Selbstdatenschutz - Tools und Technik

Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)
http://svs.informatik.uni-hamburg.de

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Sommerakademie des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD), Kiel, 19. September 2016

Gliederung

In dem Vortrag werden verschiedene technische Möglichkeiten vorgestellt und bewertet, die geeignet sind, die Privatsphäre bei der Internetnutzung zu schützen.

- Grundlagen
- E-Mail-Verschlüsselung
- Verschlüsselte Cloud-Speicher
- Zusammenfassung

Schutzziele

Voydock, Kent 1983

- Klassische IT-Sicherheit berücksichtigt im Wesentlichen Risiken, die durch *regelwidriges Verhalten* in IT-Systemen entstehen.

Vertraulichkeit	unbefugter Informationsgewinn
Integrität	unbefugte Modifikation
Verfügbarkeit	unbefugte Beeinträchtigung der Funktionalität

Vertraulichkeit: Verfahren und Algorithmen

Was wird geschützt?

Beispiele für Verfahren

Beispiele für Algorithmen

Verfahren des technischen Datenschutzes

Inhaltsdaten

Vertraulichkeit

Verschlüsselung

Inhalte

DES, 3-DES, OTP, IDEA, AES, RSA, ElGamal, …

Verdecktheit

Steganographie

Inhalte + Existenz

F5, …

Verkehrsdaten

Anonymität Unbeobachtbarkeit

Sender

Ort

Empfänger

Web-Anonymisierer, Remailer, anonyme Zahlungssysteme

Pseudonyme, Proxies, umkodierende Mixe, DC Netz, Private Information Retrieval, …

E-Mail-Verschlüsselung

- Unverschlüsselte E-Mail-Kommunikation
  - SMTP (Simple Mail Transfer Protocol)
  - POP (Post Office Protocol)
  - IMAP (Internet Message Access Protocol)
- Verbindungsverschlüsselung
  - SMTP/POP/IMAP over SSL
  - Verschlüsselung zwischen MTAs
  - Sicherheit von DE-Mail etc.
- «Richtige» E-Mail-Verschlüsselung = Ende-zu-Ende-Verschlüsselung
  - S/MIME
  - PGP

Herkömmliche E-Mails sind unsicher

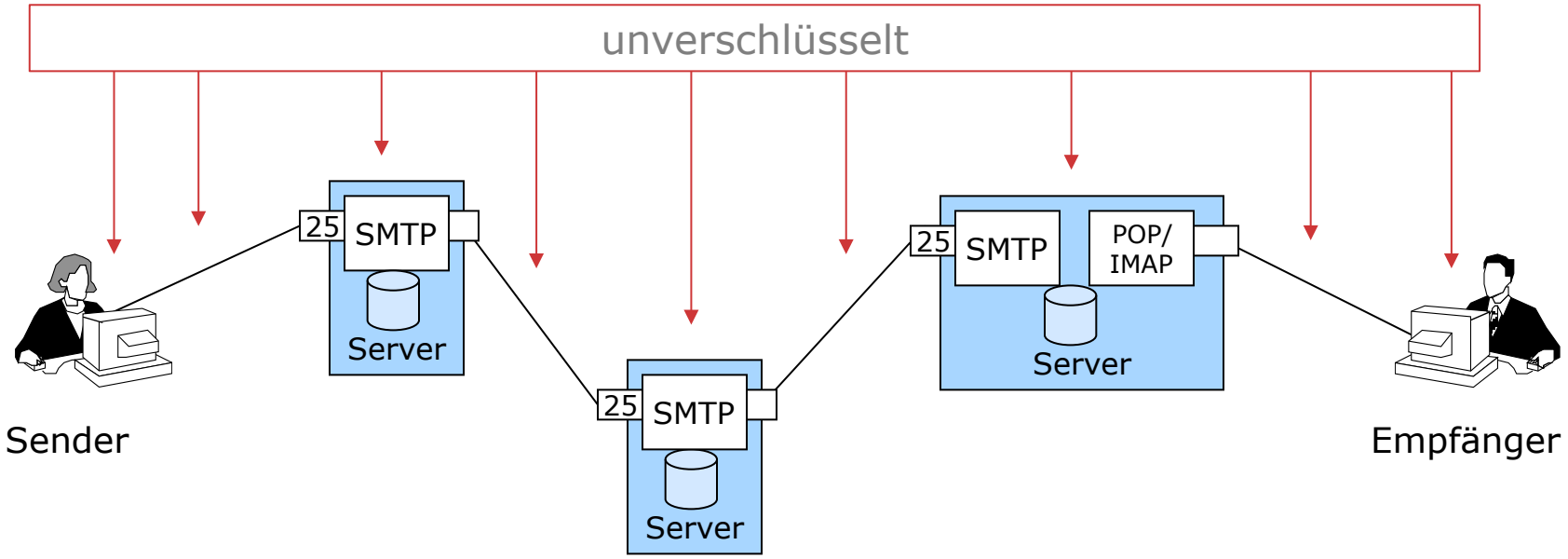
- Unverschlüsselte E-Mail (schematisch):

> Von: alice@example.de
> An: bob@mail.com
> Betreff: Abendessen
>
> Hallo Bob,
>
> wollen wir uns morgen zum Abendessen treffen?
>
> Schöne Grüße, Alice

- Übertragung von E-Mail ist unsicher
  - Mitlesen möglich
  - Fälschen des Absenders möglich
  - Fälschen des Nachrichteninhalts möglich

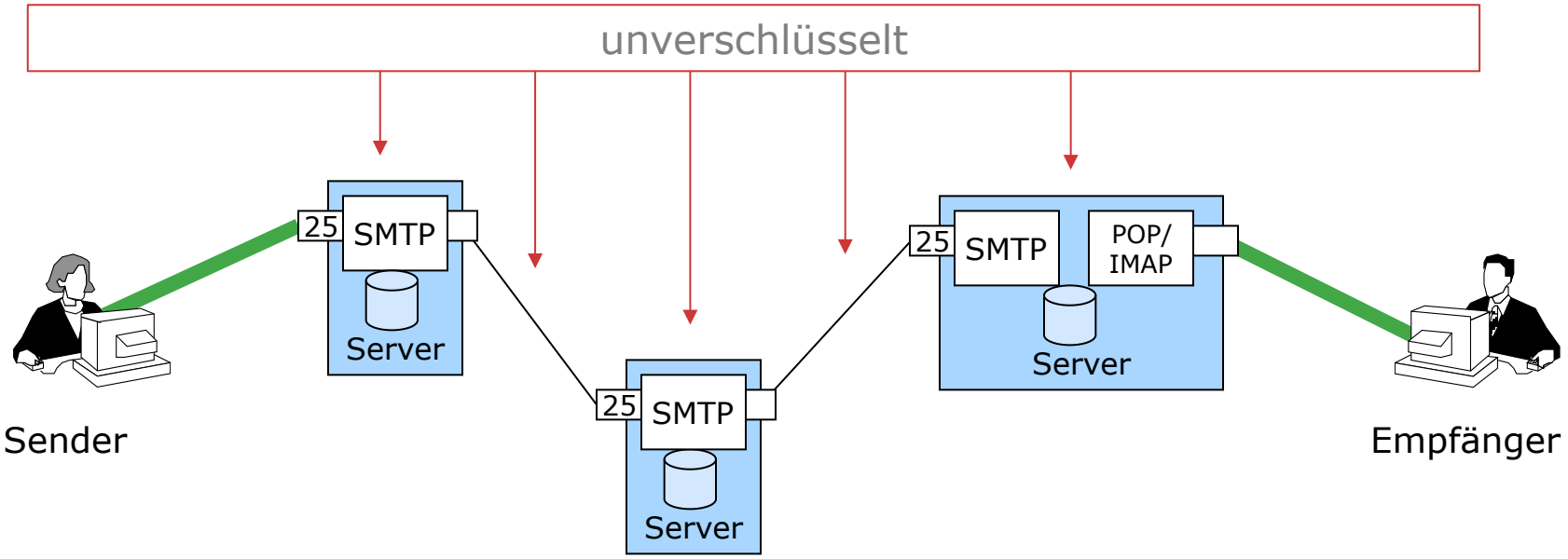
Grundlagen der E-Mail-Kommunikation

- Store & Forward-Prinzip:
  - E-Mail wird nicht direkt an Empfänger, sondern über MTA (Mail Transfer Agents) geschickt
- Senden via SMTP: Textbasiertes Protokoll auf TCP-Port 25
- Empfangen: POP, IMAP



