Karlsruhe Institute of Technology

Division II – Informatics, Economics, and Society

Institute of Theoretical Informatics (ITI) – Cryptography and IT Security

PriPay - Privacy-protecting Payment Systems

A cryptographic building block for collecting and redeeming points

PriPay is an innovative wallet technology for realization of pre/postpayments and loyalty systems. It is the first such system that is at the same time offline-capable, efficient, privacy-protecting and provably secure. Previous comparable systems only fulfill a subset of the properties mentioned. The privacy protection of PriPay users and the system's security against fraud have been proven mathematically. This means that the protocol is protected against all attackers, even those with as yet unknown attack strategies. The security properties of other systems, on the other hand, are often described only heuristically. Thanks to innovative technologies, PriPay is efficient enough to be used on devices with limited resources, such as smartphones. Since the wallet stores abstract "points", PriPay can be used to implement a variety of applications in a privacy-protecting and secure manner, such as collecting monetary units for pre/postpayment systems, or collecting loyalty points for loyalty program ratings for reputation systems.

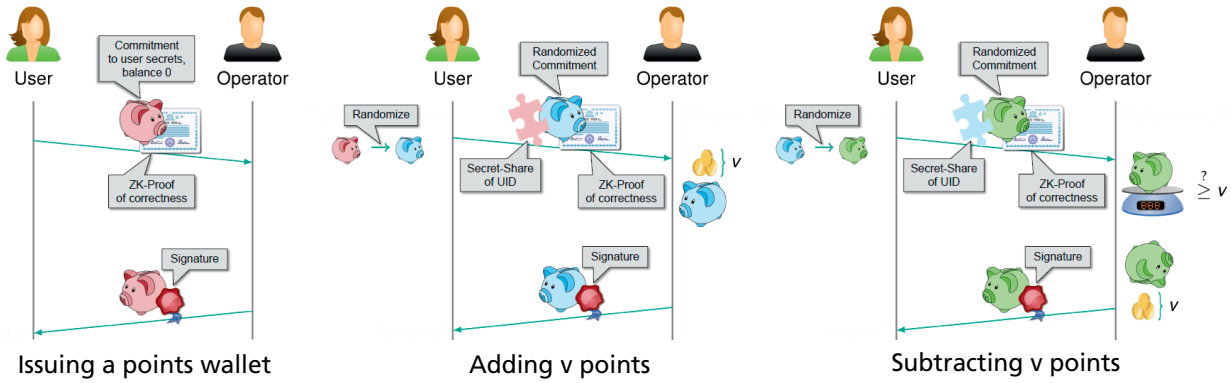
Underlying Technique

PriPay is a cryptographic building block that enables the secure, practical and at the same time anonymous transmission of abstract points. PriPay combines a multitude of innovative aspects:

1. Each wallet is managed exclusively locally and only directly on the user's device. Keeping of "shadow accounts" by the operator of the payment system is prevented.
2. With each transaction, a user exchanges his/her wallet for a new one with a controlled change in amount. The saved balance is not revealed. Before a payment transaction, it can nevertheless be guaranteed that the wallet contains a sufficiently high amount.
3. Data protection is realized in a provably secure manner without resorting to the subsequent application of pseudonymization techniques, as they are frequently used in payment systems. Although each user has a unique public key, this public key is not revealed in transactions. This prevents tracking right from the start.
4. Point of Sales can operate without a permanent network connection. Double-spending detection identifies fraudsters retrospectively and proves a case of fraud w.r.t. third parties.
5. To settle disputes and mitigate technical errors, an optional mechanism can be integrated that allows payments to be deanonymized selectively and only with the support of a Trusted Third Party.

The graphic outlines how PriPay works. At first, the user registers with the operator using his/her public key. In the scope of a cryptographic protocol, the user and the operator together then create the wallet (the piggy bank shown in the graphic). The latter contains, among other things, a random serial number, the balance "zero", and the secret key of the user. The user proves to the operator by means of efficient Zero-Knowledge Proofs (ZKP) that he/she has generated the wallet correctly and that it actually contains his/her secret key. This ensures that only he/she can use the wallet. The secret key and the serial number are not leaked to the operator. Finally, the operator signs the wallet to prevent manipulation by the user.

If the user wishes to use the wallet, he/she may not send it to the operator unchanged, but must randomize it first to avoid recognition by the latter. However, only the unchanged wallet is certified. At this point, ZKP will again be used to prove indirect certification: The user proves that the new wallet, except for a new serial number, has the same content as the original wallet and that this original wallet is certified. Now, the operator can add any number of points to the new wallet and sign it again. The withdrawal of points works analogously, with the user additionally proving that his/her wallet contains enough points.



How PriPay works

Randomization and ZKP guarantee anonymity. Signatures and ZKP prevent tampering. To prevent the reuse of an obsolete wallet, a double-spending detection mechanism is provided in addition. If a fraudulent user uses an outdated version of his/her wallet a second time, the operator learns the user's public key and can now hold him/her to account.

Prototype and Efficiency

To prove the usability and efficiency of PriPay, a prototype prepay system was implemented for the "canteen system" application scenario: An Android app on the user's smartphone implements the wallet, which he/she can charge at terminal stations. A turnstile grants access if the wallet on the smartphone has sufficient credit. A database application with a web interface implements the operator's backend. With this prototype, the practical performance could be demonstrated. Various optimization options (e.g., precalculation of protocol steps, better NFC transmission) remain to be implemented.

Karlsruhe Institute of Technology (KIT)
Institute of Theoretical Informatics (ITI) – Cryptography and IT Security
Dr. Andy Rupp
Am Fasanengarten 5
76131 Karlsruhe, Germany
Phone: +49 721 608-46289
Email: andy.rupp@kit.edu
http://crypto.iti.kit.edu

Karlsruhe Institute of Technology (KIT)
Institute of Theoretical Informatics (ITI) – Cryptography and IT Security
Matthias Nagel
Am Fasanengarten 5
76131 Karlsruhe, Germany
Phone: +49 721 608-46294
Email: matthias.nagel@kit.edu
http://crypto.iti.kit.edu

Gefördert durch DFG Deutsche Forschungsgemeinschaft

GEFÖRDERT VOM Bundesministerium für Bildung und Forschung

Karlsruhe Institute of Technology (KIT) · President Professor Dr.-Ing. Holger Hanselka · Kaiserstraße 12 · 76131 Karlsruhe, Germany · www.kit.edu