TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Institut für Systemarchitektur, Lehrstuhl für Datenschutz und Datensicherheit

Beweise für die Kellertür

Die Tür die nix weiß!

Benjamin Kellermann

Wien, 15. November 2008

2nd level Anforderungen

„must-have“

- keine Überwachung

2nd level Anforderungen

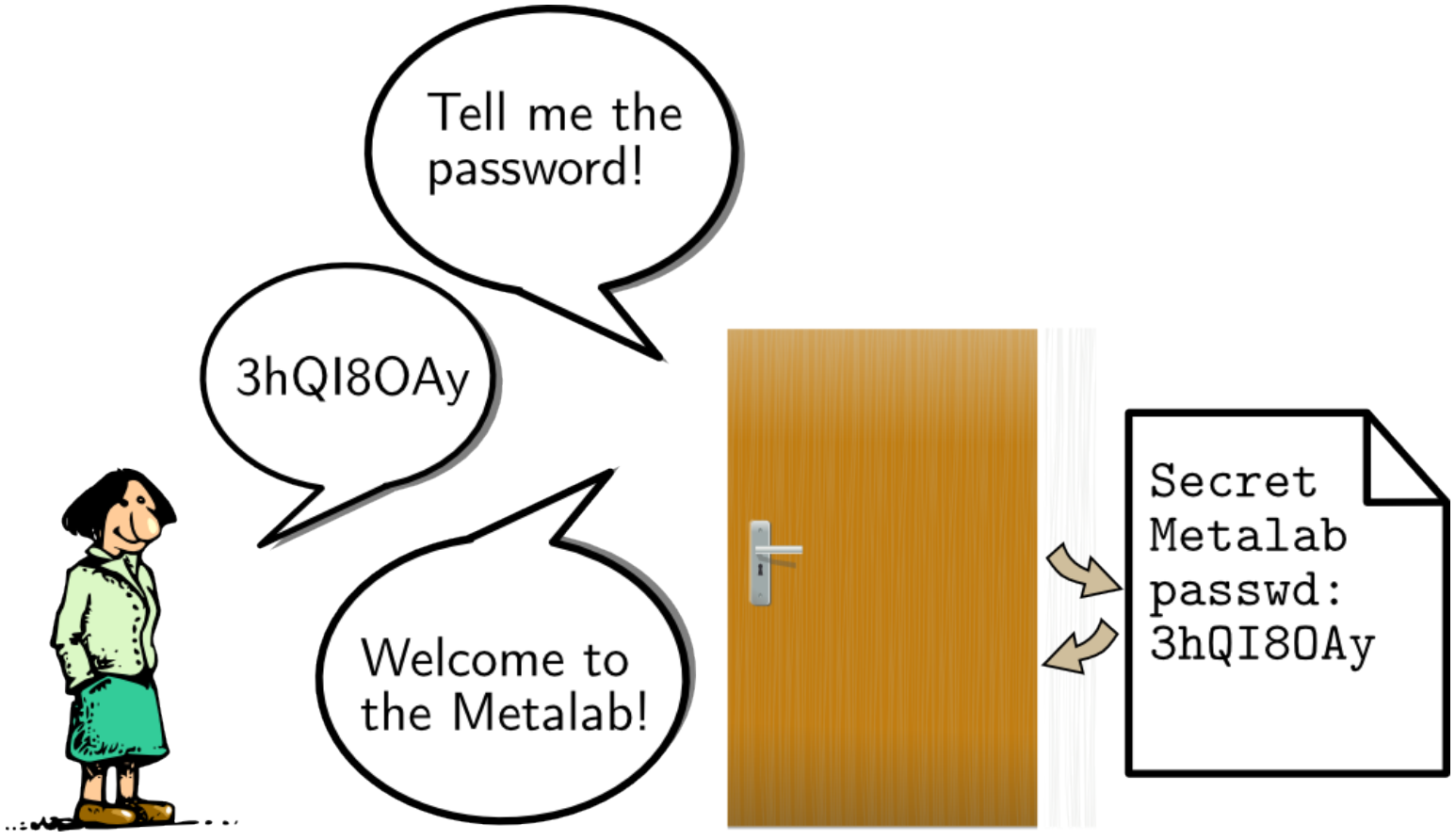
„must-have“

- keine Überwachung

„nice-to-have“

- einzelne User sperren
- keine Weitergabe

Passwort


Tell me the password!
3hQI8OAy
Welcome to the Metalab!
Secret Metalab passwd: 3hQI8OAy

