# Prüfungsamt
# Fachbereich Wirtschaftswissenschaften

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Professur/Chair: Mobile Business and Multilateral Security

Sommer/Summer Semester2013

| 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*: MB2

Themensteller/*Lecturer:*Prof. Dr. Kai Rannenberg

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

**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 | 8 | Summe/Sum |
|---|---|---|---|---|---|---|---|---|---|
| Punkte/Points: | | | | | | | | | |

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

# Question 1: Cryptography (18 Points)

a) Nennen Sie zwei unterschiedliche Arten von Verschlüsselungssystemen.

*Name two different types of encryption systems.*

(2 Points)

Symmetric Cryptography (1 point)
Asymmetric Cryptography (1 point)

b) Nennen Sie einen Vorteil und einen Nachteil für jedes Verschlüsselungssystem.

*Name one advantage and one disadvantage for each of the systems in Section a.*

(4 Points)

1 point for each

| | *Advantage* | *Disadvantage* |
|---|---|---|
| *Symmetric Cryptography* | Fast Algorithm | Difficult Key Exchange |
| *Asymmetric Cryptography* | No Key Exchange Problem | Complex Operations/Very Slow |

c) Stellen Sie sich einen englischen Text vor, der mit der Caesarchiffre verschlüsselt ist. Beschreiben Sie kurz zwei Möglichkeiten, wie man diesen Text entschlüsseln kann, ohne den geheimen Schlüssel zu kennen.

*Imagine an English text encrypted using the Caesar Cipher algorithm. Briefly describe two ways that you can break this cipher text without knowing the secret key.*

(4 Points)

Method 1: Trying all the possible 26 keys and see if the decryption is something meaningful.
Method 2: Count the occurrence of the characters and check it against the statistics for typical English text to find the mapping between the characters. E.g. “E” is the most repeated letter in English text so probably the letter repeated the most in the cipher text is the transformation of “E”.

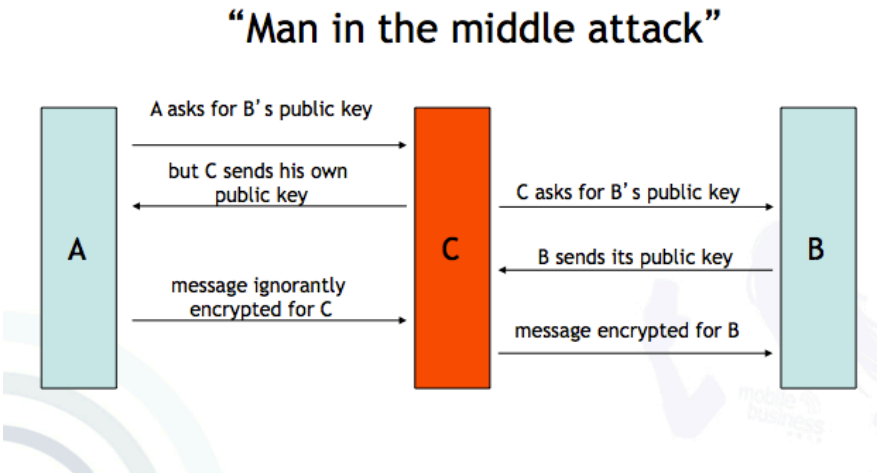
d) Welcher Schaden entsteht durch eine “Man in the middle attack”? Zeichnen Sie ein Interaktions-Diagramm, das zeigt, wie eine “Man in the middle attack” funktioniert.

*What is the damage caused by a “Man in the middle attack”? Show how this attack works by sketching an interaction diagram.*

(8 Points)

Damage: The attacker manages to inject herself to a communication between the two parties and can read and manipulate the exchanged messages without the communication parties being aware of it. (2 Points)

Diagram: 6 steps – 1 point for each.



# Question 2: Location-based Services and Business Models (12 Points)

a) Nennen und beschreiben Sie zwei unterschiedliche Ortungsmethoden, die auf der Quelle der (Orts-)Information basieren.

