

# "If HTTPS Were Secure, I Wouldn't Need 2FA"- End User and Administrator Mental Models of HTTPS

Alexandra Mai and Katharina Pfeffer

## Problem & Motivation

HTTPS is the most widely used protocol to secure communication on the internet. However, there are still many websites which are not sufficiently secured since they either still use HTTP, or a weak HTTPS configuration.

To understand the reasons for these problems, we conducted the first qualitative mental model study of HTTPS which assesses end users' and administrators' perceptions of HTTPS.

## User Study

- ▶ semi-structured interviews
- ▶ pilot studies (N=6)
- ▶ main study participants (N=30)
  - ▷ 12 administrators
  - ▷ 18 end-users
- ▶ post-hoc validity study (N=9)

### Design & Procedure:

- ▶ 3 drawing tasks
- ▶ multiple rounds of inductive coding
  - ▷ 2 rounds open coding
  - ▷ selective coding
  - ▷ axial coding

## Results

### HTTPS

#### ▶ Model

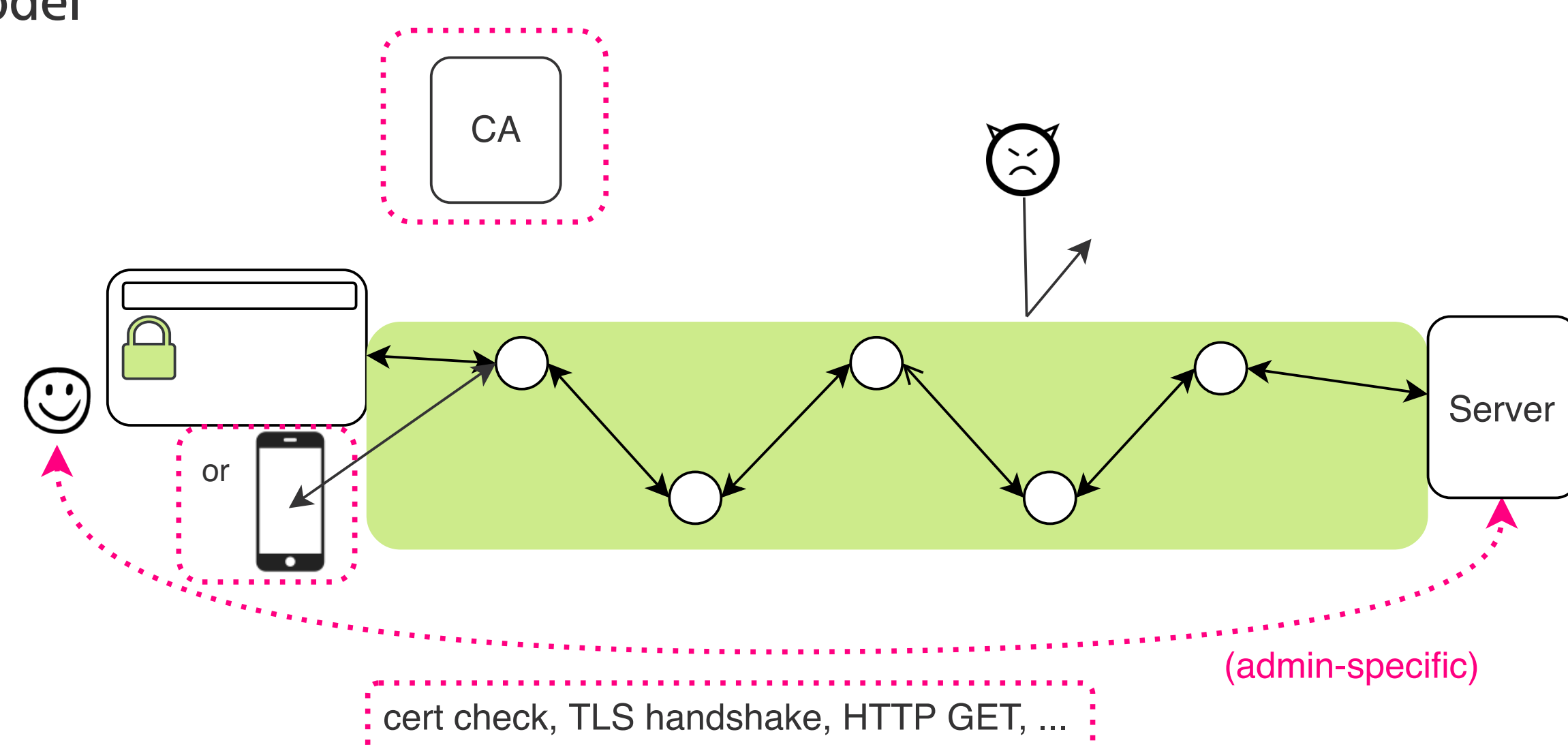


Figure 1: Model of HTTPS. Entities that are solely reflecting administrator mental models are highlighted (dashed boxed in pink).