Passwort

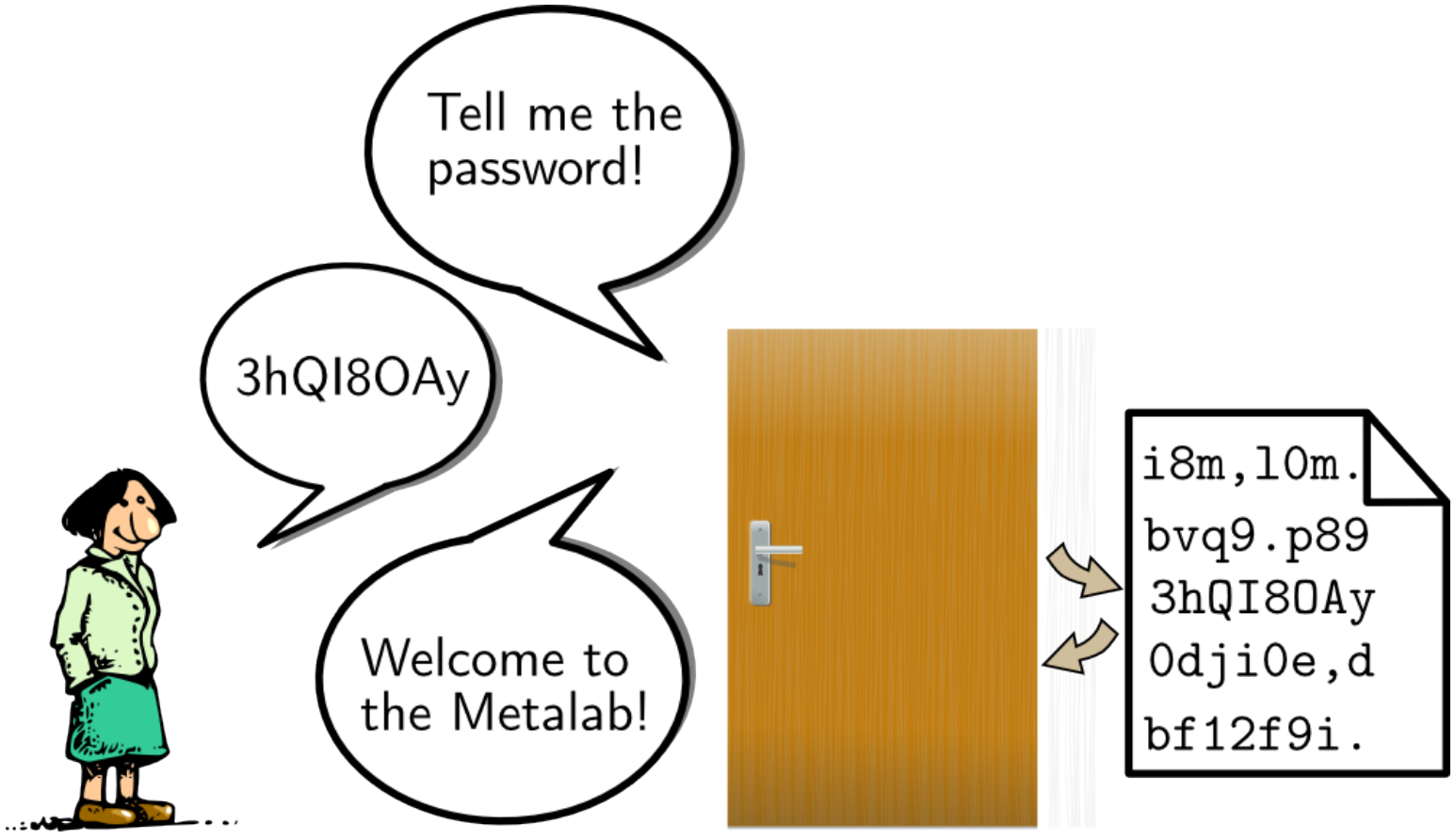
Problem

- Weitergabe
- einzelne User sperren

Triviale Lösung

- wöchentlich/monatlicher Wechsel

Jeder ein Passwort



Jeder ein Passwort

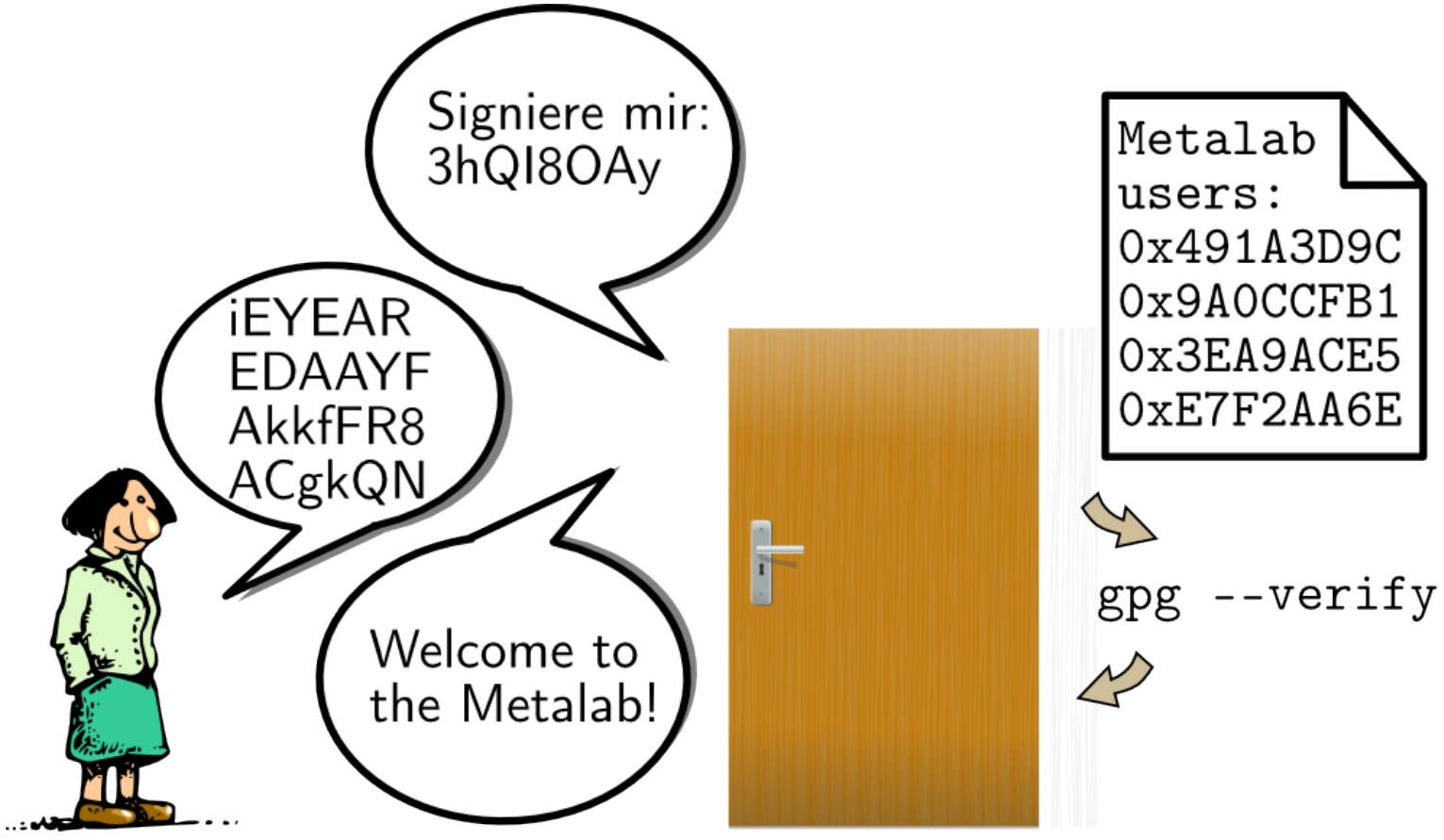
