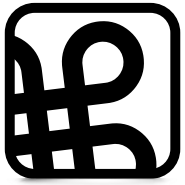


Macoun

Die Magie hinter Handoff und Continuity

Alexander Heinrich

Ablauf

- Einleitung
- Protokoll Ablauf
  - Bluetooth Low Energy
  - WiFi Kommunikation
- Evaluierung
- Fazit

Über mich

- App Entwickler seit 8 Jahren
  - Indie Apps
  - Projektaufträge
- Master Student in IT-Sicherheit

SEEMOO @ TU Darmstadt

- Prof Dr. Matthias Hollick und Milan Stute
- Reverse Engineering von Apple Wireless Protokollen
- Open Source Implementierung
  - Apple Wireless Direct Link (OWLink)
  - AirDrop (OpenDrop)

Einleitung

Continuity

Integration

WiFi Password Sharing

AirDrop

Continuity Camera

Universal Clipboard

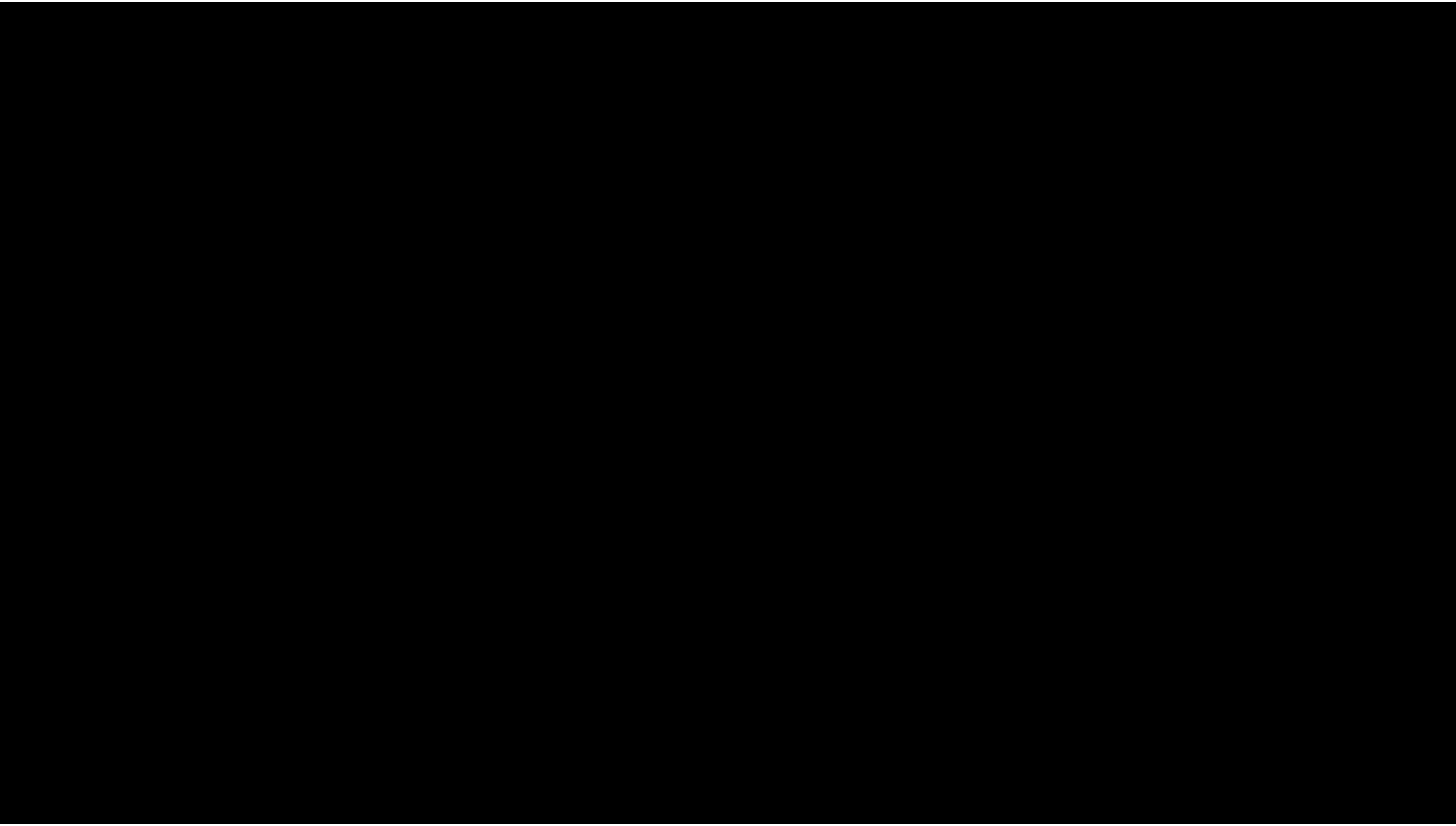
Handoff

Continuity

Integration

Universal Clipboard

Handoff



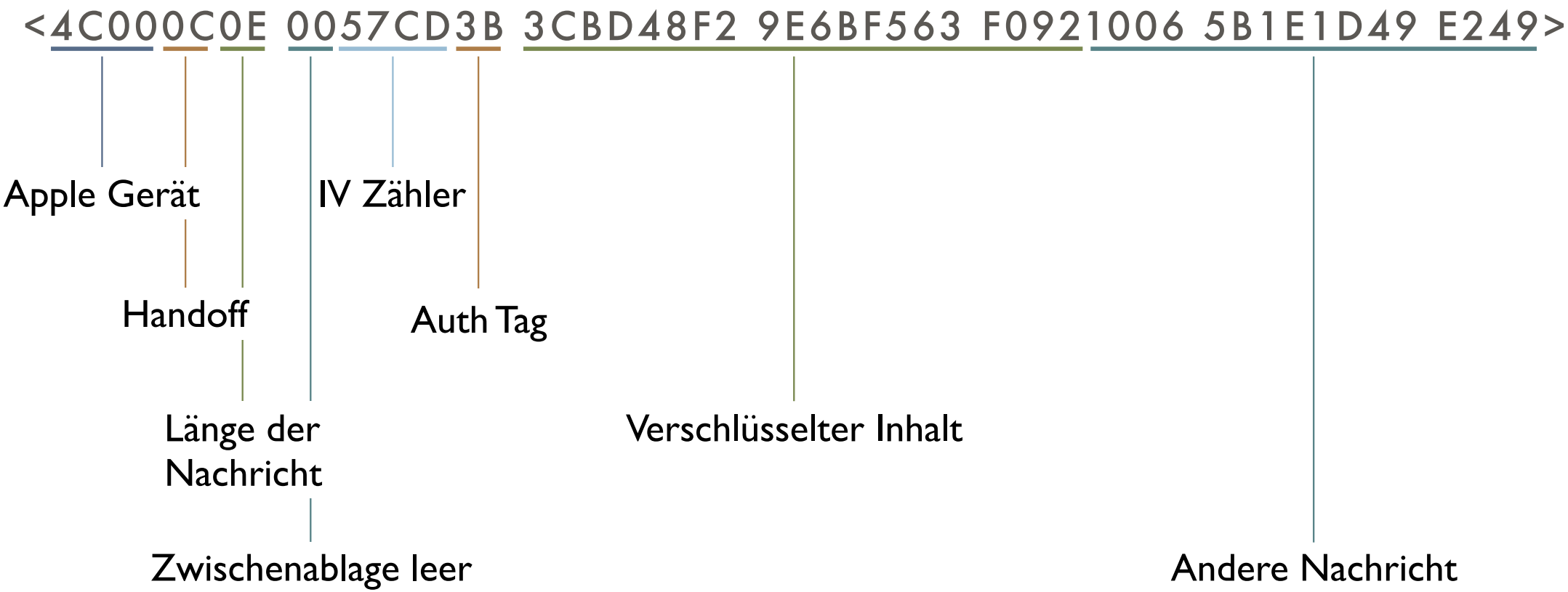
Protokoll Ablauf

Bluetooth Low Energy


09:41
All iCloud
Hallo Macoun

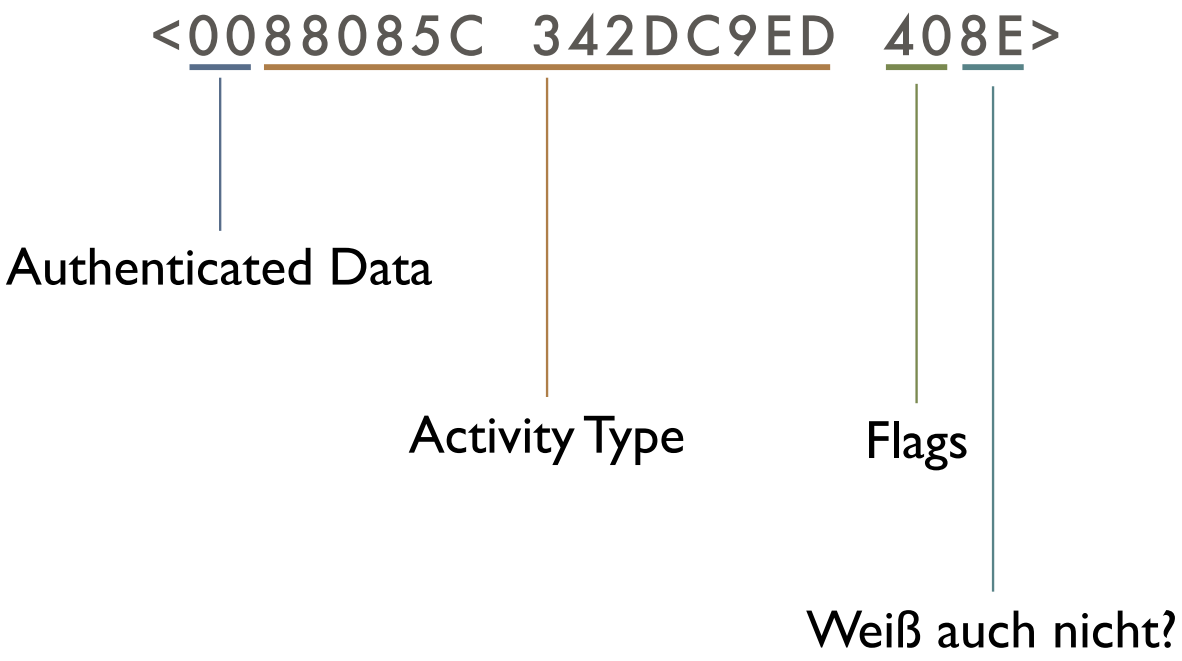
Bluetooth Low Energy

- Advertisement mit jeder Aktion
  - Text kopieren
  - Gerät entsperren
  - Handoff App verwenden
- Advertisments sind **öffentlich** aber **verschlüsselt**


