MUNI
MED

Computer network user

Klimeš Daniel, Šmíd Roman, Krejčí Jan

Organisation of the course

Conditions for credit

- Registration in is.muni.cz
- Learning this material
- Passing the electronic test

Course outline

- Network connection
  - Connection options, what is needed, comparison
- Network services
  - HTTP, FTP, DHCP, DNS, E-mail, remote access
- Network security
  - Passwords and Explorer in general, Firewall, email, spyware, phishing
  - Mobile devices
- Encryption and electronic signature
- Czech E-government (optional)

- Electronic health care in the Czech Republic

Network connection

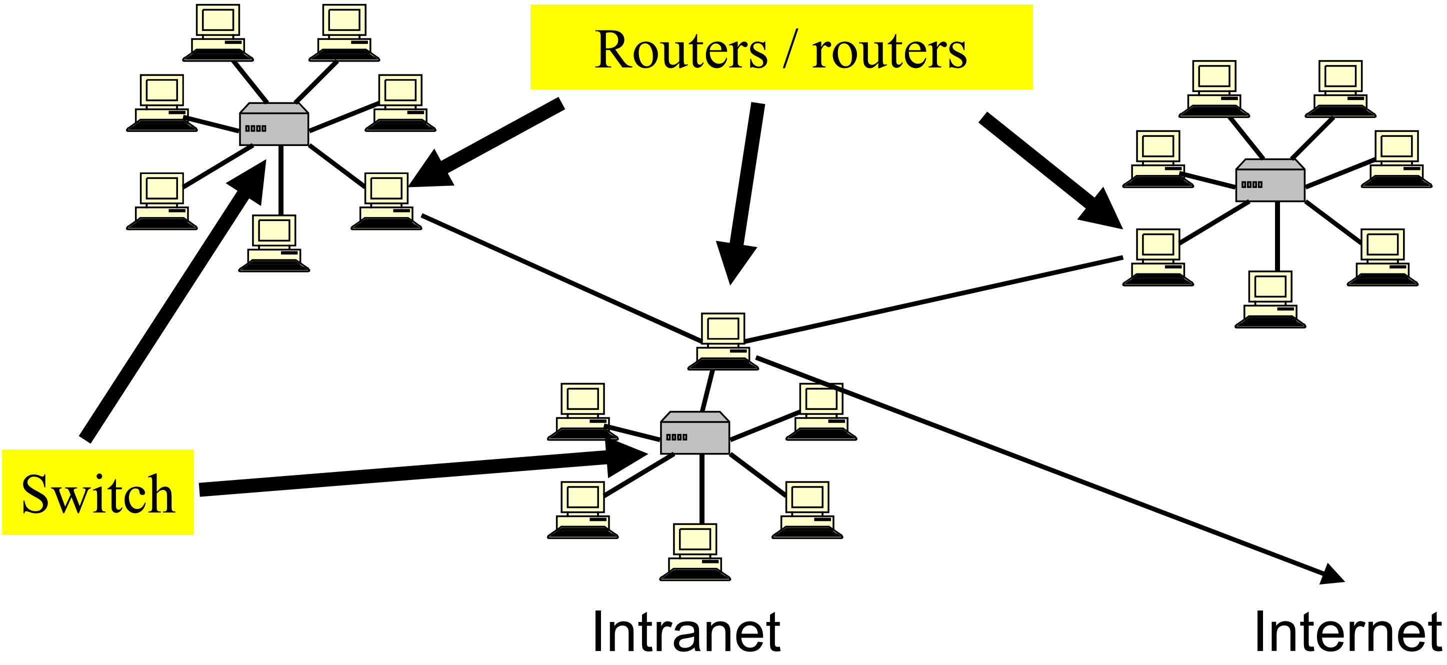
Data and its volume

- How to express information
- **1 bit (b) - basic information unit 1/0**
- **1 Byte (B) - 8 bits, integer from 0 to 255,**
  - **1 text character (ASCII), e.g. "A" = 65**
- 1 Kb = 1024 bits
- 1 KB = 1024 Bytes

Computer network

- Connecting two or more computers
- Network elements are part of the network
  - Computer (device) with network card, modem, wifi adapter
  - Cabling (metallic, optical)
  - Hubs, routers and switches, wifirouters, antennas
  - Devices providing network services, network printers...
- The quality of a network, or a particular path in a network, can be assessed by
  - Network **throughput** (speeds) - (K/M/G) bits per second (**b/s**)
  - **Response speeds** (milliseconds) - **ping**

Connecting local networks



Identifying PCs on the network

- Network card identification

  Worldwide "unique" MAC address (physical address)
  00-0A-E4-C0-36-81

- IP address (similar to an ID number or phone number)

  Globally "unique"
  147.251.147.76

- Internet name (similar to a postal address) - URL

  Worldwide unique
  www. iba.muni.cz

IP address

IPv4 x IPv6

- IPv4: 32b = 2^{32} IP address => approx. 4 * 10^{9} address
- IPv6: phased in 128b => 3.4 * 10^{38} addresses

Same computer transferred to another network usually has a different IP address!

IP address

- Fixed x dynamic IP address
- Public x non-public IP address

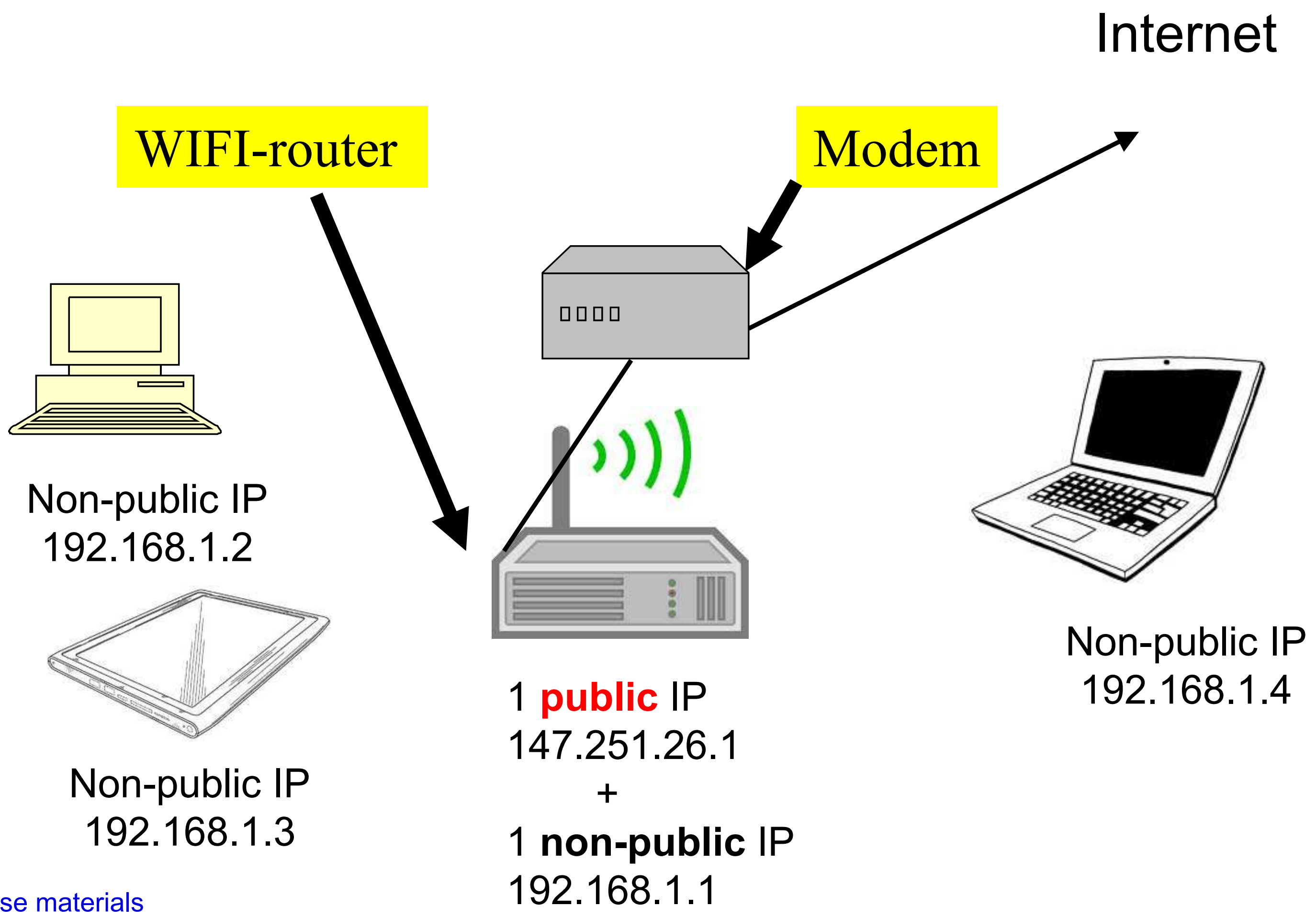
  - Non-public IP is not globally unique - only within the local subnet
  - Non-public addresses do not have an associated Internet name
  - Dynamic + non-public IP - typical service consumer
  - Fixed + public IP - typical service provider

