Unit 2 - Technical Basics

1.1Relevance of technology in healthcare

The capacity to systematically develop things and to examine them scientifically is presumably one of the most unique characteristics of mankind. Looking at the history of evolution in connection with technical developments, it quickly becomes clear that these developments are exponential. After all, technology and its respective development and distribution is one of the most significant economic sectors of our modern times.

In the 1920s, the Soviet economist Nikolai Kondratieff developed his theory on the "Long Waves of the Business Cycle," which is still used today as the theoretical basis for paradigm shifts in the economy. Kondratieff's theory describes that there is no uniform course in the market economy, but a regular upswing and downswing (cycles). The long waves of a period have a time span of about 40 to 60 years. During this period, particularly groundbreaking inventions (basic innovations) play a role and have a longer-term impact on the market economy.

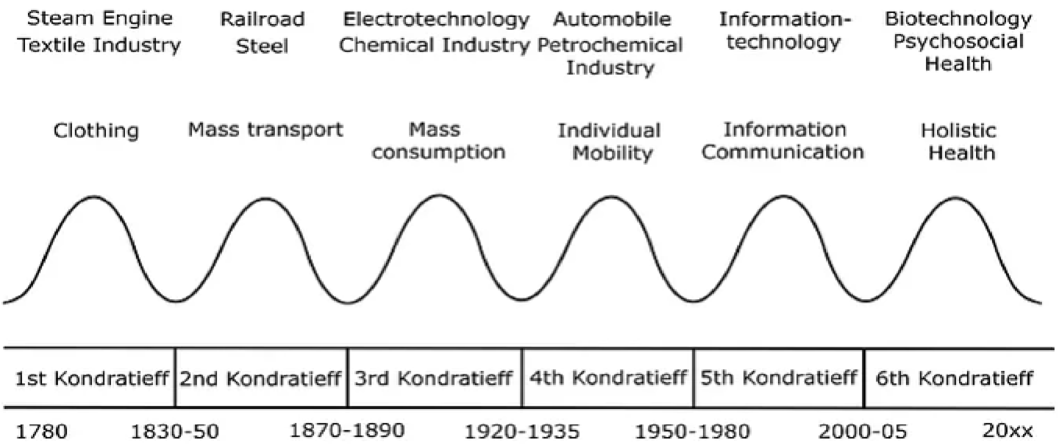


Figure 1: Kondratieff cycles with basic innovation and important fields of application[1]

[1] Source: http://www.gfmonline.de/hintergrund.html (accessed 11/23/2020).

The 5th and 6th cycles are particularly significant for the development of healthcare telematics. In the 5th Kondratieff cycle, information technology continued to grow and has since provided the basis for globalized communication. The 6th cycle describes the growing importance of health as an economic good. These two development cycles thus paved the way for new techniques and procedures in medicine and are the "foundation" of new and modern fields such as health telematics. [2]

Medicine has always been revolutionized by new technical procedures, and in recent years the focus has increasingly been on optimizing and further developing existing technologies.

Digitization enables medical concepts and strategies to be implemented more quickly and allows treatment techniques to be designed with greater effectiveness and efficiency. In this context, particular emphasis should be placed on medical technology, which is equivalent to a technical interface between diagnostics and therapy. In this area, existing technological developments from other fields of technology are primarily adopted and integrated into medical processes with the objective of improving medical care to benefit the patient. Medical technology is thus not only an important component of the healthcare system, but also a special focus of health telematics. From the point of view of health policy, the use of technology in medicine or in the healthcare system has the following main tasks:

- Ensuring the quality of medical care
- Improvement of diagnostic and therapeutic options
- Promotion of medical and technical research
- Reduction of costs by shortening the duration of illness and hospital stays (economic benefit effects)
- Easing the workload of the medical-therapeutic staff
- Meeting process and performance quality in health care

[2] cf. http://www.kondratieff.net/#!kondratieffcycles/c1xd0
[3] cf. http://www.newbooks-services.de/MediaFiles/Texts/5/9783642161865_Excerpt_001.pdf

Basics of communication

Transmission rates

The term "data transmission rate" describes the possible amount of digital data that can be sent over the respective transmission channel in a specific unit of time. The smallest data unit is a BIT, which is why the data transmission rate is mostly specified in bits per second (b/s). If, for example, a transmission rate of 250 Mbps is specified, this means that the transmission channel in question has a transmission rate of 250,000 bits per second. Today (year 2020), common speeds for Internet connections for business customers vary from 100 Mbit/s, or 250 Mbit/s, to 1,000 Mbit/s for a fiber optic connection. For the transmission of digital data and, above all, digital images, the upload speed to the Internet is important in addition to the so-called download speed from the Internet, for example, when digital X-ray images are transmitted from a physician's office to the telematics infrastructure. Depending on the connection contract selected with a provider, the upload speed varies from 50 Mbit/s for a 250 Mbit/s connection contract to 100 Mbit/s for a 1,000 Mbit/s connection contract.

The calculation of the size of a digital image can be described with the following formula, where the image resolution is described in dpi (dots per inch):

File width (inch) x file height (inch) x image resolution (in dpi) = file size in bytes

The size of a digital image depends on the recording method (color depth, 3D recording, image sequences, video) and the compression method. The size can vary from a few megabytes (MB) to several gigabytes (GB). The transmission of the image from the sender to the receiver then takes a correspondingly long time.

DSL

DSL is the improved successor to the ISDN connection. In this case, the abbreviation DSL stands for Digital Subscriber Line and can be described simply as a private line. As a new transmission standard, DSL enables a much higher transmission rate and improves the quality of Internet performance for residential customers, especially through high download and upload rates. To achieve this, a larger frequency range is used, which means that two modems are required (at the provider's exchange and at the user's premises). To enable a good Internet and telephone connection in parallel, the customer's bandwidth is split into different channels. As the frequency range used for fixed-network telephony is much higher, a splitter is used in order to cut out this range. The digital signals from the customer's DSL modem (Internet) and NTBA (telephony) are transmitted to the network provider via a subscriber line (local loop). [4]

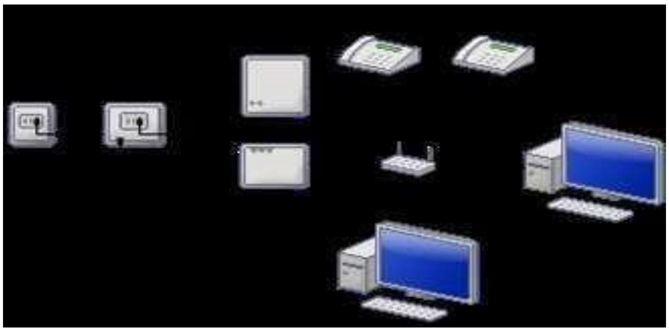


Figure 2: Exemplary structure of a DSL connection[5]

GPRS / UMTS / LTE

The abbreviations GPRS, UMTS, and LTE generally refer to different types of data transmission that use mobile communications as a common basis.

General Packet Radio Service (GPRS)

The General Packet Radio Service (GPRS) represents a packet-oriented service for data transmission. GPRS was developed as an extension to the previous standard for fully digital mobile communications networks, the so-called GSM (Global System for Mobile Communications, second-generation mobile communications standard - 2G), and enables a transmission rate of up to 50 kbit/s. This technology is mainly used in mobile phones. GPRS provides a permanent virtual Internet connection that only occupies free radio space when the user actually transmits data.

[4] cf. http://www.teltarif.de/internet/dsl/technik.htm

[5] Source: www.teltarif.de

Universal Mobile Telecommunications System (UMTS)

Contrary to GPRS, a Universal Mobile Telecommunications System (UMTS) is not an extension of an existing standard, but a data transmission standard as such. UMTS is a third- generation (3G) mobile communications standard and provides much higher data transmission rates than the previous GSM standard. UMTS makes transmission rates of up to 384 kBit/s possible. Various enhancements, such as HSDPA (High Speed Downlink Packet Access) or HSPA (High Speed Packet Access), make it possible to achieve even higher transmission rates. Basically, the UMTS standard converts voice into data packets and transmits them. Furthermore, the UMTS standard uses a larger frequency range than the GSM standard, which enables faster transmission of the data packets. Once they reach the receiver, the data packets are sorted, decrypted, and converted back into voice or individual data. This process makes for a more efficient use of the available bandwidth and creates space for simultaneous transmissions. [6]

Long Term Evolution (LTE)

To meet the growing demand for bandwidth and data transmission due to the booming smartphone industry, the fourth generation (4G) mobile communications standard was created with Long Term Evolution (LTE). With its extremely high data transmission volume of up to 300 Mbit/s, LTE provides a new level of mobile communications quality. The even higher frequency range creates mobile broadband coverage, especially in rural areas.