<4C000C0E 0057CD3B 3CBD48F2 9E6BF563 F0921006 5B1E1D49 E249>
Apple Gerät
Handoff
Länge der Nachricht
Zwischenablage leer
IV Zähler
Auth Tag
Verschlüsselter Inhalt
Andere Nachricht

BLE Verschlüsselung

- AES - GCM
  - 256-bit Schlüssel
  - 2 byte Counter
  - 1 byte Authentication Tag
- Schlüssel liegen in der Login-Keychain


<0088085C 342DC9ED 408E>
Authenticated Data
Activity Type
Flags
Weiß auch nicht?

Activity Type

```
let u = NSUserActivity(activityType:“de.macoun.handoff”)

u.isEligibleForHandoff = true
```

Activity Type

88085C 342DC9ED → “com.apple.notes.activity.edit-note”

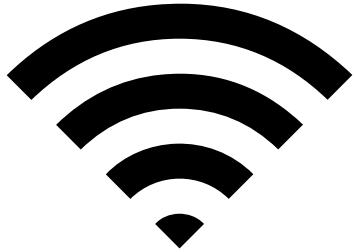
“com.apple.Notes”

Handoff Flags

flags & 0x1 != 0	Beinhaltet URL - Browser
flags & 0x2 != 0	Datei URL
flags & 0x4 != 0	Cloud Docs URL
flags & 0x8 != 0	Universal Clipboard verfügbar
flags & 0x10 != 0	Universal Clipboard Version Bit
flags & 0x20 != 0	Activity Auto Pull - Automatisches Laden

Demo

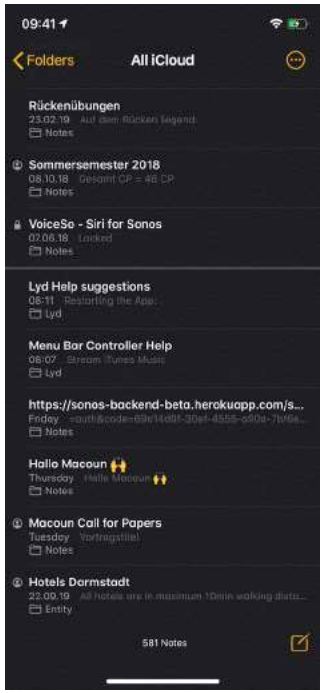
WLAN



Schlüsselaustausch

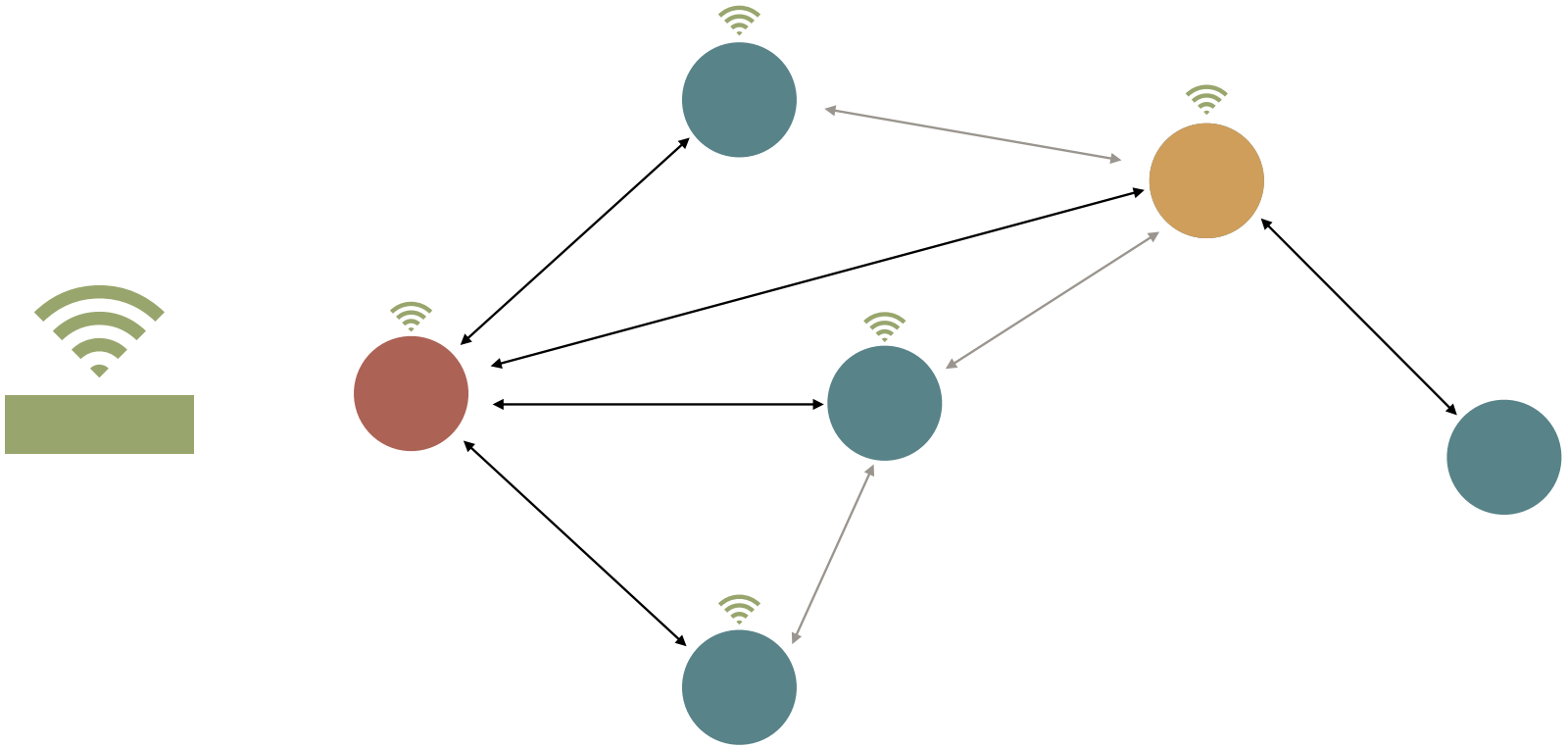
Anfrage für Zwischenablage

Daten aus Zwischenablage



Apple Wireless Direct Link (AWDL)

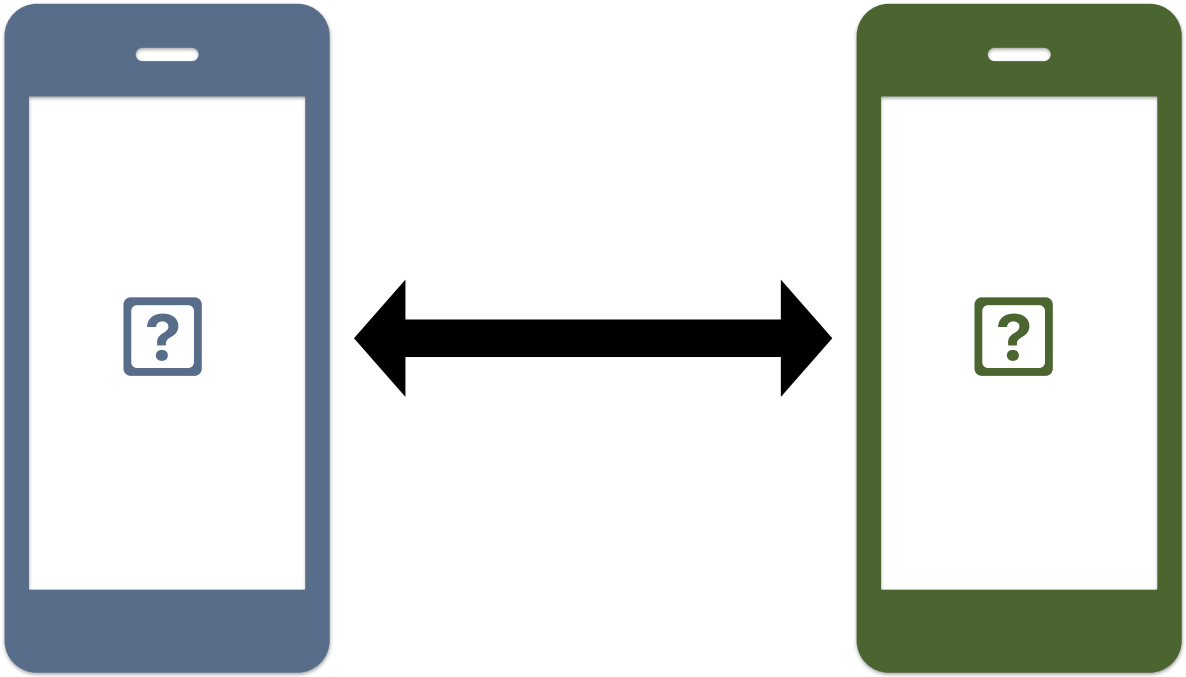
- Parallel zur bestehenden WLAN Verbindung
- Peer-to-Peer Verbindung mit mehreren Geräten
- Ein Master pro Netzwerk
  - Mehrere Slaves möglich
  - Multi Hop Netzwerke möglich



