Solving Security Problems of Free-Floating Car Sharing

Nicholas Bushway

Division of Science and Mathematics
University of Minnesota, Morris
Morris, Minnesota, USA

April 21, 2019

Outline

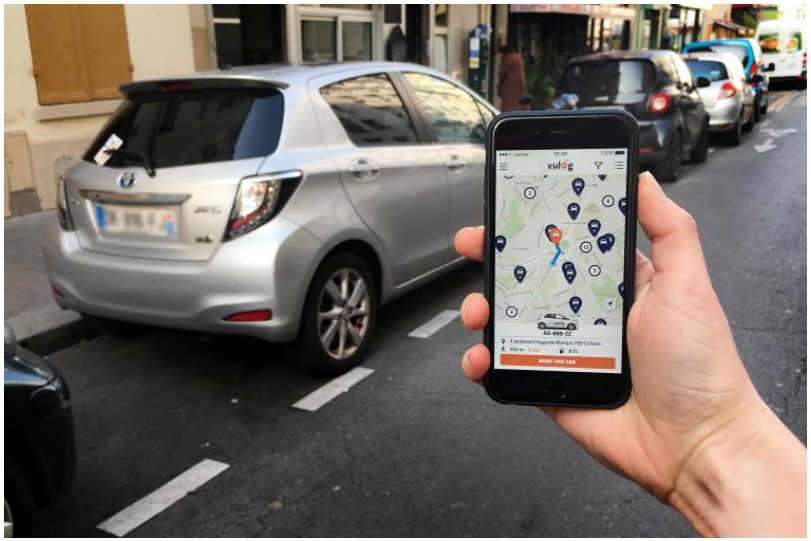
Outline

The Problem

- Owning a car is expensive
- Made worse in metro areas
- Car-sharing more cost-effective for all parties

What is free-floating car sharing?

- Smart phone based car-sharing
- Location services
- No physical key exchanged



Free-Floating Car Sharing
`https://tr.im/Jue9Y`

Outline

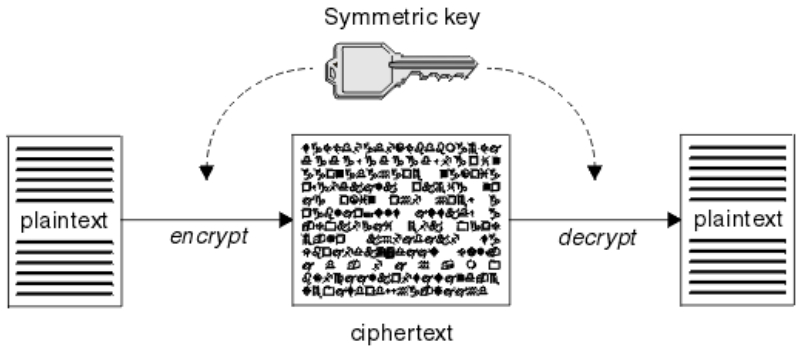
Encryption

- We encrypt data we want hidden
- Plain text
- Cipher text

Cipher text: cropped from `https://ibm.co/2VWR5ky`

Symmetric Keys

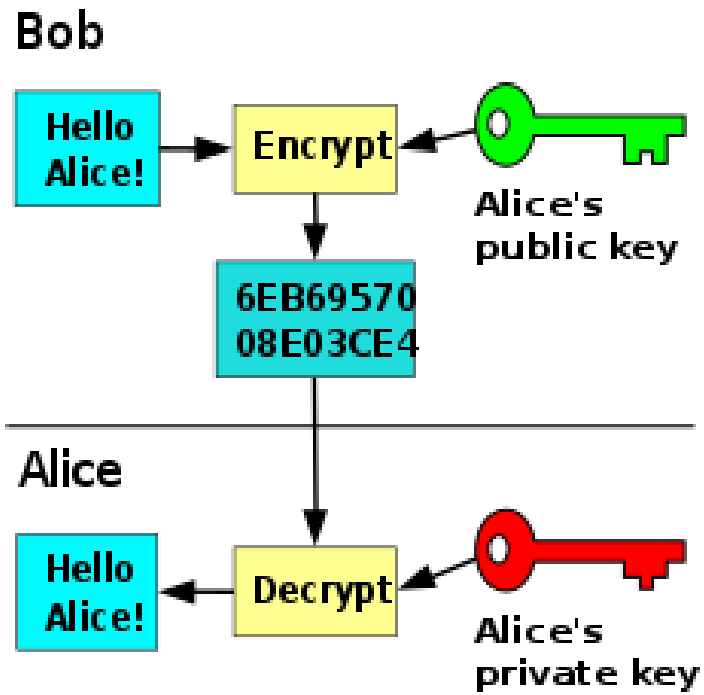
- Data gets encrypted/ decrypted by a key
- Symmetric Key approach uses the same key for both