5G Next Generation Mobile Network

The successor to LTE (4G), 5G is the 5th generation of mobile communications, enabling up to 10 times faster data transmission and communication in real time. This means that an extremely high data rate of up to 10Gbit per second can be transmitted.
Providing telemedicine to rural regions, better network stability at major events, or fast mobile Internet for mobile gaming and streaming, for example, would be feasible.

[6] cf. http://www.izmf.de/de/content/was-versteht-man-unter-dem-mobilfunkstandard-umts

Bluetooth

The term Bluetooth refers to a radio technology for data transmission in the near-field range, which is used especially for mobile end devices (e.g. laptops or smartphones). With this method, the end device changes the transmit frequency each time a data packet is sent by converting the narrowband signal into a signal with a larger bandwidth.

This is to prevent many narrowband signals from being transmitted in the same frequency range, which would overload the network capacity. This process is referred to as frequency hopping, which usually takes place after each transmission of a data packet.

LAN / WLAN

Various types of communication networks are used for the further transmission of data. These networks can be classified according to their geographical extent.

The Local Area Network (LAN) is a network limited in its spread to a company, university, private household or hospital complex. Metropolitan Area Networks (MAN) are the next level of networks. They are regionally bounded networks that interconnect local area networks. LANs and MANs are closed networks. Wide Area Networks (WAN) and Global Area Networks (GAN) are the next tiers. These are public networks that form the basis for global networking. The various telecommunications services such as telephone and Internet are based on them.

[7] cf. http://informationszentrum-mobilfunk.de/der-neue-mobilfunkstandard-lte#header

[8] Cf. https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/was-ist-5g-vorteile-und-risiken-der-5-generation- mobilfunk-52004

Local Area Network (LAN)[9]

In a LAN, the individual computers (clients) are connected by cable to a switch or router and thus networked with each other. A connection to the Internet is also possible through this connection. The DHCP server (Dynamic Host Configuration Protocol) of the router assigns the corresponding IP addresses to the clients connected to the network. The speed or the level of the data transfer rate depends, among other things, on the type of cable used (electrical or optical) and is between 10 Mbit/s and a maximum of 10 Gbit/s. In addition to computers, other devices such as printers or fax machines can also be integrated into the network, enabling data exchange between the other connected devices as well.

Wireless Local Area Network (WLAN)

Contrary to the LAN, the Wireless Local Area Network represents a wireless network in which data transmission is ensured by corresponding radio standards (e.g. IEEE-802.11). In principle, WLAN allows all network or Internet-capable devices (computers, laptops, printers, smartphones, tablet PCs, etc.) to be connected wirelessly to an existing network and to access the Internet, for example. Basically, WLAN can be implemented in two different architectures. The two variants are *ad hoc mode on* the one hand and *infrastructure mode on* the other.

Ad-hoc mode does not require a router (access point) to be accessed by the connected device (client). The clients communicate with each other using WLAN cards, for example, and thus create self-contained small networks. However, if only a few end devices are to be networked, other transmission methods such as Bluetooth are recommended.

To achieve wireless Internet access or communication between several clients, the so-called infrastructure mode is used. A WLAN router with DSL modem forms the necessary base station (access point).

[9] cf.https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungWLAN-LAN/Funktionsweise/funktionsweise_node.html

Wide Area Network (WAN)[11]

A wide area network (WAN) is a computer network that covers a large geographical area. The concrete extent of a wide area *network* can be up to 10,000 km. WANs are used, for example, to interconnect several LANs, since an unlimited number of computers can be integrated into a WAN.

In Europe, the WANs are mostly operated by the major network providers and enable transmission rates of between 64 kbit/s and up to 622 Mbit/s. For these high transmission rates, however, the user must be provided with an asynchronous transfer mode (ATM)[12] by the provider.

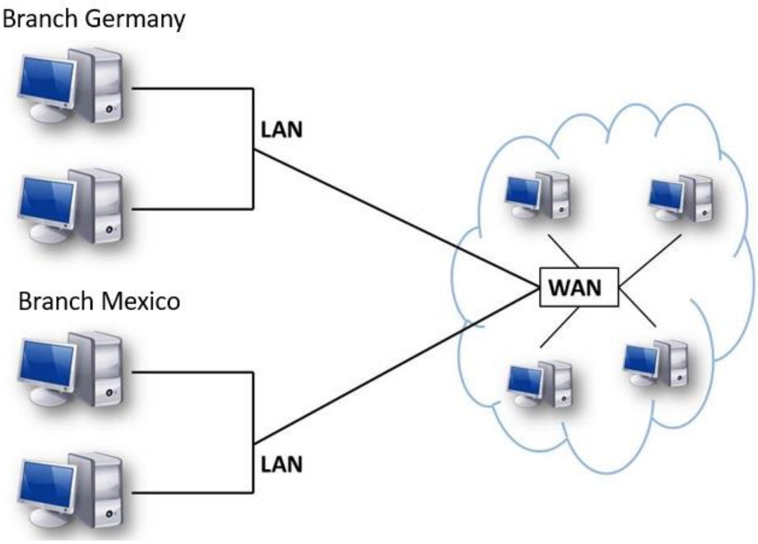


Figure 3: Exemplary networking of several LANs with one WAN[13]

[10] cf. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m03/m03058.html

[11] cf. http://www.itwissen.info/definition/lexikon/wide-area-network-WAN-Weitverkehrsnetz.html

[12] Special communication protocol for transmitting data, voice and video.

BAN

Body Area Networks (BANs) are networks consisting of sensors, which are used to transmit personal (vital) data for medical or sports monitoring of the wearer. The values collected can be parameters such as blood pressure, blood sugar, ECGs or heart rates. The sensors and actuators belonging to the network transmit the recorded values to a so-called body gateway, which is also worn on the body. The body gateway bundles the data and transmits it to the corresponding receiver (e.g., medical facility) with the help of an intelligent node (linking point of transmission paths). [14]

Since the BAN concept is mostly used in mobile applications, it is usually referred to as a wireless body area network (WBAN), which is fundamentally based on the wireless personal area network standard and uses transmission technologies such as Bluetooth. BANs are used frequently in telemedical applications, such as telemonitoring.

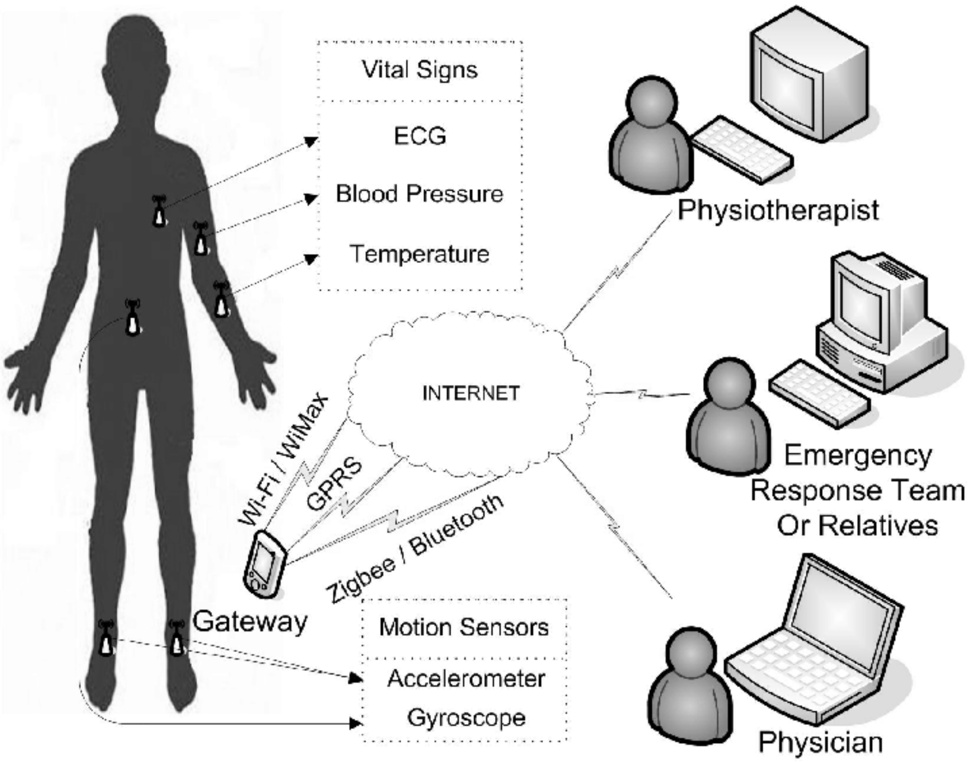


Figure 4: Systematics of a BAN[16]

