Secure and Privacy-Preserving Car-Sharing Systems

Lukas Malina, Petr Dzurenda, Norbert Lovinger, Ijeoma Faustina Ekeh*, Raimundas Matulevičius*

Brno University of Technology, *University of Tartu
malina@vut.cz

ARES/SP2I 2024

Co-funded by the European Union

Motivation, Research Questions and Contributions

- Our work analyzes **Car-Sharing Systems** (CSS) and its security and privacy features.

- **RQ1**: What are security and privacy threats in CCS and which privacy-preserving techniques (PETs) can be suitable?
- **RQ2**: How to design a cryptographically secure car-sharing system that protects users' privacy and is practical for deployment on constrained devices and handheld devices?

- **Analysis** of legal aspects, PETs and threats in CSS.
- **Proposal** of privacy-preserving solution for CSS based on group signatures
- Security and performance **assessment** of the proposal.

Threats and Legal Issues

- General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and Digital Service Act (DSA) increased the **transparency** of how user data are processed.
- CSS suffers by typical threats such as **man-in-the-middle attack**, **impersonation attack**, **data tampering attack**, **unauthorized access**, etc.
- More details in the paper.

PETs in CSS

- For CCS we detect these useful PETs:
  - **Data Anonymization Techniques** - e.g. masking vehicle license plates and user IDs in trip records, generalizing trip start/end locations, etc.
  - **Secure Multi-party Computation (SMPC)** - e.g. calculating the price per ride, average trip distance, and more, without revealing individual user data.
  - **Zero-Knowledge Proofs (ZKP)** - e.g. proving a user's valid driver's license without disclosing personal details.
  - **Group Signatures (GS)** - e.g. proving access to vehicles, holding valid access tokens (GS enable users to sign messages on behalf of group to preserve anonymity.)
- Our solution deploys Kim *at al.*'s group signature scheme from 2023 [3] (KSAP23).