Symmetric Keys `https://ibm.co/2VWR5ky`

Public Key Cryptography

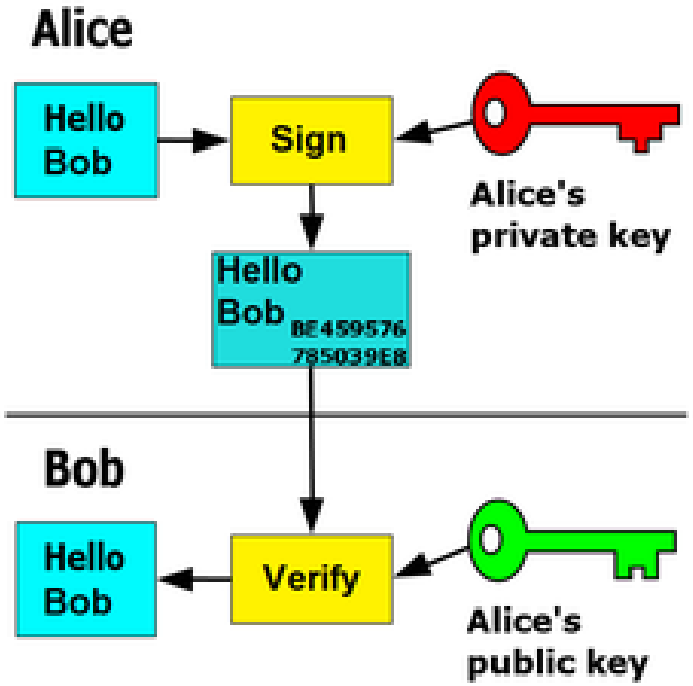
- Public keys can be shared
- Private keys are kept by the owner



