Karlsruher Institut für Technologie

Bereich II – Informatik, Wirtschaft und Gesellschaft

Institut für Theoretische Informatik (ITI) – Kryptographie und Sicherheit

PriPay – Privatsphärenschützende Zahlungssysteme

Ein kryptographischer Baustein zum Punktesammeln und -einlösen

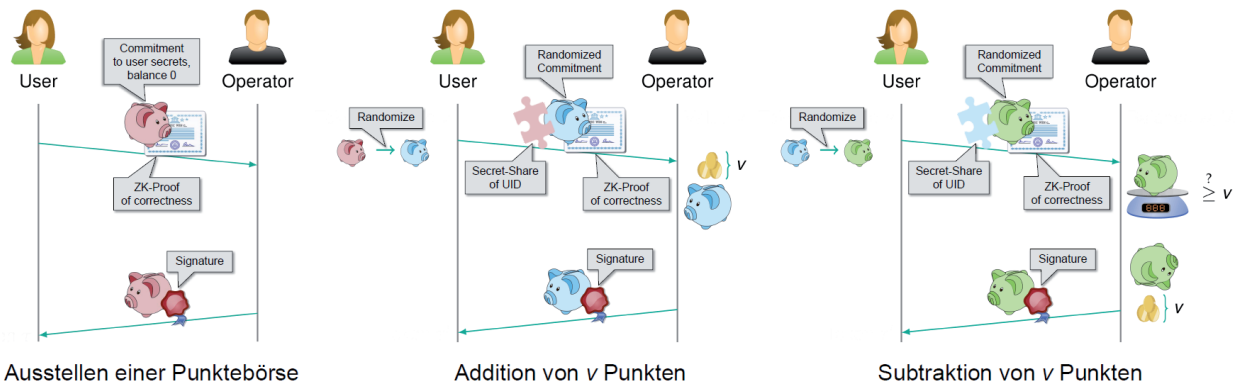
PriPay ist eine innovative Geldbörsentechnologie zur Realisierung von Pre-/Postpayments und Loyality-Systemen. Es ist das erste derartige System, das gleichzeitig offline-fähig, effizient, privatsphärenschützend und beweisbar sicher ist. Bisherige, vergleichbare Systeme erfüllen immer nur eine Teilmenge der genannten Eigenschaften. Bei PriPay wurden der Privatsphärenschutz der Nutzer und die Systemsicherheit des Betreibers gegen Betrug mathematisch bewiesen. Dies bedeutet, dass das Protokoll gegen alle Angreifer, auch solche mit noch unbekannter Angriffsstrategie, nachweislich geschützt ist. Die Sicherheitseigenschaften anderer Systeme sind hingegen häufig nur heuristisch beschrieben. Dank innovativer Techniken ist PriPay sehr performant und kann auch auf Geräten mit eingeschränkter Leistungsfähigkeit, wie z.B. Smartphones, eingesetzt werden. Da die Geldbörse abstrakte „Punkte" speichert, können auf Basis von PriPay vielfältige Anwendungen privatsphärenschützend und sicher realisiert werden, wie z.B. das Sammeln von Geldeinheiten für Pre-/Postpayment-Systeme, oder das Sammeln von Treuepunkten für Loyalitätsprogramme sowie von Bewertungspunkten für Reputationssysteme.

Die zugrundeliegende Technik

PriPay ist ein kryptographischer Baustein, der die sichere, praktikable und zugleich anonyme Übertragung von abstrakten Punkten ermöglicht. Hierbei vereint PriPay eine Vielzahl innovativer Aspekte:

1. Jede Geldbörse wird ausschließlich dezentral und nur unmittelbar auf dem Gerät des Nutzers verwaltet. Die Führung von „Schattenkonten" durch den Operator des Zahlungssystems ist ausgeschlossen.
2. Bei jeder Transaktion tauscht ein Nutzer seine Geldbörse gegen eine neue mit einem kontrolliert veränderten Betrag ein. Dabei wird der gespeicherte Punktestand nicht aufgedeckt. Vor einem Bezahlvorgang kann dennoch garantiert werden, dass die Börse einen ausreichend hohen Betrag enthält.
3. Datenschutz wird beweisbar sicher realisiert, ohne auf die nachträgliche Anwendung von Pseudonymisierungstechniken zurückzugreifen, wie sie bei Zahlungssystemen häufig eingesetzt werden. Zwar besitzt jeder Nutzer einen eindeutigen öffentlichen Schlüssel; dieser wird jedoch bei Transaktionen nicht aufgedeckt. Dadurch wird Tracking schon im Ansatz verhindert.
4. Point-of-Sales können ohne ständige Netzwerkverbindung agieren. Durch Double-Spending-Detection werden Betrüger im Nachhinein identifiziert und ein Betrugsfall gegenüber Dritten nachgewiesen.
5. Um Dispute zu schlichten und technische Fehler abzufangen, kann optional ein Mechanismus integriert werden, der es erlaubt, Zahlungen selektiv und nur mit Unterstützung einer dritten, vertrauenswürdigen Partei zu deanonymisieren.

