Stand:20.04.2015

Prüfungsamt
Fachbereich Wirtschaftswissenschaften

Professur / Chair: Mobile Business and Multilateral Security

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Sommersemester / *Summer Semester* 2016

Matrikelnummer / *Student ID number:* _____

Bitte auch auf jedes Blatt oben rechts eintragen! / *Please also write on each page top right.*

Modulkürzel / *Module Code*: MOB2

Prüfer / *Examiner:* Prof. Dr. Kai Rannenberg

Modultitel /*Module Title:* Mobile Business II Application Design, Applications, Infrastructures, and Security

Wichtig: **Durch Ihre Unterschrift in der Unterschriftenliste 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 **Prüfungsordnung**, 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 nur die vom Prüfer zugelassenen **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 auf Ihrer Klausur und unterschreiben dies. Informieren Sie die Aufsicht unverzüglich und **erklären Sie ausdrücklich den Abbruch der Klausur wegen Erkrankung**.
2. Geben Sie die Klausur und alle Prüfungsblätter ab und achten Sie darauf, dass die Abgabe in der Unterschriftenliste vermerkt wird.
3. Falls Sie Hilfe benötigen, wenden Sie sich an die Aufsicht.
4. Gehen Sie am Tag des Prüfungsabbruches **ohne Verzögerung** zum Arzt und reichen Sie **unverzüglich** ein Attest beim Prüfungsamt ein. Bitte verwenden Sie hierfür das vom Prüfungsamt vorgegebene Formular.
5. Wenn Sie trotz gesundheitlicher Probleme Ihre Klausur mitschreiben und abgeben, geht das Risiko einer eventuell verminderten Prüfungsleistung zu Ihren Lasten.

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

- You have **read the following text** and **agree to all points**.
- You feel **healthy** and able to take the examination.
- You have informed yourself about the **exami-nation regulations** regarding the participation in 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 collected and don't leave the room until the examinations have been counted and it is determined that all examinations have been submitted.
- Only the **resources** and aids approved by the examiner are allowed.
- Carrying **mobile phones** or other electronic communication devices during the exam is forbidden. Violating this will be counted as an **attempt to cheat**.
- Please leave sufficient space in the margin for marking and please do **not** write with a **pencil** or **red ink**.

In case of **illness** 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 of your discontinuance due to illness explicitly**.
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 **without delay** on the day on which you discontinued the examination and submit the required medical certificate to the Examination Office **immediately**. Please use the form prescribed by the Examination Office.
5. If you write and hand in your examination despite your health problems, the risk of eventual diminished examination performance will be at your own expense.

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

Ergebnis */ Result*	**Aufgabe** */ Question*	1	2	3	4	5	6	7	8	9	10	**Summe** */ Sum*
	Punkte */ Points*											

Punkte *Points*	**Note** *Grade*	**Unterschrift des Prüfers** *Signature of the Examiner*

Question 1: Mobile Surveillance and Data Protection (15 Points)

1 A) There is a variety of different types of telecommunication surveillance methods. Name four types of these telecommunication surveillance methods.
(2 points)

- *Eavesdropping (0.5P)*
- *Storage and analysis of connection data (0.5P)*
- *Automated content analysis (BND) (0.5P)*
- *Identification of mobile phone users and eavesdropping (IMSI Catcher) (0.5P)*
- *Data retention (0.5P)*
- *Determination of the location of callers (0.5P)*

(0.5 points per surveillance method)

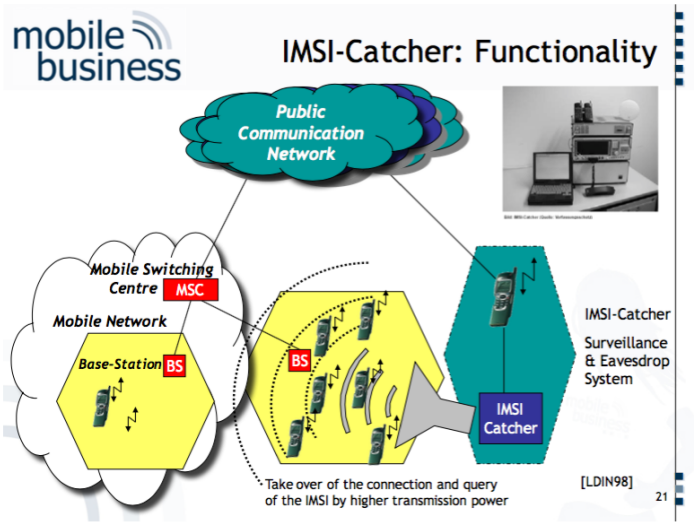
1 B) Why do governmental organizations carry out telecommunication surveillance?
(2 points)

