Sichere elektronische Kommunikation

Vortrag vom 24.02.2016

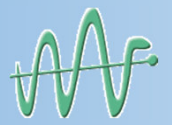
Gesundheitsnetz Charlottenburg-Wilmersdorf

Dr. med. Ralph E. Mertens

GESUNDHEITSNETZ
Charlottenburg-Wilmersdorf

Gliederung

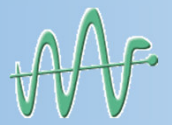
- Sicherheitsbewusstsein
- Sicherheitsaspekte
  - Gesetzliche Grundlagen
  - Datenschutz
- Sicherheitsmechanismen
- Sichere Kommunikation im Internet am Beispiel Email
  - Ausgangslage
  - Lösungsstrategien
  - Verschlüsselung
  - Zertifizierung vs. Web of Trust
- Schlüsselverwaltung
- Qualifizierte elektronische Signatur mit dem neuen Personalausweis



Sicherheitsbewußtsein

- Oft mangelndes Problembewusstsein
- Unkenntnis
  - der geltenden Vorschriften
  - des EDV-Status
  - menschliche und technische Risiken
- Gründe für fehlende Sicherheitsaspekte
  - Fehlende Zeit
  - Fehlende finanzielle Resourcen
  - Hoher technischer und organisatorischer Auswand

(siehe www.datenschutzzentrum.de/medizin)



GESUNDHEITSNETZ
Charlottenburg-Wilmersdorf

Sicherheitsaspekte

- Gesetzliche Grundlagen
  - Eid des Hippokrates (ärztliche Schweigepflicht, Patientengeheimnis): Anvertrauen als Schutz des für Hilfe notwendigen Vertrauensverhältnisses
  - Berufliche Schweigepflicht §203 Strafgesetzbuch, Heilberufsordnungen
  - Schutz der Gesundheitsdaten wegen besonderer Sensibilität (§§3 IX BDSG, 67 XII SGB X)
  - Schutz durch Spezialnormen: KrankenhausGe, GesDG, KrebsRG, GenDiagnG, InfSchG, AMG, TransplantG ...
  - Datenschutz, informationelle und medizinische Selbstbestimmung

Sicherheitsaspekte

- **Datensicherheit** verfolgt das Ziel, im Prozess der Datenverarbeitung vor Verlust, Zerstörung, Verfälschung, unbefugter Kenntnisnahme und unberechtigter Verarbeitung der Daten zu schützen
- Es muss gewährleistet sein, dass insbesondere
  - der Zugriff auf die Daten und somit deren Kenntnisnahme ausschließlich durch **autorisierte Benutzer** erfolgt; das Gleiche gilt für die Modifikation (Ändern und Löschen) von Daten,
  - Daten **nicht unbemerkt** verändert werden können, sondern Änderungen **nachvollziehbar** sind,
  - der **Zugriff auf Daten** innerhalb eines festgelegten Zeitraums für entsprechend autorisierte Nutzer gewährleistet ist und die **Funktionalität der IT-Systeme** nicht beeinträchtigt ist.

Sicherheitsaspekte (am Beispiel Email)

- **Was** für Daten sind betroffen
  - Email-Briefe, Adressdaten
- **Wo** sind meine Daten abgelegt
  - Mailprovider (gmx, google, web.de, one.com etc), eigener Mailserver, Cloud
- **Wie** sind meine Daten abgelegt
  - Reine Textdaten, verschlüsselte Datenablage
- **Wer** kann auf die Daten zugreifen
  - Arzt, Praxismitarbeiter, EDV-Beauftragter, Provider-Administratoren(?)

