Privacy-Enhancing Technologies

Using Identity-Based Public-Key Cryptography with Images to Preserve Privacy

Sebastian Pape, Nabil Benamar

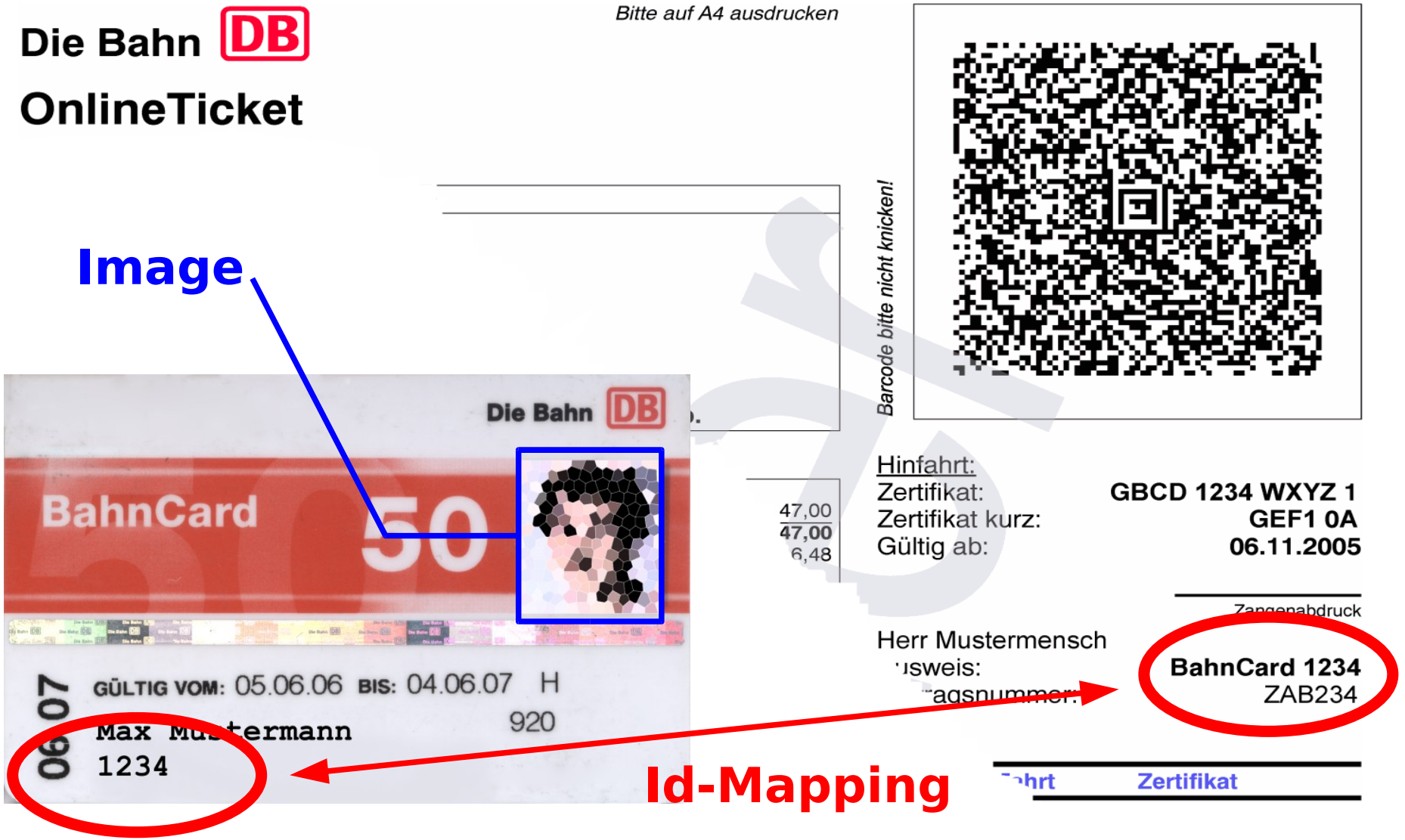
UNIKASSEL
VERSITÄT

Overview

- Motivation
- Identity Based Public-Key Cryptosystems
- Scenario & Setup
- Creation & Validation of tickets
- Privacy Issues & Security Aspects
- Conclusion & Prospect

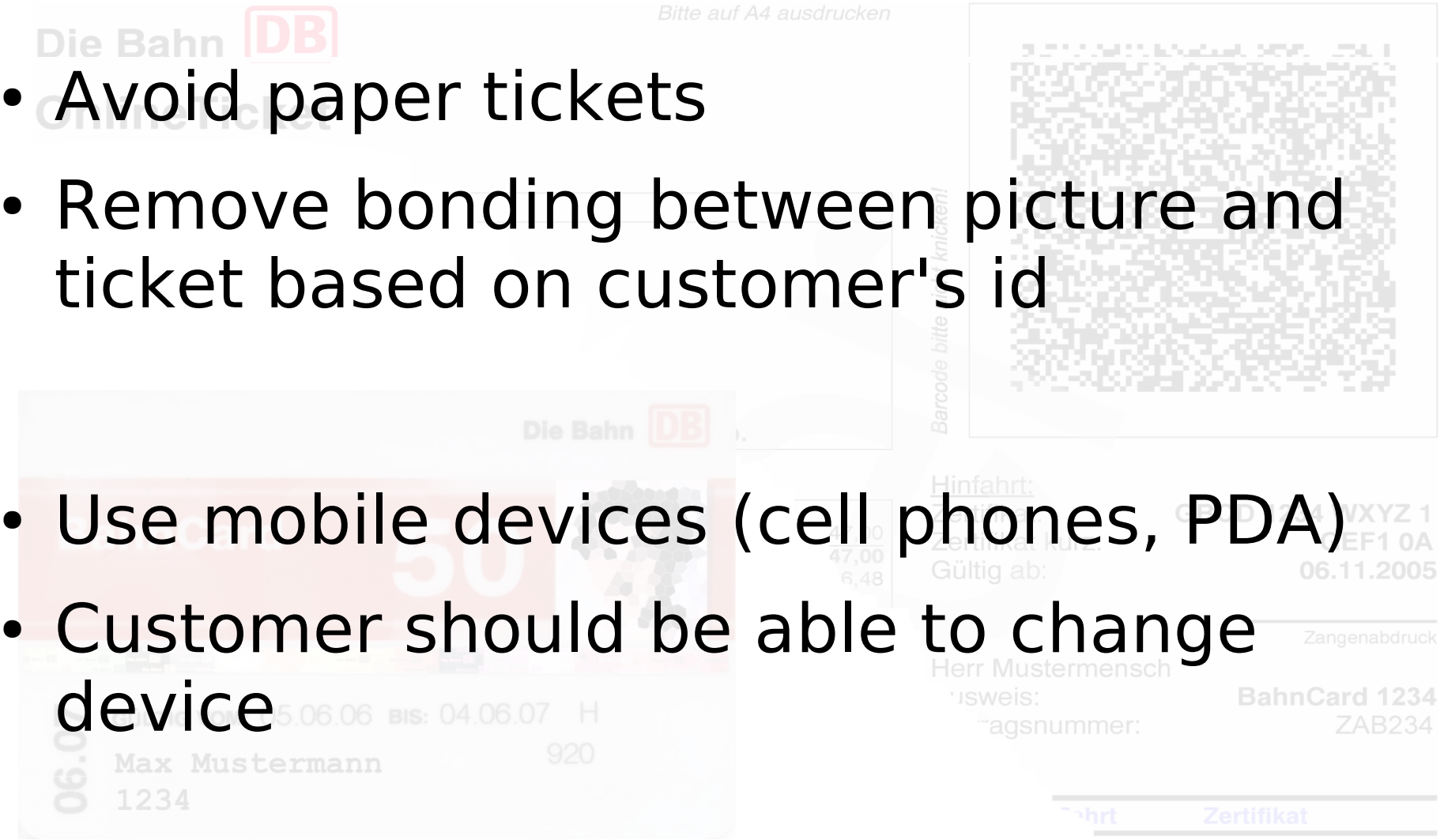
Motivation / Scenario

Motivation / Scenario



Motivation / Intention

- Avoid paper tickets
- Remove bonding between picture and ticket based on customer's id



- Use mobile devices (cell phones, PDA)
- Customer should be able to change device

Motivation / Conclusion I

- Avoid paper tickets ➔ Electronic tickets
- Remove bonding between picture and ticket based on customer's id

  ➔ Bonding between picture and ticket
- Use mobile devices (cell phones, PDA)
- Customer should be able to change device

  ➔ Tickets have to be stored at database

Motivation / Conclusion I

- Customer's knowledge and control of information flow
  - ➔ Encrypted storage at database
  - Identity-Based Public-Key CS

- Use mobile devices (cell phones, PDA)
- Customer should be able to change device

  ➔ Tickets have to be stored at database

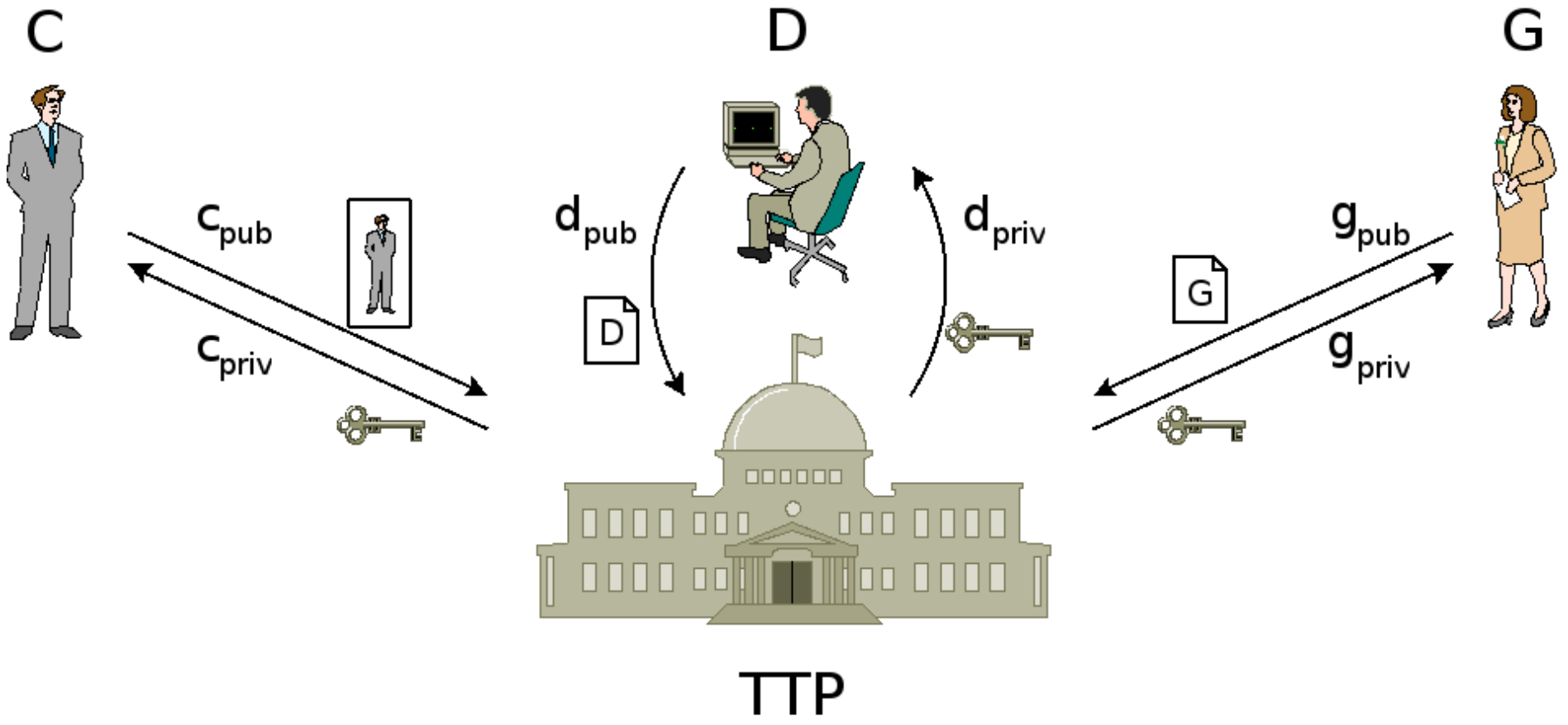
Identity-Based Public-Key CS

- Shamir ('85) based on Blom ('82)
- Assymetric system

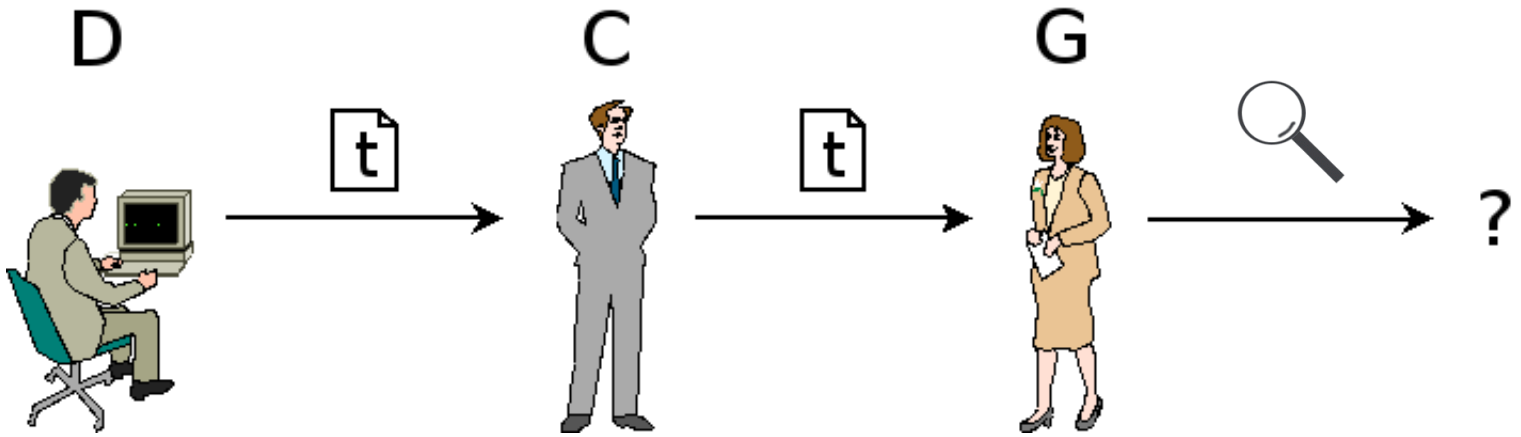
- Public identific. information ~ public key
- No explicit public key

- Priv. key computed by trusted authority
- Trusted authority needs priv. information

Setup



Scenario

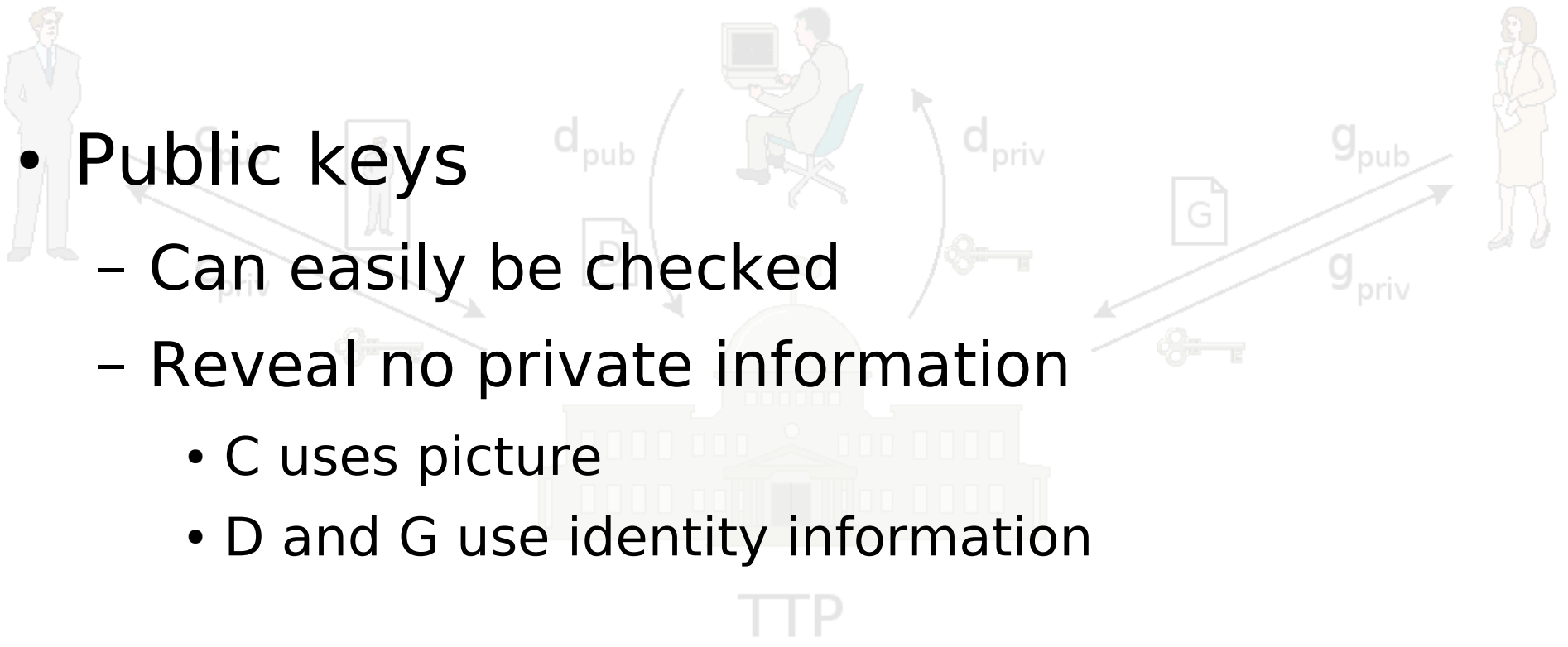


- All participants have key pairs

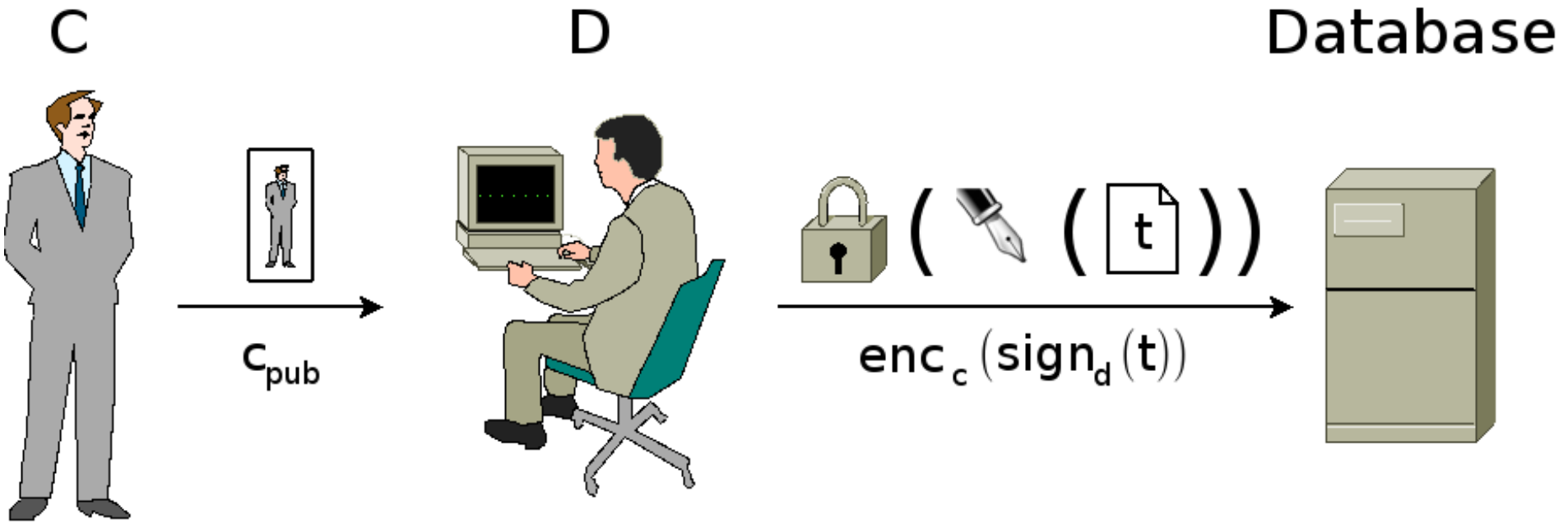
  ➔secure communication

Setup II

- C has face to face contact with G (and D?)
- Public keys
  - Can easily be checked
  - Reveal no private information
    - C uses picture
    - D and G use identity information

