GNU Privacy Guard im Detail

ghostav@riseup.net

jugendclubbureau

16. Juli 2014

Ziele der Veranstaltung

- Aktuelle “Enthüllungen” zeigen Notwendigkeit, sich selbst um seine Privatsphäre zu kümmern

Ziele der Veranstaltung

- Aktuelle “Enthüllungen” zeigen Notwendigkeit, sich selbst um seine Privatsphäre zu kümmern
- mehr Workshop als Vortrag, denn
  - Es gibt bereits zahlreiche Tools, die sich dem Problem annehmen
  - aber oftmals für nicht-“Nerds” unverständlich
  - $\Rightarrow$ Das Rad nicht neu erfinden, aber massentauglich machen!

Ziele der Veranstaltung

- Aktuelle “Enthüllungen” zeigen Notwendigkeit, sich selbst um seine Privatsphäre zu kümmern
- mehr Workshop als Vortrag, denn
  - Es gibt bereits zahlreiche Tools, die sich dem Problem annehmen
  - aber oftmals für nicht-“Nerds” unverständlich
  - $\Rightarrow$ Das Rad nicht neu erfinden, aber massentauglich machen!
- Treffpunkt für Interessierte um Antwoten auf die eigenen Fragen zu bekommen (vorzugsweise mit Bezug zur IT-Sicherheit...)

Ziele der Veranstaltung

- Aktuelle “Enthüllungen” zeigen Notwendigkeit, sich selbst um seine Privatsphäre zu kümmern
- mehr Workshop als Vortrag, denn
  - Es gibt bereits zahlreiche Tools, die sich dem Problem annehmen
  - aber oftmals für nicht-“Nerds” unverständlich
  - $\Rightarrow$ Das Rad nicht neu erfinden, aber massentauglich machen!
- Treffpunkt für Interessierte um Antwoten auf die eigenen Fragen zu bekommen (vorzugsweise mit Bezug zur IT-Sicherheit...)

$\Rightarrow$ Themengebiet kann auch spontan geändert werden, falls Teilnehmer gerade andere Fragen/Themen wichtiger finden

Do and don't

Do

- Mitbringen der eigenen Hardware um alles direkt auszuprobieren
- Auch parallel zum Vortrag bereits angesprochene Tools herunterladen/installieren/testen

  ESSID `Cryptoparty`
  Passwort `CryptoParty`
- Bei Zwischenfragen (zum Thema) direkt unterbrechen

Do and don't

Do

- Mitbringen der eigenen Hardware um alles direkt auszuprobieren
- Auch parallel zum Vortrag bereits angesprochene Tools herunterladen/installieren/testen

  ESSID `Cryptoparty`
  Passwort `CryptoParty`
- Bei Zwischenfragen (zum Thema) direkt unterbrechen

Don't

- Streaming/Filesharing
- Fotos, Videos oder Tonaufnahmen
- Klarnamenzwang oder verlangen von Ausweisen
- Mitschneiden von Datenpaketen, Portscanner, Man-in-the Middle (ARP-,DNS-,DHCP-Spoofing,...)

Do and don't

Do

- Mitbringen der eigenen Hardware um alles direkt auszuprobieren
- Auch parallel zum Vortrag bereits angesprochene Tools herunterladen/installieren/testen

  ESSID `Cryptoparty`
  Passwort `CryptoParty`
- Bei Zwischenfragen (zum Thema) direkt unterbrechen

Don't

- Streaming/Filesharing
- Fotos, Videos oder Tonaufnahmen
- Klarnamenzwang oder verlangen von Ausweisen
- Mitschneiden von Datenpaketen, Portscanner, Man-in-the Middle (ARP-,DNS-,DHCP-Spoofing,...)

$\Rightarrow$ gegenseitiges Achten auf Privatsphäre

Die heutigen Themen

1. Begriffe und Allgemeines zur IT-Sicherheit
   - Passwörter und worauf dabei zu achten ist
2. Wie funktioniert Kommunikation via Email?
   - der Weg der Email
   - "automatisches Sicherheit"?
3. GNU Privacy Guard
   - Was ist das?
   - Wie funktioniert das?
   - Integrität und Authentizität
   - Praxis: Thunderbird+Enigmail und GnuPG
4. (sicheres) Verteilen der öffentlichen Schlüssel
   - Attribute und Eigenschaften von Schlüsseln
   - Web of Trust – vertrauen über mehrer Stufen
   - Schlüsselserver

Übersicht

Definitionen

Daten physisches Phänomen (Anordnung von Bits)

Information richtige Interpretation von Daten

Metadaten beschreibende Daten;
teils zur richtigen Interpretation/Verarbeitung von Daten
(z.B: Empfänger) nötig

Hashfunktion Einwegfunktion, die aus Daten einen eindeutigen
Hash(wert) erzeugt.

Verfügbarkeit Zugriff auf die Information ist jederzeit möglich

Definitionen

Integrität keine (unerlaubte) **Modifikation** der **Daten**

Authentizität Die **Daten** stammen von der richtigen Person

Abstreitbarkeit **Authentizität** ist nicht Nachweisbar

Vertraulichkeit Nur beteiligte Personen kennen die **Information** der **Daten**

Beobachtbarkeit **Daten**zugriff kann bemerkt werden

Anonymität **Beobachtbar**, aber kein Wissen über die Identität

“Naturgesetze” des Cyperspaces

Automatisierbarkeit Daten sind leicht erhebbar und schnell verarbeitbar

räumliche Entgrenzung Lokalität ist nich von Bedeutung

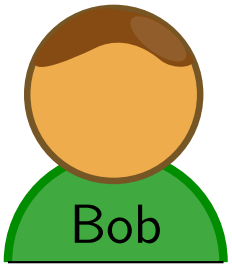
Kopierbarkeit Daten lassen sich kopieren.
Unterscheidbarkeit von Original und Kopie nicht möglich

Komplexität Programme haben unüberschaubare Funktionalität

$\Rightarrow$ (absichtliche und unabsichtliche) “Zusatzfunktionen” können Sicherheitslücken sein

Personen

versucht (geheime) Informationen an Bob zu senden



wartet als rechtmäßiger Emfänger auf die Informationen von Alice

versucht sich unerlaubt Zugang zu den Nachrichten zwischen Alice und Bob zu verschaffen

- Verbreitetes Mittel der Authentifikation/Zugangskontrolle
- wird (sollte) als Hashwert abgespeichert
- meist schwächstes Glied in der Authentifikationskette

Angriffsformen

Bruteforce probieren aller Möglichkeiten
Beispiel `oclHashcat`: ca. $2 * 10^9$ SHA512/s

Dictionary probieren einer Liste von Wörtern
Beispiel `rockyou.txt`: 14.344.391 Wörter (134MB)

Mask Ein fester Wortstamm wird um eine Zeichenklasse erweiterter:
Beispiel "asdf" und 3 Zahlen
`asdf000, asdf001, ..., asdf998, asdf999`

natürlich sind auch Kombinationen möglich

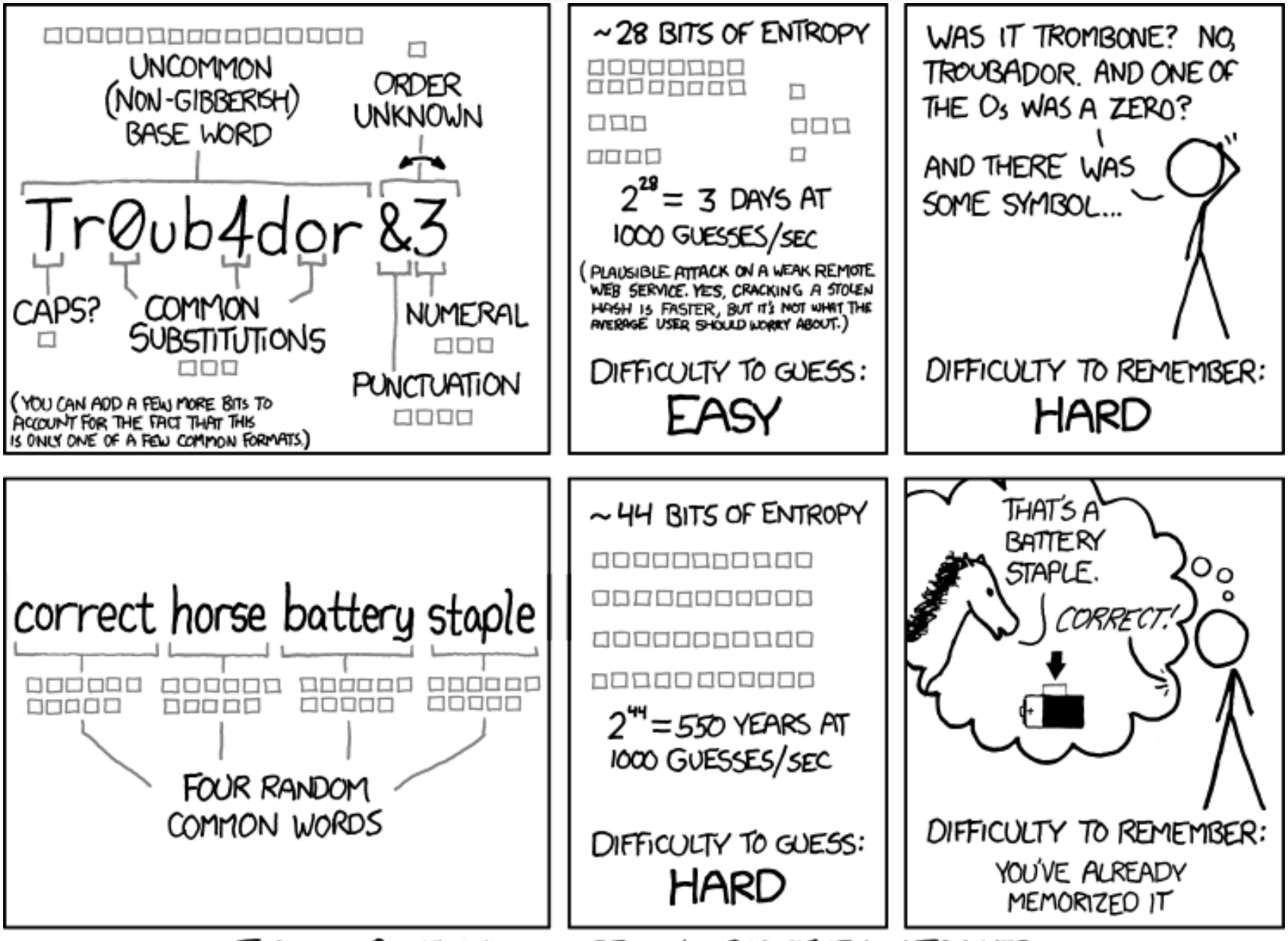
Tips für sichere Passwörter

Bruteforce
- lange Wörter erhöhen den Aufwand exponentiell
- breite Zeichenpallete verwenden
- Metadaten (Länge, Position von Buchstaben/Zeichen/Zahlen) helfen den Aufwand zu vermindern

Dictionary
- Keine (nicht nur) Wörter aus Duden und anderen Lexikas
- Bereits kleine Abwandlungen helfen

Mask
- Nur sinnvoll einsetzbar falls Metadaten verfügbar

$\Rightarrow$ "Die Mischung machts"
- keine Metadaten über Passwörter aufschreiben
- Wiederholungen spiegeln sich in Hashes meist nicht wieder


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Übersicht

Email – was ist das?

bekannt sollte wohl jeder schonmal gehört haben ;)

Email – was ist das?

bekannt sollte wohl jeder schonmal gehört haben ;)

verbreitet laut Wikipedia “meistegenutzter Dienst des Internets”

Email – was ist das?

bekannt sollte wohl jeder schonmal gehört haben ;)

verbreitet laut Wikipedia “meistegenutzter Dienst des Internets”

universell ist an kein Datenformat gebunden

Email – was ist das?

bekannt sollte wohl jeder schonmal gehört haben ;)

verbreitet laut Wikipedia “meistegenutzter Dienst des Internets”

universell ist an kein Datenformat gebunden

Postkarte häufiger: Vergleich mit Brief
es gibt aber keinen Briefumschlag!
$\Rightarrow$ Zusteller kann mitlesen!

Email – was ist das?

bekannt sollte wohl jeder schonmal gehört haben ;)

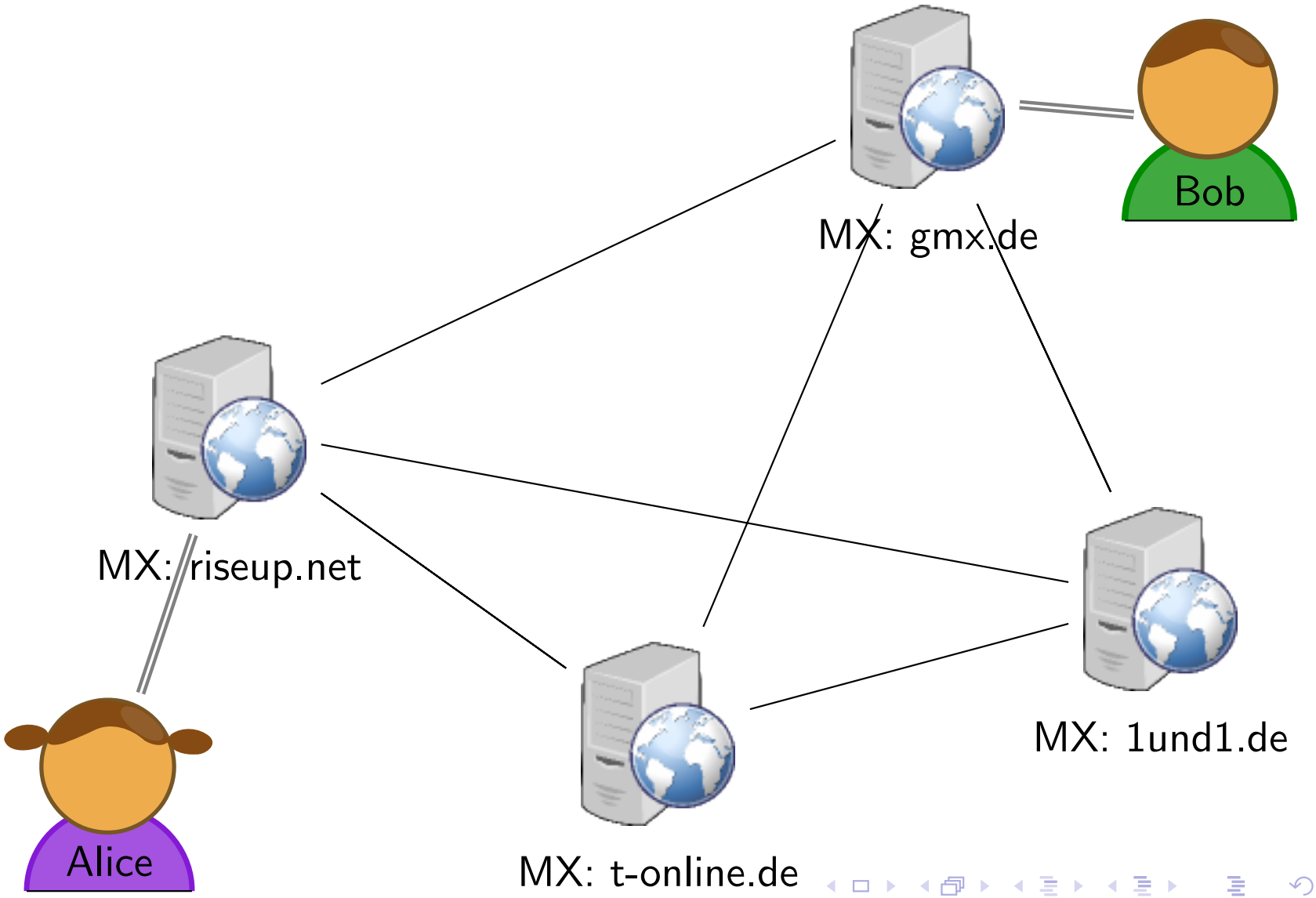
verbreitet laut Wikipedia “meistegenutzter Dienst des Internets”

universell ist an kein Datenformat gebunden

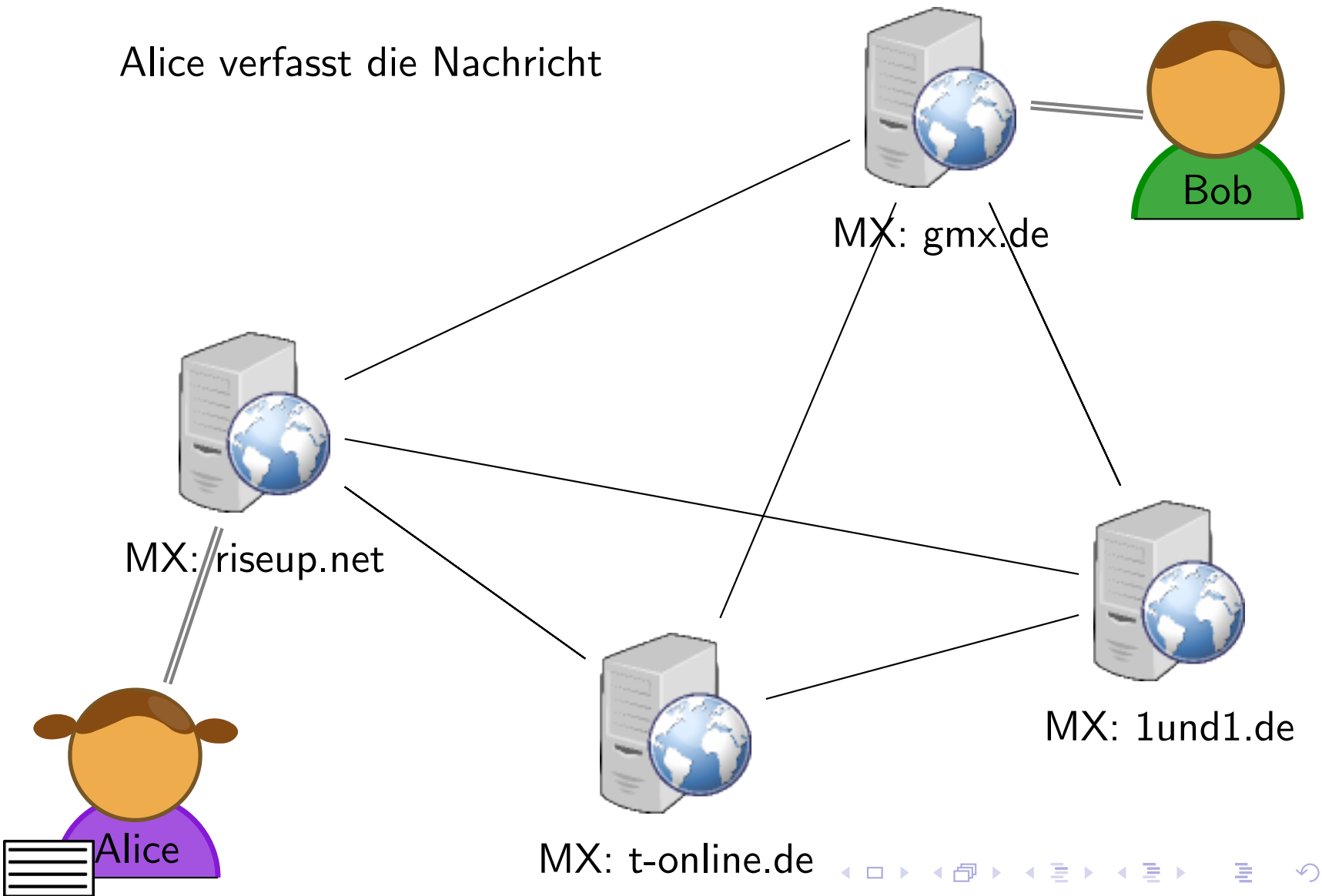
Postkarte häufiger: Vergleich mit Brief
es gibt aber keinen Briefumschlag!
$\Rightarrow$ Zusteller kann mitlesen!

