Nachrichtenverschlüsselung im Alltag

CLT 2014

15. März 2014

Tommy Sauer
Linux Consultant & Developer
B1 Systems GmbH
sauer@b1-systems.de

Inhaltsverzeichnis

Vorstellung B1 Systems

- gegründet 2004
- primär Linux/Open Source-Themen
- national & international tätig
- über 60 Mitarbeiter
- unabhängig von Soft- und Hardware-Herstellern
- Leistungsangebot:
  - Beratung & Consulting
  - Support
  - Entwicklung
  - Training
  - Betrieb
  - Lösungen
- dezentrale Strukturen

Schwerpunkte

- Virtualisierung (XEN, KVM & RHEV)
- Systemmanagement (Spacewalk, Red Hat Satellite, SUSE Manager)
- Konfigurationsmanagement (Puppet & Chef)
- Monitoring (Nagios & Icinga)
- IaaS Cloud (OpenStack & SUSE Cloud)
- Hochverfügbarkeit (Pacemaker)
- Shared Storage (GPFS, OCFS2, DRBD & CEPH)
- Dateiaustausch (ownCloud)
- Paketierung (Open Build Service)
- Administratoren oder Entwickler zur Unterstützung des Teams vor Ort

Private Kommunikation

Wo kommunizieren wir?

- Kaffeeküche
- ÖPNV
- Bar bei Bier mit Freunden
- Konventions
- Zu Hause
- ...

Unsere Kommunikation findet an vielen öffentlichen und privaten Orten statt.

Wie kommunizieren wir?

- Gespräche
- Gestik/Mimik
- Smartphones/Telefone
- PCs/Notebooks

Verschmelzung von Kommunikationsmitteln

Eigenschaften

- Vertraulich
- Persönlich
- Wir bestimmen den/die Empfänger
- Nicht nachweisbar

Problem Einhaltung ist nicht selbstverständlich.
Auf digitaler Ebene liegt die Verantwortung bei *dir*!

Verschlüsselung

Who needs encryption?

Abbildung : Encryption – funpic

Ziele

- Nachrichten an ausgewählten Empfänger
- Verifizierung des Empfängers
- Mitlesbarkeit erschweren/verhindern
- Sicherheit für sensible Informationen
- Variation je nach eingesetzter Technologie

Notwendigkeit

Abbildung : Edward Snowden

Notwendigkeit

- Überwachung von Geheimdiensten
- Unschuldsvermutung
- Je mehr, desto besser!
- Recht auf Privatsphäre!