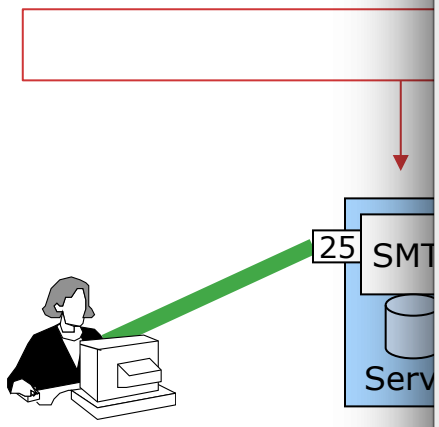
Verbindungsverschlüsselung

- SMTP/POP/IMAP over SSL
  - Verschlüsselte Teilstrecke zwischen
    - Sender und MTA
    - MTA und Empfänger
  - alle MTAs können mitlesen

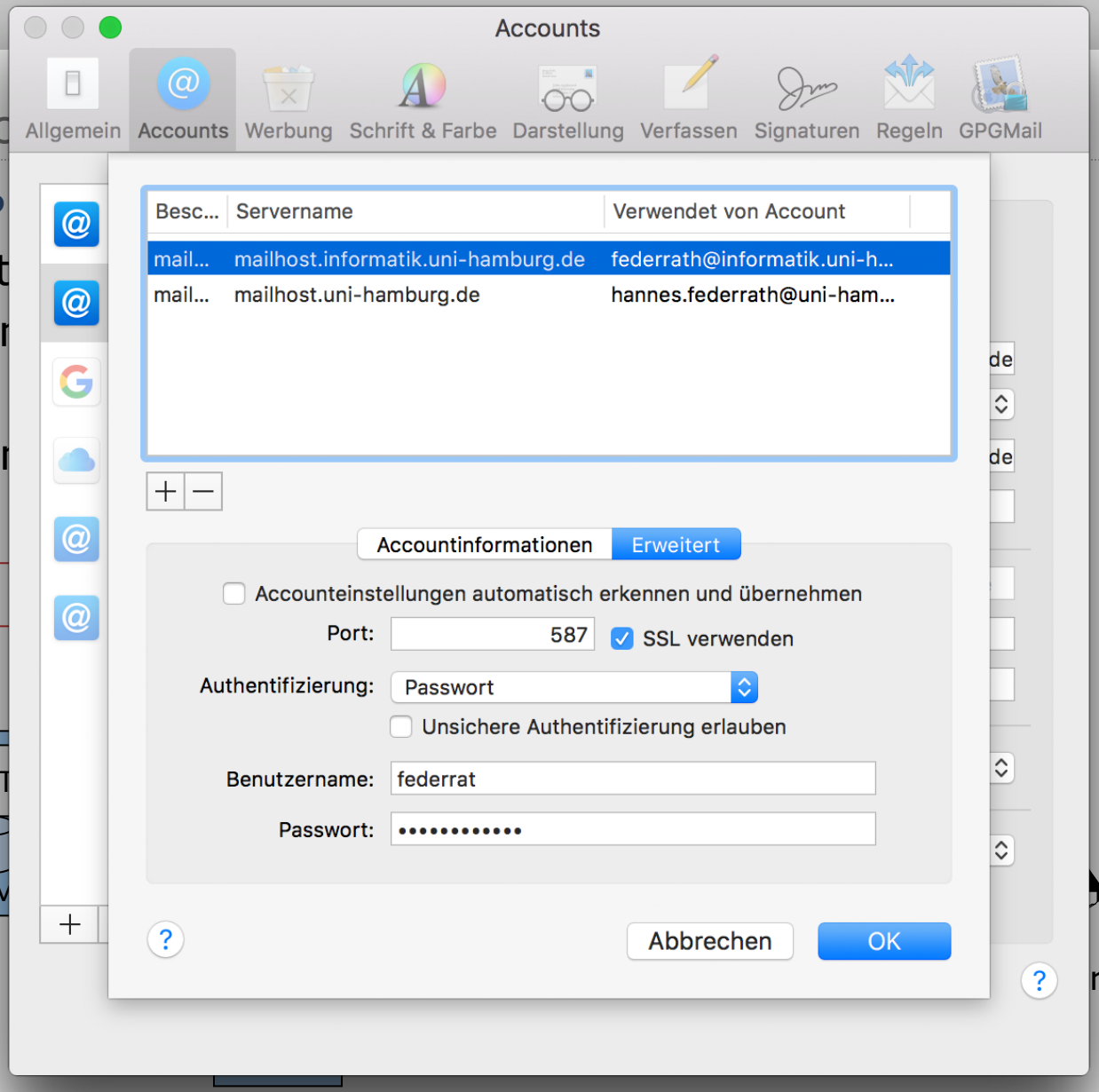


Verbindungsversc

- SMTP/POP/IMAP
  - Verschlüsselt
    - Sender ur
    - MTA und
  - alle MTAs kön

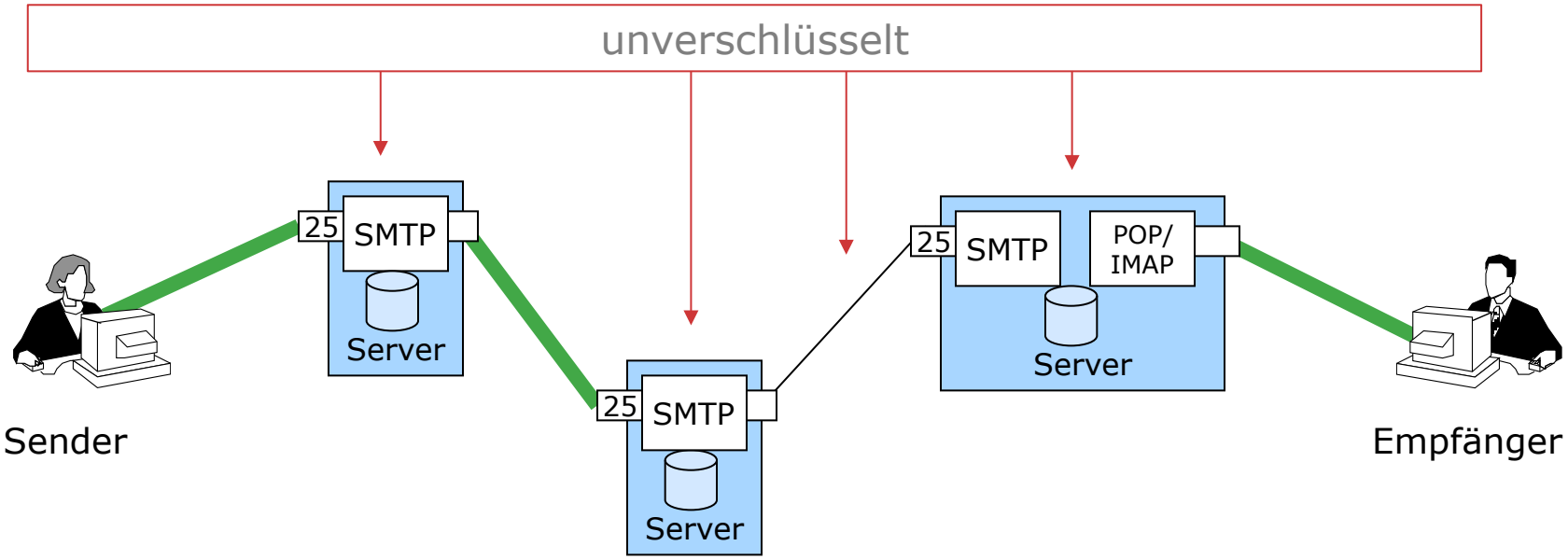


Sender



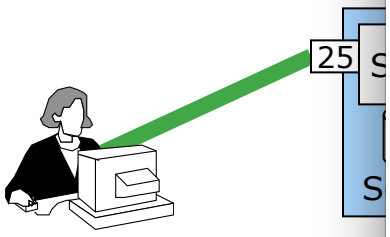
Verbindungsverschlüsselung

- SMTP/POP/IMAP over SSL
- Verschlüsselung zwischen MTAs
  - Verschlüsselte Teilstrecke zwischen MTAs
  - nicht alle Teilstrecken müssen verschlüsselt sein
  - alle MTAs können mitlesen



Verbindungsver

- SMTP/POP/IMA
- Verschlüsselun
  - Verschlüsse
  - nicht alle T
  - alle MTAs k



Sender

www.heise.de/newsticker/meldung/E

heise online

"E-Mail Made in Germany": SSL-Verschlüsselung für (fast) alle

UPDATE

09.08.2013 12:40 Uhr – Detlef Borchers

Die Web-Mailer der Telekom, von GMX und web.de zeigen ab sofort an, wenn ein E-Mail-Empfänger aus dem Verschlüsselungs-Verbund "E-Mail made in Germany" kommt.