#### ▶ Anti-Model

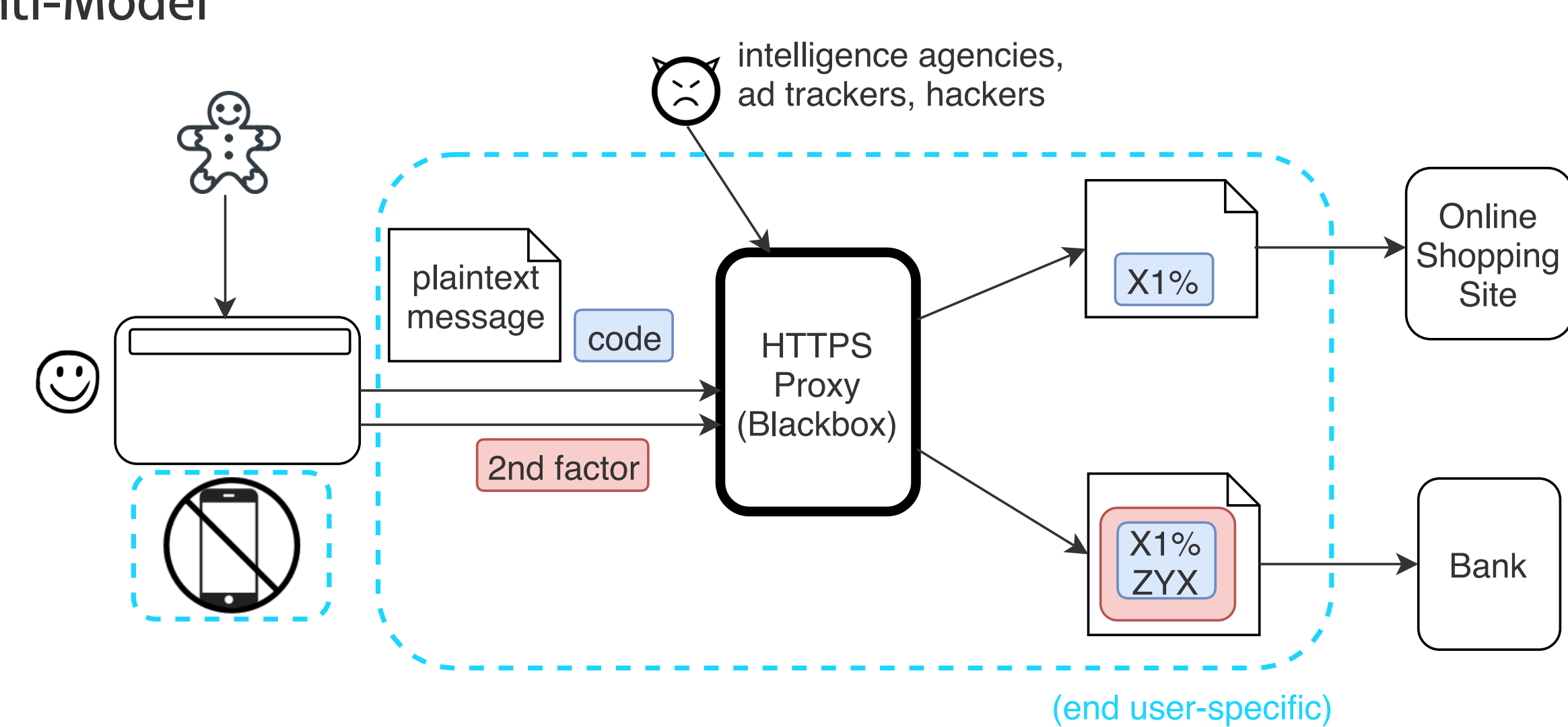


Figure 2: Anti-model of HTTPS. Entities that are solely reflecting end user mental models are highlighted (dashed boxes in blue).

