xTOTP Generator Device

Degree programme: Master of Science in Engineering
Specialisation: Mechatronics and Automation
Thesis advisors: Prof. Andreas Habegger, Prof. Dr. Christian Grothoff
Expert: Rico Zoss (ED Wabtec)
Industrial partner: Taler Systems SA, Erpeldange, Luxembourg

Comprehensive digital payments, privacy and security are key to replacing physical money. The GNU Taler payment system offers a modern, privacy-preserving, tax-friendly and secure method for digital payments. To address this, a new device has been developed that generates an extended Time-based One-Time Passcode (xTOTP) for offline verification.

Motivation

In the current digital payment landscape, merchants without online access to banking systems face real-time challenges in verifying mobile payments. This limitation poses a security risk that can be mitigated through an offline verification mechanism. This thesis presents the development of an embedded device that generates an extended Time-based One-Time Passcode (xTOTP), enabling secure offline transaction validation. Integrated with the GNU Taler payment system, this solution advances secure and privacy-respecting digital payment technologies.

Methodes

The xTOTP generation relies on three key inputs: the transaction amount, the current time, and a shared secret stored both on the device and in the merchant's backend. Based on these requirements, the system architecture was designed to include a user interface, a microcontroller, a time synchronisation module, and a power supply unit (see figure 1).

A graphic LCD was selected for its energy efficiency and ability to display intuitive user interface elements. The input interface consists of numeric buttons and three multifunctional auxiliary buttons. A GPS module was chosen for accurate time synchronisation due to its global availability and precise UTC time output. Initial prototypes used a CR2430 coin cell battery. However, due to the GPS module's high power consumption, a supercapacitor was added to extend operational time. This setup proved insufficient under weak GPS signal conditions, prompting a redesign using a rechargeable battery with wireless charging based on the Qi1 standard, commonly used in smartphones and widely supported.

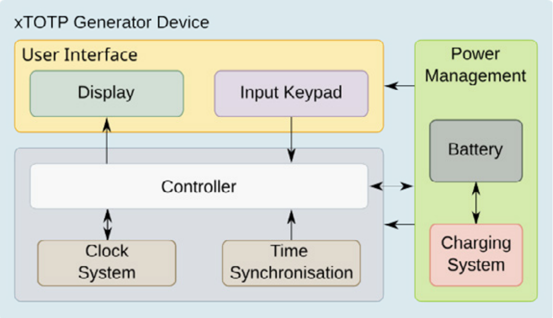

Fig. 1: Device Components Overview

The software, written in C, employs a modular architecture. Hardware abstraction is achieved through interface structures and function pointers, allowing the application layer to remain hardware-agnostic and easily portable to other microcontrollers.

Results

Integrating wireless charging and a rechargeable battery enhances the device's robustness, longevity, and environmental sustainability. The system functions reliably, and transaction amounts can be verified against the GNU Taler merchant backend. Additionally, a digital twin of the device was implemented on a GNU/Linux system, significantly accelerating development and testing cycles.

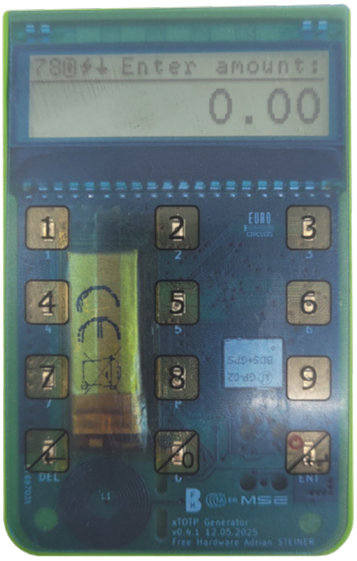

Fig. 2: xTOTP Device

Adrian Steiner
adi.steiner@hotmail.ch