- fight organized crime, i.e. for investigation and prevention
- socio-political goals, i.e. protect democracy from extremists, from foreign intelligence services or keep up the preparedness of the military service

(1 point per reason)

1 C) Explain the IMSI-Catcher in detail. You can also draw a schematic for your explanation. What problems arise with the use of this method?
(6 points)

- Explanation: The IMSI-Catcher simulates a strong base station, causing all mobile phones in the network of the respective operator to connect to this simulated base station. The person to be observed can be identified via the IMSI of the SIM, which can be queried at the mobile operators' databases (if the operator is in a cooperating country). The communication basically gets intercepted. (4P for explanation or schematic with explanatory notes)



- Problems:
  - Are due to the constitution due to the rerouting of phones of persons that are not being observed and (1P)
  - ...due to technical interferences between the IMSI catcher and normal base stations (1P)

(4 points for the description and 2 points for the problems)

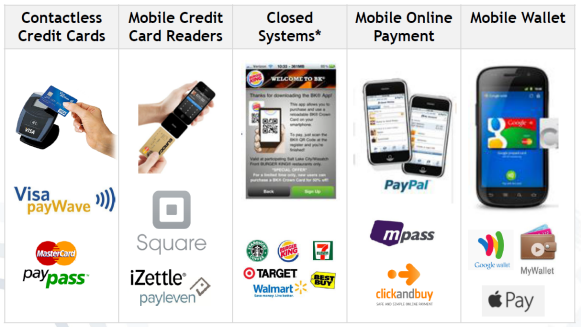
1 D) Name five of the nine principles of the EU privacy law. Describe them briefly. (5 points)

- Intention and notification: The processing of personal data must be reported in advance to a Data Protection Authority. (1P)
- Transparency: The person involved must be able to see who is processing her data for what purpose. (1P)
- Finality principle: Personal data may only be collected and processed for specific, explicit and legitimate purposes. (1P)
- Legitimate grounds of processing: The processing of personal data must be based on a foundation referred to in legislation, such as permission, agreement, and such. (1P)
- Quality: Personal data must be as correct and as accurate as possible. (1P)
- Data subject's rights: The parties involved have the right to take cognisance of and to update their data as well as the right to raise objections. (1P)
- Processing by a processor: This rule states that, with the transfer of personal data to a processor, the rights of the data subject remain unaffected and that all restrictions equally apply to the processor. (1P)
- Security: A controller must take all meaningful and possible measures for guarding the personal data. (1P)
- Transfer of personal data outside the EU: The traffic of personal data is permitted only if that country offers adequate protection. (1P)

(1 point per principle with short description)

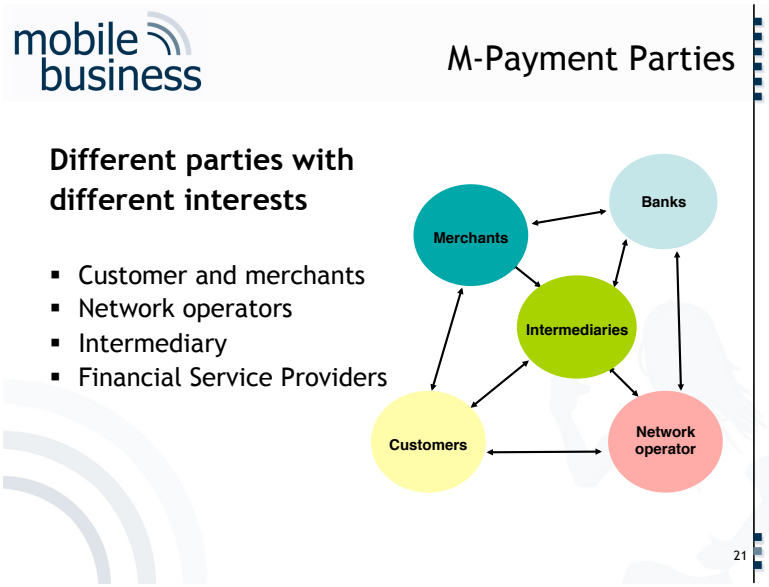
Question 2: Mobile Payment (10 Points)