http://www.ip-adress.com/

cmd - ipconfig

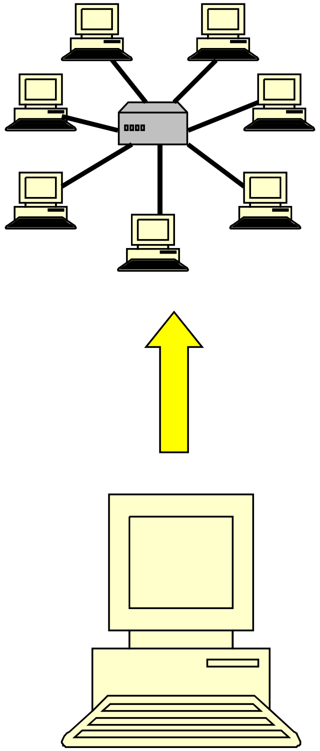
Non-public IP addresses

192.168.*.*



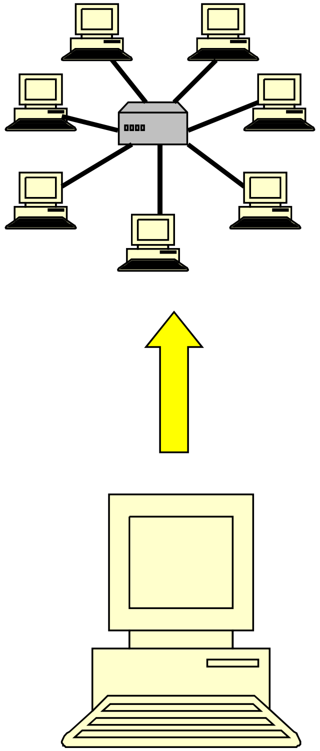
Physical connection of the PC to the network

- Cable TV
  - Modem, metallic network x optical network
- Telephone line
  - xDSL modem
- Mobile connection
  - LTE modem or mobile phone
- Wireless - WiFi
  - Special equipment/card, antenna

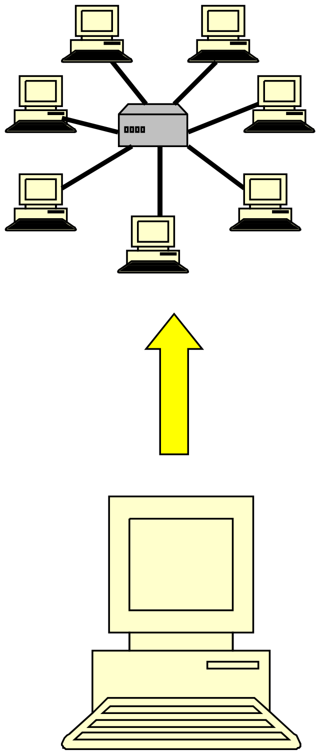


Cable TV

- In places where cable TV is available
- Speed up to 500 Mbps
- Metallic x optical connection
  - Metallic has significantly worse upload
- Special modem
- Main providers
  - http://www.vodafone.cz
  - http://www.netbox.cz
  - http://www.selfnet.cz
  - http://rychlost.cz/pripojeni-internetu/kabelova-tv/



Telephone line

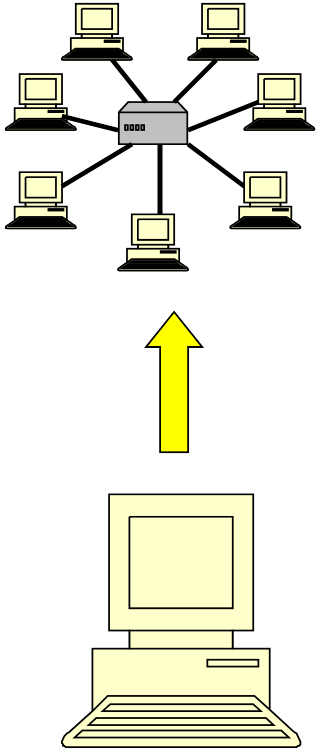


- ADSL (up to 16 Mbps)
- VDSL (up to 100 Mbps)
  - Offered within 1.3 km of the exchange
- Each type requires a specific modem

WiFi-connection

- Outdoor/indoor
- Commercial/community networks
- Speed up to 54 Mbps
- Special affordable equipment
- Risk of interference, eavesdropping, unauthorised connection
- Access point /Access point/ hot spot
- http://www.internetprovsechny.cz/wifi/
- https://it.muni.cz/sluzby/wifi
  - Eduroam

