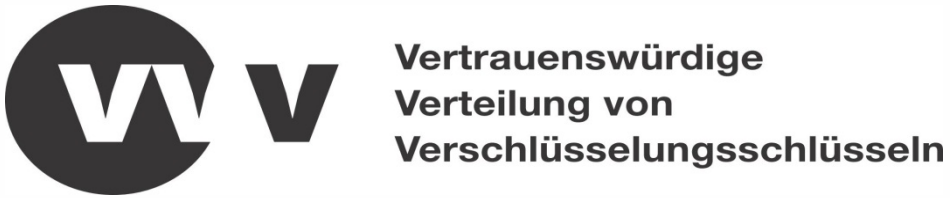
Selbstdatenschutz

E-Mail-Verschlüsselung und Verteilung von öffentlichen Schlüsseln



von

Susan Gonscherowski

Warum Selbstdatenschutz?

Ich habe doch nichts zu verbergen!

Was ist denn schon dabei?! Steht ja nichts Wichtiges drin.

Die können doch eh jede Verschlüsselung knacken!

Warum Selbstdatenschutz?

Stellen Sie sich vor:

- Ihre Bank hängt Ihre Kontoauszüge öffentlich aus.
- Ihr Finanzberater versendet Ihre Unterlagen versehentlich an die falsche E-Mail-Adresse.
- Ihre Steuerunterlagen werden an Ihre Nachbarn oder an Ihren Ex-Partner versendet.
- Details aus Ihrem Liebesleben werden in der Zeitung abgedruckt.

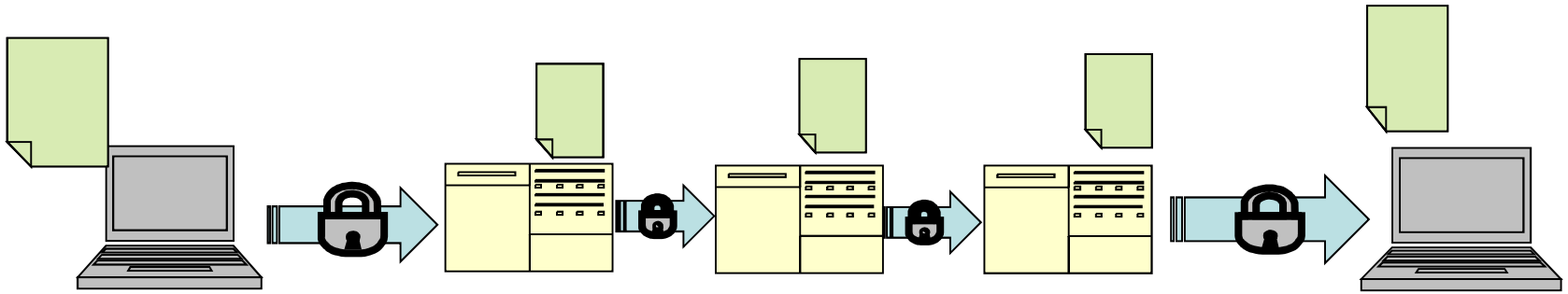
Darum Selbstdatenschutz!

- Mündige Bürger statt bevormundete Bürger – Sie sollen entscheiden, wann eine Nachricht persönlich und schützenswert ist

- Schützen und Nutzen Sie Ihre Grundrechte – Sie haben ein Recht auf „Geheimnisse" (Brief, Telefon, Arzt, Anwalt, Geschäft/Unternehmen, Privatsphäre)

Warum Ende-zu-Ende-Verschlüsselung?

- E-Mail heute (unverschlüsselt)



Verfasser Server Empfänger

- Unverschlüsselte Inhalte sind schlicht günstige Gelegenheiten für jeden „Angreifer"

Warum Ende-zu-Ende-Verschlüsselung?