[13] Source: own representation

[14] cf. http://www.itwissen.info/definition/lexikon/body-area-network-BAN-Koerpernahes-Netzwerk.html

[15] This is identical to WLAN, with the difference that WPANs are designed exclusively for the immediate vicinity of the carrier (approx.0.2 to 0.5 meter range)

[16] Source: https://www.researchgate.net/figure/Example-of-a-Body-Area-Network_fig4_255358241 [accessed Nov. 03, 2020].

Examples of modern solutions available on the market are fitness wristbands. When these have a Bluetooth interface and are therefore able to connect to a smartphone or a corresponding app, they are referred to as a BAN.

Figure 5: Modern fitness wristband and application using the Microsoft Band as an example[17]

IP protocol

The Internet Protocol (IP) is a network protocol and represents the worldwide network standard in LAN and WAN. The purpose of IP is the addressing (routing) and transmission (forwarding) of data packets between transmitter and receiver across different networks. The transmission is carried out connection-free and packet-oriented. [18]

IP addresses are the basis for transmitting data packets using IP protocols. These are addresses in computer networks that are assigned to corresponding devices that are connected to a network. The end devices can thus be clearly addressed (routing) and reached (forwarding) by others. An IP address could be compared to a postal address, for example, which enables the sender to send letters or packages to a targeted recipient. IP addresses consist of a fixed series of numbers, one consisting of the address part for the network identifier (net-id) and the other of the user part for the host identifier (host-id). The length of these number strings depends on the version of the Internet protocol used (example of an IPv4 address: 205.012.356.246). [19]

[17] Source: http://www.microsoft.com/Microsoft-Band/en-us

[18] cf. http://www.itwissen.info/definition/lexikon/Internet-protocol-IP-IP-Protokoll.html

[19] cf. http://www.itwissen.info/definition/lexikon/IP-Adresse-IP-address.html

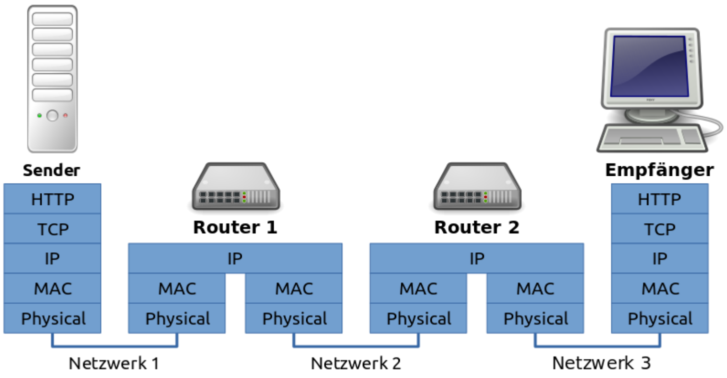


Figure 6: IP packet routing across two networks[20]

IP addresses can be assigned in two different ways. For this reason, a distinction is made between *static* and *dynamic* IP addresses. Static IP addresses are already assigned during the configuration of a device and cannot be changed. [21] In contrast, dynamic IP addresses are generated by a so-called Dynamic Host Configuration Protocol (DHCP). The DHCP protocol is a service that serves a dynamic and automatic configuration of end devices (e.g., the assignment of IP addresses).

Classically, the required IP addresses are requested from the DCHP server by a connected DCHP client and assigned. [22] This service can be performed, for example, via the router of a local area network (LAN).

DNS

The Domain Name System (DNS) plays a central role in IP-based networks. It represents an online distributed database system that translates IP addresses of computers into domain names. However, the DNS can also convert domain names into IP addresses; in this context, it is referred to as *name resolution*. The domain is the name of a computer on the Internet that people can understand, e.g. www.th-deg.de. At the heart of this service is a so-called DNS server. When a name query is made for a specific IP address, the domain name server uses the domain address to establish a connection to the next higher or lower name server within a domain. Roughly described, the DNS can therefore be described as a hierarchical directory service based on globally distributed servers, whose task is to manage the namespace of the Internet. [23]

[20] Source: Wikipedia
[21] cf. http://www.itwissen.info/definition/lexikon/Statische-IP-Adresse-static-IP.html
[22] cf. http://www.itwissen.info/definition/lexikon/dynamic-host-configuration-protocol-DHCP-DHCP-Protokoll.html
[23] cf. http://www.itwissen.info/definition/lexikon/domain-name-system-DNS-DNS-System.html

The representation of names on the Internet (domain namespace) is based on different domain levels and is called hierarchy. The top level of the DNS hierarchy is the *root server*. The effective range of the root server includes the names and IP addresses of all *name servers* and the *top-level domain (TLD)*. The top-level domain represents the second level and, in addition to the geographical assignment of the domain (Country Code Top Level - ccTLD), information about the organization. The third level of the DNS hierarchy is the so- called *second-level domain (SLD)*, which may only occur once within the TLD and contains specific information about the service. The TLD is subordinate to another level (*third-level domain*), which is colloquially referred to as a subdomain. Subdomains serve the logical and physical separation of services within domains of an organization. [24]

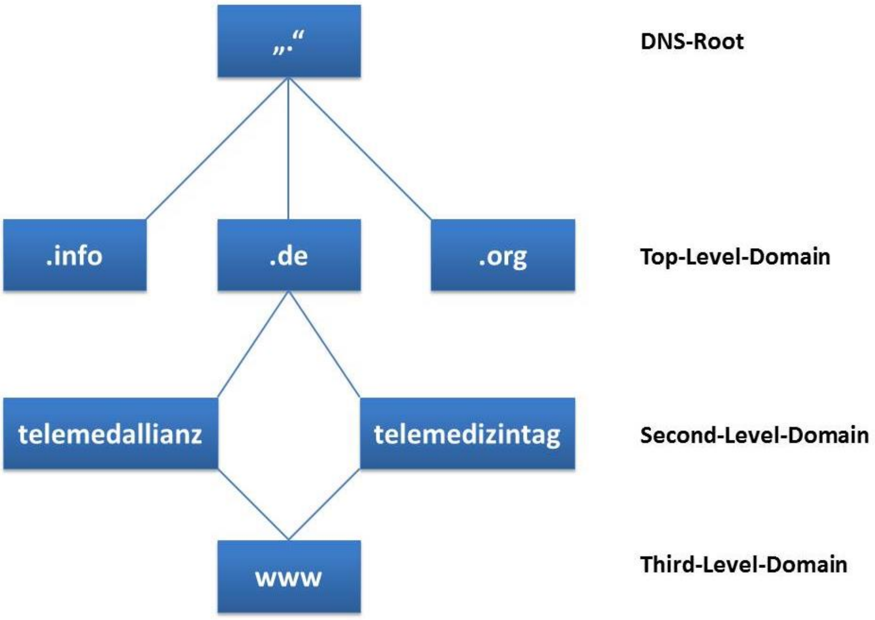


Figure 7: Hierarchy of the DNS address using the example of the domain www.telemedallianz.de and www.telemedizintag.de[25]

[24] cf. ibid.

[25] Source: own representation

HTTP/S

The acronyms HTTP and HTTPS are data transfer protocols within the framework of the Internet.

HTTP stands for Hypertext Transfer Protocol and is a stateless (general, stateless and object- oriented) protocol for the transmission of data. It is used, in addition to general data transfer, primarily to address Internet addresses (hypertext documents) from the Internet (World Wide Web) and load them in a browser. More precisely, the user's web client (browser) sends a request to the web server, which responds with a response to the client. Each time a new request for a document is made, the browser connects to the web server using the IP protocol and enables the transmission of the requested HTML documents. In this context "stateless protocol" that information from older requests of the client is lost. So-called cookies are used to store this information beyond a session. These make it possible, for example, to assign status information and run applications that require status or session properties. The addition "S" of the HTTP stands for *secure* and offers an encryption of the HTTP by means of a so-called SSL protocol[26].

