BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2025
http://excel.fit.vutbr.cz

Bytestring Gatekeeper: Passwordless Account Solution

Dominik Kaspar*

Abstract
Account management across multiple services is becoming increasingly cumbersome for many users. Keeping track of usernames and passwords across different platforms is exhausting, and users are often tempted to reuse passwords for convenience, even at the expense of account security. Password managers attempt to mitigate this problem, but what if we removed the cause entirely? Gatekeeper addresses this issue through a passwordless authentication process utilizing Ed25519 cryptographic key pairs and QR code scanning, delivered as a REST API that can integrate with all modern applications. The system eliminates password-related vulnerabilities while providing features such as profile-based identity management, guarantees of real human users, and fine-grained permission controls. This solution offers significant benefits to both users and developers by simplifying the authentication process while enhancing security, making it valuable for applications requiring robust account management.

*xkaspad00@vut.cz, *Faculty of Information Technology, Brno University of Technology*

1. Introduction

[Motivation] Digital identity management has become increasingly complex as users navigate dozens of accounts across various platforms. Current authentication methods force users to choose between security and convenience, leading to poor practices such as password reuse or reliance on third-party password managers. This creates significant vulnerabilities that affect both users and service providers. Modern applications need a more secure, user-friendly authentication solution that does not compromise either security or user experience.

[Existing solutions] Current solutions to authentication challenges include single sign-on (SSO) services, two-factor authentication (2FA), and password managers. Although these approaches improve certain aspects of authentication, they often introduce new complexities or still rely on passwords as a fundamental component. SSO services centralize access but create a single point of failure. 2FA improves security but adds friction to the login process. Password managers solve the memory problem, but not the underlying password vulnerability issues.

[Our solution] Gatekeeper is a comprehensive account solution that replaces traditional authentication with a cryptographic approach based on Ed25519 standard key pairs. Users authenticate through a mobile app that scans a QR code, initiating a secure handshake where the mobile device signs a hashed login gateway with its private key. This completely eliminates passwords from being transferred while strengthening security. Currently, the system assumes that service providers place absolute trust in the centralized solution, which serves as the source of truth for the user's identity. In the future, decentralized and self-hosted variants are planned.

2. System Architecture

2.1 Gateway Creation

When a user attempts to log in to an application, the application server creates a login gateway through the Gatekeeper REST API. This gateway contains metadata about the login attempt (device information, IP address, geolocation), required user data, permission scopes, and a redirect URL. The application then redirects the user to the gateway portal.

2.2 QR Code Authorization

The gateway portal displays a QR code containing the gateway identifier. Users scan this code using the Gatekeeper mobile app, which retrieves the gateway data from the server. The mobile app then hashes this data and signs it with the user's private key

(securely stored on the device). This signature, along with the user's selected profile information, is sent to the Gatekeeper server for verification. In the future, the gateway portal will be able to prompt a locally installed Gatekeeper app using deep links.

2.3 Session Establishment

Once verified, the user is redirected back to the application. The application server then requests the authenticated user data from the Gatekeeper API using a previously established session token and creates a session.

3. Key Features

3.1 Passwordless Authentication

Gatekeeper eliminates passwords entirely, replacing them with cryptographic signatures based on the Ed25519 standard. This approach avoids common vulnerabilities associated with traditional passwords.

3.2 Profile-Based Identity Management

Users create a single verified account but can generate multiple profiles for different contexts:

- Real-name profiles for personal interactions
- Pseudonymous profiles for social media
- Verified legal entities for business transactions

Each profile operates independently with its own permissions and access controls, allowing users to maintain separation between different aspects of their digital identity.

3.3 Fine-Grained Permission Controls

The system provides detailed permission management at multiple levels:

- Resource permissions that define what data the authenticated session can access
- Application-specific permissions that specify what the session is authorized to do
- Sharing permissions that control which account can also use your identity

4. Implementation and Performance

The Gatekeeper system has been implemented as a high-performance REST API designed for scalability. Key implementation decisions include:

- Stateless API design to enable horizontal scaling
- Built on top of a highly performant tech stack
- Uses an in-memory key-value database similar to Redis as the main database

The front end is built with SvelteKit, chosen for its compiled and highly efficient builds. The backend API service is a Rust native application, which uses the Axum + Hyper stack. For the database, we chose the promising Skytable, due to its being written in Rust, enabling seamless SDK integration and offering read-write speeds exceeding Redis under certain conditions.

5. Conclusions

Gatekeeper represents an advancement in authentication technology by eliminating passwords while enhancing security through cryptographic verification. This concept can already be seen in deployment by large services like Steam, Discord, NIA, and even in the banking sector. Gatekeeper takes this concept further by implementing a centralized, yet privacy-focused identity account system, which provides flexibility for users while maintaining strong security boundaries.