08 – Secure Sockets

//// Design of Distributed Systems
///

Dipl.-Inf. Michael Krug

VSR.*Informatik*.TU-Chemnitz.*de*

1 Repetition

#

We were looking for a solution so that a server application can actively send messages to a specific client at any time

→ WebSockets

# Homework

Solutions?

Advantages

- Server can actively use the connection (bi-directional)
- No HTTP overhead
- No delay due to polling
- Supported by many Web browsers
  Example: Google Chrome (JavaScript):

```
// Open Socket end receive data
var s = new WebSocket(host);
s.onmessage = function (e) {…};
…
// Send data
var xxx = inputBox.value;
s.send(xxx);
```

3 Secure Sockets

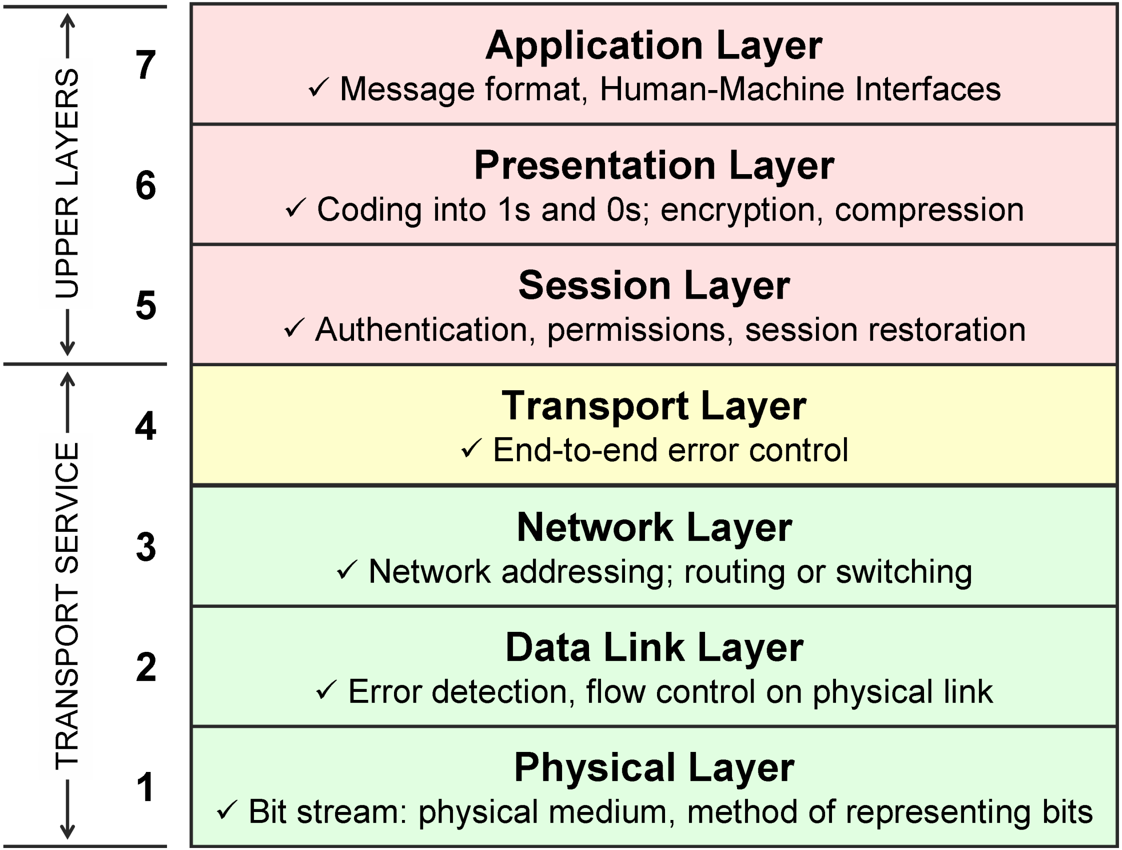
? What is SSL / TLS

So far, we normally send application data as plain text

We want to establish an encrypted link between a server and a client

Therefore, we need a communication protocol that specifies how to secure the channel and encrypt our data