This additional encryption of the protocol enables a secured transaction of the requests as well as authentication. [27]

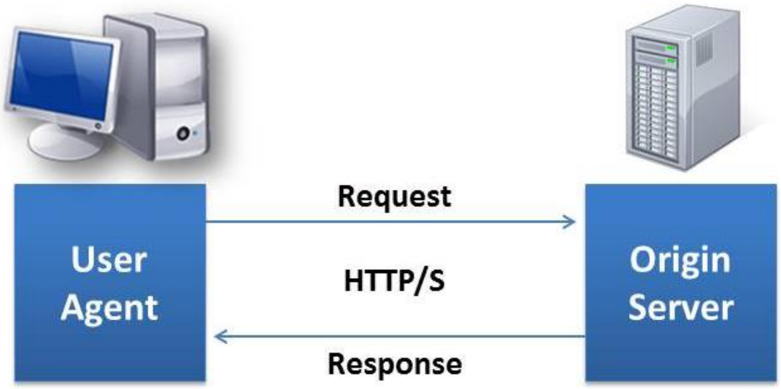
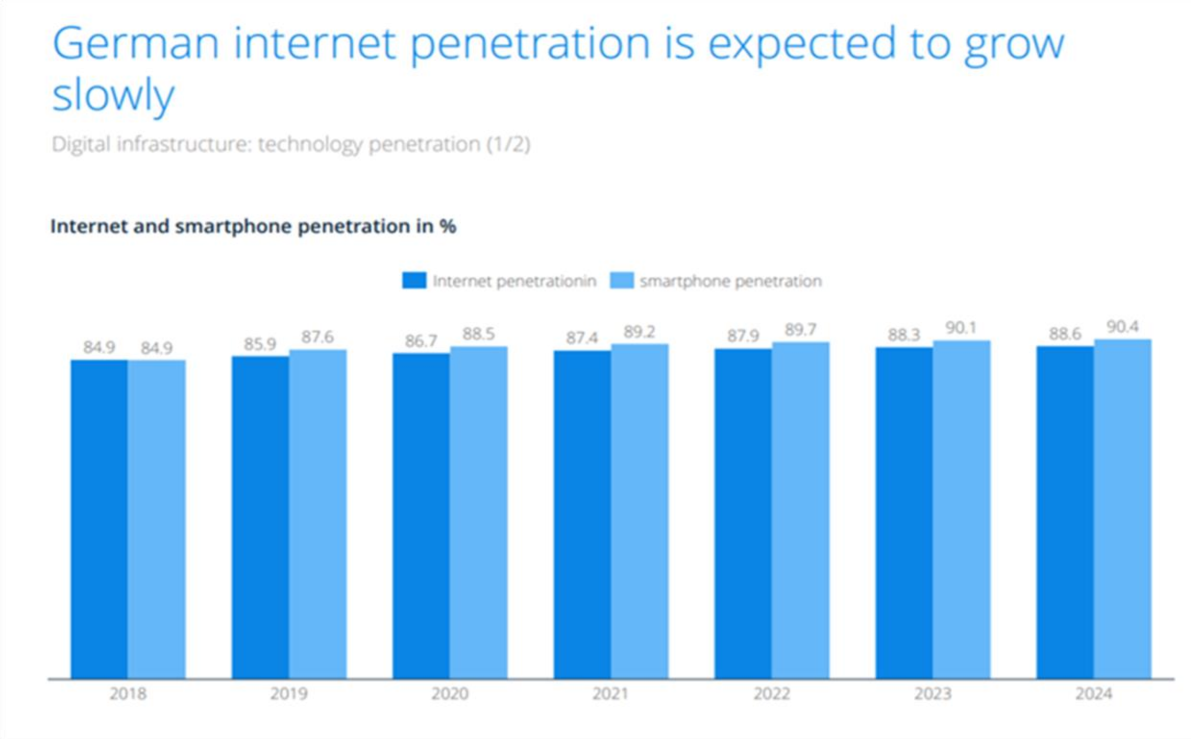


Figure 8: Request-response method of HTTP/S[28]

[26] This is primarily used for the secure transmission of data on the Internet. For more information, see http://www.ssl.de/ssl.html

[27] cf. http://www.itwissen.info/definition/lexikon/hypertext-transfer-protocol-HTTP-HTTP-Protokoll.html

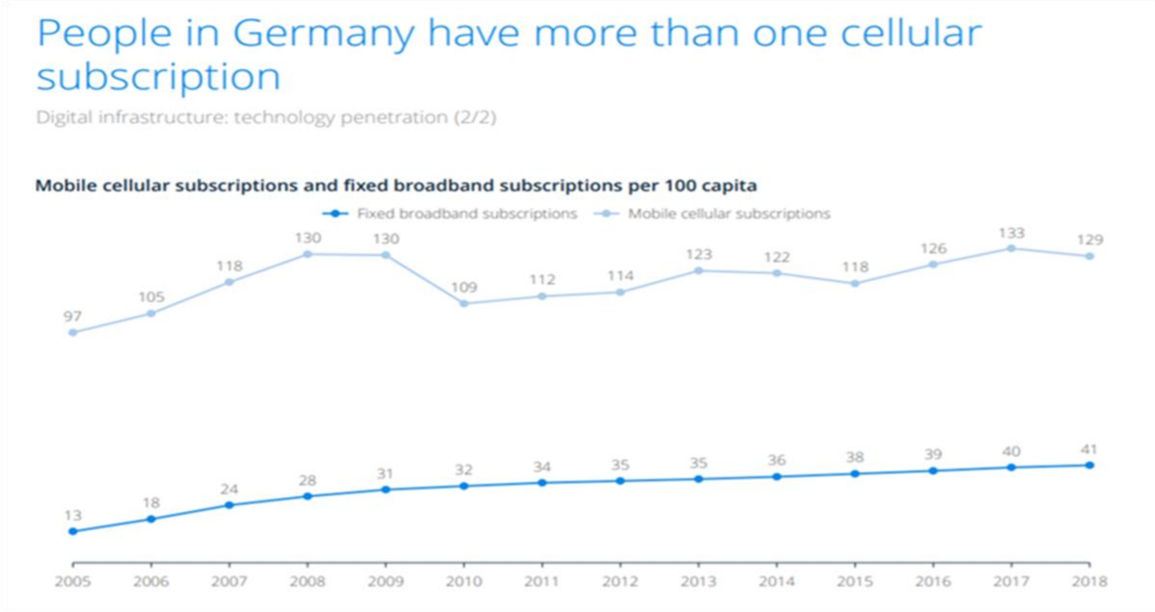
[28] Source: own representation



German internet penetration is expected to grow slowly

Digital infrastructure: technology penetration (1/2)

Internet and smartphone penetration in %



People in Germany have more than one cellular subscription

Digital infrastructure: technology penetration (2/2)

Mobile cellular subscriptions and fixed broadband subscriptions per 100 capita

[29] Source: https://de.statista.com/statistik/studie/id/50712/dokument/ehealth-market-report-germany/, retrieved 11.03.2021

[15]Source: https://de.statista.com/statistik/studie/id/50712/dokument/ehealth-market-report-germany/, retrieved 11.03.2021

