Public Key Authentication

One of the most dangerous situations in communication is when a malicious attacker intercepts the communication channel and alters the keys without being noticed. This can be prevented by involving a trusted third party that provides additional authentication.

Steps of Authentication

1. A **Certificate Authority (CA)** issues a certificate in which it verifies a person's public key using its own digital signature. It is assumed that both communicating parties trust the CA.

2. A public key is generated that contains the CA’s digital signature.

3. Bob uses his private key to encrypt his document, as usual.

4. He sends the encrypted message to Alice.

5. If Alice can read the message using the authenticated public key, she can be sure that it was sent by Bob.

6. An attacker intercepting the communication cannot alter the key, because it is signed by a trusted third party (the CA).

What Trust Is Required from the CA?

Trust is required in ensuring that the CA’s **private key** remains secret and is not compromised.

Authentication is not free. Standards dictate that the authenticated signature is only valid for a pre-determined period of time.