(okay, Postkarten haben keinen Anhang. . .)

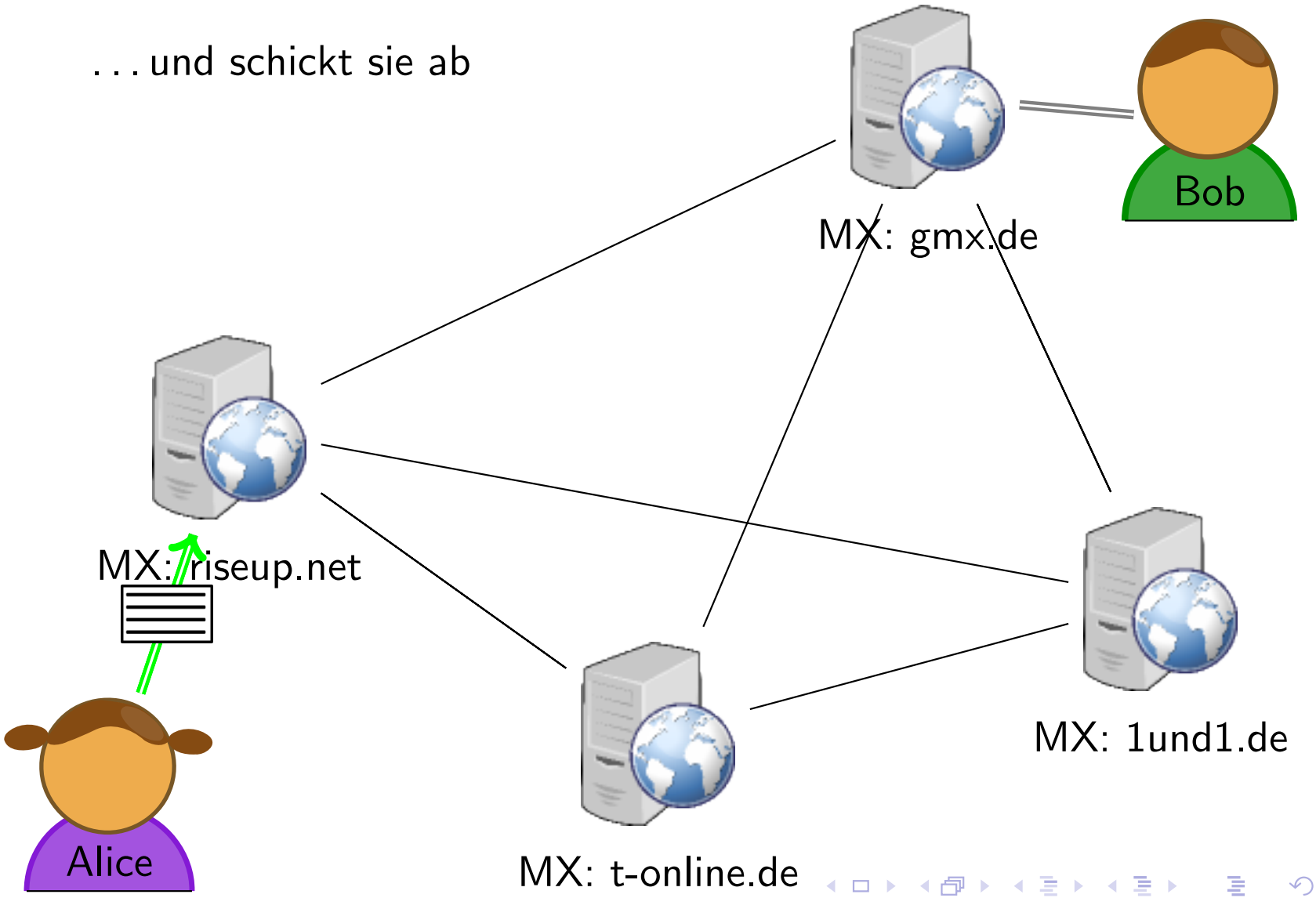
Stationen und Bedrohungen



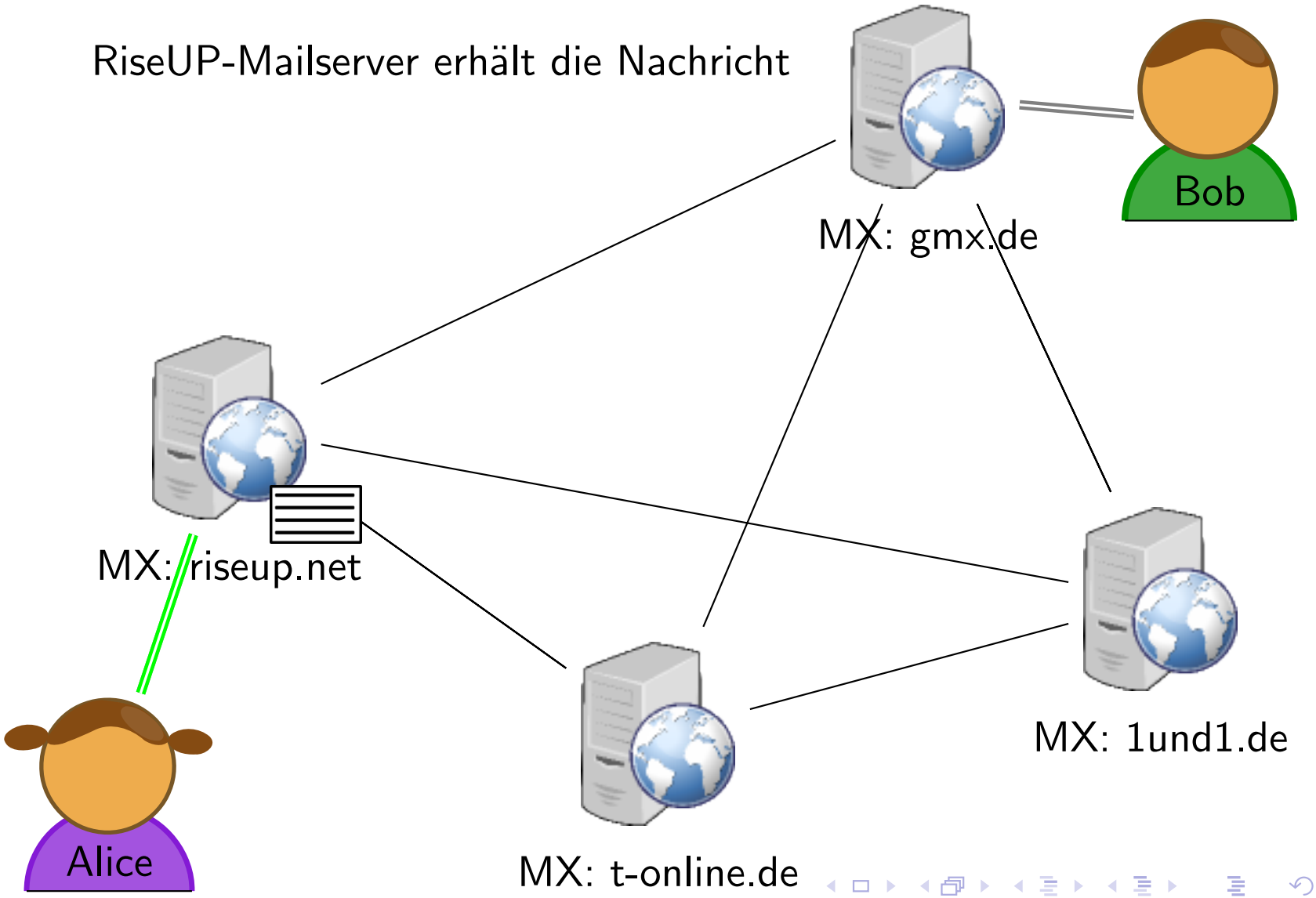
Stationen und Bedrohungen



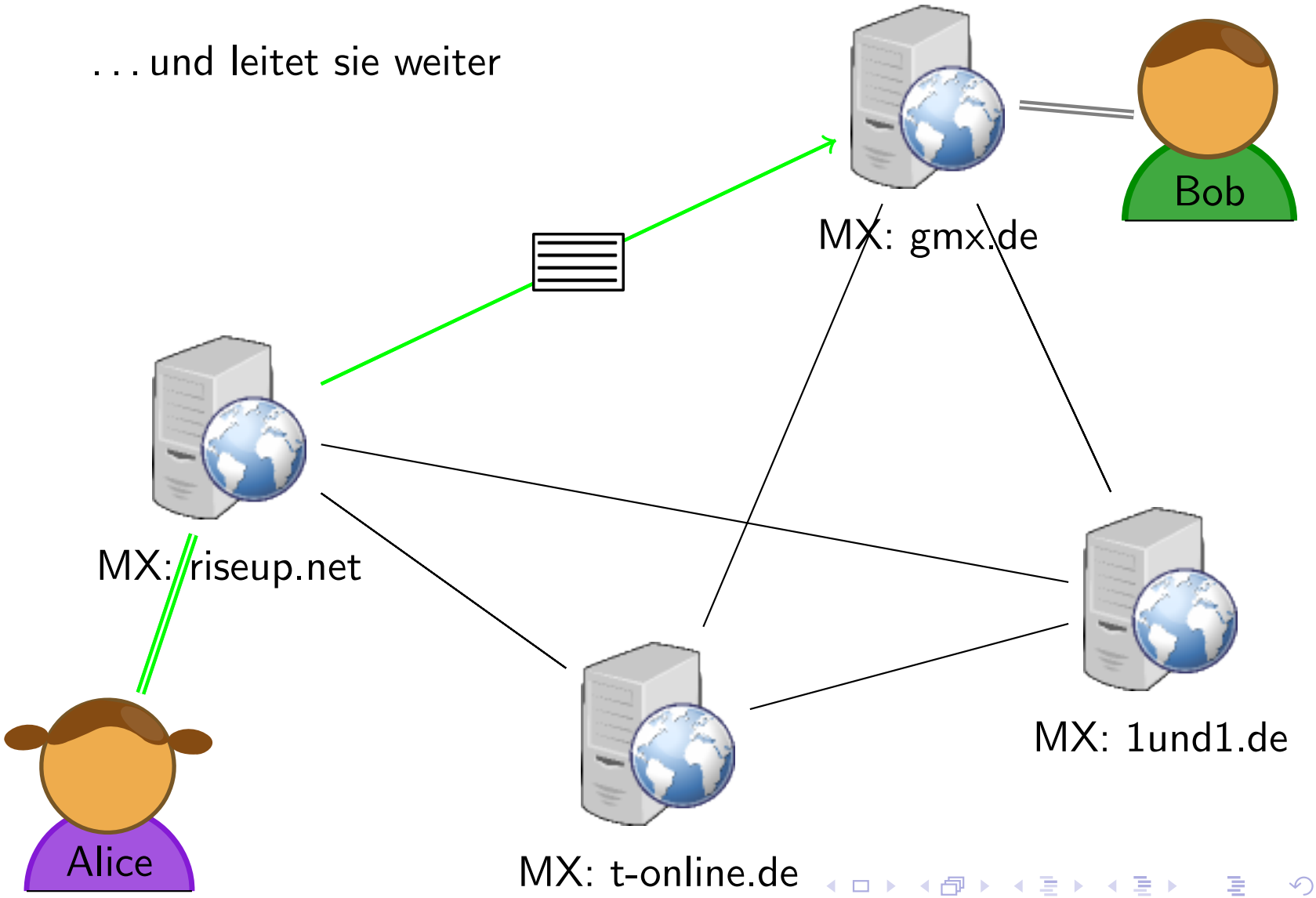
Stationen und Bedrohungen



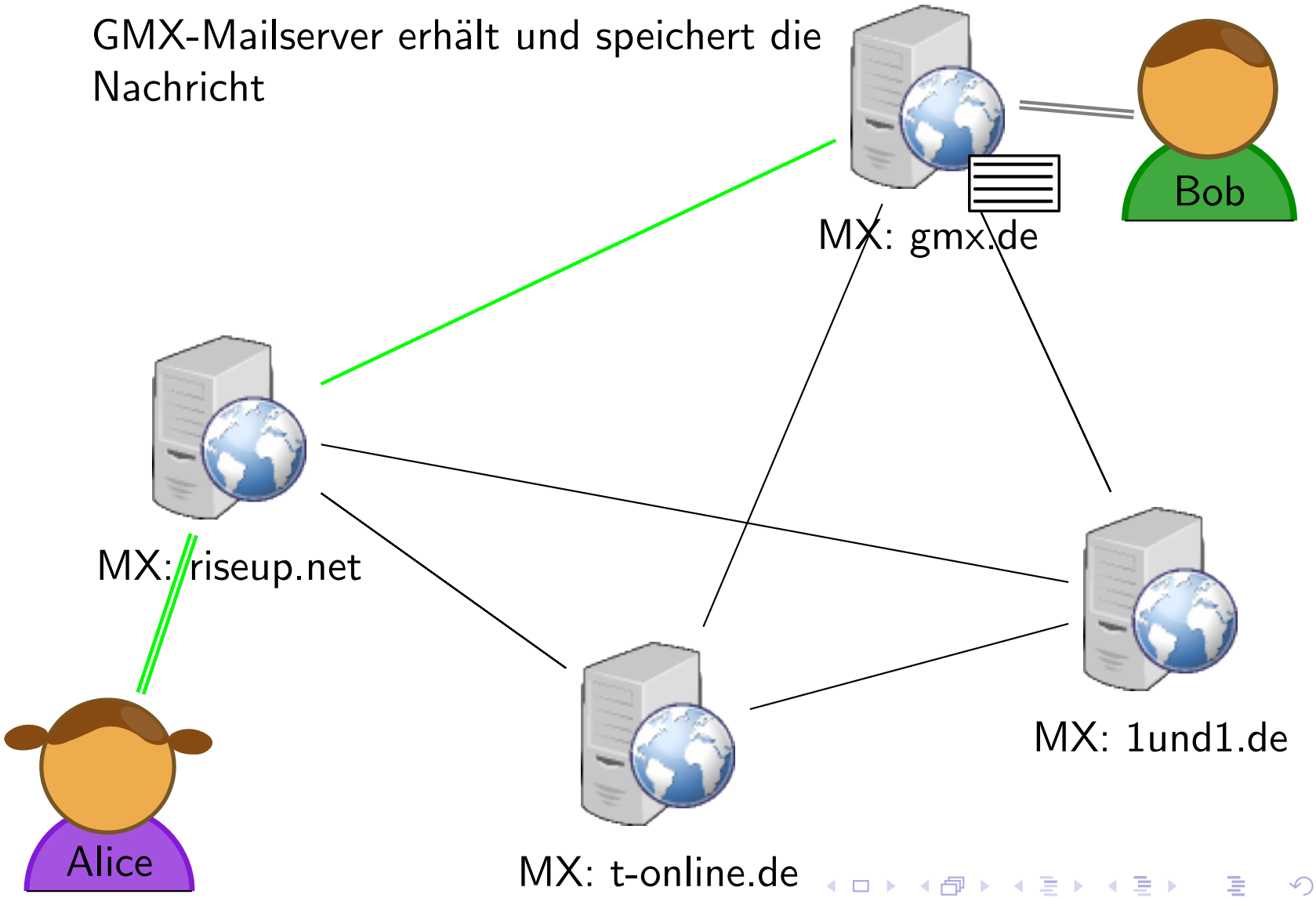
Stationen und Bedrohungen



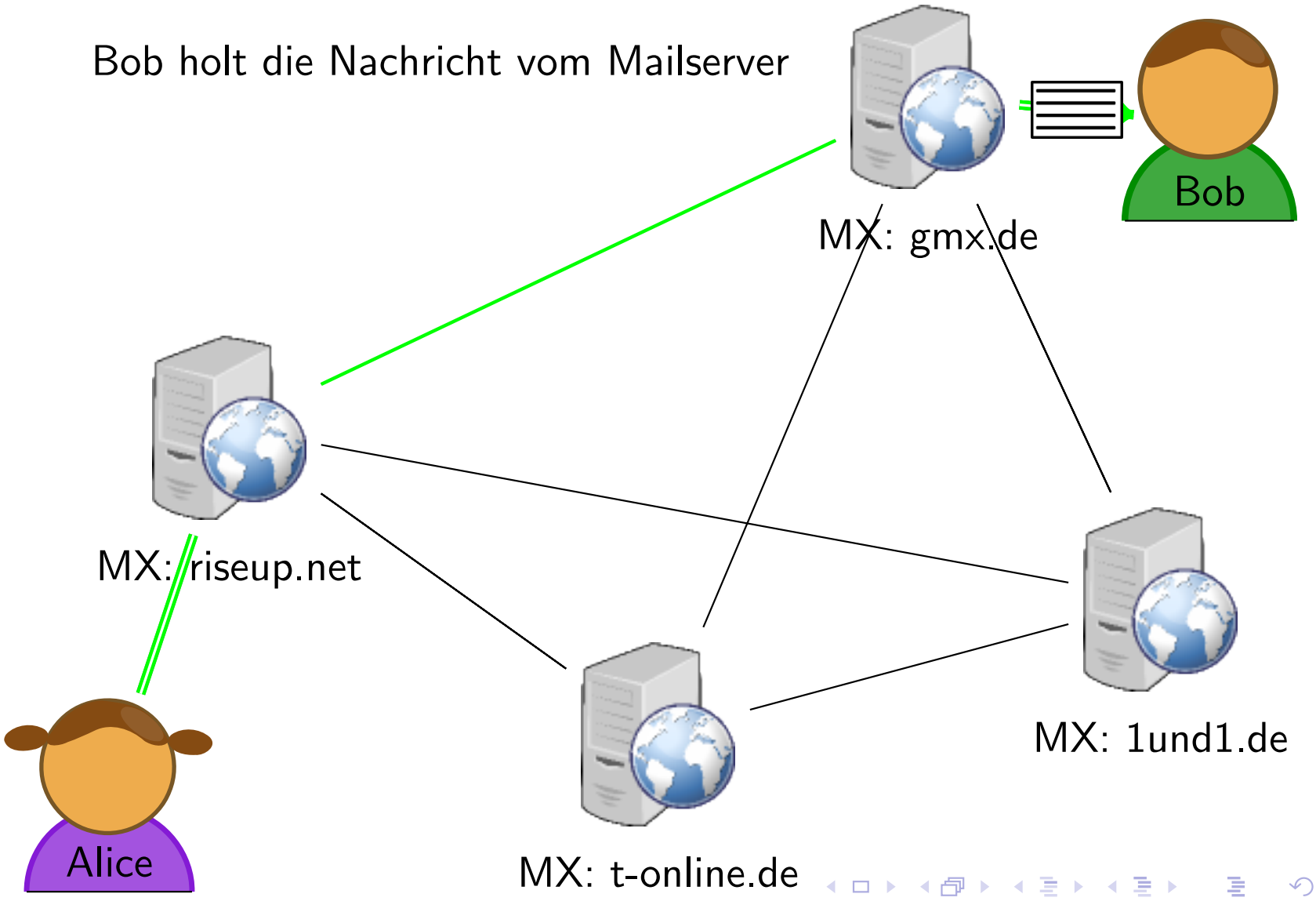
Stationen und Bedrohungen



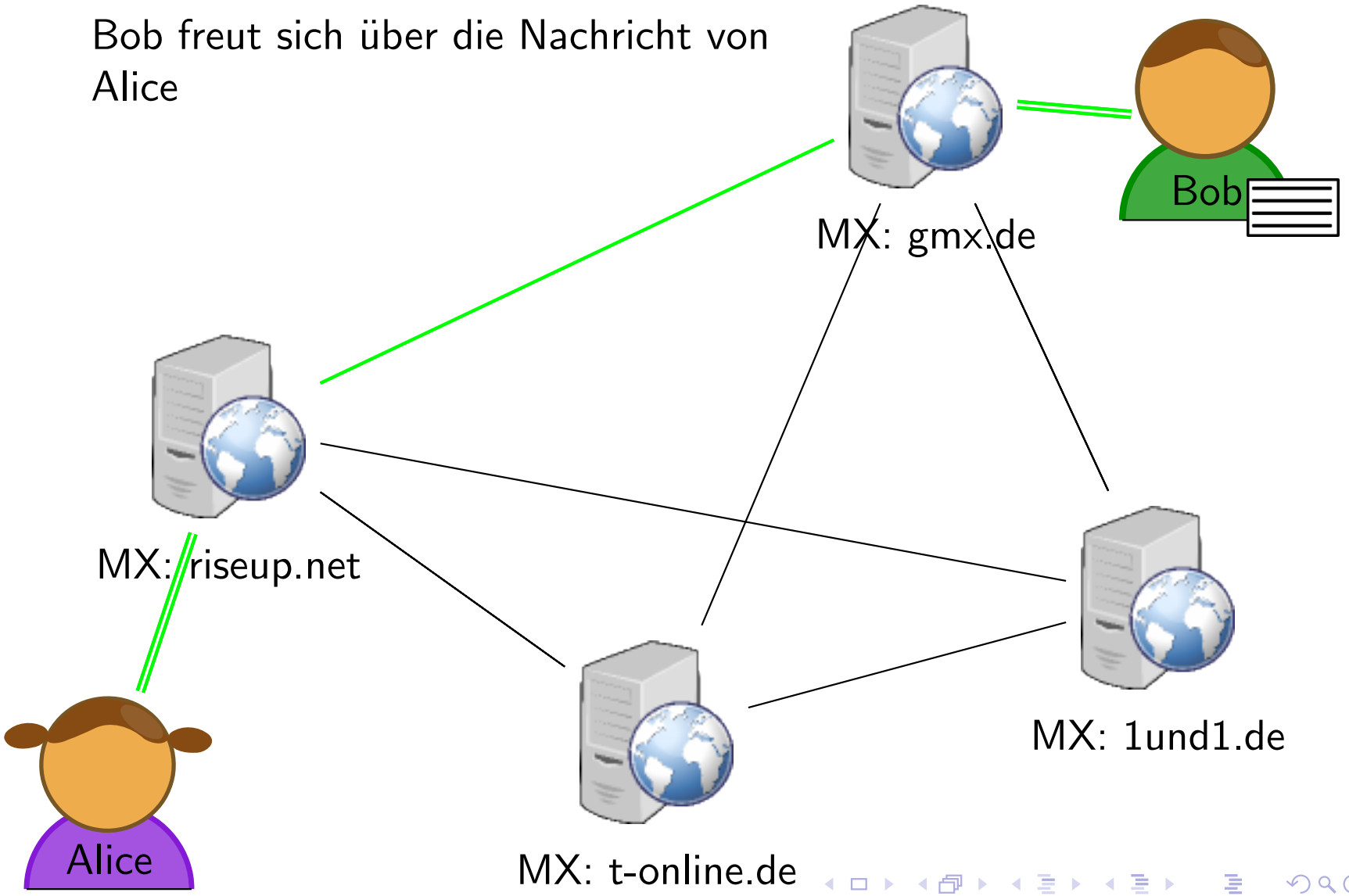
Stationen und Bedrohungen



