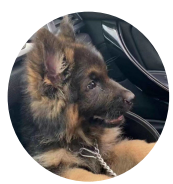
WebAuthn 密钥管理器

「开源软件供应链点亮计划——暑期2025」(OSPP 2025) 项目成果分享



@inuEbisu / 犬戎

2025 年 11 月 15 日

Part 1. 项目背景

自我介绍

犬戎是我常用的网名

- 浙江大学 24 级计算机科学与技术专业
- 浙江大学 AAA 战队 成员

五点钟刚考完大雾，光速准备 Tunight 😭

无密码的未来

新一代认证方式：**通行密钥** (PassKey)

> 通行密钥是一种基于公钥密码学的无密码登录标准，由 FIDO 联盟和 W3C（万维网联盟）共同制定，并得到了苹果、谷歌、微软等科技巨头的一致支持和推动。

- 无需密码
- 防钓鱼攻击
- 快速便捷

无密码的未来

中国科学技术大学的统一身份验证已强势支持通行密钥！~~浙江大学你看看你~~

道阻且长

Dart/Flutter 生态尴尬

- nfcim/fido2 库功能不全
    - 注册/验证功能缺失
- 没有好用的跨平台密钥管理工具

我的任务

1. 完善 FIDO2 Dart 库
    - 实现 `makeCredential` (注册) 和 `getAssertion` (登录) 流程
2. 使用 Flutter 实现一个跨平台 WebAuthn 密钥管理器