Public Key Encryption `https://bit.ly/1wEBIiP`

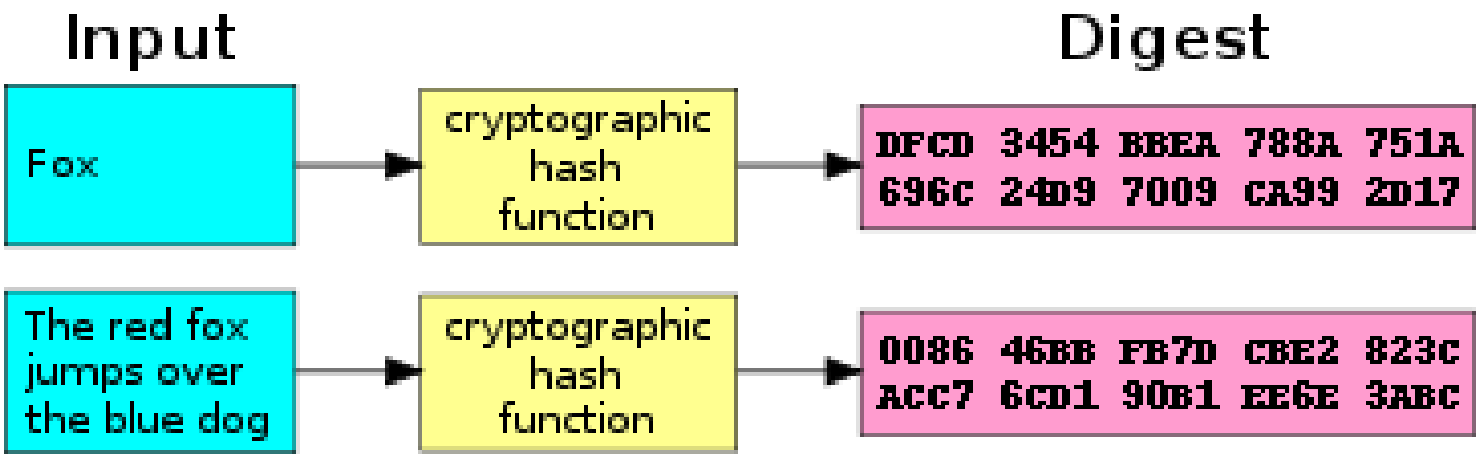
Public Key Cryptography

- Encryption can verify the origin of data
- Digital Signatures



Digital Signatures `https://bit.ly/1wEBIiP`

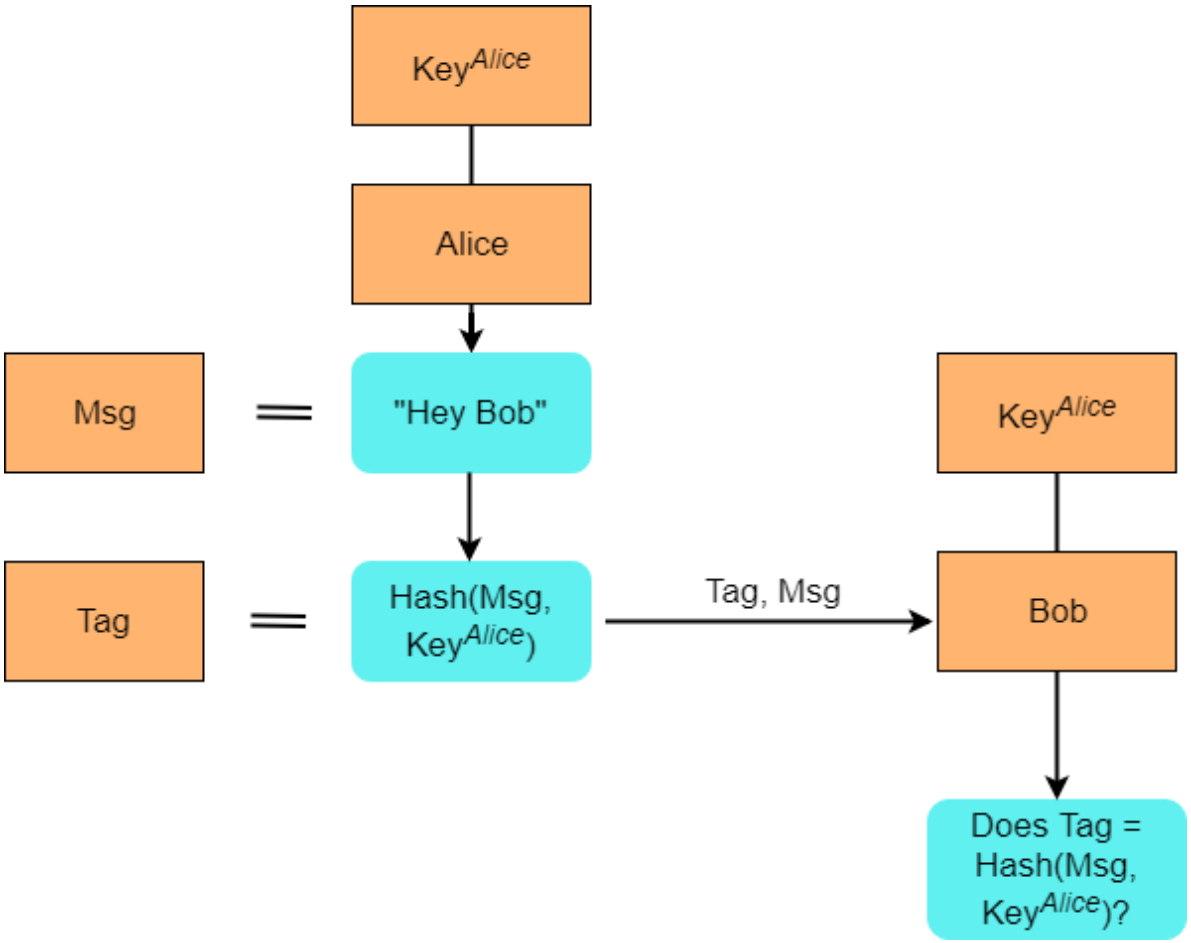
Hash Functions



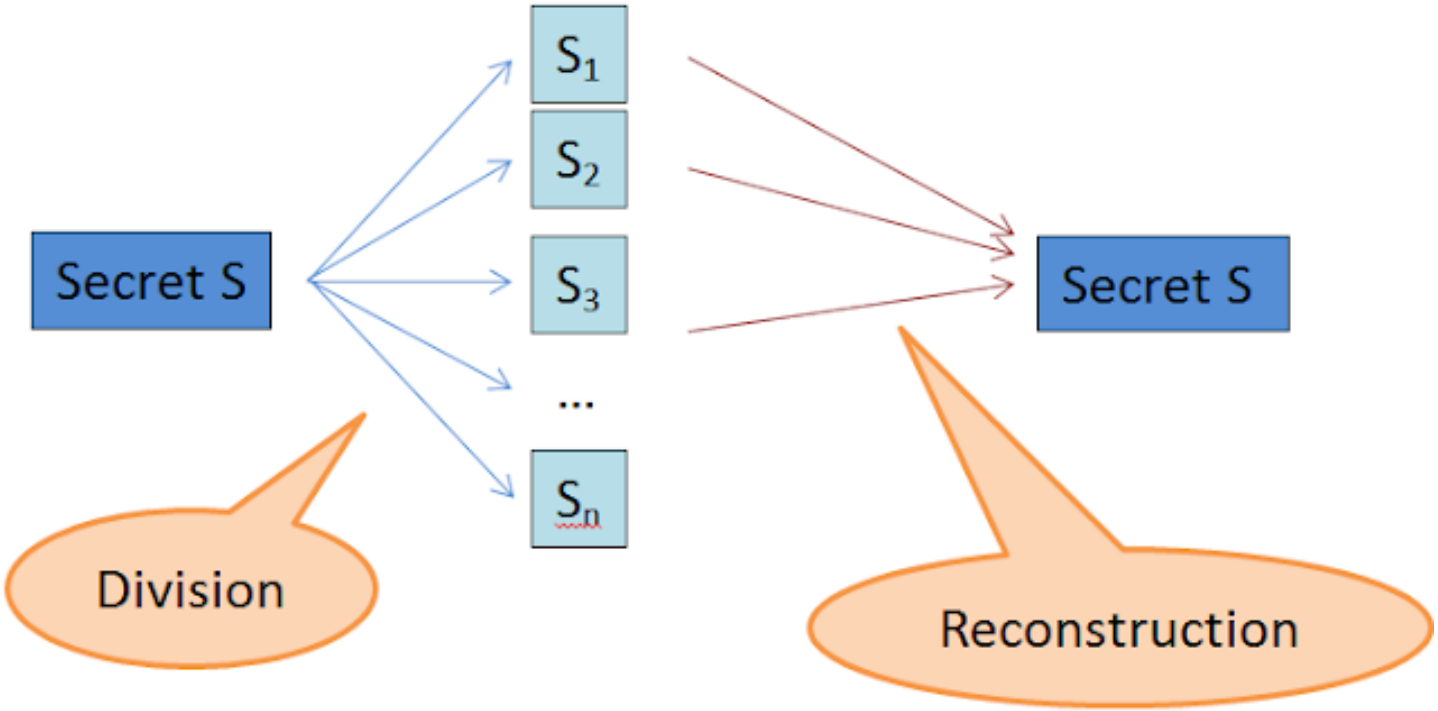
- Plain text gets "hashed"
- Extremely difficult to reverse
- Can verify integrity of data