### Message - Encryption

#### ▶ Model

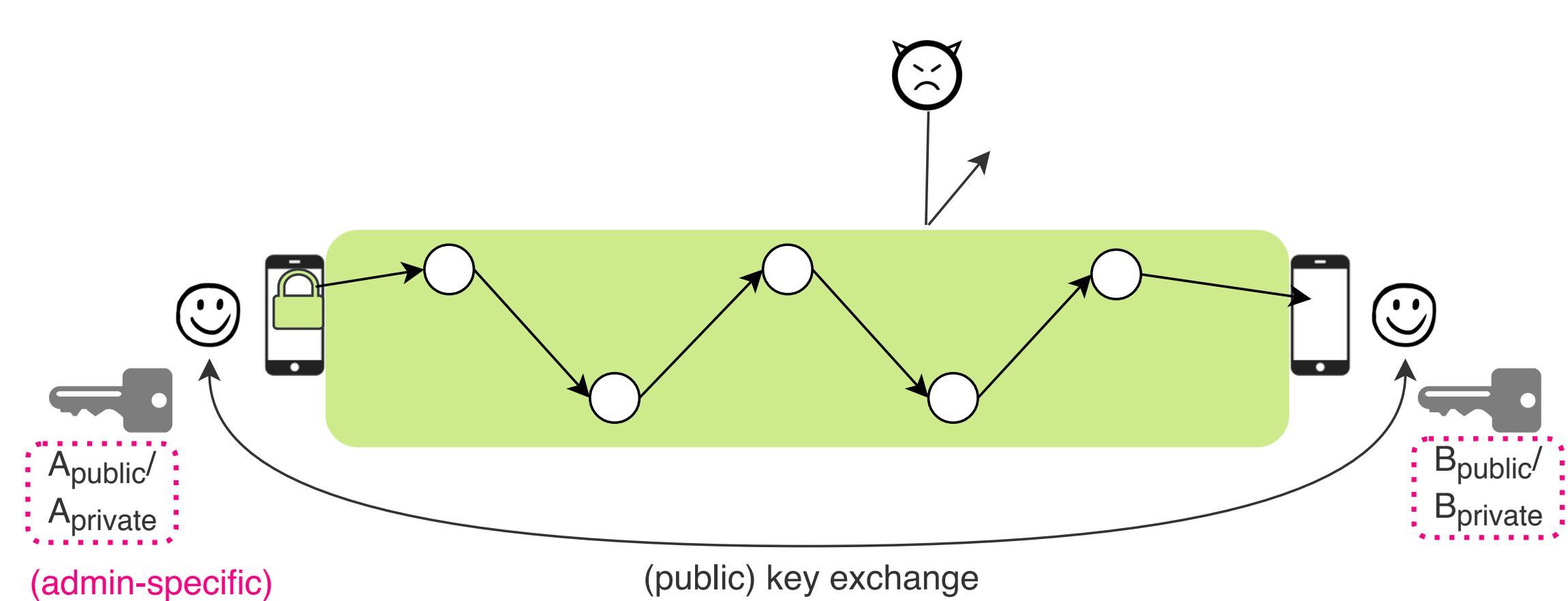


Figure 3: Model of message encryption. Entities that are solely reflecting administrator mental models are highlighted (dashed boxes in pink).