Our Solution

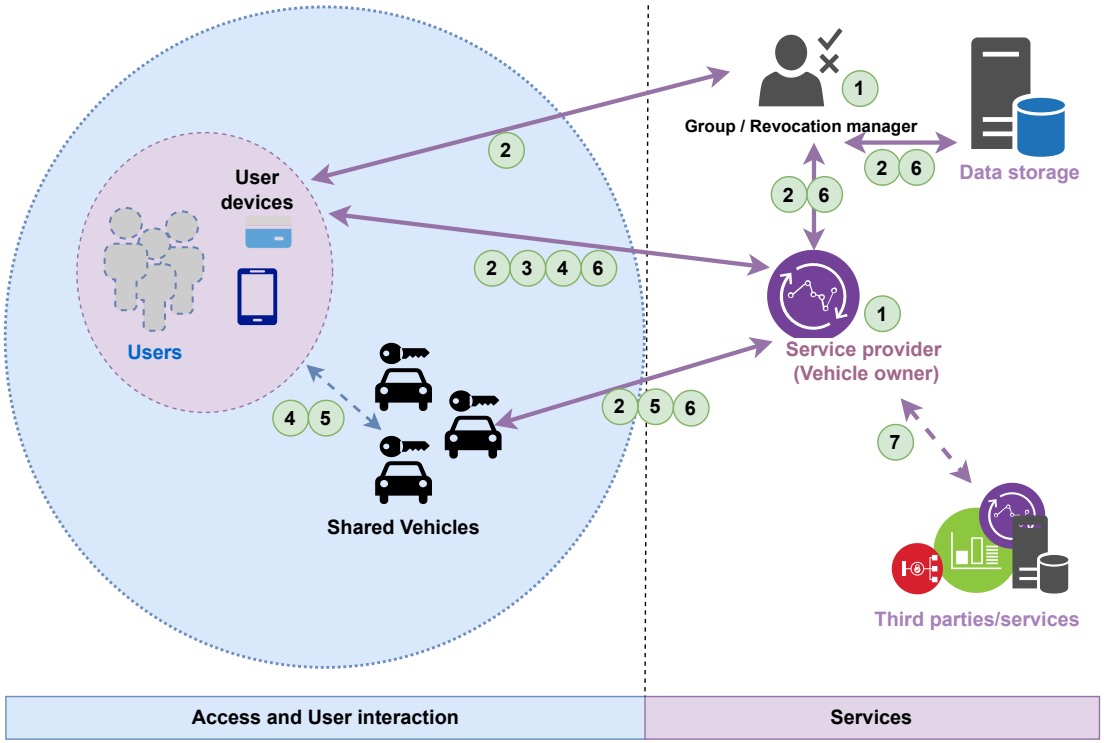