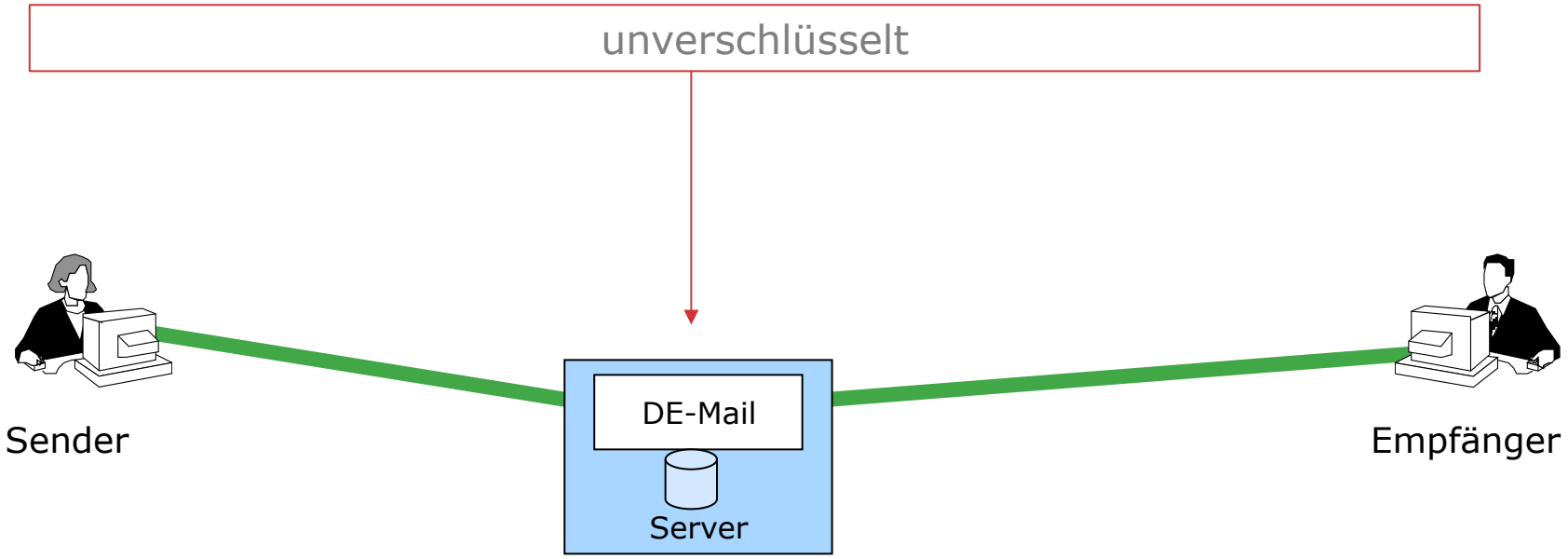
Die Deutsche Telekom und United Internet haben das Projekt **"E-Mail made in Germany" [1]** in Berlin vorgestellt. Dabei handelt es sich um eine SSL/TSL-Verschlüsselung zwischen den Mail-Servern und Rechenzentren der beteiligten Firmen, die ab sofort genutzt werden kann. Ab 2014 sollen nur noch SSL-verschlüsselte Mails transportiert werden. Rund 20 Millionen Kunden der Telekom und 30 Millionen von GMX und Web.de sollen die "deutsche E-Mail" nutzen können. Sie ist bereits in den Webmailern der beteiligten Firmen freigeschaltet und kommt automatisch zum Einsatz: Bei Eingabe von Empfängeradressen aus dem Mail-Verbund wird eine Information angezeigt, dass die Mails verschlüsselt übertragen werden. Bislang gibt es allerdings noch keine entsprechende Anzeige bei empfangenen Mails.

Wie Telekom-Chef René Obermann erklärte, hofft man, dass sich andere Wettbewerber wie Freenet oder Arcor der deutschen Initiative anschließen werden. Geprüft werde derzeit, wie die Tochterfirmen Strato (Telekom) und 1&1 (United Internet) in das System eingebunden werden können, damit auch Kleingewerbetreibende mit Domains wie z.B. Obermann.de die sichere deutsche "Mail made in Germany" nutzen können. Zudem hofft Obermann darauf, dass aus der deutschen Initiative eine europäische wird. Ralph Dommermuth von United Internet erklärte, dass 90 Prozent der Mail innerhalb von Deutschland ausgetauscht werde und somit die "E-Mail made in Germany" zum Standard werde.

Meldung: https://heise.de/-1932962

Verbindungsverschlüsselung

- Sicherheit von DE-Mail etc.
  - gleiche Sicherheit wie «E-Mail Made in Germany»
  - keine Ende-zu-Ende-Verschlüsselung
  - Server kann mitlesen



Verbindungsverschlüsselung

- Sicherheit von DE-Mail etc.
  - gleiche Sicherheit wie «E-Mail Made in Germany»
  - keine Ende-zu-Ende-Verschlüsselung
  - Server kann mitlesen

Systeme von Absender und Empfänger die Identität der jeweils anderen Seite sicherstellen können. Eine Möglichkeit hierfür ist der Einsatz digitaler Zertifikate.

- Eine abschnittsweise Verschlüsselung der Übertragungswege soll Sicherheit gegen den Zugriff durch Unbefugte bieten.

Quelle: Wikipedia

Bei besonders hohen Anforderungen an die Vertraulichkeit der Nachrichten haben De-Mail-Nutzer wie bei herkömmlichen E-Mails die Möglichkeit, die mit De-Mail übermittelten Inhalte noch zusätzlich selbst zu verschlüsseln („Ende-zu-Ende-Verschlüsselung“). In diesem Fall erfolgt die Verschlüsselung auf dem Rechner des Absenders und die Entschlüsselung der Inhalte erst auf dem Rechner des Empfängers. Hierfür ist jedoch die Installation zusätzlicher Software erforderlich, die die Ver- und Entschlüsselung durchführt. Der Verzeichnisdienst, der bei De-Mail obligatorisch durch den Diensteanbieter angeboten werden muss, unterstützt den Anwender, indem dieser seinen öffentlichen Schlüssel anderen Anwendern zur Verfügung stellen kann. Es soll also ermöglicht werden, an einer zentralen Stelle nach öffentlichen Schlüsseln von Personen suchen zu können, um mit diesen vertraulich zu kommunizieren. Dies ist bisher nur schwer möglich und stellt den wesentlichen „Hemmschuh“ für die Verbreitung von Verfahren zur Ende-zu-Ende-Verschlüsselung („Wo finde ich den gültigen Verschlüsselungsschlüssel meines Kommunikationspartners?“). Mit De-Mail soll auf diese Weise der Einsatz der Ende-zu-Ende-Verschlüsselung unterstützt und gefördert werden.

S/MIME oder OpenPGP können zusätzlich durch den Nutzer für die Abbildung der Ende-zu-Ende-Sicherheit eingesetzt werden. Die Liste der hauptsächlichen Sicherheitsfunktionen wurden in einem Dokument des BMI zusammengefasst.