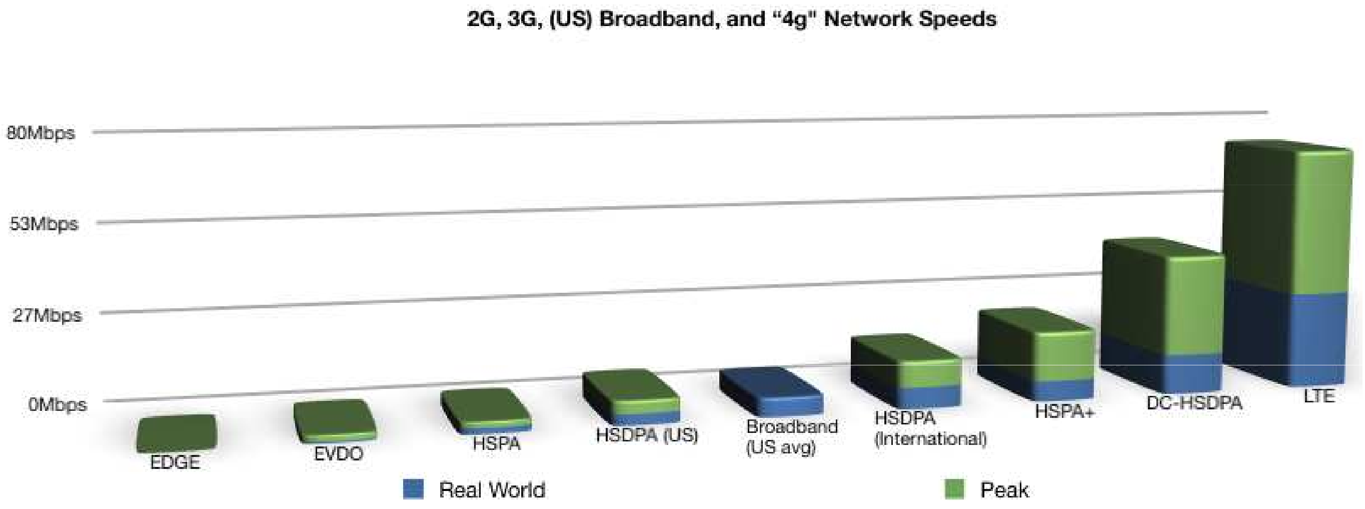
Mobile connection



- GPRS (up to 128 kbps)
- 2G - EDGE (up to 512 kbps)
- 3G - UMTS/HSDPA (1024 kbps and more)
- **4G - LTE (80 Mbps or more)**
  - **More coverage than 3G**
  - Newer smartphones and modems

GSM connection speed

- Many terms and abbreviations - GPRS, EDGE, UMTS, HSPA, HSPA+, HSDPA, HSUPA, WCDMA, 3G, 4G, LTE....



Source: tasel.wordpress.com

LTE coverage

- Great dynamics
- Provider websites or
- http://lte.ctu.cz/pokryti/
- For all operators

- LTE bands
  - LTE-800 = basic for the Czech Republic

Choosing an internet connection

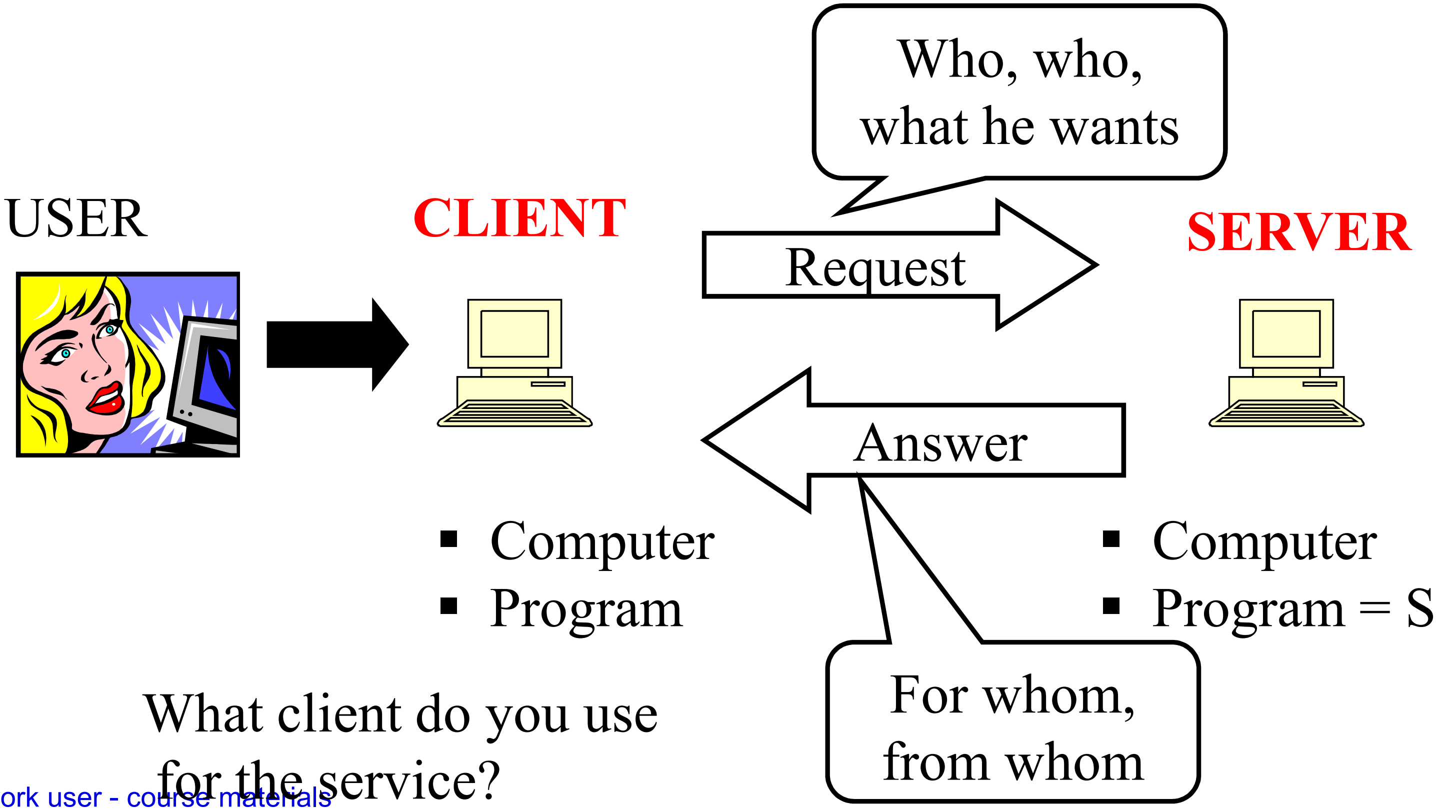
- Method of use - fixed PC x notebook
- Availability in given locations, coverage
- Speed, usually in Mbps
  - symmetric x **asymmetric** (download, upload)
  - (e.g.: 20/2 Mbps)
  - Actual speed verified in practice
- Fair user policy (FUP) - speed limitation after transferring a certain amount of data
- Aggregation (e.g.: 1:32) - (ADSL, wireless)

The actual speed between two computers can be measured indicatively using speedmeters

E.g.: http://nastroje.lupa.cz/mereni-rychlosti/, www.dsl.cz

Intercommunication of computers in the network

Client - Server model



Who, who, what he wants

USER

CLIENT

Request

Answer

SERVER

- Computer
- Program

- Computer
- Program = SERVICE

For whom, from whom

What client do you use for the service?

Network services

Network services

- A network service is a service provided to users over a computer network
- The main ones are DHCP, DNS, HTTP, FTP, SSH, POP3, IMAP, SMTP, ...
- Typically one server provides multiple services
- The server is identified by its IP address *(phone number)*, the service by its number called port
- The complete service address is always the server IP address + port number
- Each service has a defined standard port, e.g. HTTP has port 80, SSH has port 22, ...

