A Real-World Solution to Anonymous Subscription and Discounts

Degree programme: BSc in Computer Science
Thesis advisors: Prof. Dr. Christian Grothoff, Prof. Dr. Emmanuel Benoist
Expert: Han van der Kleij

This thesis presents a solution for account-less and privacy-preserving subscriptions based on GNU Taler. The solution is convenient for customers, affordable for merchants, and resistant to abusive sharing of subscriptions. Conventional subscriptions allow constructing a personality profile that can reveal sensitive information about subscribers.

Motivation

Subscription-based services are more popular than ever, with a significant portion of digital goods, such as newspaper articles, music, movies, and TV shows, sold through this business model. These services are generally tied to a user account. As a result, the use of a subscription leaves a data trail. Service providers can use collected usage data to build a personality profile that can reveal information about political views, sexual orientation, health complications, or other sensitive topics. This information, in the wrong hands, can have critical implications, especially in regions with repressive regimes. Ideally, a solution to this problem also addresses the challenge of subscribers sharing their credentials with groups of people online.

Solution

Our solution utilizes a wallet storing digitally signed subscription tokens on the customer's device. A wallet can be a mobile app or integrated into a web browser as an extension. Such a browser extension allows for a seamless user experience using a token-based subscription in a web browser.

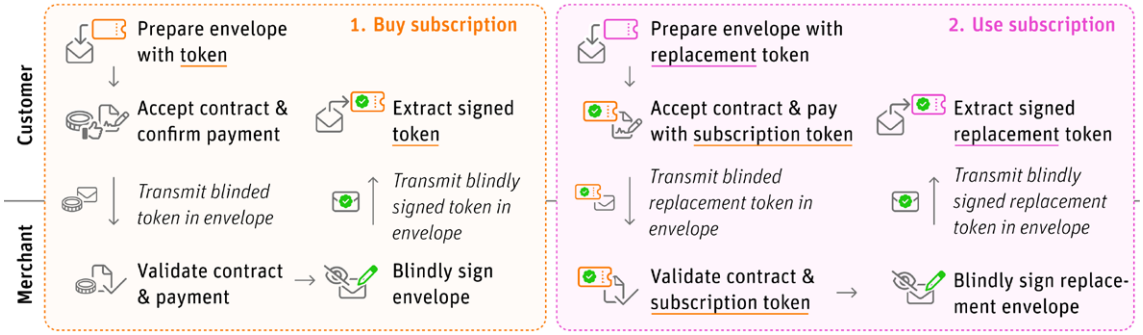
Upon purchasing a subscription, the merchant issues a blindly signed token to the customer, who then stores it in their digital wallet. The customer can subsequently use this token to access a subscription good, such as reading an article or watching a movie. Each token is used only once to ensure unlinkability. When a token is used, the merchant issues a fresh, blindly signed token to the customer in the same transaction.

The solution will be available as free and open source software as part of the GNU Taler payment system. This allows the code to be audited, adopted and modified by anyone, building trust and eliminating the vendor lock-in common to similar solutions.

The flexible design of the solution allows it to be used for a wide range of use cases beyond subscriptions. These include discounts, loyalty stamps, multi-entry event ticketing, membership programs, deposit systems, and privacy-preserving gifts. In addition, the solution's low operational costs, coupled with its built-in protection against abusive sharing of subscriptions, make it highly attractive to merchants.

Scan QR code for more information.

Christian Blättler
IT Security



Overview of buying and using a token-based subscription, that employs blind signatures for privacy.