Technische Konzeption [Bearbeiten | Quelltext bearbeiten]

Das technische Konzept ist innerhalb von technischen Richtlinien beschrieben, die auf der Web-Seite des BSI[19] veröffentlicht sind.

Standardmäßige Transportsicherheit [Bearbeiten | Quelltext bearbeiten]

Sowohl die Kommunikation der De-Mail-Nutzer mit ihren De-Mail-Provider als auch die Kommunikation von De-Mail-Anbietern untereinander verläuft grundsätzlich über TLS-gesicherte Kommunikationskanäle.[5] Reicht einem Nutzer das dadurch realisierte Sicherheitsniveau nicht

Ende-zu-Ende-Verschlüsselung schützt die Vertraulichkeit

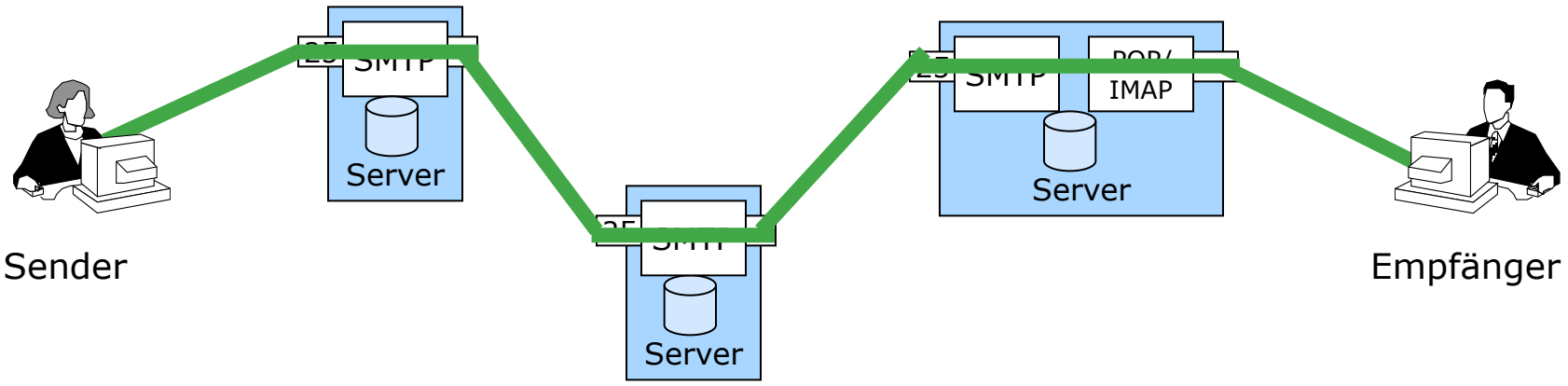
- Verschlüsselte E-Mail (schematisch):

Von: alice@example.de
An: bob@mail.com
Betreff: Abendessen

-----BEGIN ENCRYPTED MESSAGE-----
AkRFMRcwFQYDVQQDEw5Sb2xmIFdlbmRvbHNreTEUMBI
GA1UECBMLRGV1dHNjaGxhbmQxEzARBgNVBAcTClJlZ2V
uc2J1cmcxDzANBgNVBAoTBnByaXZhdDEkMCIGCSqGSIb
3DQEJARYVcm9sZi53ZW5kb2xza3lAZ214LmRlMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQDUVvgaQK9OQP
XvgZm2bU/QqDnsbemv8p83gDiSuCq07S/cSMiGFjEZas6
5MZ47W951LlNLvFTSdkjwS2fUfsZ5oAxfU+RDWb3GgijZp
5cAxTfFKQ/amaWAmtmCkt1FMntRXZ393gOkSSUlWQ7Cr
6GWAYF+deC5CuWpRPpSLYRqSwIDAQABMA0GCSqGSIb
3DQEBBAUAA4GBAIGVTNbu0eOTfGuuL0MWHLfVD
-----END ENCRYPTED MESSAGE-----

Ende-zu-Ende-Verschlüsselung schützt die Vertraulichkeit

- Ende-zu-Ende-Verschlüsselung
  - Inhalte sind durchgehend verschlüsselt
  - MTAs (Server) können nicht mitlesen
  - Adressierungsinformation kann nicht mit verschlüsselt werden
- Konkrete Ende-zu-Ende-Verschlüsselungslösungen
  - S/MIME
  - PGP

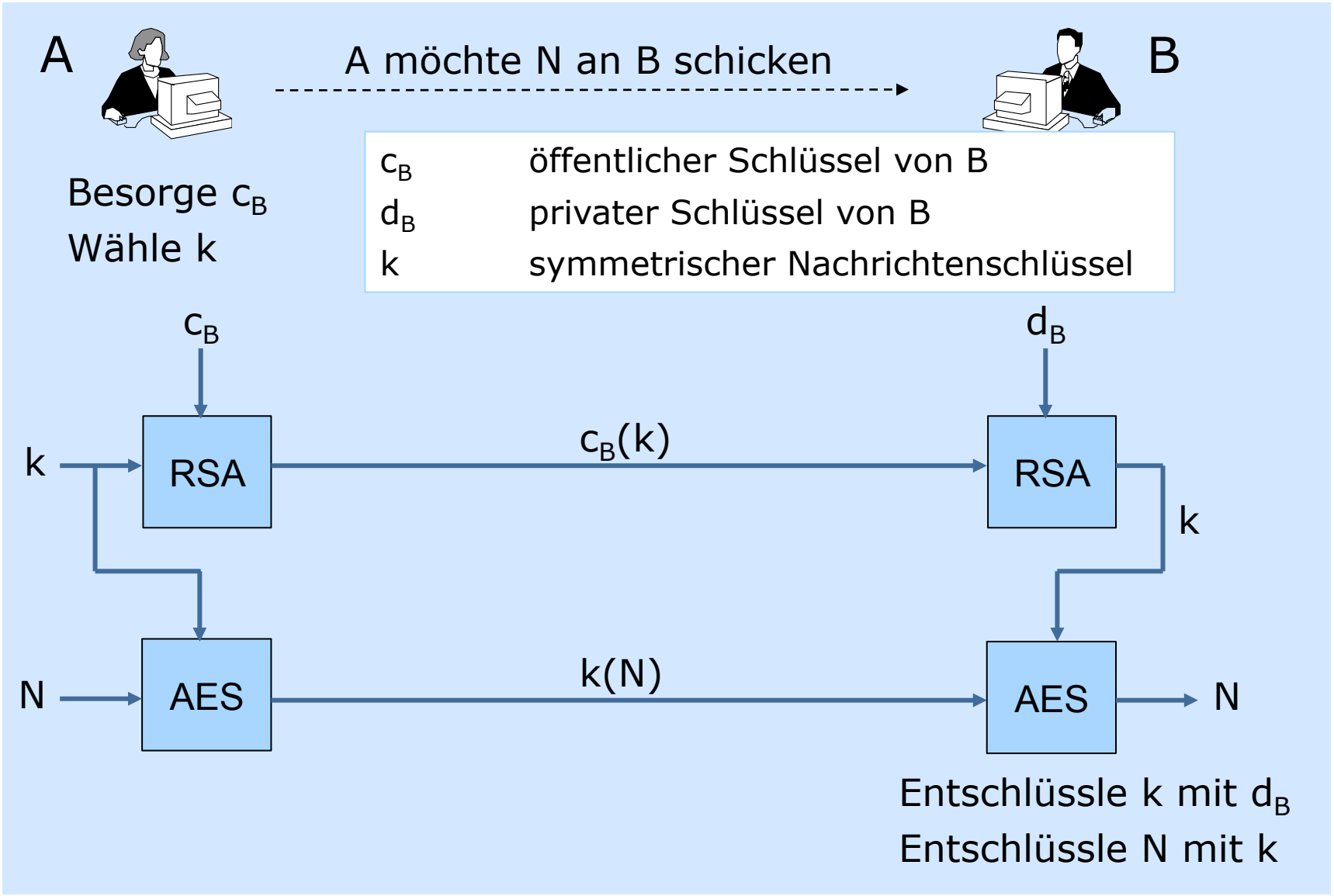


Konkrete Ende-zu-Ende-Verschlüsselungslösungen

- S/MIME (Secure Multipurpose Internet Mail Extensions)
  - ursprünglich von RSA Data Security Inc.
  - S/MIME v3 im Juli 1999 als IETF-Standard verabschiedet
  - Internet Standards RFCs 2632-2634 (und weitere)
  - in die meisten E-Mail-Clients integriert
  - E-Mailverschlüsselung und –signatur
  - One-pass processing: Die Mail ist in einem Schritt verarbeitbar, da alle benötigten Daten in die Mail selbst integriert sind

