

A glowing blue circuit board with a central padlock and key icon. The padlock is open, and a bright light emanates from the keyhole, with a key visible inside. The circuit lines are intricate and glowing, creating a high-tech, digital atmosphere.

Steffen Dröbler

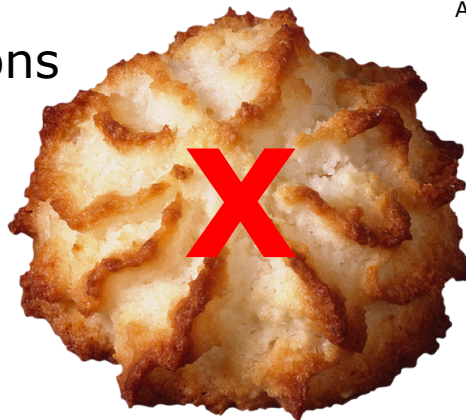
Macaroons

What are "Macaroons" and for what might they be useful?

09.03.2021

Abbildung 1: Makronen

Macarons



Macaroons



Abbildung 2: Macaroons



Macron

Abbildung 3: Emmanuel Macron

Problemstellung

- kontrolliertes Teilen in **dezentralisierten verteilten Systemen** (Cloud) basiert auf
 - HTTP-Cookies
 - Linksharing (per Mail o.Ä.)
- Problem
 - nicht „abhörsicher“
 - Registrierung und/oder Authentifizierung

Quelle: [1, 2]

Was sind Macaroons?


- Macaroons sind *bearer tokens* (Inhaber-Token)
 - Client übergibt Macaroon bei Request (vgl. Cookies)
- String aus characters ohne leerzeichen

```
MDAxY2xvY2F0aW9uIE9wdGlvbmFsLmVtcHR5CjAwMThpZGVudGlmawVyIGH \
sQ0krem1RCjAwMTVjawQgawlkOnBGTTA1MnJTCjAwMjFjawQgawQ6MjAwMj \
sxMDAxLDIwMDIsMDtwYXVsCjAwMjhjawQgYmVmb3JlOjIwMTktMDQtMTdUM \
Dk6NTE6MjIuODQwWgowMDE5Y2lkIGhvbWU6L1VzZXJzL3BhdWwKMdAyZnNp \
Z25hdHVyZSCT6Lea6oBIEpiF2K0sZ1FQvLeoXve_a3q38TZTBWhM1Qo
```

Abbildung 4: Macaroon-Token

Quelle: [3]

Bestandteile eines Macaroons

- key:value Paare
 - identifier → Name des Macaroon
 - location → URL
 - caveats → Bedingungen, Einschränkungen
 - resources
 - activity (read, write, download, ...)
 - ...
 - 3rd-party-caveats
 - signature → to verify that the macaroon has not been modified
- 
- können von jedem Inhaber des Macaroons hinzugefügt werden
 - können nur vom Ersteller entfernt werden
 - **alle** caveats müssen erfüllt sein

Quelle: [4, 5]

3rd-Party-Caveat

- zweiter Macaroon eines vertrauenswürdigen Services
 - alle caveats müssen erfüllt sein
- i.d.R. wird dadurch Authentifizierung delegiert
- weitere Einschränkungen addiert, bspw:
 - Mitglied einer Gruppe
 - bestimmte Zeit gültig

Quelle: [4]

Verschlüsselung eines Macaroons

- verketteter Message Authentication Code
 - $\text{signatur}_1 = \text{HMAC}(\text{key}, \text{id})$
 - $\text{signatur}_n = \text{HMAC}(\text{signatur}_{(n-1)}, \text{'Einschränkung'})$
- Verschlüsselungsmagie

Quelle: [5]

Ein Beispiel

- zwei Macaroons
- limitierte Zeit
- read
- authentication mit 3rd-party-Macaroon