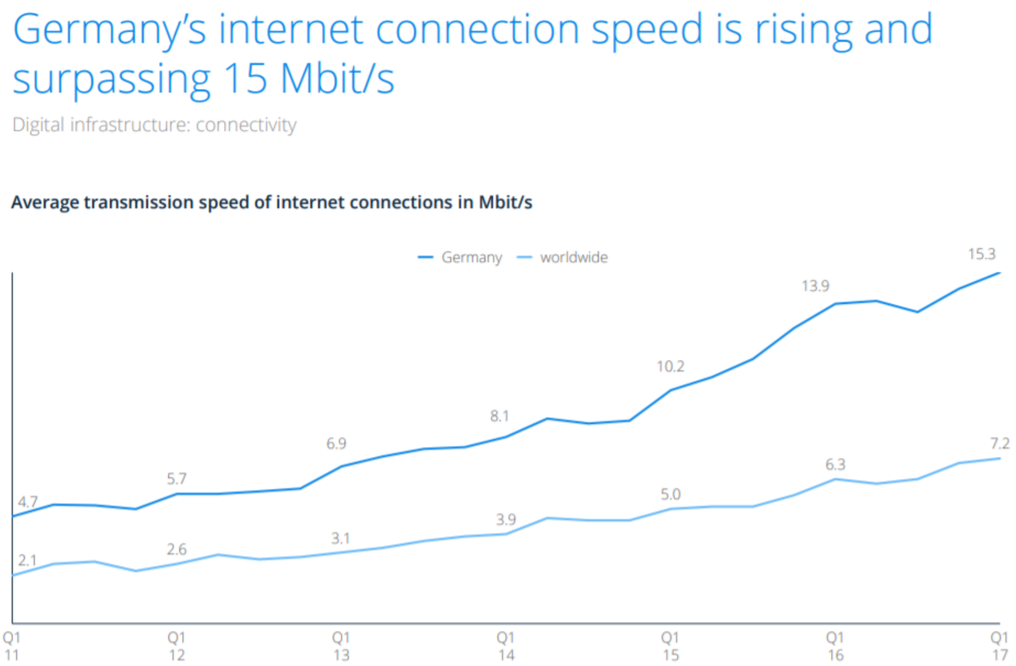


Figure 9: Internet connection speed in Germany[31]

1.3 Security mechanisms

The various wireless communication infrastructures as well as mobile end devices contribute not least to the improvement of our mobility and flexibility. However, advancing digitization also entails a steadily increasing desire for data privacy and data security, thus generating an increased need for digital security mechanisms and "secure" transmission procedures. The rule is: "Access to data and systems should only be granted to those who are authorized to do so or have a legitimate reason to do so." General requirements for security mechanisms and systems are[31]:

- *Confidentiality*
  - Authorized users can only access secure data through authorization or identification.
- *Integrity* (*Integrity*)
  - Used data must be intact and the operation of the requested service must be correct.
- Availability (*Availability*)
  - A service must always be available when it is needed

[31]Source: https://de.statista.com/statistik/studie/id/50712/dokument/ehealth-market-report-germany/, retrieved 11.03.2021

[32] cf. https://www.datenschutzzentrum.de/backup-magazin/backup01.pdf

The best-known mechanisms for securing data are encryption procedures. Basically, encryption methods can be used in two areas.

This is, on the one hand, the encryption of data in order to transmit it over an insecure line and, on the other hand, encryption of data in a particular system in order to protect it from unauthorized access.

Electronic signatures

Electronic or digital signatures serve to guarantee the integrity of transmitted data. These procedures are intended to ensure that both the sender and the recipient have the same data basis and that unauthorized changes during data transmission can therefore be ruled out.

However, the terms *digital signature* and *electronic signature* must be taken separately. The electronic signature is a legal term and describes an electronically generated, personal confirmation/identification.
A Digital signature is the technical term for an electronic signature. It therefore describes a specific technology or procedure.

To ensure data integrity, the digital signature creates a hash value (checksum) and uses it to sign and encrypt a file using a public key. To verify the authenticity and integrity of a file as a recipient, the corresponding hash value must first be recalculated, and the digital signature decrypted using the public key.

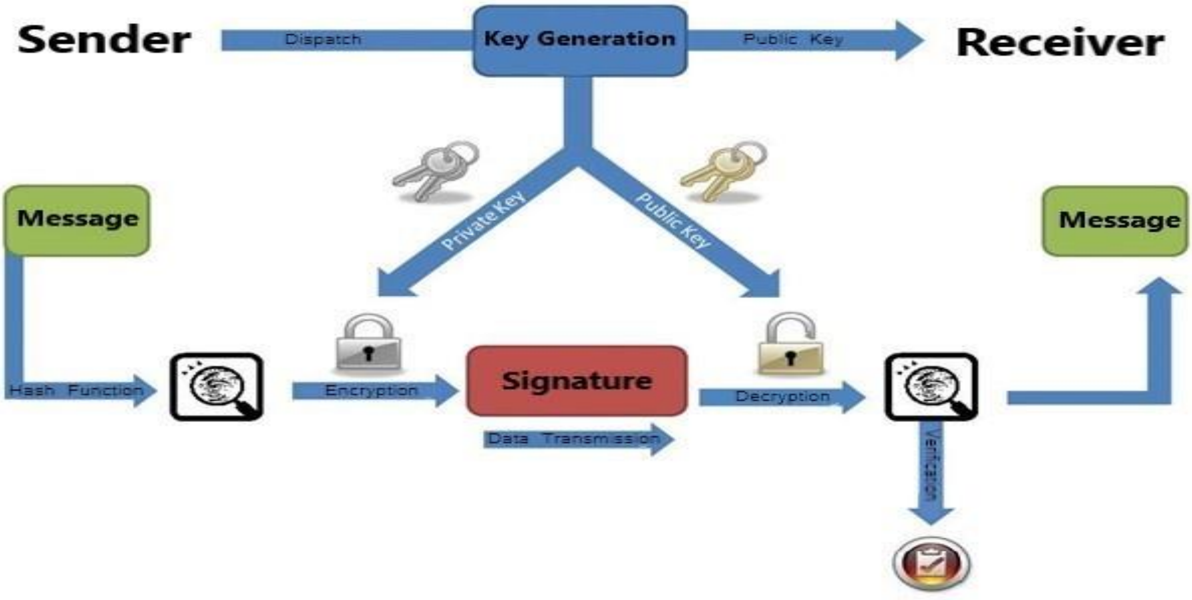


Figure 10: Message transmission with encrypted signature[34]

[33] cf. http://www.signature-perfect.de/docs/Leitfaden_Elektronische_Signatur.pdf
[34] Source: own representation

Digital certificates

The procedures presented so far have been about securing data by means of a special key. Digital certificates, on the other hand, are digital identity certificates whose purpose is to ensure the secure exchange of the respective keys. Like an ID card, digital certificates have the task of making a person or object identifiable in order to guarantee the unambiguous authenticity and integrity of data vis-à-vis third parties. [35]

One popular area of application is the *public key procedure*, in which the use of digital certificates is intended to ensure that public keys actually originate from the sender. For this purpose, a certificate is issued by a *certification authority* (also known as a *trust center* or *certification authority*) after careful verification of the sender. This system is known as the *public key infrastructure. The* certificates issued are electronic documents that contain not only the respective public key but also personal details or attributes of the sender. Furthermore, certificates contain information about the issuer as well as the issuer's digital signature. A certification authority can be, for example, a provider of digital signatures, a company department or even an authority. Certificates often comply with the X.509 standard and contain the following data fields[36]:

- the X.509 version number (today mostly v3)
- a serial number of the certificate
- an identifier of the used signing algorithm
- the validity period of the certificate
- the name of the issuer (certification body)
- the name of the owner
- the public key of the owner
- id numbers for holders and exhibitors
- if applicable, information on the type and scope of the certificate, alternative names for users and issuers, and other private issuer-specific enhancements.
- and a digital signature of the issuer

[35] cf. http://www.internet-sicherheit.de/institut/buch-sicher-im-internet/workshops-und-themen/verschluesselung-und- identities/cryptography/electronic-certificates/