Sicherheitsmechanismen

- Zugangssicherung (Authentifizierung, Identifizierung)
  - Passwort, OTP, Hardwareschlüssel (z.B. Yubikey, Personalausweis, NFC)
- Verschlüsselung des Kommunikationsweges (SSL, TLS)
- Verschlüsselung der Daten (symmetrisch, asymmetrisch)
- Datensicherung (Backup lokal, Cloud)
- Datenhaltung (lokal, Provider, Cloud, Mobiltelefon)

Klassische Postkarte

Liebe Frau Mustermann,

die Gesundheit Ihres Tieres liegt uns sehr am Herzen. Daher erinnern wir Sie gerne an den Jahrescheck für Ihren Hund

Allan

Im Rahmen einer optimalen Vorsorge sind regelmäßige Untersuchungen und individuelle Impfungen wichtig.
Rufen Sie uns bitte an und vereinbaren einen Termin:

Telefon: 0123/000 00 00

Mit freundlichen Grüßen
H. Schmid

Ihr Team der
Tierarztpraxis Dr. Peter Test
Teststr. 12
00000 Musterstadt
Fax: 0989/8765 543
email: info@mustertierarzt.de
weitere INFO www.mustertierarzt.de

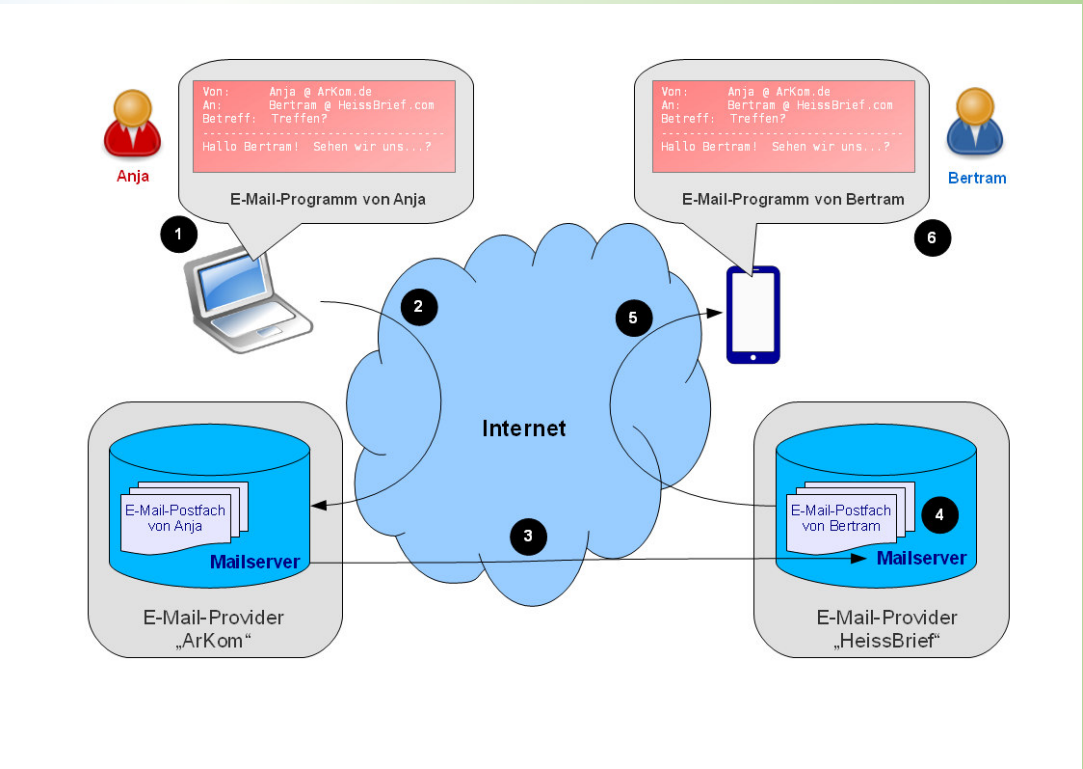
Öffnungszeiten:
Mo, Di 9 Uhr bis 18 Uhr
Mi 8 Uhr bis 13 Uhr
Do , Fr 9 Uhr bis 16 Uhr