Typen von Verschlüsselung

Symmetrisch

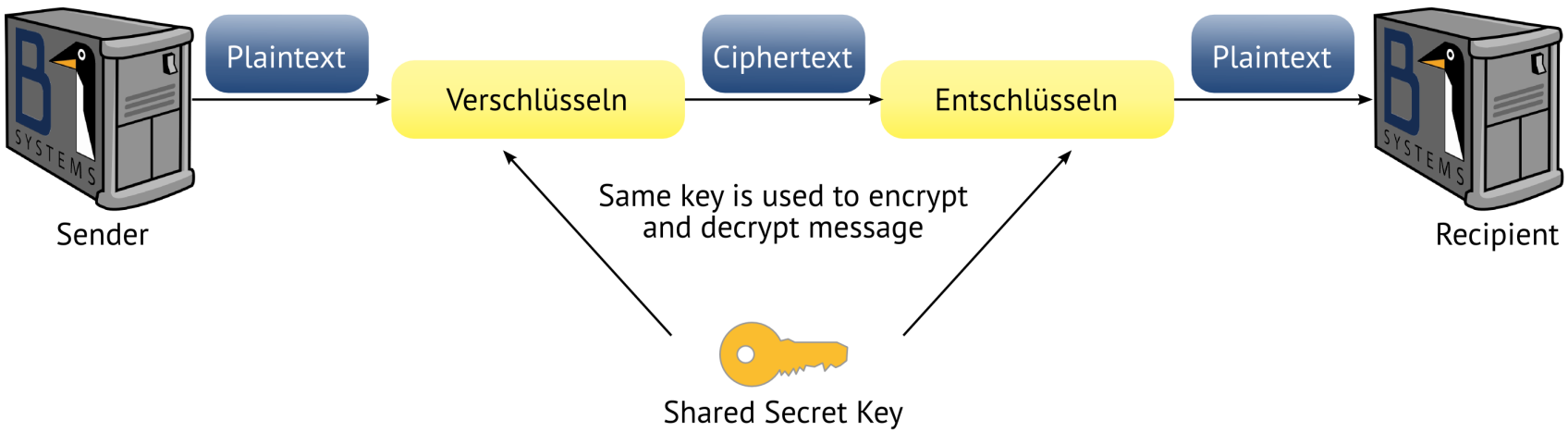

Abbildung : Symmetrische Verschlüsselung

Asymmetrisch

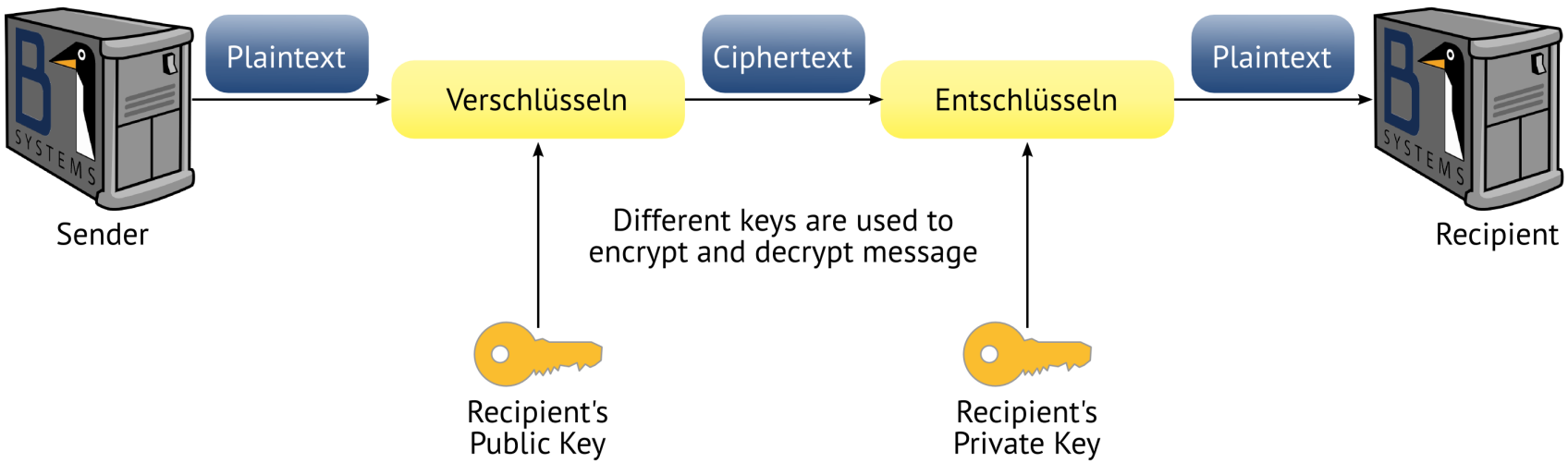

Abbildung : Asymmetrische Verschlüsselung

Vergleich

Vergleich der Verschlüsselungstypen

	Symmetrisch	**Asymmetrisch**
Vorteile	schnelleres Computing einfache Implementierung	Sicherer Tausch von Pubkeys
Nachteile	Keyaustausch über sicheren Zweitkanal notwendig	Langsameres Computing
Beispiele	AES	RSA, DSA

OTR im Detail

Was ist OTR?