- Secure Sockets Layer (SSL)
  - Version 1.0 by Netscape Communications (1994)
- Transport Layer Security (TLS)
  - IETF-standard from the year 1999 (RFC 2246)
- Network protocol for secure data transfer
- Since Version 3.0 SSL is being further developed under the name TLS
  - Minor differences between SSL 3.0 & TLS 1.0
  - TLS 1.0 is presented as SSL 3.1
  - Currently TLS 1.2



UPPER LAYERS

7 **Application Layer**
✓ Message format, Human-Machine Interfaces

6 **Presentation Layer**
✓ Coding into 1s and 0s; encryption, compression

5 **Session Layer**
✓ Authentication, permissions, session restoration

TRANSPORT SERVICE

4 **Transport Layer**
✓ End-to-end error control

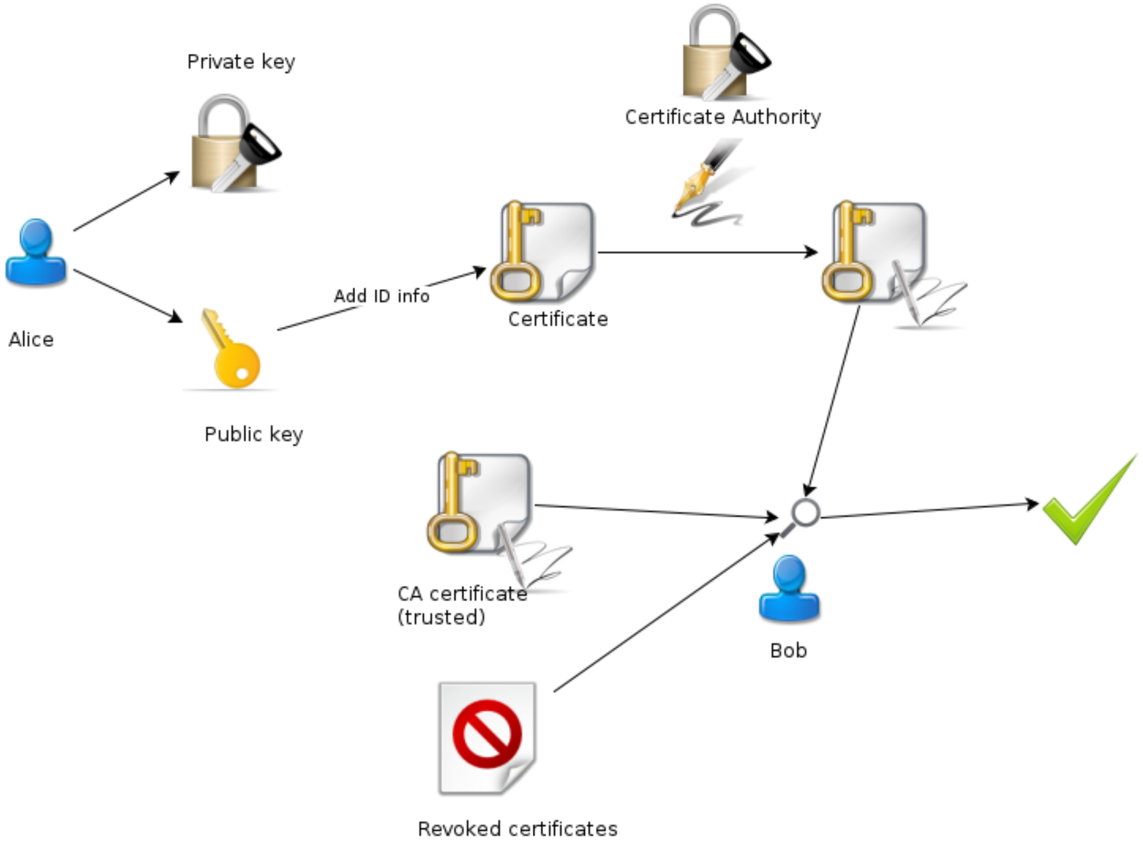
3 **Network Layer**
✓ Network addressing; routing or switching