Frau
Clara Mustermann
Musterstraße 00
00000 Musterstadt

GESUNDHEITSNETZ
Charlottenburg-Wilmersdorf

Email ohne Verschlüsselung

1. Ausgangstext
2. Verbindungsweg zu ArKom
3. Verbindungsweg zu HeissBrief
4. Datenablage auf HeissBrief
5. Verbindungsweg zum Handy
6. Datenablage auf dem Handy

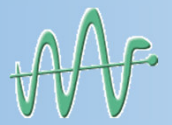


GESUNDHEITSNETZ
Charlottenburg-Wilmersdorf

Sichere Email-Kommunikation

- Unsicherheitsfaktoren der Email ohne Verschlüsselung
  - Unbedachtes Versenden von Informationen an falschen Empfänger

  - Abfangen der Email auf JEDEM Kommunikationsschritt
  - Lesen der Email
  - Adressfälschung
  - Inhaltsfälschung
  - Einbau von Emailviren
  - Missbrauch der eigenen Mailadresse (Absenderadresse)
  - Missbrauch der Emfängeradresse(n)



Sichere Email-Kommunikation

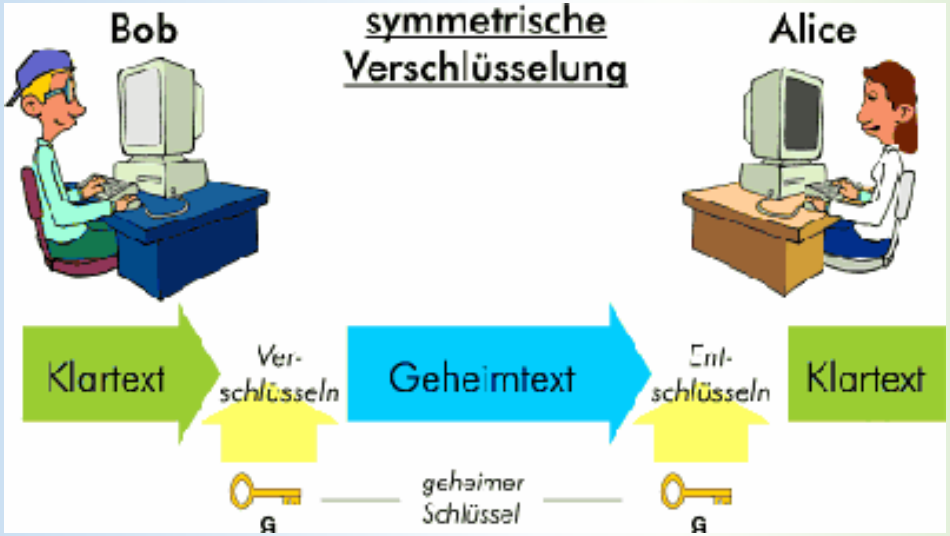
- Forderungen
  - Elektronische Unterschrift (elektronische Signatur) -> Unterschreiben
    - Rechtliche Voraussetzung für die beweiskräftige Dokumentation von Willenserklärungen
    - Authentizität (diese Unterschrift bzw. diese Mailadresse gehört nachweisbar zum Author)
    - Fälschungssicherung des Textes (Integrität des Textes)
  - Verschlüsselung der Textnachricht -> Einlegen in einen Briefumschlag
  - Adressierung an sichere Adressaten (zertifizierte Mailadresse) -> Adresse auf den Umschlag schreiben

Sichere Email-Kommunikation

- Lösungsstategien
  - Intranet-Lösungen: KV-Flexnet über VPN, Telemed, DGN
    - Sicherer Kommunikationsweg, KV-eigener Mailserver: Datenablage (?)
  - D-Mail (1&1, gmx.de)
    - Sicherer Kommunikationsweg, zertifizierte Emailadresse, unverschlüsselte Datenablage
  - E-Brief (Deutsche Post)
    - Sicherer Kommunikationsweg, zertifizierte Emailadresse,
    - teuer, geschlossener Standard, langsame Zustellung, rechtlich dem Fernmeldegeheimnis zugeordnet
  - Offene Standards
    - PGP (pretty good privacy), OpenPGP (GnuPG)
    - S/MIME