2 A) Identify the five different types of mobile payment services and name one example product and provider for each type.
(5 points)



(0,5 points per type, 0,5 per example)

2 B) Name the five different parties that are typically involved in a "mobile payment" scenario and describe their different interests in bullet points.
(5 points)



Customers: Only a small number of (trustworthy) parties should have access to personal financial data.

Merchants: Accepted payments should be enforceable.

Network operators: Offering of new (security-relevant) services (e.g. billing services)

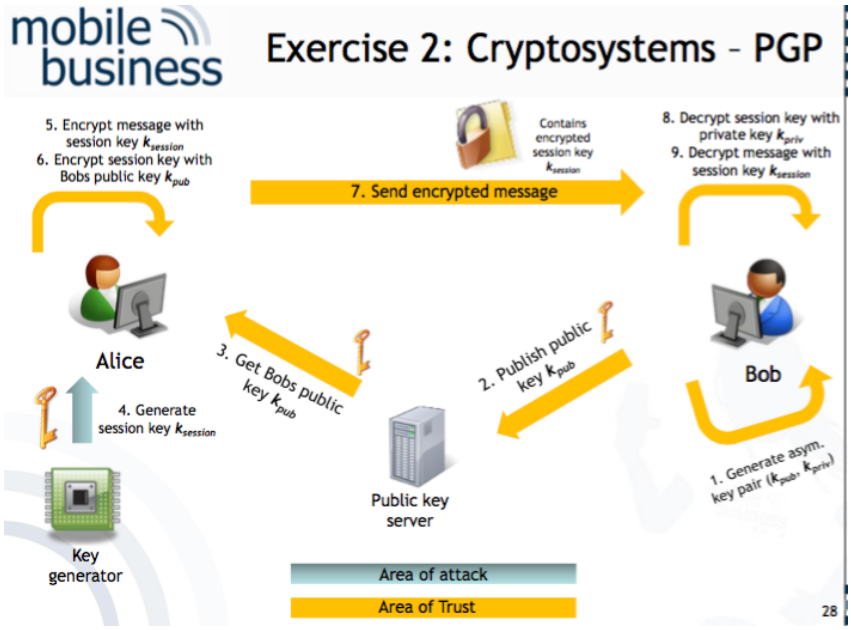
Banks: Controlling the payment-process

Central Banks: No direct C2C payments to avoid a shadow currency

(1 point per party and description of interests)

Question 3: Cryptography (7 Points)

3 A) Imagine you want to confidentially send an e-mail. For that purpose, you use a hybrid cryptosystem. Explain the process of a hybrid cryptosystem in a few steps that are required for an encrypted e-mail communication.
(4,5 points)



(0,5 points per step)

3 B) Name advantages and disadvantages of symmetric and asymmetric cryptosystem. You can get 0.5 points per advantages or disadvantage with a maximum of 2.5 points for the whole exercise.
(2,5 points)

Symmetric cryptosystem:

Advantages:

- Algorithms are very fast

Disadvantages:

- Complex key exchange

Asymmetric cryptosystem:

Advantages:

- No secret must be shared
- Only one key per endpoint

Disadvantages:

- Algorithms are very slow
- Man-in-the-middle-attack

Question 4: The Privacy Paradox (13 Points)

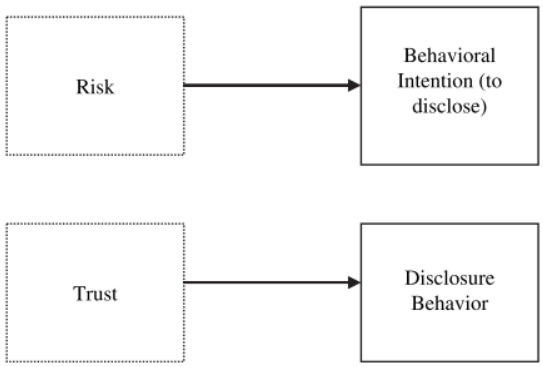
The article by Norberg et al. (2007) with the title „The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors“ from the Journal of Consumer Affairs was discussed among other articles in the first exercise.
(13 points)

4 A) What is the research problem or the research question of the article?
(1 points)

The purpose of this exploratory study is to investigate whether people say one thing (intend to limit disclosure) and then do another (actually provide personal details) during marketing exchanges.