2 **Data Link Layer**
✓ Error detection, flow control on physical link

1 **Physical Layer**
✓ Bit stream: physical medium, method of representing bits

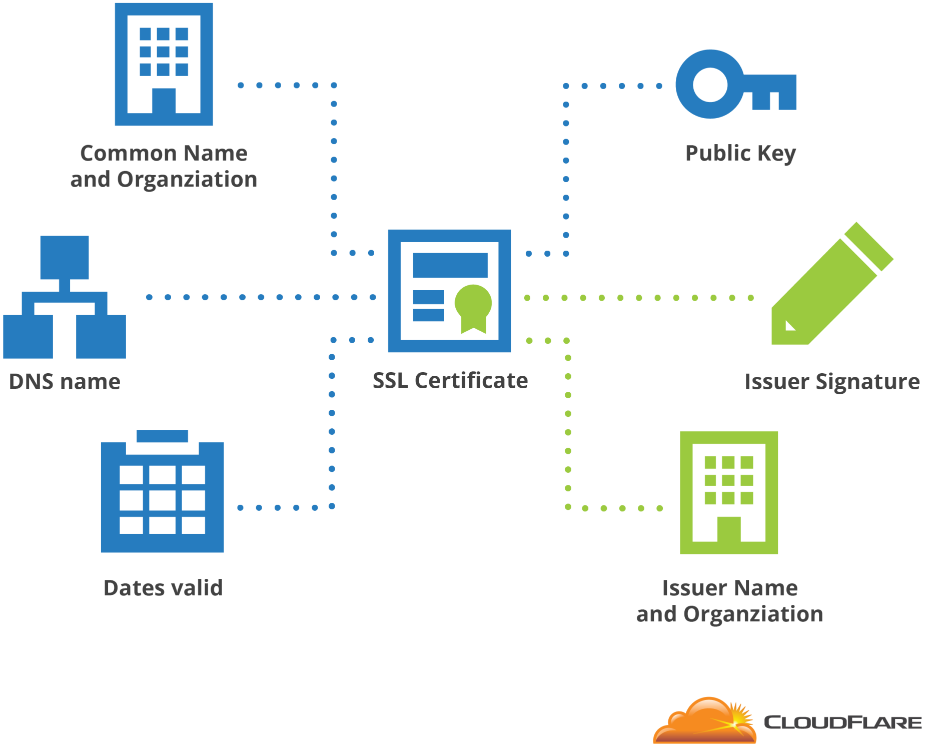
Source: http://nhprice.com/wp-content/uploads/2013/03/1-tutorial-osi-7-layer-model1.gif

- In OSI-model in layer 6
- In TCP/IP-model
  - Above the Transport layer (i.e. TCP,...)
  - Below the Application layer (i.e. HTTP,...)
- Basic idea: generic security layer

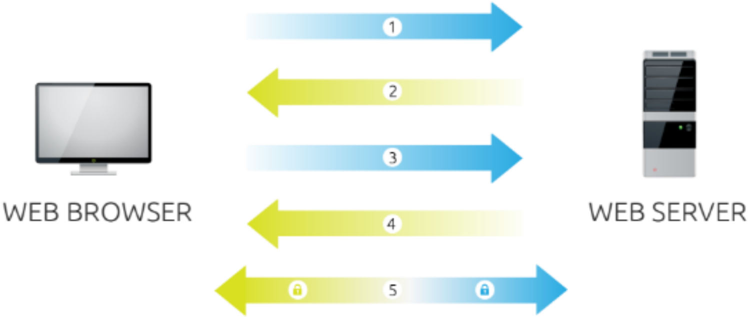


Source: http://swift.siphos.be/aglara/images/04-ca_certificate.png

The anatomy of a certificate



Source: https://blog.cloudflare.com/content/images/2015/06/illustrations-ssl-blog-june-2015-02.png



1. **Browser** connects to a web server (website) secured with SSL (https). Browser requests that the server identify itself.