DNS service (name resolution)

- Translating Internet names to IP addresses
- Not every IP address has a defined Internet name
- The translation is performed by DNS servers that maintain a list of known Internet names and query other DNS servers for unknown names
- Internet names cannot be used without the availability of this service, only IP addresses
- For example: med.muni.cz => 147.251.128.10

DHCP service (IP address allocation)

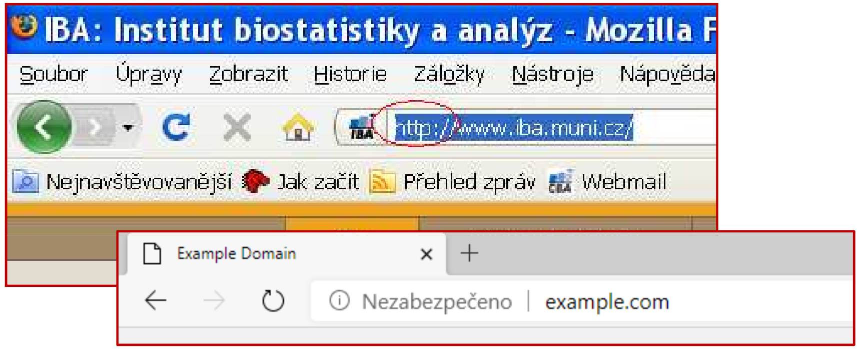
- Automatically configure your computer's network connection on your local network

- The DHCP protocol sets all the parameters necessary to connect the PC to the network, in particular
  - **IP address of the** PC (147.251.140.250)
  - **Netmask (**255.255.255.0)
  - Gateway **IP address** (147.251.147.1)
  - **DNS server IP address** (147.251.26.1)

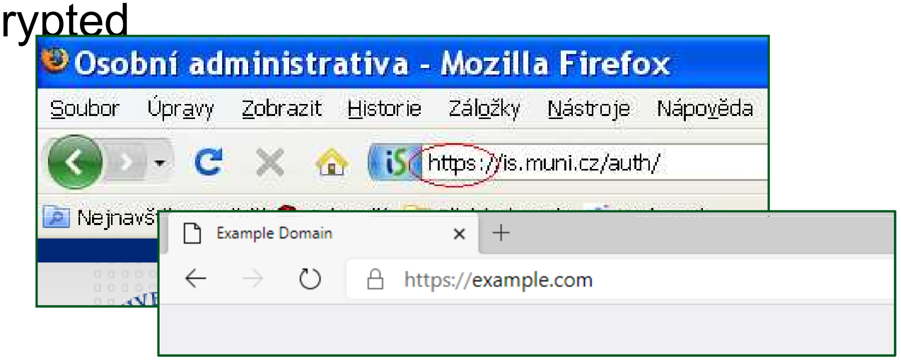
- Computer connections (network cards = MAC addresses) can be enabled/disabled by the network administrator

HTTP and HTTPS protocols (web pages)

- Web page transfer protocol
- HTTP
  - transmits data in readable form
  - Port 80
- HTTPS
  - communication between client and server is encrypted
  - data is unreadable during transmission
  - HTTPS has its own port 443
- Nowadays most sites are already HTTPS
  - Browsers automatically warn the user when unencrypted HTTP is being used

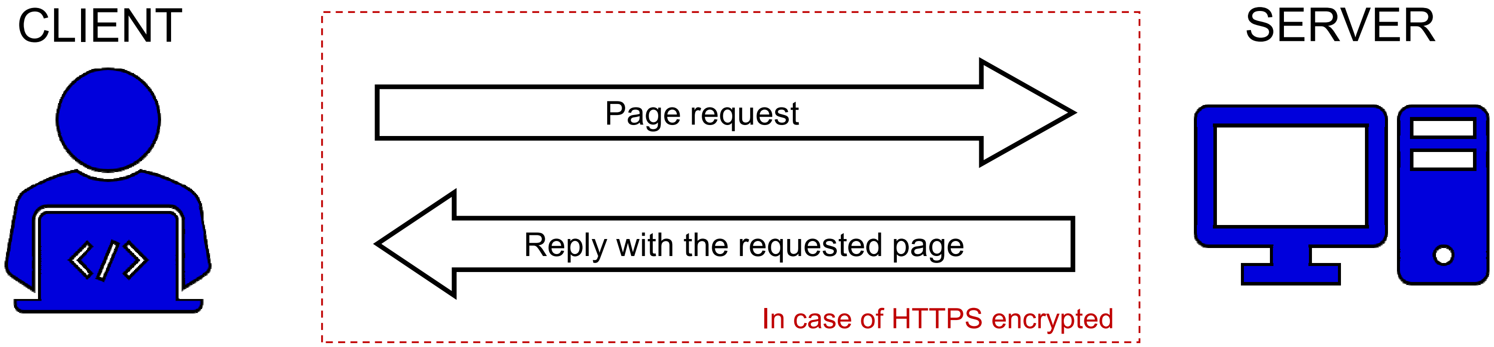

IBA: Institut biostatistiky a analýz - Mozilla F
Soubor Úpravy Zobrazit Historie Záložky Nástroje Nápověda
http://www.iba.muni.cz/
Nejnavštěvovanější Jak začít Přehled zpráv Webmail
Example Domain
Nezabezpečeno | example.com

Unencrypted transmission using HTTP


Osobní administrativa - Mozilla Firefox
Soubor Úpravy Zobrazit Historie Záložky Nástroje Nápověda
https://is.muni.cz/auth/
Nejnavš
Example Domain
https://example.com

Encrypted transmission using HTTPS

HTTP(S) websites



Browsers:

- Microsoft EDGE
- Mozilla Firefox
- Google Chrome
- Apple Safari

Servers:

- IIS
- Apache

Ports:

- 80 (HTTP)
- 443 (HTTPS)

Cookies - what they are for

- Small files stored on your computer
- Tied to a specific server
- The browser sends them with a request to the server
- The server creates/modifies them, sends them to the browser
- The server "remembers" you
- Privacy Campaign
- Risk of connection takeover after you log in to the open WIFI service, if the connection is not encrypted

Cookies - how to remove them

- MS Edge
  - Settings -> Clear browsing data
- Mozilla Firefox
  - Options menu -> Privacy -> Remove cookies
- Google Chrome
  - Settings -> Privacy -> Delete browsing data
- Apple Safari
  - Settings -> Safari -> Advanced -> Site Data -> Delete all site data

Email services

- Mailbox = files primarily located on the mail server
- Mail servers communicate with each other - they forward mails
- Email programs versus email via web interface
- Mail reading services (POP3 and IMAP)
- Service for sending mail (SMTP)

IMAP and POP3 services (receiving mail)

- IMAP and POP3 protocols are used to read mail on a mail server using a mail client

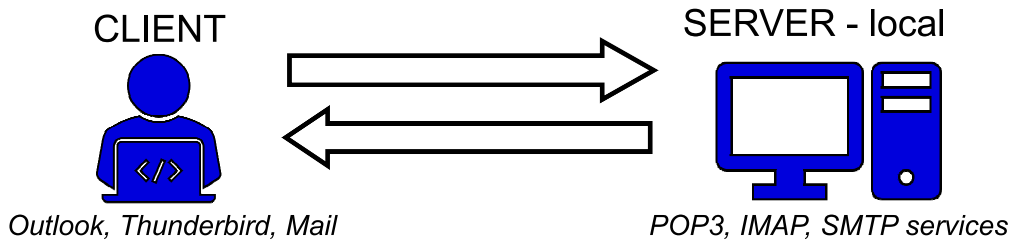
IMAP protocol

- Sends email headers only
- The content of the email will be sent upon request
- All email folders are on the server
- Convenient when reading mail from multiple computers

POP3 protocol

- Sends all new whole emails
- Removes them from the server
- Sorting emails into folders on the local computer
- Suitable for offline reading