- Unberechtigte Empfänger
- Provider: Der „Briefträger" kann mitlesen
- Ermittlungsbehörden und Geheimdienste (auch von Drittstaaten) haben z.Z. fast unbegrenzten Zugang zu Daten
- Hacker haben es leichter

Empfänger

- unberechtigter Empfänger:
  - Ein falscher Klick im Adressbuch und die E-Mail an Ihren alten Schulfreund Thomas Müller geht an Ihren Chef Thomas Müller

  thomas-mueller@gmx.de oder thomas-mueller@web.de

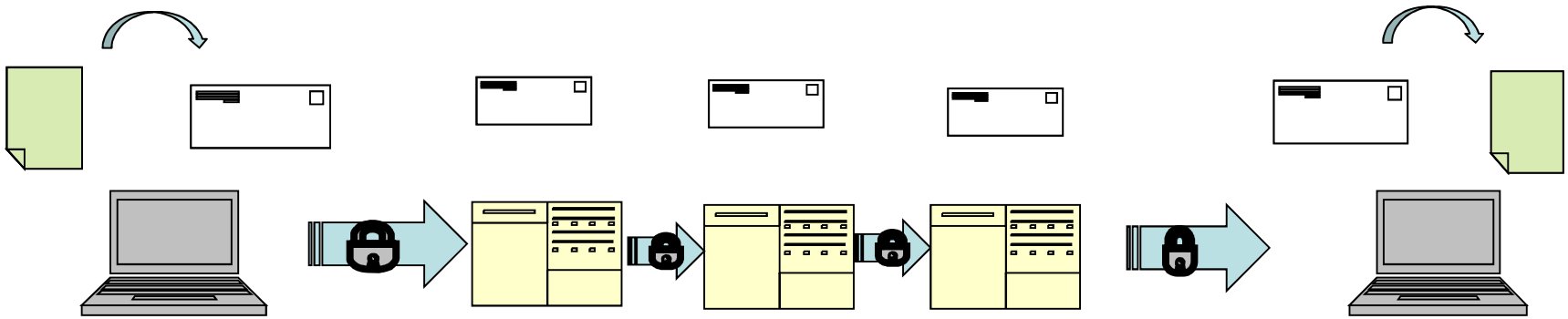
  Weil die Mail nicht verschlüsselt ist, weiß nun auch Ihr Chef, dass…

  - Eine Verwechslung beim Eintippen einer Adresse fällt noch weniger auf, z.B.

  thomas68@example.de oder thomas86@example.de

Das Prinzip der E-Mail-Verschlüsselung

- E-Mail verschlüsselt



- E-Mail-Verschlüsselung ist ein elektronischer Briefumschlag
- E-Mail-Verschlüsselung schützt vor Kenntnisnahme Dritter

Das Prinzip der Verschlüsselung

- Verschlüsseln:
  - (einen Text) nach einem bestimmten Schlüssel (Formel) umwandeln
  - unkenntlich machen und nur für Berechtigte sichtbar werden lassen

http://www.duden.de/rechtschreibung/verschluesseln#Bedeutunga

- Methoden sind z.B.:
  - Verstecken **K**alle **a**rbeitet **t**äglich **z**wei **E**inheiten**!**

  (immer der 1. Buchstabe) -> Katze!
  - Austauschen 3537 (3=E, 5=S, 7=L) -> ESEL

Das Prinzip der Verschlüsselung

- Symmetrische Verschlüsselung (der Klassiker)
  - Sender und Empfänger der Botschaft müssen den geheimen Schlüssel kennen.
    - Immer der 1. Buchstabe oder (3=E, 5=S, 7=L)

- Schwachstellen der symmetrischen Verschlüsselung
  1. Um geheim zu kommunizieren, muss man vorher vertraulich kommunizieren können.
  2. Wird der Schlüssel einem Dritten bekannt, kann dieser ebenfalls die Botschaft decodieren.
  3. Mit jedem neuen Gesprächspartner muss wieder ein neuer Schlüssel getauscht werden.

Das Prinzip der Verschlüsselung

- Asymmetrische Verschlüsselung
  - Der Empfänger stellt einen öffentlichen Schlüssel für alle bereit
  - Der Empfänger besitzt einen zweiten, geheimen Schlüssel

- Die 3 genannten Schwachstellen der symmetrischen Verschlüsselung sind hier nicht mehr von Bedeutung

Wie funktioniert Verschlüsselung?