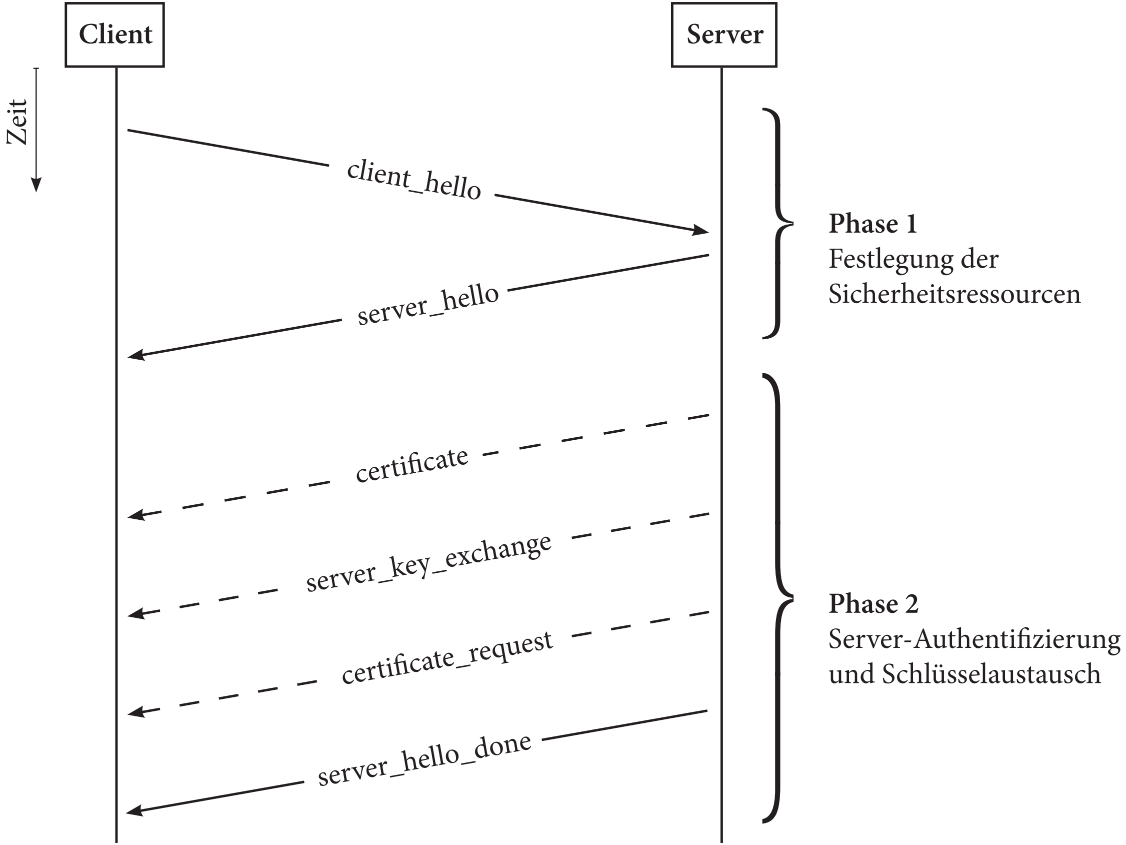
2. **Server** sends a copy of its SSL Certificate, including the server's public key.

3. **Browser** checks the certificate root against a list of trusted CAs and that the certificate is unexpired, unrevoked, and that its common name is valid for the website that it is connecting to. If the browser trusts the certificate, it creates, encrypts, and sends back a symmetric session key using the server's public key.

4. **Server** decrypts the symmetric session key using its private key and sends back an acknowledgement encrypted with the session key to start the encrypted session.

5. **Server** and **Browser** now encrypt all transmitted data with the session key.