Vorteil

- einzelne User sperren

Problem

- Weitergabe
- Überwachung

GnuPG benutzen



GnuPG benutzen

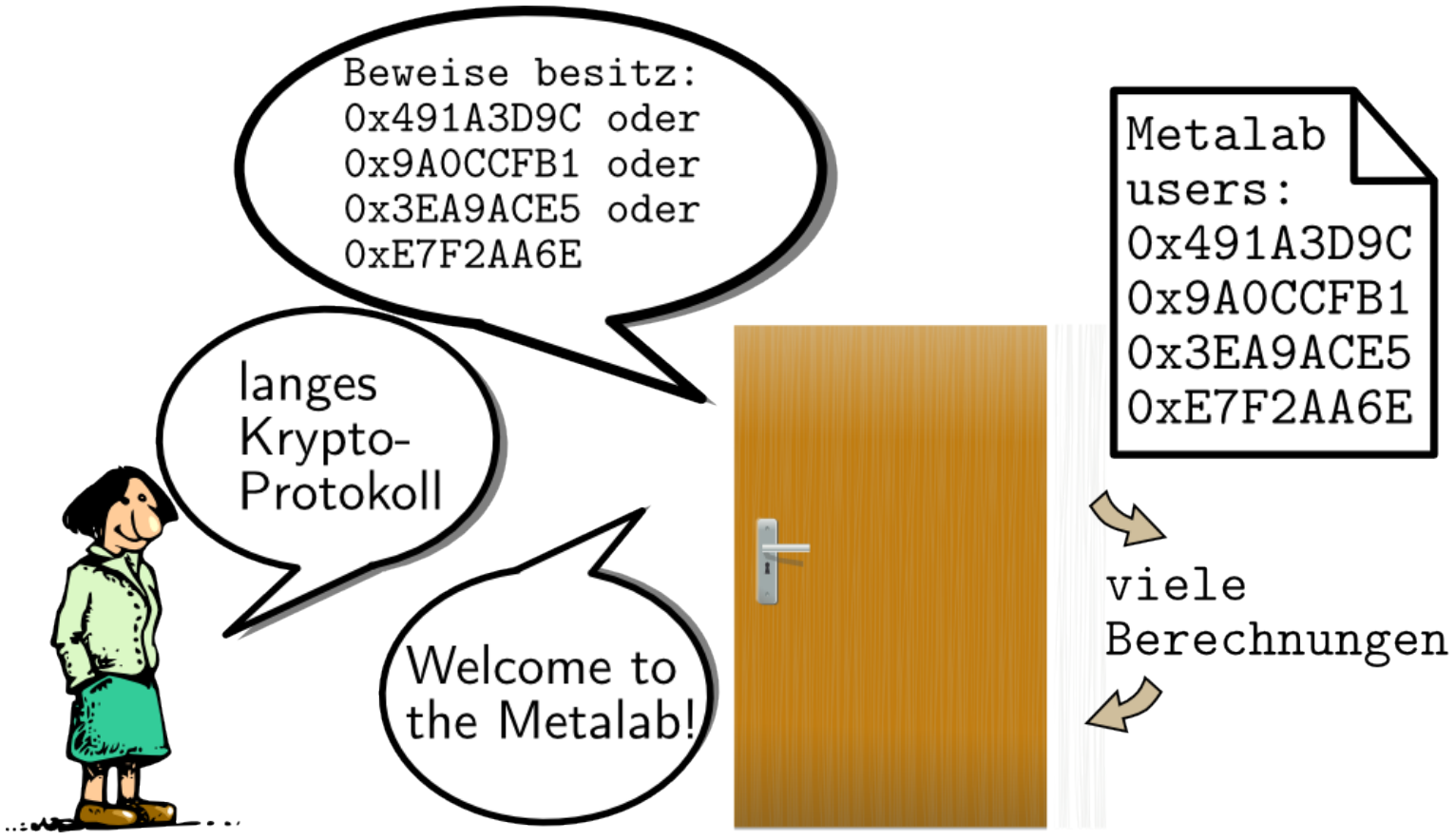
Vorteil

- einzelne User sperren
- keine Weitergabe

Problem

- Überwachung++

Zero-Knowledge mit Or-Beweis



Zero-Knowledge mit Or-Beweis

Vorteil

- einzelne User sperren
- keine Weitergabe
- keine Überwachung

Problem?

- geht nur mit ElGamal Schlüsseln?

Zero Knowledge für Einsteiger

Welcome to the cave