- off-the-record Messaging
- Verfahren zum verschlüsselten Kommunizieren über Instant Messenger
- entwickelt 2004 von Nikita Borisov, Ian Goldberg, Eric Brewer
- Symbiose aus verschiedenen kryptografischen Technologien
- leicht einzusetzendes Protokoll
- weit verbreitet in der Linux-Welt

Voraussetzung

- Beide Nutzer benötigen einen OTR-fähigen Messenger
  - Linux
    - Pidgin + OTR-Plugin
    - Jitsi
  - Android
    - Xabber
    - Chatsecure
- Internet
- Wunsch, privat miteinander zu kommunizieren

Grundsätze

Encryption Verschlüsselung der Nachrichten

Authentication Kommunikation mit Zielperson

Deniability Nachrichten lassen sich abstreiten

Perfect forward secrecy Private Keys dürfen keine Gefahr für frühere Konversationen sein

MAC

- Message Authentication Code
- Verifizieren des Senders gegenüber dem Empfänger (Authentication)
- keine Signaturen (Abstreitbarkeit)

MAC

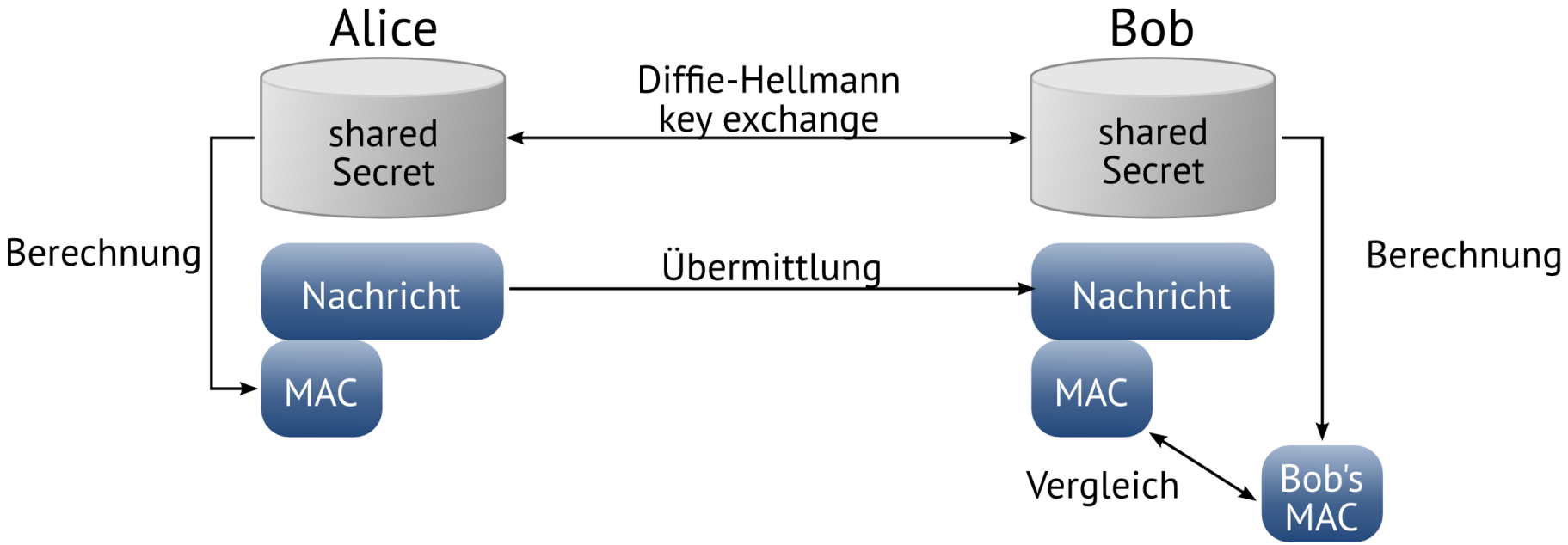

Abbildung : Message Authentication Code

MAC

- Secret Key kennen nur Alice und Bob
- Sender hatte Secret Key $\rightarrow$ Sicherheit des Absenders
- Empfänger kann Nachricht selbst schicken (Deniability)
- Veröffentlichen der MAC nach Nachricht Senden in der folgenden Nachricht $\rightarrow$ Niemand kann Absender feststellen