Hash Function `https://bit.ly/1bgyDDz`

Message authentication



Secret Shares



- Keep data "secret" when sharing with multiple entities
- Each entity gets part of it

Secret Shares `https://bit.ly/2GoRTs7`

Analysis Background

- Threats and vulnerabilities
- Threat Model
- Security Requirements

Outline

KSS Model

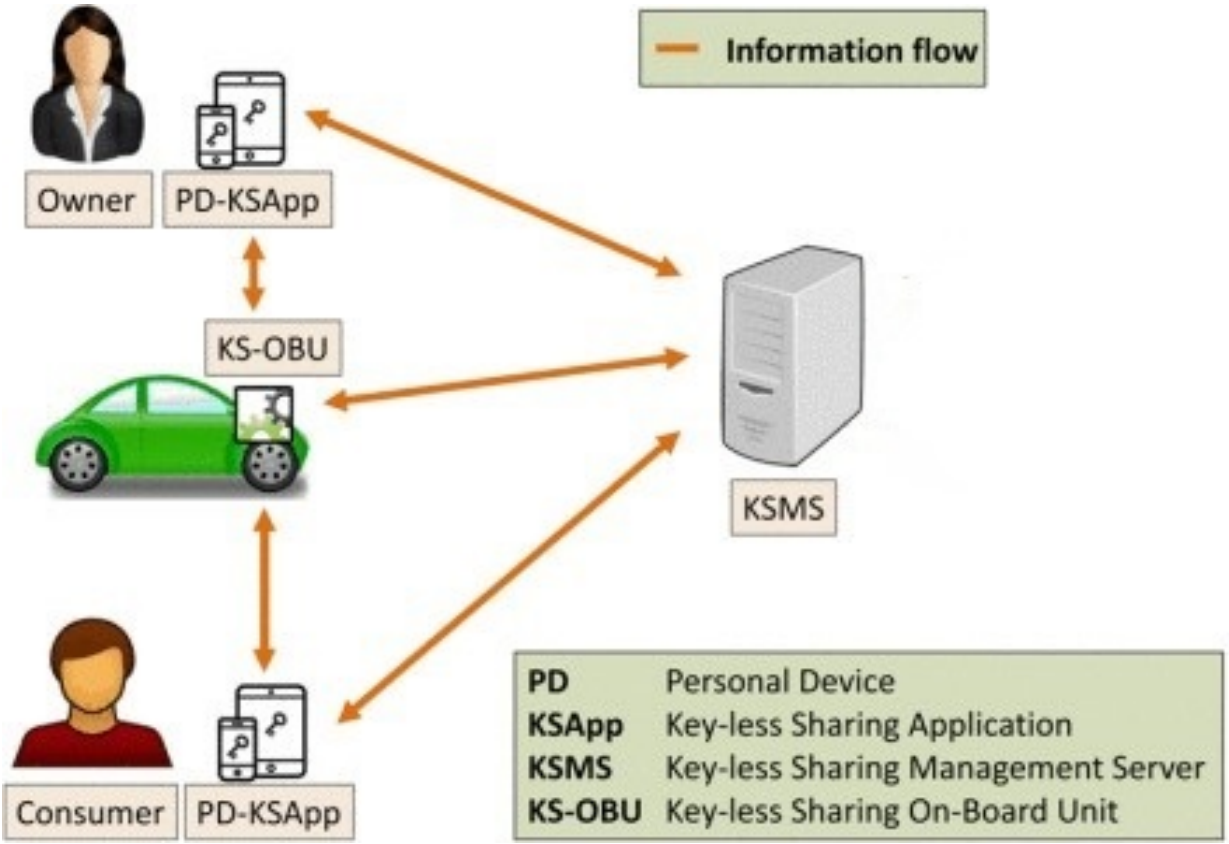


Figure: KSS Model modified from Symeonidis et al. “Keyless car sharing system: A security and privacy analysis”

Threat Model

- Users: "Untrustworthy or even malicious"
- Keyless Sharing Management Server (KSMS): "Honest-but-curious or even semi-honest"
- Keyless Sharing On-Board Unit (KS-OBU): "Untrustworthy but tamper evident"
- Keyless Sharing App (KSApp): "Untrustworthy but tamper evident"

