



openHPI course "Digital Identities Secure Authentication"

Prof. Dr. Christoph Meinel

Hasso Plattner Institute, University of Potsdam

Secure authentication with one-time passwords

- Each password can only be used once for authentication - **One-Time Passwords** (OTP)
- Password loses its validity immediately after first use
 - Interception and spying useless
- One-time passwords are **automatically** and **randomly generated character strings** that are provided to the user via a second, independent transmission channel.



Provision of one-time passwords

■ **challenge**

- Both the user and the authentication authority must know which one-time passwords are accepted as valid.

■ 2 possible **solutions**

- password lists
 - List of valid one-time passwords is generated by the authentication authority and handed over to the user via a secure transport route.
 - e.g. TAN lists
- password generators
 - Dynamically generate passwords that are valid for a specific period of time

password generators

- Small devices (**tokens**) or applications
- Password generators produce one-time passwords based on special algorithms
- A distinction can be made between 3 generation methods:
 - **Time-controlled** generation
 - **Event-driven** generation
 - **Challenge-Response-controlled** generation

Time-controlled Generation of one-time passwords

- Token and authentication point work synchronously in time
- Both sides calculate one-time passwords at the same time interval, which are valid until use or the next calculation iteration.
- Authentication point allows a temporal tolerance range, since the clock in the token does not always work 100% exactly
- Examples:
 - Google Authenticator
 - SecurID



SecurID



Google Authenticator

Event-driven Generation of one-time passwords

- Generation of a one-time password is triggered by the user, e.g. by pressing a key on the token.
- Token and authentication authority remember the number of passwords generated so far
- Calculation of the one-time password including previously generated passwords
- Authentication authority allows a tolerance range in case the user has not used a generated password

Challenge-response controlled generation of one-time passwords

- User wants to authenticate himself and asks at the authentication authority
 - Authentication authority sends random value to token
 - Token applies calculation algorithm to received value and outputs result (one-time password)
 - User sends generated one-time password to authentication point
 - The authentication authority knows the calculation algorithm and checks the value calculated by the token.
- If correct, the user is authenticated.

Secure Public-Key Authentication

Application of methods of **public-key cryptography**:

- User gets a key pair of public and private key handed out
- Public key will be made known to all interested parties
- Users can identify themselves using their digital signature, generated with the private key:
 - Authentication service checks / "verifies" the signature using a public key
 - Only possible with "correct" public key, i.e. the one that belongs to the private key with which the signature was generated.
- **Optional:** Protection of the private key with password
 - ➔ **2-factor authentication**

Secure authentication with smart cards

- Storage of the private key on a smartcard
- Key can only be used by the owner of the smartcard
- A PIN must be entered to access the key.
- E.g. new identity card (nPA)

→ **2-factor authentication**

- Possession (map)
- Knowledge (PIN)



■ **Secure authentication methods:**

- one-time passwords
- smart cards

■ **one-time passwords**

- Each password can only be used 1x.
- Deployment using password lists and password generators
- Password generators can be divided into 3 categories:
 - Time-controlled generation
 - Event-driven generation
 - Challenge-Response-controlled generation

■ **smart cards**

- Provide private keys for authentication in PKIs
- Securing with 2-factor authentication (possession + knowledge)

■ **Secure authentication methods:**

- one-time passwords
- smart cards

■ **one-time passwords**

- Each password can only be used 1x.
- Deployment using password lists and password generators
- Password generators can be divided into 3 categories:
 - Time-controlled generation
 - Event-driven generation
 - Challenge-Response-controlled generation

■ **smart cards**

- Provide private keys for authentication in PKIs
- Securing with 2-factor authentication (possession + knowledge)