IRMA Verified Assurer

Securely storing identity document chip data onto IRMA cards

Geert Smelt

Radboud University Nijmegen
Kerckhoff's Institute

November 6th, 2015

Outline

Authentication

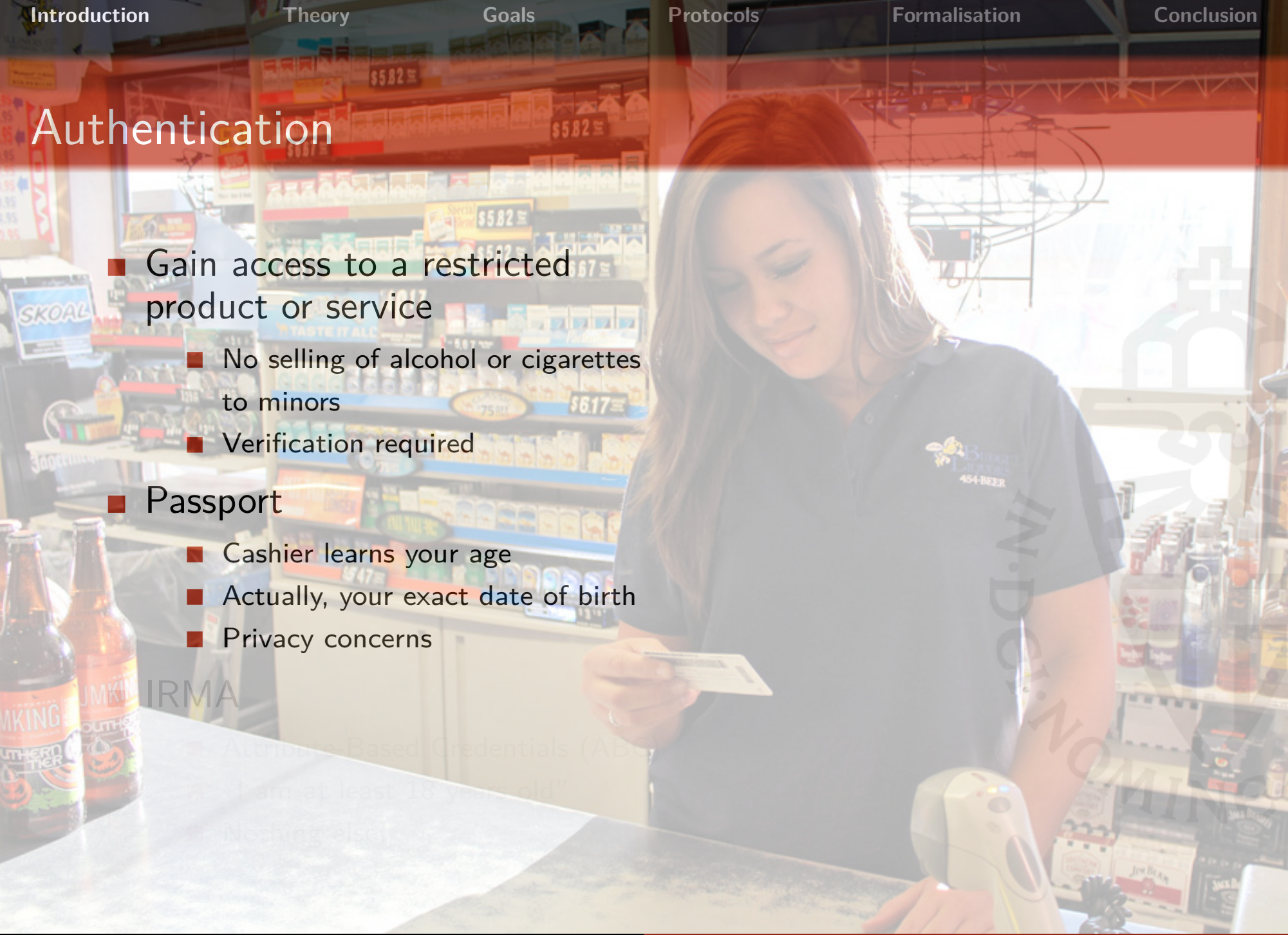
- Gain access to a restricted product or service
  - No selling of alcohol or cigarettes to minors
  - Verification required
- Passport
- IRMA

Authentication

- Gain access to a restricted product or service
  - No selling of alcohol or cigarettes to minors
  - Verification required
- Passport
  - Cashier learns your age
  - Actually, your exact date of birth
  - Privacy concerns

IRMA

- Attribute-Based Credentials (ABC)
- I am at least 18 years old
- No data stored



Authentication

- Gain access to a restricted product or service
  - No selling of alcohol or cigarettes to minors
  - Verification required
- Passport
  - Cashier learns your age
  - Actually, your exact date of birth
  - Privacy concerns
- IRMA
  - Attribute-Based Credentials (ABC)
  - "I am at least 18 years old"
  - Nothing else!

IRMA

Passport

Designing the protocol

- Connection should be encrypted with strong cryptography
- ...

Goals

Goals

- Authenticity
- Accountability
- Confidentiality
- Integrity
- Availability

TLS handshake protocol

```
 Client                                          Server
------------                                    ------------
ClientHello                 -------->
                                                    ServerHello
                                                   Certificate*
                                             ServerKeyExchange*
                                            CertificateRequest*
                            <--------           ServerHelloDone
Certificate*
ClientKeyExchange
CertificateVerify*
[ChangeCipherSpec]
Finished                    -------->
                                             [ChangeCipherSpec]
                            <--------                Finished
Application Data            <------->        Application Data
```

IRMA Assurer

Protocol

Protocol

Lorem ipsum

Model

Example

-

Passport