Threat Model and Security Requirements

- Confidentiality
- Non-repudiation
- Integrity

Threat Model and Security Requirements

- Confidentiality
- Non-repudiation
- Integrity

Threat Model and Security Requirements

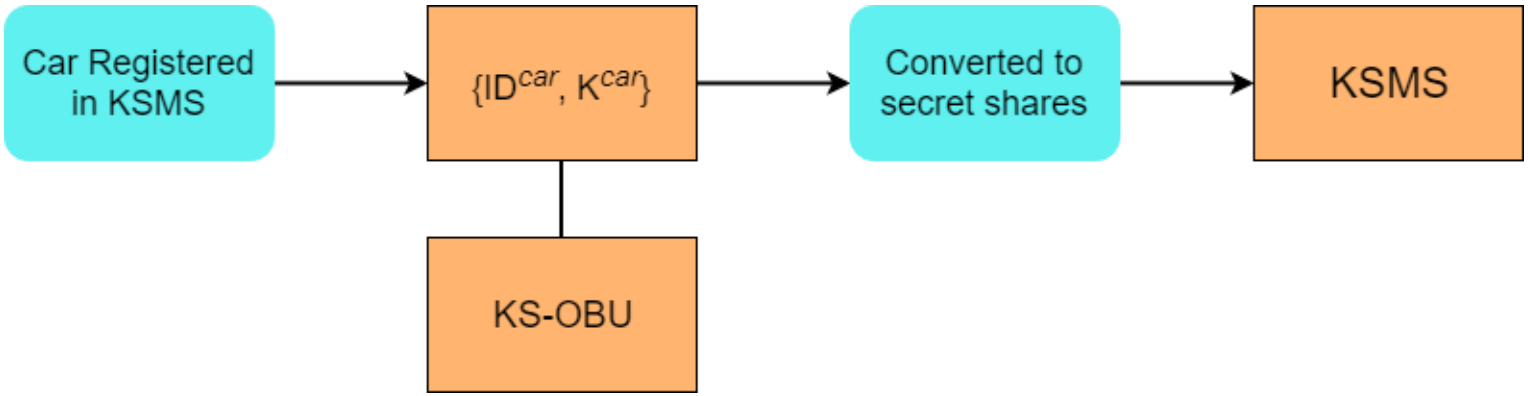
- Confidentiality
- Non-repudiation
- Integrity

Outline

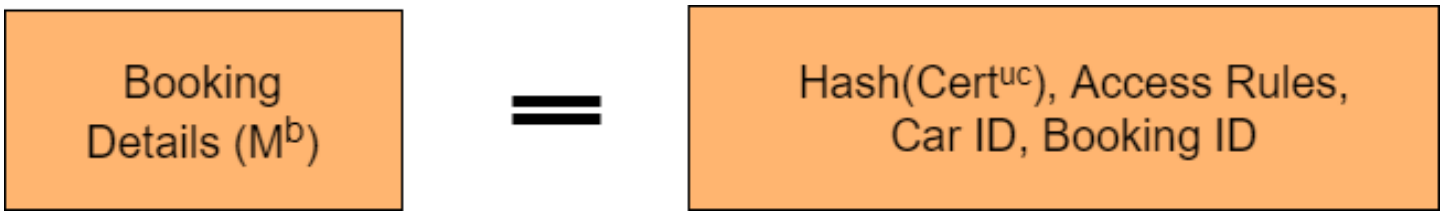
SePCAR overview

- Symeonidis et. al [2]
- Shares the KSS Model
- Decentralized KSMS with multiple servers
- Assumes booking has been agreed upon
- Public Ledger