- PGP (Pretty Good Privacy)
  - 1991 von Philip Zimmermann entwickelt
  - E-Mail- und Dateiverschlüsselung und –signatur
  - heute: Open PGP, GnuPG (Gnu Privacy Guard)
  - Zahlreiche grafische Frontends erhältlich, z.B. GPA, WinPT
  - Plugins für verschiedene Mailclients, z.B. Outlook, Thunderbird, Pegasus, KMail

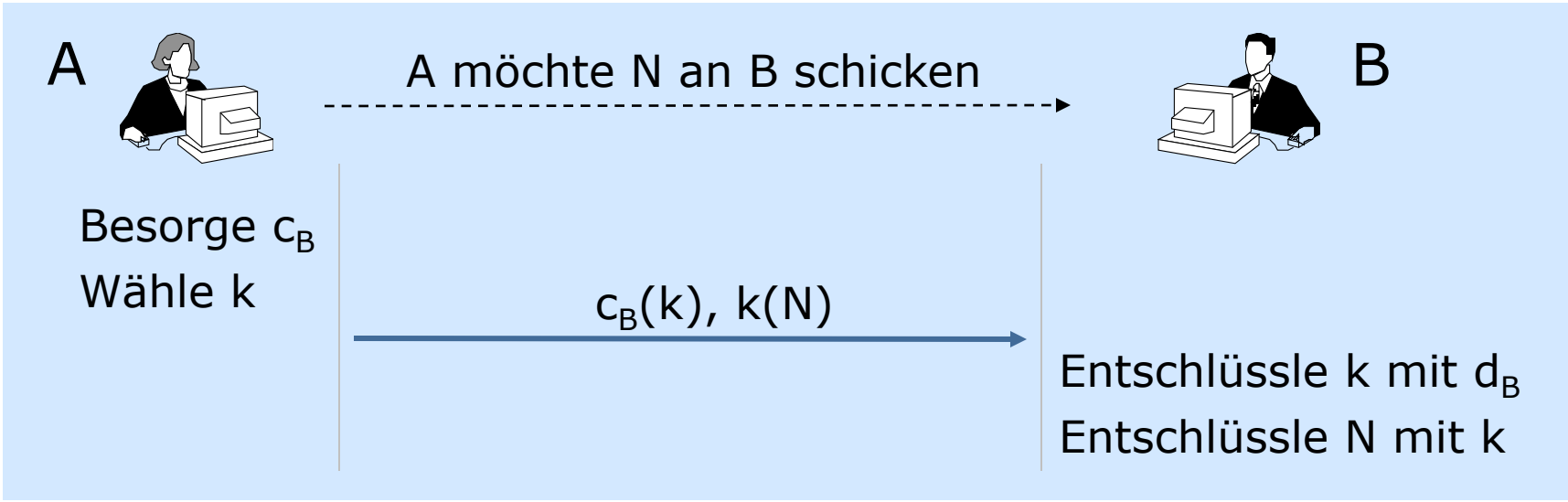
S/MIME und PGP nutzen hybrides Verschlüsselungsverfahren



S/MIME und PGP nutzen hybrides Verschlüsselungsverfahren

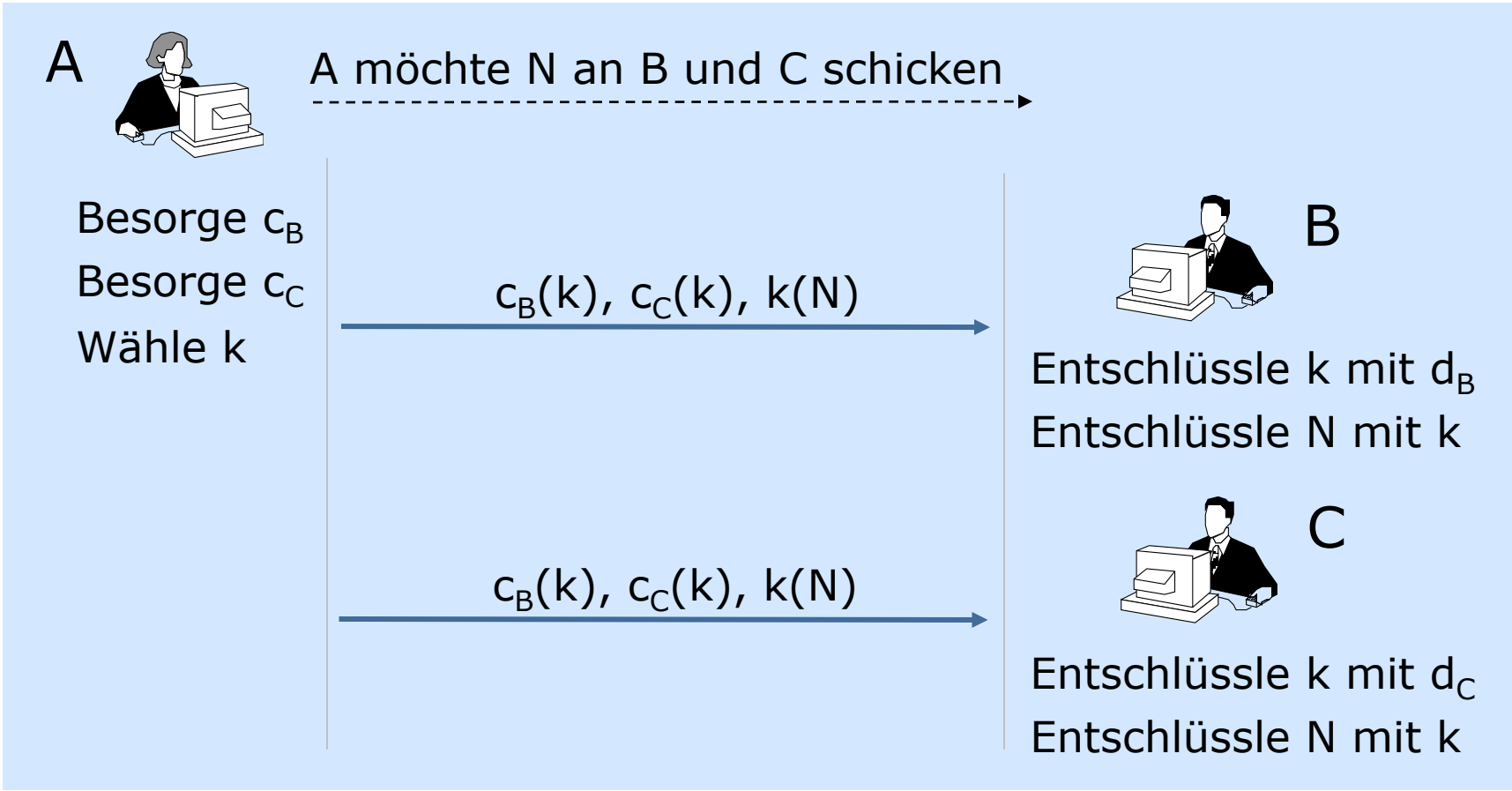
- Hybrides Verschlüsselungsverfahren
  - Nachrichten selbst werden symmetrisch verschlüsselt
  - Nachrichtenschlüssel werden asymmetrisch verschlüsselt

c_B	öffentlicher Schlüssel von B
d_B	privater Schlüssel von B
k	symmetrischer Nachrichtenschlüssel