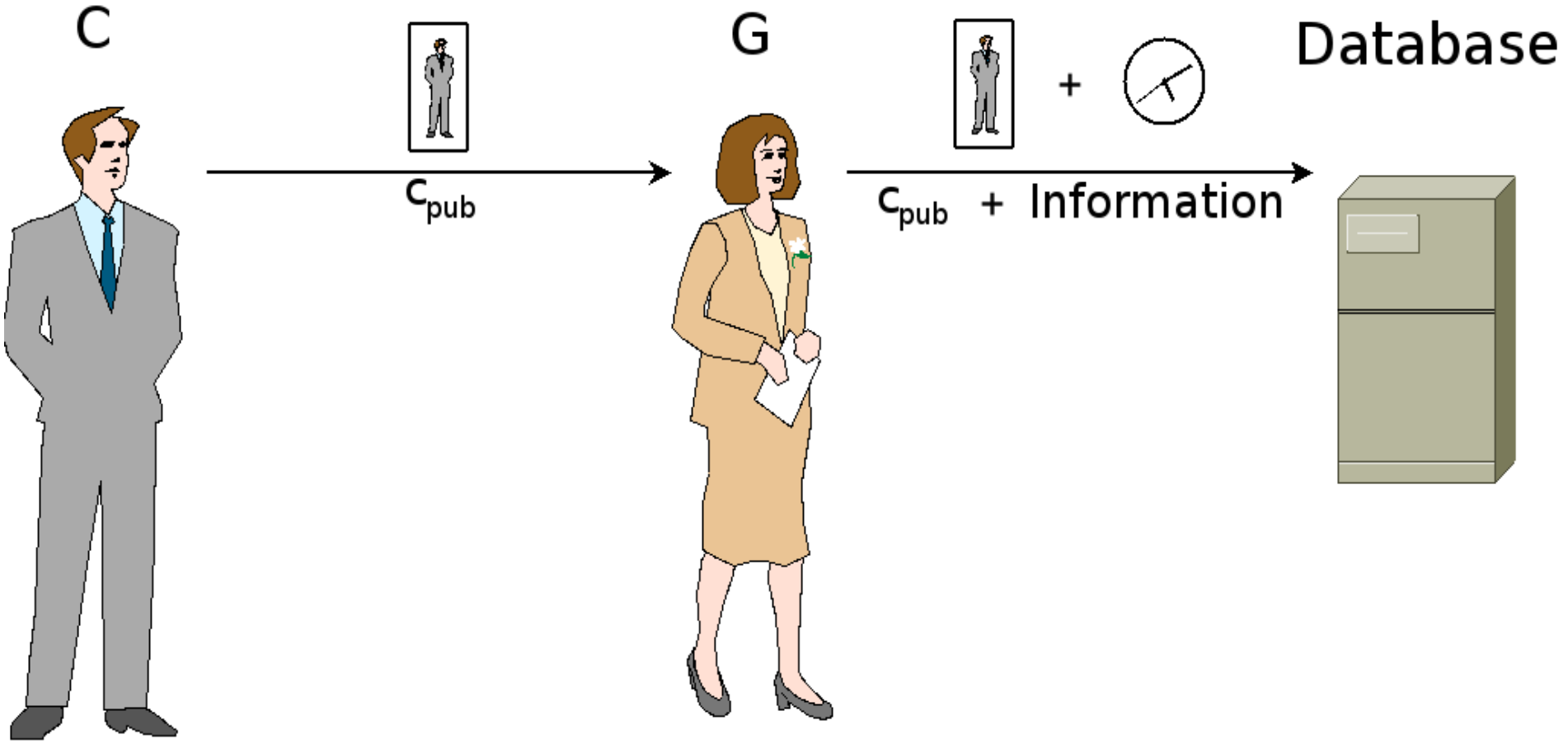


Creation of Tickets

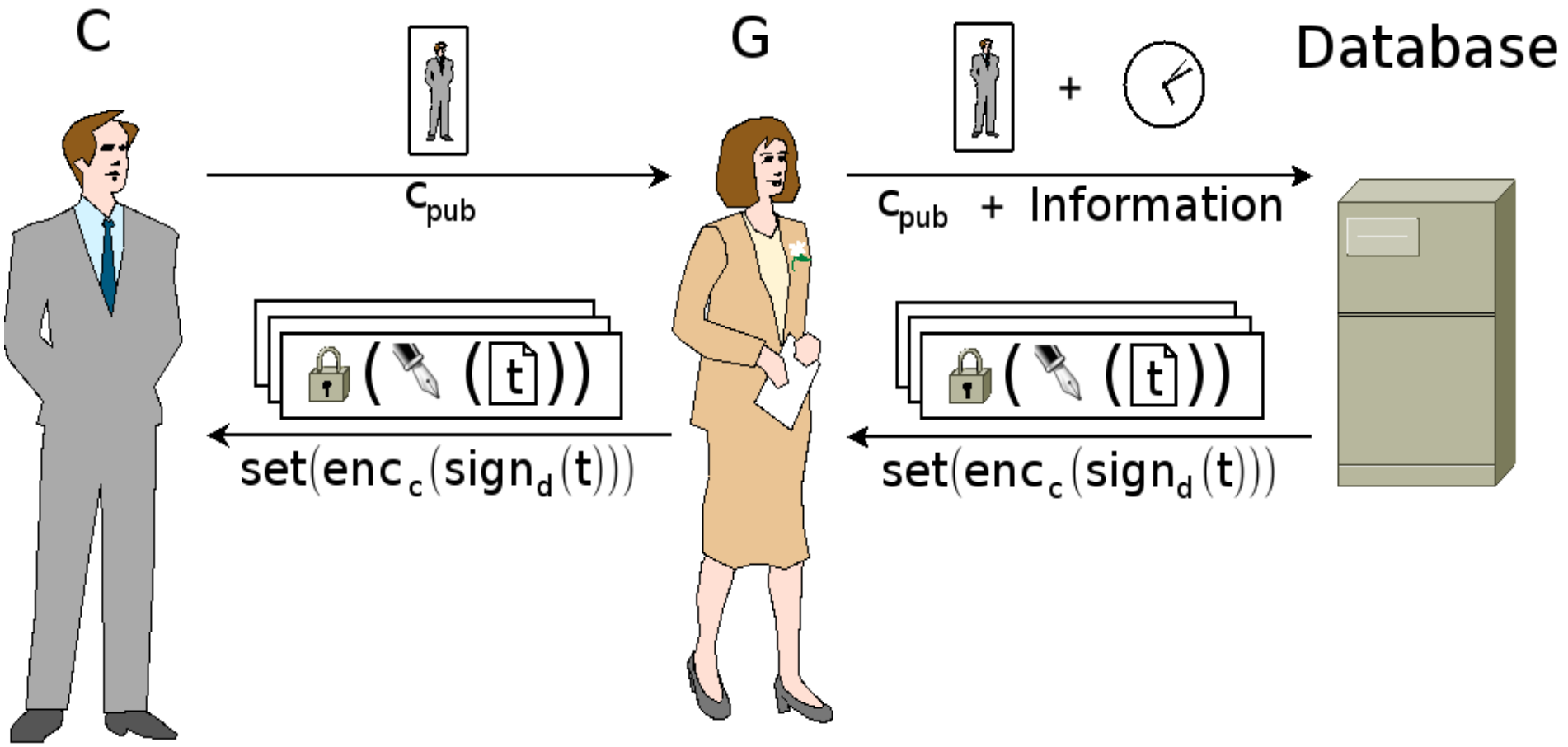


- Tickets stored in relation to C's public key
- Additional information may be necessary
  - Performance vs. privacy