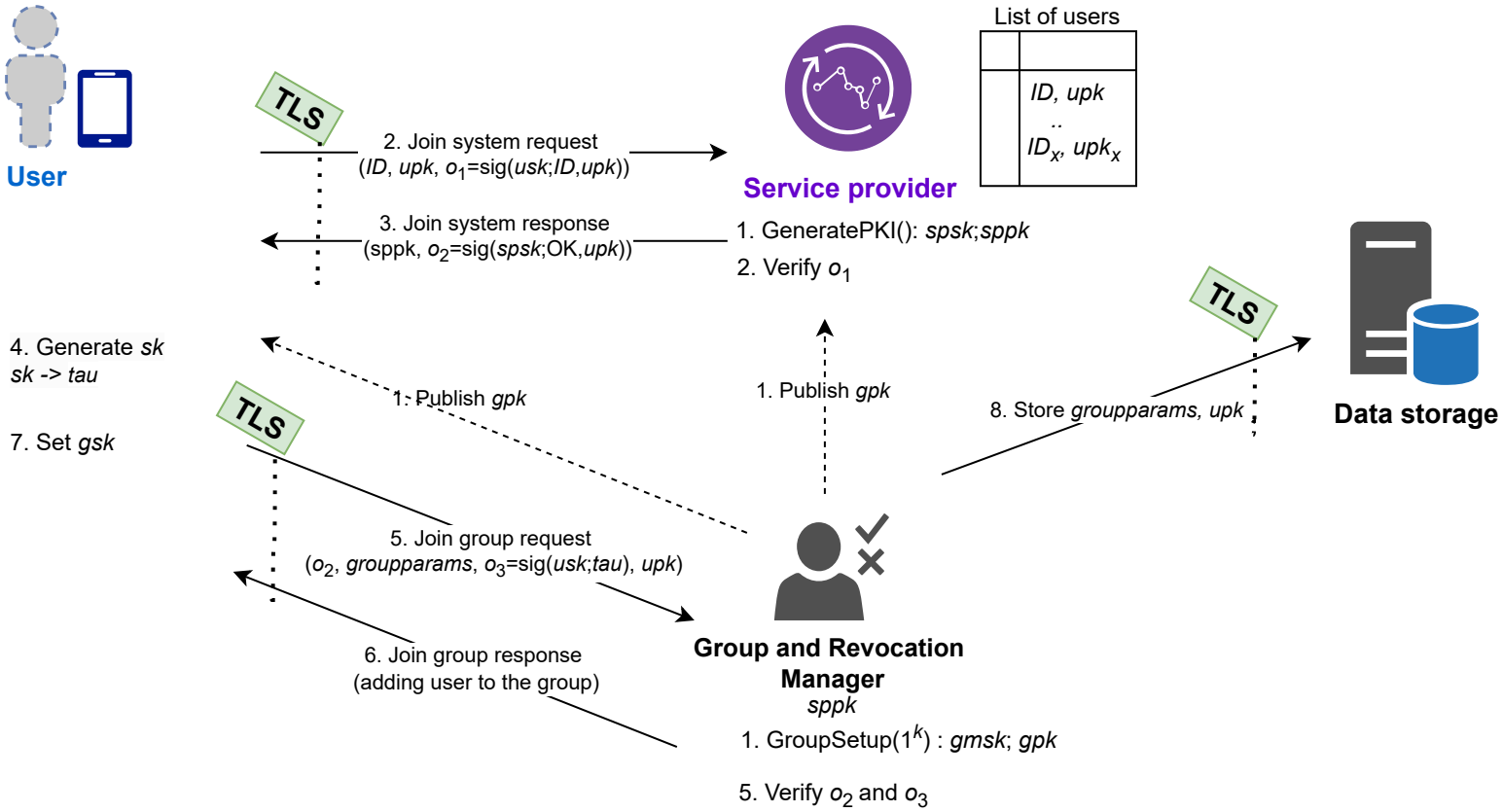
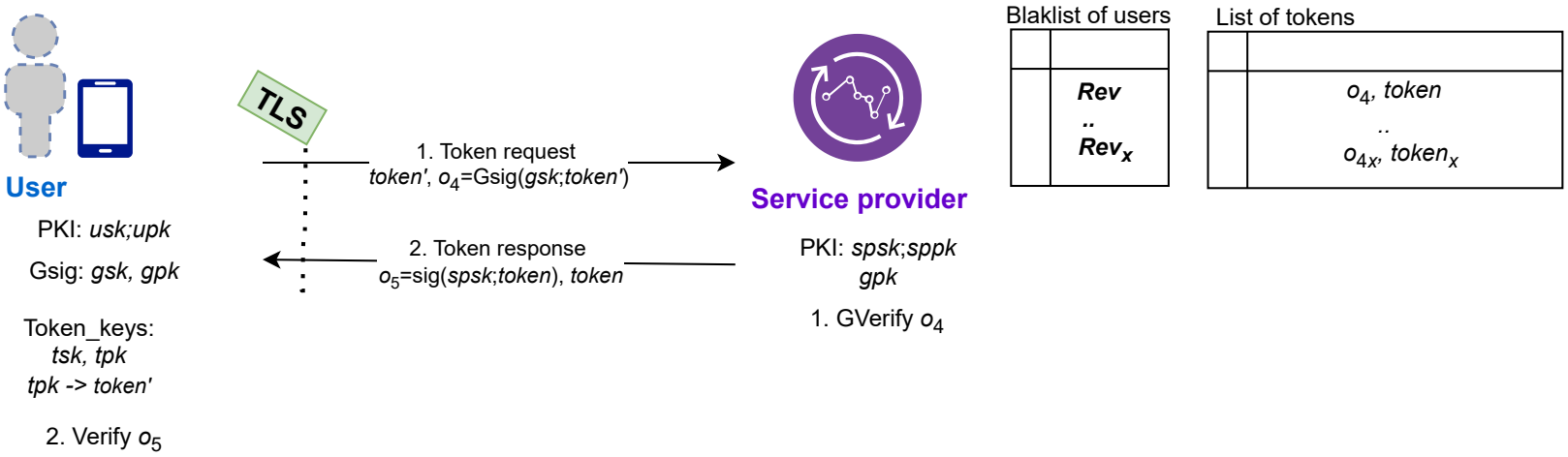