- Mit dem öffentlichen Schlüssel lässt sich nur **VER**schlüsseln

-> Jeder darf und soll den Schlüssel kennen

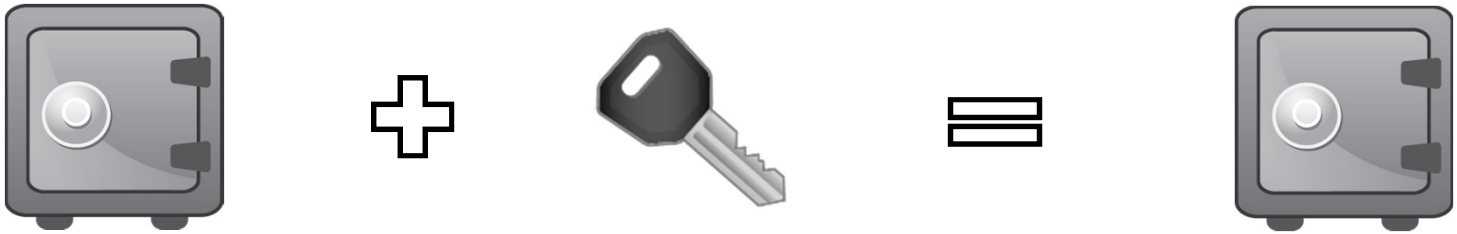
öffentlicher Schlüssel

Quelle Cliparts: Libre Office Writer Version: 5.1.5.2

Wie funktioniert Verschlüsselung?

- Zum **ENT**schlüsseln wird der private Schlüssel gebraucht

-> Nur Sie dürfen diesen Schlüssel kennen



öffentlicher Schlüssel

Privater Schlüssel (geheim)

Quelle Cliparts: Libre Office Writer Version: 5.1.5.2

2 Möglichkeiten 1 Prinzip: GPG und S/MIME

- Hauptunterschied der beiden Verfahren ist das unterschiedliche Vertrauensmodell

- GPG – Web of Trust:
  - Die Nutzer bestätigen sich gegenseitig, dass sie dem öffentlichen Schlüssel des anderen vertrauen

- S/MIME – Certificate Agency:
  - Eine Agentur prüft die Zugehörigkeit eines Schlüssels zu einer Mail-Adresse/Person und bestätigt dies in einem Zertifikat

Wie funktioniert Ende-zu-Ende-Verschlüsselung?