*Name and describe the two different groups of positioning methods depending on the source of the (location) information.*

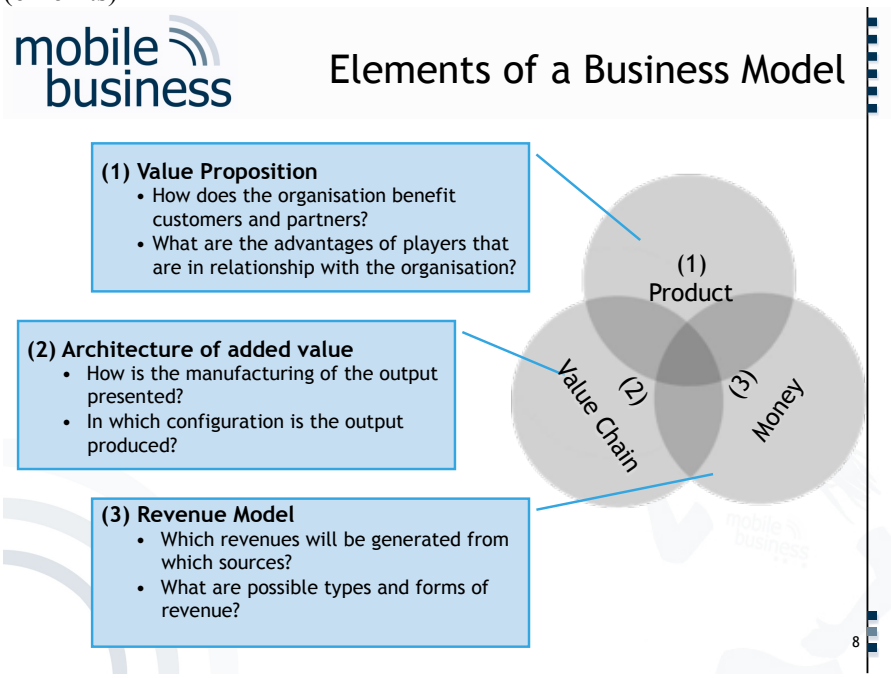
(6 Points)

- *Positioning Methods*
  - ***Network External** Source of Information about Location*
    - *Positioning system outside of the control of the network operator;*
    - *Positioning system is provided by a third party.*
    - User input to the device; Satellite Systems: GPS (USA), Galileo (EU), GLONASS (Russia); Position sender (Radio, Infrared); WLAN positioning; Peer2Peer;
  - ***Network internal** Source of Information about Location – the location is provided from the capabilities inside the network.*
    - *Cell-ID; Time Difference of Arrival (TDOA); Enhanced Observed Time Difference (E-OTD); Angle of Arrival (AOA); Signal Attenuation (SA)*
- ***Hybrid Solutions** – combination of both above. Example: A-GPS*
- Often the terminal is involved in the positioning
  - Terminal positioning
  - Hybrid positioning

b) Nennen und beschreiben Sie kurz drei wesentliche Elemente eines Geschäftsmodells.

*Name and briefly describe three main elements of a Business Model.*

(6 Points)



# Question 3: HCI Issues (12 Points)

a) Benennen Sie die drei wesentlichen Aktivitäten beim Design mobiler Interaktionen wie in der Vorlesung erläutert. Beschreiben Sie jede der Aktivitäten kurz.

*List the three main activities in the Mobile Interaction Design, as explained in the lectures and briefly describe each one.*

(6 Points)

1) ***Understanding users (capabilities and limitations)***

*For an effective interaction design, it is necessary to understand potential users of a system.*

- *The user group needs to have a significant impact on the design process.*
- *User-centered service design can significantly affect the user's perception of mobile devices and services.*

*Possible methodologies:*

- *Field studies (observe and probe a particular group in situations of interest)*
- *Laboratory experiments (observe and probe a particular group within a controlled environment)*
- *Direct questionnaire (e.g. to validate impressions and interpretations from the field)*