Figure: Entities and phases in our solution based on group signatures (KSAP23 scheme [3]).

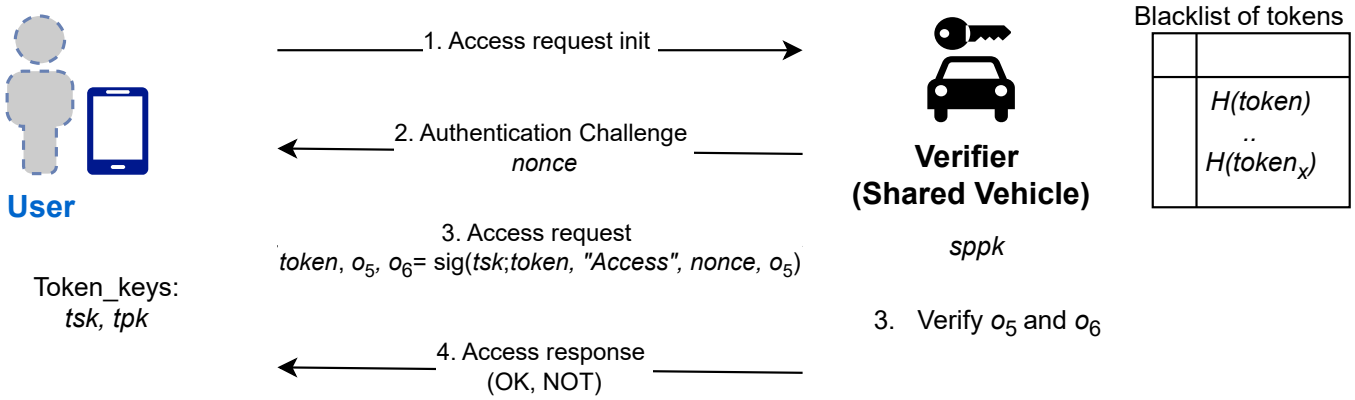
Solution Phases - Registration/Join



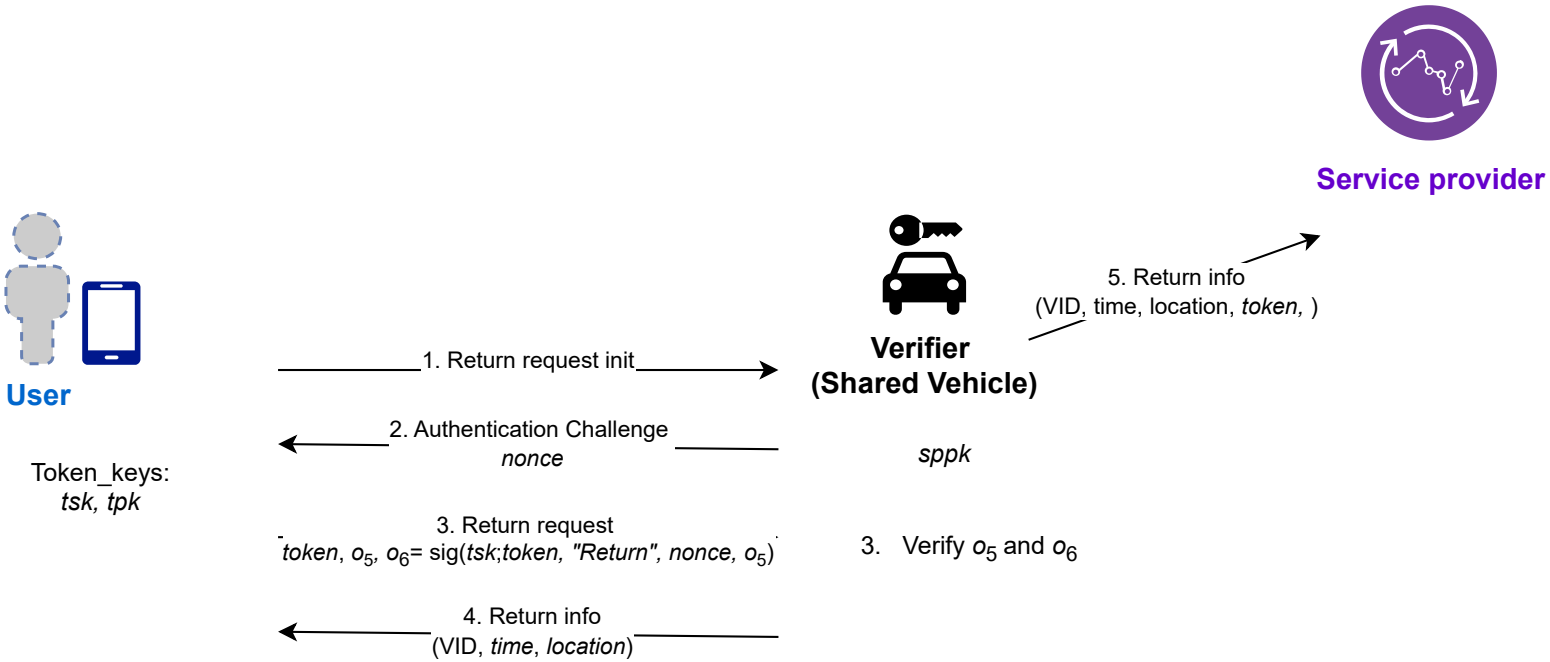
Solution Phases - Token Acquiring



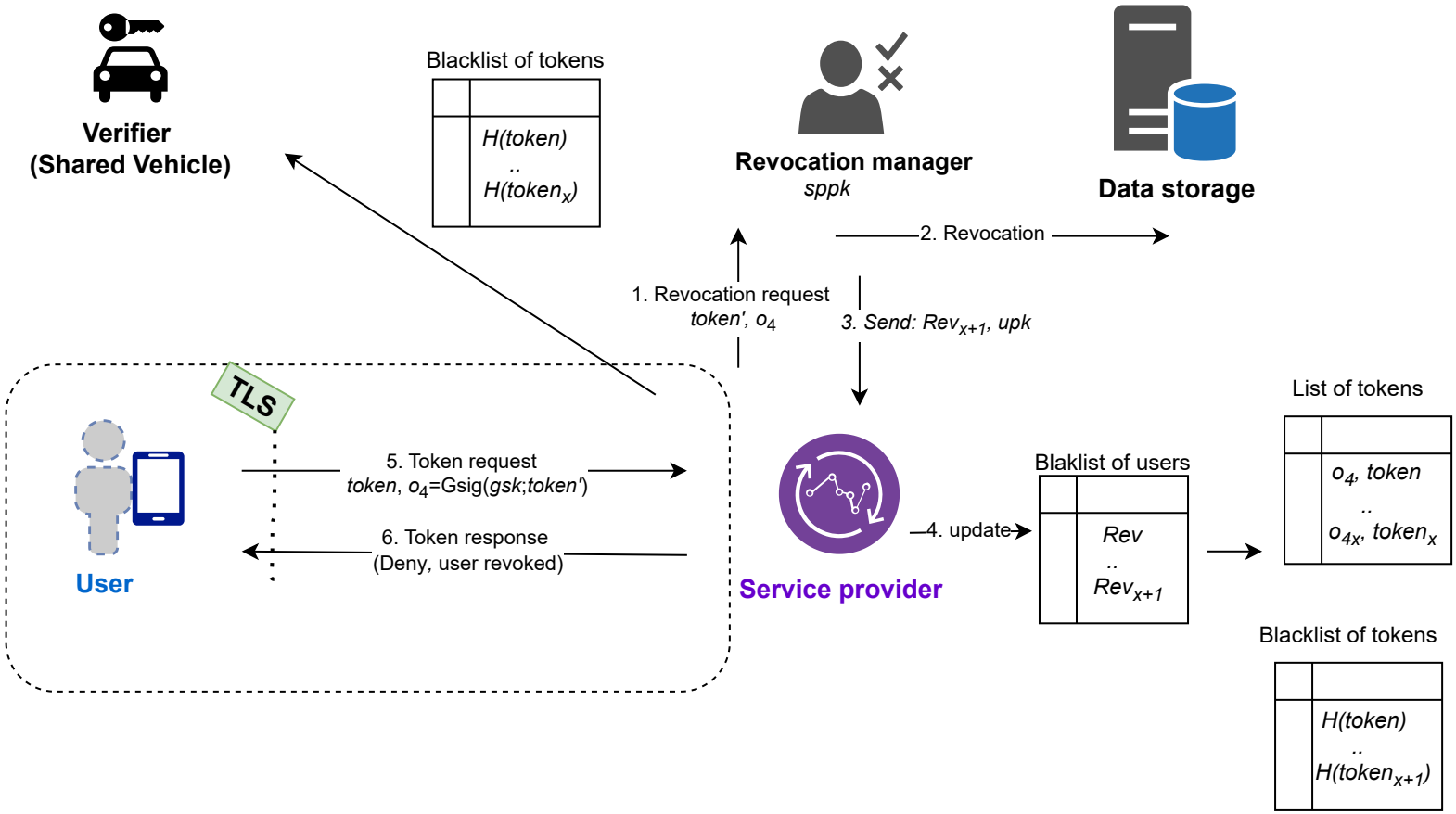
Solution Phases - Vehicle Access



Solution Phases - Vehicle Returning



Solution Phases - Revocation



Security Evaluation

The solution supports the following security properties (the full description is in the paper):

- **Soundness and completeness** - by phases, rules and group signatures (GS).
- **User anonymity** - by using GS.
- **User unlinkability** - by using GS.
- **Token unforgeability** - by using asymmetric cryptography - dig. signature (DS).
- **Token non-delegability** - by using DS.
- **Non-repudiation** - by using DS and GS.
- **Traceability** - by cooperation of GRM and SP, SP can detect the identity of malicious users.
- **Revocation** - by cooperation of GRM and SP. Blacklist of revoked users.