- Öffentlicher Schlüssel des ULD:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQSuBFXe+LkRDACqYurI1BcXZiYeP96K/fLomhYu4Ry4ihZf/8I+v89b9NIr5g/k
CXWmjTjTRr45pHhBUPD4X8CNql+oEzv4FeVLWPbFsaYzF3nDI3O9xJl8wT9ewZ9g
4TqEKxxAkXr3V9NXGPFedSrLydqIcMbe0ydP7S7lvndHnfw3zczEo07YEnB3N4IN
pnUl8n0m1JEqmWyaB4EBkpJiX4rxTE2bCdTfeaJsozUWH/kyOHKw89eJyJ91teLO
D5/9X4LsSGdwOwNrjDSzt1EaeFIjpswcYjeUdNnAbQ/VmwOSc60pN+8UVl6A2Nfx
jtj8frR4Dkd9FEUrkEue7HKjU7ZB8lLavVNrbr1481l3VipxPuu5cuNrzLXfi2lR
tGcclGnSeVOPq2oFezCM/egvJAYf0RZ5u3gc61uvH/qAPamCLGqWZ6uYXM8EA5Qv
fWuW0oGM/OJdEBtC1bZJ1Qfe9DRhfnXZIINHjaVbLC4c6PfLuiYwnWsBWteYSQdl
LhGui0HuAUdQZYsBAJkvBl3qxOUcgve0pUoUh4OVmzBbS38GgqnDpxTrByw5DACY
W6Lhfyk9VPmf+VKbIoQRob3V5MrOWIi+zOWi85laLKHn2StxSHQJBa1+S6EZ16Ov
m4wE+LKvJ7/beqq0VBNHi/vuhjzLozeHe+BeXM9cLXzSU0TQXQxqa8A4J1bwikvb
OLFTgI/2LKn5zylyeljJUNRmgQMsITqaQbHlw8jw7LT/3mVplHT+wWxRQ+RZcOQZ
qbI+SF3TlgLj4kf0ZA8muYbfUAc2PlythbVsdk8KTXJK3u5v/0bvvPjtPxkzCsmW
l7XsaF+MKkczhin9fw9IofwNnkGsYR4YYJSuBtXJs+6jyhAUH4vqKusNC/Tt6PjR
3QX+e6A0o+c6XVKoaJzG3kTDghsbYJxDOqPKDj6SzlZUURQQ65MUSxBKN0De8Qmm
Pgy7N1sPD9MCet338/rMWFYH6lq74gK8J7SO/tzA/OyWEWTaig5tdwkV7PU+Rx2m
0l5LX0cDXVPSNxwZ7NjQohvu6bmJ4QD6yw1j0n3DlJbcaYvZOkbb+UXjbLuJsMIL
/AmyLFz1FIUV8TESy/9AZmtihzxaP0Z1JuCIxOBqFOziPmrYRpkiifg1knptxIxa
GCvvY+czFpcHsLn1F5Y4hQzyTFZFdgV8UnlIZpWhMO6/NmEer13G15zO1QLSTPHx
aoRKGzwCtRTEJQ+nxwPIP73E+rGha0sOPwvT6zNi7d248RuVrpT8EsfScDn4W7So
4Odiwf6+Nv63BtMjEDlxURVpf6jTqVxrqWqGzR4boI06jqa4tZk6NLQEP91JgpRN
kchLpGsDzbw5Zu2ZyMtaBMq9HcwDlOxw8lTbL9t43TRUnE/y88eikXJ44bnzE39d
lvu/YmtIcwNYgs/tF5t+DuxLTmNqQbJp3487cRpy86EuubmXJT4fWnlE4W3dR2zS
vkG7eMNkOe4ru9YbL4NasNhUVGSeoryL9/xu3WVqTX7bLsFSljws2jDZXAe7JhBD
7sceS7auieC/HgPWFYDH8PGJ8dEmvn2PJfh/99MCdZz1h7o+bXqF13r6jevqmpBX
MbRcVW5hYmjDpG5naWdlcyBMYW5kZXN6ZW50cnVtIGbDvHIgRGF0ZW5zY2h1dHog
U2NobGVzd2lnLUhvbHN0ZWluIDxtYWlsQGRhdGVuc2NodXR6emVudHJ1bS5kZT6I
gwQTEQgAKwIbAwUJCWYBgAIeAQIXgAUCVd77RwkLCQgHAwQKAQIFFQoJCAIFFgID
AQAACgkQZtXAVZkcUGCFnAD+M9di8gCJGFBjcUTUnqdUO0ioC/KBk0egdiTFTnO9
MdYBAIN2i1SloEnHGRGg2pvahzCxq8EligdY75YckmMhM9xyiF4EExEIAAYFAlXe
/U0ACgkQDXUZnhE1cyT5OgD+JdVpiTRWywrPcpZXAKRK3P0KMBwtxS+9YHGaLgu1
eq8A/1In4txqzBPc0QlUdmY7Coit5t0k3vtlyGyKnsDJMwnsuQMNBFXe+LkQDADH
bYLO257CKI29UbfjP2Jw7uoSzMe5iO3ZcPRB1145iVdZkHNPXd0BfuWEEWlWOvl8
OitlgSS9ovzWQBizKJD4w2mXfcHlFtoE95Ei1MkdAYISuQ4mFi0CA7Ic7YHSBYGU
G+/95PC1+9A2ZX3VF2KDJ3WZ9ZZh8eygZvRqStE+OuFdqvtYYpqr9lN8tszAORAe
xeUp2tJbQyEnMg4KDdleSyVi8L1CvCCAkg5WAsxlEzrNNmC/ox66R+Q3ktMMfmJs
zGLh75DPFiko+ebNgkSDDr5kg4J/GUfcBHzXMcxalAOJxFb3O4VPhzOvvwCzoRFK
DRb/R8Ad+UTZ+HHVjgVEIpuRDUZncp9eSG+6AR07vMixXhLbdz7IuwsbiHDBN+dq
rL8RFVoxAXnWVWLvs74DVvY0pKcRc24Aj+eqpTPhfeQyccI0rvity5ll9kd6fwRL
U1qSDiTINkPxv212hm0JhSlvrT/VKE919ApzQpTDc+lo9RS6sRiBj/D3M8zIH8cA
AwUMAMYmYypKSeMlb7dc40r/OQ+tspXWRx2oGLtUhMp/J9C2/ZLULfT1C/4e/INr
XLWpq8DjOUo0v1xcEcII5SGq7yOLzQLgMJlFEMw3NRpRJ5YZoMJ9KFbG6vNoVxF9
CkFK0D9hJ91enI+nJePt3e0zl3J81JdnINQ363cN2q2uOospkXFHpjeFY2pmfRJO
vOKBtZF8dtUqNNSyj4pewizcDocrhtaR1MrERgZNNiQWBFScmkBKfgbktqLGaONR
9ltH2F+ElkJ4e2CILI/GcLALcuEeLZeBGSwWnKwPCYDumN+dikieY9nA725nTD7r
CmSqEI66a5WZPnG+d5lLPzAnTve7qNOQYLfVO5LLFgijOdyguIwsit/FcWZYIS2L
ZQndVUJneScUJ5C0WFT/rk+OKKz9r/swe1wl5s28tTkMX1Z8ALLo2fb5xHigO9U2
U5TGxoig5qisJToXvQ+HdQZQtmR1IMlICH7QEBf10YaFL4DzQIAbfAg0GHaRuG9O
mWfNAYhnBBgRCAAPBQJV3vi5AhsMBQkJZgGAAAoJEGbVwFWZHFBgtg0A/2GjtyAX
cHhSA28ZGSkhd4IrvGQnFNZD0ZF8I3O2UwZbAP9Wcq1wMEqL23g37ZF/ISTY1jPa
VgqKx0g1G8QYueDznw==
=1tKG
-----END PGP PUBLIC KEY BLOCK-----