Handshake Protocol – Part 1

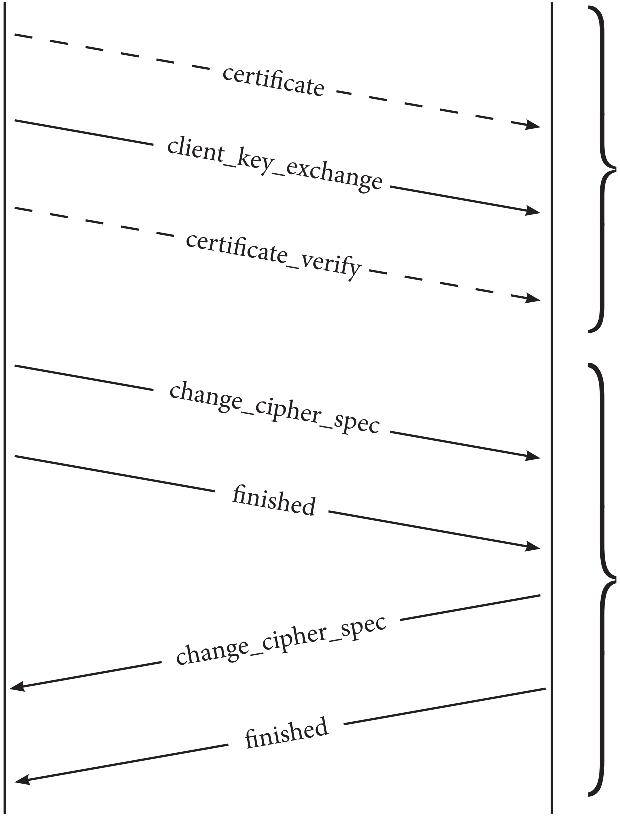


Phase 1
Festlegung der
Sicherheitsressourcen

Phase 2
Server-Authentifizierung
und Schlüsselaustausch

Source: http://www.repges.net/SSL/Architektur_SSL/HANDSH_1/handsh_1.HTM

Handshake Protocol – Part 2



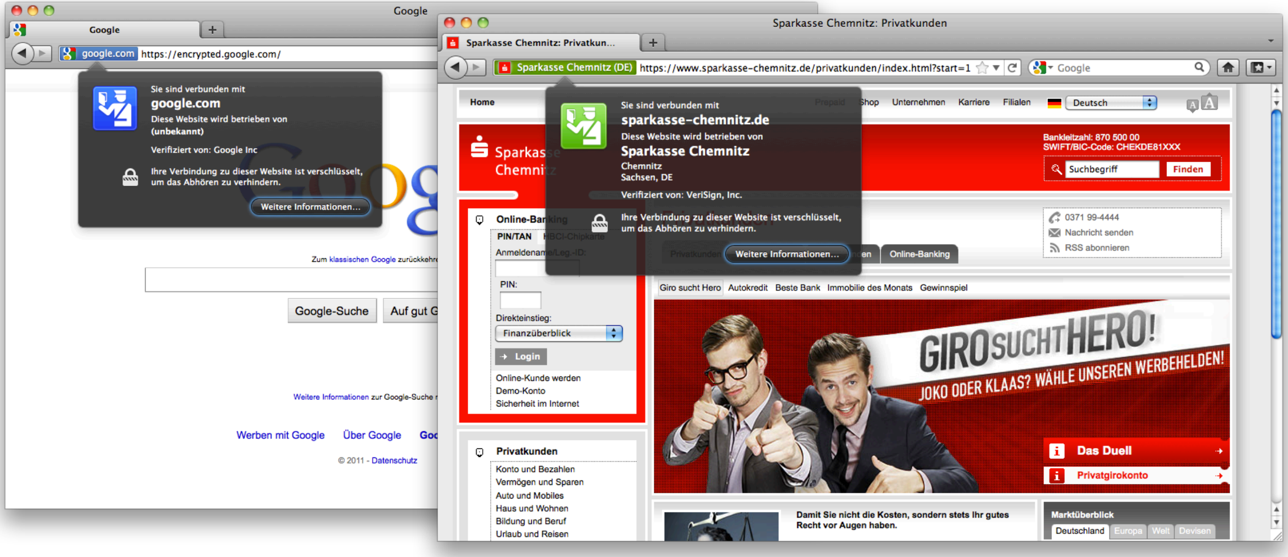
Phase 3
Client-Authentifizierung
und Schlüsselaustausch

