Fabric国密改造
基于GmSSL的Go API接口GmSSL-Go

赵晓濛@GmSSL 项目组

2020-6-19

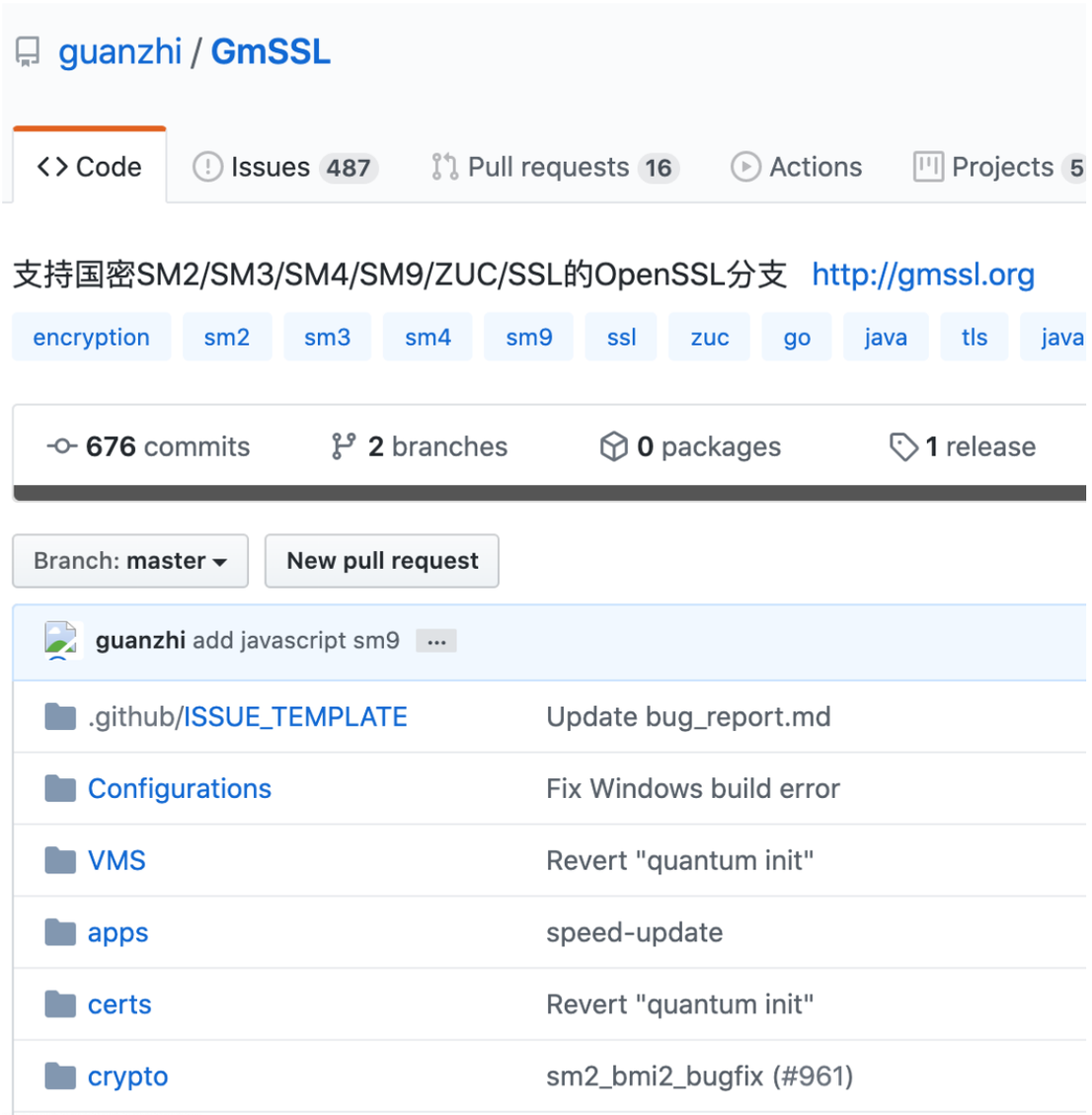
GmSSL 简介

- 2010年国家密码管理局公开了包括SM2公钥密码、SM3哈希算法和SM4分组密码等商用密码算法的相关标准(简称国密算法)
- 2018年密码行业标准化技术委员会公布了所有密码行业标准文本
- 2020年 1 月 1 日起密码法颁布实施