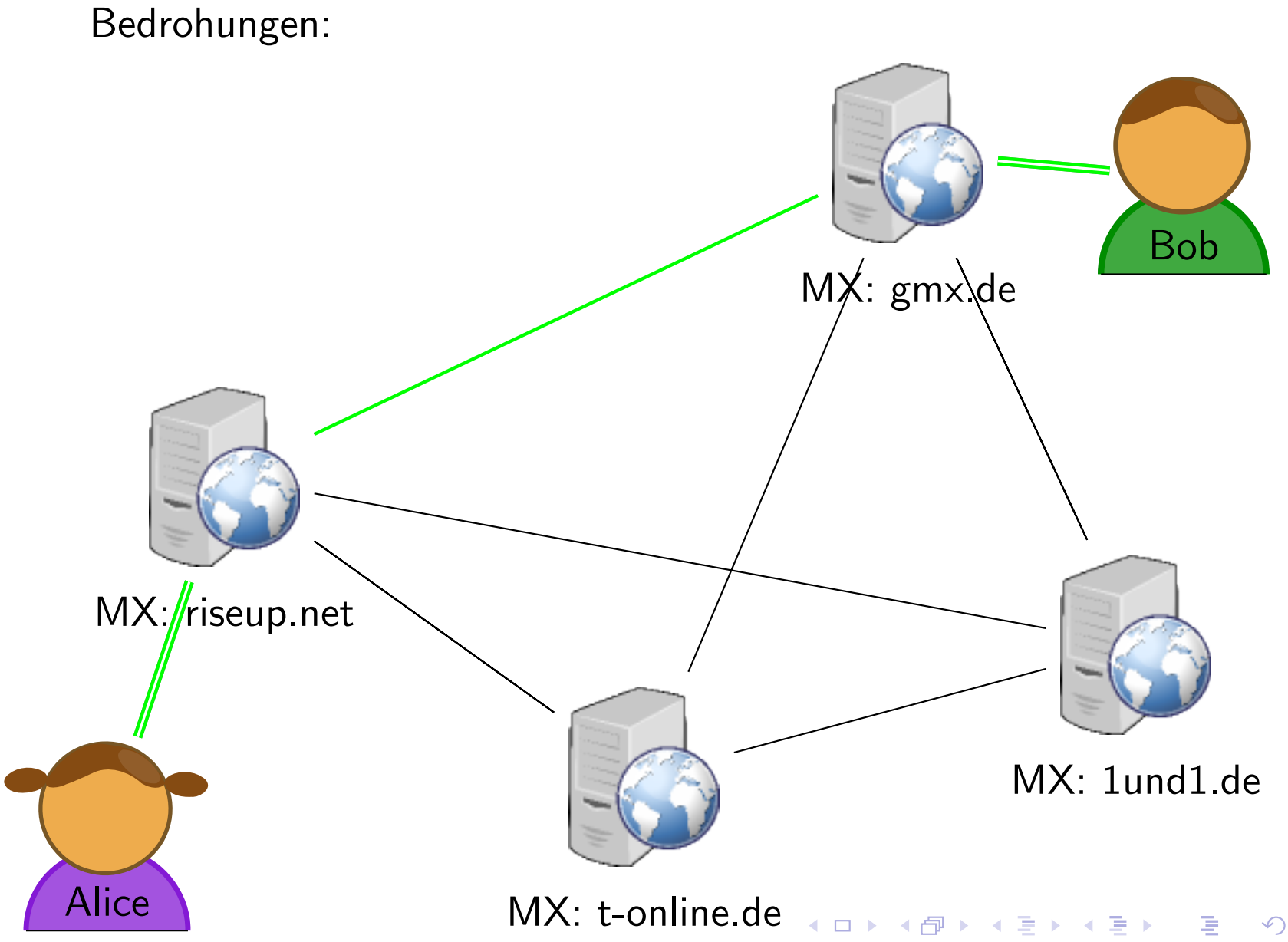
Stationen und Bedrohungen



Stationen und Bedrohungen



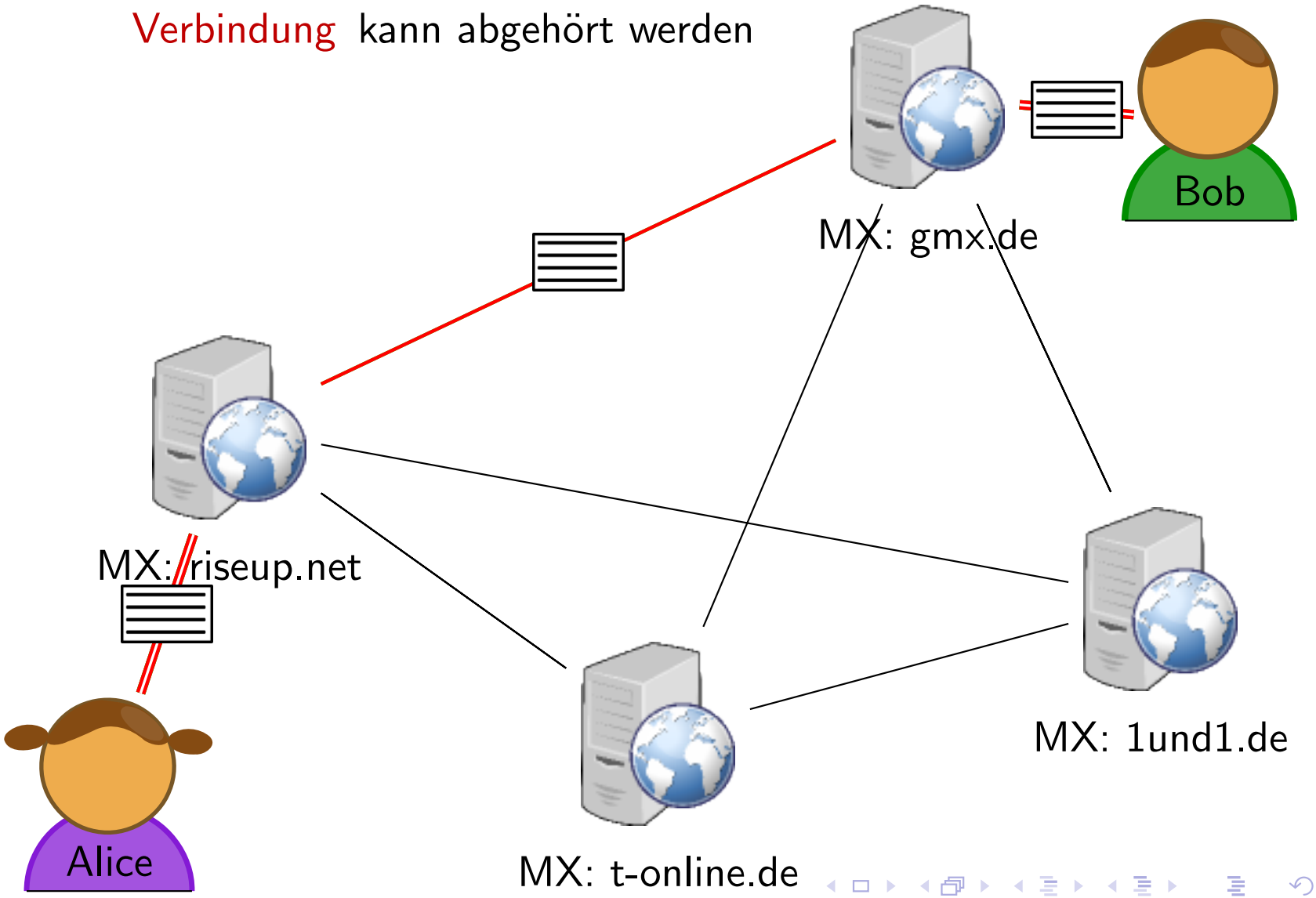
Stationen und Bedrohungen



Stationen und Bedrohungen

Bedrohungen:

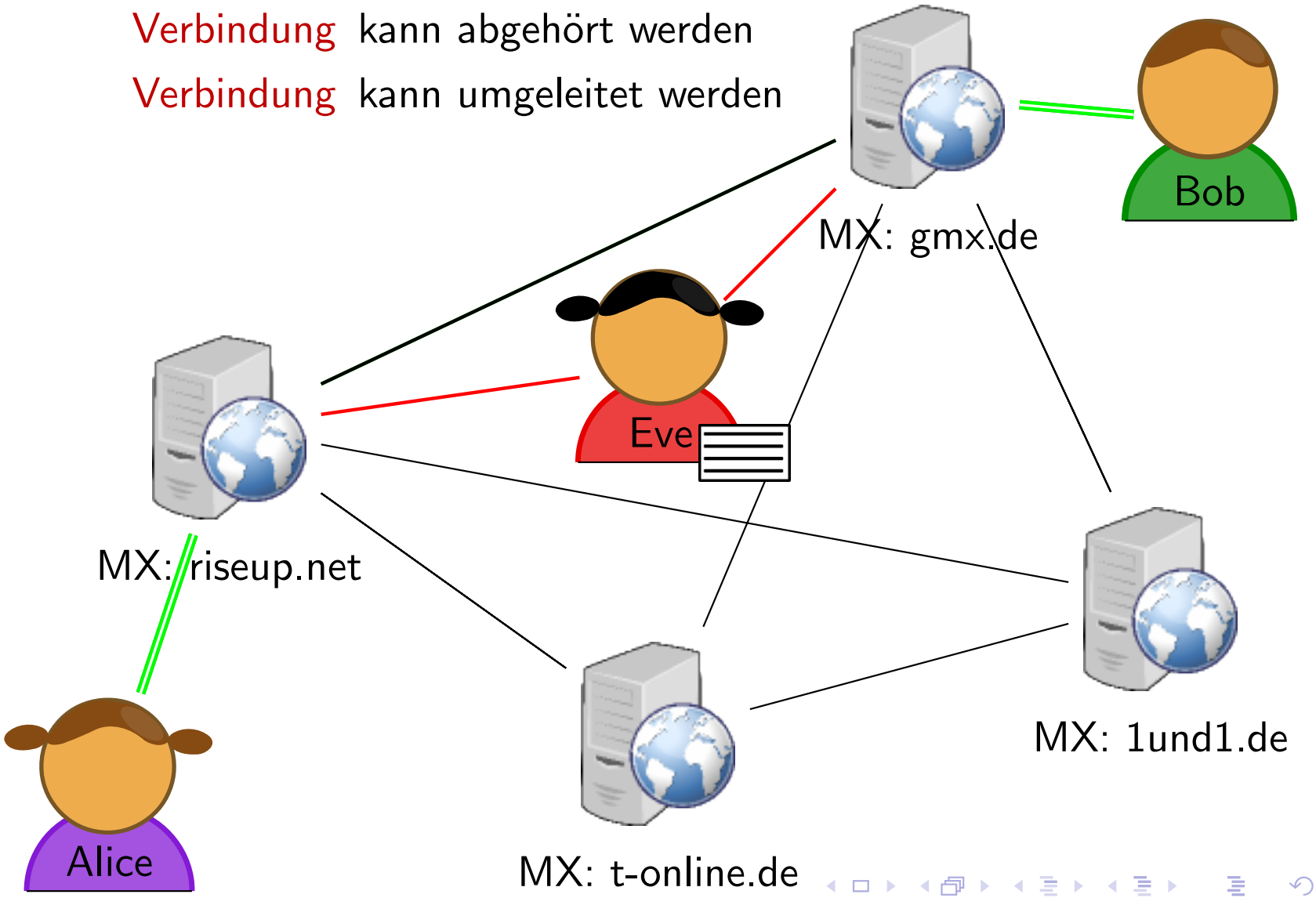
Verbindung kann abgehört werden



Stationen und Bedrohungen

Bedrohungen:

- Verbindung kann abgehört werden
- Verbindung kann umgeleitet werden



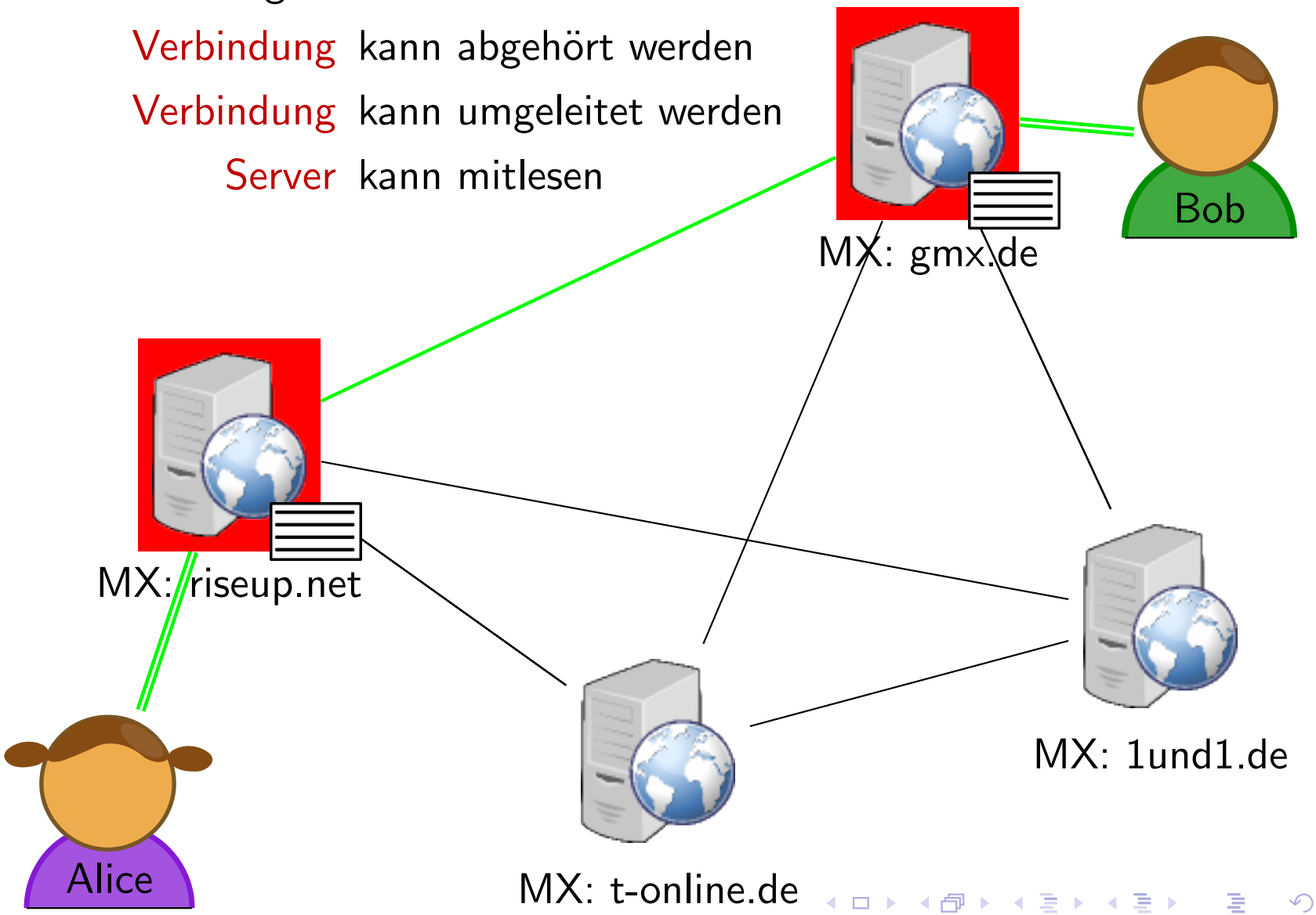
Stationen und Bedrohungen

Bedrohungen:

Verbindung kann abgehört werden

Verbindung kann umgeleitet werden

Server kann mitlesen



Versuche, automatische Sicherheit zu erlangen

Versuche, automatische Sicherheit zu erlangen

De-Mail gesetzlich geregeltes pendant zur Briefpost

- Anbieter brauchen staatliche Zertifizierung
- Verschlüsselung des Transportweges
  $\Rightarrow$ Klartext auf Mailservern
- "Sicher per Gesetz"

Versuche, automatische Sicherheit zu erlangen

De-Mail gesetzlich geregeltes pendant zur Briefpost

- Anbieter brauchen staatliche Zertifizierung
- Verschlüsselung des Transportweges
  $\Rightarrow$ Klartext auf Mailservern
- "Sicher per Gesetz"

Email made in Germany Zusammenschluss deutscher Email-Provider

- Antwort auf "NSA-Skandal"
- Verschlüsselung des Transportweges
  $\Rightarrow$ Klartext auf Mailservern
- Zwar nur wenige Anbieter im "Kreis der Auserwählten", dennoch kein Zertifikatpinning
  $\Rightarrow$ Man-in-the-Middle Attacken möglich

Versuche, automatische Sicherheit zu erlangen

De-Mail gesetzlich geregeltes pendant zur Briefpost

- Anbieter brauchen staatliche Zertifizierung
- Verschlüsselung des Transportweges
  $\Rightarrow$ Klartext auf Mailservern
- "Sicher per Gesetz"

Email made in Germany Zusammenschluss deutscher Email-Provider

- Antwort auf "NSA-Skandal"
- Verschlüsselung des Transportweges
  $\Rightarrow$ Klartext auf Mailservern
- Zwar nur wenige Anbieter im "Kreis der Auserwählten", dennoch kein Zertifikatpinning
  $\Rightarrow$ Man-in-the-Middle Attacken möglich

wieso nicht früher? Die Technologie gibt es bereits seit knapp 10 Jahren

Versuche, automatische Sicherheit zu erlangen

De-Mail gesetzlich geregeltes pendant zur Briefpost

- Anbieter brauchen staatliche Zertifizierung
- Verschlüsselung des Transportweges
  $\Rightarrow$ Klartext auf Mailservern
- "Sicher per Gesetz"

Email made in Germany Zusammenschluss deutscher Email-Provider

- Antwort auf "NSA-Skandal"
- Verschlüsselung des Transportweges
  $\Rightarrow$ Klartext auf Mailservern
- Zwar nur wenige Anbieter im "Kreis der Auserwählten", dennoch kein Zertifikatpinning
  $\Rightarrow$ Man-in-the-Middle Attacken möglich

wieso nicht früher? Die Technologie gibt es bereits seit knapp 10 Jahren

Automatisierbar? Ohne Eingriff des Nutzers ist keine Sicherheit möglich!

Übersicht

1. Begriffe und Allgemeines zur IT-Sicherheit
2. Wie funktioniert Kommunikation via Email?
3. GNU Privacy Guard
   - Was ist das?
   - Wie funktioniert das?
   - Integrität und Authentizität
   - Praxis: Thunderbird+Enigmail und GnuPG
4. (sicheres) Verteilen der öffentlichen Schlüssel

GNU Privacy Guard

Open-Source Im Gegensatz zu dem Original ("Pretty Good Privacy"; 1991 Phil Zimmermann) quelloffen und kostenlos

Standardkonform Zwar fehlen patentierte Algorithmen, dennoch wird der OpenPGP Standard von GPG komplett unterstützt

Cross-Platform Version für Windows, Mac OS X und Linux stehen auf der Projekthomepage (https://gnupg.org) zum Download bereit

Integration Es gibt Erweiterungen für die verbreiteten Mailclients (später am Beispiel von Thunderbird+Enigmail)

Verbreitet viele Projekte vertrauen zur Integritätsprüfung auf Signaturverfahren

Etwas Theorie zu Beginn

Asymetrisch Jeder besitzt einen **privaten** (🔑_{priv}) und einen **öffentlichen** (🔑_{pub}) Schlüssel

Etwas Theorie zu Beginn

Asymetrisch Jeder besitzt einen **privaten** (🔑_{priv}) und einen **öffentlichen** (🔑_{pub}) Schlüssel

- Mathematisch lässt sich theoretisch von einen auf den anderen Key schliessen

Etwas Theorie zu Beginn

Asymetrisch Jeder besitzt einen **privaten** (🔑_{priv}) und einen **öffentlichen** (🔑_{pub}) Schlüssel

- Mathematisch lässt sich theoretisch von einen auf den anderen Key schliessen
- Praktisch jedoch zu hoher Rechenaufwand um tatsächlich eine Gefahr darzustellen

Etwas Theorie zu Beginn

Asymetrisch Jeder besitzt einen **privaten** (🔑_{priv}) und einen **öffentlichen** (🔑_{pub}) Schlüssel

- Mathematisch lässt sich theoretisch von einen auf den anderen Key schliessen
- Praktisch jedoch zu hoher Rechenaufwand um tatsächlich eine Gefahr darzustellen
- Es gilt:

$$Decrypt_{\text{🔑}_{priv}}\left(Encrypt_{\text{🔑}_{pub}}(X)\right) = X$$

Etwas Theorie zu Beginn

Asymetrisch Jeder besitzt einen **privaten** (🔑_{priv}) und einen **öffentlichen** (🔑_{pub}) Schlüssel

- Mathematisch lässt sich theoretisch von einen auf den anderen Key schliessen
- Praktisch jedoch zu hoher Rechenaufwand um tatsächlich eine Gefahr darzustellen
- Es gilt:

$$Decrypt_{\text{🔑}_{priv}}\left(Encrypt_{\text{🔑}_{pub}}(X)\right) = X$$

$\Rightarrow$ Weitergabe des 🔑_{pub} möglich

Etwas Theorie zu Beginn

Asymetrisch Jeder besitzt einen **privaten** (🔑_{priv}) und einen **öffentlichen** (🔑_{pub}) Schlüssel

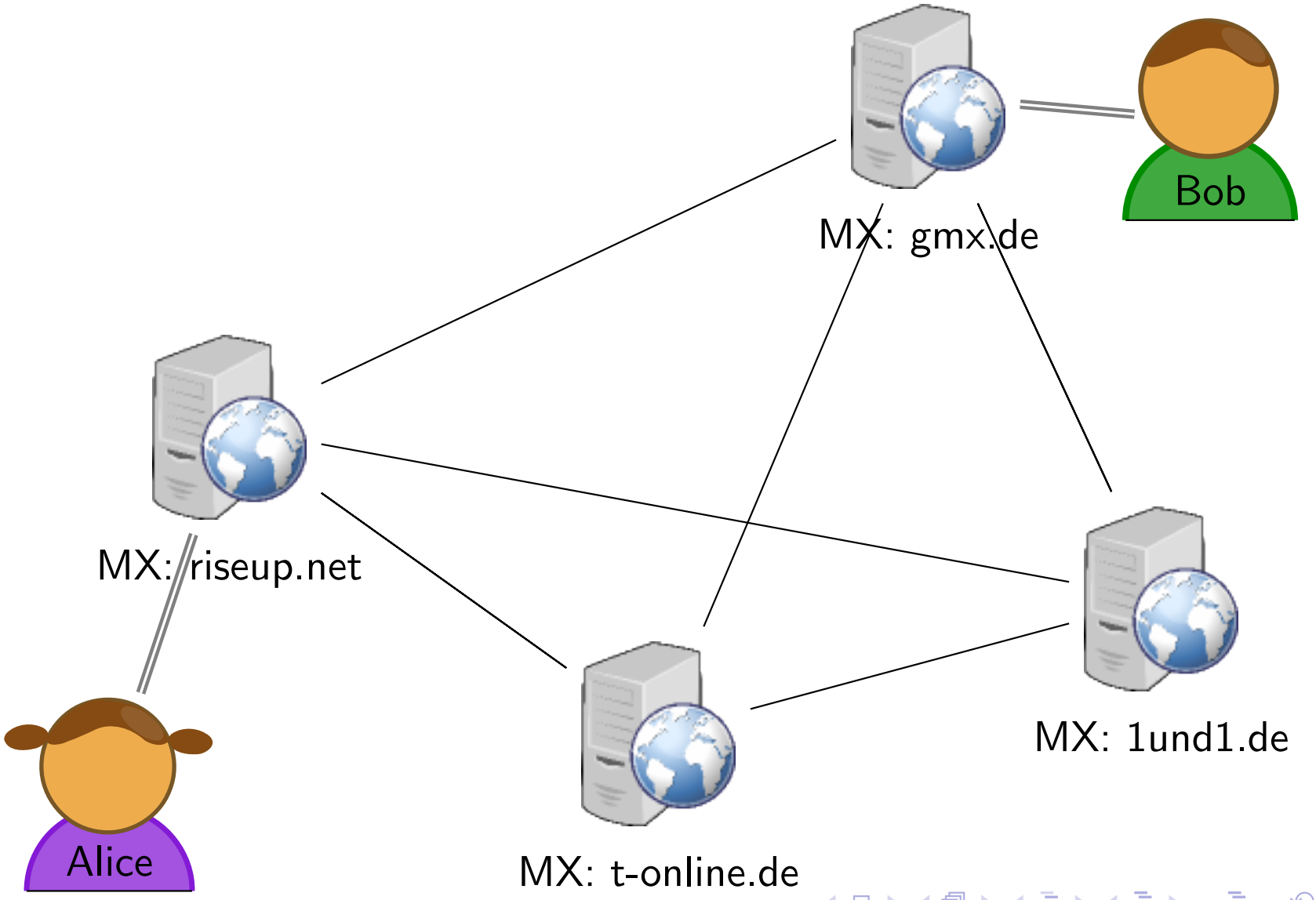
- Mathematisch lässt sich theoretisch von einen auf den anderen Key schliessen
- Praktisch jedoch zu hoher Rechenaufwand um tatsächlich eine Gefahr darzustellen
- Es gilt:

$$Decrypt_{\text{🔑}_{priv}}\left(Encrypt_{\text{🔑}_{pub}}(X)\right) = X$$

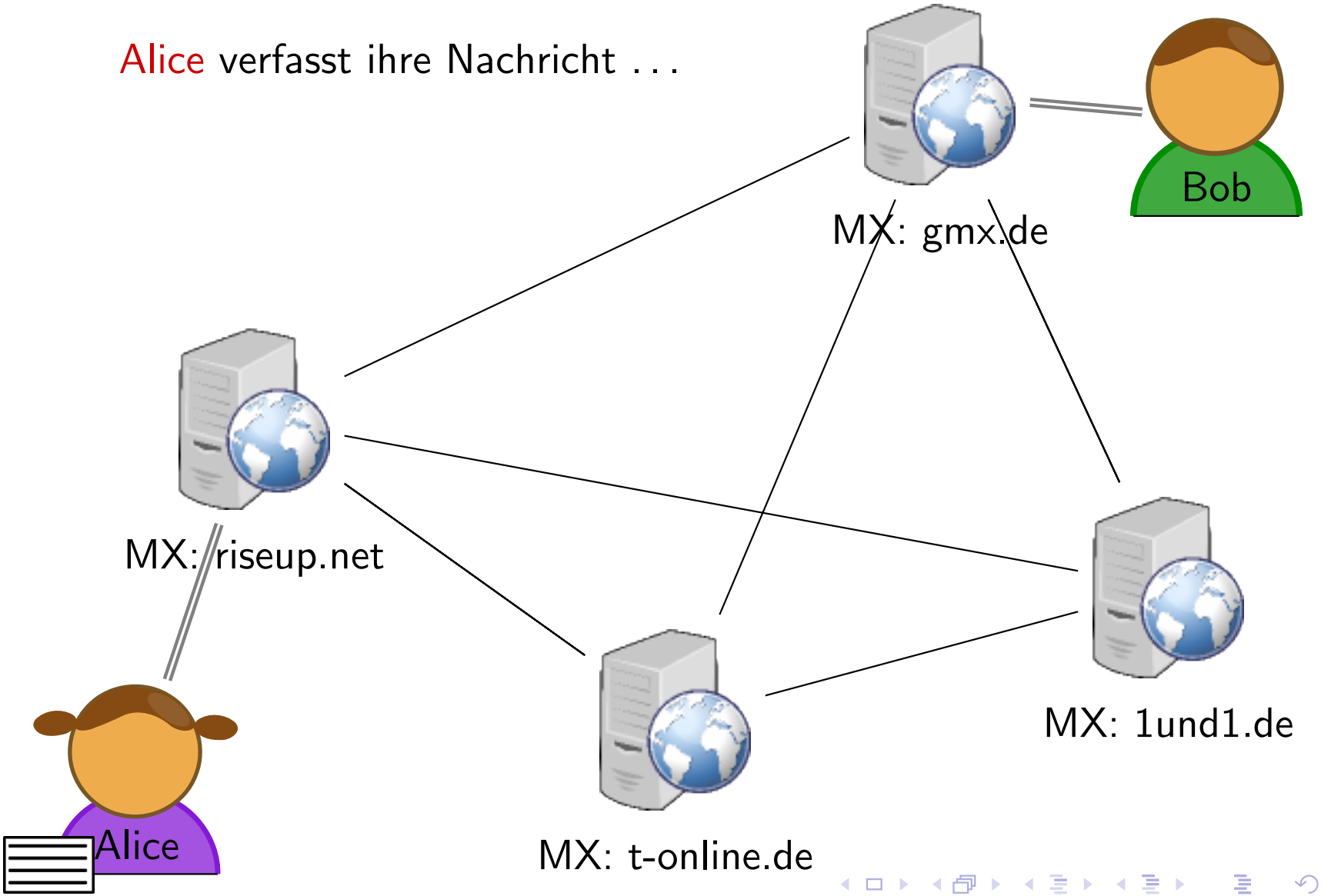
$\Rightarrow$ Weitergabe des 🔑_{pub} möglich

Identifikation jeder Schlüssel hat (mindestens) eine Mailadress hinterlegt
sicherer: Identifikation über **Hashwert** (=Fingerprint)

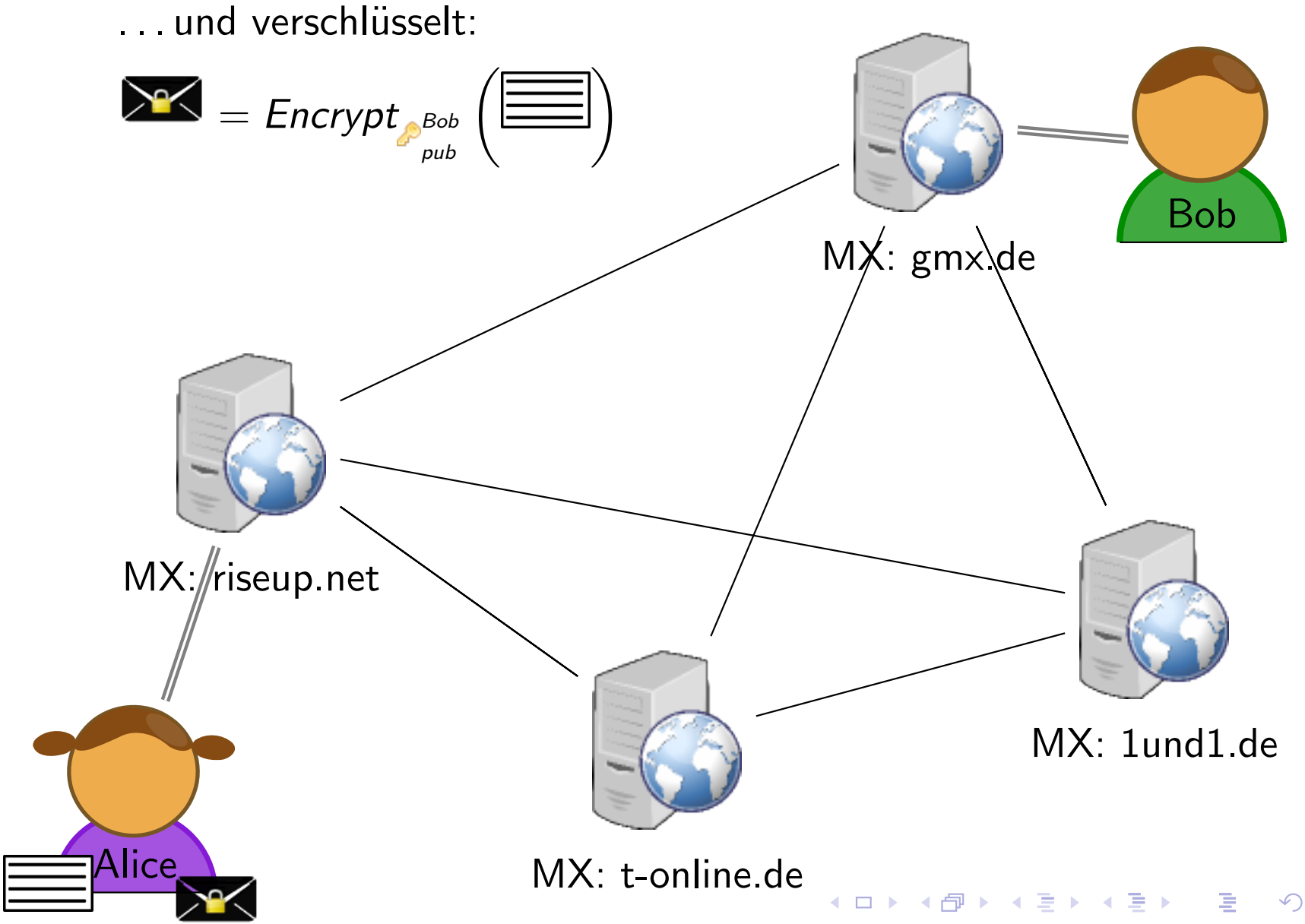
(zusätzliche) Schritte beim Emailverkehr