2) ***Developing prototype designs*** *((Demonstration of proposed interaction design)*

- *HCI-Prototypes are built in order to express a design idea as quickly as possible.*
- *One can differentiate how closely a prototype resembles the appearance of the final product.*

3) ***Evaluation*** *(Identification of strengths and weaknesses of a design)*

- Evaluation is done in order to understand how users will use the design in the real world, Compare different prototype designs, Assess whether the product to be developed meets usability requirements, and Ensure that the product conforms to industry standards.
- Methodologies: Direct observation; Interviews; Questionnaires; Experiments

b) HCI-Prototypen dienen dazu, Design-Ideen so schnell wie möglich auszudrücken. Beschreiben Sie in Ihren Worten die Unterschiede zwischen „low-fidelity"- und „high-fidelity"-Prototypen.

*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.*

(6 Points)

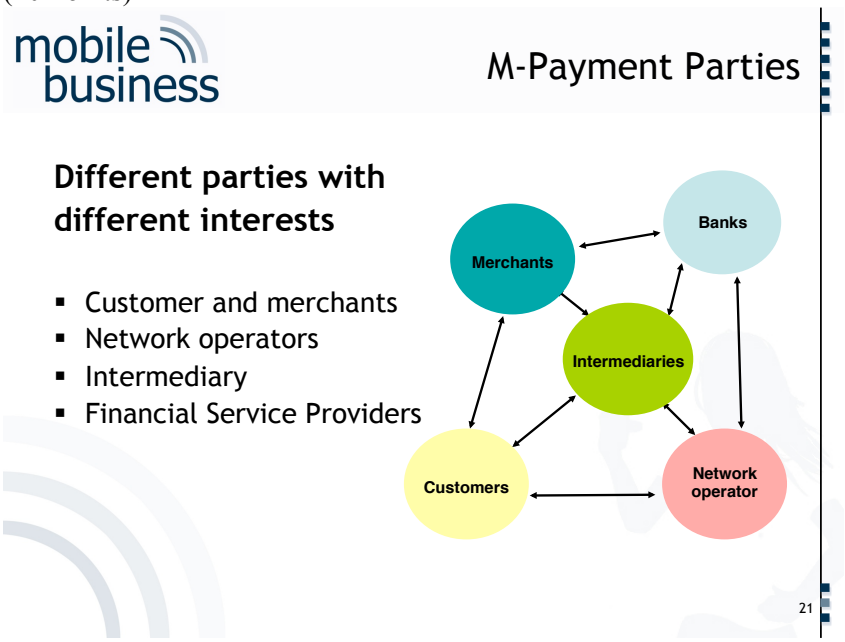
- *One can differentiate how closely a prototype resembles the appearance of the final product. In* ***low-fidelity****, the prototype uses materials different to those in the final incarnation.*
  - *Check for inconsistency*
  - *Give a common specification for the design team*
  - *Afford reflection*
  - *Check interaction scenarios*
  - *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. (PC-based, platform specific prototype designs, etc.)*

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

# Question 4: M-Payment (10 Points)

a) „Mobile Payment“-Szenarios involvieren unterschiedliche Parteien („actors“) mit unterschiedlichen Interessen („stakes“). Nennen Sie die 5 Parteien, die typischerweise in einem „Mobile Payment“-Szenario beteiligt sind und beschreiben Sie kurz deren individuelle Interessen.

*Mobile Payment scenarios concern multiple parties (actors) with different interest (stakes). Name the 5 different parties involved in a typical mobile payment scenario and briefly describe their individual interests.*
(10 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

# Question 5: Mobile Brokerage (14 Points)

a) Welche zwei Phasen des Aktienhandels fallen in den Bereich mobile Endgeräte?