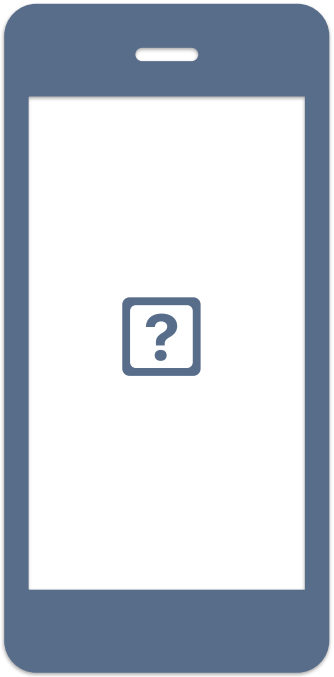
Bonjour

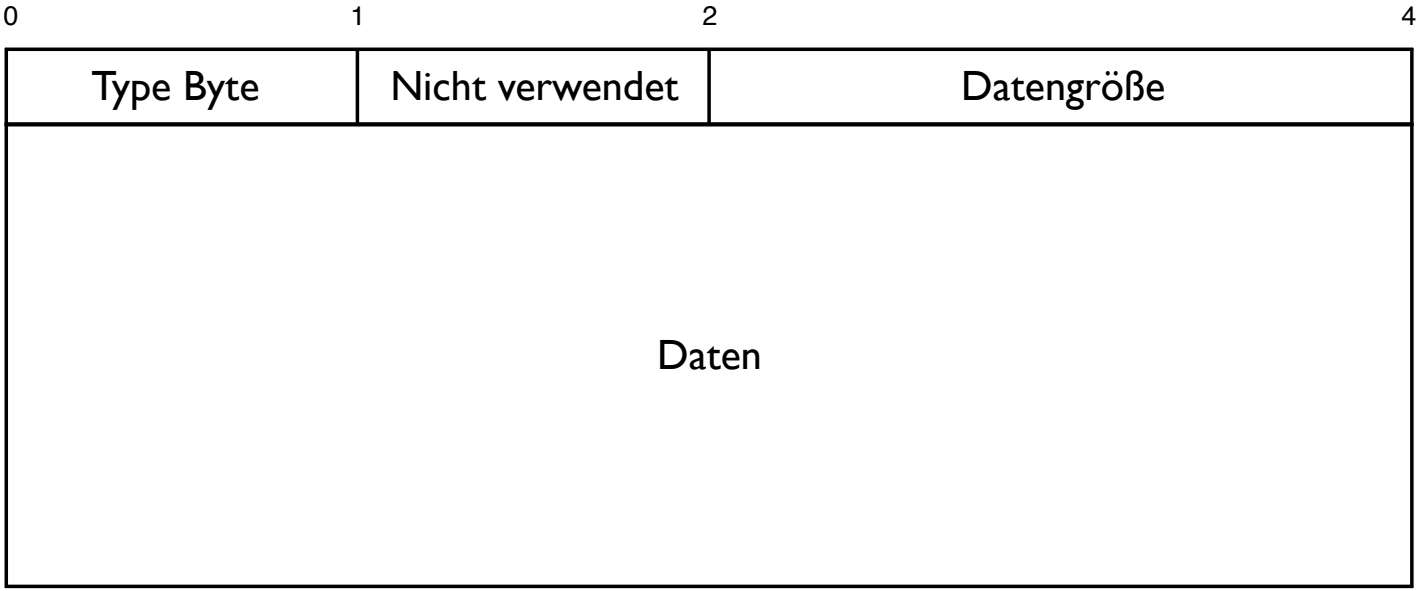
clink-13ecb3b507a5._companion-link._tcp.local: type SRV, class IN, cache flush, priority 0, weight 0, port 51306, target Alexanders-iPad.local