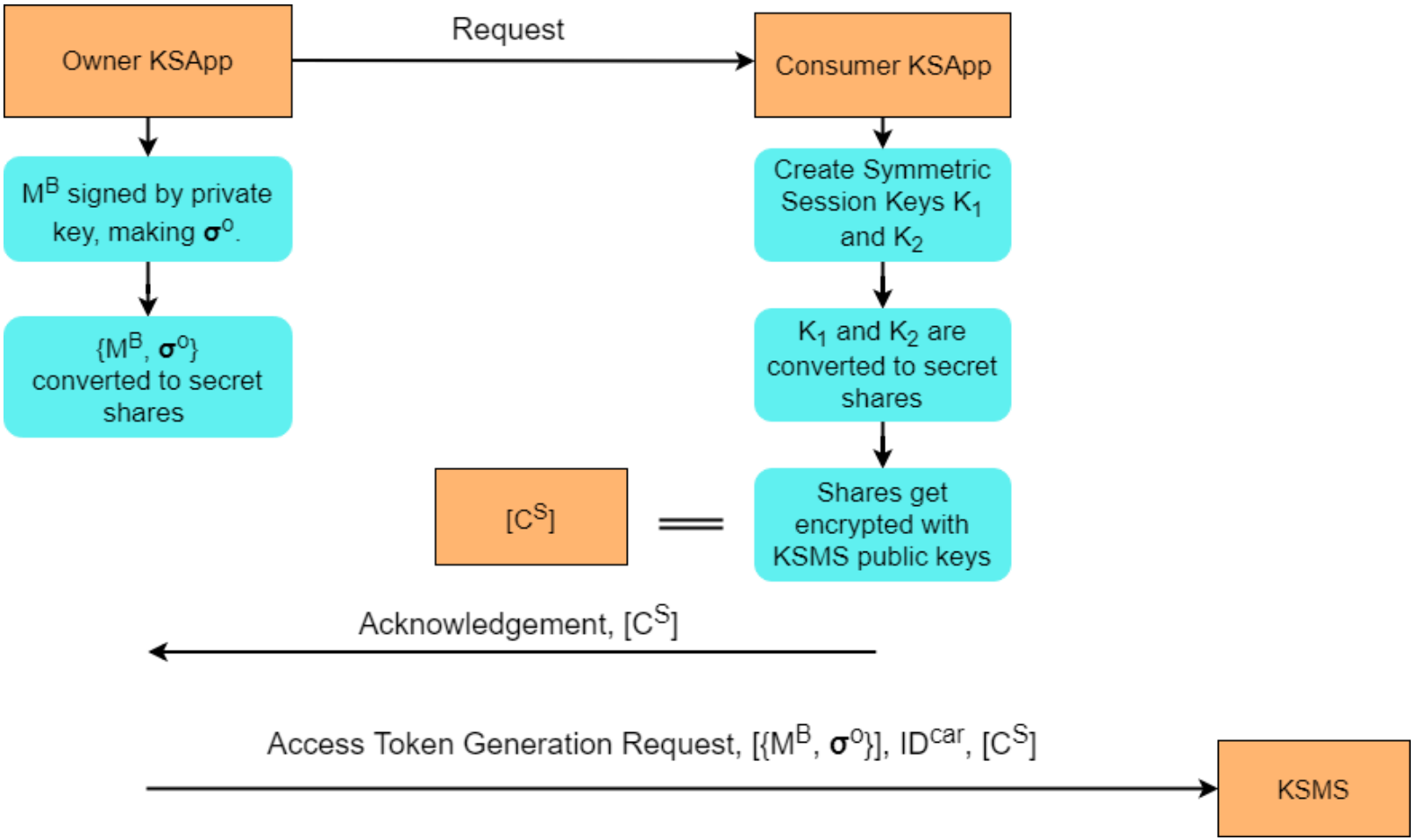
Car Key Distribution



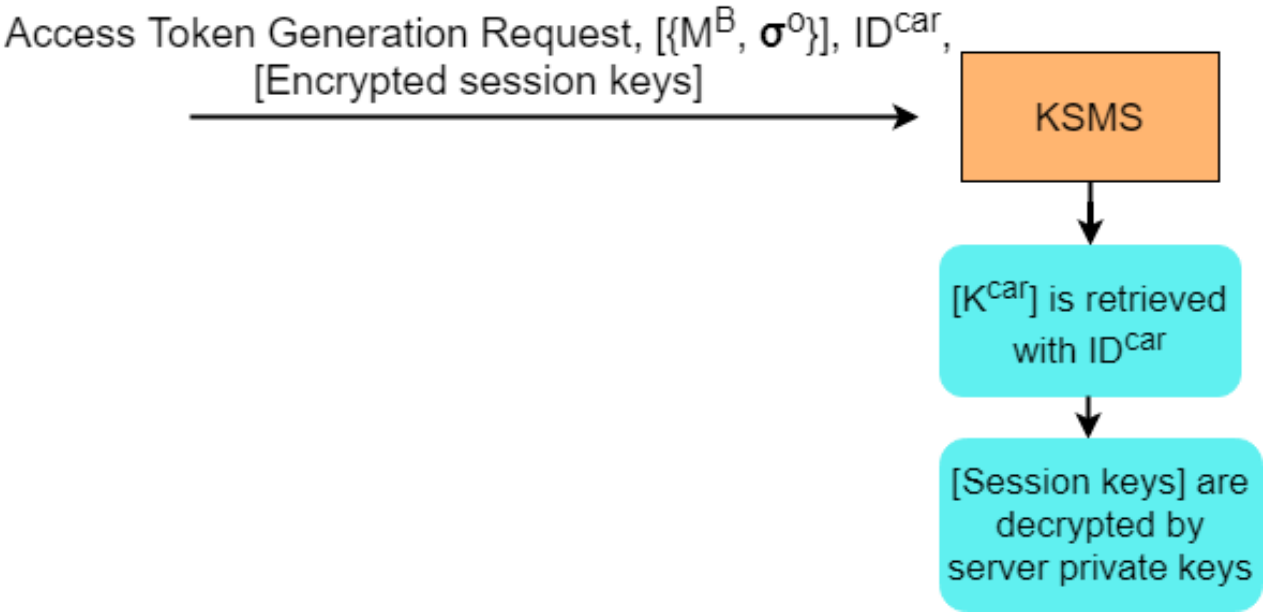
Booking Details



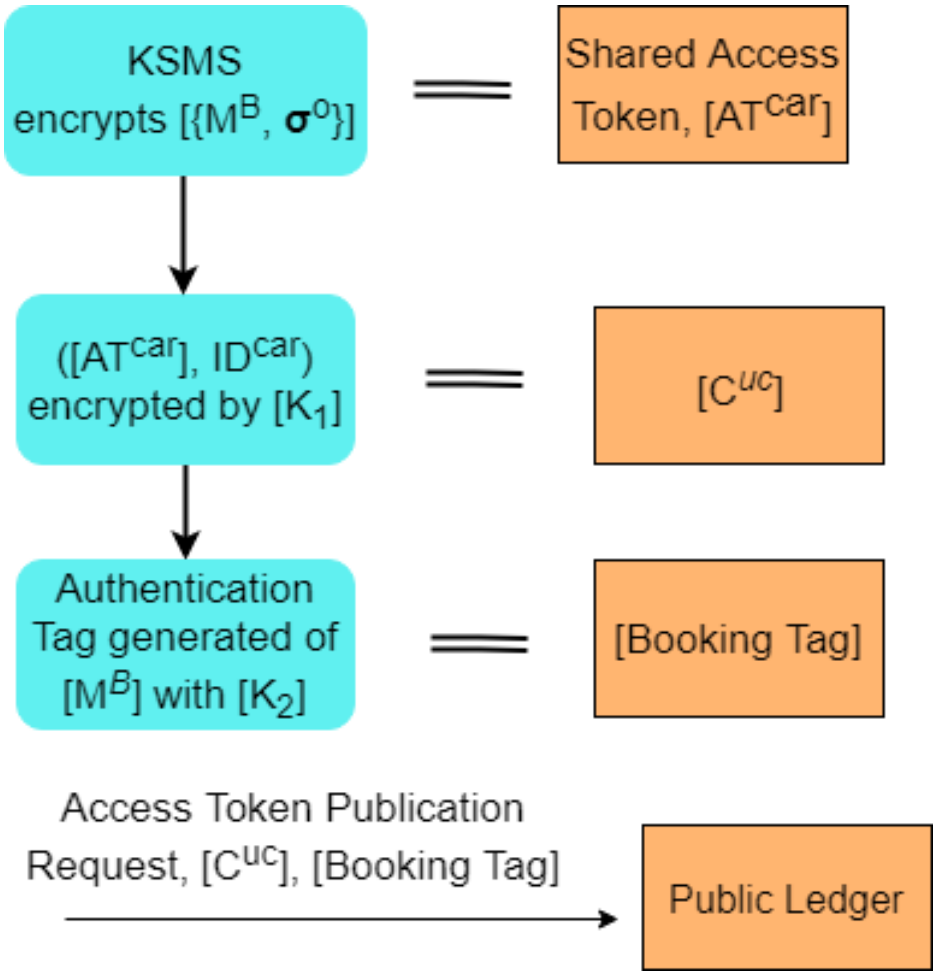
Session Key Generation



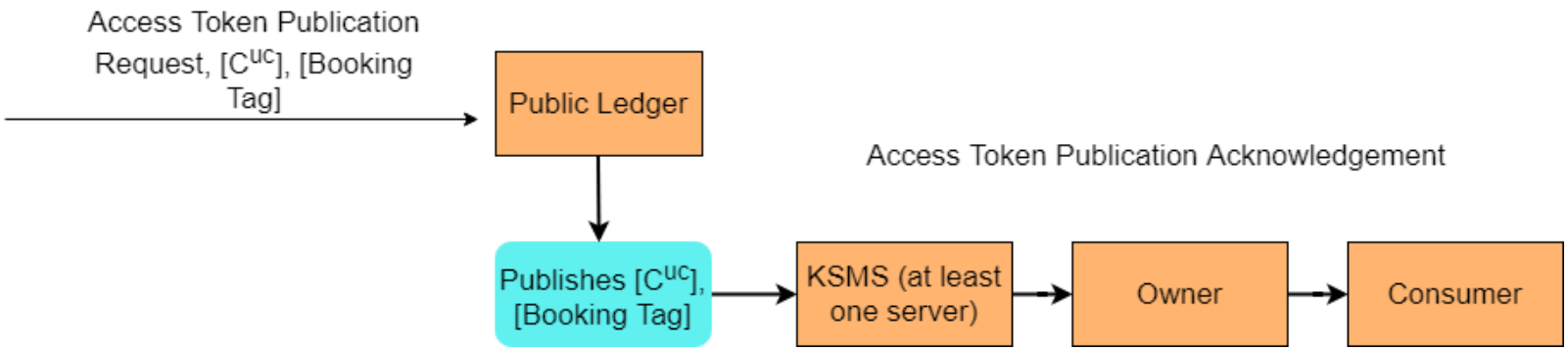
Access Token Generation



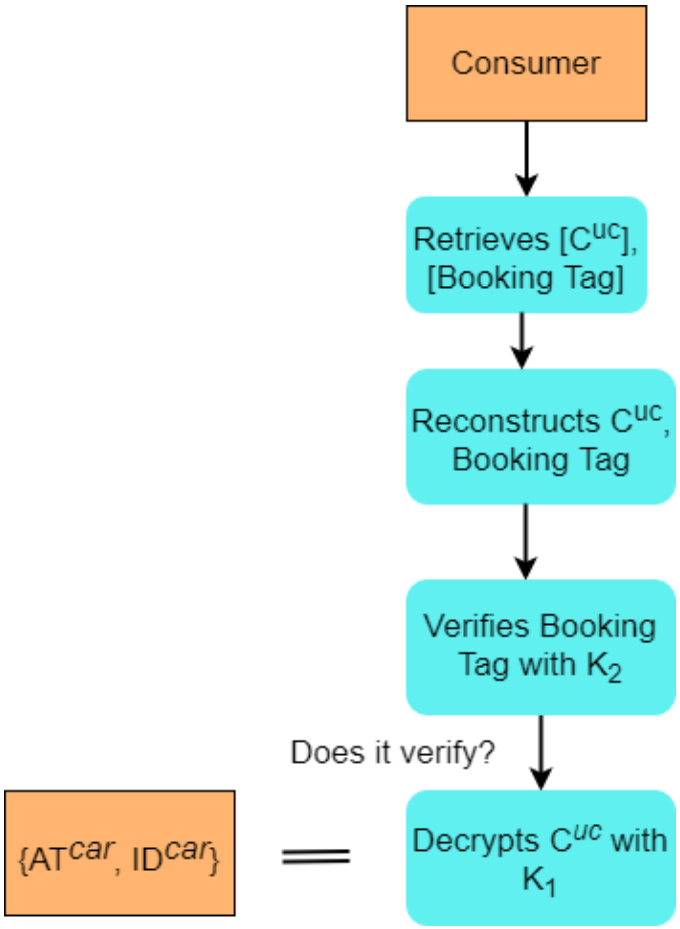
Access Token Generation



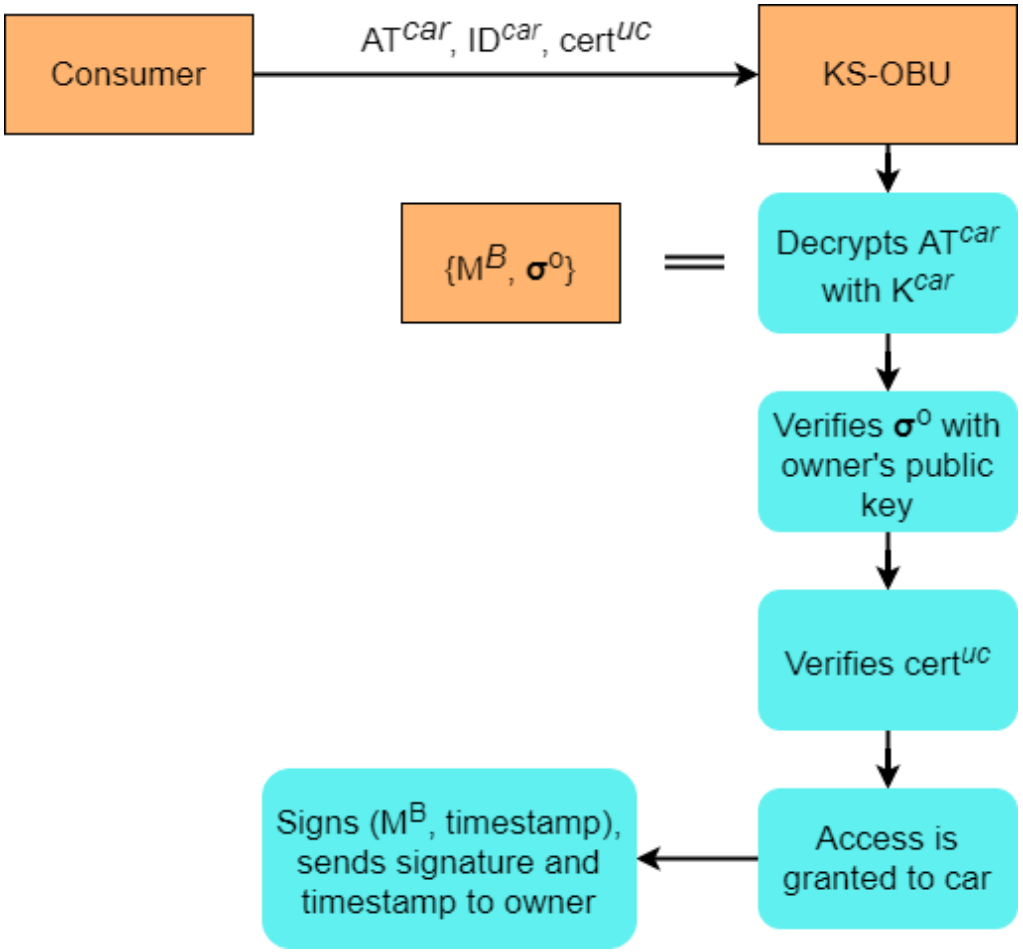
Access Token Distribution



Access Token Distribution



Car Access


Consumer
AT^{car}, ID^{car}, $cert^{uc}$
KS-OBU
$\{M^B, \sigma^O\}$
Decrypts AT^{car} with K^{car}
Verifies σ^O with owner's public key
Verifies $cert^{uc}$
Access is granted to car