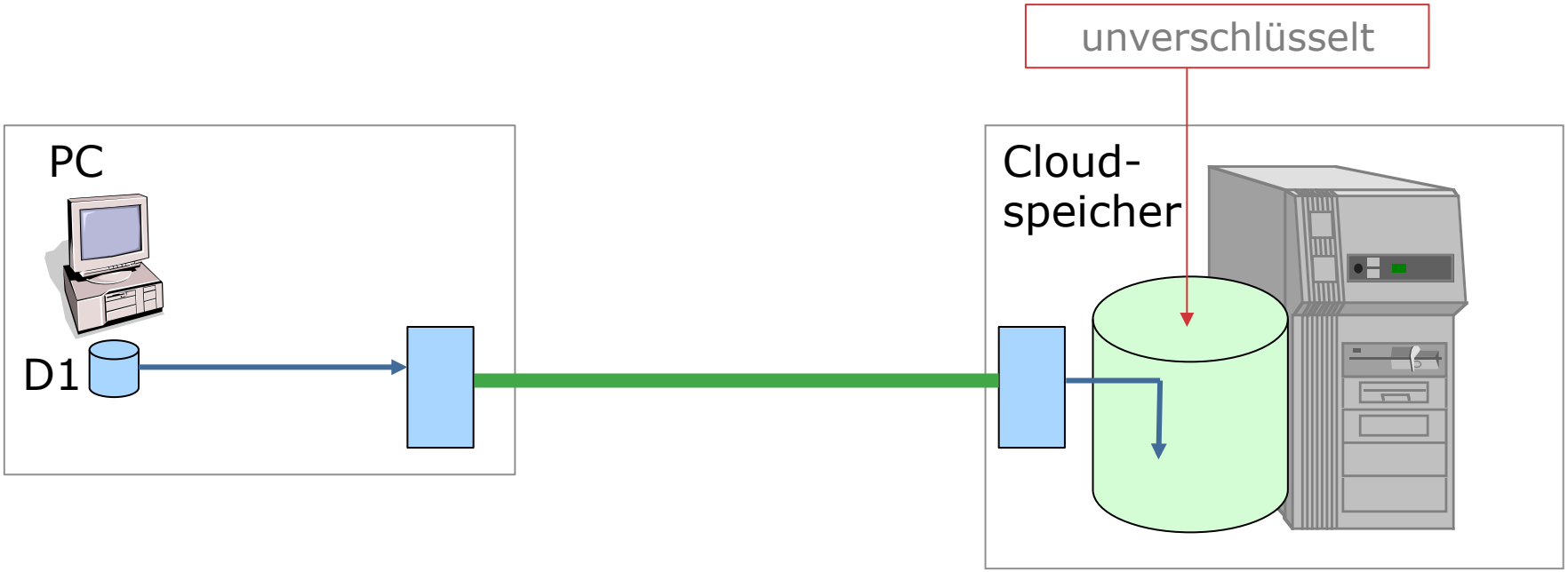
S/MIME und PGP nutzen hybrides Verschlüsselungsverfahren

- Hybrides Verschlüsselungsverfahren
  - Nachrichten selbst werden symmetrisch verschlüsselt
  - Nachrichtenschlüssel werden asymmetrisch verschlüsselt