TCP Socket

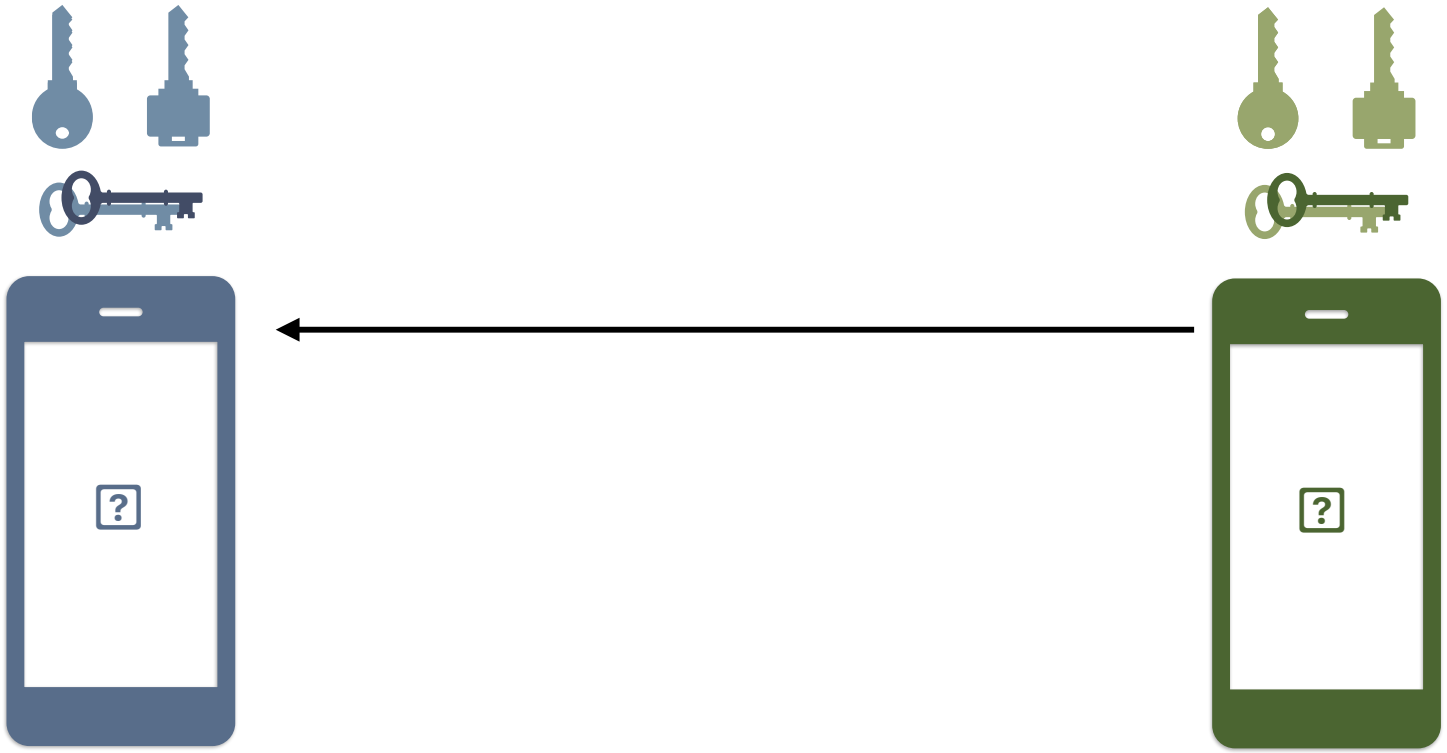


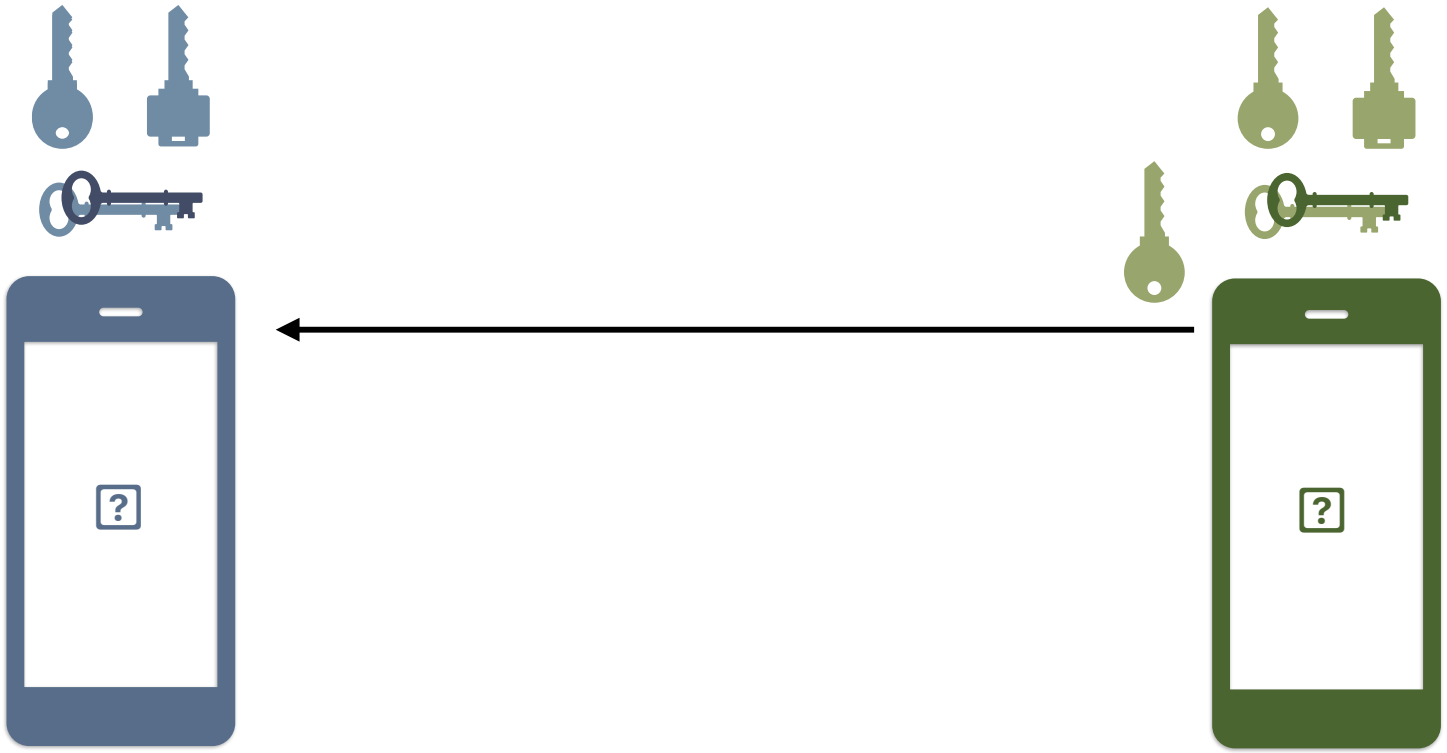
Socket Nachrichten

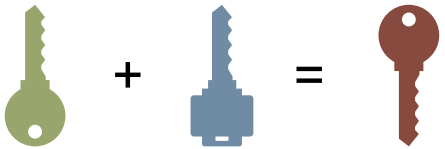


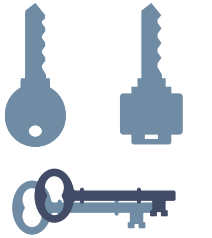


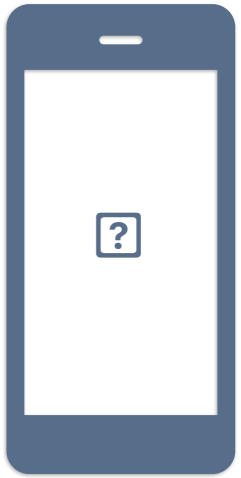
Schlüsselaustausch

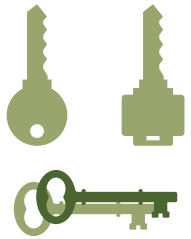