*What are the two phases of the stock trading process that fall into the sphere of mobile devices?*

(2 Points)

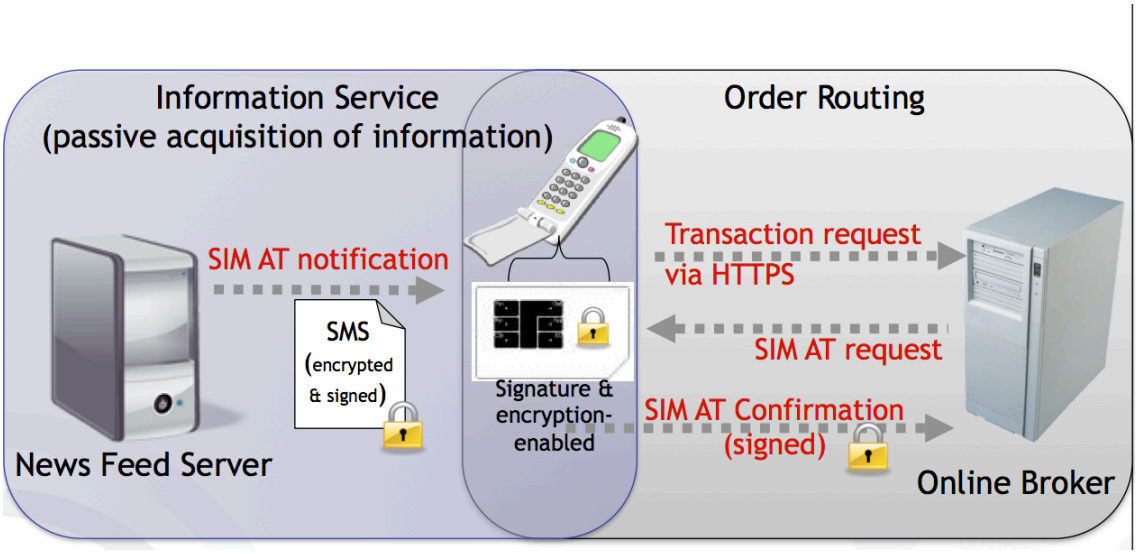
Information Acquisition
Order Routing
(1 point each)

b) Zeichnen Sie eine Architekturskizze, mit Prozessschritten für eine der von Ihnen unter a) genannten Phasen. Die Architektur sollte umfassend von SIM-Karten profitieren, die mit digitalen Signaturen ausgestattet sind.

*Sketch an architecture figure with process steps for one of the phases you named in Section a. The architecture should maximally benefit from a digital signature-enabled SIM card.*

(8 Points)

(The students are supposed to draw either the right half or the left half of the following figure.

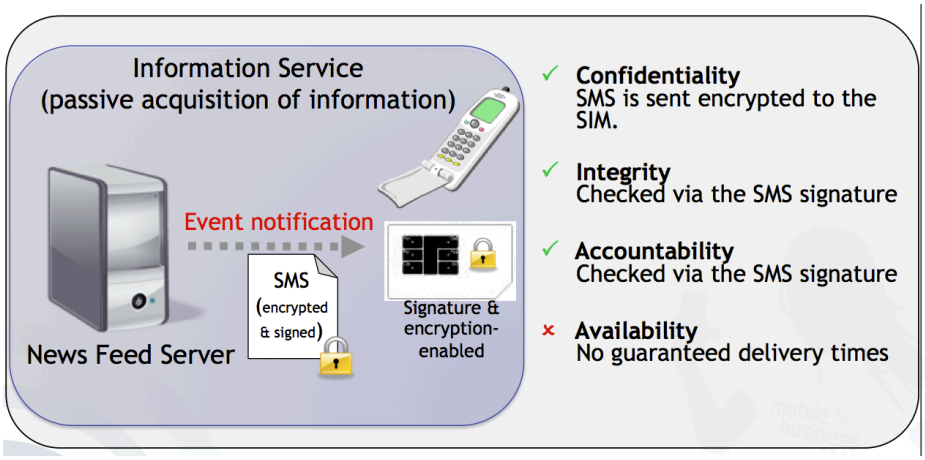


c) Inwiefern kann die Architektur die 4 generellen Schutzziele von IT-Systemen erfüllen?