Email via local client



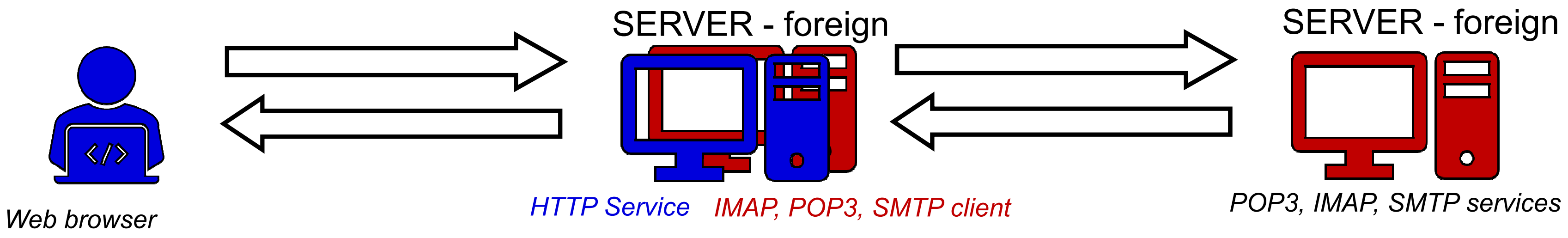
CLIENT

SERVER - local

Outlook, Thunderbird, Mail

POP3, IMAP, SMTP services

Email via web interface



SERVER - foreign

SERVER - foreign

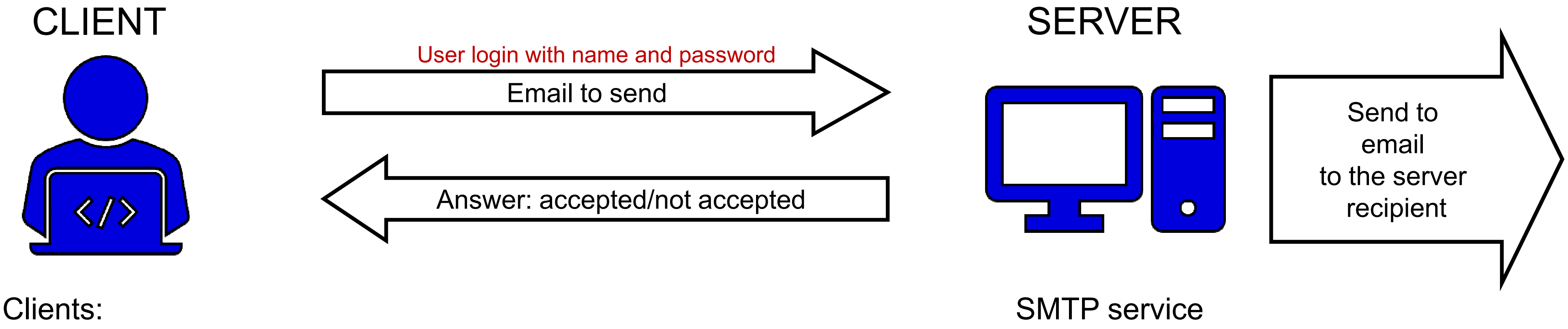
Web browser

HTTP Service IMAP, POP3, SMTP client

POP3, IMAP, SMTP services

SMTP service (sending mail)

- SMTP is a service for sending email, especially when using email clients


CLIENT
SERVER
User login with name and password
Email to send
Answer: accepted/not accepted
Send to email to the server recipient
SMTP service

Clients:

- MS Post 10
- MS Outlook
- Mozilla Thunderbird
- Apple Mail

Virtual private network (VPN) service

- The service simulates the connection of a remote computer to the local network
- "Tunnel" to the remote network
- The remote computer is assigned a local IP address
- The remote PC then becomes "almost" a full-fledged part of the internal network
- Used for remote access to work, for example in HO
- It is always necessary to install some client software
- Nowadays, PCs with Windows, MacOS and Linux are mostly supported, but also mobile devices with Google Android or iOS.

VPN service for MU students and employees

- The MUNI VPN provides staff and students with access to the university network from home, abroad or another university.

- To log in, you need to know the User ID + secondary password

- This allows students and staff to use services that are only available from the university network, even if they are not currently on the network. By connecting to the VPN, you get a public address from the MU range, for example:
  - access to MU's paid information resources: http://ezdroje.muni.cz/prehled/abecedne.php?lang=cs
  - Access to paid university licenses: https://it.muni.cz/sluzby/software
  - access to services available only from the MU network (e.g. specialised equipment and devices)

- For more information visit: http://vpn.muni.cz/ (OpenVPN)

Network services

IT security policies

See file

Network security.pptx

MUNI
MED

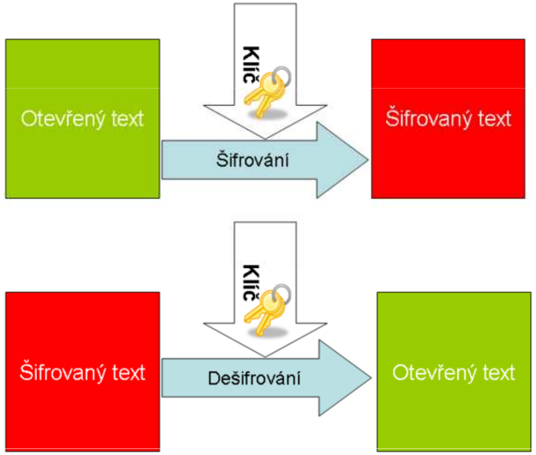
Encryption and electronic signature

Encryption

- Changing the form (encoding) of text and data into a form that is unreadable without knowledge of the decryption key (password)

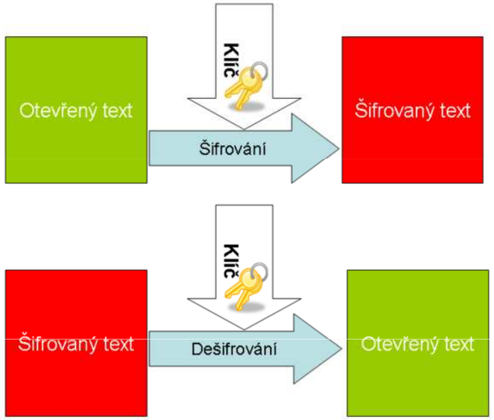
- You can encrypt e.g.
  - Documents (7zip, winrar - symmetrically)
  - Emails (email client support, recipient public key)
  - Network communication (https, sftp, imaps, ssh)
  - Disks (truecrypt, realcrypt, bitlocker)

- Confidentiality of communications and documents

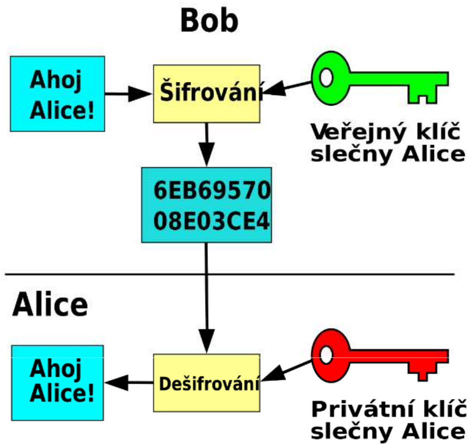


Types of encryption

- Symmetric encryption
  - Simpler form, a single key is used for encryption and decryption - the password



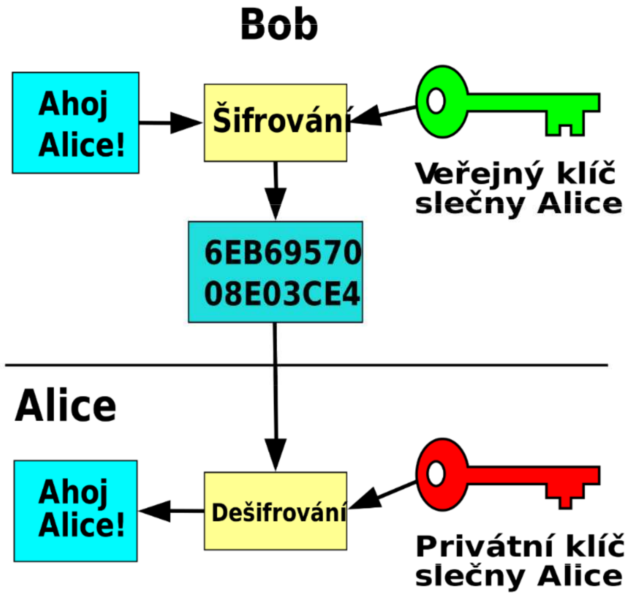
- Asymmetric encryption
  - The key has two parts, **private** and **public**