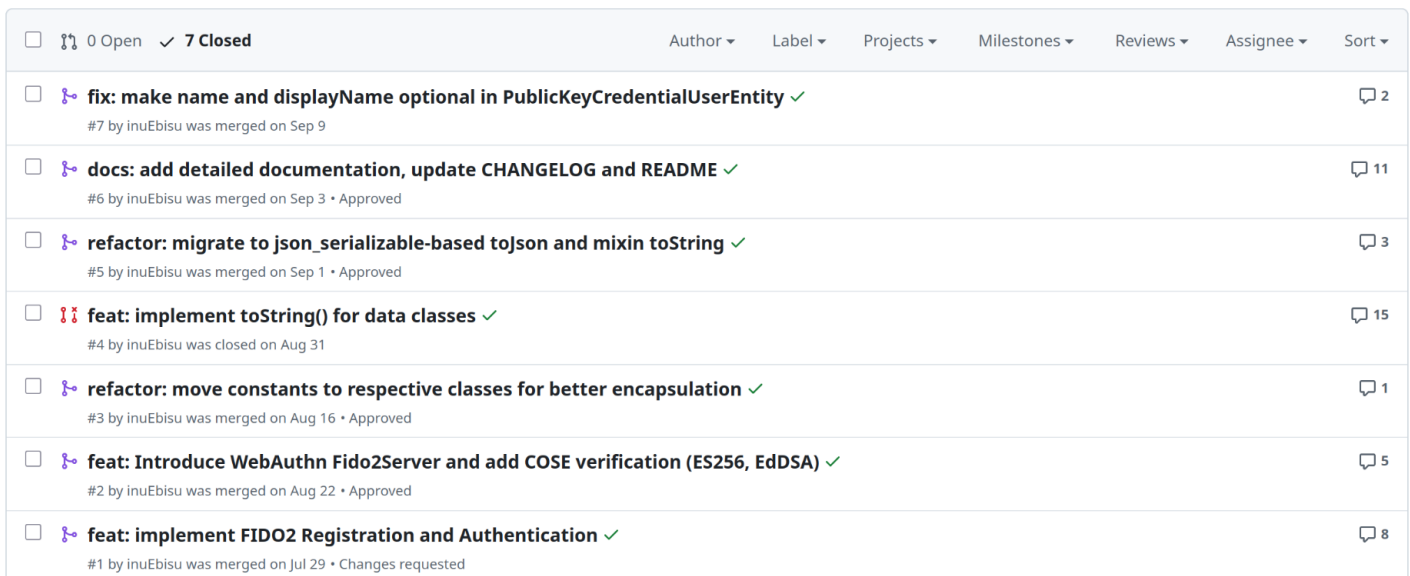
Part 2. 项目成果

一库一应用

fido2

- GitHub: nfcim/fido2

核心协议实现，服务端逻辑构建，密码学能力扩展，工程化与架构优化，很多测试



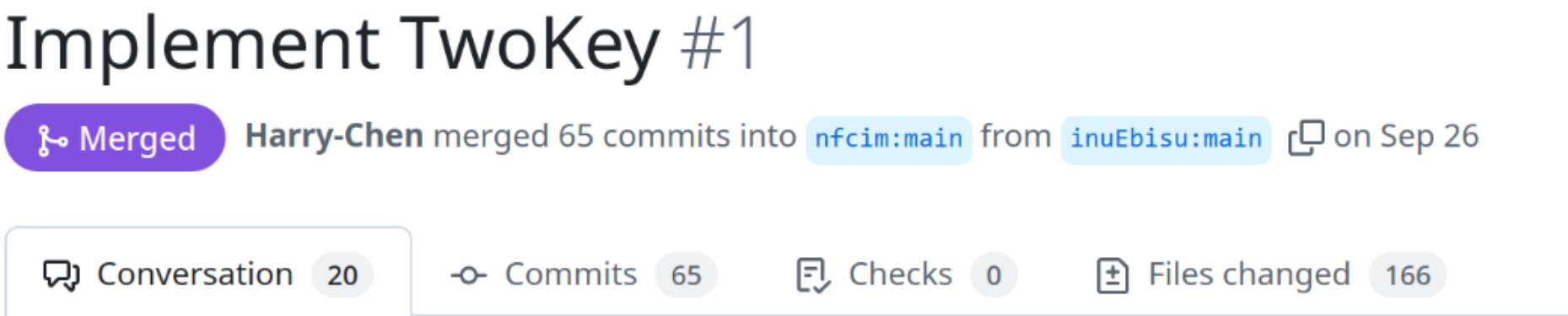
一库一应用

TwoKey

- GitHub: nfcim/twokey

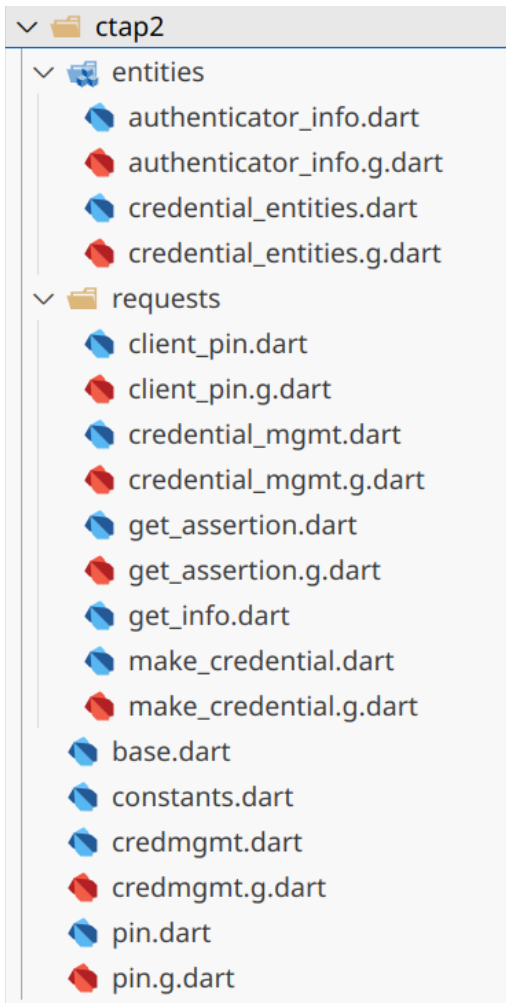
实现了

- 全功能跨平台应用
- CCID 与 NFC 通信



fido2: 搞定底层协议

补全客户端的 `makeCredential` 和 `getAssertion` 两个操作



fido2: 实现 Fido2Server

支持注册生成、注册校验、验证生成与验证校验

```dart
import 'package:fido2/fido2.dart';
import 'package:cbor/cbor.dart';

final server = Fido2Server(Fido2Config(rpId: 'example.com', rpName: 'Example'));

// 1) Registration
final regOptions = server.generateRegistrationOptions('user@example.com', 'User');
// send regOptions to client and store regOptions['challenge']

// After client returns base64url strings: clientDataJSON, attestationObject
final regResult = server.completeRegistration(
  clientDataBase64,
  attestationObjectBase64,
  expectedChallenge,
);
// Persist regResult.credentialId and regResult.credentialPublicKey (CborMap)

// 2) Authentication (Assertion)
final assertOptions = server.generateVerificationOptions();
// send to client and store assertOptions['challenge']

final verification = await server.completeVerification(
```