Sichere Email-Kommunikation

- Symmetrische Verschlüsselung

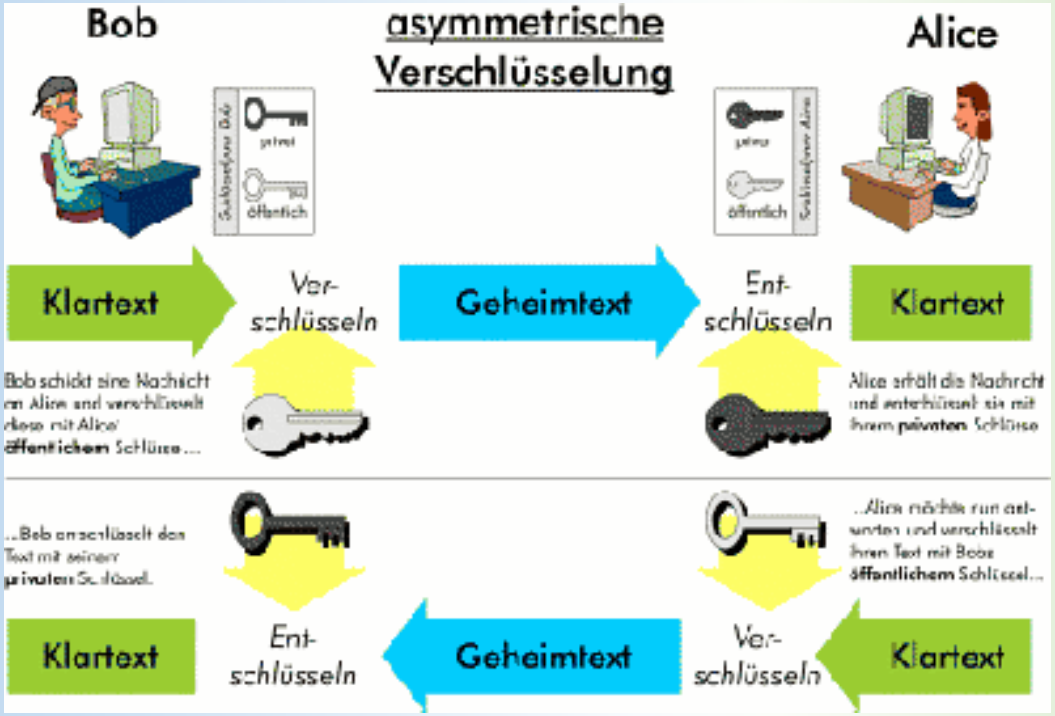


- Problem: der Schlüssel muss über einen weiteren Weg ausgetauscht und kopiert werden

GESUNDHEITSNETZ
Charlottenburg-Wilmersdorf

Sichere Email-Kommunikation

- Asymmetrische Kommunikation



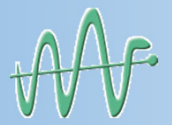
GESUNDHEITSNETZ
Charlottenburg-Wilmersdorf

Sichere Email-Kommunikation

- Hybride Verschlüsselung
  - Die Nachricht wird mit einem symmetischen Schlüssel verschlüsselt
  - Mit dem öffentlichen Schlüssel wird der symmetische Schlüssel verschlüsselt und an die Nachricht angehängt
  - So ist die Entschlüsselung deutlich schneller

Sichere Email-Kommunikation

- OpenPGP (GnuPG)
  - Sichere quelloffene Version von PGP
  - Unbegrenzt gültige Schlüssel erstellbar
  - Zertifizierung über „Web ob Trust“
  - Zusatzsoftware notwendig (z.B. GPG4Win, EnigMail als Thunderbird-Addon, WinPT für Outlook, GPGSuite für Mac)
- S/MIME
  - Schlüssel nur 1 bis 3 Jahre gültig, bei Zertifizierungsstelle (CA) zu beantragen
  - Kostenlose Zertifikate bei StartSSL.com, Comodo.com, CACert.org (noch nicht akkreditiert), kostenpflichtig bei D-Trust.com, TeleSEC.de
  - Keine Zusatzsoftware notwendig