Asymmetric encryption

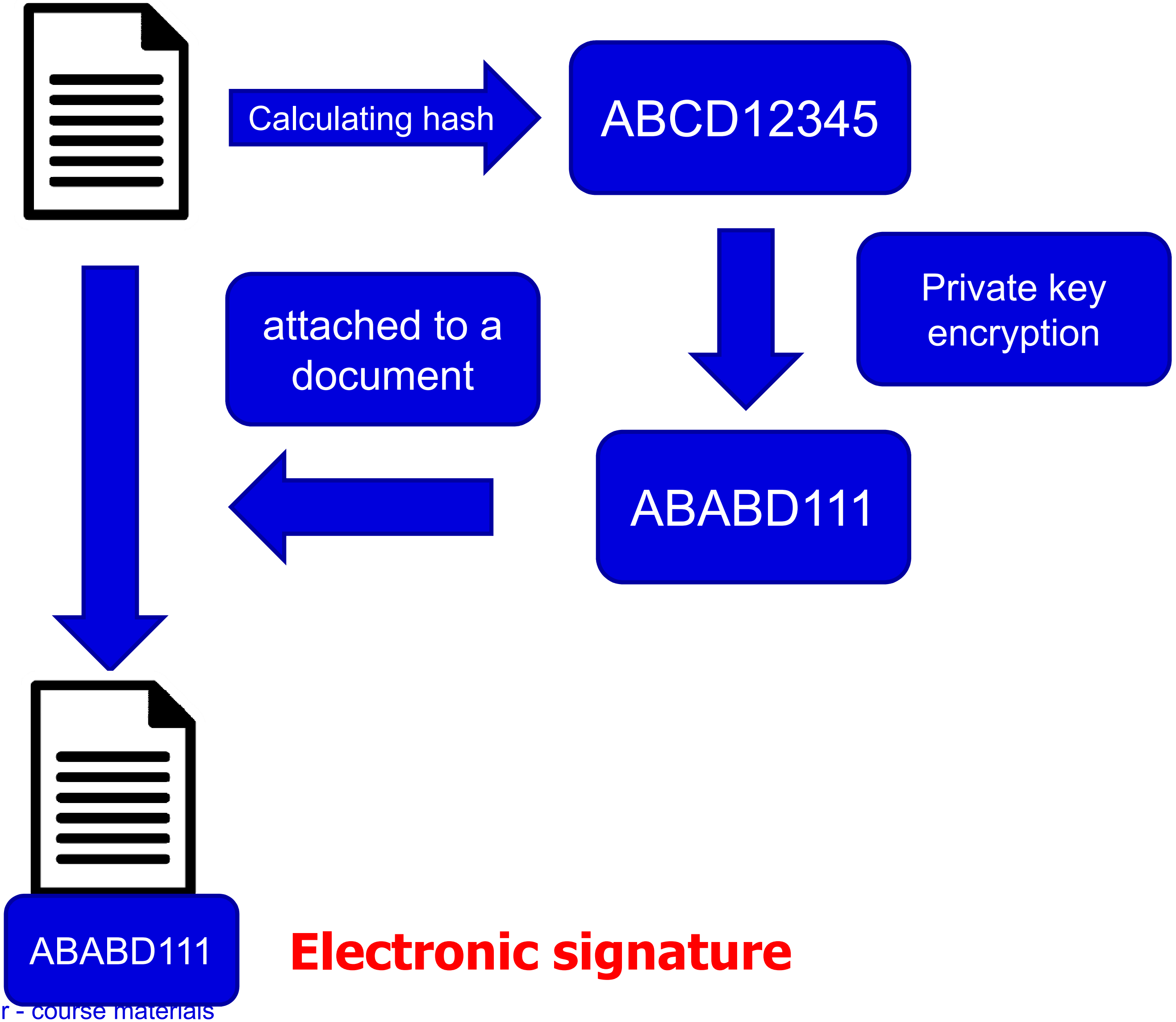
The key has two parts, **private** and **public**

- If someone wants to send me **encrypted** information, they encrypt it using the **public part of the recipient's key**.
- The only one who can decrypt this data is the owner of the private part of the key, i.e. me