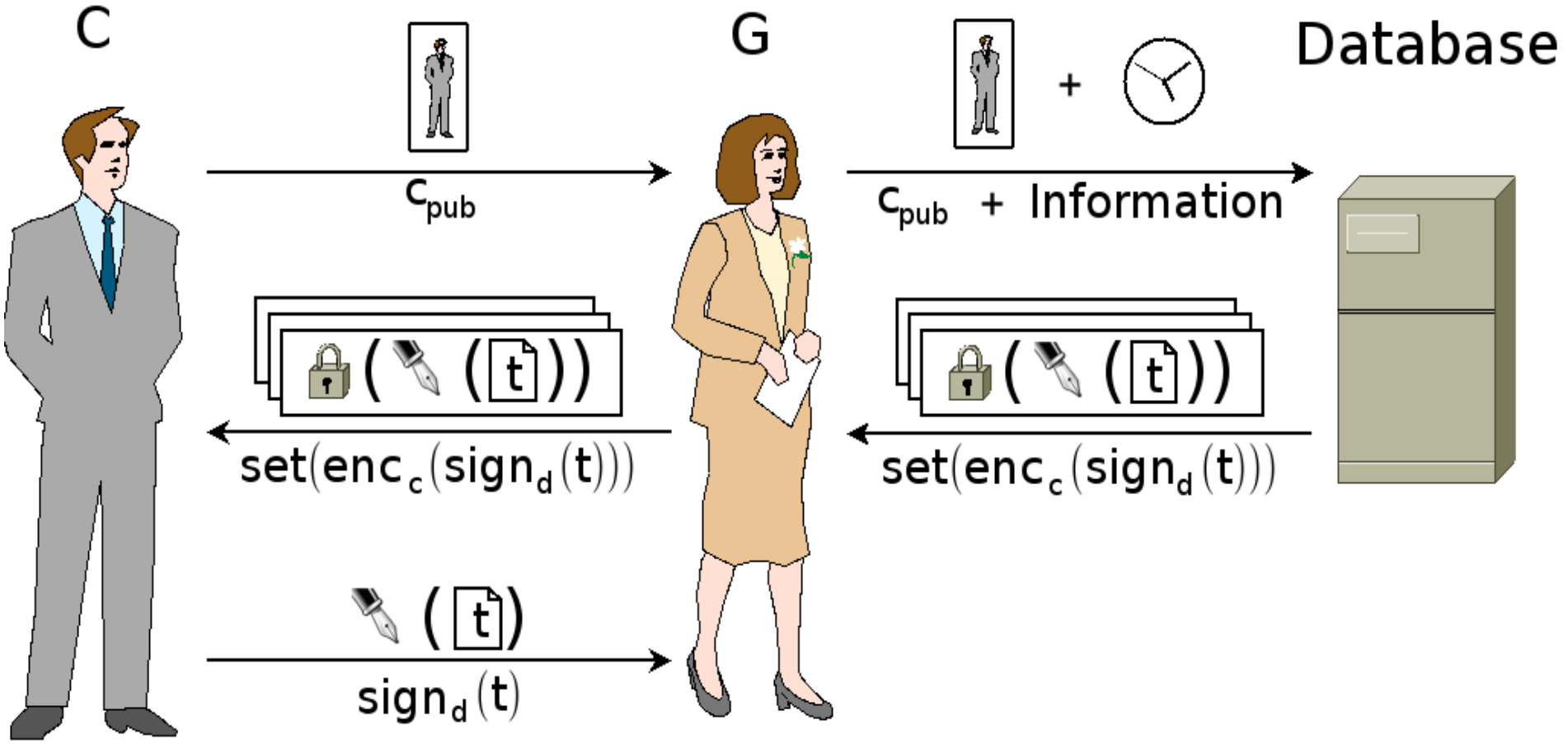
Validation of Tickets



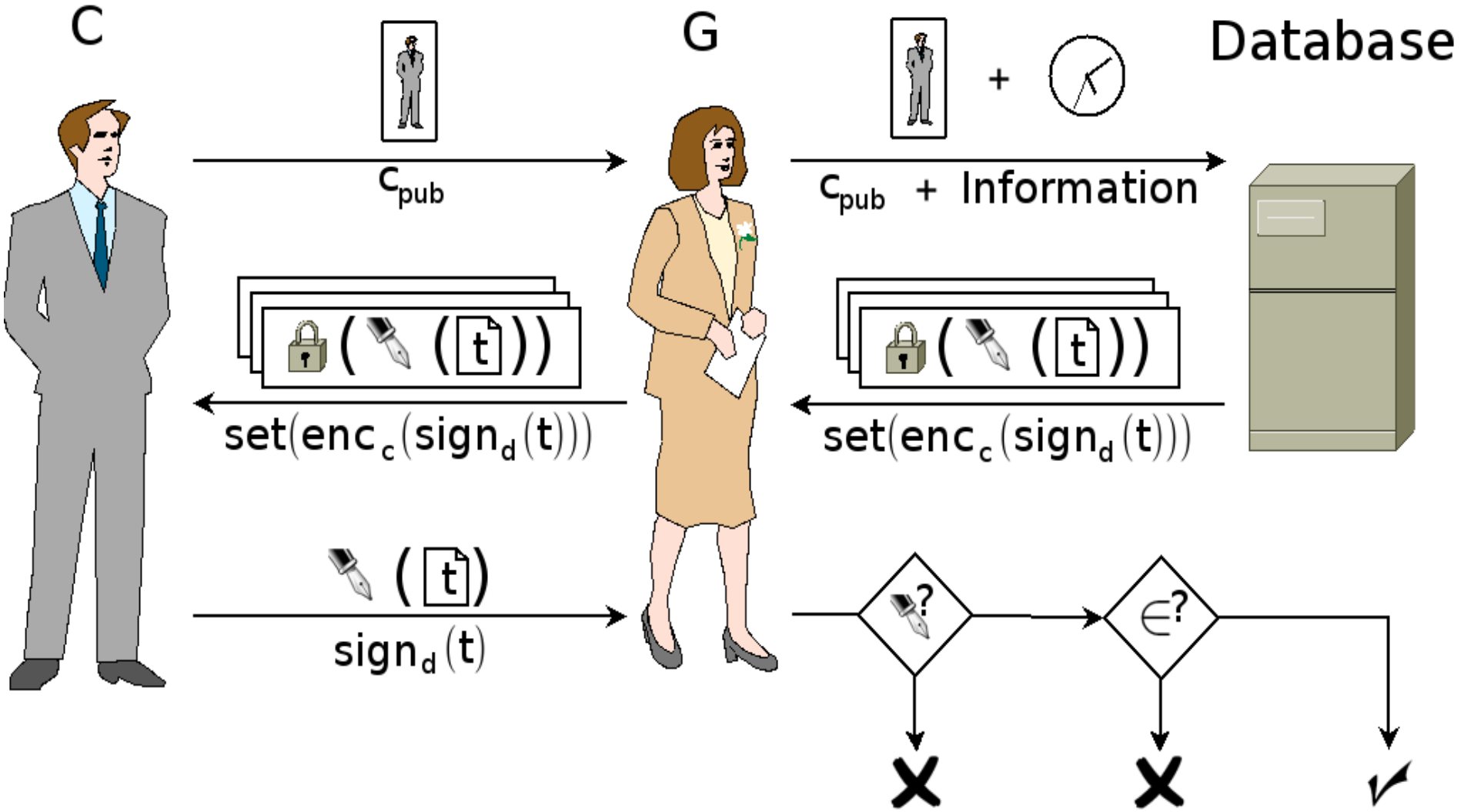
Validation of Tickets



Validation of Tickets



Validation of Tickets



Privacy Issues

- Additional information vs. performance
  - Sparse information to find the ticket faster
- G should not learn anything about the dealers C prefers
  - Group signature schemes
  - Trusted authority could act as group manager if problems arise

Security Aspects (C)

- C is unable to forge tickets
  - Valid signature of dealer needed
- C is unable to pass tickets to C'
  - G checks if it originates from database

Security Aspects (D)

- D is unable to forge tickets
  - valid signature of dealer needed
- Denial of Service
  - D deletes tickets ➔ database interface
  - D floods database ➔ additional database layer with information who inserted ticket (C has to complain)

Security Aspects (G)

- G can alter data before reaching it to C
  - Aim? G could refuse C's legitimation anyway

  ➔Sign tickets by database
  - Any honest G can prove opposite
- Can manipulate legitimation test
  - Aim? working together with C?

  ➔C & D no other combination makes sense

Security Aspects (C & D)

- Ticket signed by D and encrypted by C
  - G proves both

- G cannot read the ticket
  - No win ticket could be changed by C

Conclusion

- Application is secure as long as
  - The underlying cryptosystem holds
  - The guard really examines the tickets
- Implicit key management given
- No unnecessary information revealed
  - Customers know symbolic identity
  - Dealer and guard check picture/appearance
- Customer has control about data

Prospect

- Most concrete Identity-Based Public-Key Cryptosystems include additional data

- "Perfect" face recognition software

  ➔Derive the customer's key straightly from a digital camera