fido2: COSE 密码学校验

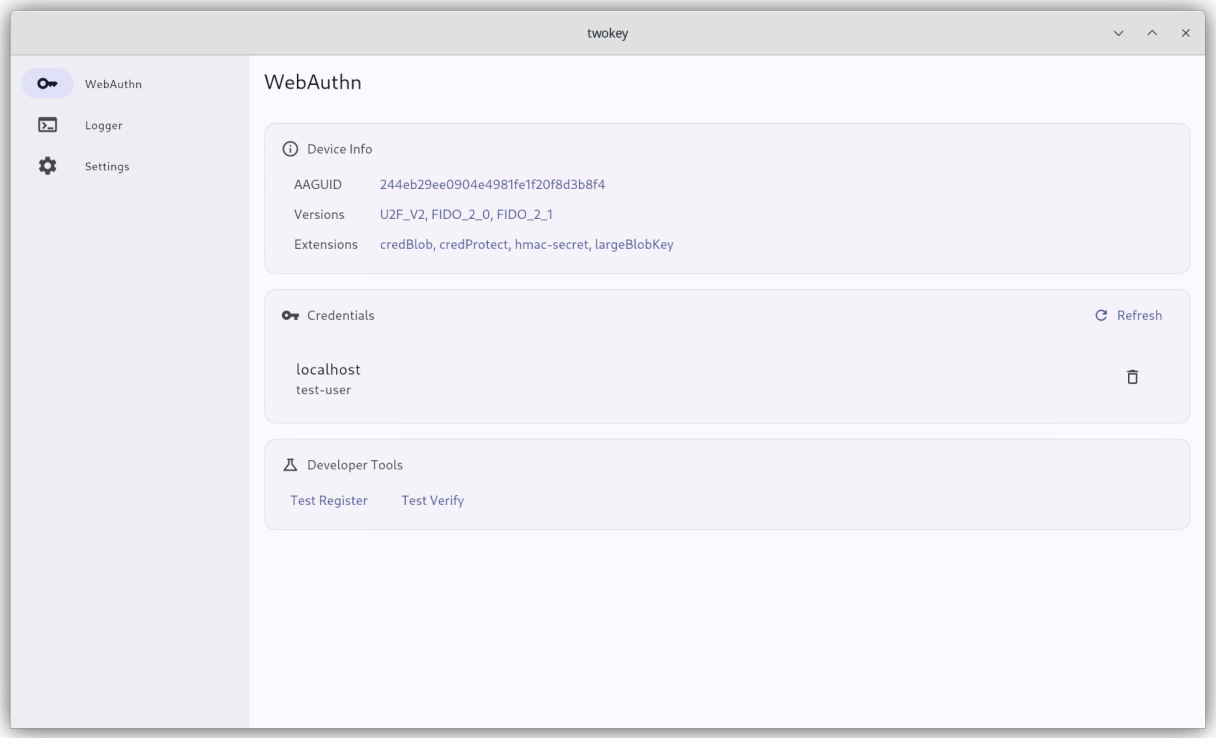
手写密码学校验，真的假的 💥

- 没库，用 `pointycastle` 自己实现了

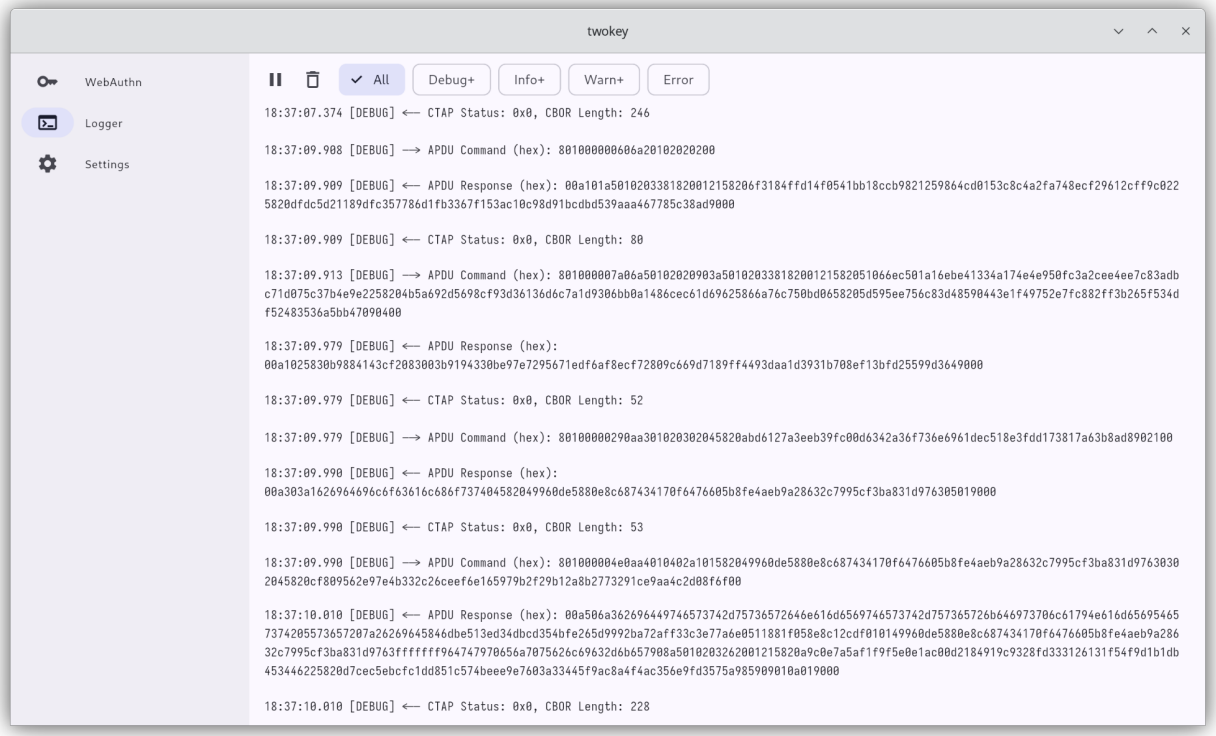
```
154  class ES256 extends CoseKey {
185    Future<void> verify(List<int> message, List<int> signature) async {
202      if (parser.hasNext()) {
203        throw Exception(
204            'ES256 verification failed: trailing bytes present in DER signature.');
205      }
206      final rObj = obj.elements[0];
207      final sObj = obj.elements[1];
208      if (rObj is! asn1.ASN1Integer || sObj is! asn1.ASN1Integer) {
209        throw Exception(
210            'ES256 verification failed: DER must contain two integers.');
211      }
212      final rBytes = rObj.valueBytes();
213      final sBytes = sObj.valueBytes();
214      final r = bytesToInt(rBytes);
215      var s = bytesToInt(sBytes);
216
217      // Build PointyCastle public key
218      final domain = pc.ECDomainParameters('secp256r1');
219      final q = domain.curve.createPoint(bytesToInt(xBytes), bytesToInt(yBytes));
220      final pubKey = pc.ECPublicKey(q, domain);
221
222      // Low-S normalization to prevent malleability: use s = min(s, n - s)