GmSSL 简介

GmSSL

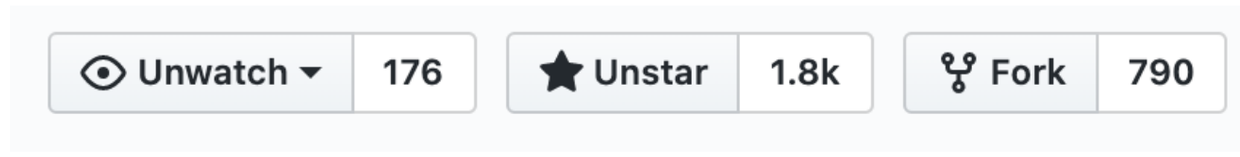
- GmSSL是一个高性能原生密码库
- 支持SM2/SM3/SM4/SM9等国密(国家商用密码)算法、SM2国密数字证书及基于SM2证书的SSL/TLS安全通信协议支持国密硬件密码设备
- 提供符合国密规范的编程接口与命令行工具，可以用于构建PKI/CA、安全通信、数据加密等符合国密标准的安全应用。



GmSSL 简介

GMSSL

- 开源中国社区6个密码类推荐项目之一(全部68个)
- Github 1786 Star 790 Fork
- 2016年德勤区块链大赛优胜奖
- 国家电网信息安全主动防御技术及装备项目获得电力科学技术进步一等奖