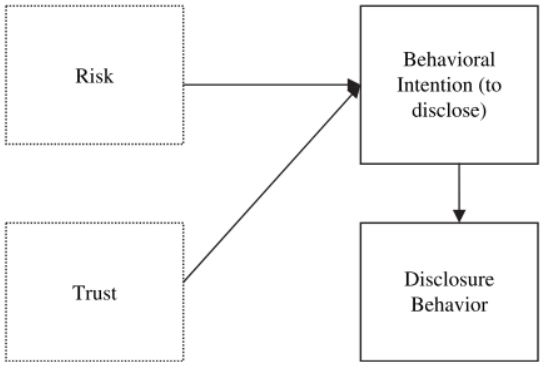
4 B) Sketch and explain briefly the underlying theoretical model that is the basis of the research. How is the new model different to the previous models?
(4 points)

FIGURE 2
Conceptual Model—Privacy Paradox



It is argued by the authors that behavioral intention is not predictive of actual behavior because risk influences one’s intention to disclose, while a trust heuristic operates in actual disclosure contexts. (2P)

FIGURE 1
Conceptual Model of Disclosure Based on Previous Research



Whereas the more traditional model shows that both risk and trust influence behavioral intentions that would then influence actual behavior, we argue that this is not the case. (2P)

(2 points for the explanation of the underlying research model, including the relation of the constructs and 2 points for the previous figure or a detailed comparison between the models.)

4 C) The tables shown below from the article display the results of the statistical tests for hypothesis 1 and hypotheses 2 and 3. Please state the three tested hypotheses. Discuss and justify whether the hypotheses are met based on the tables.
(6 points)

TABLE 3
Study 2 Hypotheses 1 Results: Differences between Intended and Actual Disclosure

Condition	Mean (SD)—Items Willing to Disclose (Phase 1)	Mean (SD)—Items Actually Disclosed (Phase 2)	*t*-Statistic	Significance	Effect Size
Overall	10.49 (3.10)	15.16 (1.15)	−10.02	$p = .001$	.65
Bank	10.38 (3.17)	15.13 (1.21)	−7.41	$p = .000$	.64
Pharma	10.65 (3.07)	15.22 (1.09)	−6.66	$p = .000$	.67

TABLE 4
Study 2, Hypotheses 2 and 3: Regression Results for Risk and Trust Relationships

IV	DV	R^2	df	Beta	*F*	*p*
Risk	Intention to disclose	.118	53	−.344	6.973	.011
	Actual disclosure	.045	45	−.212	2.075	.157
Trust	Intention to disclose	.026	54	.162	1.428	.237
	Actual disclosure	.011	45	−.104	.486	.489

Note: IV = "Independent Variable" and DV = "Dependent Variable".

H1: Individuals will actually disclose a significantly greater amount of personal information than their stated intentions indicate. H1 is supported which is shown in Table 3. It can be seen from the overall condition that the means of the number of items of the willingness to disclose phase and the actually disclosed phase are to a great extent different with a t-statistic of -10.02 which indicates that these two means are highly statistically significant different from each other with a p-value of .001. (2P)

H2: Risk perceptions will have a significant negative impact on individuals' stated intentions to disclose personal information. The regression result for the risk–intention to disclose relationship was found to be significant ($F = 6.973$, $p = .011$), and the result for the risk–actual disclosure relationship was found to be not significant ($F = 2.075$, $p = .157$). Thus, we found support for H2 as it does appear that risk is salient when asking for behavioral intention responses but is less so in actual disclosure situations. All relationships were in the expected direction (see the beta coefficients for the direction). (2P)

H3: Trust perceptions will have a significant positive impact on individuals' actual personal information disclosure. With regard to H3, it was expected that trust would have a greater positive influence on disclosure behavior than it would on intention to disclose. None of the relationships between trust and the dependent variables were significant. (2P)

(2 points per description of the hypothesis and corresponding results.)