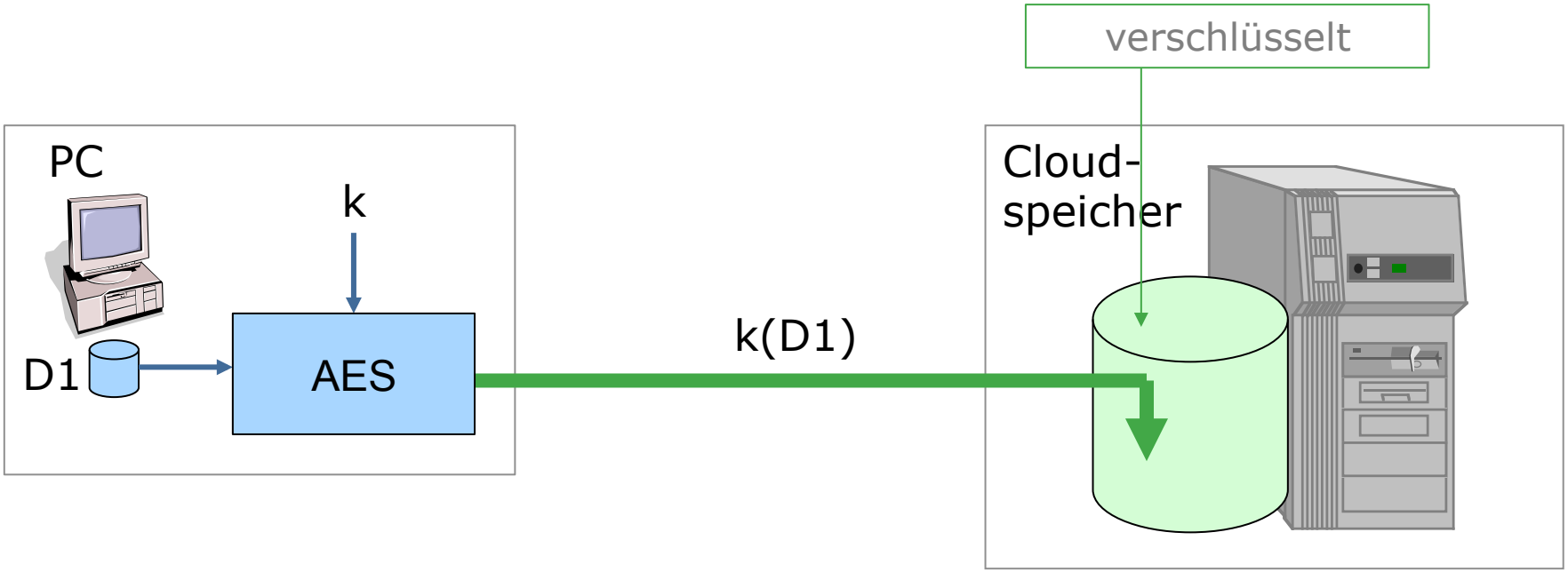
Verschlüsselte Cloud-Speicher

- Verbindungsverschlüsselung ist heute Standard



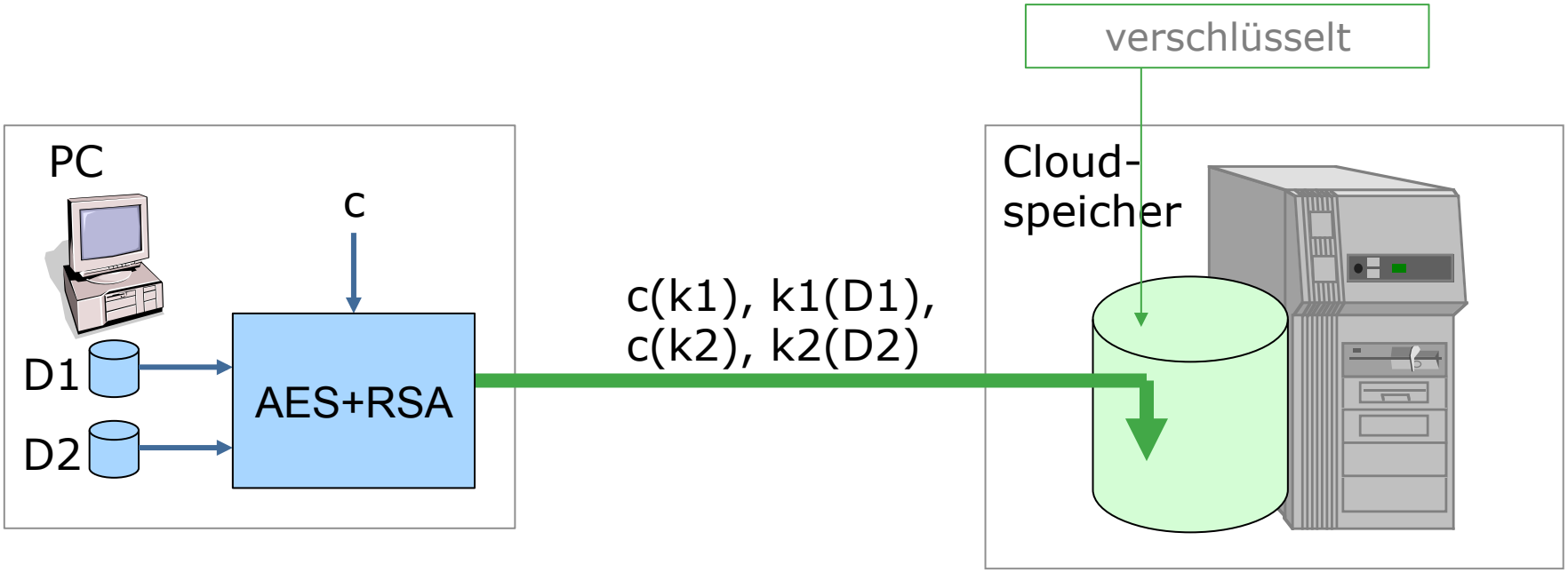
Verschlüsselte Cloud-Speicher

- Ende-zu-Ende-Verschlüsselung wäre kein Problem



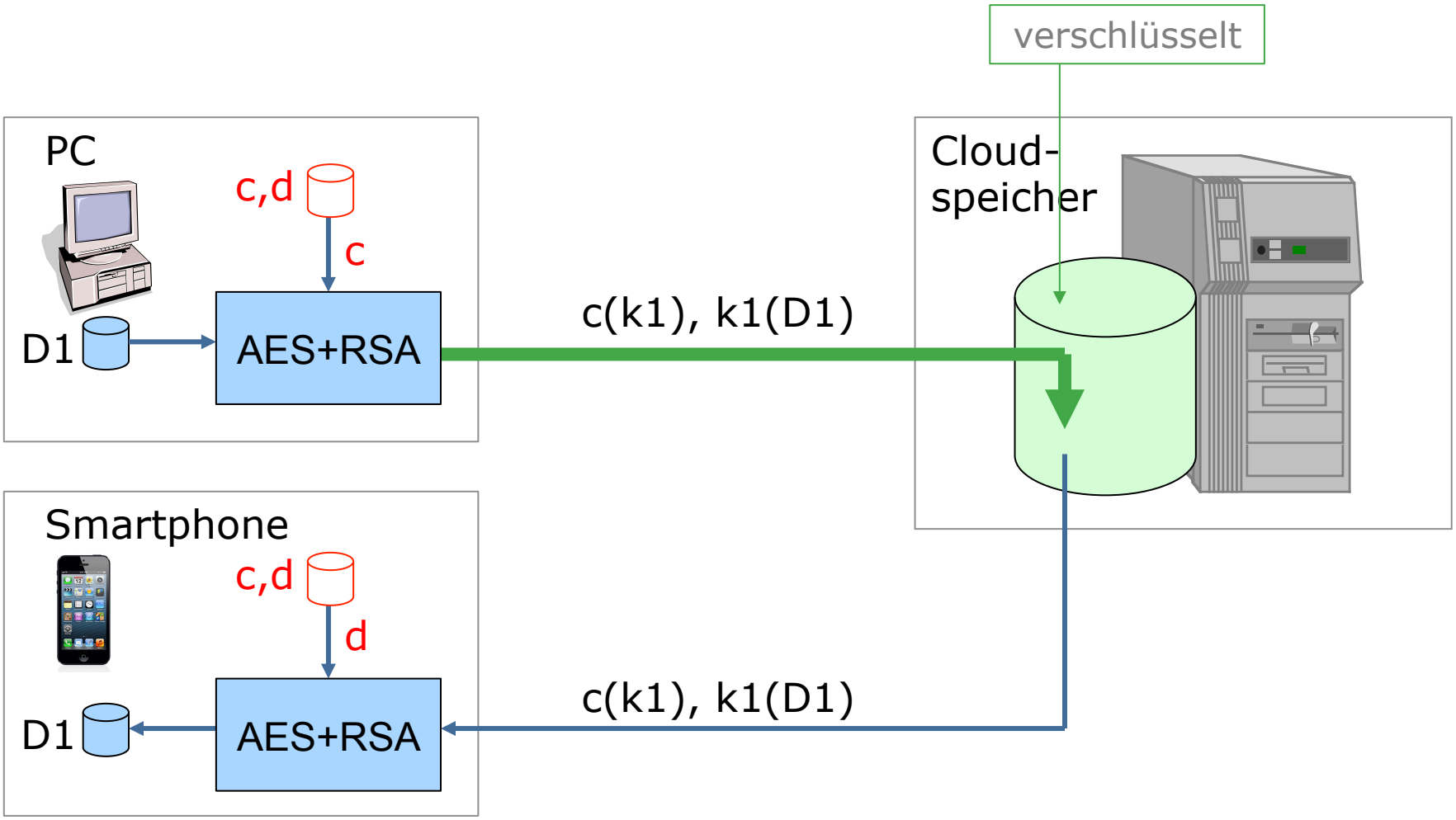
Verschlüsselte Cloud-Speicher

- Ende-zu-Ende-Verschlüsselung besser hybrid …



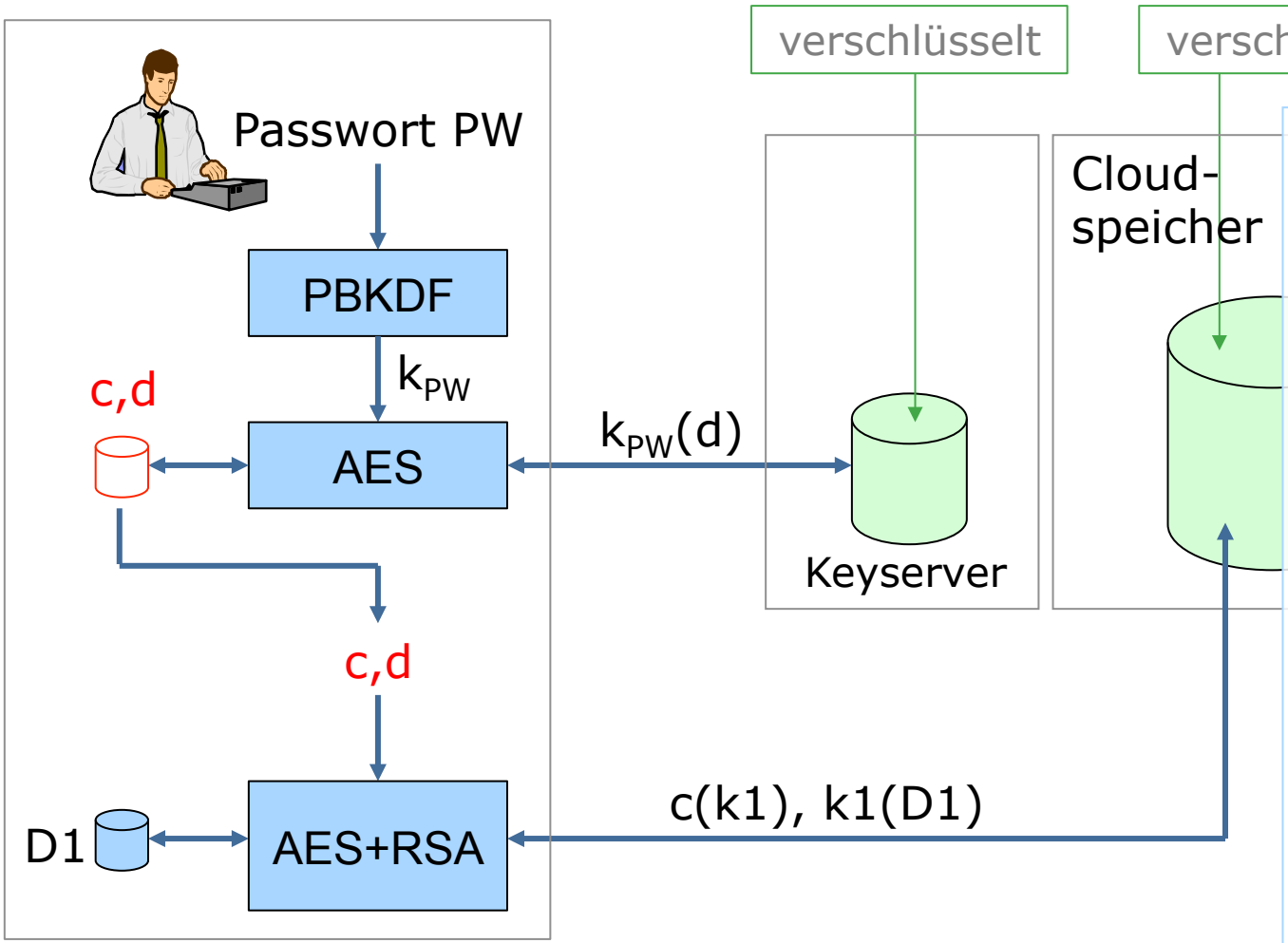
Verschlüsselte Cloud-Speicher – Usability-Aspekte

- Wie bekommt der Nutzer auf alle seine Geräte seine(n) Schlüssel?