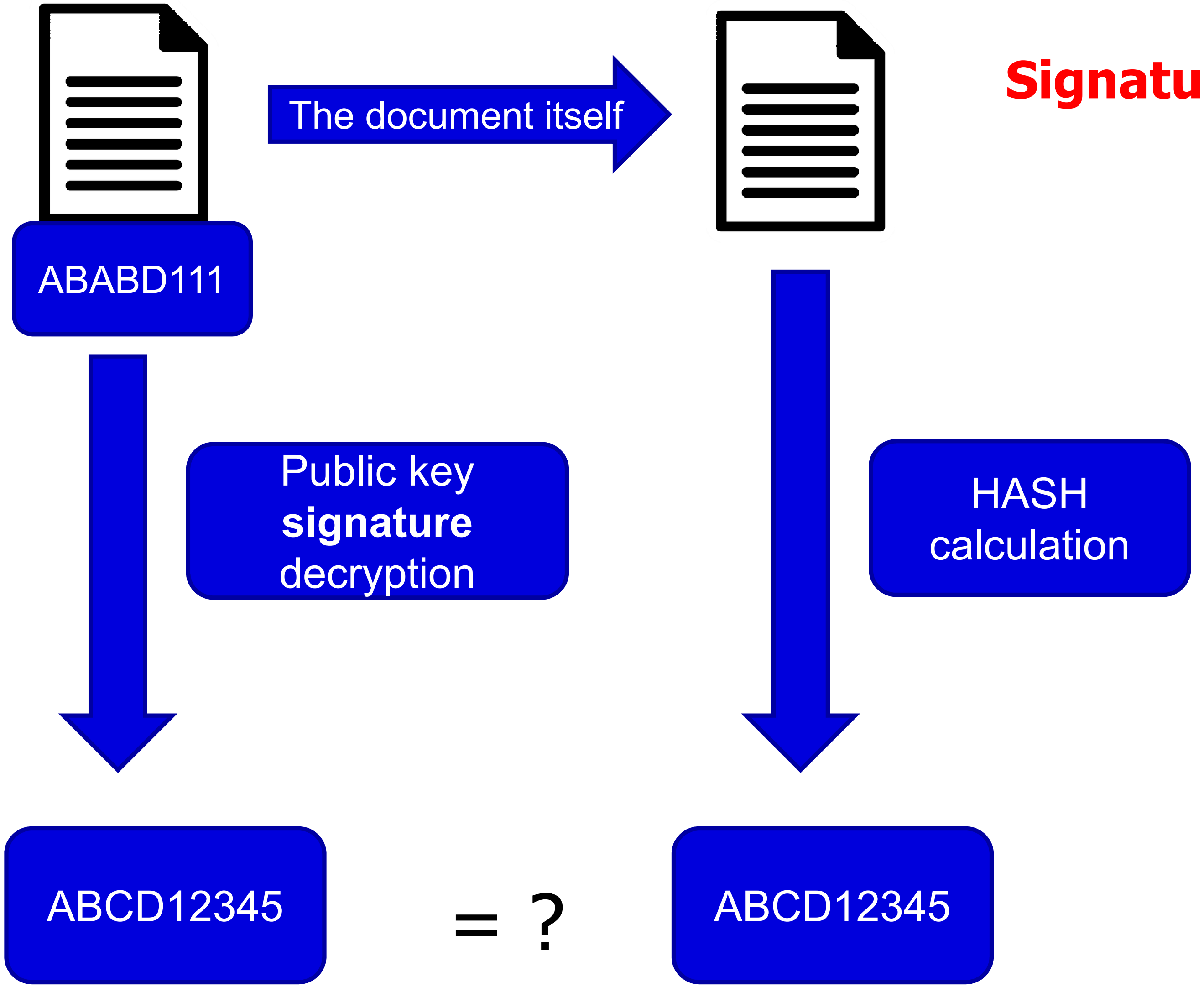
Electronic signature

- **Uses elements of asymmetric encryption**
- If I want to digitally **sign** some text, I just need to use the **private** part of the key for signing (done by email client, PDF editor)
- Anyone who knows the public part of my key (it is sent automatically with the signed email) can then digitally sign the text
  - Read more
  - **Verify that I am the author/submitter**
  - **To verify that the text has not been tampered with**
- Signed email/document **is not encrypted!!**
  - You don't have to "calculate" or remember anything, an email client or other application (pdf reader) will do the job
- **In its basic form, it is not intended for signing archival documents with long-term validity**



Electronic signature

Signature verification



The document itself

ABABD111

Public key **signature** decryption

HASH calculation

ABCD12345

= ?

ABCD12345

Digital certificate

Physical = computer file from the certification authority

- Issued by a certification authority
- Limited certificate validity (usually 1 year)

Contains

- **Subject data** (user, server)
  - Name
  - E-mail address
  - Other identification data
- **Subject public key**

The separate component is the corresponding private key

Can be revoked (revoked) if the private key is disclosed

Qualified x commercial certificate

Qualified x commercial certificate

Act No. 297/2016 Coll., the Act on trust services for electronic transactions

Qualified certificate

- **Issued by a qualified** trust service **provider**
- **https://www.mvcr.cz/clanek/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru.aspx**
  - Czech Post (PostSignum)
  - First Certification Authority, a. s.
  - eIdentity a. s.

Digital certificate - how to get it practically

Issued by so-called certification authorities (e.g. Czech Post)

1. Login to the web (or download the off-line) application
2. Self-generated and saved key pair with password
3. Completing the application
4. Visit a branch with an application, verify data
5. Inclusion of the public part of the key by the CA in the list of authenticated keys
6. Receiving a signed certificate with a public key and identification

Can be easily integrated into used email applications in the form of a certificate = guaranteed digital (electronic) signature

At MU, you can obtain a free personal digital certificate for users at http://pki.cesnet.cz/cs/tcs-personal.html

Electronic signature and eIDAS

electronic signature (FO) - expresses consent

electronic seal (PO)

a. Qualified Electronic Signature (QES):
- Must be based on a qualified certificate for electronic signature
- It must be created using a qualified (secure) electronic signature creation device (smart card and USB token = **QSCD** (from: Qualified Signature Creation Device).

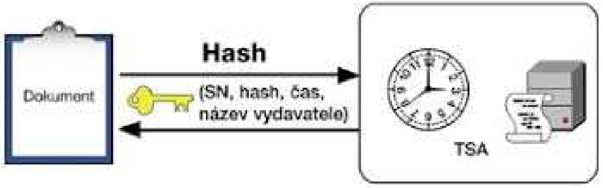
b. **a guaranteed electronic signature based on a qualified certificate**
- Must be based on a qualified certificate
- A qualified device (certified smart card/token) is not required.

c. Advanced Electronic Signature (AdES)
- No specific certificate requirements

Recognized electronic signature = common designation for a. and b.

Electronic time stamp

- Evidence that the document existed in the relevant form at the time.
- Combined with electronic signature
  - "Extend" the validity of the e-signature
- Limited validity, but longer than e-signature
- Simple and qualified stamp

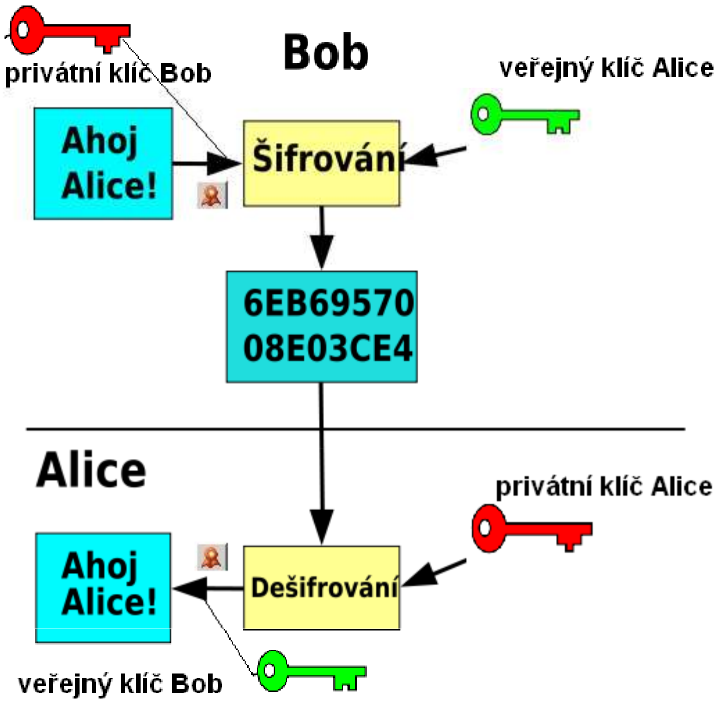


Electronic signatures in practice

Application behaviour

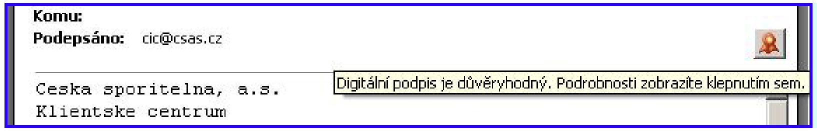
- When programs tell us that a particular signature is valid, we have to find out for ourselves whether it is a recognized signature or a commercial certificate signature.
- Conversely, if they tell us that they can't verify the validity of the signature (i.e. the validity of the signature is unknown), it may just be because the certificate is not in the right place in the trusted certificate store.
- Applications often do not verify certificate revocation
- The email signature does not include the subject line or the sender's address
- The sender's email is not verified to match the email in the certificate

Encrypted email



1) Bob **signs the** message **to** Alice with his private key

2) The email **is encrypted** with Alice's public key



Komu:
Podepsáno: cic@csas.cz

Digitální podpis je důvěryhodný. Podrobnosti zobrazíte klepnutím sem.

