, dass eine unautorisierte Person mindestens einmal akzeptiert wird?**(8 points)**

$p(n) = 1 - (1-p)^n$
$p = FAR = 0,05$
$n = 50$
$p(50) = 1 - (1 - 0,05)^{50} = 0,92 = 92\%$

Exercise 6: Computer System Security (8 Points)

a) What can cause a Buffer Overflow and what would be the effect on the procedure call stack? Please explain in detail, how an attacker could (mis)use a Buffer Overflow to perform his attack **(6 points)** **Was kann einen "Buffer Overflow" verursachen und was würde der Effekt auf den "Programmausführungs-Stack" sein? Bitte erklären Sie detailliert, wie ein Angreifer den Buffer overflow "miss"brauchen könnte, um einen Angriff erfolgreich auszuführen?**

- Moving a value which is larger than the space allocated for a variable. A part of the 'larger' value contains malicious code (4 points)
- It would overwrite the return address in the procedure call stack (4 points)

Exercise 7: Network Security (12 Points)

a) You want to avoid connecting your corporate web server directly to the corporate local area network (LAN). But you still want it to be accessible from the Internet and from the corporate LAN. Sketch how such an infrastructure could look like. Please consider the concept of a DMZ. Label the used components, networks, and zones (6 **points)**.
Sie wollen Ihren Unternehmens-Webserver direkt ans Unternehmensnetzwerk (LAN) anschließen. Er soll aber trotzdem gleichzeitig vom Internet und vom Unternehmensnetz aus zugreifbar sein. Skizzieren Sie, wie solch eine Infrastruktur sicher aufgestellt werden könnte. Beachten Sie den Einsatz einer DMZ bei Ihrer Architektur. Kennzeichnen Sie die skizzierten Komponenten, Netzwerke und -zonen).

b) How content confidentiality is achieved in GSM communication? Sketch how the session key is derived. **(6 points)**
Wie wird die Vertraulichkeit des Inhalts bei der Kommunikation über GSM gewährleistet? Skizzieren Sie, wie der Sitzungsschlüssel gewonnen wird.

The content is transmitted in an encrypted form between the subscriber and the network operator (1 point).

In the figure: Shared secret key Ki(1 point), rand (1 point), transmission of the rand from the network to SIM (1 point), showing the combination of Ki and rand (1 point)
No algorithm name or key length is required!

c)