Fabric nodejs SDK security extension
October, 2019

Fabric nodejs SDK security extension

- **Introduction**
  - **Name**: Hengming Zhang
  - **Location**: Shanghai, China
  - **University**: Fudan University
  - **Mentor(s):** David Liu - Mediconcen
  - **Hyperledger project**: fabric-sdk-node, fabric-client-flutter and fabric-server-node.

Fabric nodejs SDK security extension

- **Project Description**:

  The project is to build the crypto infrastructure for the Hyperledger Fabric SDK for Node.js.

- **Technology:**

  Node.js: the Chrome's V8 based JavaScript runtime for server side. Use it as the server side programming language for the fabric-server-node project.

- **Frameworks:**

  Hyperledger Fabric: the enterprise-grade permissioned distributed ledger framework. Leverage it as the network and infrastructure block to build apps and Node.js SDK.

  Flutter: the Google's mobile app SDK for crafting high-quality native interfaces on iOS and Android. Take it as the fabric-client-flutter project's framework to find the native crypto support of offline signing for the Hyperledger Fabric.

Fabric nodejs SDK security extension

- **Frameworks Con't:**

  Express.js: the web application framework for Node.js. Utilize it as the backend Node.js restful http/https server for the fabric-server-node project to send and/or receive request.

- **Tools:**

  VS Code: for the open source projects development.
  GitHub: for documenting SoftHSM tutorials.
  Gerrit: for committing and contributing code and collaborating the code review.
  Hyperledger Jira: for tracking issues, commits, and tasks.
  Hyperledger Wiki: for the project plan and completions.
  Hyperledger Chat: for chatting with the Hyperledger Fabric contributors and raising questions.
  Jenkins: for checking and running the code build.

Fabric nodejs SDK security extension

- **Project Objectives**:
  - Obj 1: fix on integration test failure on various OS.
  - Obj 2: keyStore class design refactor.
  - Obj 3: HSM compatibility enhance
  - Obj 4: offline signing

Fabric nodejs SDK security extension

- **Project Deliverables:**
  - Deliverable 1: computing resources checklist: cloud account, virtual machine snapshot, and mobile devices.
  - Deliverable 2: fix on integration test failure on various OS - only fixed on Ubuntu/macOS. b/c the Hyperledger Fabric Node SDK not supported on Windows platforms.
  - Deliverable 3: keyStore class design refactor - refactored the crypto key store design to the modern object-oriented design.
  - Deliverable 4: HSM compatibility enhance - enhanced the HSM compatibility about fabric-sdk-node. The enhancement includes fixing the current issues of SoftHSM.
  - Deliverable 5: offline signing - find mobile native crypto support on the offline signing scenario.
  - Deliverable 6: readme update: new HSM support - updated the README doc and moved it into github.io tutorials.

Fabric nodejs SDK security extension

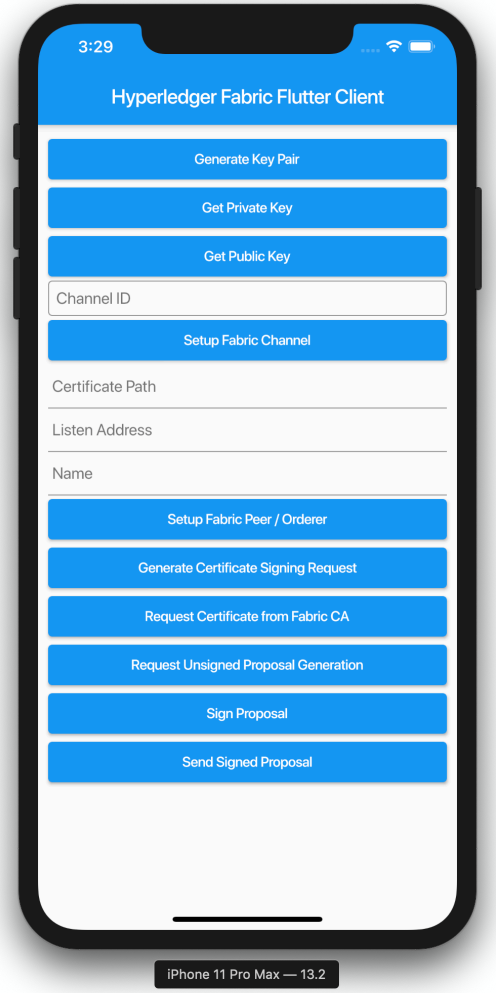
- **Project Execution & Accomplishments**:

- Accomplishments: computing resources checklist, fix on integration test failure on various OS, readme update: new HSM support, and offline signing.
- Not yet completed: keyStore class design refactor - reason is rejected by the maintainer b/c the change was not needed on master branch. Now the new commits are being reviewed on the release-1.4 branch.
- Partially completed: HSM compatibility enhance - SoftHSM part completed while the CloudHSM component not completed. Reason is out of cost to run the Cloud HSM service on AWS.
- Most proud of things: committed codes are approved and merged by fabric maintainers, and built a mobile app interacting with fabric network to generate keys, sign and verify proposals using cryptographic operations.
- The challenging: operate a fabric network that can be used to verify certificate signing request.
- Documented bugs: integration test failures and segmentation fault on Hyperledger Jira and GitHub.