Performance Evaluation

Our solution deploys the group signature KSAP23 [3] that requires:

- for signing: 12 exponentiations in G_1,
- for verification: 3 pairings and 10 exponentiations in G_1,
- signature length: 5352 b (composed of 6 $|G_1|$ and 3 $|Z_p|$),
- KSAP23 scheme [3] allows efficient revocation but is less efficient than BBS04 [1].

Performance Comparison

Phase:	This work	PRESTvO (Groza *et al.* [2])
Registration / Setting	3 Sig/Ver	7 IdSig/IdVer
Acquiring / Delegation	1 Sig/Ver + 1 Gsig/Gver	2 Gsig/Gver + 2 IdSig/IdVer
Access / Execute	1 Sig/Ver	(1 Gsig/Gver or 1 IdSig/IdVer) + 1 IdSig/IdVer
Return	1 Sig/Ver	not proposed
Revocation	1 GS Revocation	not described

Conclusion

- We presented main legislative, security and privacy issues and threats in car-sharing services.
- We proposed the efficient and practical privacy-preserving security solution for car-sharing systems.
- The solution allows instant revocation and requires less operations (compared with related solution PRESTvO).
- Future Work - focus on a beta implementation and field tests on real vehicles.

Thank you!

This work is supported by the DOPRAVA 2020+ programme under the Technology Agency of the Czech Republic grant agreement No. CK03000040 (Protection of data flows in shared means of transport) and by the European Union under Grant Agreement No. 101087529 CHESS.

malina@vut.cz

T A
Č R

BRNO UNIVERSITY OF TECHNOLOGY

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Co-funded by the European Union

References


Boneh, D., Boyen, X., and Shacham, H.
Short group signatures.
In *Crypto* (2004), vol. 3152, Springer, pp. 41–55.


Groza, B., Andreica, T., Berdich, A., Murvay, P.-S., and Gurban, E. H.
Prestvo: Privacy enabled smartphone based access to vehicle on-board units.
IEEE Access 8 (2020), 119105–119122.


Kim, H., Sanders, O., Abdalla, M., and Park, J. H.
Practical dynamic group signatures without knowledge extractors.
Designs, Codes and Cryptography 91, 3 (2023), 853–893.