Contents

cameoNet Security Whitepaper

Overview

cameoNet ist ein Multi-Plattform/Device/Identitäten Messenger. Mit cameoNet können Nutzer sicher vor Datenmißbrauch und ungewolltem Mitlesen von Dritten einfach kommunizieren. cameoNet ist offen für die leichte Einbindung von externen Kontakten (per Mail oder SMS) sondern legt auch den Quelltext vollständig

@TODO

Implementation Details

Source Code

Der vollständige Source Code steht bei github zur Verfügung:

https://github.com/memoConnect

Der Source Code des cameoNet Server ist in folgendem Repository zu finden:

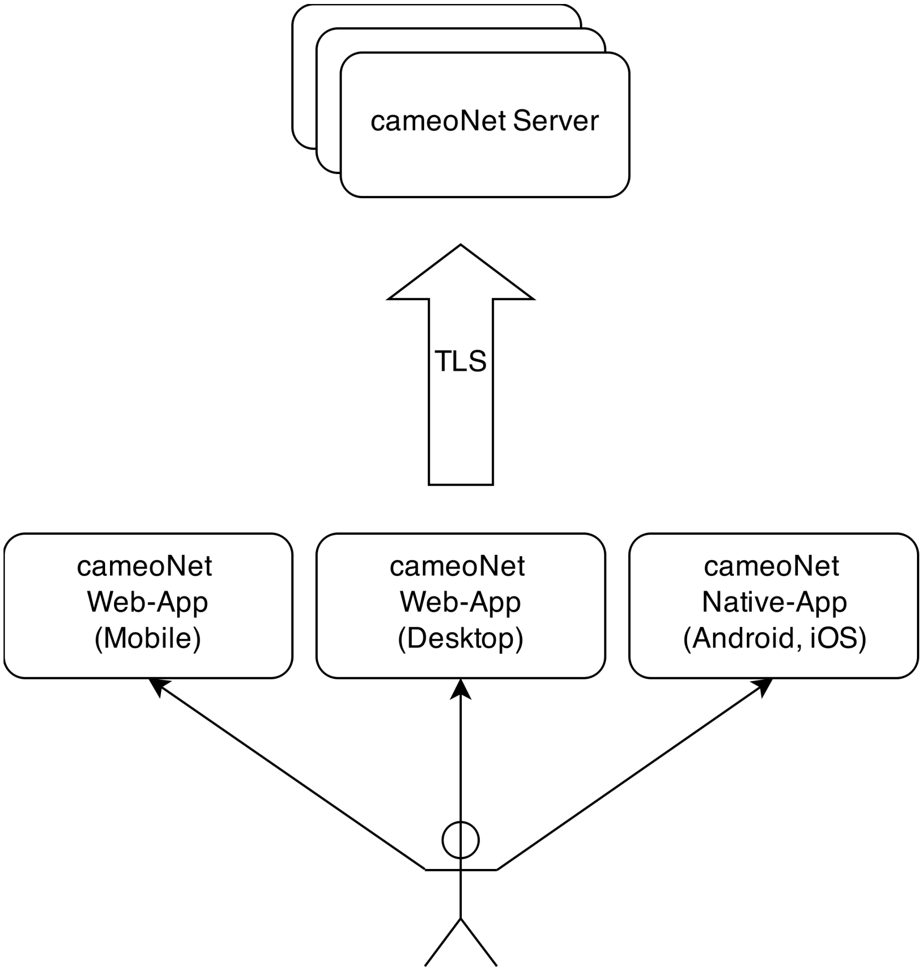
cameoNet Server
TLS
cameoNet Web-App (Mobile)
cameoNet Web-App (Desktop)
cameoNet Native-App (Android, iOS)

Figure 1: cameoNet Overview

https://github.com/memoConnect/cameoServer

Der Source Code des cameoNet Client ist in folgendem Repository zu finden:

https://github.com/memoConnect/cameoJSClient

Encryption Frameworks

@TODO

Transport Encryption

All communication between cameoNet Clients (Web and Apps) is protected by TLS.