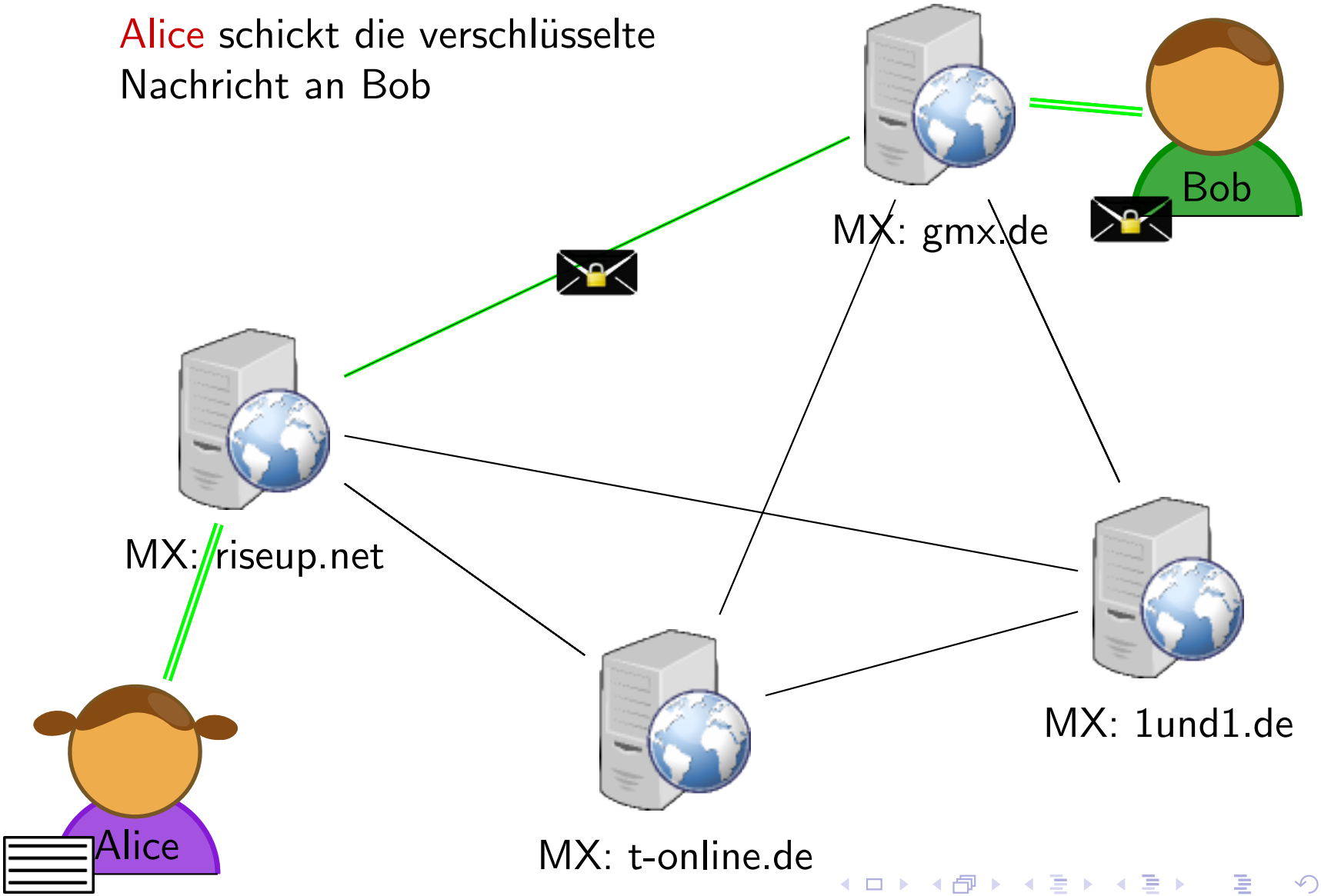
(zusätzliche) Schritte beim Emailverkehr



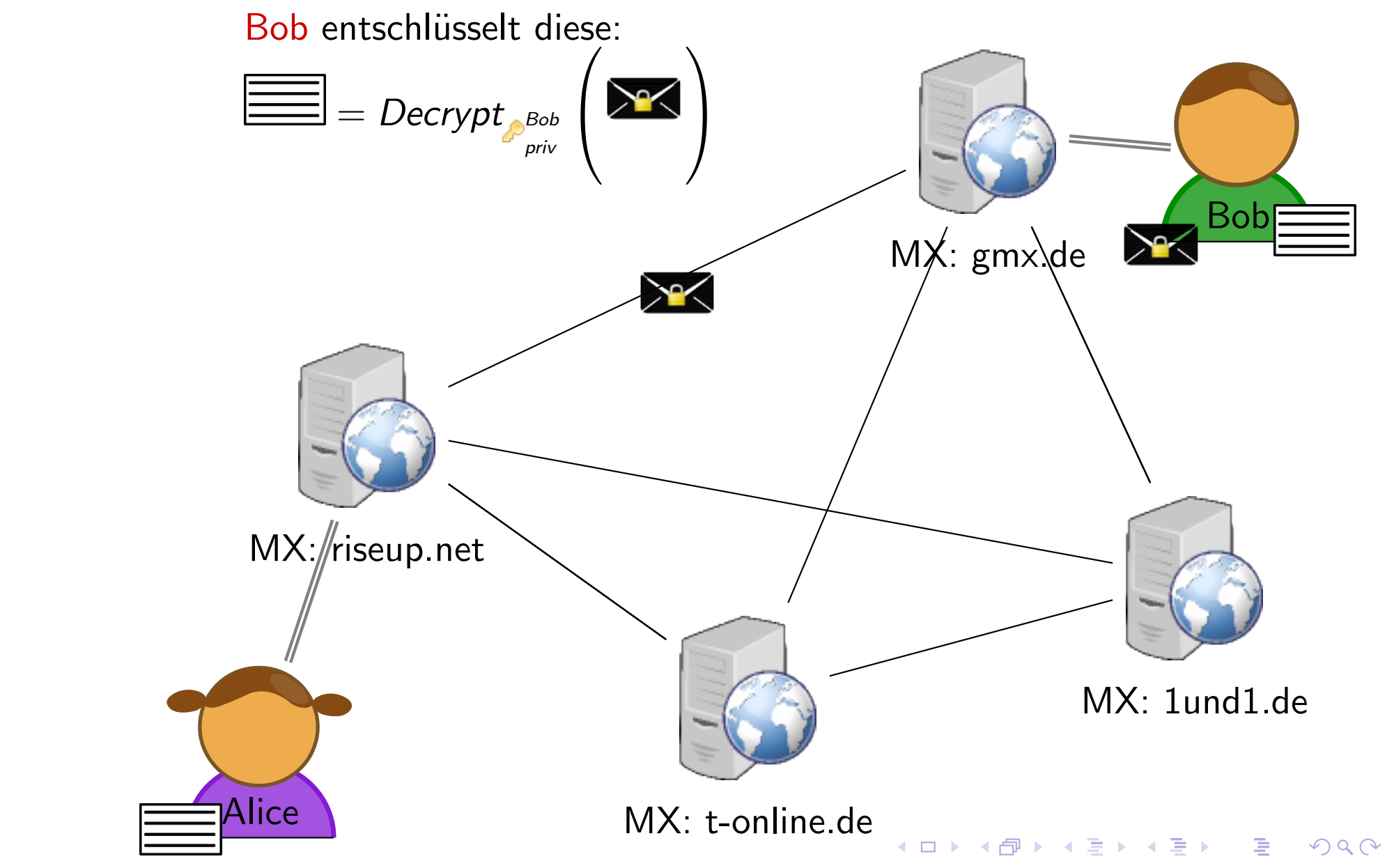
(zusätzliche) Schritte beim Emailverkehr



(zusätzliche) Schritte beim Emailverkehr



(zusätzliche) Schritte beim Emailverkehr

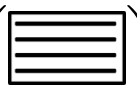


Nochmal auf einen Blick

Alice möchte  an Bob schicken:

Alice holt sich Bob_{pub}

Alice verschlüsselt mit Bob_{pub}

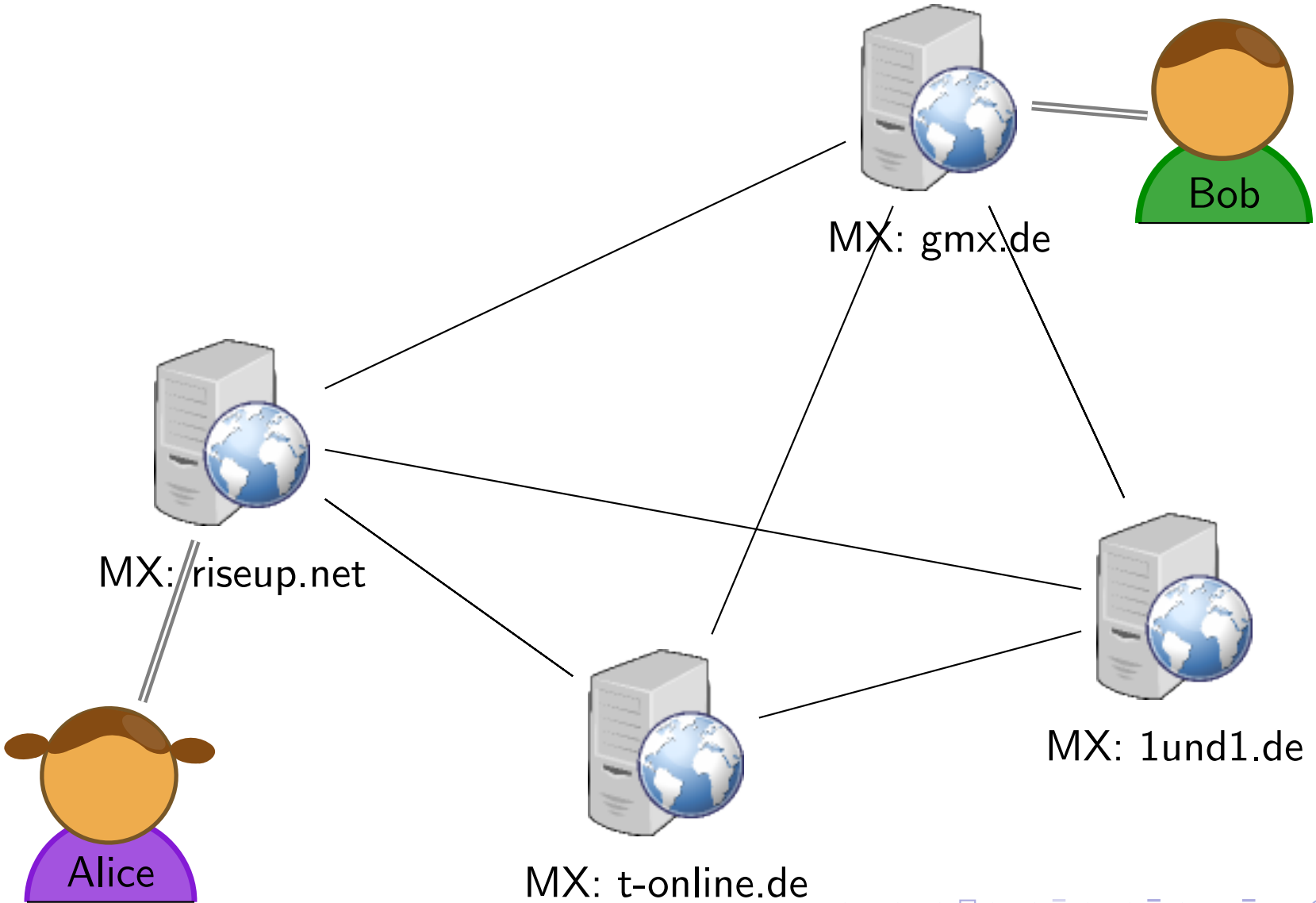
 $= Encrypt_{\text{Bob}_{pub}}$ 

Alice schickt  and Bob

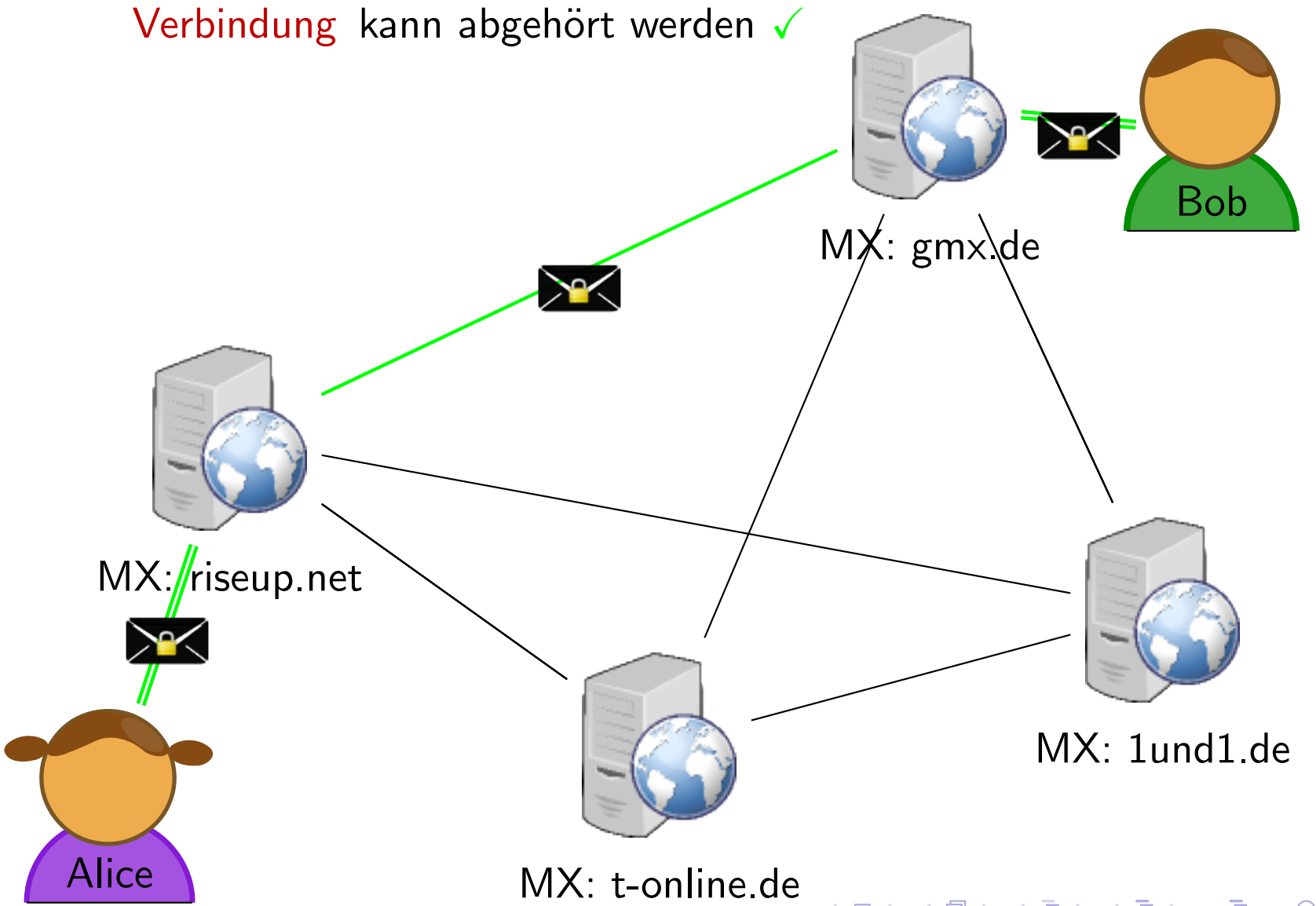
Bob empfängt und entschlüsselt

 $= Decrypt_{\text{Bob}_{priv}}$ 

Bedrohungen gelöst?



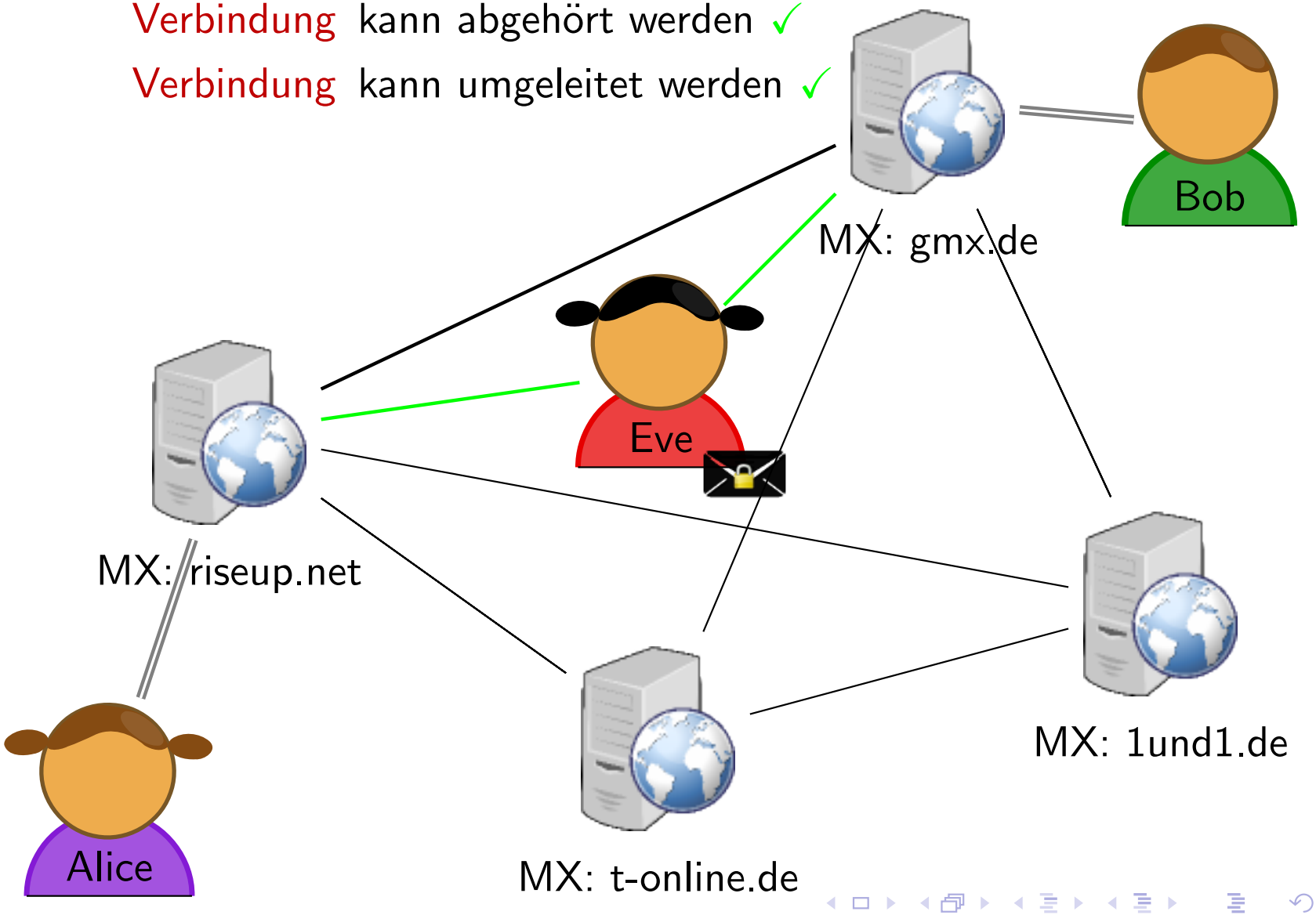
Bedrohungen gelöst?