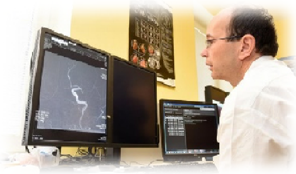
```
Ceska sporitelna, a.s.
Klientske centrum
```

3) Alice **decrypts the** message with her private key

4) **She'll verify** Bob's signature with his public key

Remote Person Authentication

... or how to remotely prove it's me



1) Something unique I know

Means of proving identity

2) I have something unique

Level of assurance

- **Low**
- **Considerable**
- **High**

eidentita.cz
KLÍČ K ELEKTRONICKÝM SLUŽBÁM

Security level of proof of electronic identity

Means by level of trust:

Low - e.g.: login + password
Substantional - two-factor authentication = SMS confirmation, OTP = One Time Password
High (chip card, electronic ID card)

Means of proving identity

- **Passwords**
- **Tokens**
- **Cards**
- **Biometrics**
- **Mobile phones**

The issuance of these resources and the actual authentication of access is handled by

- **A) Target service provider**

- **B) According to the NIA concept of "Identity provider"**
  Identity resource provider

eidentita.cz
KLÍČ K ELEKTRONICKÝM SLUŽBÁM

Identity resource provider

- State
  - Electronic ID card from 1 July 2018
  - Password + one-time SMS code

- Private provider
  - Running certification
  - Banking Identity

Where electronic signatures can be used

- when submitting a statement of income and expenses for self-employed persons
- for registration and deregistration for sickness insurance
- for VAT returns
- in electronic communication with the state administration
- electronic communication with regional and municipal authorities
- electronic communication with health insurance companies
- when applying for social benefits
- when applying for EU funding
- when signing invoices
- as an electronic signature of PDF documents

Source: en.wikipedia.org

Czech E-government

Optional chapter for international students

Czech E-government

- Data boxes
- Basic registers
- Electronic ID card
- Citizen Portal

Data boxes

- It can be used for the same purpose as an electronic signature in communication with the state administration
- Setting up and communicating with the state administration free of charge
- Not limited validity as for certificates
- Retains documents for 90 days only
- Works like a "web email", instead of an email address there is a mailbox code
- Communication outside the public authorities is subject to a fee
- Set up at the post office, simple form and OP

Basic registers

- ROB - population register
  - Linked to the population and foreigners register
  - Restricted access
- ROS - register of persons (business)
- RUIAN - Register of Territorial Identification, Addresses and Real Estate
- Birth number x AIFO (agenda identifier of a physical person)
  - Different citizen identification in different agendas

Electronic ID card

- Issued from 1.7. 2018
- Contact technology
- Allows you to log in to electronic government services
- Activation required at the office
- Allows you to upload a signing certificate
- You need a card reader (laptop or external)
- Access codes (PIN)
  - BOK, IOK, DOCK, PIN, PUK, QPIN

Citizen Portal

- https://obcan.portal.gov.cz
- Login via eOP or data box
- Gradual rollout of services
- Overview of documents
- e-Prescription

Electronic health care

National register of health professionals

- According to Act 372/2011 Coll.
- Medical and non-medical staff
- The record is created automatically by the educator after the completion of education
  - Basic field, specialization, certification courses
- Registration of employees by the employer (health service provider)
- **Employee** = looks up, adds contact details, takes a printout
- **Provider** - obligation to register employed healthcare workers

E-prescription

- Central recipe repository
- Identification of patients against ROB is ongoing (not necessary)
- Around 5 million e-prescriptions per month
- Server certificate (for the provider = for the ID)
- Recognised electronic signature (doctor)
- Login and password of the doctor, pharmacist
- https://www.epreskripce.cz/

Clinical data exchange in the Czech Republic

Types of communication

- Between information systems within the facility
- Between health facilities (HF)
  - Image data
    - PACS, DICOM ,
    - ePACS (http://www.epacs.cz/)
    - ReDiMed (https://www.medimed.cz/redimed)
  - Clinical data
    - **eMeDOcS ,** MEDICAL NET (CGM)**,** MISE (STAPRO), E-message
- Between health insurance companies and insurance companies
  - K-Benefits
  - Health insurance portals (commercial certificates)

International data exchange

- Patient summary
- ePrescription and eDispensation
- https://www.nixzd.cz/

Data structure (1/2)

- Laboratory data
  - NČLP - National codebook of laboratory items
  - Division: system (blood), component (ERY), quantity (number), unit, procedure (FLOWCYT)
- Medicines
  - SÚKL code - corresponds to the code in the VZP codebook
    - 7-digit number
    - Specific product
    - 0046224 - Panadol - POR TBL FLM 24X500MG
    - http://www.sukl.cz/modules/medication/search.php
  - ATC classification
    - Active ingredient
    - Anatomical-therapeutic-chemical groups
    - Hierarchical code layout
    - N02BE01 - Paracetamol (N Nervous system)
    - L01BC02 - Fluorouracil (L **Cytostatics and immunomodulatory drugs)**
    - www.whocc.no, http://www.sukl.cz/modules/medication/atc_tree.php

Data structure (2/2)

- Healthcare payers
  - Standard VZP (K Benefits)
  - Methodology for the acquisition and transmission of VZP ČR documents
  - www.vzp.cz - Providers
  - Dialers
    - Performance dial
    - HVLP - mass-produced medicinal products
    - Medical devices
    - ICD-10 - International Classification of Diseases version 10

MKN 10

- Czech translation of ICD - 10
- International Statistical Classification of Diseases and Related Health Problems
- Approximately 14 thousand items
- Hierarchical code structure
  - Xnnnn, Xnn - disease
  - A, B - Infectious diseases
  - C - malignant tumours
    - C50 breast cancer
    - C502 breast cancer - upper inner quadrant of the breast
- Web: https://mkn10.uzis.cz

Classification in oncology

- MKN classification - O
  - Currently version 3
  - Translation of the International Classification of Diseases (ICD) - O
  - Morphological code
    - **M - 8140/ 3 1**
      - **histology/behavior (grade)**
  - Topographic code
    - **C50.2 Upper inner quadrant of the breast**
- TNM classification
  - Extent of cancer
    - T - size of the tumour itself (T1 to T4)
    - N - involvement of adjacent lymph nodes (N0 - N3)
    - M - metastatic involvement (M0/M1)

HL7

- Health level 7
- Worldwide distribution
- Centre in the USA
  - www.hl7.org
- Branches in individual countries
  - www.hl7.cz
- "Factory" for communication standards in healthcare
- Limited distribution in the Czech Republic

CDA

Clinical document architecture

- HL7 application
- Formalized clinical document (medical reports)
- 3 levels of formalisation
  - Formalized header + unstructured text
  - Header + split text into blocks
  - Fully structured machine-processable content
- CDA templates prepared for specific documents
- Applied e.g. in Austria, Poland

SNOMED

- Clinical terminology
- Managed by the International Health Terminology Standards Development Organisation (IHTSDO)
- Not only the terms, but especially the links
- Multi-axial arrangement
- Basic unit = concept
- Basic structure
  - Concept (Concept)
  - Description
    - FSN - **Fully Specified Name**
    - *Preferred Term*
    - *Synonyms*
  - Bonds (Relationship)

SNOMED

- Approximately 400 thousand concepts
- **19 root concepts**
  - Observable entity (questions)
  - Clinical finding (answers)
  - Procedure
  - Body structure
  - Organism
  - Substance
  - Pharmaceutical products
  - Physical force
  - Physical object
  - ..
- **Concept name (**"semantic tag"**)**
- Fracture of foot (disorder)

Test

- In IS:
  - Student -> select subject UPS -> Answering machines
  - Select "UPS test english version" -> "I want to build the first set of questions"
  - At the end "Save and evaluate"
- Answered by
  - 20 questions
  - 60 minutes - Cannot be interrupted
  - 5 attempts to carry out the evaluation
  - For some there are more than one correct answer (each for a point)
  - Deduction of points for incorrect answers
  - The minimum to qualify is 15 points

MASARYKOVA UNIVERZITA