Wie funktioniert Ende-zu-Ende-Verschlüsselung?

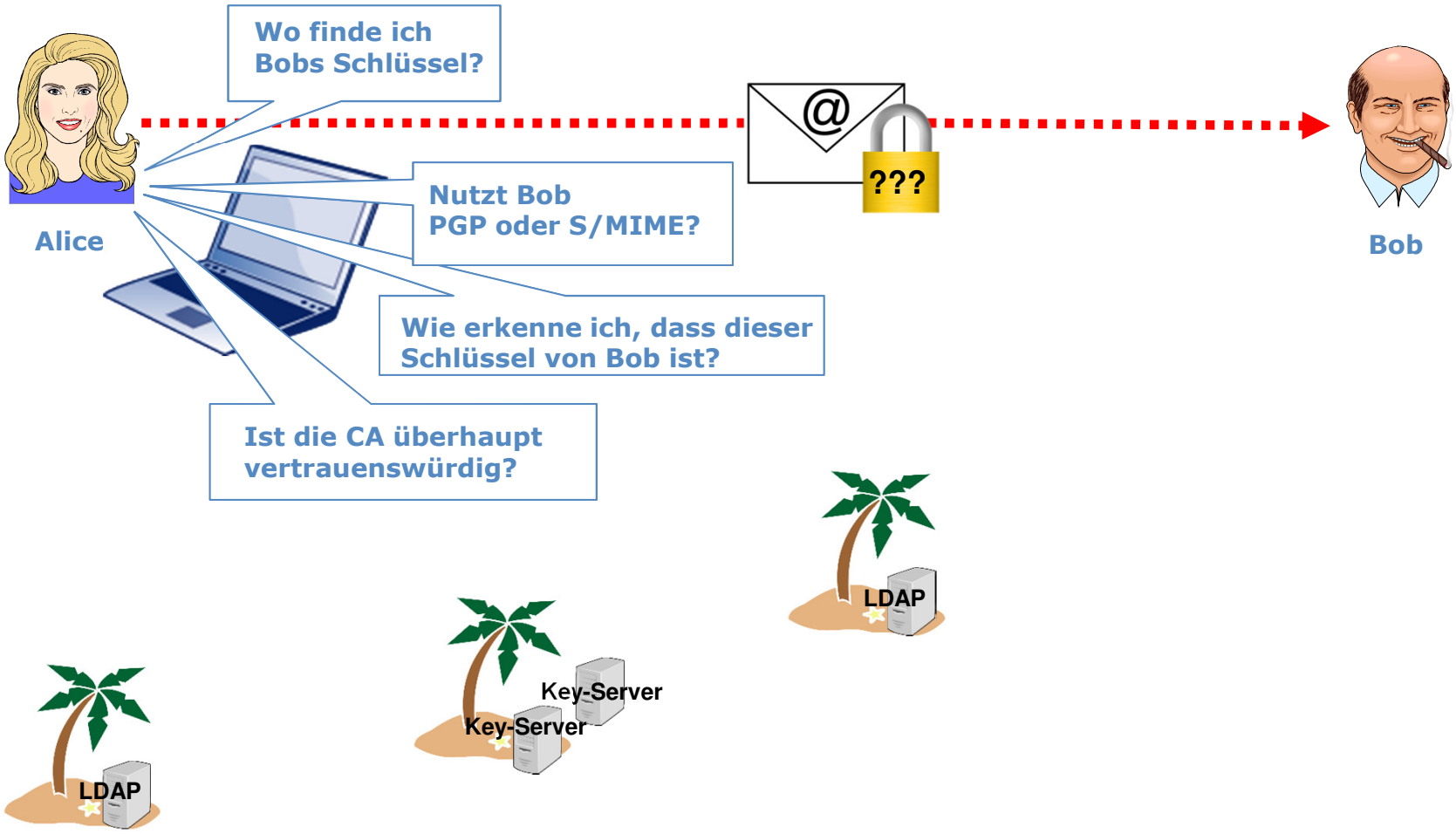
- 1. Schritt: Verschlüsselte Mails **empfangen** können
  - Erstellen eines Schlüsselpaares
  - Veröffentlichen des öffentlichen Schlüssels
  - Eingegangene Mails mit dem privaten Schlüssel decodieren