Account/Identity Modell

Account

Each user has at least one account. cameoNet does nothing to avoid that users create more than one account. An account consists at least of a username and a password. The username must have at least 3 characters. A user hast at least one Identity per account. The first identity will be created during registration.

Identity

A user get's in touch with other users only through one of his identites. Each Identity has its own contacts/keys/talk. Each identity of a user is complete indepentent. Other users could not determine which identites belongs to which account.

Data Encryption

cameoNet uses AES and RSA encrption. AES will be used with a key length of 256 bit. RSA keys have at least a length of 2048 bit.

All messages and assets will be encrypted using AES. A rondom AES key will be created for each talk. All messages and assets of a talk will be encrypted with the same AES key.

The AES key will be encrypted with all public keys of the recipients. In the case Alice uses a smartphone and a PC and Bob uses a PC and a tablet the AES key will be encrpted 4 times. That makes it possible for Alice and Bob to read this talk on all their devices.

@TODO

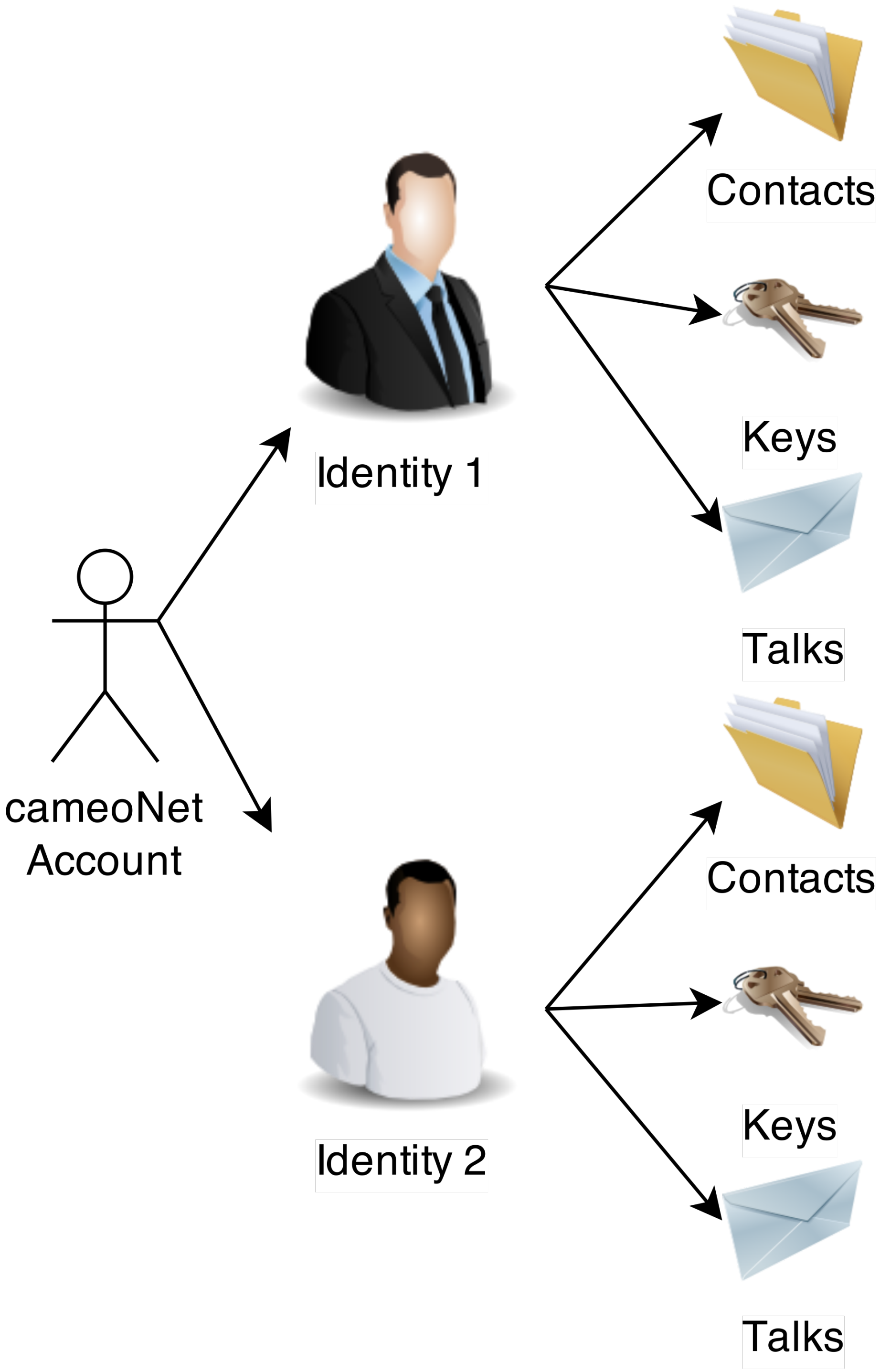

Figure 2: cameoNet Identitites

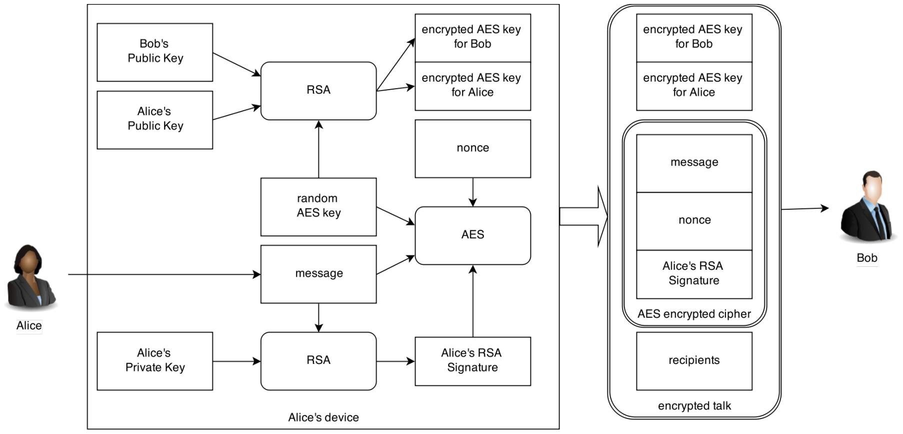

Figure 3: cameoNet Crypto System

Encryption Levels

@TODO

Authentication

Key authentication is used to establish trust between two keys. This is done between multiple keys of one identity and between keys of different identities.

The following is assumed before an authentication is started: * The public keys have been exchanged via an insecure channel * The cameoId of the owner of each key is known

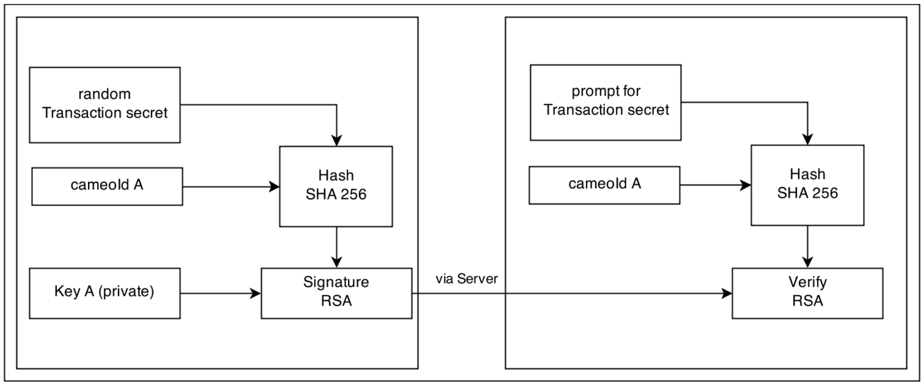

Figure 4: Handshake

When the authentication was successful the authenticated key will be signed. Future conversations with this key will be marked as trusted.

Authentication between Identites

@TODO

Random Numbers

@TODO