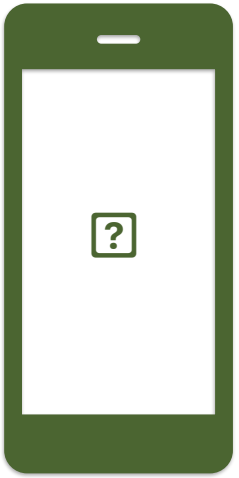


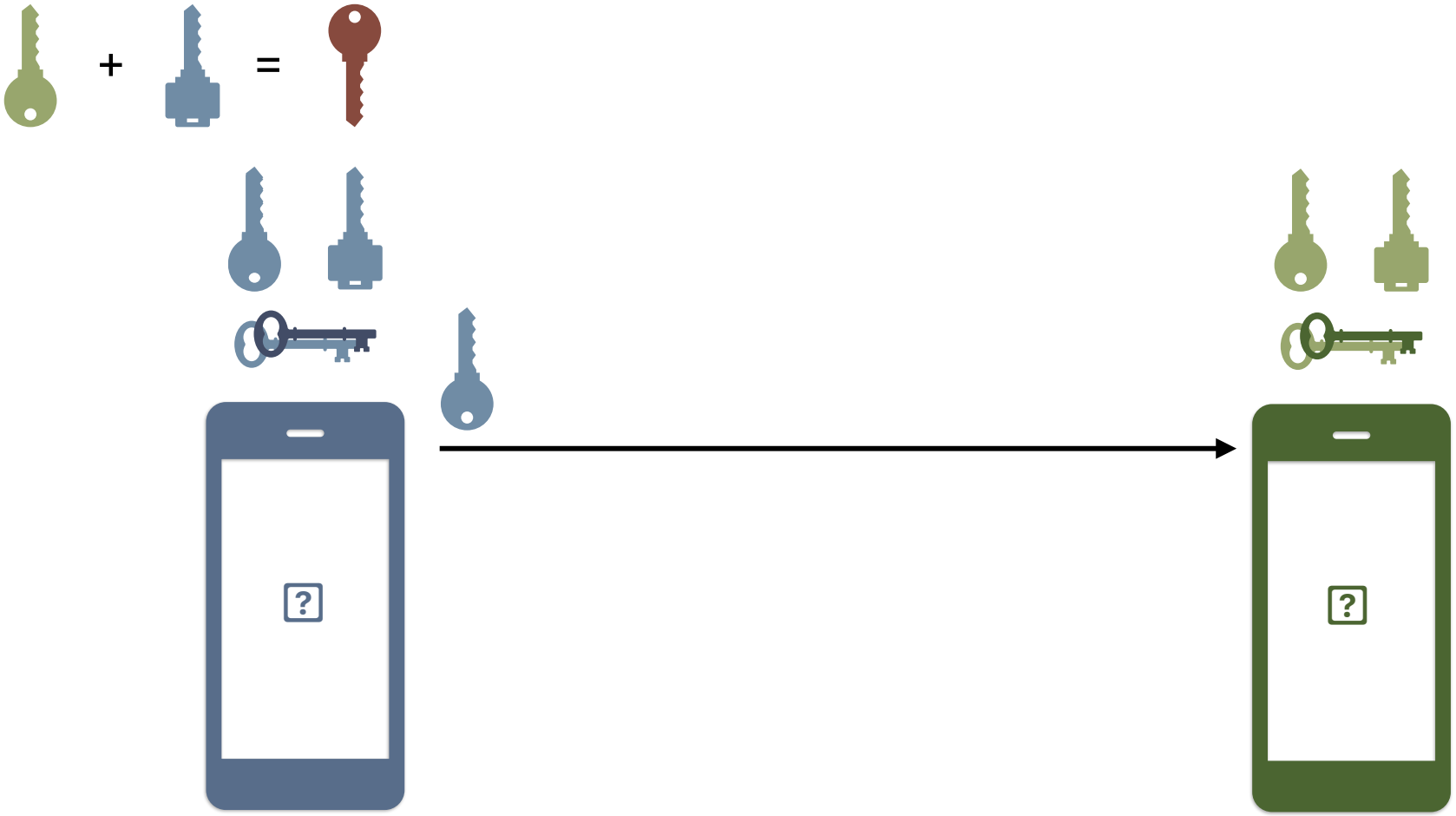


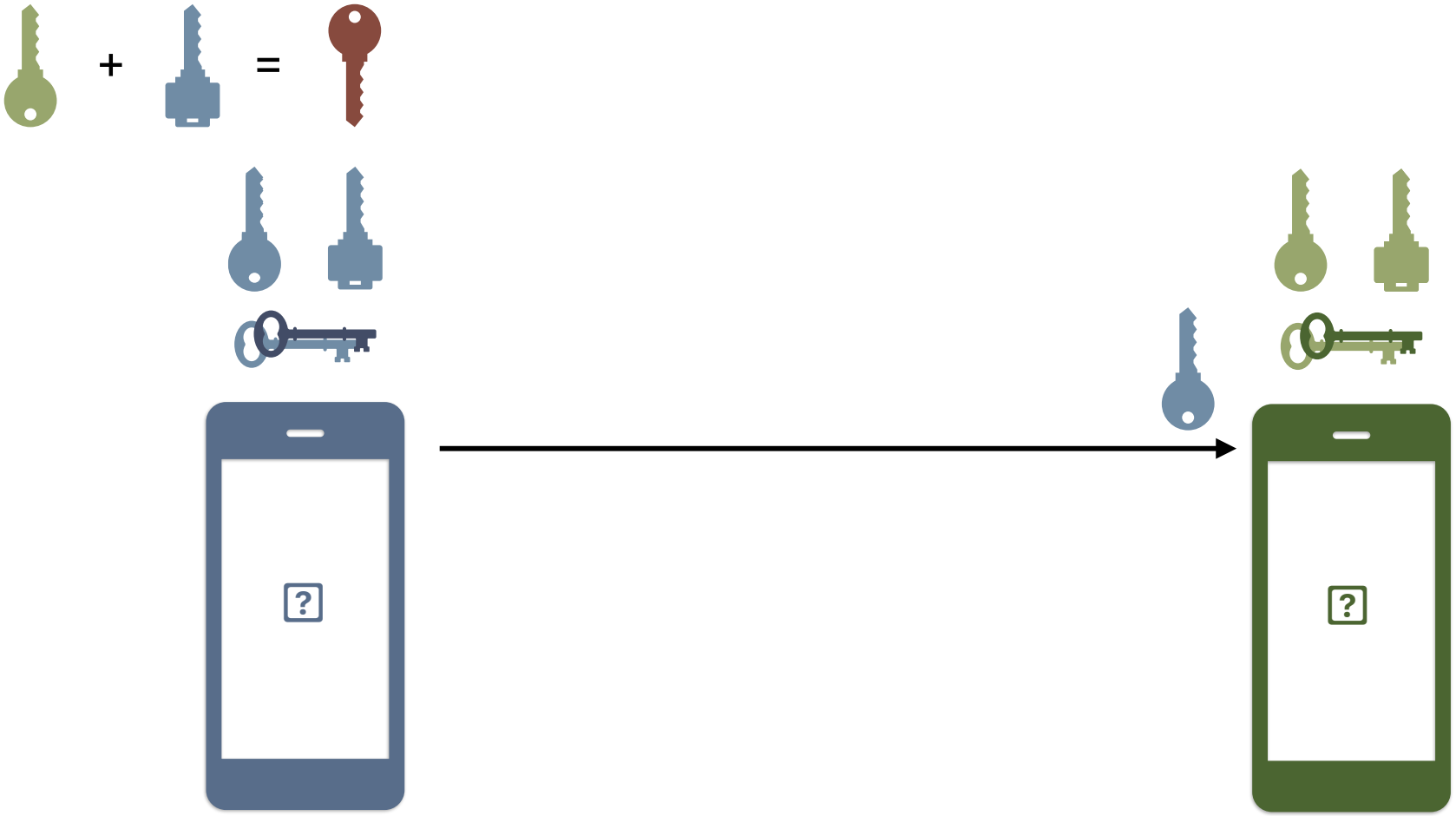


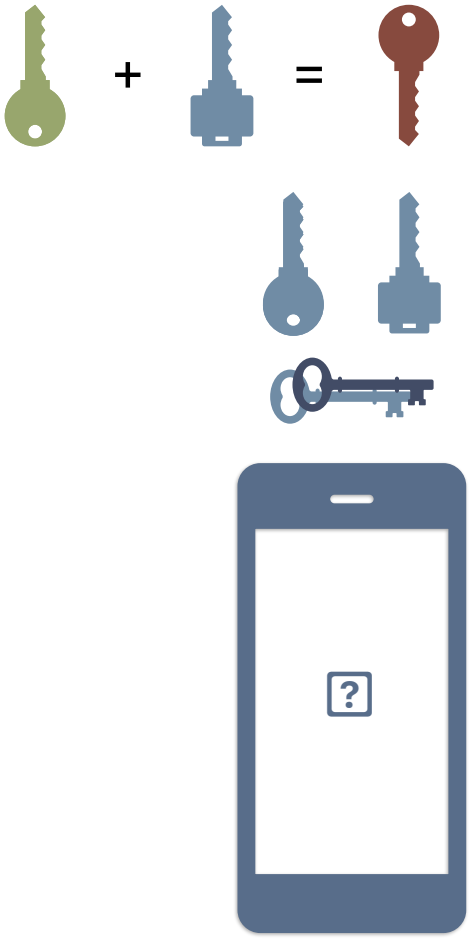


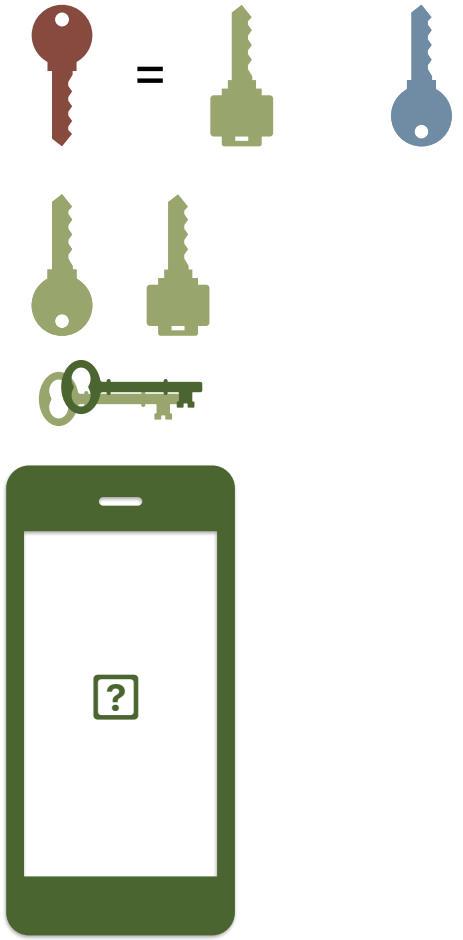


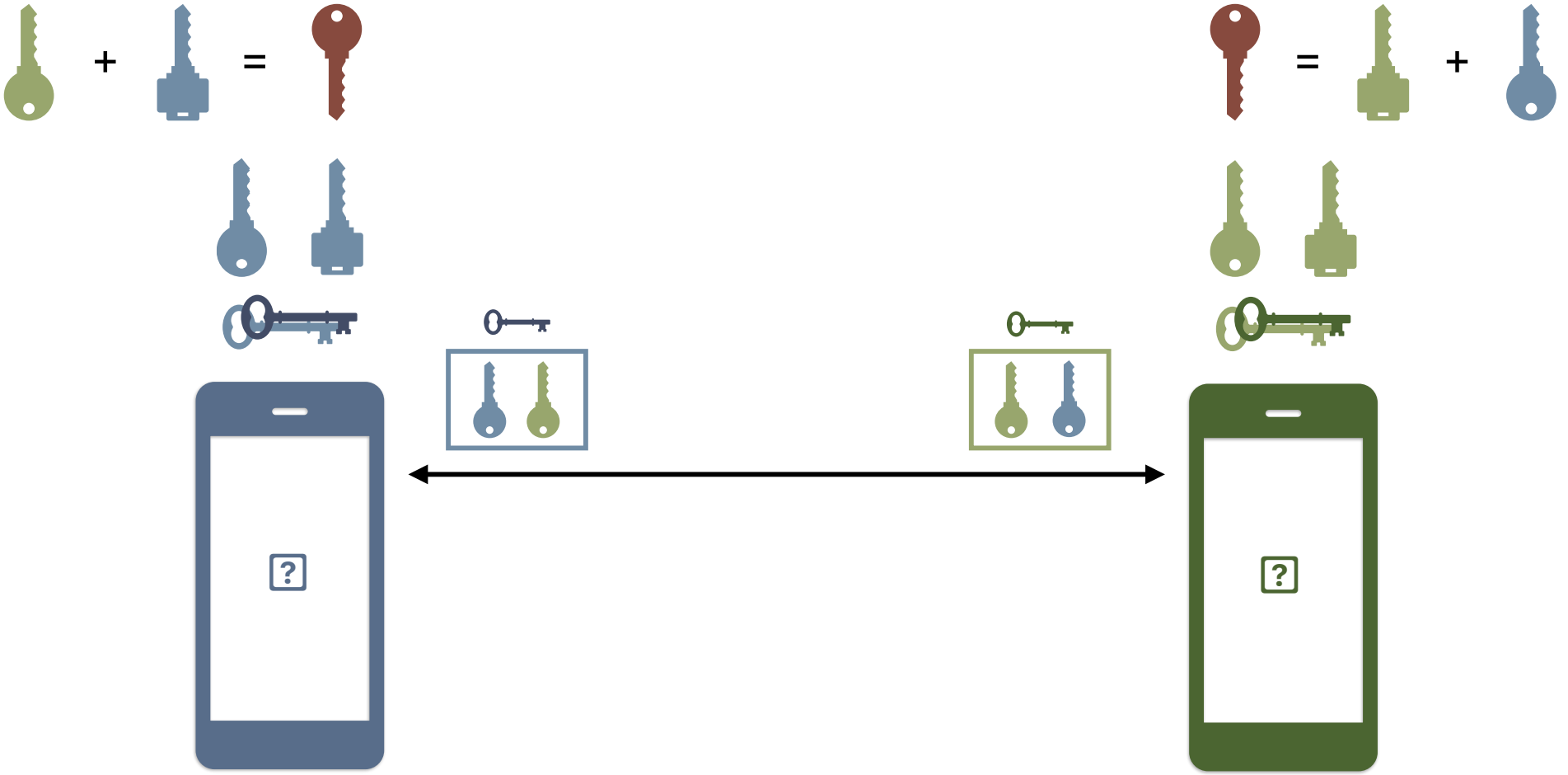


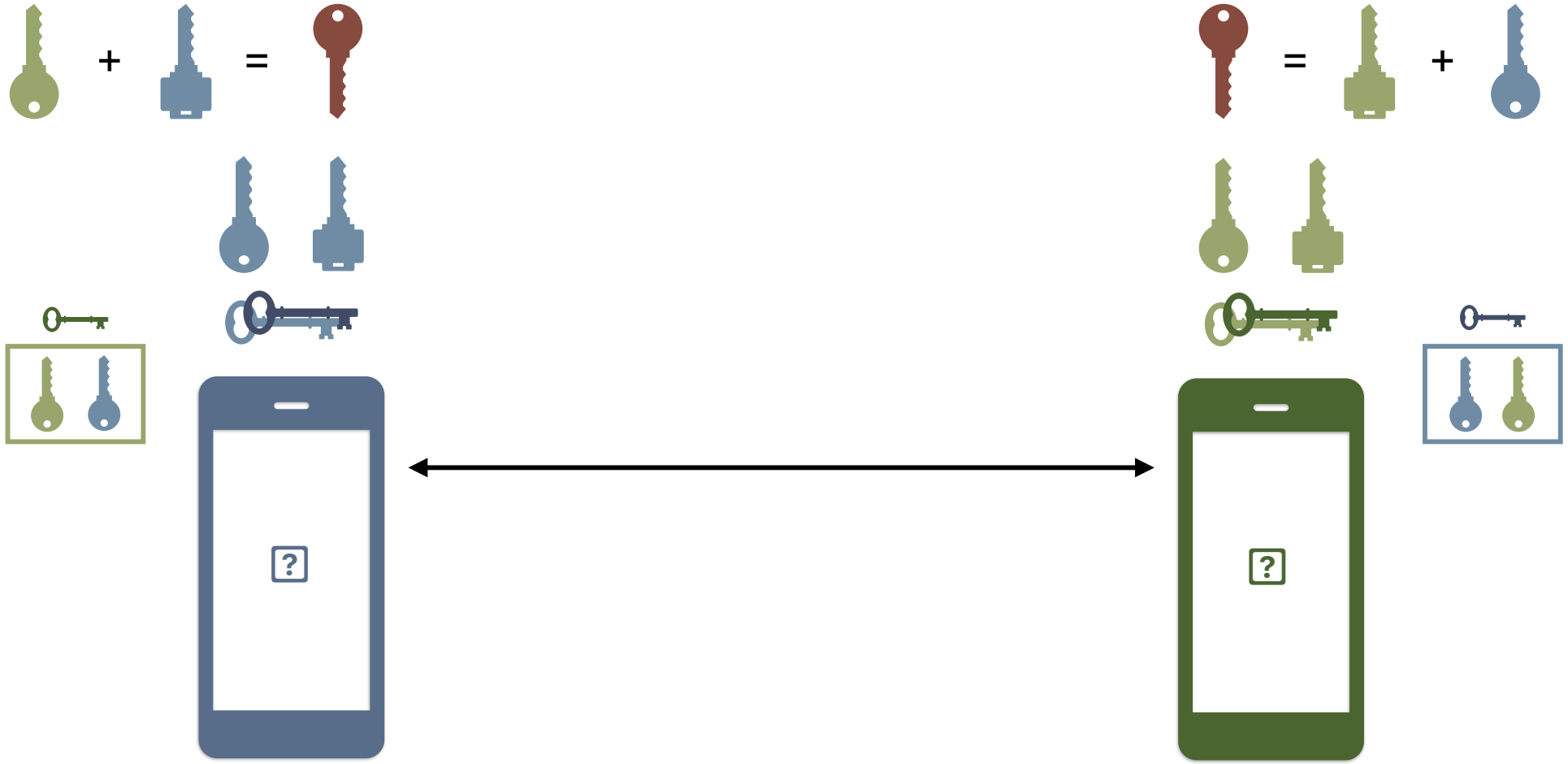