- 2. Schritt: Verschlüsselte Mails **senden**
  - Suchen des öffentlichen Schlüssels des Empfängers
  - Nachricht mit dessen öffentlichen Schlüssel verschlüsseln
  - Senden

Warum verwenden nur wenige Ende-zu-Ende- Verschlüsselung?

- GPG und S/MIME sind nicht interoperabel
- Es ist nicht ersichtlich, ob und wenn ja, welche Verschlüsselung vom Kommunikationspartner verwendet wird
- Dem Nutzer ist oft nicht klar, wo die öffentlichen Schlüssel zu finden sind
- Nutzer wissen oft nicht, wo sie eigene Schlüssel bekommen
- Vorhandene Tools sind schwer zu verstehen, wenn das Prinzip dahinter nicht verstanden wurde

Ausgangslage: Alice ist ratlos...



Quelle: VVV

Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln

Informationsabend zum Thema „Selbstdatenschutz“

Windbergen, 07.11.2016

Gefördert vom Bundesministerium für Bildung und Forschung

© Fraunhofer-Gesellschaft 2016

Design Research Lab

Fraunhofer SIT

mailbox.org damit Privates privat bleibt

provet Projektgruppe verfassungsverträgliche Technikgestaltung

ULD

Forschungsprojekt VVV

- **Lösungsanforderungen** (Auswahl):
  - Einfachheit: Die Kenntnis der E-Mail-Adresse soll ausreichen.
  - Privatsphäre: Nur die absolut notwendigen Daten sollen vorgehalten werden.
  - Authentizität: Die DNSSEC-Infrastruktur soll genutzt werden.

VVV Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln

Forschungsprojekt VVV

- **Was wird entwickelt:**
  - Plugin zur Verwaltung öffentlicher Schlüssel sowohl für native Mail-Clients (Thunderbird) als auch WebMail-Clients (Open-Xchange)
- **Was soll die Erweiterung bewirken:**
  - Schlüssel über vertrauenswürde Kanäle verteilen
  - Schlüssel der Kommunikationspartner automatisch ermitteln
  - Schlüssel der Mail-Anwendung zur Verfügung stellen

VVV Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln

Ziele von VVV

- **Verschlüsseln wird insgesamt benutzungsfreundlicher**

-> Mail-Provider veröffentlich die Schlüssel auf Weisung des Nutzers

- **Zu jeder Adresse kann ein OpenPGP- und ein S/MIME- Schlüssel hinterlegt werden**