#### ▶ Anti-Model

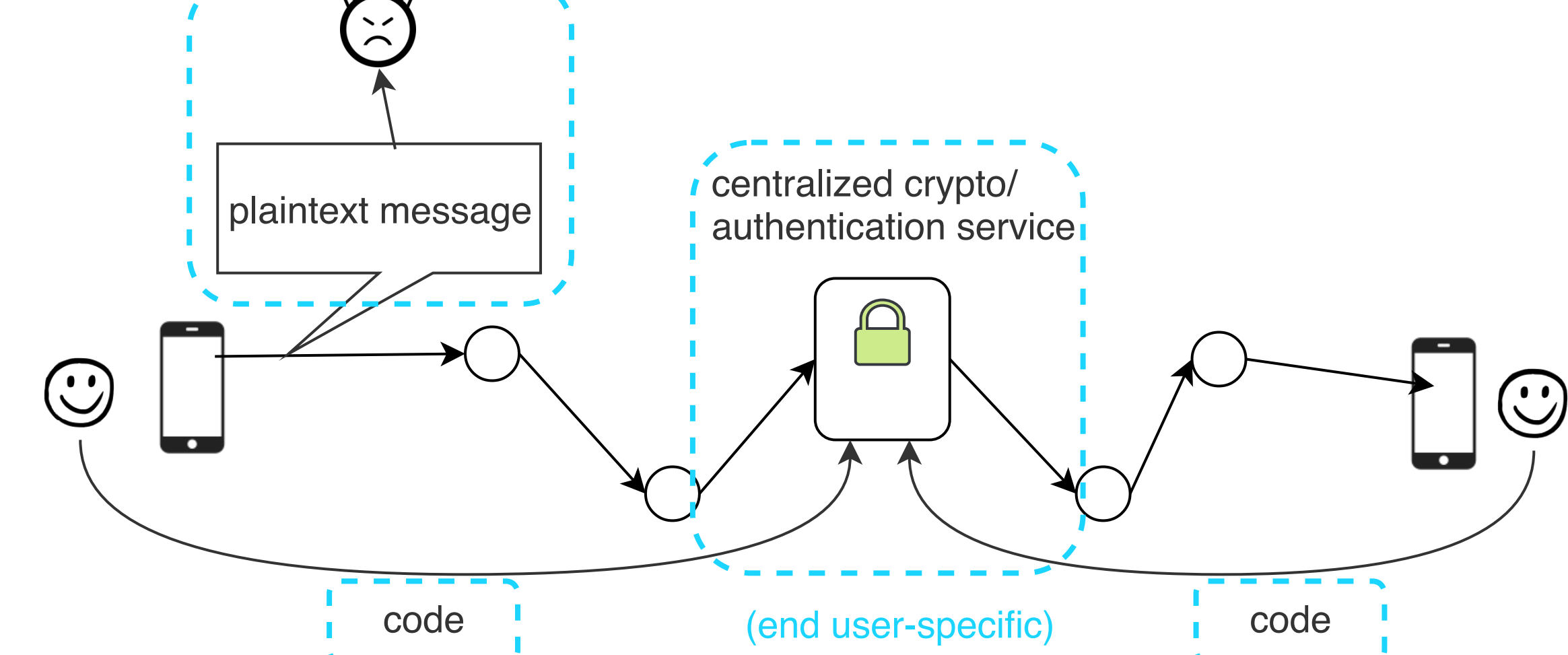


Figure 4: Anti-model of message encryption. Entities that are solely reflecting end user mental models are highlighted (dashed boxes in blue).

## Conclusion

- ▶ Administrators: correct even if sparse mental models
- ▶ End users: conceptual and sparse mental models; sometimes wrong or non-existent
- ▶ Most participants mixed up authentication and encryption
- ▶ Incorrect mental models lead end users to mistrust the security of HTTPS and administrators to configure HTTPS incorrectly
- ▶ Recommendation: Provide encryption by default and highlight linkage between certificates and encryption during configuration