Kommunikation

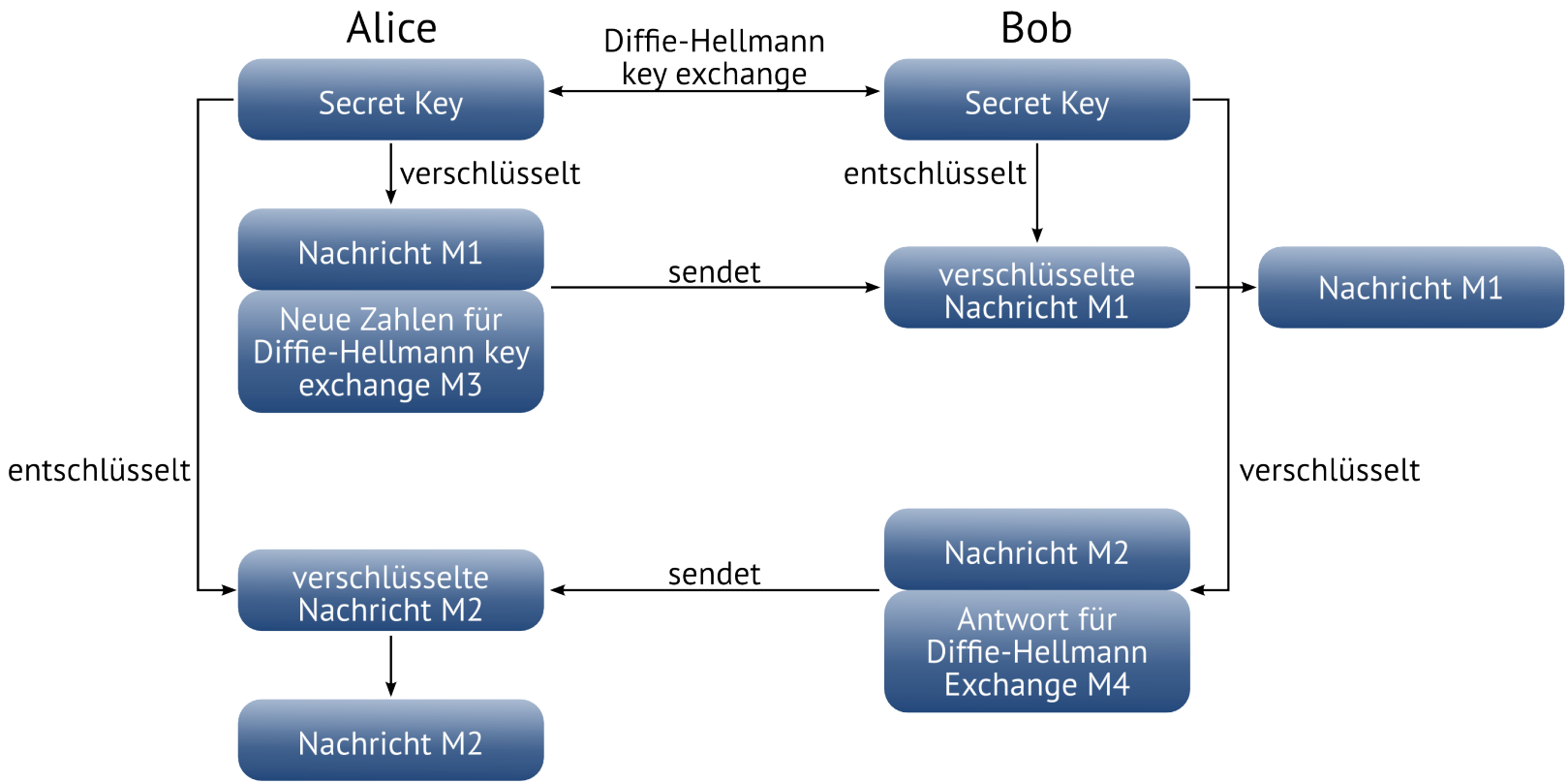

Abbildung : OTR Kommunikation

Verschlüsselung

- Verschlüsselung mit stream cipher AES (Encryption)
- Diffie-Hellmann-Exchange liefert Encryption Key (Perfect forward secrecy)
- malleable (verformbare) Verschlüsselung
  - Manipulation des verschlüsselten Textes durch Angreifer möglich und gewollt
  - $\rightarrow$ jeder kann Nachricht gesendet oder manipuliert haben (Deniability)
  - Verschlüsselung liefert keine Authentizität und Integrität (Nutzung von MACs)

Fingerprint

- wird generiert pro Kommunikationsmedium und Account
- Sicherstellen des richtigen Gesprächspartners
- jeder Fingerprint ist erst unsicher
- Verifikation durch
  - Frage und Antwort
  - vorher geteiltes Geheimnis
  - Vergleichen des Fingerprints
- Verhinderung von Man-in-the-middle attack

Zusammenfassung

OTR

- ist perfekt für Verschlüsselung von IMs
- ist leicht zu bekommen
- ist leicht zu bedienen
- schützt eure Privatsphäre

PGP im Detail

Was ist PGP?