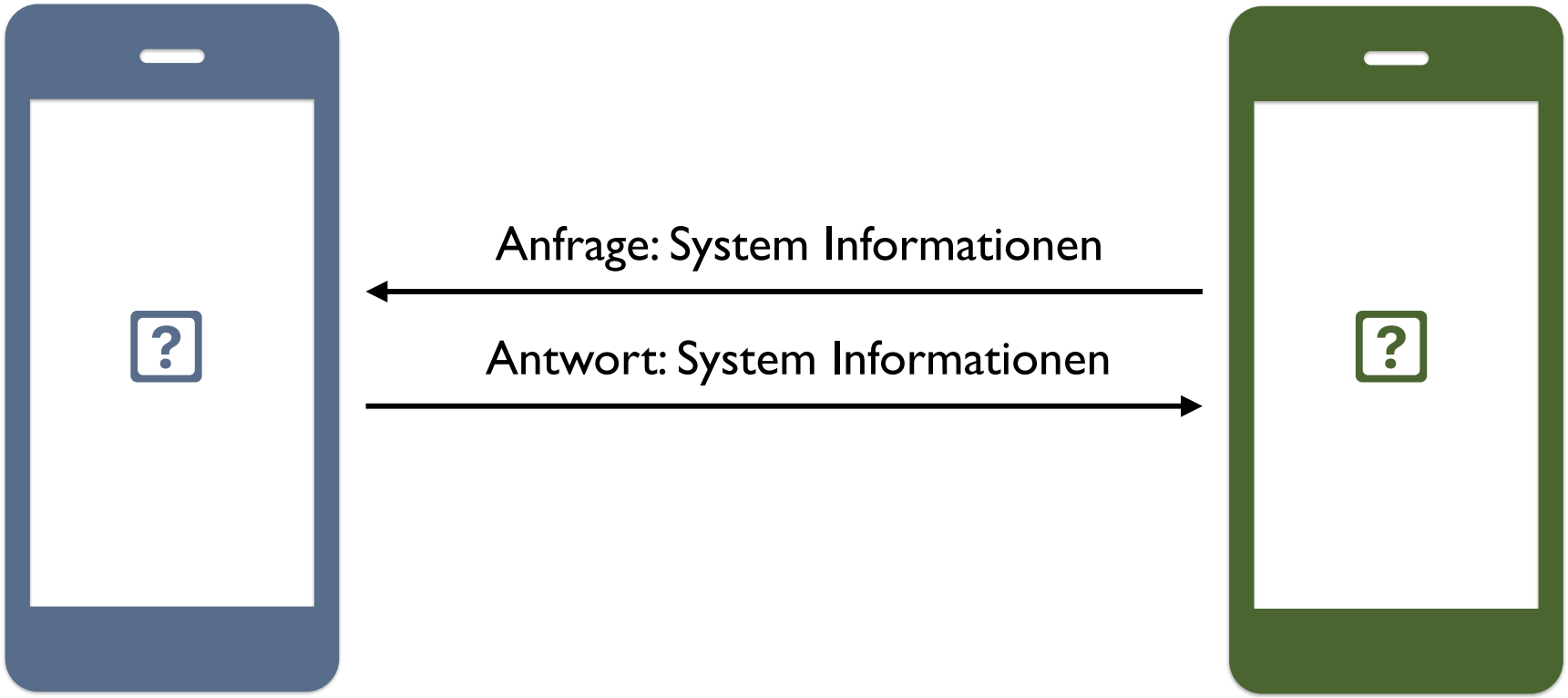


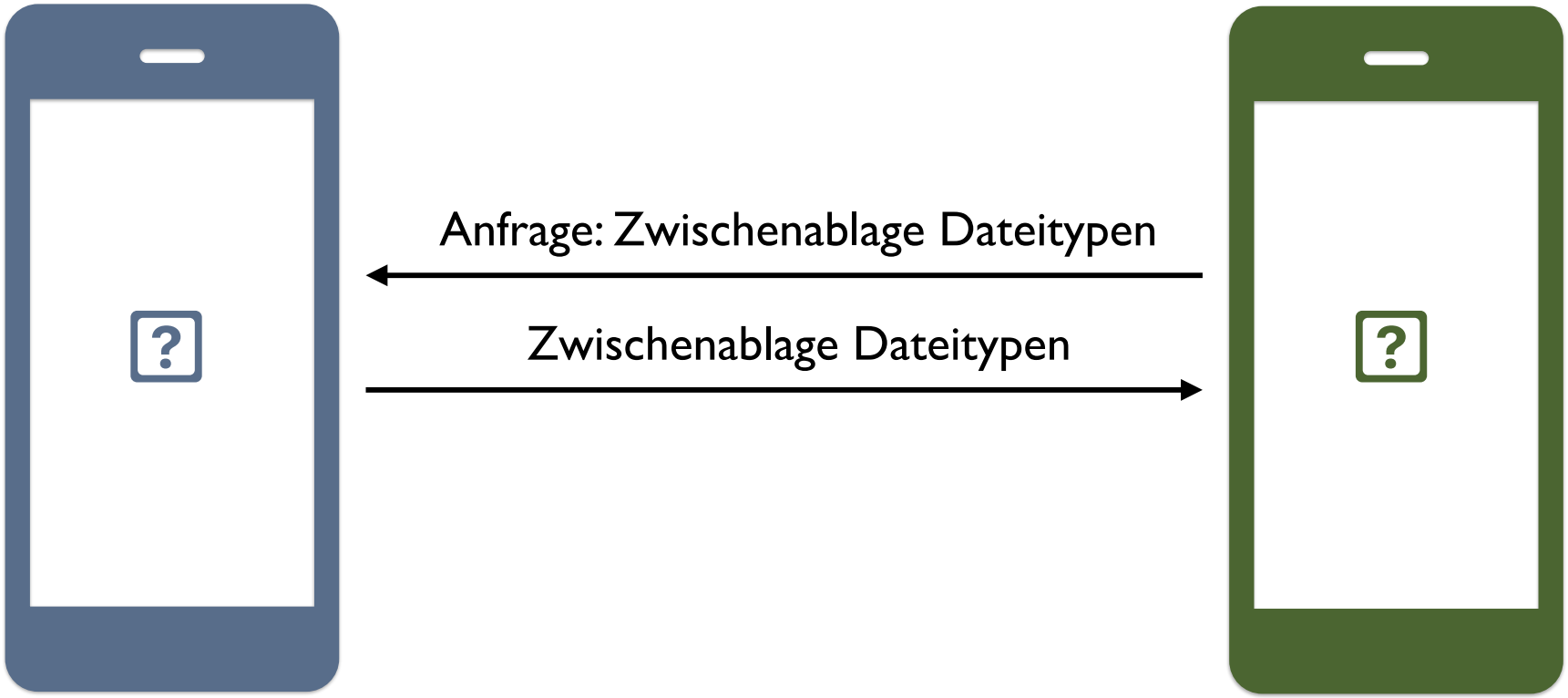






Daten Übertragung

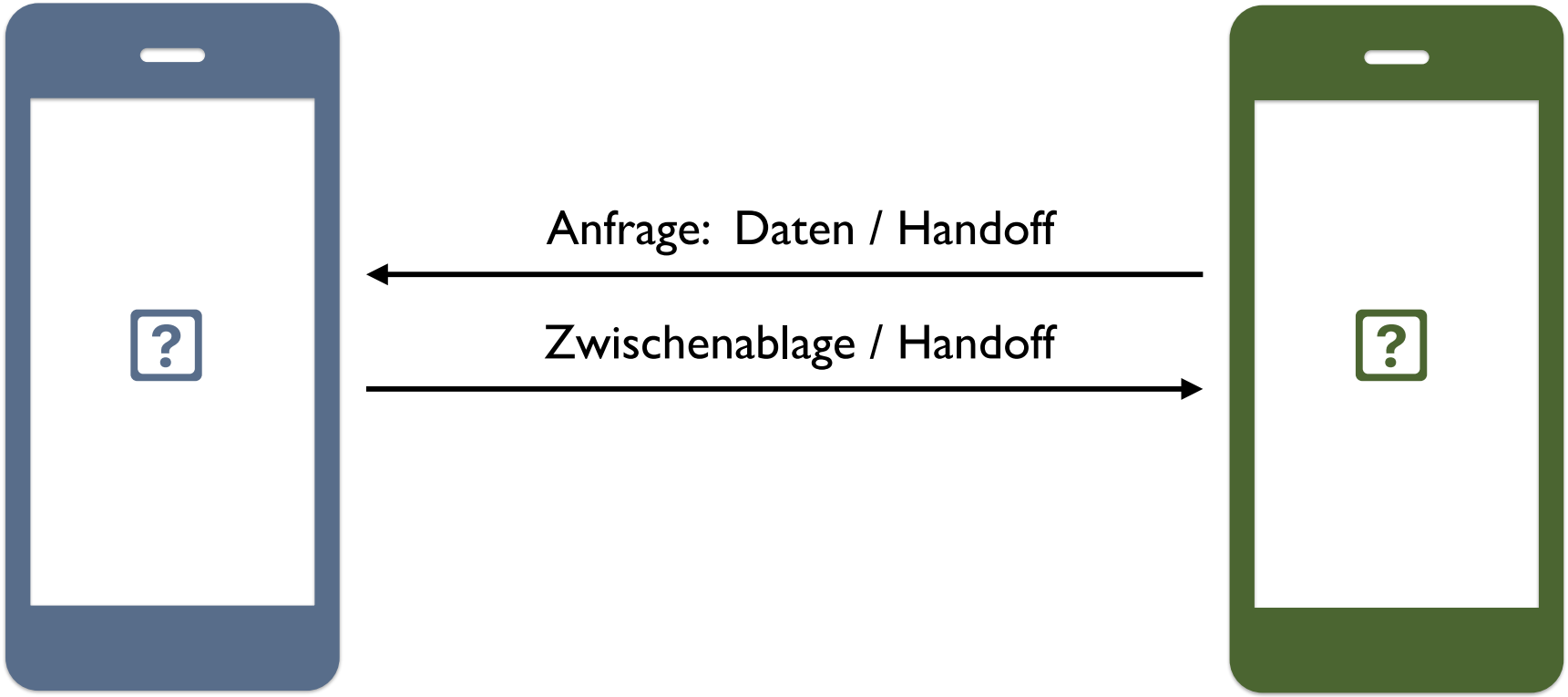

Anfrage: System Informationen
Antwort: System Informationen


Anfrage: Zwischenablage Dateitypen
Zwischenablage Dateitypen

Dateitypen

public.utf8-plain-text	UTF-8 enkodierter Text ohne Formatierung
com.apple.icns	Bild im icns Icon format
public.file-url	Datei
public.png	Eine PNG Bilddatei

Datenübertragung



Handoff Inhalt der Daten

```
let u = NSUserActivity(activityType:“de.macoun.handoff.talk”)

u.isEligibleForHandoff = true

u.userInfo = [“talkId”:“talk1234”]
```