Die Grafik (siehe Rückseite) skizziert die Funktionsweise von PriPay. Zu Beginn registriert sich ein Nutzer mit seinem öffentlichen Schlüssel beim Operator. Im Rahmen eines kryptographischen Protokolls erstellen beide gemeinsam die Börse (das Sparschwein in der Grafik). Sie enthält in verdeckter Form u.a. eine zufällige Seriennummer, den Punktestand „Null" sowie den geheimen Schlüssel des Nutzers. Der Nutzer weist dem Operator mittels effizienter Zero-Knowledge-Beweise (ZKB) nach, dass er die Börse korrekt erzeugt hat und diese tatsächlich seinen geheimen Schlüssel enthält. Das sorgt dafür, dass nur er die Börse nutzen kann. Der Operator erfährt dabei nichts über den geheimen Schlüssel oder die Seriennummer. Abschließend signiert der Operator die Börse, um nutzerseitige Manipulationen zu verhindern.
Möchte der Nutzer die Börse verwenden, darf er sie nicht unverändert an den Operator senden, denn dieser würde sie wiedererkennen. Daher muss der Nutzer seine Börse zunächst randomisieren. Allerdings besitzt nur die unveränderte Börse eine Zertifizierung. An dieser Stelle werden wieder ZKB eingesetzt, um eine indirekte Zertifizierung nachzuweisen: Der Nutzer weist nach, dass die neue



Die Funktionsweise von PriPay

Börse, bis auf eine neue Seriennummer, den gleichen Inhalt besitzt wie die ursprüngliche und dass diese ursprüngliche Börse zertifiziert ist. Nun kann der Operator eine beliebige Anzahl von Punkten zur neuen Börse hinzufügen und diese wiederum signieren. Die Entnahme von Punkten funktioniert analog, wobei der Nutzer zusätzlich verdeckt nachweist, dass seine Börse genügend Punkte enthält.
Randomisierung und ZKB garantieren Anonymität. Signaturen und ZKB verhindern Manipulationen. Um einer Wiederverwendung einer veralteten Börse vorzubeugen, existiert zusätzlich ein Double-Spending-Detection-Mechanismus. Verwendet ein betrügerischer Nutzer eine veraltete Version seiner Geldbörse ein zweites Mal, erfährt der Operator den öffentlichen Schlüssel des Nutzers und kann diesen nun zur Verantwortung ziehen.

Prototyp und Effizienz

Um die Einsatzfähigkeit und Effizienz von PriPay nachzuweisen, wurde für das Anwendungsszenario „Kantinensystem“ ein prototypisches Prepay-System implementiert: Eine Android-App auf dem Smartphone des Nutzers realisiert die Geldbörse, die er an Terminalstationen aufladen kann. Eine Drehsperre gewährt Zutritt, wenn die Geldbörse des aufgelegten Smartphones ein hinreichendes Guthaben aufweist. Eine Datenbankanwendung mit Weboberfläche realisiert das Backend des Operators. Mit diesem Prototyp konnte die praxistaugliche Performanz belegt werden. Zahlreiche Optimierungsmöglichkeiten (z.B. Vorberechnung von Protokollschritten, bessere NFC-Übertragung) wurden dabei noch nicht implementiert.

Karlsruher Institut für Technologie (KIT)
Institut für Theoretische Informatik (ITI) –
Kryptographie und Sicherheit
Dr. Andy Rupp
Am Fasanengarten 5
76131 Karlsruhe
Telefon: +49 721 608-46289
E-Mail: andy.rupp@kit.edu
http://crypto.iti.kit.edu

Karlsruher Institut für Technologie (KIT)
Institut für Theoretische Informatik (ITI) –
Kryptographie und Sicherheit
Matthias Nagel
Am Fasanengarten 5
76131 Karlsruhe
Telefon: +49 721 608-46294
E-Mail: matthias.nagel@kit.edu
http://crypto.iti.kit.edu

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Karlsruher Institut für Technologie (KIT) · Präsident Professor Dr.-Ing. Holger Hanselka · Kaiserstraße 12 · 76131 Karlsruhe · www.kit.edu