„It's personal. It's private. And it's no one's business but yours."

- Phil Zimmermann 1991
- Pretty Good Privacy
- Verschlüsselung, Signierung und Entschlüsselung von Emails und Dateien

Voraussetzung

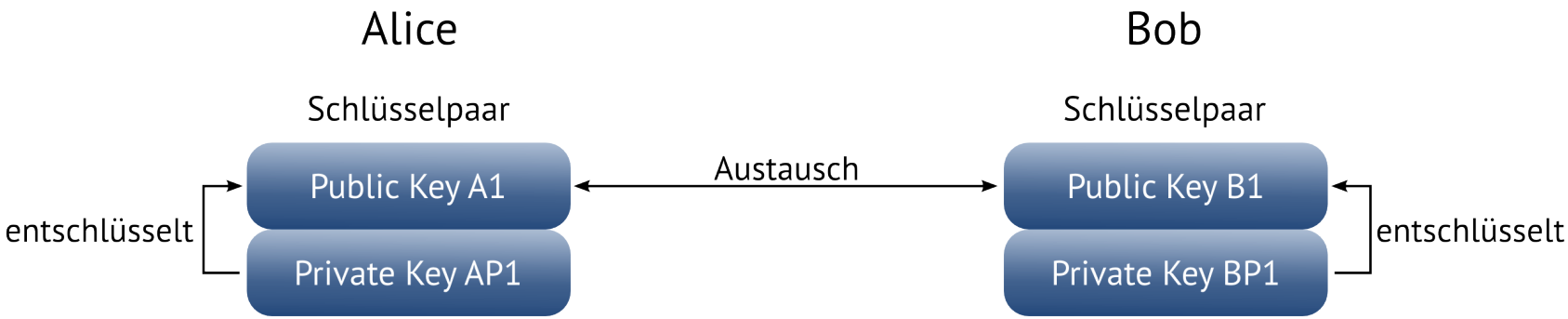

Abbildung : PGP – Voraussetzung

Vorhandenes Schlüsselpaar ist erforderlich

Funktionsweise Verschlüsselung

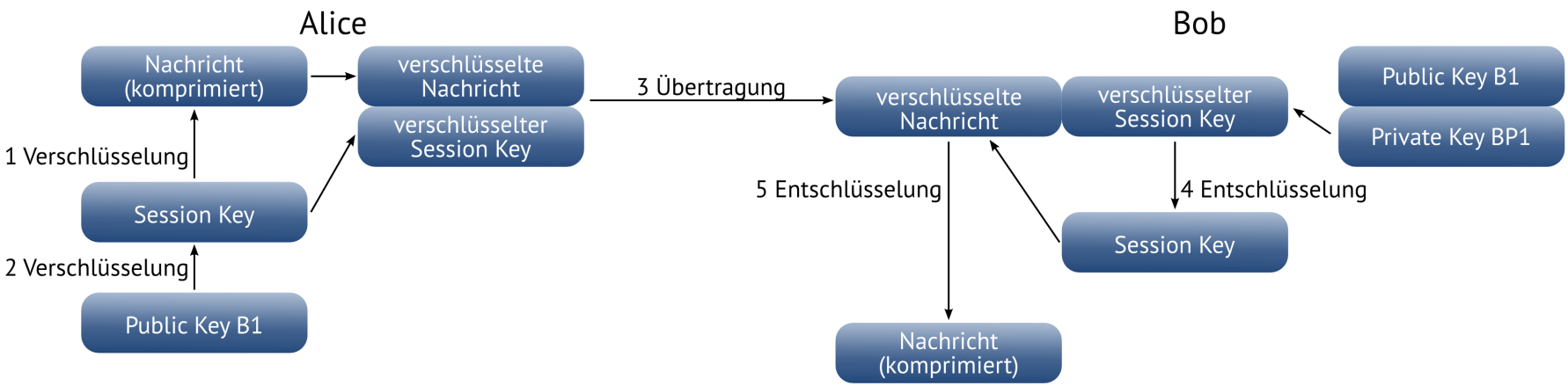