GmSSL的优势

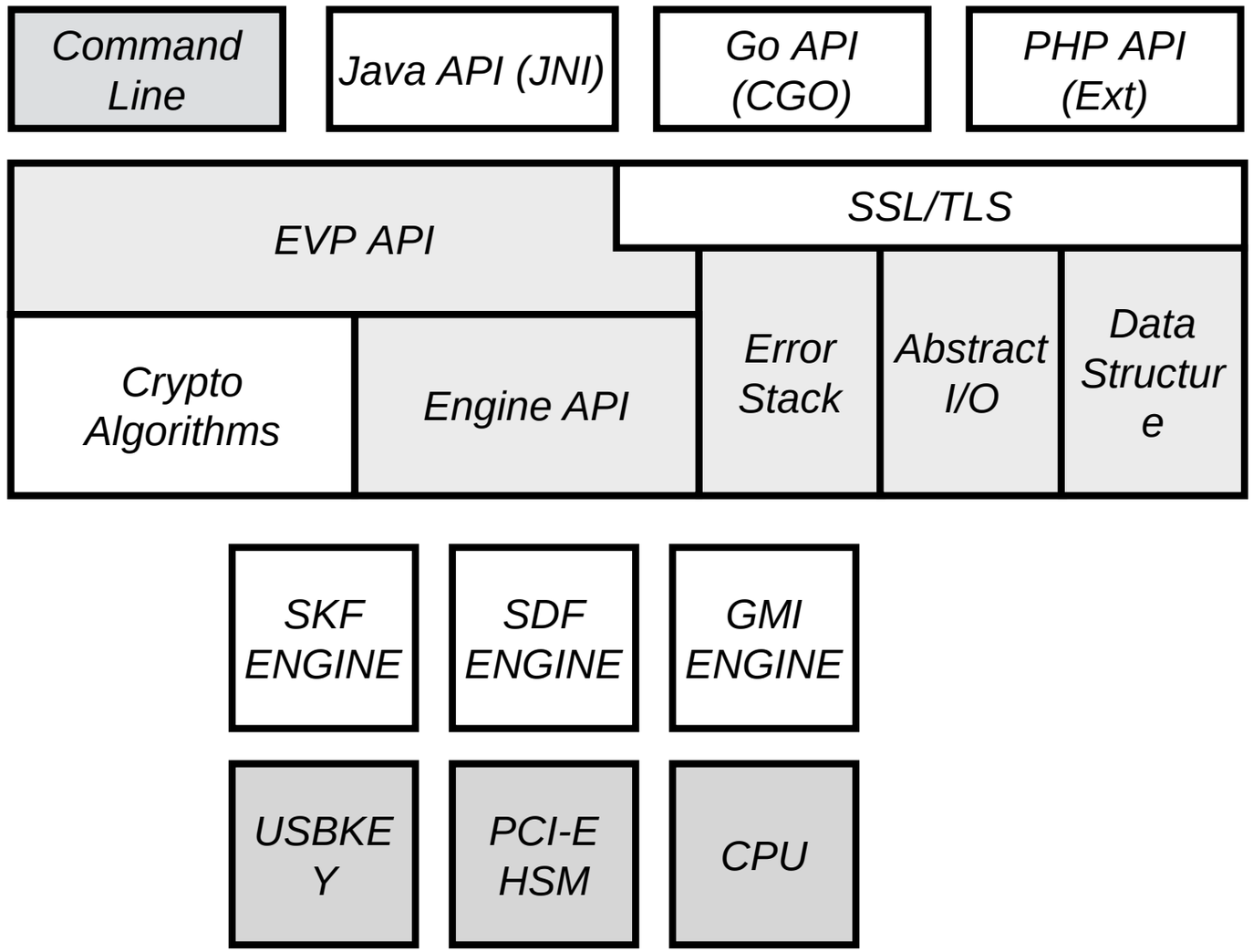
GMSSL

- 高性能：SM2、SM3、SM4 性能明显超过国内外同类密码库
- 易用：与OpenSSL保持API兼容
- 专业：来自北京大学信息安全实验室的开发和维护
- 开放：源码BSD/Apache风格许可证，目前在 Github、开源中国、GitLab上开源。
- 安全：抗侧信道、白盒攻击等

GmSSL/OpenSSL 架构

GMSSL

封装C Java Go 等接口



支持国密SSL标准

新增国产密码算法模块

支持国密数字证书

支持国产密码硬件

GmSSL-Go

GMSSL

- GmSSL-Go 是GmSSL库的Go语言接口绑定，为Go语言应用提供密码算法、X.509/PKCS证书、SSL/TLS协议和Engine等功能。
- GmSSL-Go以CGO方式将GmSSL的高层接口封装为Go语言组件，是一个与GmSSL库松耦合的轻量级的中间层，所有的密码功能均由底层的GmSSL库提供。