[36] cf. Wind M. & Kröger D., 2006, pp. 284 - 285

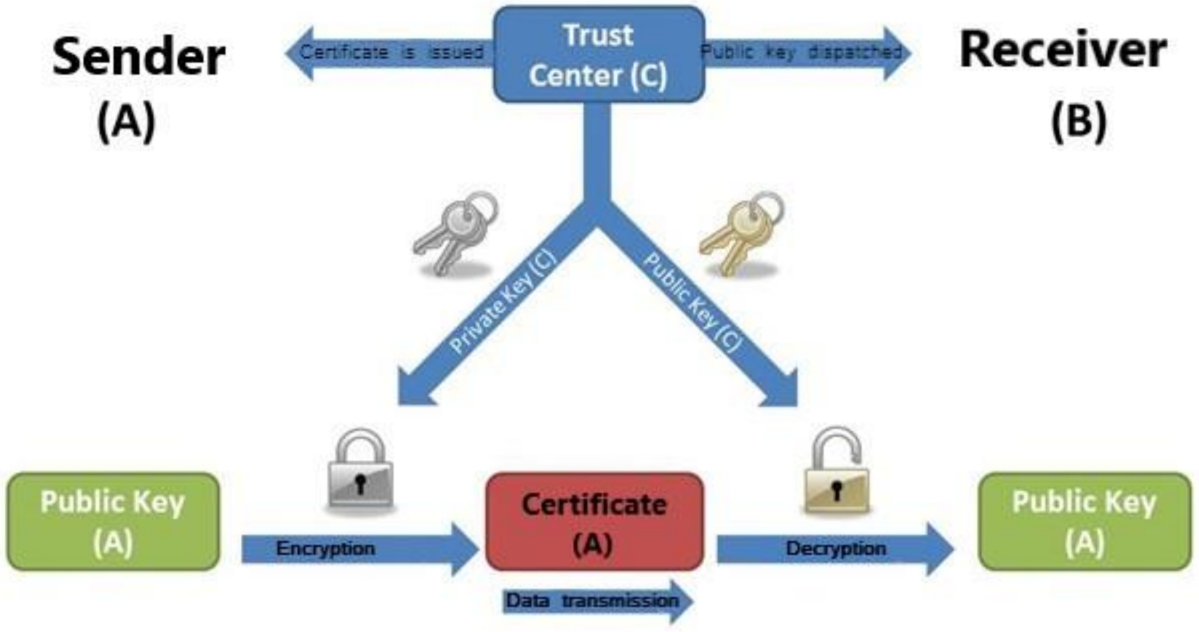


Figure 11: Public key infrastructure[37]

Biometric signatures

The biometric signature can be seen as an extension of the electronic signature and can be used, for example, for qualified electronic signatures. Authentication of users by means of biometric signatures is performed by recognizing specific physical characteristics, such as fingerprints, iris patterns, facial geometry or even digital signatures. First, a specific physical (biometric) feature is captured by optical, thermal, acoustic, chemosensory or pressure-sensitive methods. The captured features are converted into a digital pattern (template) using a special algorithm and stored on the intended medium (centralized or decentralized). [38] For the authentication process, the corresponding physical feature is captured using the same methods and then converted into a template using the same algorithm, which is compared with the one stored. [39]

Signature pads are becoming increasingly common in the clinical sector. These enable, among other things, the electronic documentation and archiving of a doctor's or patient's signature (e.g., on patient information forms). For this purpose, the captured signature is converted into a non-alterable and archivable PDF.

[37] Source: own representation

[38] cf. https://www.teletrust.de/publikationen/broschueren/authentisierung/

[39] cf. https://www.datenschutz.rlp.de/downloads/oh/ak_oh_biometrie.pdf

In combination with an electronic patient information form and an electronic patient file, for example, electronic archiving can lead to significant cost and space savings.

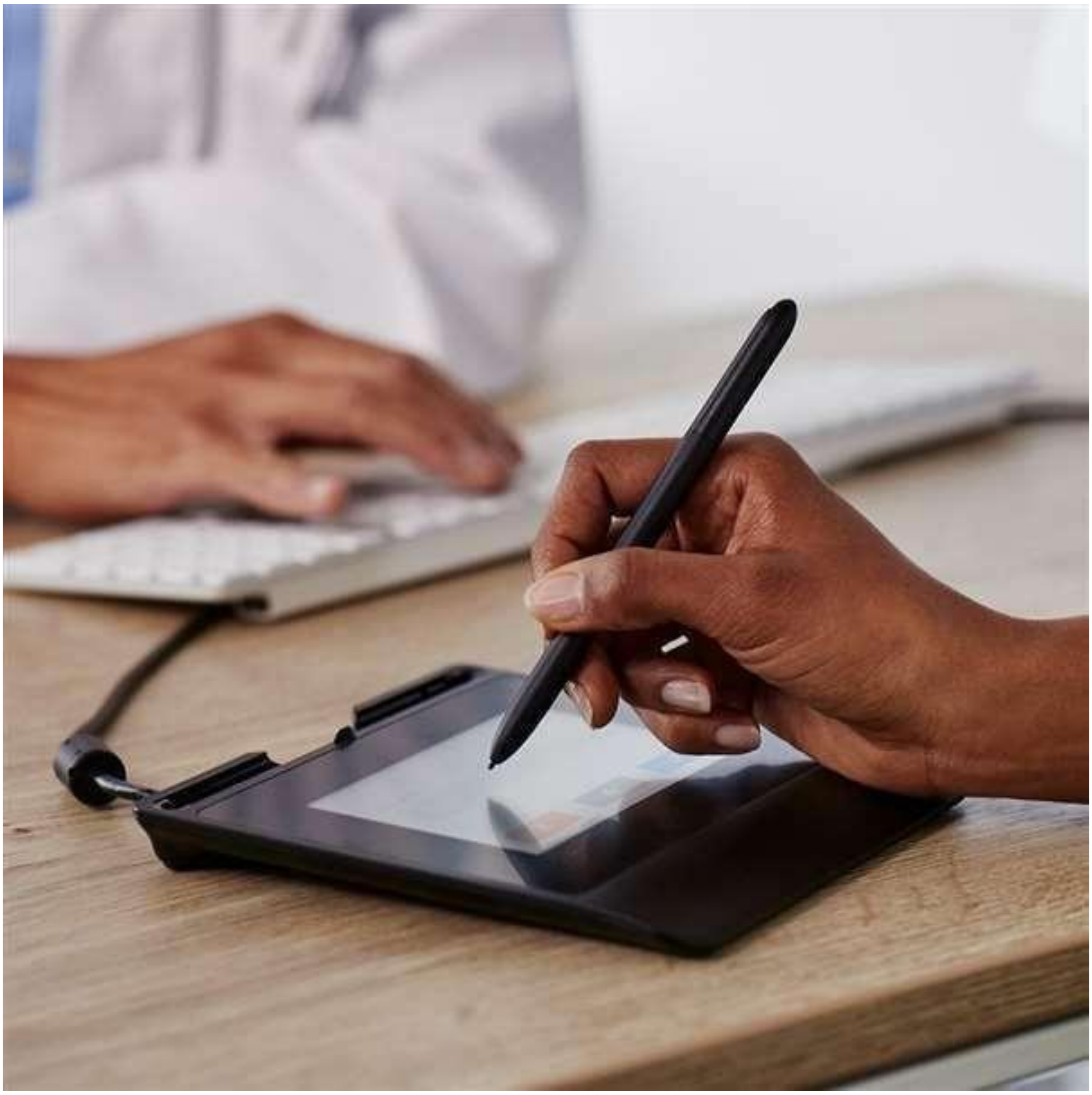


Figure 12: Signature pad from Wacom[41]

[40] cf. http://www.econsentpro.de/die-softwareloesung/elektronische-unterschrift/
[41] Source: https://www.wacom.com/de-de/for-business/products/signature-pad-stu-540-541 (accessed 11/23/2020).

VPN method

Virtual Private Network (VPN)

In principle, a Virtual Private Network (VPN) establishes a secure communication channel (tunnel) over an existing Internet connection.

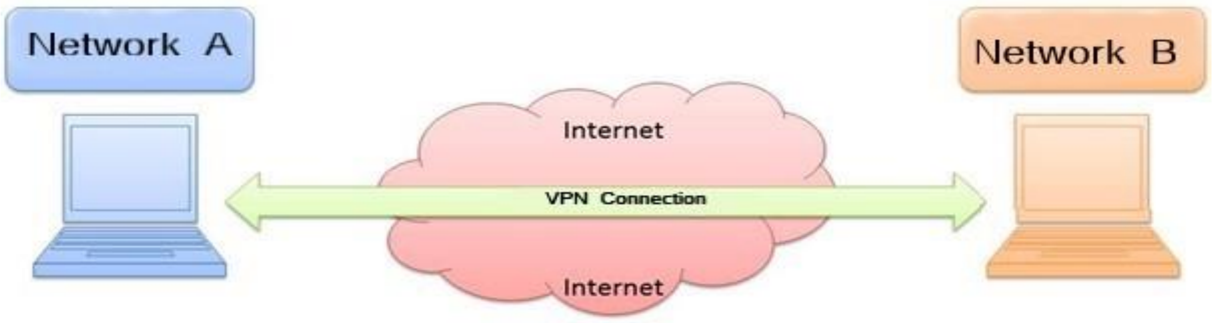


Figure 13: VPN tunnel[42]

VPNs therefore allow data to be exchanged securely between local networks via a public network.