Abbildung : PGP – Funktionsweise

Digitale Signaturen

Digitale Signaturen

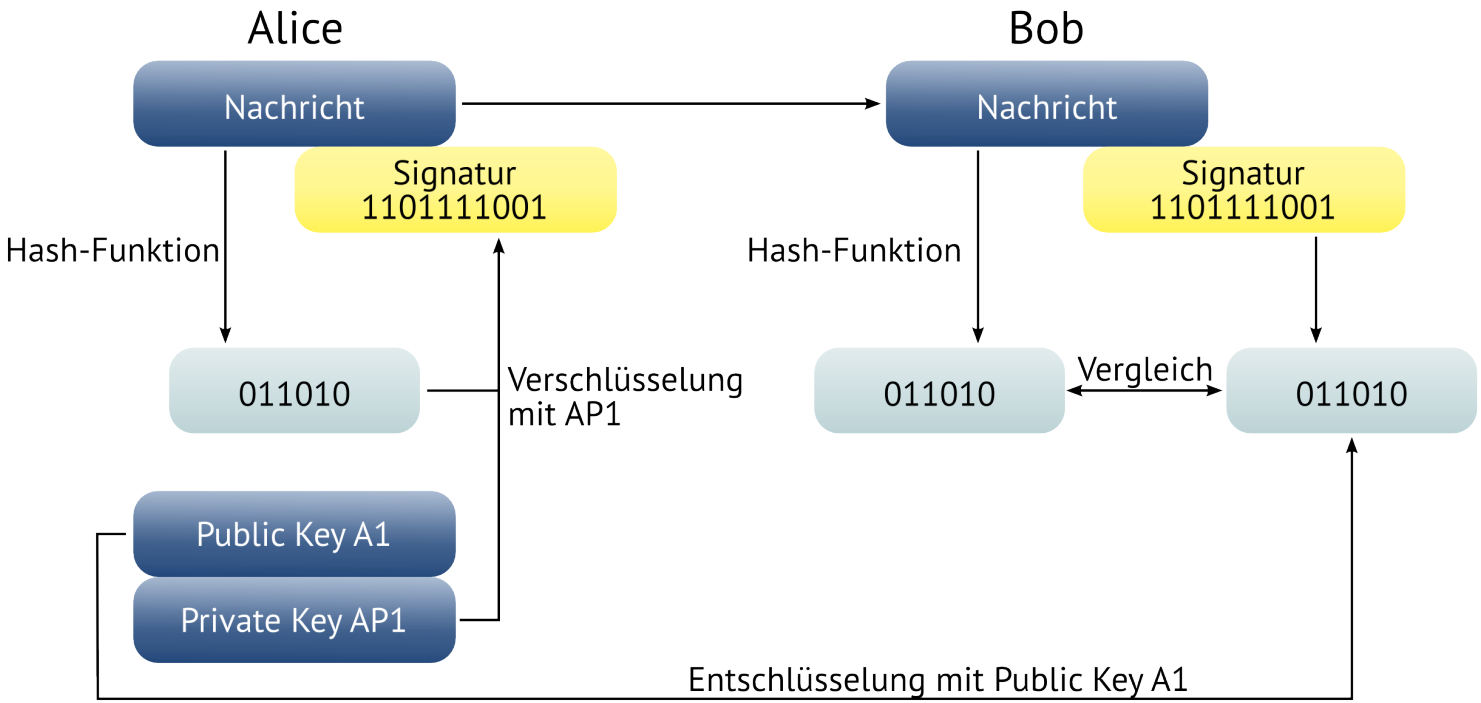

Abbildung : PGP – Digitale Signatur

Digitale Signaturen

- Authentifikation des Senders
- Integrität der Nachricht
- *Nicht*-Abstreitbarkeit
- „Digitale Unterschrift”

Zertifikate

Zertifikate

Zertifikat Annahme, dass Key zu seinem Eigentümer gehört. Bestätigung durch Dritten.