OpenPGP Anleitung

(emailselfdefense.fsf.org)

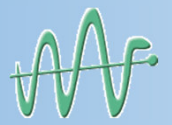
- 1. GnuPG (GPG4Win) herunterladen und installieren
- 2.a Emailprogramm (Thunderbird), Outlook vorbereiten
- 2.b Enigmail-Addon für Thunderbird, WinPT (Outlook), GPGSuite (Apple Mac)
- 3.a Schlüsselpaar erstellen (Schlüsselbund aus privatem und öffentlichem Schlüssel)
- 3.b öffentlichen Schlüssel auf einen Schlüsselserver hochladen
- 4 Test-Email an edward-de@fsf.org schreiben

GESUNDHEITSNETZ
Charlottenburg-Wilmersdorf

S/MIME Anleitung

(von-wachter.de/smime.htm#pgp)

- S/MIME-Zertifikat beantragen (z.B. bei StartSSL.com)
  - (Anmerkung: der private Schlüssel wird immer lokal auf dem Rechner erzeugt)
- Das Zertifikat/Schlüsselpaar wird automatisch im Browser gespeichert
- Im Zertifikatsmanager des Browsers das erstellte Zertifikat markieren und „Sichern“ (eine PKCS12 [.p12] – Datei wird erzeugt)
- Die erstellte „.p12“-Datei im Emailprogramm im Zertifikatsmanager importieren
- In den Kontoeinstellungen S/MIME aktivieren und signieren und/oder verschlüsseln selektieren
- Jede jetzt verschickte Email wird mit einer Unterschriftsignatur und einem Zeitstempel versehen



Sichere Email-Kommunikation

- Jede Email sollte signiert (digital unterschrieben) werden!
  - Der Empfänger sieht, das die Email von einem zertifizierten Absender stammt
  - Durch die Signierung wird der gesamte Inhalt gegen Ver-änderungen abgesichert (Hashfunktion)

GESUNDHEITSNETZ
Charlottenburg-Wilmersdorf

Schlüsselverwaltung /Schlüsselsicherung

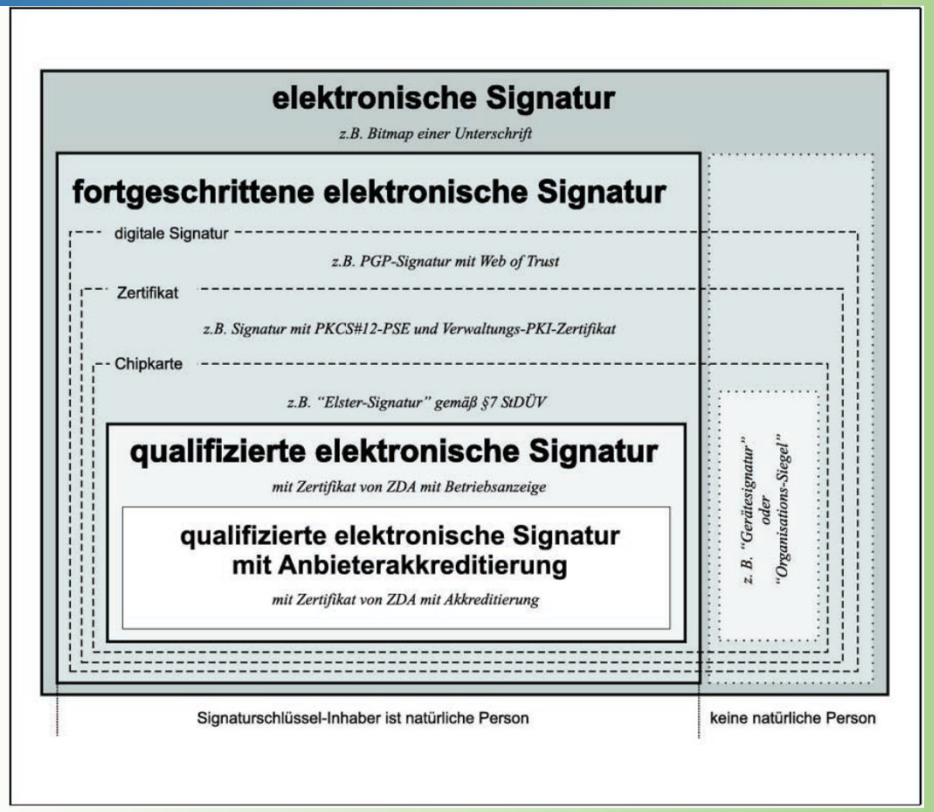
- Jeder private Schlüssel (sollte) gegen Missbrauch mit einem Passwort oder einer Passphrase gesichert werden
  - (z.B. „Hkg13dwWh“ ->
    „Hänschen klein ging allein in die weite Welt hinein“
    erster Buchstabe, Vokale als Zahlen)