Bedrohungen gelöst?

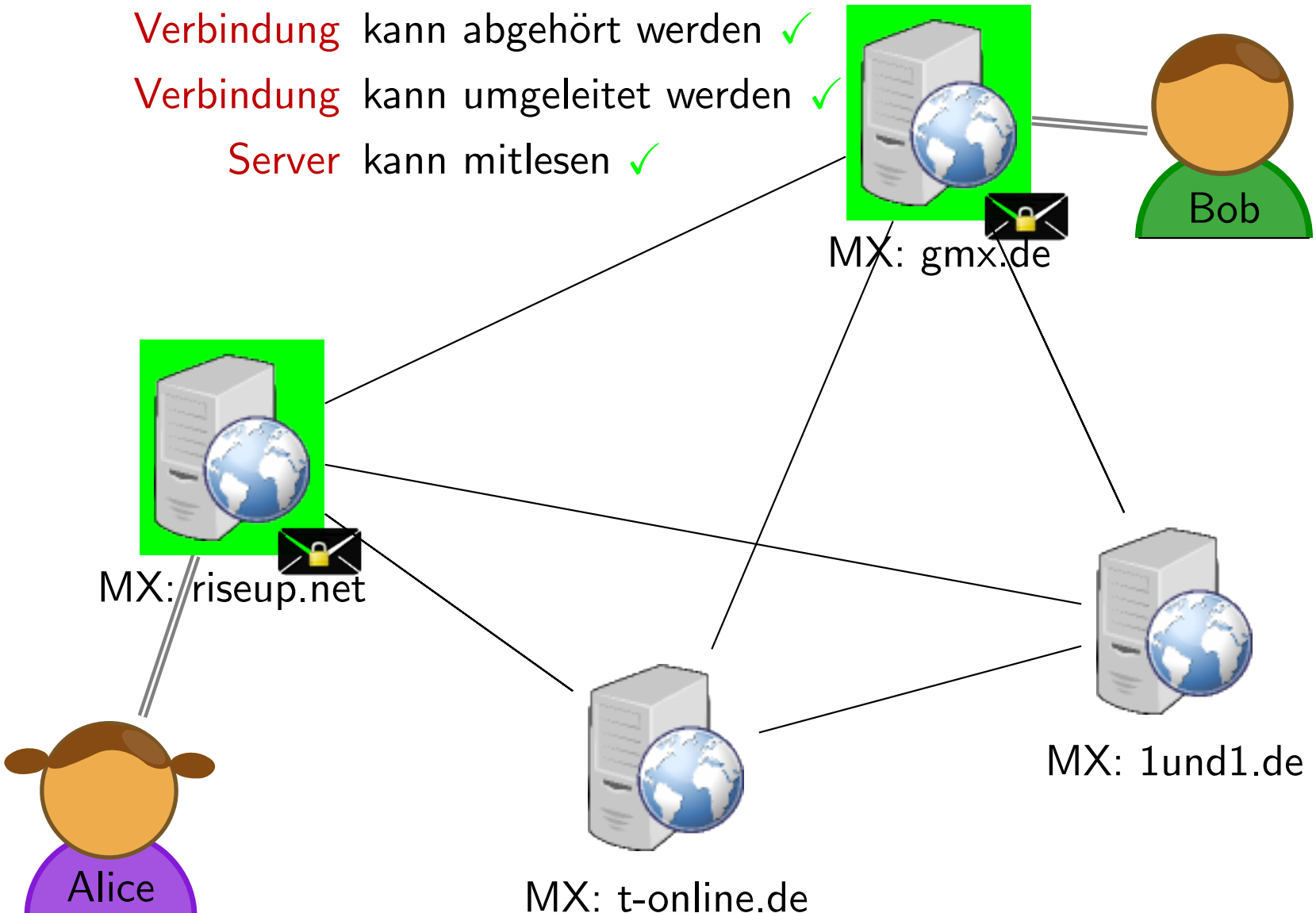
Verbindung kann abgehört werden ✓

Verbindung kann umgeleitet werden ✓



Bedrohungen gelöst?

Verbindung kann abgehört werden ✓
Verbindung kann umgeleitet werden ✓
Server kann mitlesen ✓



Was haben wir erreicht?

Vertraulichkeit Nur wer 🔑_{priv} kennt, kann die Nachricht entschlüsseln

Was haben wir erreicht?

Vertraulichkeit Nur wer 🔑_{priv} kennt, kann die Nachricht entschlüsseln

ABER Es gibt noch ein paar Probleme:

Was haben wir erreicht?

Vertraulichkeit Nur wer 🔑_{priv} kennt, kann die Nachricht entschlüsseln

ABER Es gibt noch ein paar Probleme:

Metadaten lediglich der Emailinhalt wird verschlüsselt
Betreff bleibt im Klartext erhalten
$\Rightarrow$ sind bei Emails unabdingbar...

Was haben wir erreicht?

Vertraulichkeit Nur wer 🔑_{priv} kennt, kann die Nachricht entschlüsseln

ABER Es gibt noch ein paar Probleme:

Metadaten lediglich der Emailinhalt wird verschlüsselt
Betreff bleibt im Klartext erhalten
$\Rightarrow$ sind bei Emails unabdingbar...

Schlüssel gehört der Schlüssel wirklich Bob?

Was haben wir erreicht?

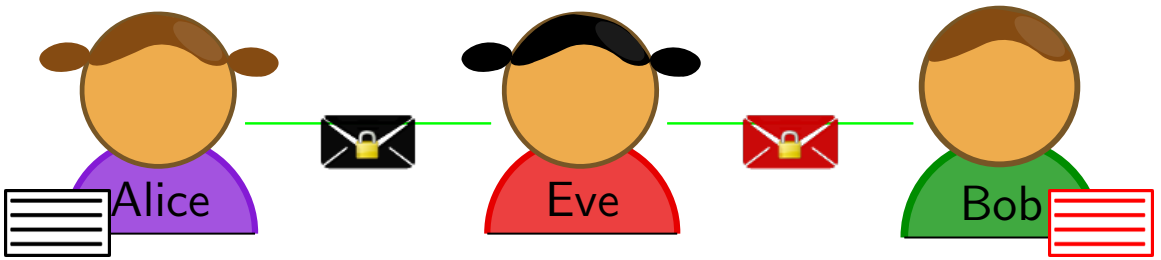
Vertraulichkeit Nur wer 🔑_{priv} kennt, kann die Nachricht entschlüsseln

ABER Es gibt noch ein paar Probleme:

Metadaten lediglich der Emailinhalt wird verschlüsselt
Betreff bleibt im Klartext erhalten
$\Rightarrow$ sind bei Emails unabdingbar...

Schlüssel gehört der Schlüssel wirklich Bob?

Integrität Wurde die Nachricht unterwegs manipuliert?



Was haben wir erreicht?

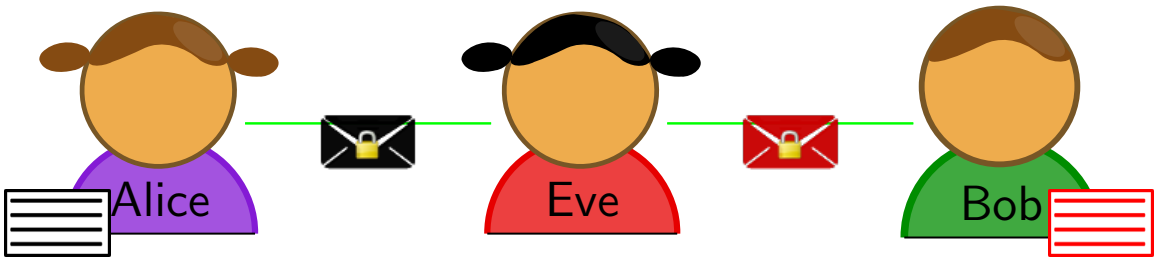
Vertraulichkeit Nur wer 🔑_{priv} kennt, kann die Nachricht entschlüsseln

ABER Es gibt noch ein paar Probleme:

Metadaten lediglich der Emailinhalt wird verschlüsselt
Betreff bleibt im Klartext erhalten
$\Rightarrow$ sind bei Emails unabdingbar...

Schlüssel gehört der Schlüssel wirklich Bob?

Integrität Wurde die Nachricht unterwegs manipuliert?



Authentizität Kommt die Nachricht tatsächlich von der Person, von der wir vermuten?

Herstellen von Integrität und Authentizität

Problem Integrität und Authentizität werden verletzt:

- $\overset{Bob}{pub}$ muss(sollte) frei zugänglich sein
  $\Rightarrow$ jeder kann an Bob verschlüsseln
- Nur wer $\overset{Bob}{priv}$ hat, kann Inhalt lesen

Herstellen von Integrität und Authentizität

Problem Integrität und Authentizität werden verletzt:

- $\overset{Bob}{\underset{pub}{\text{🔑}}}$ muss(sollte) frei zugänglich sein
  $\Rightarrow$ jeder kann an Bob verschlüsseln
- Nur wer $\overset{Bob}{\underset{priv}{\text{🔑}}}$ hat, kann Inhalt lesen

Lösung Wir schicken eine "Unterschrift" mit

Herstellen von Integrität und Authentizität

Problem Integrität und Authentizität werden verletzt:

- $\mathit{Bob}_{\mathit{pub}}$ muss(sollte) frei zugänglich sein
  $\Rightarrow$ jeder kann an Bob verschlüsseln
- Nur wer $\mathit{Bob}_{\mathit{priv}}$ hat, kann Inhalt lesen

Lösung Wir schicken eine "Unterschrift" mit

Idee Reihenfolge der Schlüssel lässt sich vertauschen

$$\mathit{Decrypt}_{\mathit{Bob}_{\mathit{pub}}}\left(\mathit{Encrypt}_{\mathit{Bob}_{\mathit{priv}}}(X)\right) = X$$

Herstellen von Integrität und Authentizität

Problem Integrität und Authentizität werden verletzt:

- $\mathit{Bob}_{\mathit{pub}}$ muss(sollte) frei zugänglich sein
  $\Rightarrow$ jeder kann an Bob verschlüsseln
- Nur wer $\mathit{Bob}_{\mathit{priv}}$ hat, kann Inhalt lesen

Lösung Wir schicken eine "Unterschrift" mit

Idee Reihenfolge der Schlüssel lässt sich vertauschen

$$\mathit{Decrypt}_{\mathit{Bob}_{\mathit{pub}}}\left(\mathit{Encrypt}_{\mathit{Bob}_{\mathit{priv}}}(X)\right) = X$$

$$\text{Unterschrift} = \mathit{Encrypt}_{\mathit{Bob}_{\mathit{priv}}}(\mathit{Hash}(X))$$

Integrität und Authentizität gesichert!

Überprüfen Bob erhält also Nachricht und Unterschrift und kann Integrität und Authentizität prüfen:

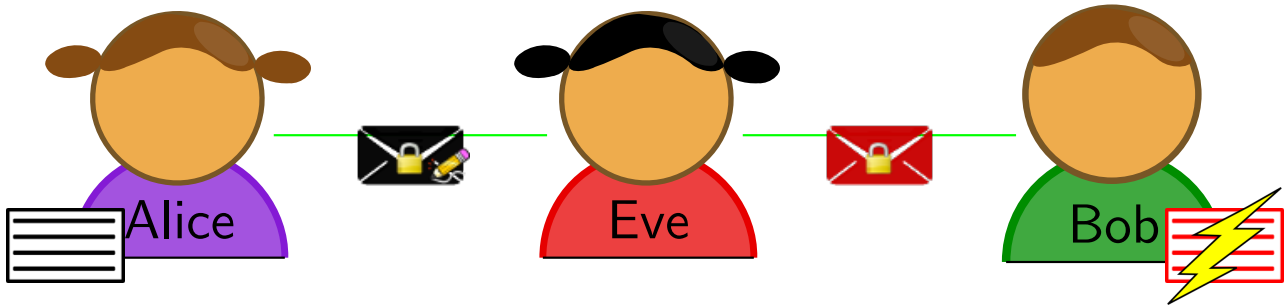
$$Decrypt_{\underset{pub}{Alice}}(Unterschrift) \stackrel{!}{=} Hash\left(Decrypt_{\underset{priv}{Bob}}(Nachricht)\right)$$

Integrität und Authentizität gesichert!

Überprüfen Bob erhält also Nachricht und Unterschrift und kann Integrität und Authentizität prüfen:

$$Decrypt_{\underset{pub}{Alice}}(Unterschrift) \stackrel{!}{=} Hash\left(Decrypt_{\underset{priv}{Bob}}(Nachricht)\right)$$

ACHTUNG Eve kann natürlich Nachricht abfangen und ohne Unterschrift weitersenden



$\Rightarrow$ Unterschrift überprüfen!!

Genug Theorie – auf zur Praxis

GnuPG Paketverwaltung ;)

Gpg4win `https://www.gpg4win.org`

GPGTools `https://www.gpgtools.org/gpgsuite.html`

Thunderbird `https://www.mozilla.org/de/thunderbird/`

Enigmail `https://addons.mozilla.org/de/thunderbird/addon/enigmail/`

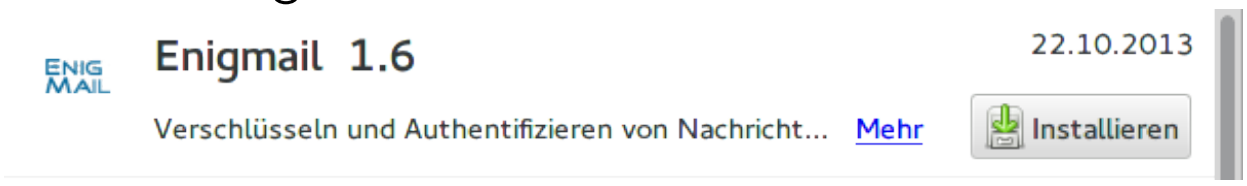
Vorgehensweise I

Nur grob – vor Ort direkt gezeigt

Installation von Thunderbird und GPG (je nach Betriebssystem verschieden)

Enigmail Thunderbird öffen

- ≡ > Add-Ons
- suche: "Enigmail" → Installieren



- Thunderbird neustarten

Einrichten OpenPGP-Assistent sollte sich automatisch öffnen

- Den Anweisungen des Assistenten folgen und nach eigen Bedürfnissen konfigurieren
- Bei Frage nach OpenPGP-Schlüssel abbrechen (erstellen selbst einen mit 4096Bit statt 2048Bit)

Vorgehensweise II

Nur grob – vor Ort direkt gezeigt

OpenPGP ≡ > OpenPGP > Schlüssel verwalten

- Erzeugen > Neues Schlüsselpaar...
- Maske nach eigenen Wünschen ausfüllen
- Reiter "Erweitert" > Schlüsselstärke: 4096
- Schlüsselpaar Erzeugen & warten...
- Wiederrufszertifikat abspeichern!
- Datei > "Schlüsselzwischenspeicher neu laden"

Senden auf Icons rechts unten achten

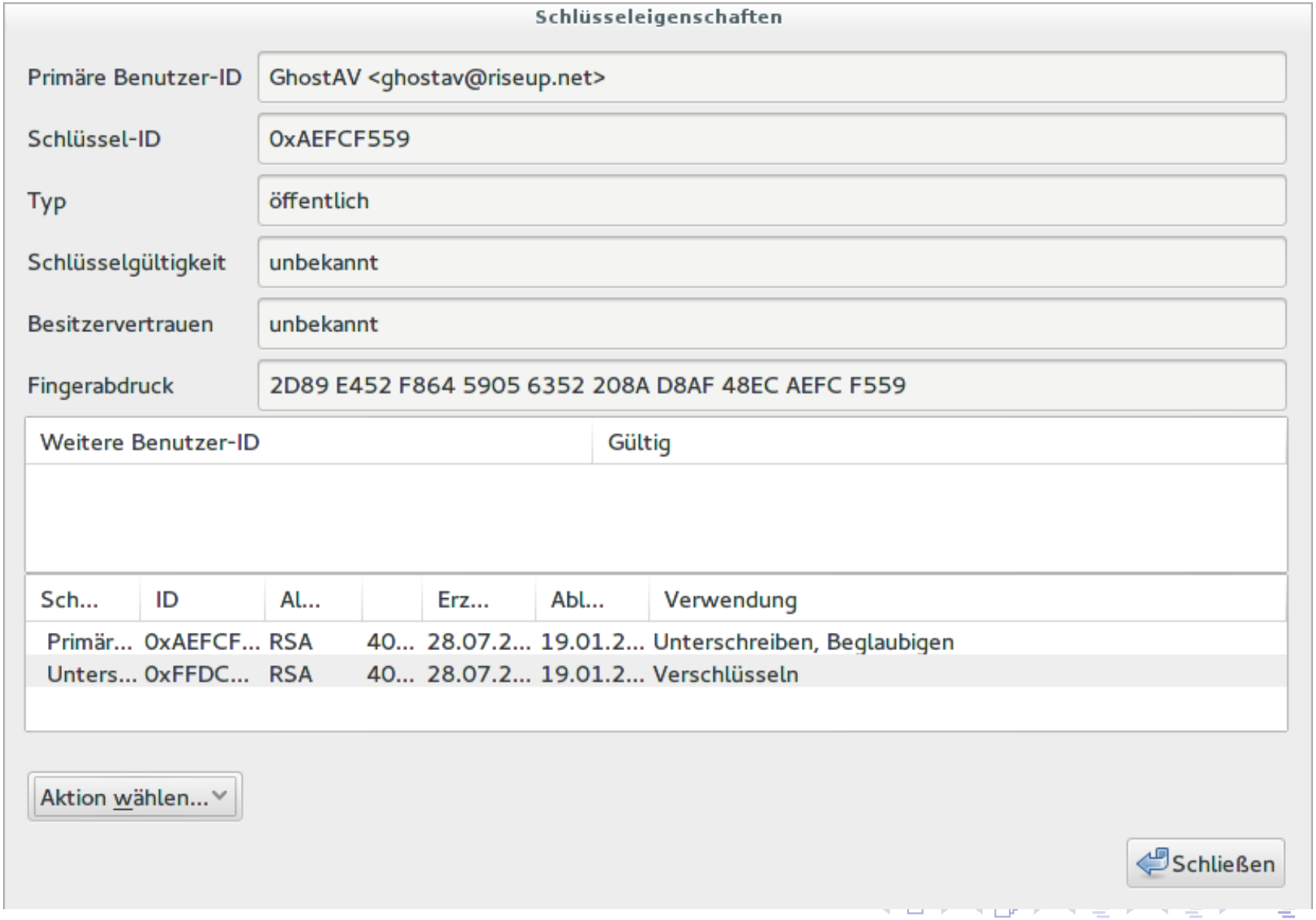
- Verschlüsselung aktiv (inaktiv=grau)
- Unterschreiben aktiv (inaktiv=grau)

Übersicht

1. Begriffe und Allgemeines zur IT-Sicherheit
2. Wie funktioniert Kommunikation via Email?
3. GNU Privacy Guard
4. (sicheres) Verteilen der öffentlichen Schlüssel
   - Attribute und Eigenschaften von Schlüsseln
   - Web of Trust – vertrauen über mehrer Stufen
   - Schlüsselserver

Attribute und Eigenschaften von Schlüsseln

☰ > OpenPGP > Schlüssel verwalten... > Rechtsklick > Schlüsseleigenschaften



Eigenschaften von PGP-Schlüsseln

Benutzer-ID Emailaddresse(n) zu der der Schlüssel gehört

(Ändern: über “Aktion wählen” > “Benutzer-IDs verwalten”)

Eigenschaften von PGP-Schlüsseln

Benutzer-ID Emailaddresse(n) zu der der Schlüssel gehört
(Ändern: über "Aktion wählen" > "Benutzer-IDs verwalten")

Schlüssel-ID letzten 8 Zeichen des Fingerabruck
VORSICHT kann erzwungen/manipuliert werden!