Unterstützte Zertifikate PGP Keys, X.509

Zertifikate

```
pub   2048R/34C7ED8E 2013-10-01
      Key fingerprint = 777D 058A 01EB BABF 07EA  658B A398 EC7B 34C7 ED8E
uid                  Tommy Sauer <sauer@b1-systems.de>
sig 3        34C7ED8E 2013-12-10  Tommy Sauer <sauer@b1-systems.de>
sig 3        34C7ED8E 2013-10-01  Tommy Sauer <sauer@b1-systems.de>
sig 3        7FCE971B 2013-10-14  Theodor Reppe (B1 Systems) <reppe@b1-systems.de>
sig 3        253F4A52 2013-10-14  Tobias Wolter <tobias.wolter@b1-systems.de>
sig          BED04EB5 2013-12-12  Lars Kalms <lars.kalms@gmx.net>
uid                  Tommy Sauer <tommy.sauer@online.de>
sig 3        34C7ED8E 2013-12-10  Tommy Sauer <sauer@b1-systems.de>
sig          BED04EB5 2013-12-12  Lars Kalms <lars.kalms@gmx.net>
sub   2048R/5E5A9152 2013-10-01 [expires: 2018-09-30]
sig          34C7ED8E 2013-10-01  Tommy Sauer <sauer@b1-systems.de>
```

Vertrauen

Vertraute Quellen

Ziel Identität des Gesprächspartners vertrauen

- Direkt
  - Quelle des Keys ist bekannt
  - z.B. Austausch mit Freund
- Hierarchisch
  - Zertifikate, die anderen Zertifikaten untergeordnet sind
  - Root CA $\rightarrow$ Corporate CA $\rightarrow$ Personen
- Web of Trust
  - Upload des Keys auf öffentlichen Keyserver (PKI)
  - Andere überprüfen Echtheit und Signieren mit ihrem private Key
  - Idealfall: Jeder hat jeden Key signiert $\rightarrow$ Jede Identität ist bestätigt

Public Key Infrastructure (PKI)

