Caught in the Maze of Security Standards

Dieter Gollmann
Hamburg University of Technology

What this talk is not about

1. Designing security protocols is difficult and error prone …
   - We have heard it before.
   - It is not true.
   - Unless you insist on repeating known mistakes.
2. Flawed protocols can be found in standards.
   - Go back to square 1.

What this talk is about

- Observations from a security evaluation of a German eCard project.
- Observations on the interplay between various security standards relevant for this project.
- eCard security is a politically charged topic; certificational weaknesses do matter.

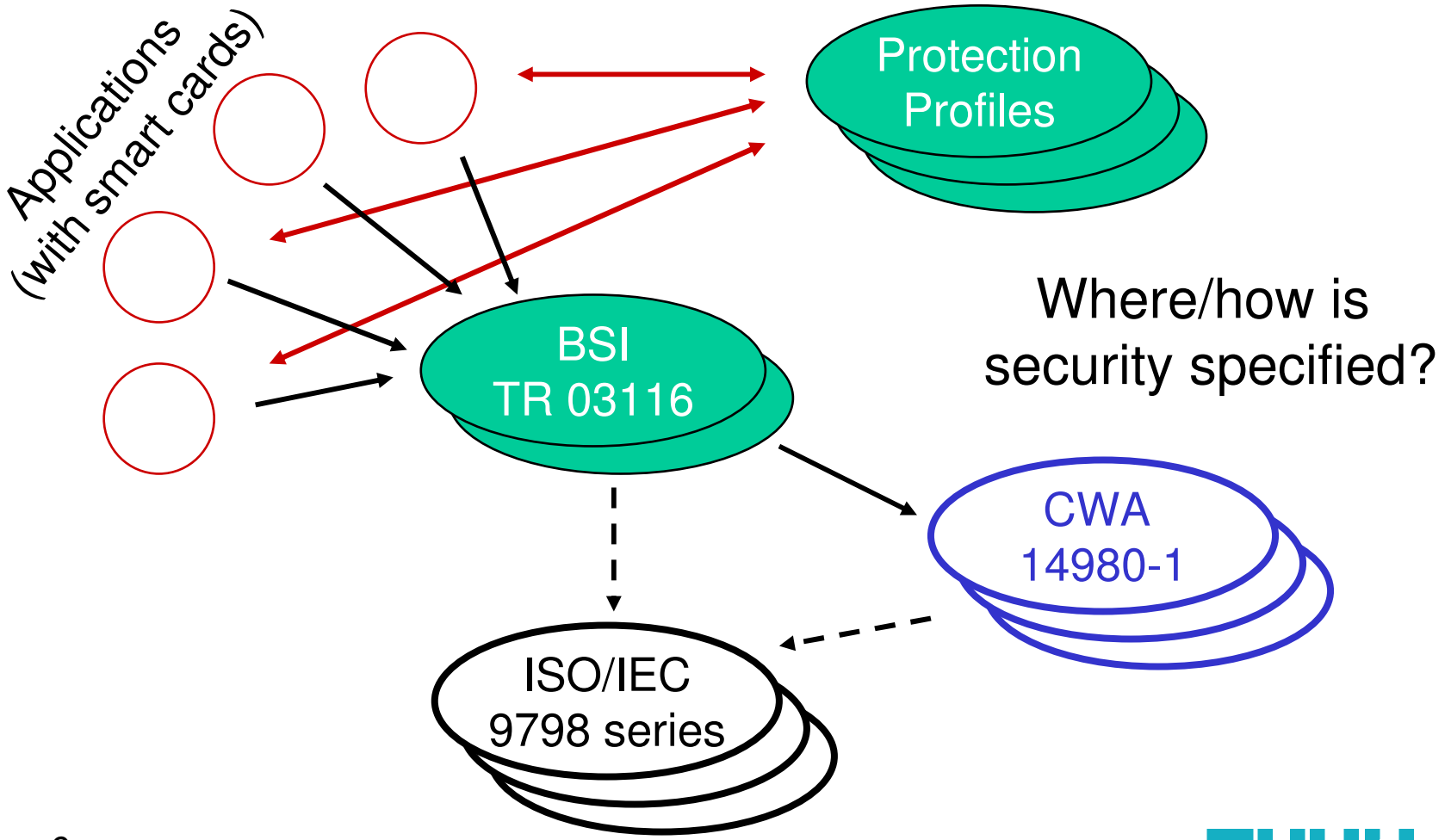
Accreditation

- Someone has to make the decision to turn on a security critical system (accreditation).
  - Executive management decision
- Components can be certified for use in certain applications (certification).
- For certification components are evaluated (evaluation).
  - Technical checks
- How are these processes coordinated?
- How are the security requirements for the different steps specified?

Case study

- Security protocols use cryptographic algorithms, names, nonces, sequence numbers, time stamps etc to meet their security goals.
- How to specify protocols and security goals?
- Who specifies protocols and security goals?
- Further considerations
  - cryptographic algorithms age; recommendations on key length and algorithms are regularly updated.

Security map …



Standards, etc.

- BSI TR03116 – eCard-Projekte der Bundesregierung
  - catalogue of cryptographic algorithms, with required key and seed lengths, regularly updated
  - does not specify protocols
  - does not specify security requirements for protocols
  - refers to international standards: CWA 14980-1, prEN 14980-1, ANSI X9.63, ISO 9798-3
  - https://www.bsi.bund.de/cln_134/ContentBSI/Publikationen/TechnischeRichtlinien/tr03116/index_htm.html

Standards, etc.

- CWA 14980-1 [CEN]: “functional specification” for smart cards, i.e. mainly interface specifications .
- Developers of card systems should not be unnecessarily restricted in their design decisions.
  - defines concrete formats for protocol messages
  - defines cryptographic algorithms
  - defines some internal checks in the card
  - instruction set from ISO/IEC 7816-4
  - No precise security properties of protocols
  - ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14890-01-2004-Mar.pdf

Standards, etc

- ISO/IEC 9798: International standard for authentication protocols
  - explains security properties of protocols; for details of authentication properties see e.g. the Handbook of Applied Cryptography
  - defines protocols generically as sequences of messages
  - abstract message formats
  - does not define specific crypto algorithms or lengths of message fields
  - useful advice on the use of optional fields

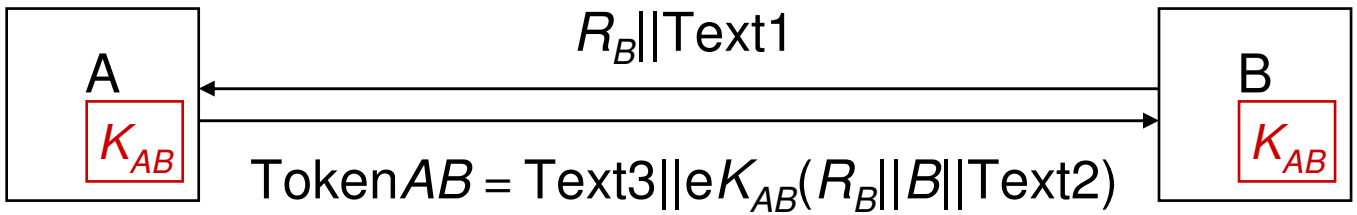
Protection Profiles

- Part of the Common Criteria evaluation methodology
  - define security requirements for application classes
  - several eCard protection profiles, e.g. ePassport, machine readable travel documents, and many more
  - specify generic protection requirements for the application (confidentiality, integrity, …)
  - no concrete requirements on security protocols
  - http://www.commoncriteriaportal.org/

Comment

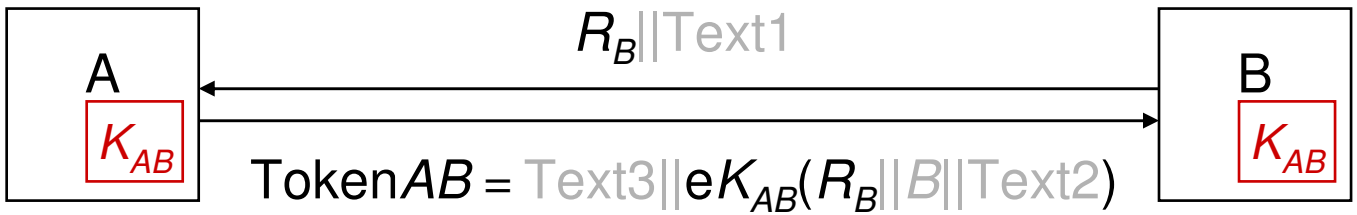
- It is very reasonable when application developers do not specify their own security protocols.
- It is very reasonable to refer to international standards and official technical guidance documents.
- Disadvantage: a lot of indirection.
- Where to find the security requirements for a given application?
- Who is in charge of coordinating this portfolio of standards and technical guidance documents?

ISO 9798-2



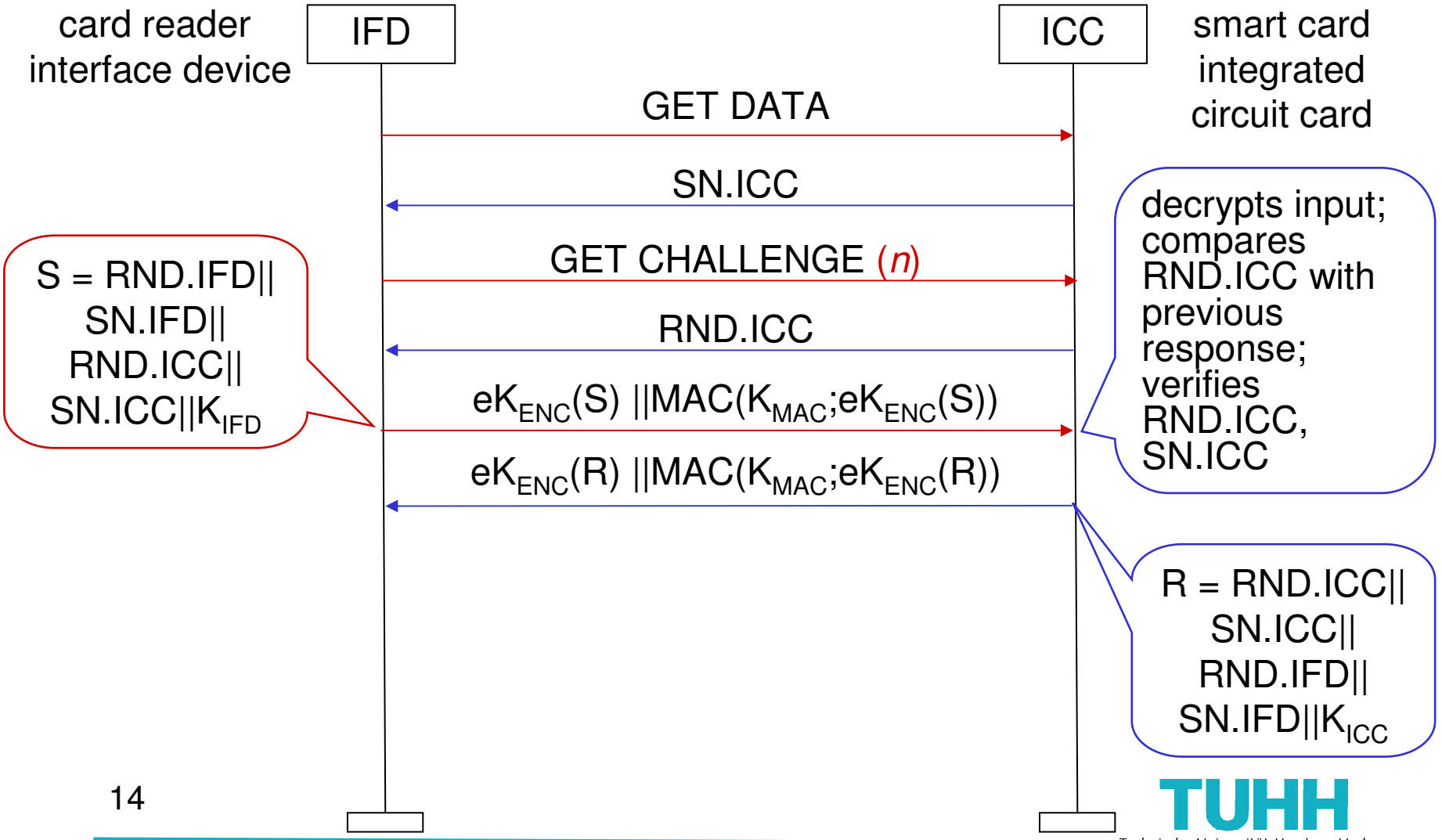
- "*B* verifies Token*AB* by deciphering the enciphered part and checking the correctness of the distinguishing identifier *B*, if present, and that the random number R_B, sent to *A* in step (1), agrees with the random number contained in Token*AB*."
- "Distinguishing identifier *B* is included in Token*AB* to prevent a so-called reflection attack."

Problem?

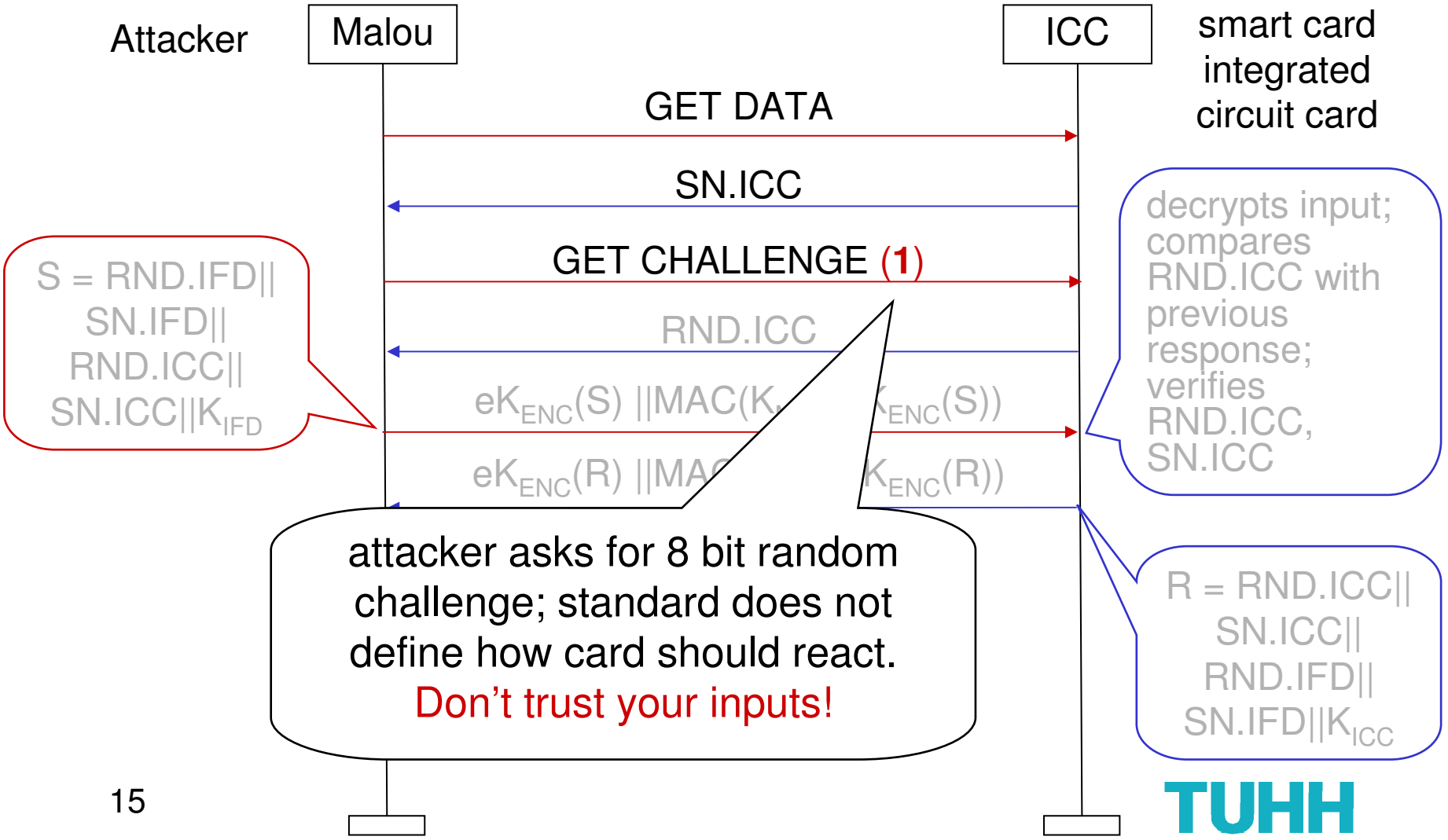


- BSI TR03116 recommends TDES (168 bit key)
- CWA 14980-1 uses 64 bit random challenge R_B, TDES in CBC mode with fixed IV=0.
- Effort to guess TokenAB: 2^{63}
- Using TDES suggests a security level that is actually not reached.

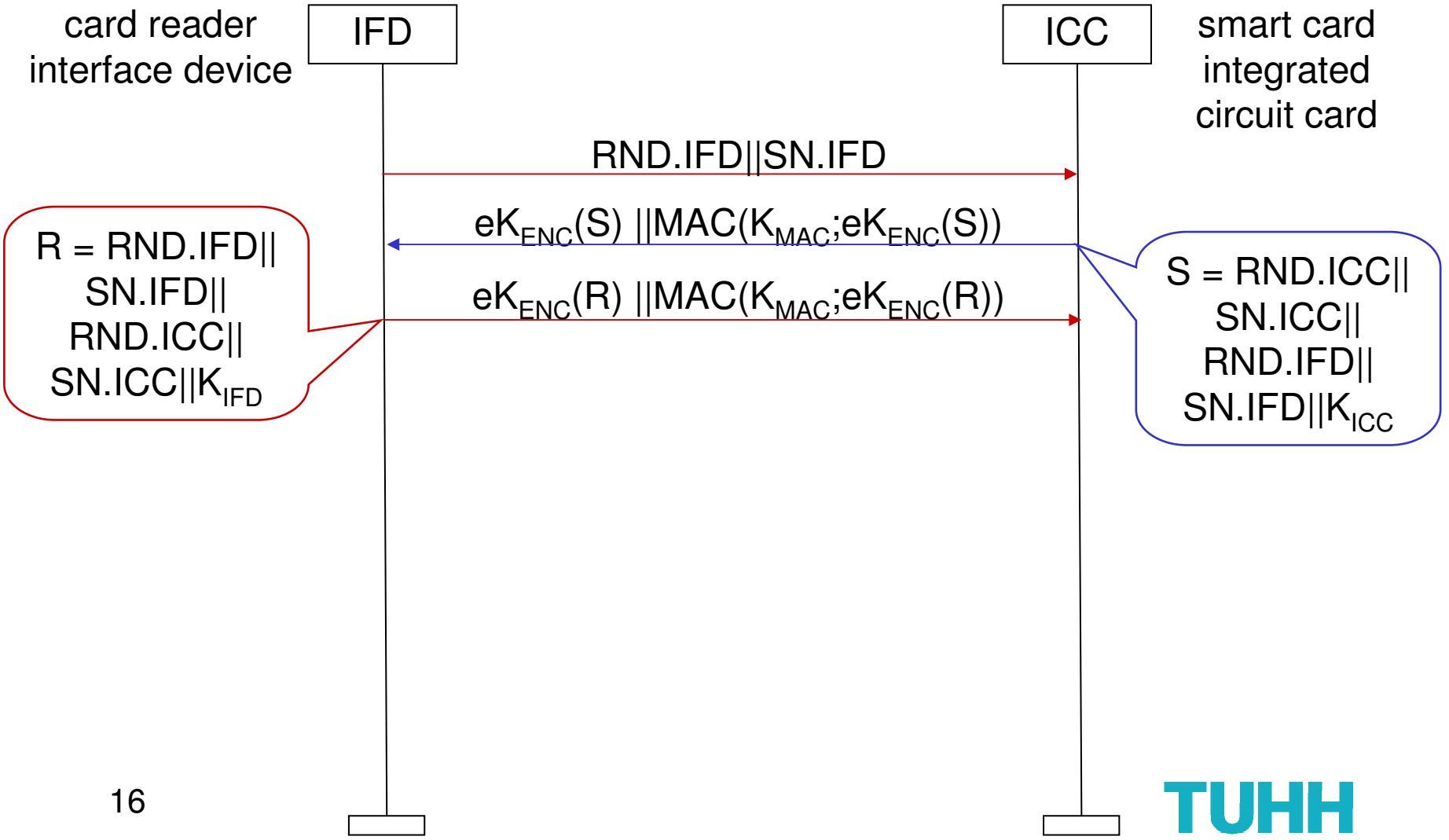
CWA 14980-1, section 8.7.1



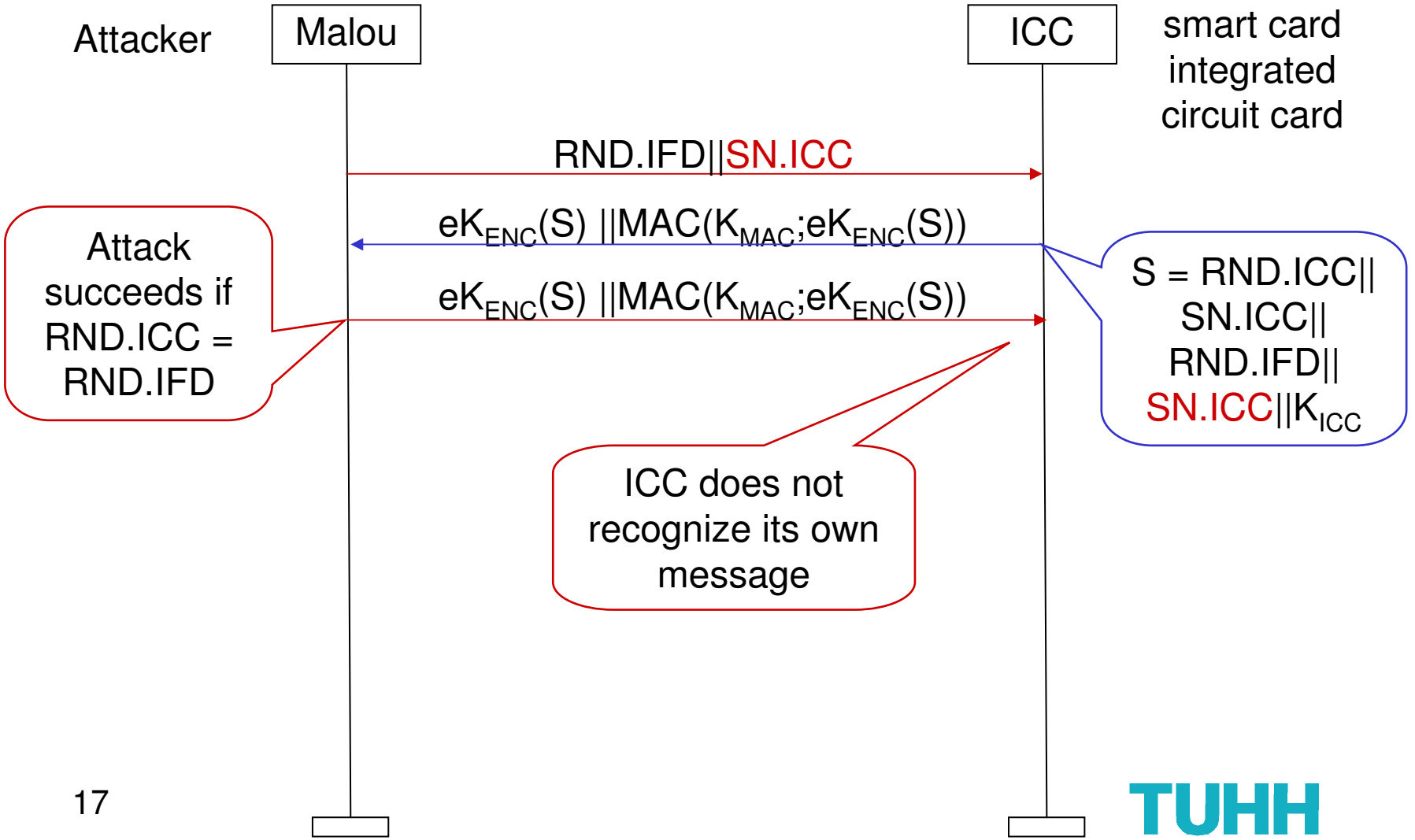
Problem?


Attacker
Malou
ICC
smart card integrated circuit card
GET DATA
SN.ICC
GET CHALLENGE (1)
RND.ICC
eK_ENC(S) ||MAC(K
K_ENC(S))
eK_ENC(R) ||MA
K_ENC(R))
S = RND.IFD|| SN.IFD|| RND.ICC|| SN.ICC||K_IFD
decrypts input; compares RND.ICC with previous response; verifies RND.ICC, SN.ICC
R = RND.ICC|| SN.ICC|| RND.IFD|| SN.IFD||K_ICC
attacker asks for 8 bit random challenge; standard does not define how card should react.
Don't trust your inputs!

… Variation


card reader
interface device
IFD
ICC
smart card
integrated
circuit card
RND.IFD||SN.IFD
eK_ENC(S) ||MAC(K_MAC;eK_ENC(S))
eK_ENC(R) ||MAC(K_MAC;eK_ENC(R))
R = RND.IFD||
SN.IFD||
RND.ICC||
SN.ICC||K_IFD
S = RND.ICC||
SN.ICC||
RND.IFD||
SN.IFD||K_ICC

Problem?


Attacker
Malou
ICC
smart card integrated circuit card
RND.IFD||SN.ICC
eK_ENC(S) ||MAC(K_MAC;eK_ENC(S))
eK_ENC(S) ||MAC(K_MAC;eK_ENC(S))
Attack succeeds if RND.ICC = RND.IFD
S = RND.ICC|| SN.ICC|| RND.IFD|| SN.ICC||K_ICC
ICC does not recognize its own message

Problem?

- K_{ICC}, K_{IFD} are 32 byte random values.
- $K_{ICC} \oplus K_{IFD}$ is input for the generation of the session key.
- In the previous scenario $K_{ICC} = K_{IFD}$.
- Attacker does not know this value, but knows $K_{ICC} \oplus K_{ICC} = 0$ and can compute the session key.
- XOR with random value does not give perfect security.

Conclusion:
All problems can be solved, but where?