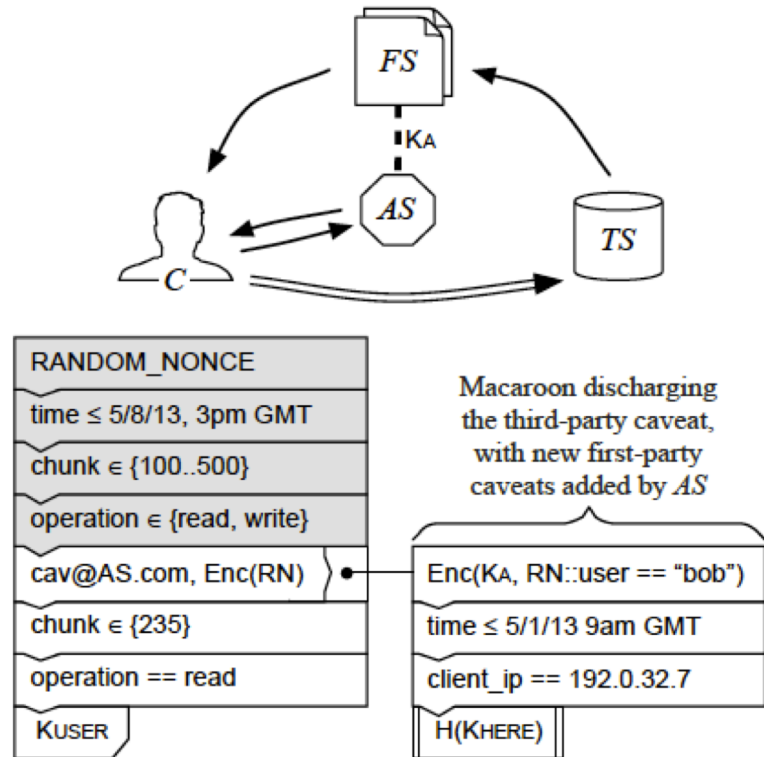


Abbildung 5: Macaroon Request-Circle

Quelle: [1]

Vorteile von Macaroons

- **dezentralisierten verteilten Systemen – Cloud**
- Teilen von Ressourcen mit (sehr präzise) bestimmten Gruppen von Nutzern
 - durch 3rd Party Caveats
- keine wesentlichen Veränderungen des bisherigen Workflows
 - → keine Registrierung bei neuem Cloud-Anbieter

Quelle: [1, 2]

Warum „Macaroons“



identifizier



Caveat1



Caveat2



Caveat3

...



signature

Quelle: [6]

eigene Darstellung nach Abbildung 2

Fragen?

Abbildungsverzeichniss

Abbildung 1: Makronen, Bildquelle: <https://pixabay.com/de/photos/makrone-essen-weihnacht-backen-1680701/> [aufgerufen am 05.03.2021]

Abbildung 2: Macaroons, Bildquelle: <http://pngimg.com/image/74086> [aufgerufen am 05.03.2020]

Abbildung 3: Emmanuel Macron, Bildquelle: <https://www.hiclipart.com/free-transparent-background-png-clipart-zkjcw/download> [aufgerufen am 05.03.2021]

Abbildung 4: Macaroon-Token, Bildquelle: <https://dcache.org/old/manuals/UserGuide-7.0/macaroons.shtml> [aufgerufen am 07.03.2020]

Abbildung 5: Request-Circle, [1]

Literatur

- [1] Birgisson, A.; Politz, J.G.; Erlingsson, U.; Taly, A.; Vrabie, M.; Lentczner, M. *Macaroons: Cookies with Contextual Caveats for Decentralize Authorization in the Cloud*; Network and Distributed System Security Symposium, Internet Society: Reston, VA, USA, 2014. Link: <https://storage.googleapis.com/pub-tools-public-publication-data/pdf/41892.pdf> [aufgerufen am 01.03.2021]
- [2] Erlingsson, Ú.: *Repost: Macaroons: Cookies with Contextual Caveats for Decentralized Authorization in the Cloud*. YouTube. uploaded by Jay Wineinger [21.04.2017]. Link: https://www.youtube.com/watch?v=CGBZO5n_SUg [aufgerufen am 01.03.2020]
- [3] dCache.org. *CHAPTER 1. UNDERSTANDING MACAROONS*. Link: <https://github.com/dCache/dcache/blob/7.0/docs/UserGuide/src/main/markdown/macaroons.md> [aufgerufen am 07.03.2020]
- [4] Escrive, R. *My First Macaroon: A New Way to do Authorization*. 2014. Link: <https://hackingdistributed.com/2014/05/21/my-first-macaroon/> [aufgerufen am 07.03.2020]
- [5] Cordell, E. *Macaroons 101: Contextual Confinement*. Elegant authorization, for a more civilized age. 2015. Link: <https://evancordell.com/2015/09/27/macaroons-101-contextual-confinement.html> [aufgerufen am 08.03.2020]