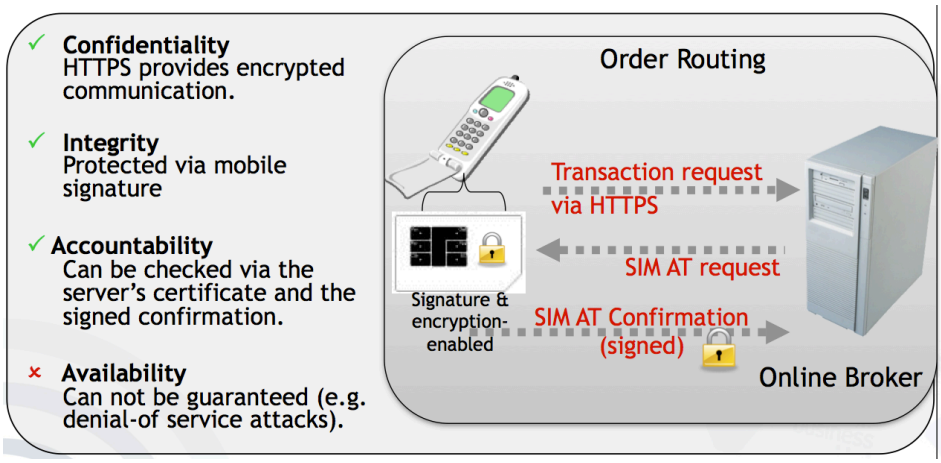
*To what extent can this architecture address the 4 general protection goals regarding IT systems?*

(4 Points)

Depending on the answer on the previous part:




or




4 goals – each one 1 point.

# Question 6: Data Protection / IdM (10 Points)

a) Nennen Sie 4 der 9 Prinzipien des EU-Datenschutzrechts?

*Name 4 of 9 principles of EU Privacy Law?*

(2 Points)

Just naming is enough. 0.5 each.

1. Intention and notification: The processing of personal data must be reported in advance to a Data Protection Authority.
2. Transparency: The person involved must be able to see who is processing her data for what purpose.
3. Finality principle: Personal data may only be collected and processed for specific, explicit and legitimate purposes.
4. 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.
5. Quality: Personal data must be as correct and as accurate as possible
6. 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.
7. 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 .
8. Security: A controller must take all meaningful and possible measures for guarding the personal data.
9. Transfer of personal data outside the EU: The traffic of personal data is permitted only if that country offers adequate protection.

b) Der Klassifizierung von Identitätsmanagementsystemen liegen die verschiedenen Schichten der Identität nach Durand zugrunde („Tier 1-3 Identities“). Nennen und beschreiben Sie diese kurz.

*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 and give a brief description of each one.*

(6 Points)

The different tiers can be distinguished by the factor ‘control’: Who controls the identity?

- Tier 1 (T1): True (‘My’) identity
  - is my true and personal digital identity and is owned and controlled entirely by me, for my sole benefit. T1 identities are both timeless & unconditional
- Tier 2 (T2): Assigned (‘Our’) identity
  - refers to our digital identities that are assigned to us by corporations (e.g. our ‘customer accounts’)
- Tier 3 (T3): Abstracted (‘Their’) identity
  - is an abstracted identity in that it identifies us through our demographics and other reputation like attributes, but does not need to do so in a 1:1 manner .

c) Nennen Sie 4 der Funktionen, die ein Identitätsmanagementsystem unterstützen muss.