- Schlüsselpaare werden als lokal Dateien gehalten (als .p12, .pks oder .gpg)
- Können in Smartcards/Hardwareschlüsseln (z.B. yubikey) installiert werden
- Auf Smartphones im „Schlüsselbund“ (Import über .p12)

GESUNDHEITSNETZ
Charlottenburg-Wilmersdorf

Qualifizierte elektronische Signatur mit dem neuen Personalausweis

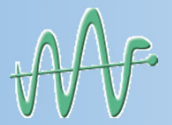
- Ausweis mit aktivierter Online-Ausweisfunktion
- Kartenlesegerät (ca. 110 €)
- Ausweis-PIN (zunächst Transport-PIN)
- AusweisAPP aus dem eigenen PC
- Zertifikat der Bundesdruckerei (D-Trust) (esign-service.de) (ca. 10 €/Jahr)
- Signatursoftware (Governikus,ca. 80 €)
- Dauer des Verfahrens ca. 3 Wochen



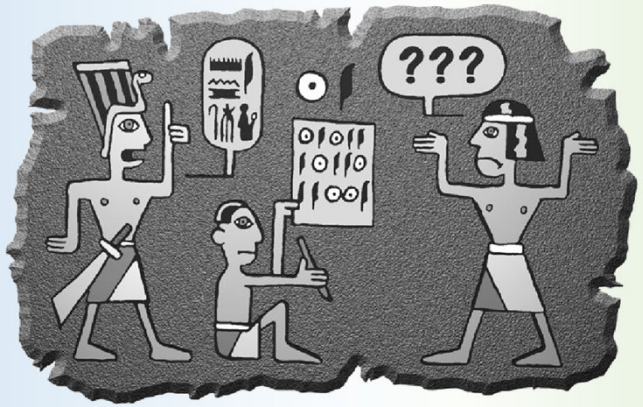
GESUNDHEITSNETZ
Charlottenburg-Wilmersdorf

Quellennachweis

- Zertifizierung
  - https://de.wikipedia.org/wiki/CAcert
  - http://www.computerwoche.de/a/rundum-sicherheit-fuer-e-mails,2363681,8
  - https://www.startssl.com/
  - https://www.bsi.bund.de/DE/Home/home_node.html esig.pdf
- Verschlüsselung
  - https://www.enigmail.net/documentation/Enigmail_Handbook_1.8_en.pdf
  - https://www.gnupg.org/gph/de/manual.pdf
  - https://www.gpg4win.de/doc/de/gpg4win-compendium.html
  - https://de.wikipedia.org/wiki/S/MIME
  - https://collabor.idv.edu/0220174/stories/10722/
  - https://de.wikipedia.org/wiki/S/MIME
  - https://www.nicolas-marschall.de/encrypt.html
  - http://von-wachter.de/smime.htm



Vielen Dank für Ihre Aufmerksamkeit



GESUNDHEITSNETZ
Charlottenburg-Wilmersdorf