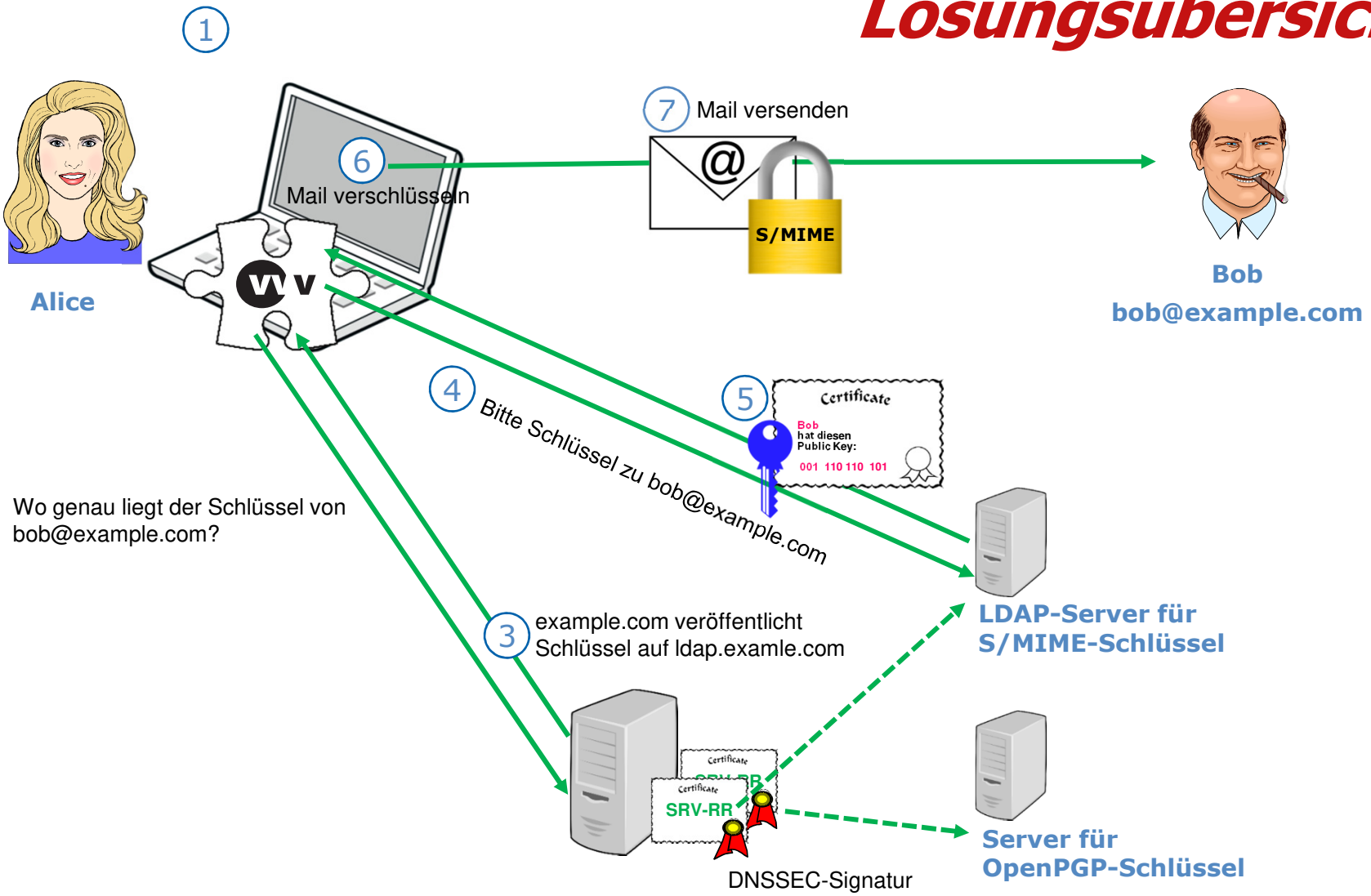
-> jeder Schlüssel gilt als aktuell und vom Nutzer autorisiert (authentisch)

- **Unerfahrene Nutzer sollen unterstützt werden, damit Ende-zu-Ende-Verschlüsselung flächendeckend zum Einsatz kommt**

- **Technische und juristische Konzeption für die Verteilung und Nutzung kryptographischer Schlüssel**