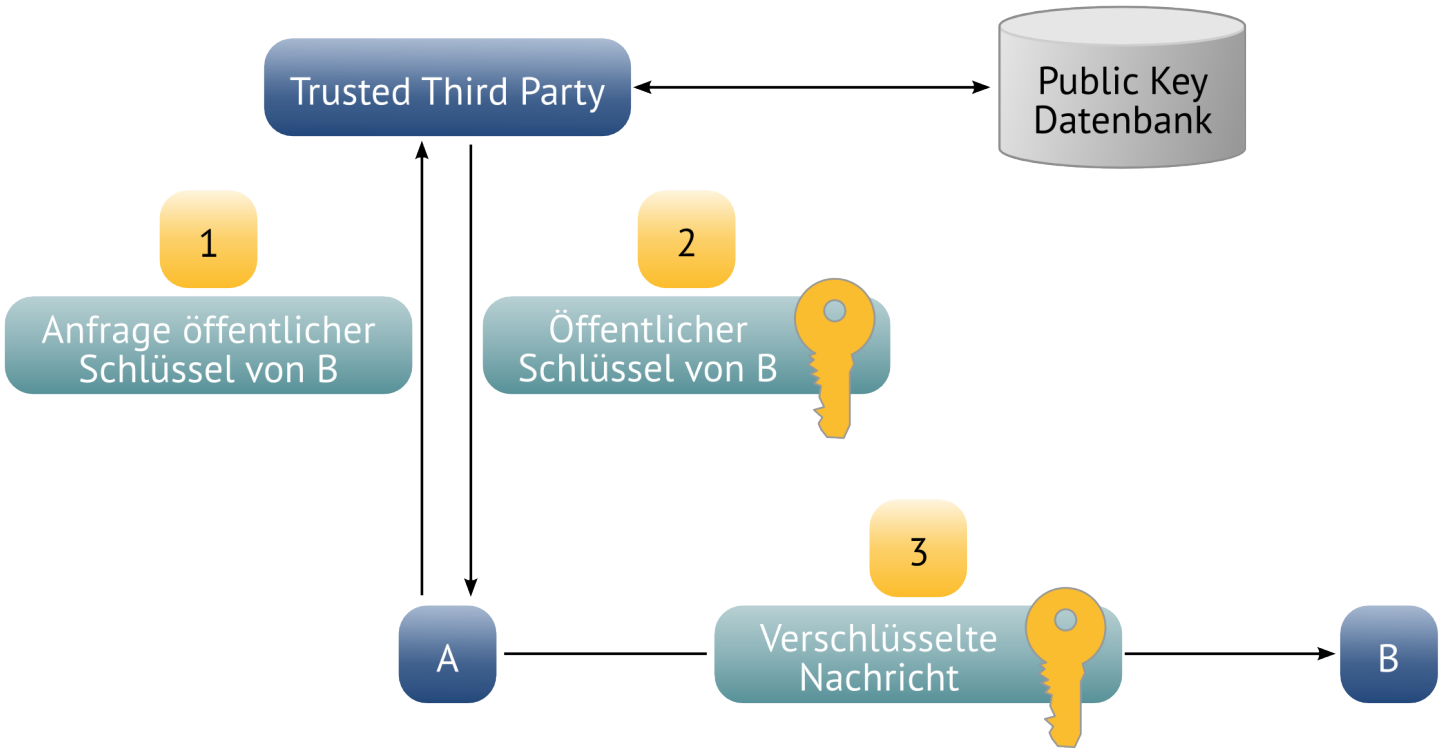

Abbildung : PKI

Chain of Trust (Vertrauenskette)

- PGP benötigt eine vollständig oder zwei teilweise vertraute Signaturen
- Vollständiges Vertrauen (*Complete trust*)
- Teilweises Vertrauen (*Marginal trust*)
- kein Vertrauen (*No trust*)

Keysigningparty

Abbildung : Fosdem 2008

Keysigningparty

- Zusammenkommen vieler Leute zum gegenseitigen Public-Key-Signen
- Oft in Zusammenhang mit Universitäten, Tagungen, LUGs
- Ziele:
  - Web of Trust stärken
  - Diskussion über Kryptografie anregen
  - Signaturen sammeln
- CLT Keysigningparty: Heute, 18:00 Uhr, Studentenclub PEB

Zusammenfassung

PGP

- ist perfekt für Verschlüsselung von Emails und Dateien
- ist super zum digitalen Signieren
- schützt eure Privatsphäre
- bringt euch zusammen
  - digital im Web of Trust
  - real beim Keysigning

Quellen

Off-the-Record Communication, or, Why Not To Use PGP. Nikita Borisov, Ian Goldberg, Eric Brewer. 2004
An Introduction to Cryptography. Network Associates, Inc. and its Affiliated Companies. 2000

https://whispersystems.org/blog/simplifying-otr-deniability/

https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

http://en.wikipedia.org/wiki/Malleability_(cryptography)

http://de.wikipedia.org/wiki/Message_Authentication_Code

http://en.wikipedia.org/wiki/Deniable_encryption http://www.programmerinterview.com/index.php/

general-miscellaneous/symmetric-vs-public-key-cryptography/

http://de.wikipedia.org/wiki/Advanced_Encryption_Standard

http://en.wikipedia.org/wiki/Off-the-Record_Messaging https://otr.cypherpunks.ca/index.php#faqs

http://en.wikipedia.org/wiki/Digital_signature http://www.pgpi.org/doc/pgpintro/

http://cryptnet.net/fdp/crypto/keysigning_party/en/keysigning_party.html#definition

http://www.cs.bham.ac.uk/~mdr/teaching/modules/security/lectures/PGP.html

http://upload.wikimedia.org/wikipedia/commons/5/5d/FOSDEM_2008_Key_signing_party_2.jpg

http://memeguy.com/photos/images/psshh-who-needs-encryption-18391.jpg

Vielen Dank für Ihre Aufmerksamkeit!

Bei weiteren Fragen wenden Sie sich bitte an info@b1-systems.de
oder +49 (0)8457 - 931096