Signs (M^B, timestamp), sends signature and timestamp to owner

Confidentiality

- Secret sharing of Booking Details
- Encrypted access token
- Secret sharing of K^{car}

Confidentiality

- Secret sharing of Booking Details
- Encrypted access token
- Secret sharing of K^{car}

Confidentiality

- Secret sharing of Booking Details
- Encrypted access token
- Secret sharing of K^{car}

Non-repudiation

- Origin of access token (signed booking details)
- Delivery of access token (notice sent to owner)

Non-repudiation

- Origin of access token (signed booking details)
- Delivery of access token (notice sent to owner)

Integrity

- Booking details signed by owner

Acknowledgements

- Thank you to Elena Machkasova for the helpful feedback.

End

Questions?

References

- Symeonidis, M. A. Mustafa, and B. Preneel, “Keyless car sharing system: A security and privacy analysis,” *2016 IEEE International Smart Cities Conference (ISC2)*, 2016.
- Symeonidis I., Aly A., Mustafa M.A., Mennink B., Dhooghe S., Preneel B. (2017) SePCAR: A Secure and Privacy-Enhancing Protocol for Car Access Provision. In: Foley S., Gollmann D., Snekkenes E. (eds) Computer Security â ESORICS 2017. ESORICS 2017. Lecture Notes in Computer Science, vol 10493. Springer, Cham