1.3 Data management

In today's age of digitization, the electronic storage of accrued or collected data is an important aspect for companies and individuals. This is especially true for the healthcare sector, as particularly relevant and sensitive data is generated here. In this context, we are talking about systems for processing patient-related data across facilities. Data storage is fundamentally understood to mean the persistent storage of data.

This means that data is archived on a storage medium during the execution of a particular application and is thus available even after the application has ended. Today's data storage systems usually store structured and unstructured data separately.

Structured data is usually stored in database or data warehouse systems and unstructured data in content/document management systems.

A data warehouse concept is a central data store that is detached from the operational databases of the respective companies and serves as a uniform and consistent database. This data basis results in the so-called data warehouse system through the extension by software components for data transformation and analytical systems.

[42] Source: own representation

Local

Local data storage is still one of the most common ways of backing up data, at least in the private sector. This refers to the storage or backup of data on a specific medium.

In the case of local data storage, the data is usually stored on:

- Internal hard disks of a PC
- External hard drives
- USB sticks
- CDs/DVDs

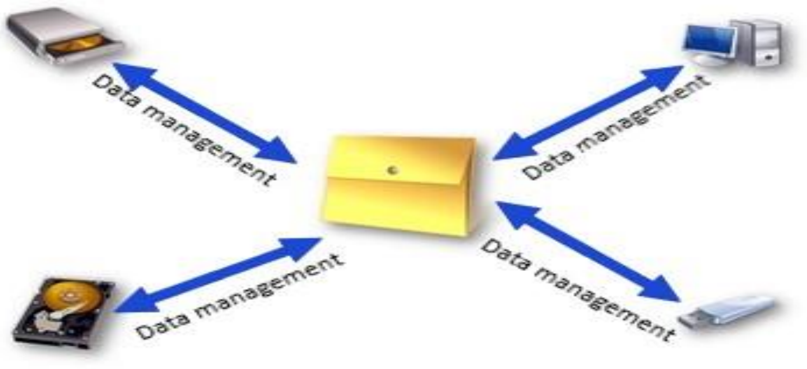


Figure 14: Local data storage[43]

Central

In central data storage, a corresponding data stock is brought together, stored at a central location and monitored. Central data storage can be archiving systems, database management systems, data warehouses or file servers, among others.

All participants (e.g. hospitals) can access the centrally stored data from their respective locations. No data is archived at the individual participants themselves (at least in the case of cross-institutional data processing), which avoids redundant data stocks. [44] Centralized data storage also enables automated data backup and the creation of back-ups.

The advantages of centralized data storage are user-friendliness, high security standards, and cost savings due to lower hardware usage. A disadvantage, however, is the high performance capacity of the databases and servers used. [45]

[43] Source: own representation
[44] cf. http://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/Telemedizin.pdf?blob=publicationFile&v=2
[45] cf. AWV Working Group 6.3 "Data and Storage Management", Project Group 5 "Centralized and Decentralized Data Management"

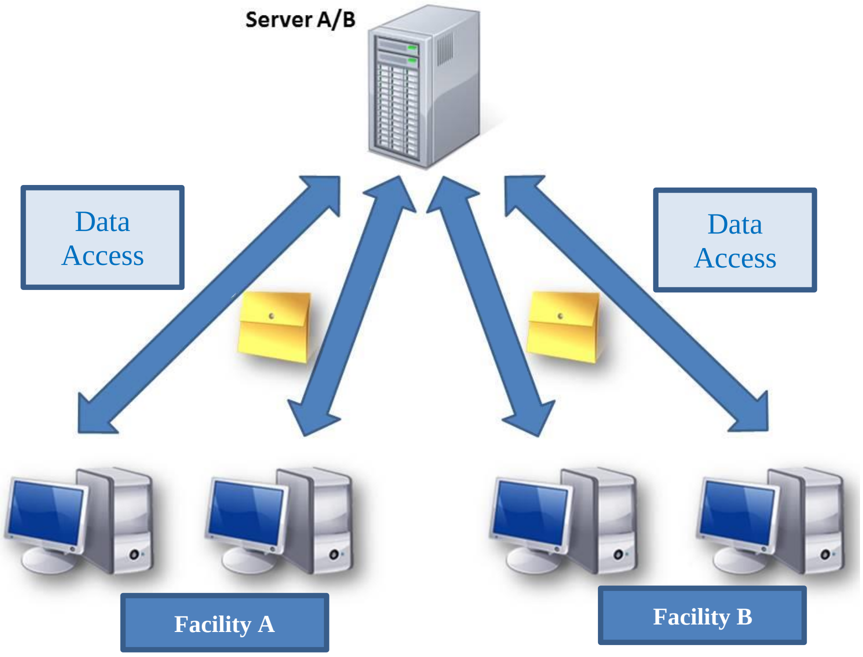


Figure 15: Central data storage[46]

In summary, the advantages or disadvantages of centralized data storage are:

Advantages:
- Less hardware (server)
- More up-to-date data
- Non-redundancy of stored data
- Efficiency
- Sharing of stored data
- Reduced administrative overhead
- Simplified data backup

Disadvantages:
o High bandwidth
o Duplication of data elements
o Line costs
o None decentralized control
o Complexity
o Limited availability in the event of network problems

[46] Source: own

Decentralized

Decentralized data storage describes the storage of data on several central data stores. This type of data storage is used, for example, when a company has several branches with different locations. Here, a common procedure is to replicate data with a high access rate and distribute it on several servers. However, synchronization of the respective servers is crucial to ensure that authorized users, regardless of location, always have access to the same or most up-to-date data. Decentralized data storage can relieve the load on individual servers and improve reliability. [47]

Applied to healthcare, decentralized data storage would mean that each medical facility within an alliance maintains its own data store. The data storage systems of the respective facilities can then communicate with each other via a network, but do not enable cross-system services. [48]

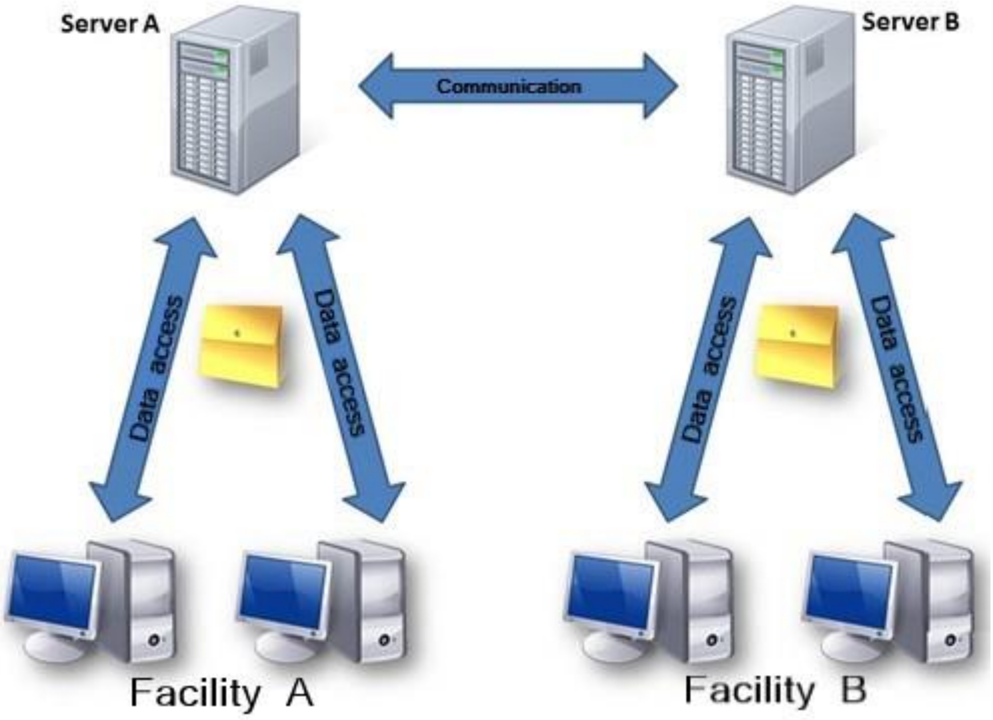


Figure 16: Decentralized data storage[49]

[47] cf. ibid.
[48] cf. http://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/Telemedizin.pdf?blob=publicationFile&v=2
[49] Source: own

In summary, the advantages or disadvantages of decentralized data storage are:

Advantages	Disadvantages
○ Low data transmission cost	○ Increased hardware
○ High availability	○ Multiple server farms
○ Independence from the public network	○ High complexity
○ Load balancing through amplification	○ Complex/vulnerable technology
○ High reliability	○ Increased administrative overhead
○ Rapid access to local data	○ Possible inconsistencies between replicas
○ No interdepartmental access	

Hybrid

In order to combine or compensate for the advantages and disadvantages of centralized and decentralized data storage, there are also mixed forms of data storage.