223      final n = domain.n;
224      final halfN = n >> 1;
225      if (s > halfN) {
226        s = n - s;
227      }
228
229      // Verify using SHA-256/ECDSA
230      final verifier = pc.Signer('SHA-256/ECDSA');
231      verifier.init(false, pc.PublicKeyParameter<pc.ECPublicKey>(pubKey));
232      final ok = verifier.verifySignature(
233          Uint8List.fromList(message), pc.ECSignature(r, s));
234      if (!ok) {
235        throw Exception('Assertion signature verification failed (ES256).');
236      }
237    }
238  }
239
```

TwoKey: 全功能跨平台应用实现

- 使用 Flutter 和 MultiProvider 状态管理
- 构建了支持五大平台（Win, macOS, Linux, Android, iOS）的统一应用



TwoKey: CCID 与 NFC 通信协议栈实现



CCID 协议通信需要手动封装 APDU 指令 🤔

Part 3. 总结与未来

这段旅程的收获与成长

技术成长

- FIDO2 / WebAuthn 协议
- Flutter 跨平台开发

更泛用的

- CI/CD
- 开源协作（Git, PR, Issue, Code Review）
- 项目管理与计划，工程经验
- 文档撰写
- ……

感谢

- 感谢党凡老师与陈晟祺老师
  - 二位老师的指导让我收获颇丰
- 感谢贺泽邦同学
  - 旅途不孤单
- 感谢我的朋友颉文
  - 是他最初鼓励我参加 OSPP

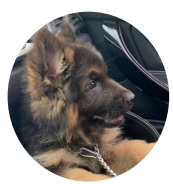
感谢

最后一杯敬自己

- 大一下学期状态非常烂
- 这个暑假在 OSPP 的同时还双开了 HPC101, CTF101 两门短学期课程
    - 机缘巧合之下度过了一个非常充实的暑假
    - 在迷茫中见到强大的人
    - 逐渐明确自己的志向

谢谢大家

Questions?



@inuEbisu / 犬戎

2025 年 11 月 15 日