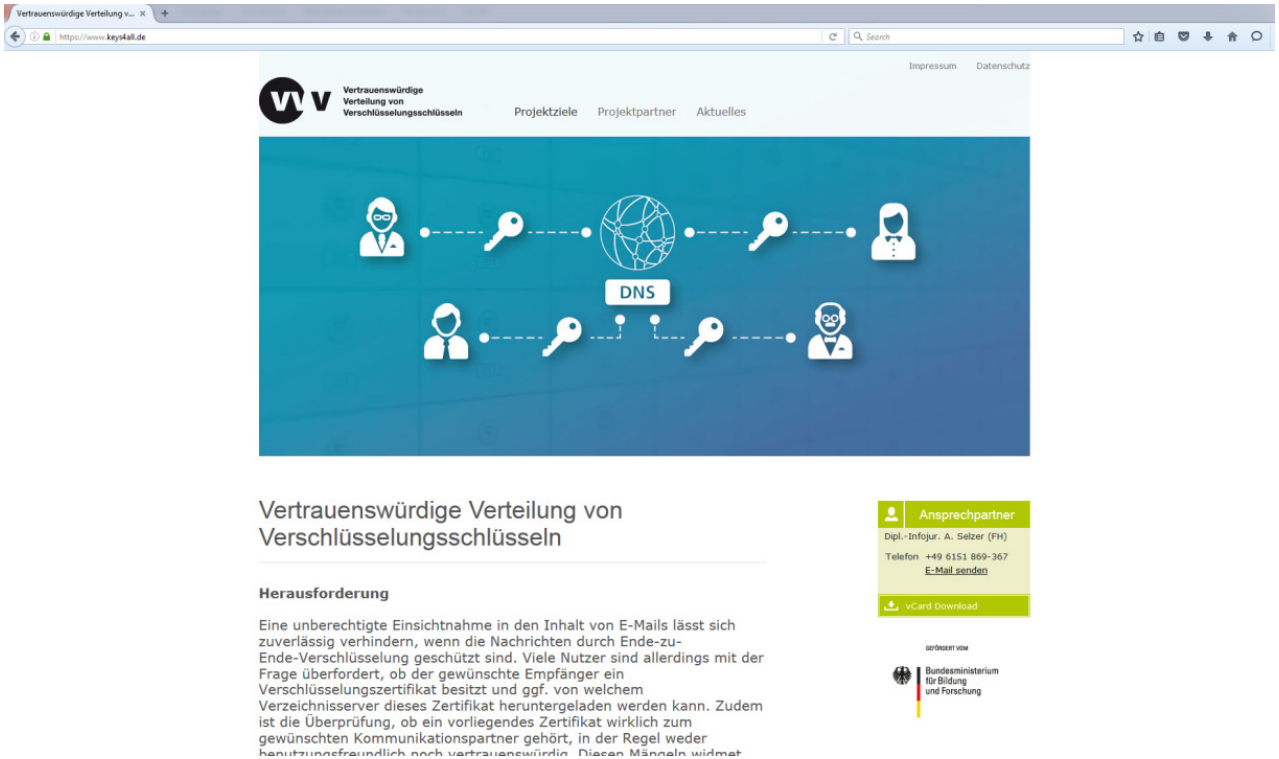
- **Implementierung eines benutzungsfreundlichen Demonstrators**

Lösungsübersicht



Quelle: VVV

Weitere Informationen zum Projekt auf www.keys4all.de



© Fraunhofer-Gesellschaft 2016

Allgemeine Hinweise

- Verschiedene Mail-Adressen für unterschiedliche Zwecke verwenden (=Identitätsmanagement)
- Mail-Provider gewissenhaft auswählen
- Sicheres E-Mail-Passwort erstellen
- Absender prüfen
- (Bei Zweifeln am Absender den ganzen Header anzeigen lassen)
- Betreff formulieren, der für den Empfänger verständlich ist, ohne dass sich auf den Inhalt schließen lässt
- SPAM-Filter verwenden und füttern
- Mails im Text-Format nicht im HTML-Format lesen und schreiben
- Anhänge verschlüsseln
- BCC statt An bei Gruppenmails
- Ausloggen nicht vergessen!

Danke für Ihre Aufmerksamkeit

Fragen?

Susan Gonscherowski

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

https://www.datenschutzzentrum.de

ULD611@datenschutzzentrum.de

0431 988-1229