Cloud

Data storage in a so-called cloud represents a sub-area of cloud computing, or more precisely, infrastructure services. In this case, the data is not managed by the company itself, as was previously the case, but is stored in a cloud. In this case, the cloud means a technical infrastructure which is offered by cloud computing systems. The cloud is therefore a service offered by which computing or storage space can be purchased.

The advantages of this type of data storage are:

- No need to acquire hardware and software
- Flexible design of the infrastructure
- Cost saving
- Neutral location (no synchronization necessary as with decentralized data storage)
- In the healthcare sector in particular, however, special security requirements apply to data- processing solutions, making it necessary to decisively test a cloud service for its suitability. Cloud services are generally divided into public, private, hybrid and community clouds. [50]

[50] cf. http://www.cloud.fraunhofer.de/de/faq/publicprivatehybrid.html

As the name suggests, public clouds are freely accessible public services provided by providers on the Internet.

However, since these public services are insufficient for data protection reasons, for example for companies, there is also the option of developing one's own cloud services or purchasing them as a service. These services, known as private clouds, can only be accessed by users belonging to the organization, which achieves the desired data security.

Hybrid clouds offer a blend of both types, enabling a public application via the Internet on the one hand and a secure application within the organization on the other. However, a strict separation of important (privacy-critical) and less sensitive data is crucial here.

When, for example, access to protected private files is required by several organizations as part of a joint project, community clouds can be used. These enable certain data to be made available to a predefined number of users on a non-public basis.

Literature and internet sources

Working Group on Technical and Organizational Data Protection Issues of the Conference of Federal and State Data Protection Commissioners, Orientation Guide - "Biometric Authentication - Possibilities and Limits," 2009, available at: https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/ak_oh_bio metrie.pdf (Accessed: 02/17/2021).

German Federal Office for Information Security, Asymmetric encryption, available at: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und- Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten- sichern-verschluesseln-und-loeschen/Datenverschluesselung/datenverschluesselung_node.html (Accessed: 02/17/2021).

Federal Office for Information Security, Introduction to WLAN Basic Terms, available at: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und- consumers/information- and-recommendations/cyber-security-recommendations/router- WLAN-VPN/WLAN-LAN- was-man-wissen-sollte/wlan-lan-was-man-wissen-sollte_node.html (Accessed: 02/17/2021).

German Federal Office for Information Security, Virtual Private Network (ISi-VPN), available at: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Router- WLAN-VPN/Virtual-Private-Networks-VPN/virtual-private-networks-vpn_node.html (Accessed: 02/17/2021).

Bundesverband IT-Sicherheit e.V., Biometrische Authentisierung, available at: https://www.teletrust.de/publikationen/broschueren/authentisierung/ (Accessed: 02/17/2021)

Fraunhofer CLOUD, Public, Private and Hybrid Cloud, available at: http://www.cloud.fraunhofer.de/de/faq/publicprivatehybrid.html (Accessed: 02/17/2021)

Law on Framework Conditions for Electronic Signatures, available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/sigg2001_pdf.pdf?__blob=publicationFile (Accessed: 02/17/2021)

Informationszentrum Mobilfunk, Was verbirgt sich hinter dem Mobilfunkstandard GPRS, available at: https://www.informationszentrum-mobilfunk.de/mediathek/glossar/gprs- general-packet-radio-service (Accessed: 02/17/2021).

Informationszentrum Mobilfunk, Was versteht man unter dem Mobilfunkstandard UMTS, available at: https://www.informationszentrum-mobilfunk.de/technik/funktionsweise/umts (Accessed: 02/17/2021).

Informationszentrum Mobilfunk, Der neue Mobilfunkstandard LTE, available at: https://www.informationszentrum-mobilfunk.de/technik/funktionsweise/lte (Accessed: 02/17/2021).

Institute for Internet Security, Electronic Certificates, available at: https://www.internet-sicherheit.de/sicher-im-internet-das-buch/workshops-und- themen/verschluesselung-und-identitaeten/kryptographie/elektronische-zertifikate.html (Accessed: 02/17/2021).

IT Knowledge, Authentication, available at: https://www.itwissen.info/Authentifizierung-authentication.html (Accessed: 02/17/2021)

IT Knowledge, BAN, available at: https://www.itwissen.info/BAN-body-area-network- Koerpernahes-Netzwerk.html (Accessed: 02/17/2021).

IT Knowledge, DHCP, available at: https://www.itwissen.info/DHCP-dynamic-host-configuration-protocol-DHCP-Protocol.html (Accessed: 02/17/2021).

IT Knowledge, DNS (domain name system), available at: https://www.itwissen.info/DNS- domain-name-system-DNS-System.html (Accessed: 02/17/2021).

IT Knowledge, IP Protocol, available at: https://www.itwissen.info/IP-Internet-protocol-IP-protocol.html (Accessed: 02/17/2021).

IT Knowledge, MAN, available at: https://www.itwissen.info/Stadtnetz-metropolitan-area-network-MAN.html (Accessed: 02/17/2021).

IT Knowledge, HTTP (hypertext transfer protocol), available at: https://www.itwissen.info/HTTP-hypertext-transfer-protocol-HTTP-Protokoll.html (Accessed: 02/17/2021).

IT Knowledge, IP Address, available at: https://www.itwissen.info/IP-Adresse-IP-address.html (Accessed: 02/17/2021).

IT Knowledge, Static IP Address, available at: https://www.itwissen.info/Statische-IP-address-static-IP.html (Accessed: 02/17/2021).

IT Knowledge, WAN, available at: https://www.itwissen.info/WAN-wide-area-network- wide-area network.html (Accessed: 02/17/2021).

Kramme R. & Kramme H., The role of technology in medicine and its importance for health policy, available at: http://www.newbooks-services.de/MediaFiles/Texts/5/9783642161865_Excerpt_001.pdf (Accessed: 02/17/2021).

Martin Wind, Detlef Kröger (eds.): Handbuch IT in der Verwaltung; Springer-Verlag, Berlin Heidelberg 2006

Nefiodov L. & Nefiodov S., On Kondratieff Cycles, 2014, available online at: http://www.kondratieff.net/#!kondratieffcycles/c1xd0 (Accessed: 02/17/2021).

Security Server Germany, How does SSL work, available at: http://www.ssl.de/ssl.html (Accessed: 02/17/2021)

Signature Perfect, Leitfaden Elektronische Signatur, 2008, available at: http://www.signature-perfect.de/docs/Leitfaden_Elektronische_Signatur.pdf (Accessed: 02/17/2021)

Teltarif, What is DSL and how does it work, available at: http://www.teltarif.de/internet/dsl/technik.htm (Accessed: 02/17/2021).

Thieme Compliance, Electronic Signature & Archiving, available at: https://thieme-compliance.de/de/software-e-consentpro/zusatzmodul-e-documentpro/ (Accessed: 02/17/2021)

VDSL rate comparison, history and development of digital communications, available at: http://www.vdsl-tarifvergleich.de/vdsl-technik/geschichte-von-isdn-ueber-dsl-bis-vdsl.html (Accessed: 02/17/2021)

VDSL rate comparison, What is actually the data transfer rate?, available at: http://www.vdsl-tarifvergleich.de/lexikon/datenuebertragungsrate.html (Accessed: 02/17/2021)

Consumer advice center, available at: https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/was-ist-5g-vorteile-und-risiken-der-5-generation-mobilfunk-52004

(Accessed: 02/17/2021)