Phase 4
Beendigung
des Handshake

Source: http://www.repges.net/SSL/Architektur_SSL/HANDSH_1/handsh_1.HTM

Hypertext Transfer Protocol Secure

- HTTP with additional transmission encryption by SSL/TLS
- Standard-Port: 443



Google

google.com https://encrypted.google.com/

Sie sind verbunden mit
google.com
Diese Website wird betrieben von
(unbekannt)

Verifiziert von: Google Inc

Ihre Verbindung zu dieser Website ist verschlüsselt, um das Abhören zu verhindern.

Sparkasse Chemnitz: Privatkunden

Sparkasse Chemnitz (DE) https://www.sparkasse-chemnitz.de/privatkunden/index.html?start=1

Sie sind verbunden mit
sparkasse-chemnitz.de
Diese Website wird betrieben von
Sparkasse Chemnitz
Chemnitz
Sachsen, DE

Verifiziert von: VeriSign, Inc.

Ihre Verbindung zu dieser Website ist verschlüsselt, um das Abhören zu verhindern.

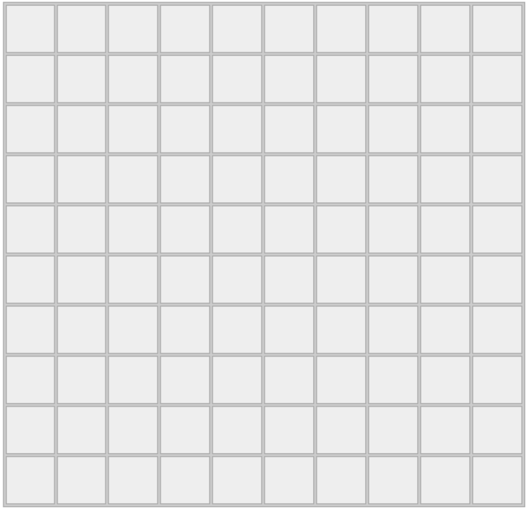
4 WSS

WSS

- WebSockets over SSL/TLS
- Prefer wss:// over ws://
- Protects against man-in-the-middle attacks