Verschlüsselte Cloud-Speicher – Usability-Aspekte

- Wie bekommt der Nutzer auf alle seine Geräte seine(n) Schlüssel?

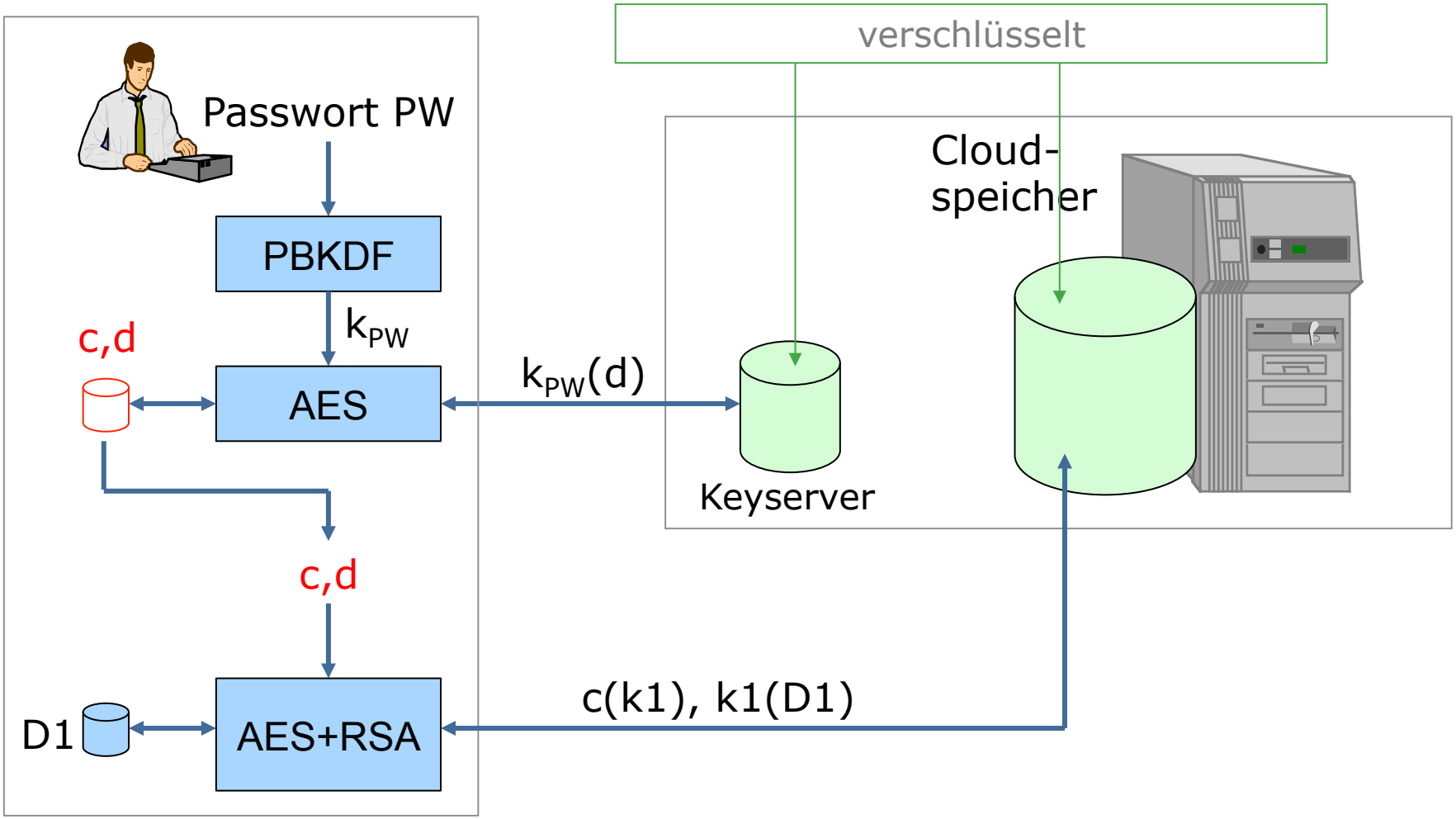


- Das Schlüsselpaar c,d wird lokal beim Nutzer erzeugt.
- Aus dem Passwort PW wird ein symm. Schlüssel k_{PW} (Passwortschlüssel) abgeleitet.
- Mit dem Passwortschlüssel wird der private Schlüssel d verschlüsselt.
- Auf dem Keyserver werden abgelegt: Nutzername, c, $k_{PW}(d)$.

- Andere Geräte können sich den (verschlüsselten) privaten Schlüssel holen und nur bei Kenntnis von PW entschlüsseln. Der Betreiber des Keyservers erfährt nichts über d und alle damit verschlüsselten Schlüssel.

Verschlüsselte Cloud-Speicher – Usability-Aspekte

- Wie bekommt der Nutzer auf alle seine Geräte seine(n) Schlüssel?



Verschlüsselte Cloud-Speicher

Ausgelagertes Objekt mit Schutz durch	Das kann der Provider des Cloudspeichers sehen	Einfachstes Angriffs-Szenario
Boxcryptor 2.0	Zahl und ungefähre Größen der Dateien, optional: Dateinamen	Passwortklau per Phishing
Boxcryptor Classic	Zahl und ungefähre Größen der Dateien, optional: Dateinamen	Passwortkla
Ctera Portal	Gesamtgröße des Speichers	Zugang zum Client-Rechner und Fake der Zwei-Faktor-Authentifizierung
Skycrypt	Zahl und Attribute der Dateien	Passwortklau, etwa durch Keylogger
SpiderOak	Zahl der gesicherten Geräte, Gesamt-Speicher je Gerät, bei WebDAV-Zugriff das Anmelde-passwort	Passwortklau, etwa durch Keylogger
SpiderOak-ShareRoom	Klartext und Metadaten	Abfangen des unverschlüsselten URL
Stackfield	Zahl, Namen und ungefähre Größe der Dateien	Passwortklau per Phishing
Teamdrive	Gesamtgröße des Spaces (Doku-mentablage in einem Datenbank-Container)	Passwortklau, etwa durch Keylogger, oder Zugang zum Client-Rechner und Fake der Zwei-Faktor-Authentifizierung
Tresorit	Zahl, Namen und ungefähre Größe der Dateien	Zugang zum Client-Rechner und Fake der Zwei-Faktor-Authentifizierung

EzE-Verschlüsselung in Cloud-Dienst integriert

c't 2015 Heft 19, S. 113

Zusammenfassung

- Die Grundprinzipien sicherer Ende-zu-Ende verschlüsselter
  - E-Mail
  - Cloud-Speicher

  sind kryptographisch sehr ähnlich.

- Usability-Fragestellungen sind häufig Ursache für weniger sichere Lösungen.

Universität Hamburg
Fachbereich Informatik
Arbeitsbereich SVS
Prof. Dr. Hannes Federrath
Vogt-Kölln-Straße 30
D-22527 Hamburg

E-Mail federrath@informatik.uni-hamburg.de

Telefon +49 40 42883 2358

https://svs.informatik.uni-hamburg.de

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG