THE UNIVERSITY OF AUCKLAND

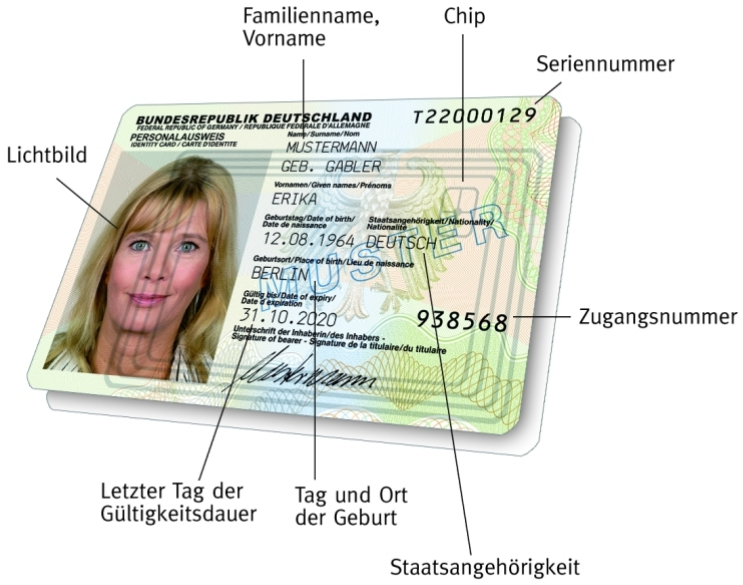
All You Can Eat – Breaking a Real-World Contactless Payment System

Kasper, Silbermann and Paar, Comment by Friedrich Ellmer

Financial Cryptography and Data Security Lecture Notes in Computer Science Volume 6052, 2010

Brief Content

- Authors were able to change amount of money on every card
- They did not find any check for card number and balance
- Typical example of secret encryption mechanism (c.f. Lampson)



example ID (not content of the paper)

Pros & Cons

THE UNIVERSITY OF AUCKLAND

- **What's good?**
  - Real world case
  - no ivory tower research

- **What's bad?**
  - What's not mentioned:
    - This payment system is **not** wide spread
    - the owner is written on the card and can't be changed!
    - No solution provided
  - It has been tested only with small values (below tolerance threshold?)

Is this enough?

THE UNIVERSITY OF AUCKLAND

- Security is always a trade-off between effort and protection
  - at least at the bank's side
- Complete security is never possible
- → You have to choose the security level wisely
  - Otherwise too much effort required or insufficient protection

- **→ Is this security level high enough for a micro payment system?**