Eigenschaften von PGP-Schlüsseln

Benutzer-ID Emailaddresse(n) zu der der Schlüssel gehört
(Ändern: über "Aktion wählen" > "Benutzer-IDs verwalten")

Schlüssel-ID letzten 8 Zeichen des Fingerabruck
VORSICHT kann erzwungen/manipuliert werden!

Schlüsselgütligkeit Validität des Schlüssels. Gegeben falls:

- Bentuzervertrauen = absolut
- eigene Unterschrift (mindestens "einfache Überprüfung")
- Web-of-Trust

Eigenschaften von PGP-Schlüsseln

Benutzervertrauen Einfluss einer Unterschrift von Bob (Benutzer-ID) auf Schlüsselgütligkeit von Charlie

Eigenschaften von PGP-Schlüsseln

Benutzervertrauen Einfluss einer Unterschrift von Bob (Benutzer-ID) auf Schlüsselgültigkeit von Charlie

[absolut] als wäre Bob ein eigener Schlüssel
Charlie wird valide
Bob ist selbst valide
$\Rightarrow$ standard für $_{priv}$

Eigenschaften von PGP-Schlüsseln

Benutzervertrauen Einfluss einer Unterschrift von Bob (Benutzer-ID) auf **Schlüsselgütligkeit** von Charlie

[absolut] als wäre Bob ein eigener Schlüssel
Charlie wird valide
Bob ist selbst valide
$\Rightarrow$ standard für priv

[voll] Charlie wird valide
Bob nicht automatisch valide

Eigenschaften von PGP-Schlüsseln

Benutzervertrauen Einfluss einer Unterschrift von Bob (Benutzer-ID) auf Schlüsselgütligkeit von Charlie

[absolut] als wäre Bob ein eigener Schlüssel
Charlie wird valide
Bob ist selbst valide
$\Rightarrow$ standard für priv

[voll] Charlie wird valide
Bob nicht automatisch valide

[gering] Charlie wird durch mehrer Unterschriften verschiedener Benutzer validiert

Eigenschaften von PGP-Schlüsseln

Benutzervertrauen Einfluss einer Unterschrift von Bob (Benutzer-ID) auf Schlüsselgütligkeit von Charlie

[absolut] als wäre Bob ein eigener Schlüssel
Charlie wird valide
Bob ist selbst valide
$\Rightarrow$ standard für $_{priv}$

[voll] Charlie wird valide
Bob nicht automatisch valide

[gering] Charlie wird durch mehrer Unterschriften verschiedener Benutzer validiert

[NICHT] keine Auswirkung

Eigenschaften von PGP-Schlüsseln

Benutzervertrauen Einfluss einer Unterschrift von Bob (Benutzer-ID) auf Schlüsselgütligkeit von Charlie

[absolut] als wäre Bob ein eigener Schlüssel
Charlie wird valide
Bob ist selbst valide
⇒ standard für $_{priv}$

[voll] Charlie wird valide
Bob nicht automatisch valide

[gering] Charlie wird durch mehrer Unterschriften verschiedener Benutzer validiert

[NICHT] keine Auswirkung

[weiß nicht] wie NICHT – aber ohne Wertung ;)
⇒ standard für $_{pub}$

Das Web of Trust

Ziel? Fingerprint vergleiche nerven auf dauer
$\Rightarrow$ muss leichter gehen

Das Web of Trust

Ziel? Fingerprint vergleiche nerven auf dauer
$\Rightarrow$ muss leichter gehen

Wie? Unterschriebene key_{pub} + Benutzervertrauen
$\dashrightarrow$ Schlüsselgültigkeit

Das Web of Trust

Ziel? Fingerprint vergleiche nerven auf dauer
$\Rightarrow$ muss leichter gehen

Wie? Unterschriebene key_{pub} + Benutzervertrauen
$\dashrightarrow$ Schlüsselgültigkeit

Modell PGP-Trust-Modell (Standard bei GnuPG)

Das Web of Trust

Ziel? Fingerprint vergleiche nerven auf dauer
$\Rightarrow$ muss leichter gehen

Wie? Unterschriebene 🔑_{pub} + Benutzervertrauen
$\dashrightarrow$ Schlüsselgültigkeit

Modell PGP-Trust-Modell (Standard bei GnuPG)

entweder $\text{🔑}^{Charlie}_{pub}$ unterschrieben von: Bob
+ Benutzervertrauen $\geq$ [voll]: 🔑^{Bob}_{pub}

Das Web of Trust

Ziel? Fingerprint vergleiche nerven auf dauer
$\Rightarrow$ muss leichter gehen

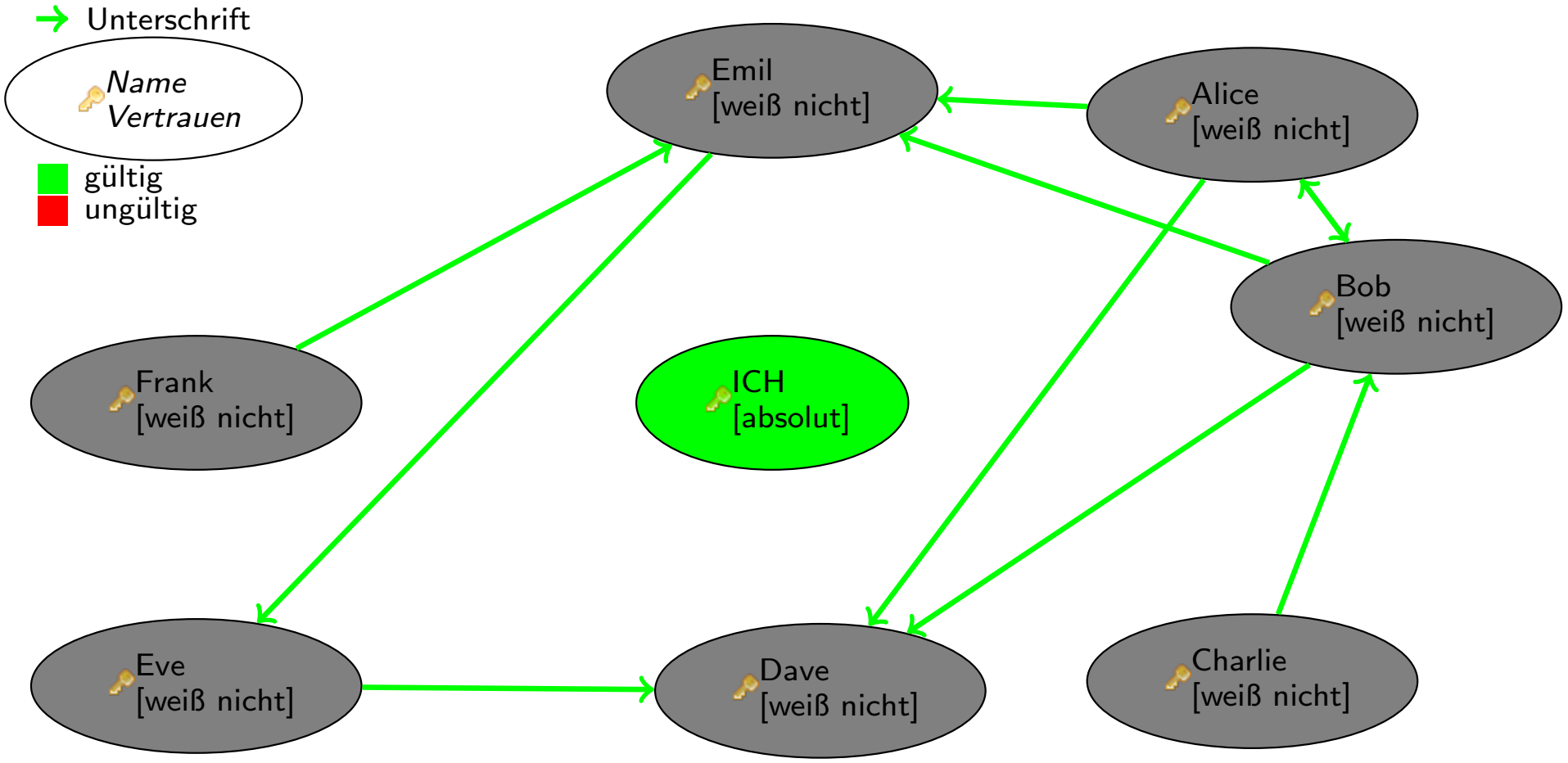
Wie? Unterschriebene 🔑_{pub} + Benutzervertrauen
$\dashrightarrow$ Schlüsselgültigkeit

Modell PGP-Trust-Modell (Standard bei GnuPG)

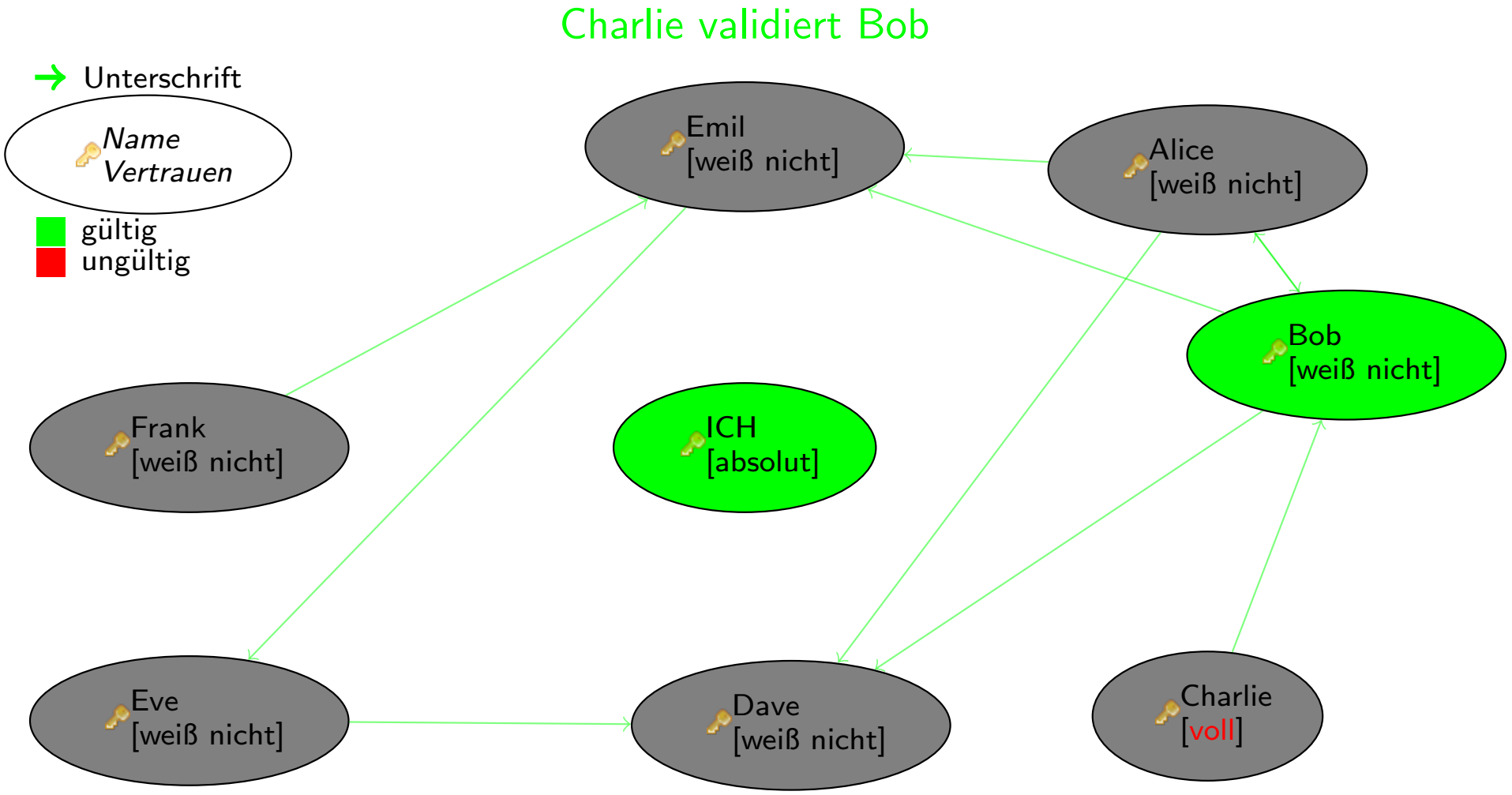
entweder $\text{🔑}^{Charlie}_{pub}$ unterschrieben von: Bob
+ Benutzervertrauen $\geq$ [voll]: 🔑^{Bob}_{pub}

oder $\text{🔑}^{Charlie}_{pub}$ unterschrieben von:
Bob,Dave , Frank
+ Benutzervertrauen = [gering]:
🔑^{Bob}_{pub} , 🔑^{Dave}_{pub} , 🔑^{Frank}_{pub}

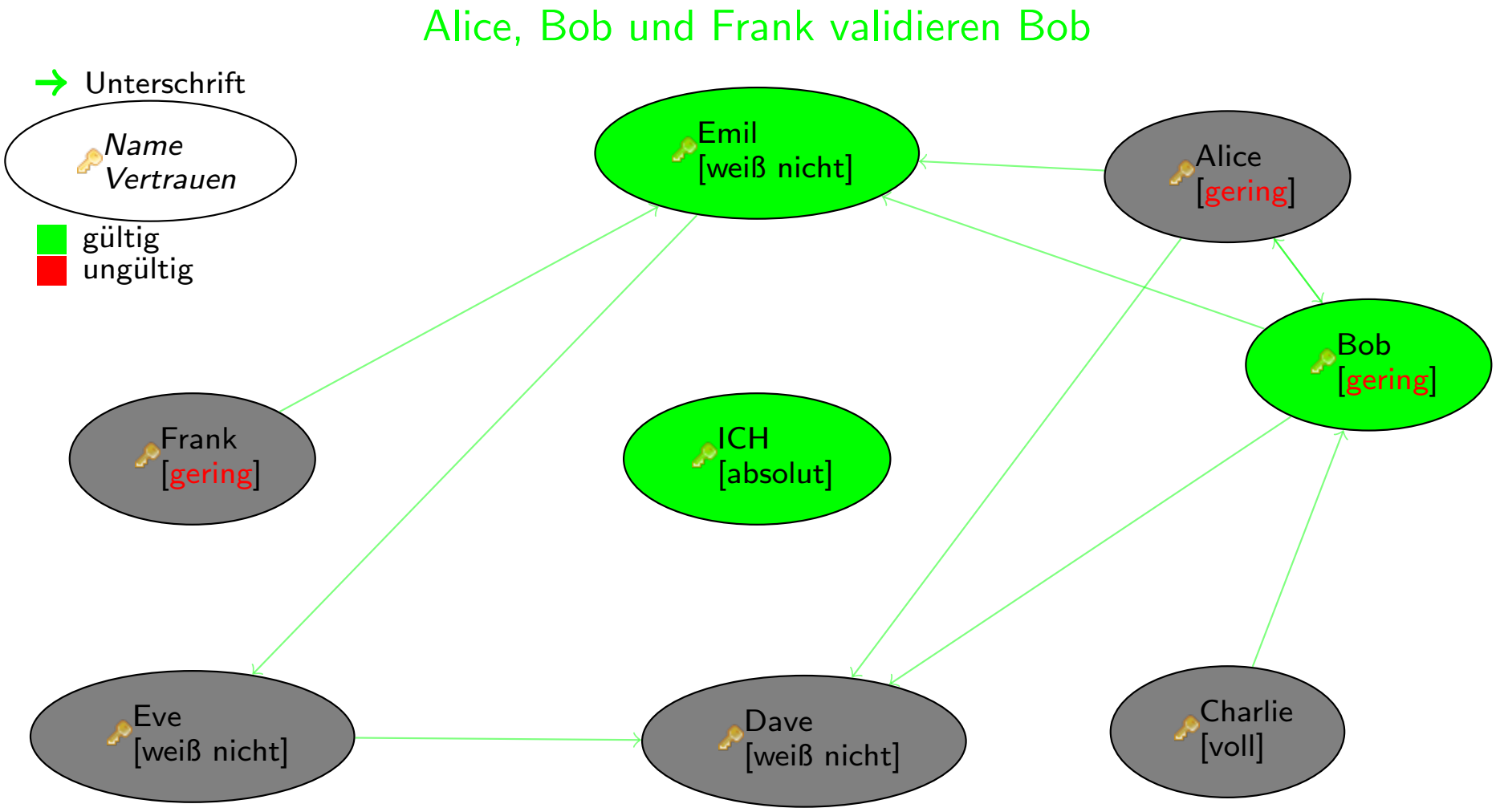
Beispiel


Unterschrift
Name
Vertrauen
gültig
ungültig
Emil
[weiß nicht]
Alice
[weiß nicht]
Bob
[weiß nicht]
Frank
[weiß nicht]
ICH
[absolut]
Eve
[weiß nicht]
Dave
[weiß nicht]
Charlie
[weiß nicht]

