# Extend libsecret file backend to use a TPM

Dhanuka Warusadura

Mentors:
Daiki Ueno
Anderson Sasaki

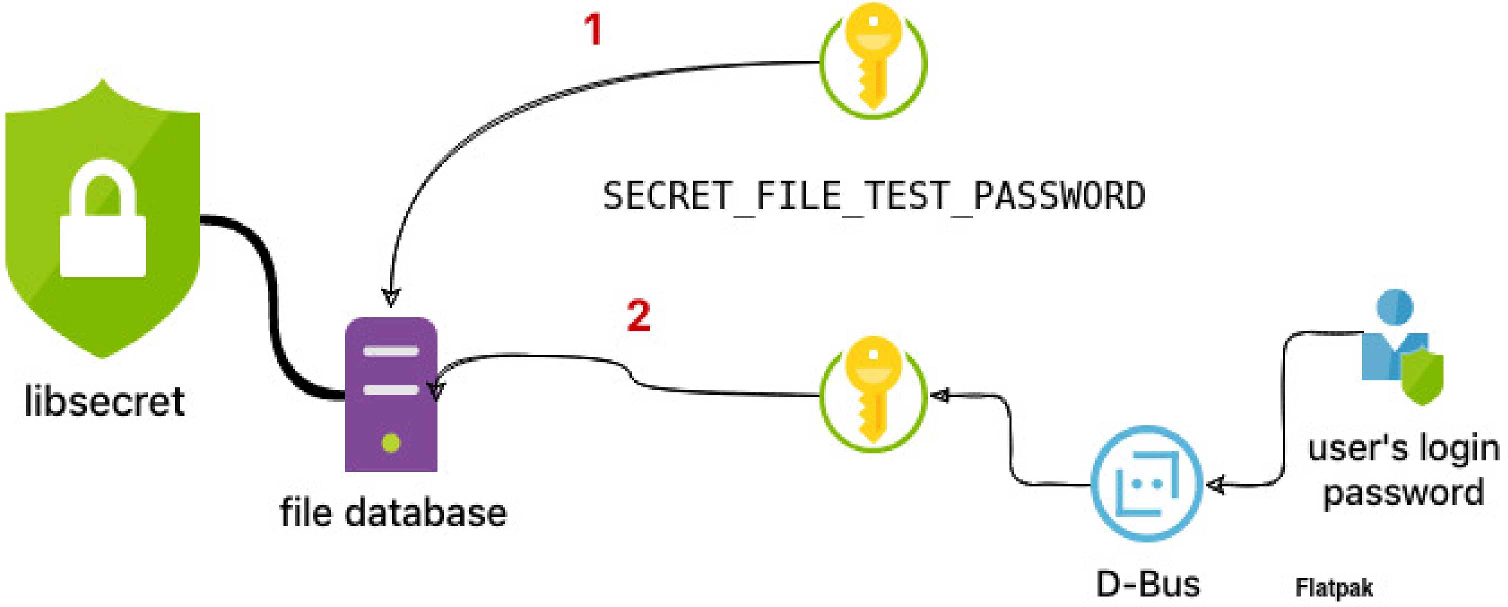
GNOME

2021 Google Summer of Code
**PROJECT UPDATE**

# What is libsecret?

- “libsecret is a library for storing and retrieving passwords and other secrets. It communicates with the "Secret Service" using Dbus” - gnome.org
- To simply put, consider libsecret as a tool that provides secrets/passwords handling services.
- Use cases: GNOME, Firefox, Google Chrome (Chromium), Epiphany (GNOME Web)
- libsecret has a relatively new feature that allows a user to store secrets in a file database or simply a file.

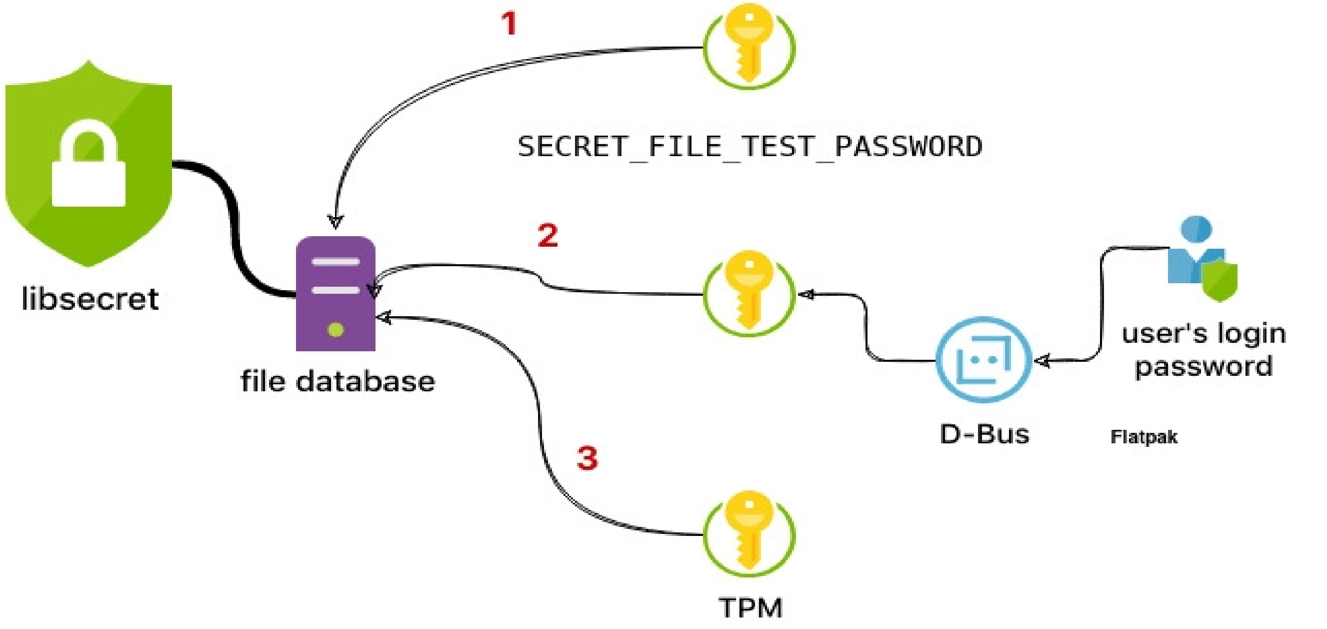
# File backend current design.



# What is a TPM?

- “Trusted Platform Module (TPM, also known as ISO/IEC 11889) is an international standard for a secure cryptoprocessor, a dedicated microcontroller designed to secure hardware through integrated cryptographic keys” - Wikipedia.
- To simply put a TPM is a hardware security module that performs everyday cryptographic tasks. Ex: key generation, key storage, true random number generator, encrypting, decrypting, ...
- There are three C APIs (API levels) that can used to talk to a TPM. SAPI, ESAPI and FAPI
- For our project we’re using ESAPI.
- For other regular TPM usage use, `tpm2-tools`

# Proposed file backend design.



# Proposed API

```
typedef struct EggTpm2Context EggTpm2Context;

EggTpm2Context  *egg_tpm2_initialize (GError **);

void  egg_tpm2_finalize (EggTpm2Context *);

GBytes  *egg_tpm2_generate_master_password (EggTpm2Context *, GError **);

GBytes  *egg_tpm2_decrypt_master_password  (EggTpm2Context *,
                                            GBytes *, GError **);
```

# Thank you!