5 The Click Game

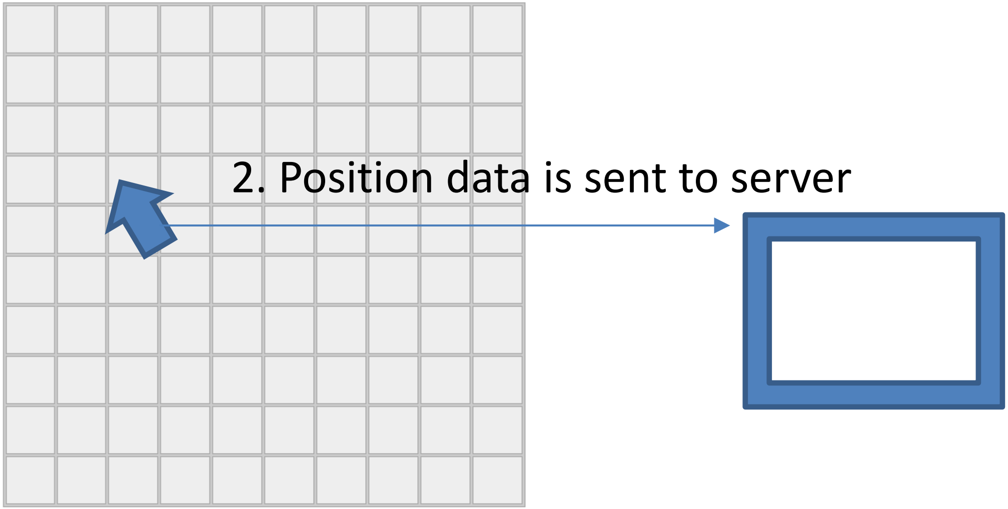
Basic Scenario



Basic Scenario

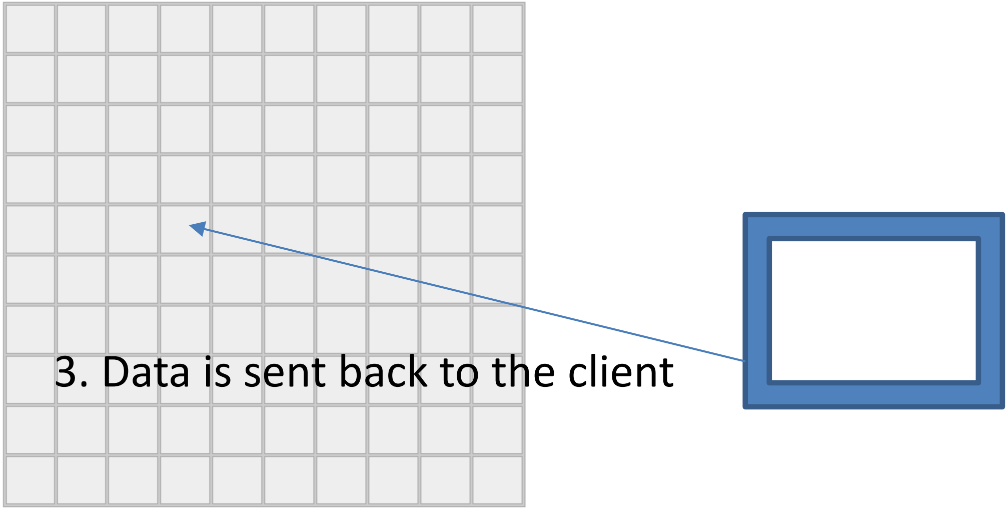
1. User Click

Basic Scenario



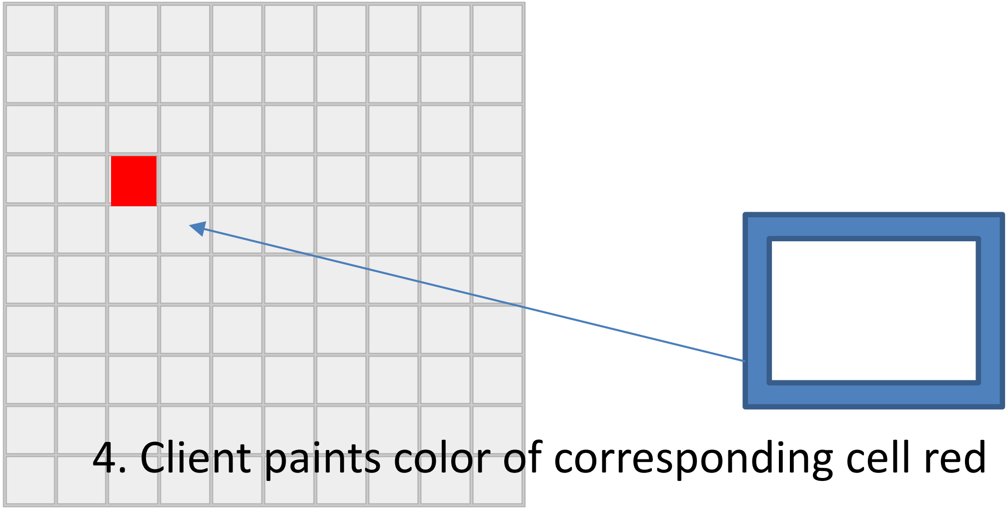
2. Position data is sent to server

Basic Scenario



3. Data is sent back to the client

Basic Scenario



4. Client paints color of corresponding cell red

Simple Task:

- Implement the requirement using AJAX and traditional server side technologies

Advanced Task:

- Implement the requirement using WebSockets

6 ToDo

Next week, we will talk about server-side development

! Please bring a **laptop** with you and install Microsoft **Visual Studio** Community 2017 in advance

Thank You!

Michael.Krug@informatik.tu-chemnitz.de

***VSR**.Informatik*.TU-Chemnitz.*de*