Which protection goal should be achieved in the following examples? Which security mechanisms can be used to solve these problems?

a) The claimed identity of a user is to be verified.

b) It is to be ensured that messages sent over an insecure channel can be read only by persons entitled to do so.

c) A service is to be used only by approved users.

d) It is to be ensured that unauthorized changes of messages sent over an insecure channel can be detected.
a) The claimed identity of a user is to be verified.
   - **Protection Goal: Authenticity**
   - *The claimed identity of a user can be verified by means of authentication.*

b) It is to be ensured that messages sent over an insecure channel can be read only by persons entitled to do so.
   - **Protection Goal: Confidentiality**
   - *Messages can be protected from unauthorised persons through the use of encryption.*

c) A service is to be used only by approved users.
   - Protection Goal: Access Control
   - *Through authorisation, it can be ensured that services and resources are used only by approved users.*

d) It is to be ensured that unauthorized changes of messages sent over an insecure channel can be detected.
   - **Protection Goal: Integrity**
   - *Unauthorized changes of messages can be detected based on digital signatures*
For the communication between an online shop and an external payment service confidentiality should be ensured?

a) Describe the necessary procedure for symmetric cryptography.

b) Describe the necessary procedure asymmetric cryptography.

c) How can both approaches be combined?
- Protection of data against unwanted access
- Guarantee **confidentiality**

- Two main operations
  - Encryption (cipher) at sender
  - Decryption (decipher) at receiver
• Same key used for encryption and decryption
• Keys created at key generator
• Keys have to be delivered to communication partners over a secure communication channel
Different keys for encryption and decryption

Unique key pair:
- Public key for encryption – distributable to everyone
- Private key for decryption – secret key
- Key pair created by key owner (e.g. based on calculus of large prime numbers)
- One-way function: inverse function not computable in relevant time frame
- One key can't be derived from the other
Symmetric keys distributed through asymmetric procedures - secure and simple

- These private keys are then used in a symmetric way for the encryption and decryption of the actual user data – guarantees high efficiency
- Procedures widespread in practice
  - (e.g. Pretty Good Privacy, Secure Sockey Layer, Transport Layer Security)
- Why should the mechanisms be combined?

- Symmetric
  - better performance compared to asym.
  - Key exchange needs effort for secure channel

- Asymmetric
  - Simple key exchange
  - Much slower than symmetric (up to 1000 times)
The customer of an online shop would like to order a set of products. The system should ensure the integrity and accountability of the order?

a) How are the public and private key used when a digital signature is to be created on the basis of asymmetric cryptographic procedures?

b) Why are symmetric cryptographic procedures not appropriate for digital signatures?
Use of Asymmetric cryptography

- Private key used for encryption (signature)
- Only owner of private key (one entity) can sign
- Public key used for decryption/checking of signature
- Everyone can check signature, certificates (trust center) required to check assignment private/public key and person/organization

Message digest/check sum to ensure that signed document is not changed after signing it
Check sum (message digest) generated by means of cryptographic secure hash procedure

Inversion of asymmetric cryptographic procedure i.e. private key for encryption and public key for decryption

Private Key only known by sender

If the check sum sent by sender and that calculated by receiver match then message was sent by authentic sender
For symmetric cryptography no 1:1 assignment between keys and persons/organizations
  • Signer can not be unambiguously identified
A customer of an online shop would like to order a set of products. In the course of this activity the online shop validates the identity of the customer and vice versa.

a) Explain the authentication procedure using a key distribution center and symmetric cryptography.

b) Sketch a sequence diagram with an example message flow that illustrates a case for missing synchronization between client and server using a KDC for authentication.

c) Describe the authentication of the customer based on asymmetric cryptography.

d) What problem can arise with asymmetric authentication and how can it be solved with the help of certificates?
centralised approach for key distribution
- relieves hosts from maintaining keys of any potential communication partner
- Trusted Entity → shares secret key with every host, hosts do not have to share keys
- basic usage
  0. Client authenticates against KDC
  1. Client requests conversation key from KDC for communication with server
  2. KDC generates conversation key and sends it to Client and server encrypted with the according secret keys $K_C$ and $K_S$
- Issues
  - Lack of synchronisation between client and server
  - Servers do not expect message from KDC (even though solicited)
Solution E6.4b

Client

KDC

Server

key_request(C,S)

response (KC{CK})

CK{rpc_request(p1, …, pn)}

response (KS{CK})
1. Client request contains client identifier $C$ and random number $Z_C$ (challenge)
2. Server decrypts $Z_C$ and sends it back to client $\rightarrow$ server identity authenticated
3. Conversation key $CK$ (to be used in further communications) and random number challenge $Z_S$ for client also sent
4. Client decrypts $Z_S$, then encrypts it with $CK$ and sends it back to server $\rightarrow$ client authenticated

$\Rightarrow$ no KDC required (see also: Diffie-Hellman Key Exchange)
- asymmetric authentication only ensures that owner of public key is communication partner
- it does not ensure that intended party is owner of key pair

- Certificate = digital confirmation of assignment of
  - public key and
  - Owner (natural or legal person)

- X.509 Certificate structure contains
  - Tuple <public key, username of owner>
  - Creator of certificate (Certification authority) – confirms pair of public key and username of owner
  - Validity period
  - Signed with private key of certification authority

- Chain of certificates can be generated
- Root certificate identifies the Root Certificate Authority (CA)
  - top-most certificate of the tree
  - has to be trusted
  - E.g. build into browsers to avoid manipulation
Authorization: State the two main methods for authorization and explain how they manage access rights. Which of these methods should be used when rights are to be frequently withdrawn?

Access Matrix can be implemented as
- Access Control list containing the rows of the matrix (subject – rights) stored on the objects to be controlled
- Capability containing the columns of the matrix (object – rights) carried by the subjects requesting access

An access matrix can be implemented in the form of access control lists or through capabilities. With access control lists, access rights are managed by the object that is to be accessed. Capabilities present the possibility of the management of access rights by individual subjects which wish to access different objects of the system.

With the use of access control lists, access rights can be withdrawn more easily because they exist centrally at the object and are controlled by the object.