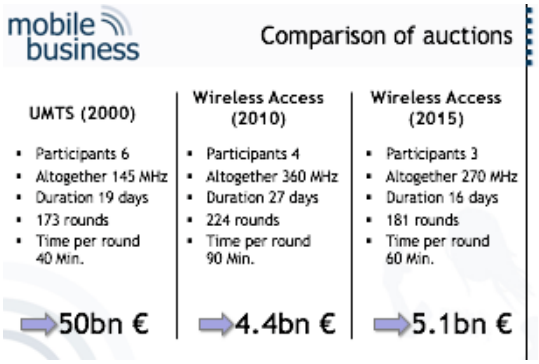
4 D) What is the relationship between the privacy paradox and cryptography and how does it influence the actual privacy of the users?
(2 points)

Due to the findings regarding the privacy paradox it has to be assumed that many people will not practically implement privacy protecting technologies although they might say that privacy is important for them. This leads to a large unprotected population in the internet which allows all kinds of surveillance and tracing actions by different parties like governments, advertisers or criminals.
Furthermore, it challenges the researchers of such technologies even more because they must include these considerations in their product development efforts besides many other important issues like usability and performance.

(2 points per rational explanation.)

Question 5: Regulation (13 Points)

5 A) Using your own words, please compare the outcome of the three German frequency auctions for wireless access from 2000, 2010, and 2015. In doing so, please include a comparison of the following aspects:
- Number of participants
- Aspiration of the bidders (which frequency band was in the focus, their primary interest?)
- The auctions' outcome (resulting licence costs, approximately).
(9 points)



(1.5 points for the correct numbers of participants and 1.5 points for the short comparison; 1.5 points for the correct frequency bands and 1.5 points for presenting the primary interests; 1.5 points for the resulting licence costs and 1.5 for the comparison of the outcomes)

5 B) What are the requirements for purchasing a licence by auction? Please explain briefly.

(4 points)

Four requirements have to be fulfilled:
- Original Proposition in German language and 15 copies + legal prerequisites for the admittance to the auction process have to be fulfilled (Telecommunications Act)
- Notification of the RegTP (approval of the statements to reliability, productivity, competence)
- Deposit (14 days before the auction)
- Bank guarantee (indefinite, unconditional, irrevocable, directly enforceable)

(1 point per requirement, including a short description.)

Question 6: HCI Issues (14 Points)

6 A) List the three main activities in the Mobile Interaction Design, as explained in the lectures and briefly describe each one. (6 points)

- Understanding users (Capabilities & Limitations)
- Developing prototype designs (Demonstration of proposed interaction design)
- Evaluation (Identification of strength and weaknesses of a design)

(1 point per activity and 1 for the short description)

6 B) HCI-Prototypes are built in order to express a design idea as quickly as possible. Describe in your words the differences between a low-fidelity and a high-fidelity prototype.

(8 points)

Low-fidelity prototype design:

- The prototype uses materials different to those in the final incarnation (often paper-based)
- Check for inconsistency
- Give a common specification for the design team (early visualization of design solutions)
- Afford reflection (provoke innovation & improvement)
- Check interaction scenarios

High-fidelity prototype design:

