ackee

Passwd

Security whitepaper

March 2023

Introduction

The constant increase in the digitalisation of all sectors of work and the growing demand for remote work is also linked to the rise in cybercrime. Companies are relying on an ever-increasing number of external and cloud-based systems to which they need to store and share login credentials between employees without fear of their data being leaked. In order to keep the data truly secure, it is necessary to generate strong and unique passwords across all accounts. Sharing so many passwords thus poses a security risk that requires time-consuming employee training and setting internal security rules.

Passwd was created as a solution to these problems. A tool that helps with simple and secure storage of sensitive data and offers a solution for creating, editing and sharing passwords and login credentials. The architecture based on Google cloud platform, provides security behind the well-known Google login and instant setup of access rights and users by importing them from Google workspace.

This document provides information on the technical and security principles used in the design and implementation of Passwd and its components.

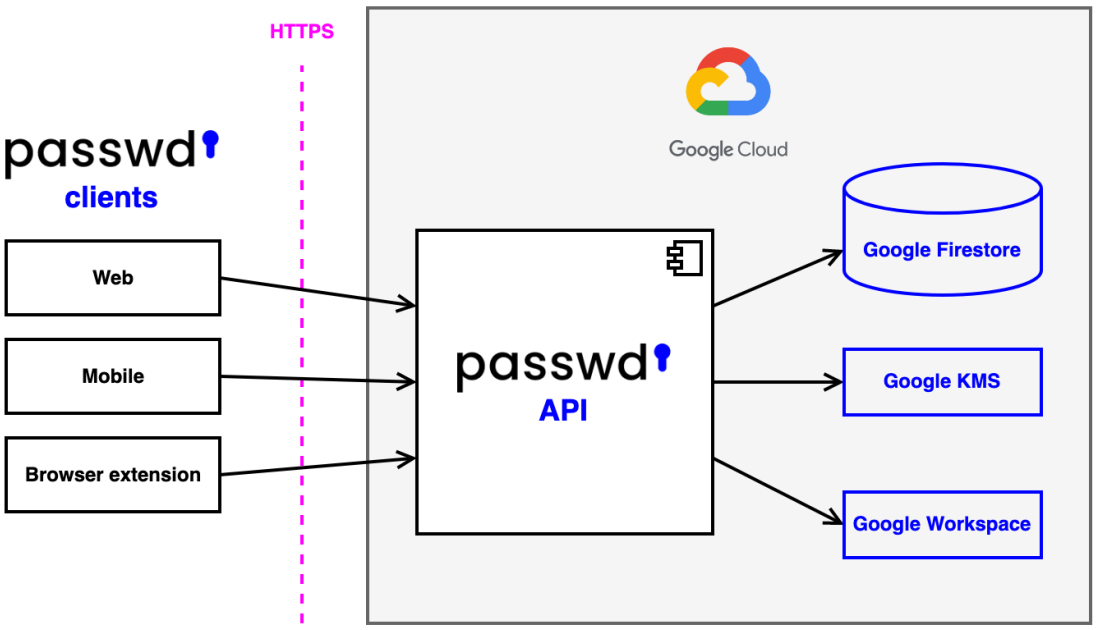
Design and security principles

All Passwd services run on Google Cloud Platform. No server infrastructure is required. The scalability, security and accessibility of the app is thus supported directly from Google. Each application is deployed on its own project based directly under the client account. Each customer thus receives their own dedicated environment with their own database system. There is no sharing of resources to run the application, database or encryption system between different organizations.

System architecture

The Passwd system currently offers three client interfaces. Users can access their data through the web, mobile apps or browser extensions. All solutions communicate with the server side of the application, running on the easily scalable Google Cloud Run infrastructure. Communication with both interfaces is secured using the Cross-Origin Resource Sharing (CORS) mechanism.

The server part of the application is used to encrypt, decrypt and synchronize stored data between the client interface and the database, to authenticate within specified records and to validate user rights with Google Workspace. Communication with the server is provided using a RESTful API completely hidden behind user authentication against Google Workspace settings. Server encrypted data stored in a secure Google No-SQL database Firestore.



Obrázek: Přehled architektury Passwd

Data transmission and encryption

Data is always sent to Passwd over a secure connection using TSL/SSL. Passwd rejects connections from insecure protocols.

Encryption

After transmission to the server, the data is encrypted using the AES-256 algorithm before being stored. For this, the application uses a key from Google Key Management Service (Google KMS). The security of the generated key is thus ensured by Google. You can read more about key security in Google's documentation.

Access to Google KMS is controlled by project administrators. Passwd developers do not have access to the key, the Passwd production application, or the database. Thus, the data is stored on the customer's Google Cloud Platform, and no one but the customer or

their authorized persons are able to read the data directly from the database or obtain the key to decrypt it.

Storage

Access to the Firestore database system is allowed through the Google Workspace admin interface or the server part of the Passwd application, no other connection to the database is allowed. Stored records are not assigned a sequential or other easily guessable identifier, which reduces the chance of an attacker gaining additional data in the event that some of the stored passwords are stolen from the system.

In the event that any of the data in the database is changed, a notification is sent directly to the client interfaces alerting them of the change in the currently viewed data. The user is thus always informed of the current status of the data he/she is viewing.

Transactions and subscriptions of the Passwd application are connected to the Stripe payment infrastructure. There is no persistent storage of transaction or customer payment data anywhere within the Passwd system.

Authentication and authorization

Security of user access to Passwd is implemented using Google Auth. The application uses the OAuth 2.0 protocol to redirect logins to Google in order to verify the user's identity and role. The security of the application is thus directly in line with the standards provided by Google and is common with logging into your other services using Google login.

User roles

Admin actions in Passwd are always subject to a check of the user role settings in the Google Workspace of the project. Additional security measures such as 2FA or password recovery are thus provided by default via the Google platform.

Access to records

Authentication of access to the data in the application is solved by checking the rights set on individual stored records. Only groups or users belonging directly to the client Google Workspace can be assigned. Sensitive data is not decrypted on the server part if the user does not have the rights to read the record. User data is always retrieved directly from Google Workspace and is not stored in the application database.

Logging and monitoring

Application activity is monitored using logs that are stored for 14 days in Google Cloud Operations Suite (formerly known as Stackdriver). Thanks to its location on Google's cloud environment, all logs can be directly accessed by the customer, as the project owner and, if applicable, his/her assigned persons. Logs can be viewed using the Google Console via a web browser. Google Monitoring provides the ability to set up metrics and dashboards for faster overview and tracking of activity within Passwd.

Server logs

All client activity on the API server part, database operations and selected important points such as external service usage are monitored. Logs are always purged of sensitive data or personal user data and security keys to external services before saving. Expected error conditions are caught and monitored. The Passwd team is alerted when an unexpected error occurs in the application with an alert, which is resolved immediately in case of an easy solution, and scheduled as quickly as possible in case a complex intervention is required.