Fabric nodejs SDK security extension

- **Project Demos on iOS Simulator:**

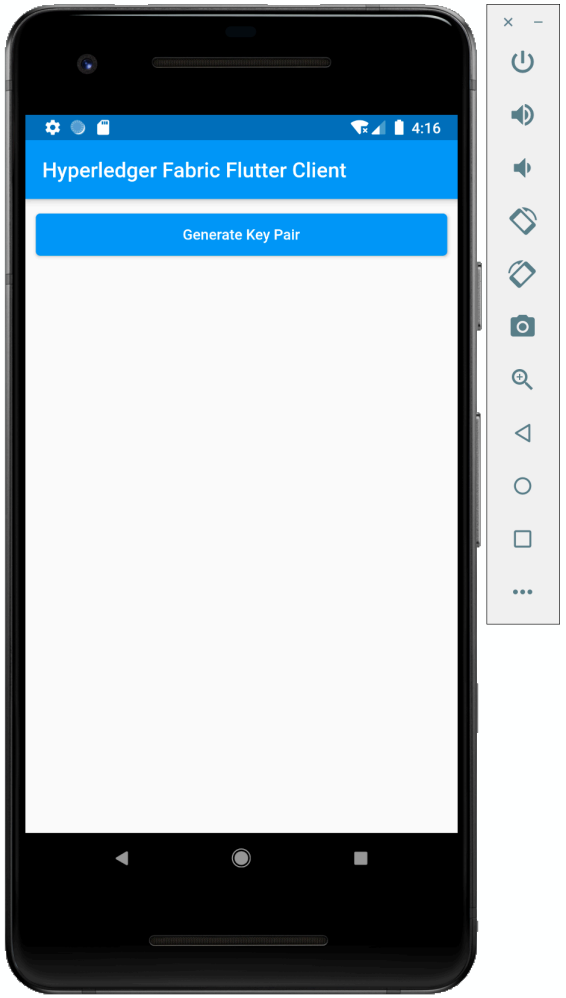
Initial UI



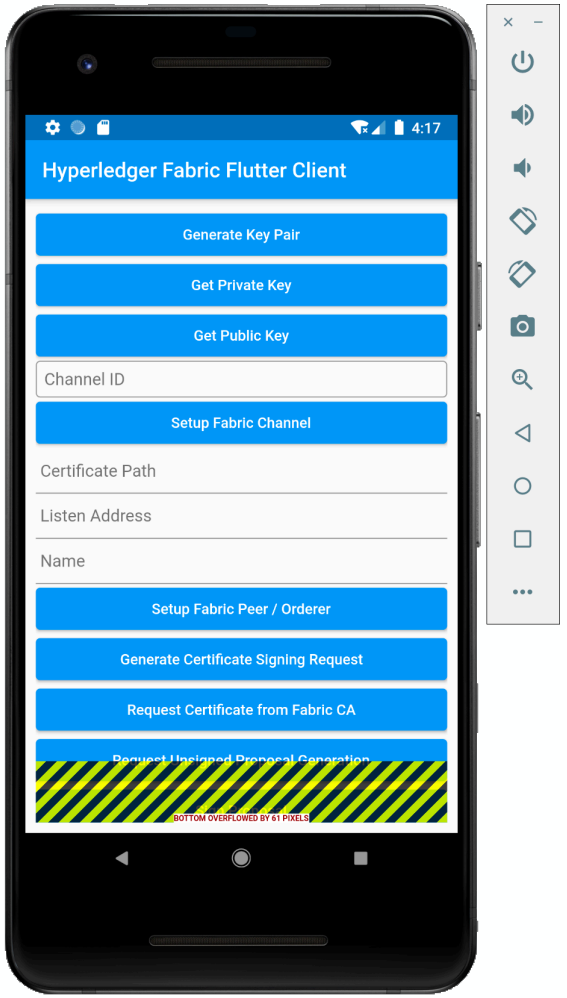
Complete UI

Fabric nodejs SDK security extension

- **Project Demos on Android Emulator:**



Initial UI



Complete UI

Fabric nodejs SDK security extension

- **Recommendations for future work:**

- The fabric-client-flutter project can be extended and implemented on other platforms such as Windows, macOS, and even IoT devices.
- The existing fabric-sdk-node project code structure can be improved by rewriting/refactoring the code to use the modern grammar so it becomes easier to read by other developers and contributors.
- The fabric-server-node project can be used to demonstrate an application that has a frontend to interact with fabric network.

Fabric nodejs SDK security extension

- **Referenced GitHub Repositories:**

- fabric-sdk-node: https://github.com/hyperledger/fabric-sdk-node

- **Hyperledger Lab Projects (To be moved into):**

- fabric-client-flutter: https://github.com/5sWind/fabric-client-flutter
- fabric-server-node: https://github.com/5sWind/fabric-server-node