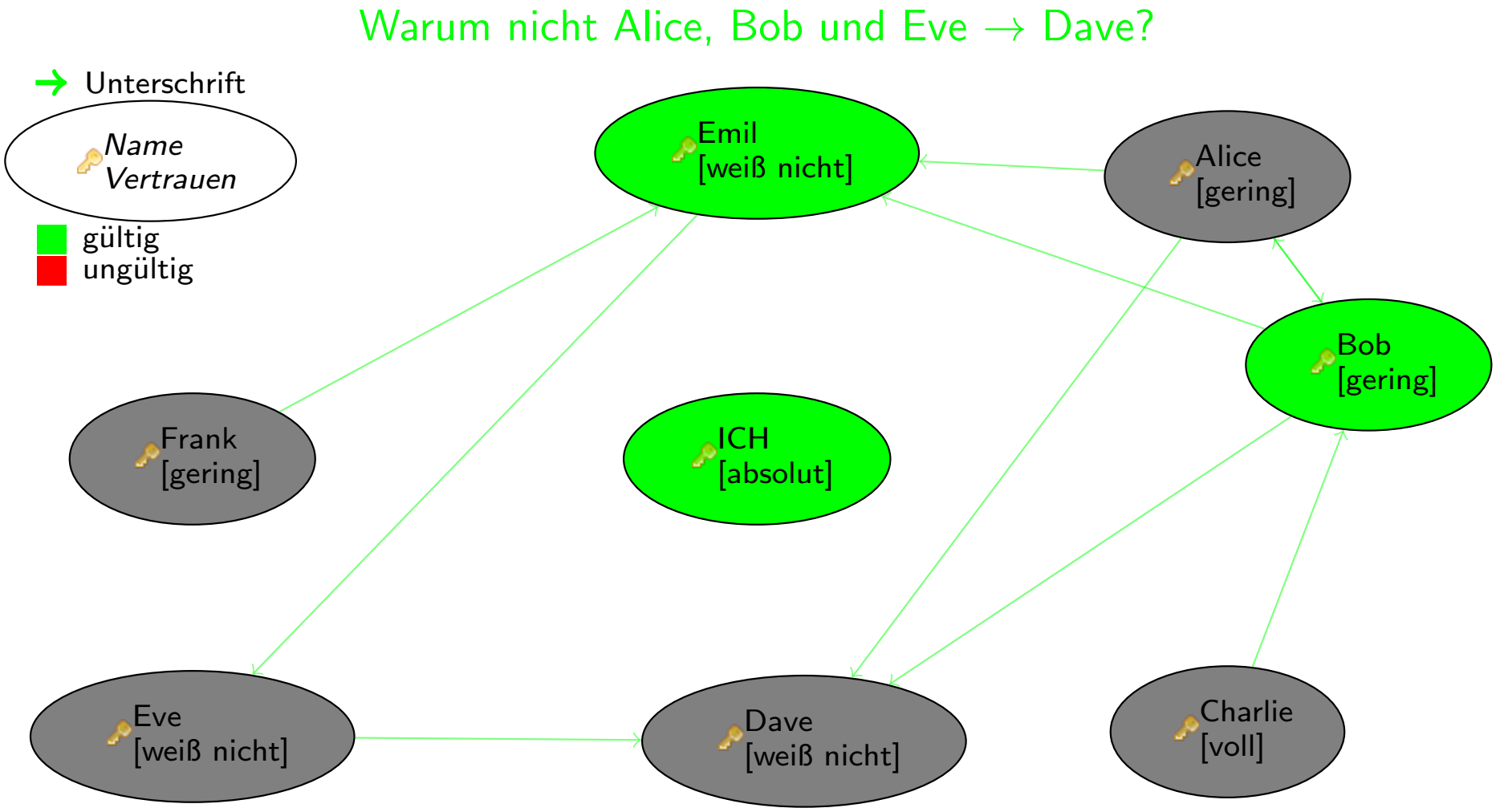
Beispiel


Charlie validiert Bob
Unterschrift
Name
Vertrauen
gültig
ungültig
Emil
[weiß nicht]
Alice
[weiß nicht]
Bob
[weiß nicht]
Frank
[weiß nicht]
ICH
[absolut]
Eve
[weiß nicht]
Dave
[weiß nicht]
Charlie
[voll]

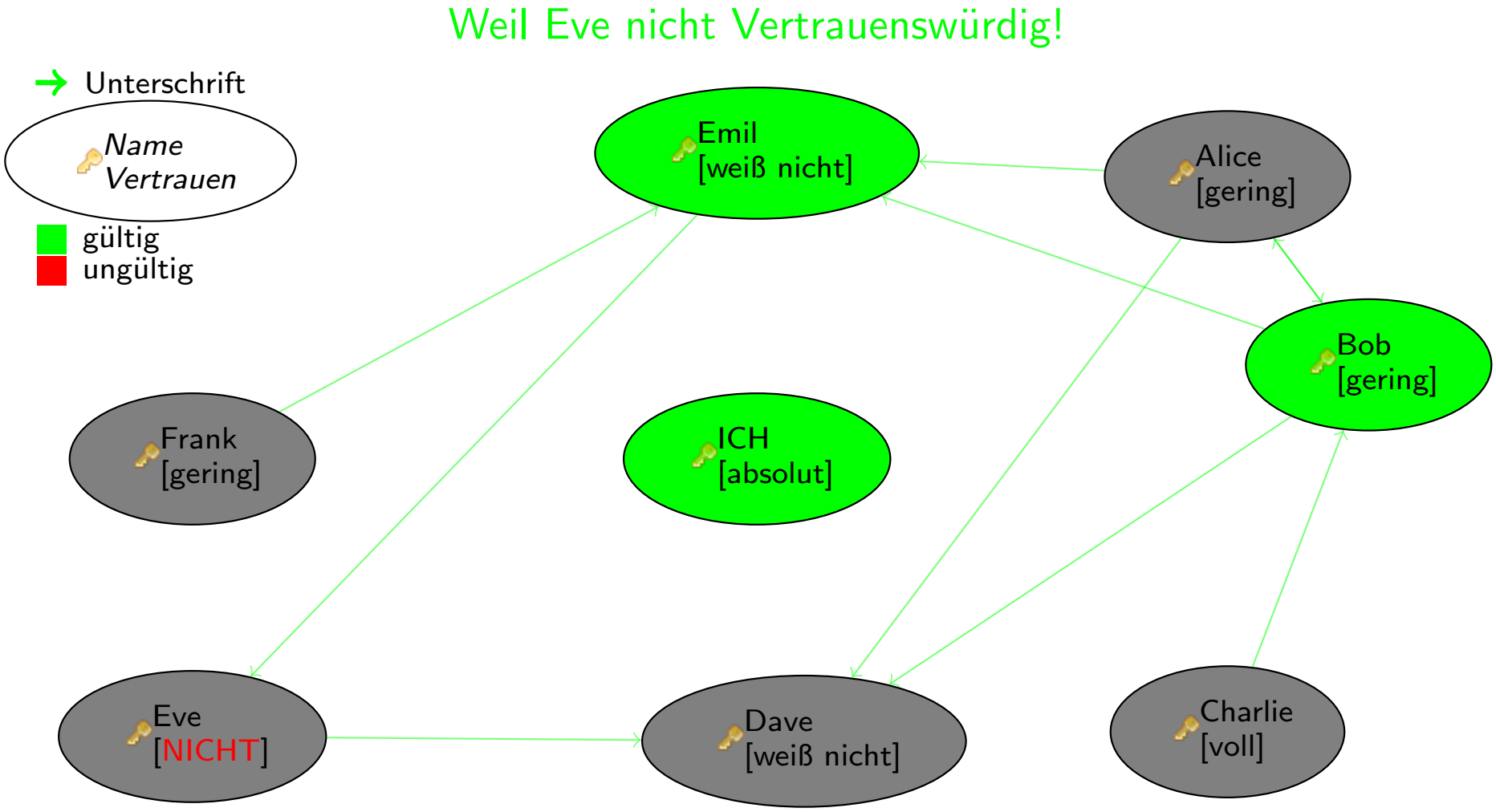
Beispiel


Alice, Bob und Frank validieren Bob
Unterschrift
Name
Vertrauen
gültig
ungültig
Emil
[weiß nicht]
Alice
[gering]
Bob
[gering]
Frank
[gering]
ICH
[absolut]
Eve
[weiß nicht]
Dave
[weiß nicht]
Charlie
[voll]

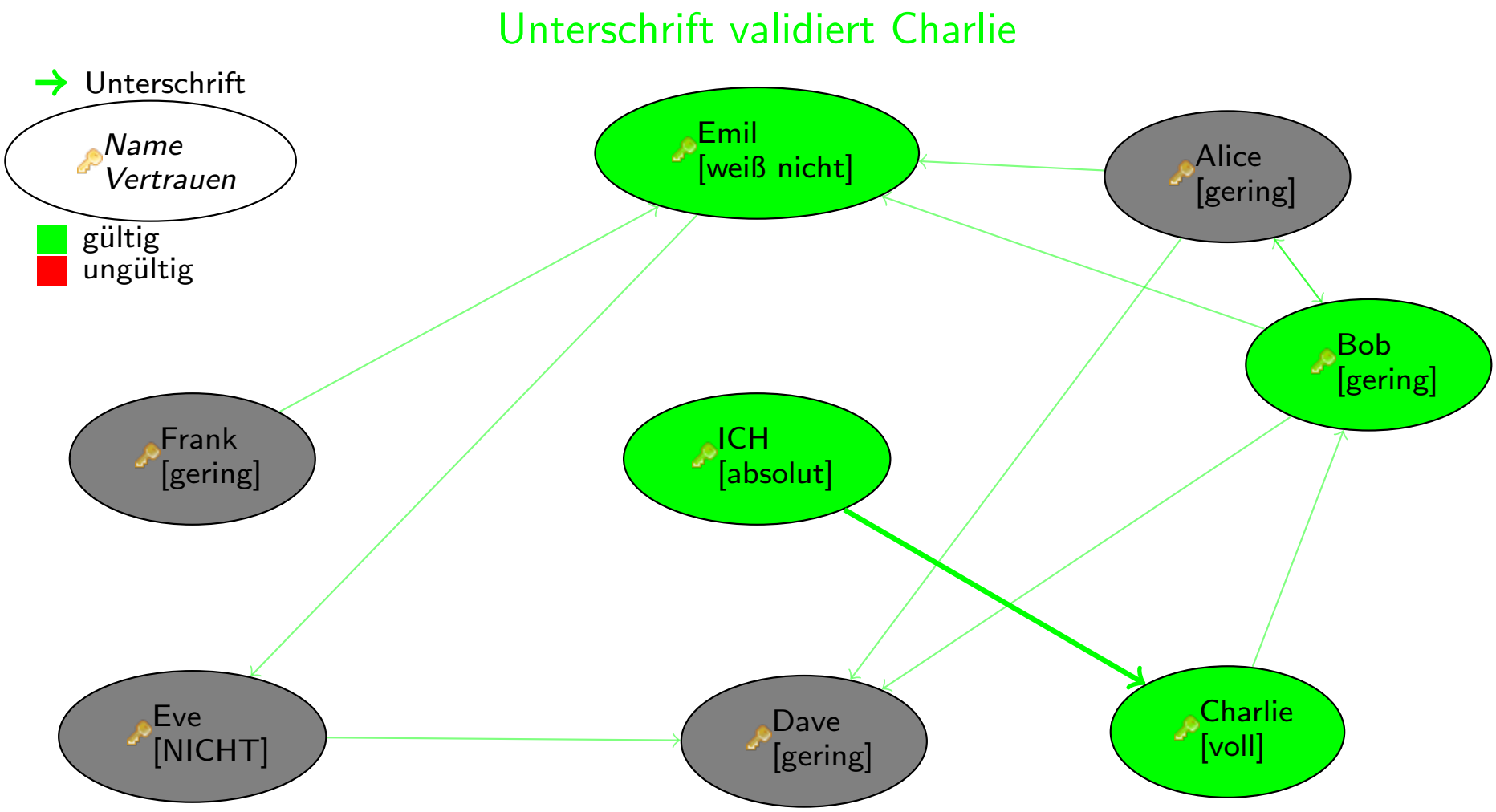
Beispiel


Warum nicht Alice, Bob und Eve → Dave?
Unterschrift
Name
Vertrauen
gültig
ungültig
Emil
[weiß nicht]
Alice
[gering]
Bob
[gering]
Frank
[gering]
ICH
[absolut]
Eve
[weiß nicht]
Dave
[weiß nicht]
Charlie
[voll]

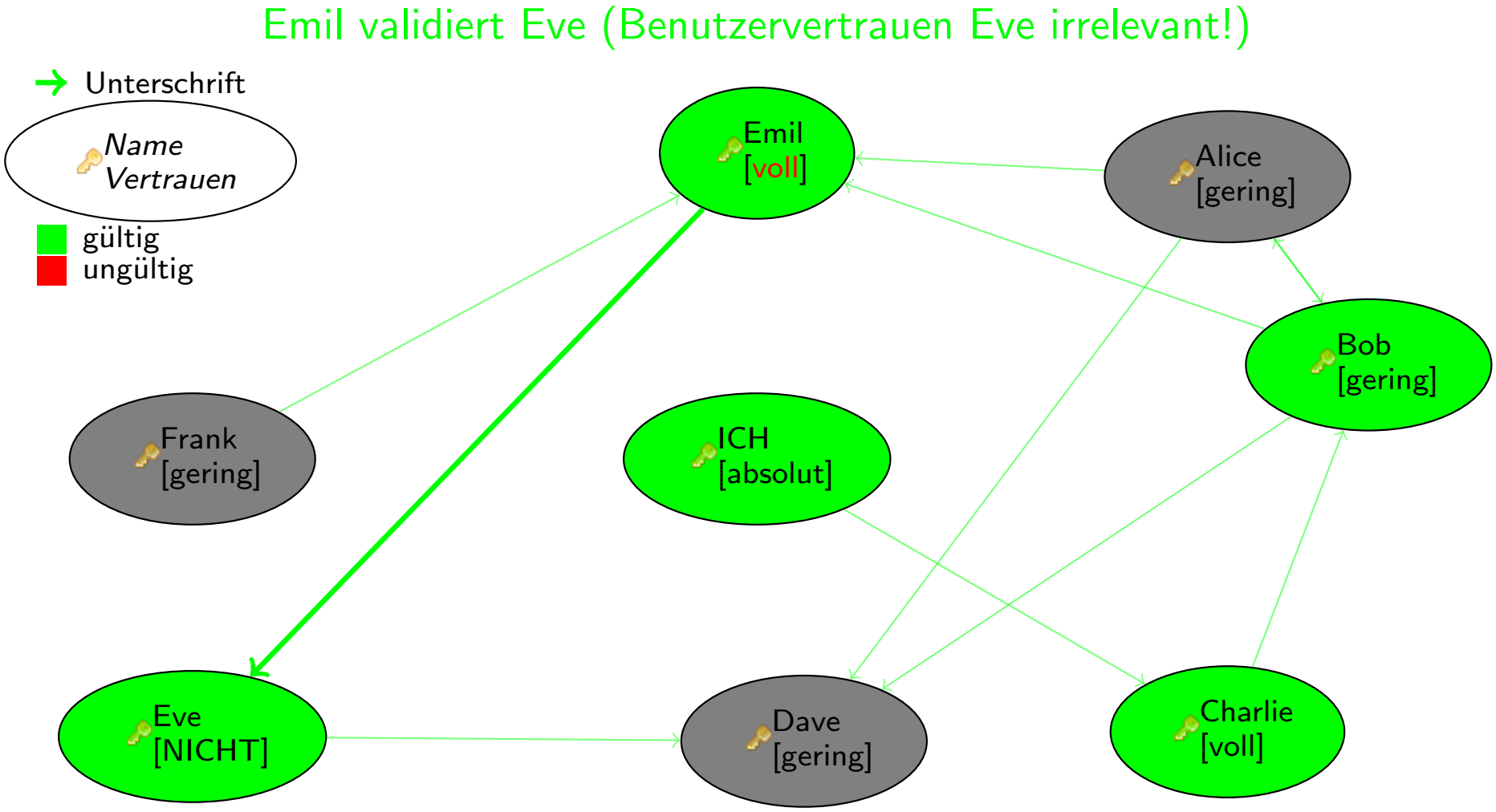
Beispiel


Weil Eve nicht Vertrauenswürdig!
Unterschrift
Name
Vertrauen
gültig
ungültig
Emil
[weiß nicht]
Alice
[gering]
Bob
[gering]
Frank
[gering]
ICH
[absolut]
Eve
[NICHT]
Dave
[weiß nicht]
Charlie
[voll]

Beispiel


Unterschrift validiert Charlie
Unterschrift
Name
Vertrauen
gültig
ungültig
Emil
[weiß nicht]
Alice
[gering]
Bob
[gering]
Frank
[gering]
ICH
[absolut]
Eve
[NICHT]
Dave
[gering]
Charlie
[voll]

Beispiel


Emil validiert Eve (Benutzervertrauen Eve irrelevant!)
Unterschrift
Name
Vertrauen
gültig
ungültig
Emil
[voll]
Alice
[gering]
Bob
[gering]
Frank
[gering]
ICH
[absolut]
Eve
[NICHT]
Dave
[gering]
Charlie
[voll]

Web of Trust

Merke Unterschied der zwei Vertrauensbegriffe

Benuterzvertrauen Vertrauen in den Benutzer, nur geprüfte Schlüssel zu signieren

Schlüsselgültigkeit Vertrauen, dass Schlüssel dem Benutzer gehört!

⇒ Kein Benutzervertrauen schliesst Schlüssgelgütligtkeit nicht aus!

Signatur hinterlässt natürlich Metadaten (Signaturbesitzer muss Schlüsselbesitzer begenet sein!)

Austausch Das System muss sich immer auf dem aktuellsten Stand (Signaturen, Rürckrufzertifikate,. . .) befinden

⇒ Wie können wir das leicht bewerkstelligen? Serverstruktur

Austausch leicht gemacht

Schlüsselserver Eine Art Telefonbuch für Schlüssel (+Unterschriften und Rückrufzertifikate)

Risikofrei Nur $_{pub}$ liegen auf dem Keyserver

Bequem Es gibt verschieden Keyserver (Ausfallsicher)
Synchronisation dieser lässt freie Wahl

Wichtig Um das Web of Trust zu ermöglichen, Unterschriften auf den Server laden

Enigmail und was sonst zu beachten ist...

Metadaten hinterlässt wissen "A kennt/hat gesehen/kontakt zu B"

Konfiguration Enigmail hat das bereits integriert

- Standardmässig holt es keine Schlüssel zum überprüfen von Signaturen
- Schlüsselunterschreiben, Benutzervertauen und Upload muss jedoch manuell erfolgen
- Alles im Kontextmenü der Schlüsselverwaltung
- Bei "kritischen" Kontakten lokale Signatur ($\Rightarrow$ kein Upload der Signatur)

Spam? Theoretisch kann dabei natürlich die Mailadresse gefunden werden
ABER: Keyserver bieten Suchfunktion, Ergebnis maximal 100 Keys
(wenn mehr, dann kein Ergebnis!)

Super Smash Bros N-64 Turnier

Veranstaltungshinweis

Meta Rhein Main Construction Days 2014

Veranstaltungshinweis

was? Vorträge zum Thema ITSicherheit, Kryptographie, Netzpolitik, Embedded Systems, Open Source Entwickung, Intelligente Verkehrsnetze, DIN EN 60880 sowie weitere thematische naheliegende Inhalte als auch Einführungen in die praktischen Anwendungen

wann? 5. bis 7. September 2014

wo? Hochschule Darmstadt Haus D14
Schfferstrae 8b, 64295 Darmstadt

31. Chaos Communication Congress

Veranstaltungshinweis

[noch in Plaungsphase → noch kein Bild verfügbar ;)]

was? Mehrtägiges Treffen der "Internationalen Hackerszene"[1]. Vorträge zu Themen rund um Technik sowie Workshops, Ausstellungen,...

wann? 27. bis 30. Dezember 2014

wo? Congress Centrum Hamburg

[1] Wikipedia

wie gehts weiter?

Fragen? Anregungen? Kritik? Themenvorschläge?

- jetzt
- per Mail an ghostav@riseup.net
  (Schlüssel gibts am Keyserver oder jetzt...)

Nächste Cryptoparty

- 20. August 2014
- Themenvorschläge? Interessen? ...

Let's start the party!

- bei Mate, Limo oder Bier weiterführende Gespräche
- Pizza?!