*Name 4 of the functions that an Identity Management System must support.*

(2 Points)

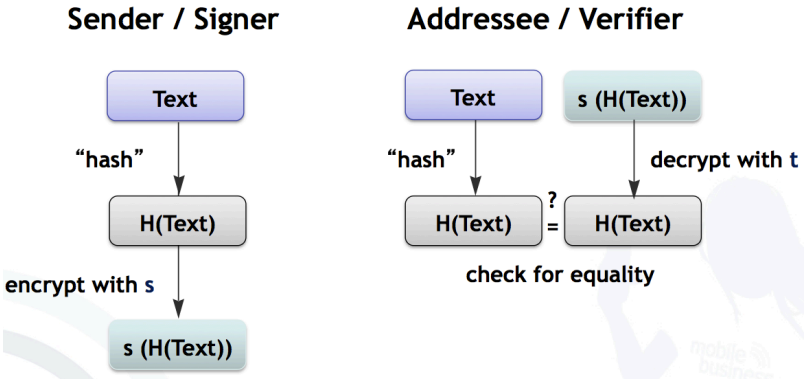
- Provisioning, Enrolling, Choosing
- Binding with Attributes
- Certifying
- Changing
- Unbinding of Attributes §§ Deleting
- ... (other examples are possible. 0.5 each)

# Question 7: Electronic Signatures (6 Points)

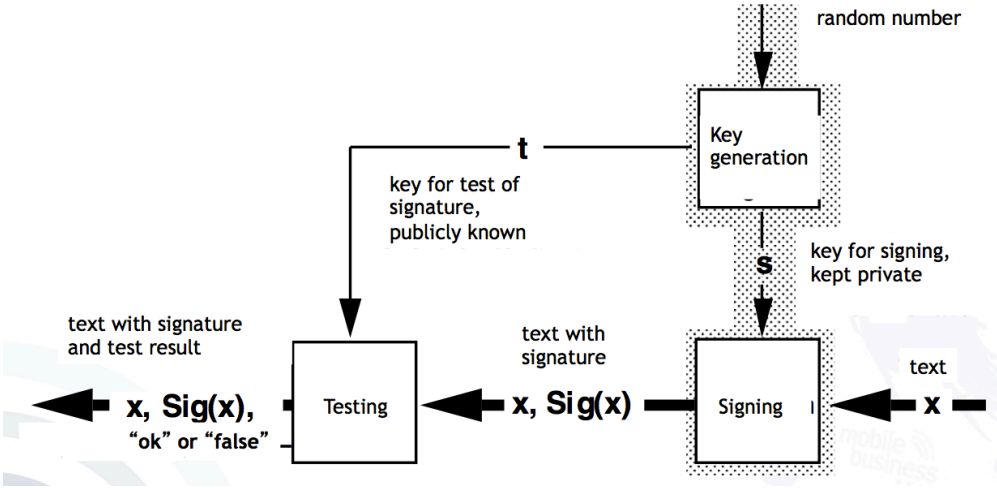
a) Stellen Sie sich ein System asymmetrischer elektronischer Signaturen vor, das eine Hash-Funktion nutzt. Zeichnen Sie auf, wie dieses System funktioniert.

*Imagine a system for asymmetric electronic signatures that uses a hash function. Sketch a figure and show how this system works.*

(6 Points)




However somebody could integrate the figure above into the general figure:



# Question 8: Regulation of Mobile Telecommunications (6 Points)

a) Nennen und beschreiben Sie kurz zwei Formen von Marktversagen.

*Name and describe briefly two types of market failure.*

(2 Points)

- Externe Effekte
- Natürliche Monopole
- Dominierende Lieferanten/Anbieter
- Politische Fehler

- Externalities: Actors and beneficiaries are different
- Natural Monopolies: One (monopoly) supplier may produce at lower costs than several suppliers in competition.
- Dominant Supplier: a supplier dominates a market and harms competition and innovation
- Political Failure: goals are not achieved.

Each one 0.5.

b) Was sind die Gründe für die Regulierung der Roaming-Gebühren innerhalb der EU? Welche konkreten Ziele werden hierbei verfolgt.

*What are the reasons for the regulation of roaming fees within the EU? What are the regulation objectives?*

(4 Points)

**Gründe:**
- Marktversagen (Telcos mit zu viel Marktmacht → Dominierende Anbieter)
- Fehlende Preistransparenz
- Zu hohe Preise

**Ziele:**
- Schutz der Konsumenten
- [allgemein] Wohlfahrtsmaximierende Verteilung von Ressourcen