Universal Clipboard Daten

public.utf8-plain-text

com.apple.notes.richtext

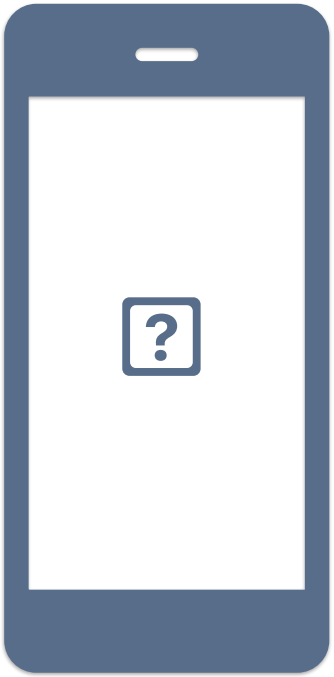
com.apple.traditional-mac-plain-text

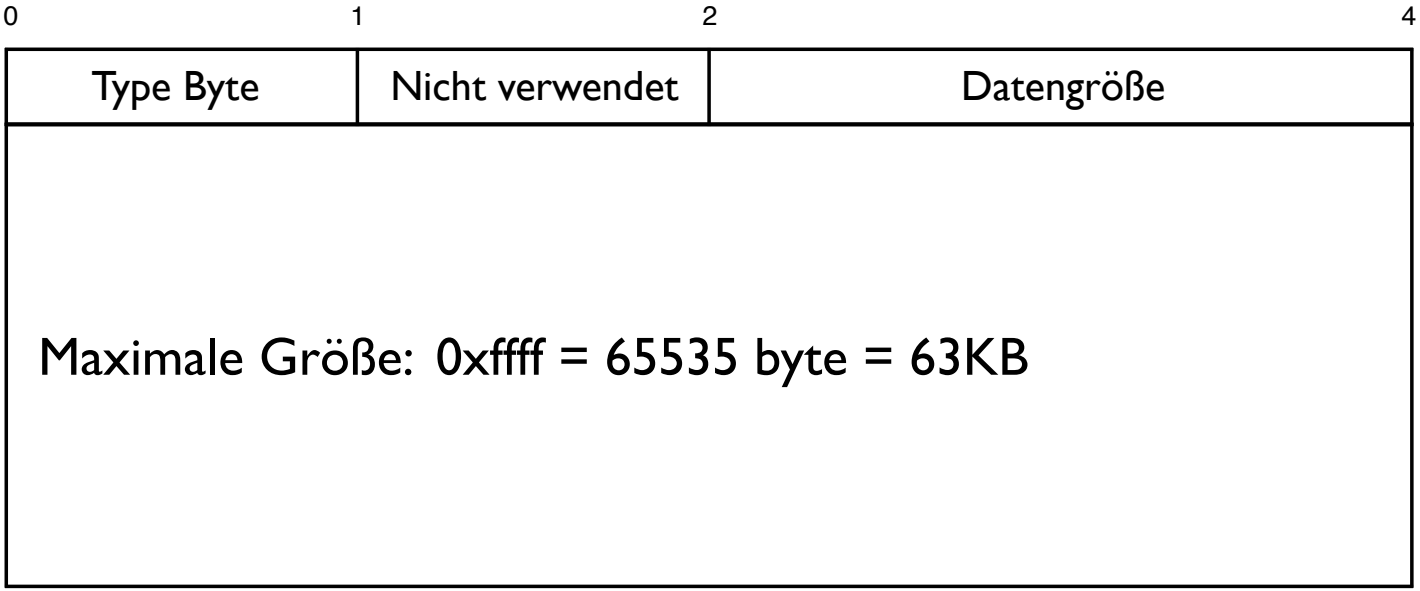
public.utf16-external-plain-text

public.rtf

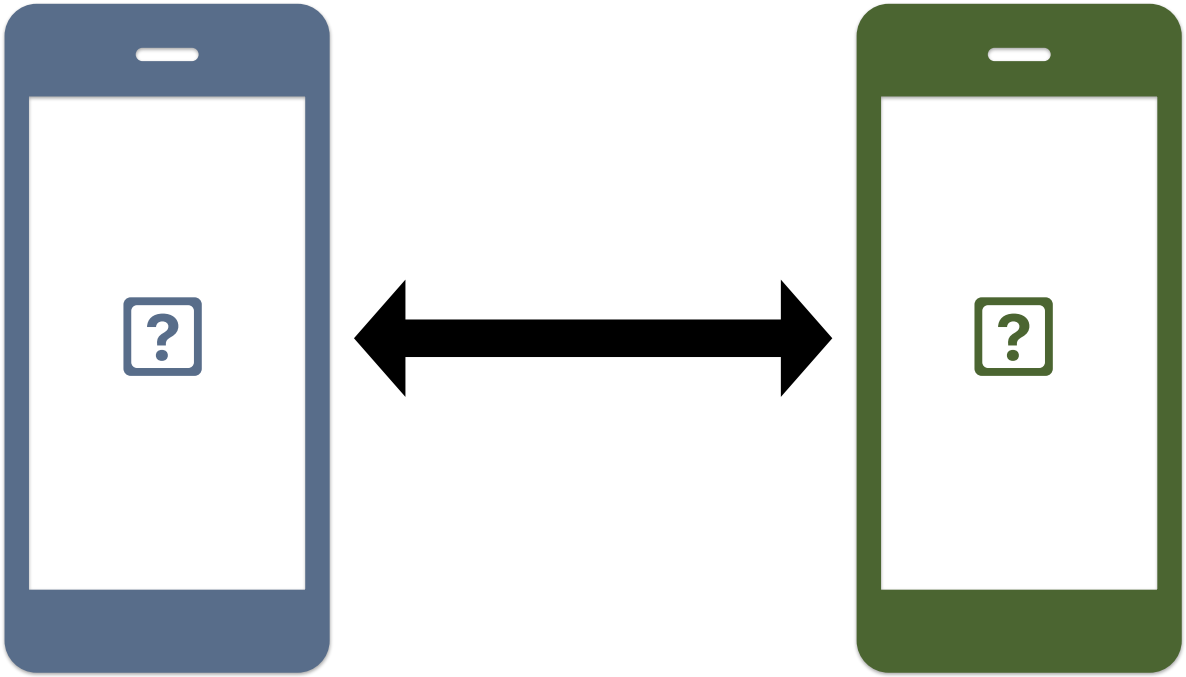
public.text

Socket Nachrichten

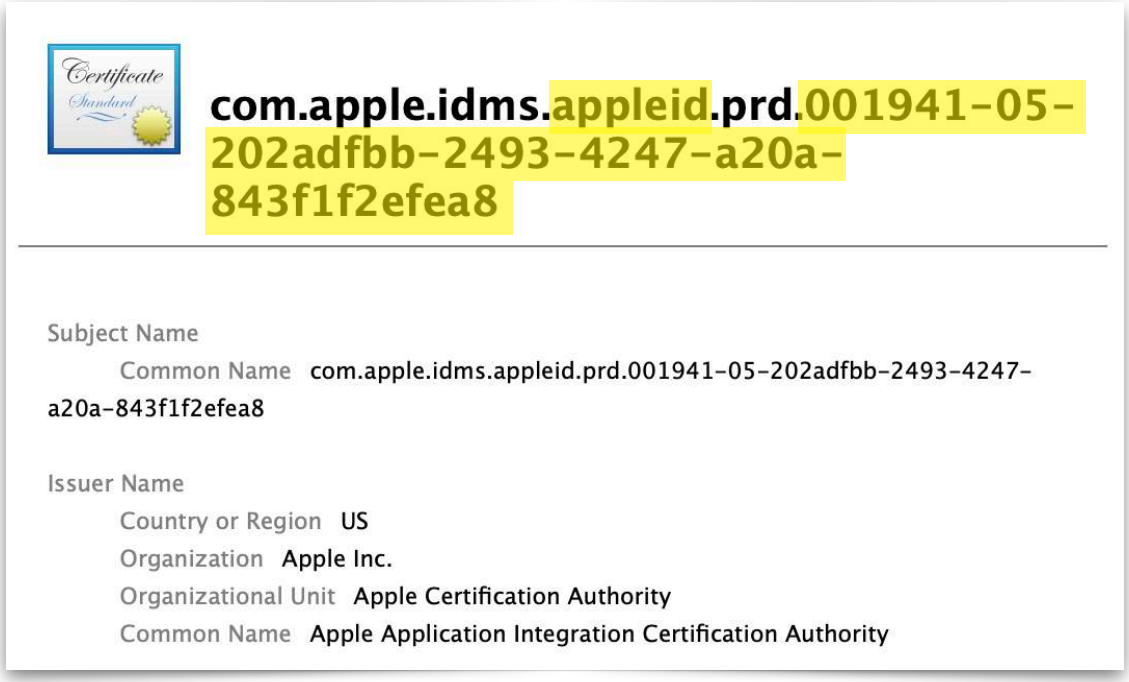


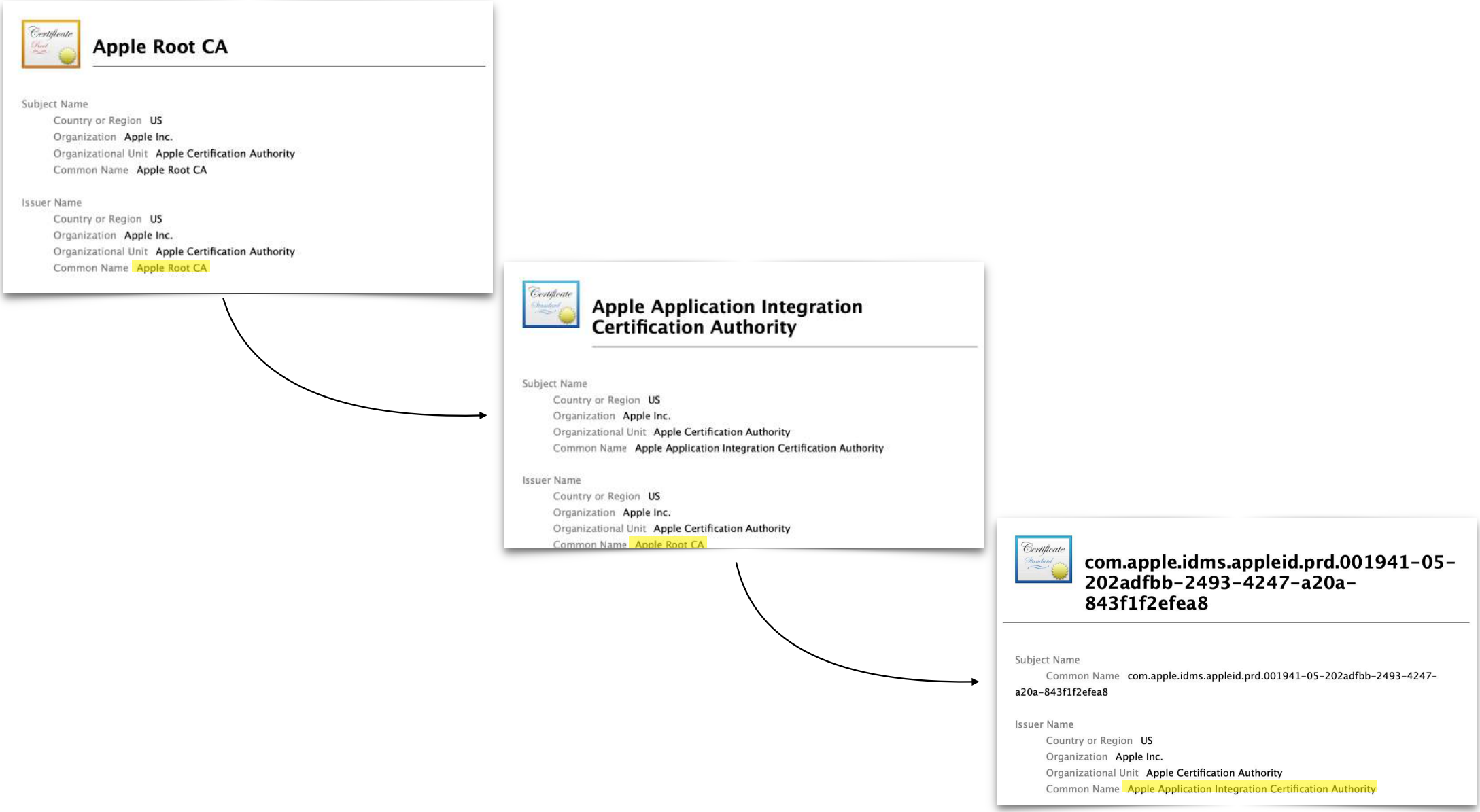


TLS Socket



TLS Zertifikate




Apple Root CA
Subject Name
Country or Region US
Organization Apple Inc.
Organizational Unit Apple Certification Authority
Common Name Apple Root CA
Issuer Name
Country or Region US
Organization Apple Inc.
Organizational Unit Apple Certification Authority
Common Name Apple Root CA
Apple Application Integration Certification Authority
Subject Name
Country or Region US
Organization Apple Inc.
Organizational Unit Apple Certification Authority
Common Name Apple Application Integration Certification Authority
Issuer Name
Country or Region US
Organization Apple Inc.
Organizational Unit Apple Certification Authority
Common Name Apple Root CA
com.apple.idms.appleid.prd.001941-05-202adfbb-2493-4247-a20a-843f1f2efea8
Subject Name
Common Name com.apple.idms.appleid.prd.001941-05-202adfbb-2493-4247-a20a-843f1f2efea8
Issuer Name
Country or Region US
Organization Apple Inc.
Organizational Unit Apple Certification Authority
Common Name Apple Application Integration Certification Authority

TLS Nachrichten

- Nachrichten mit gleichem Inhalt
- Größeres Längenfeld erlaubt Daten bis 4GB
- Verschlüsselung über TLS

Evaluation

Hohe Komplexität

- 2 verschiedene Verschlüsselungsverfahren
- 2 verschiedene drahtlose Schnittstellen
- 3 verschiedene Daemons
- 5 verschiedene Frameworks
- 5 verschiedene Serialisierungs-Formate

Serialisierung

Serialisierung

- Anfällig für Angriffe von außen
- Modifikation von Längenfeldern
- Nicht repräsentierbare Zeichen
- Unbekannte Fehlerzustände

Versuchte Angriffe

- Fuzzing auf OPACK
  - Closed Source Serialisierung
  - Über 500.000.000 Testdaten
  - Soweit keine Sicherheitslücken

Schlüsselaustausch

- Gleiches Verfahren, wie in HomeKit
- Sehr große Ähnlichkeit zu TLS
- Hohe Sicherheit durch Elliptische Kurven und Diffie-Hellman
- Sicherheit hängt von der Sicherheit der Signaturschlüssel ab

Schlüsselaustausch

- Signaturschlüssel liegen innerhalb der iCloud Keychain
- Werden synchronisiert über iCloud
- Nutzer können nicht drauf zugreifen
- Ein kompromittiertes Gerät gefährdet alle iCloud Geräte

Versuchte Angriffe

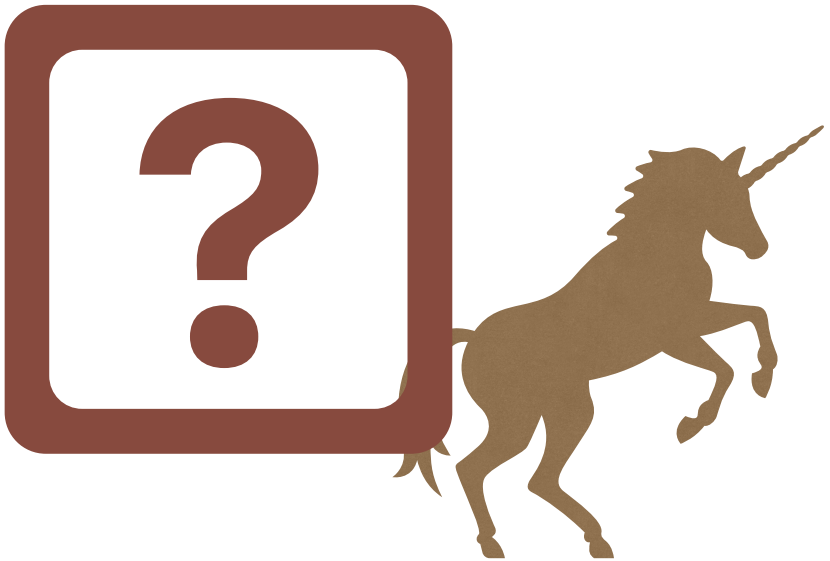
- Einpflegen eines gefälschten Schlüssels in die Keychain
- Nicht möglich ohne deaktivieren der Sicherheitsmaßnahmen
- Jailbreak öffnet die Keychain

Verschlüsselung

- Standard-Verfahren
- AES im Galois/Counter Mode
- ChaCha20 mit Poly1305

Fazit

Keine Magie?



Ist es sicher?

Vermutlich

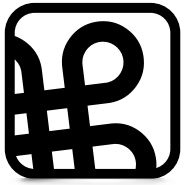
Wenn die Keychain hält

Das ungute Bauchgefühl bleibt

Fragen?

Vielen Dank

owlink.org



Macoun