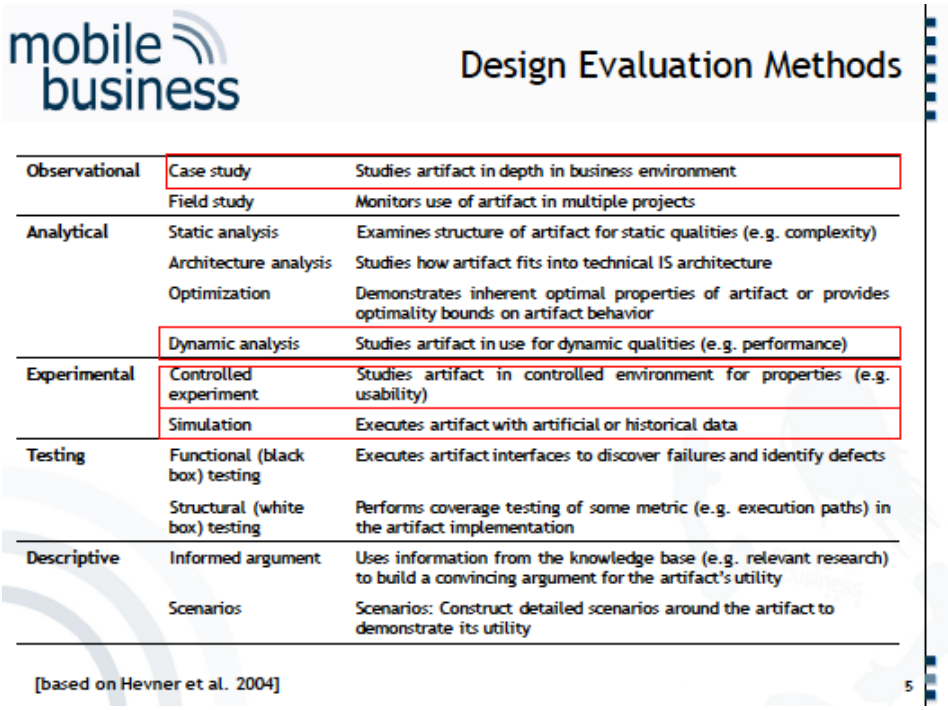
- The results of a low-fidelity prototyping process comprise a list of features that should be tested with representatives of the target group.
- High-fidelity prototype designs provide the functionality to evaluate critical tasks and functionalities that should be supported by the final product.
- Therefore, most critical features must be identified to be included in the prototype design.

Type	Advantages	Disadvantages
Low-fidelity	▪ Less time ▪ Lower costs ▪ Evaluate multiple concepts ▪ Useful for communication ▪ Address screen layout issues	▪ Little use for usability test ▪ Navigation and flow limitation ▪ Facilitator driven ▪ Poor detail in specification
High-fidelity	▪ Partial functionality ▪ Interactive ▪ User-driven ▪ Clearly defined navigation scheme ▪ Use for exploration and test ▪ Marketing tool	▪ Creation time-consuming ▪ Inefficient for proof-of-concept ▪ Blinds users for major representational flaws ▪ Users may think prototype is 'real'

(4 points for the description of the characteristics of low and high fidelity prototypes, 1 point per characteristic, max 2 points per prototype. 4 points for naming advantages & disadvantages, 0.5 for naming an advantage or disadvantage, max. 1 point per category, e.g. Low fidelity – advantages.)

Question 7: Evaluation of Mobile Application & Service Design (6 Points)

List three Design Evaluation Methods, assign them to one of the five categories introduced in the lectures & describe them briefly. (6 Points)



(1 point for naming the design evaluation method and the correct assignment to the corresponding category and 1 point for the short description.)

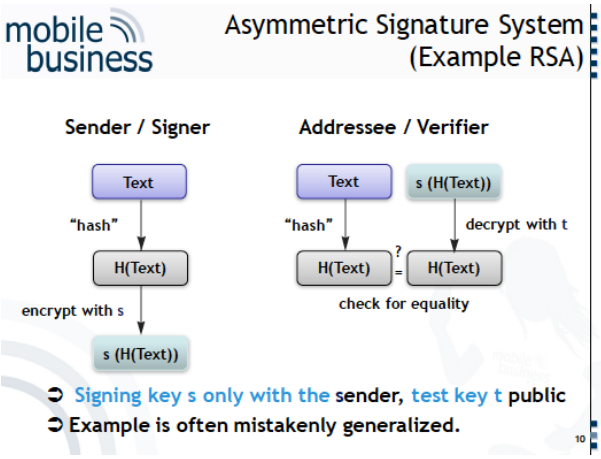
Question 8: Signatures (12 Points)

8 A) What are the requirements concerning electronic signature systems in order to provide the same level of security "traditional" signatures already do? Please name four requirements.

- Uniquely linked to the signatory
- Capable of identifying the signatory
- Created using means that the signatory maintains under his sole control
- Linked to the data to which it relates in such a manner that any subsequent change of the data is detectable

(1 points per requirement.)

8 B) Sketch a figure of a system for asymmetric electronic signatures that uses a hash function and describe how this system works.



(3 points per step (encryption & decryption, respectively) and 2 points for the description of the asymmetric signature system that uses a hash function.)