Anonymous Subscriptions & Discounts

Problem

Subscription-based services are more popular than ever and they are generally tied to a user account. As a result, the use of a subscription leaves a data trail.

Symptoms

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.



Figure 1: Buying and using a token-based subscription, that employs blind signatures for privacy.

Christian Blättler

Solution

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.

((†ALER												
	You are view	ring the i	instance	e "default"	. go l	oack						
Token Family: Subscription				de	fault: Token families							
						🗳 Token Fami	lies					+
Name	Subscription					Slug	Name	Valid After	Valid Before	Kind		
Description 0	A subscription.					subscription-1	Subscription	2024/05/11 03:39:33	2025/05/11 03:39:33	subscriptior	Update	Delete
Valid After 🜒	2024/05/11		clear	never								
Valid Before	2025/05/11		clear	never								
Duration 30d		0	forever	clear								

Further use cases

The solution's flexible design allows it to accommodate a wide range of use cases beyond subscriptions.

- Discounts
- Loyalty stamps

NG

- Event ticketing
- Memberships
- Deposit systems
- Gifts

TALER





Future work

The solution is ready to be integrated into the various GNU Taler wallets. Several online publishing platforms have already expressed their interest in such a solution.



Free and open-source

The solution will be available as free and opensource software as part of the GNU Taler payment system. This eliminates vendor lock-in and builds trust. Moreover, it ensures that users maintain control over their own data, respecting their informational self-determination.

> Berner Fachhochschule Haute école spécialisée bernoise Bern University of Applied Sciences