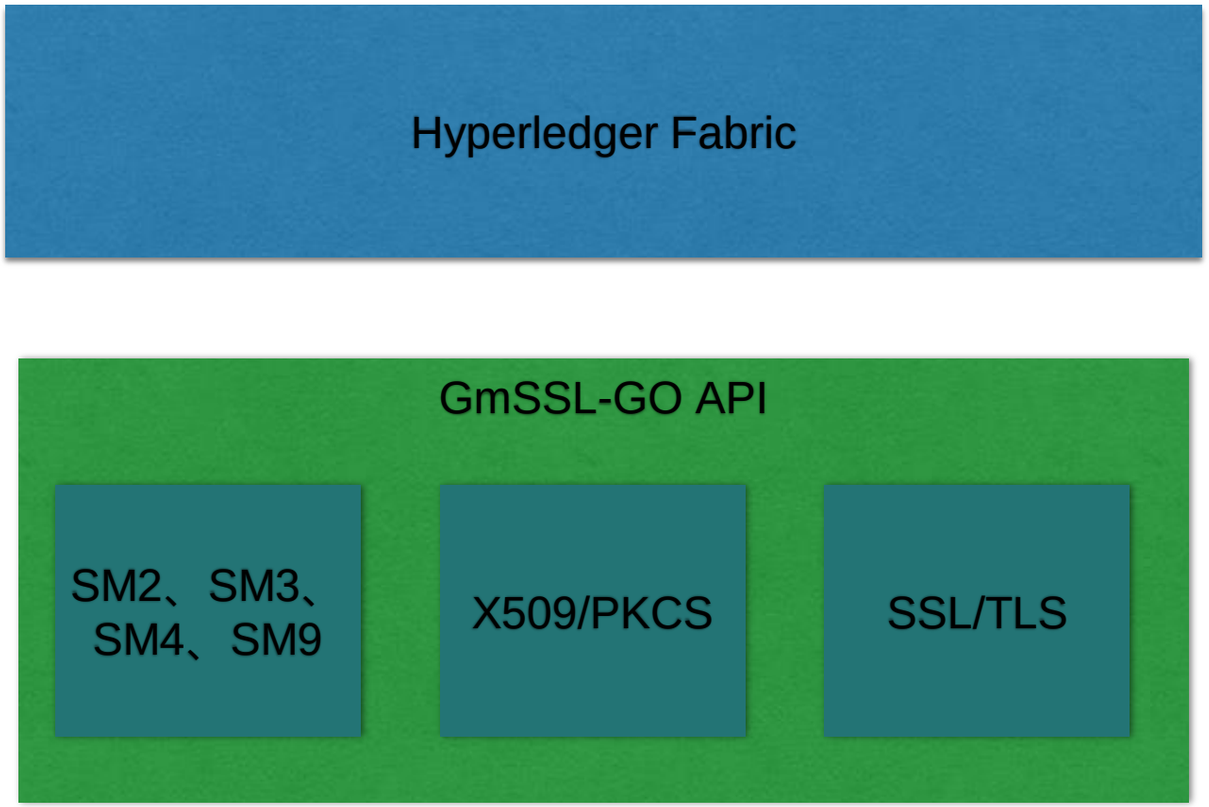
GmSSL-Go 功能

GMSSL

- SM2加密解密、签名验签、SM3散列、SM4加密解密、SM9标识密码
- X509/PKCS 证书功能
- SSL/TLS 功能
- 具体使用方法参见GmSSL-Go官方文档
  http://gmssl.org/docs/go-api.html

GmSSL-Go 总体架构

GMSSL



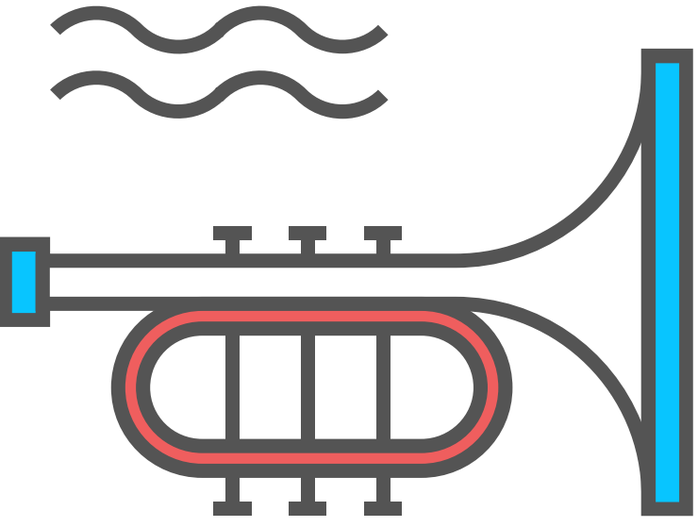
GMSSL 密码中间件

国产操作系统 **国产CPU** **国密 UKey** **国密PCI-E 卡**

GmSSL-Go 的优势

GmSSL

虽然Go语言的官方库提供了常用的密码算法包和SSL协议包，也存在一些第三方的纯Go语言的密码库，在项目中集成GmSSL-Go仍然有很多不可替代的优势：



国密硬件兼容

GmSSL-Go可以通过Engine对象满足国密标准的U盾、PCI-E加密卡等国产硬件密码设备，提供系统的安全性、可用性和密码合规性。

性能优势

GmSSL-Go以CGO方式调用GmSSL库的密码算法实现，相对于纯Go语言实现在密码算法上具有性能上的优势。

完整的国密支持

GmSSL-Go通过底层的GmSSL库提供完整、丰富的国密算法、证书和SSL协议的支持。

持续改进

GmSSL-Go的功能和性能随着GmSSL的升级获得持续的改进。

謝謝~

GmSSL

http://gmssl.org