Filière Informatique de gestion
Studiengang Wirtschaftsinformatik

Hes·so VALAIS WALLIS
School of Management

Évaluation du framework TamaGo

Étudiant : Thomas Cheseaux
Professeur : Jean-Luc Beuchat

Résumé

1. Prise en main du langage Go et recherche de frameworks existants pour le développement bare metal
2. Création d'une application de démonstration sur l'ordinateur en Go
3. Communication entre l'ordinateur et la clé USB Armory Mk II
4. Mise en œuvre et adaptation de l'application de démo sur le périphérique USB

Introduction

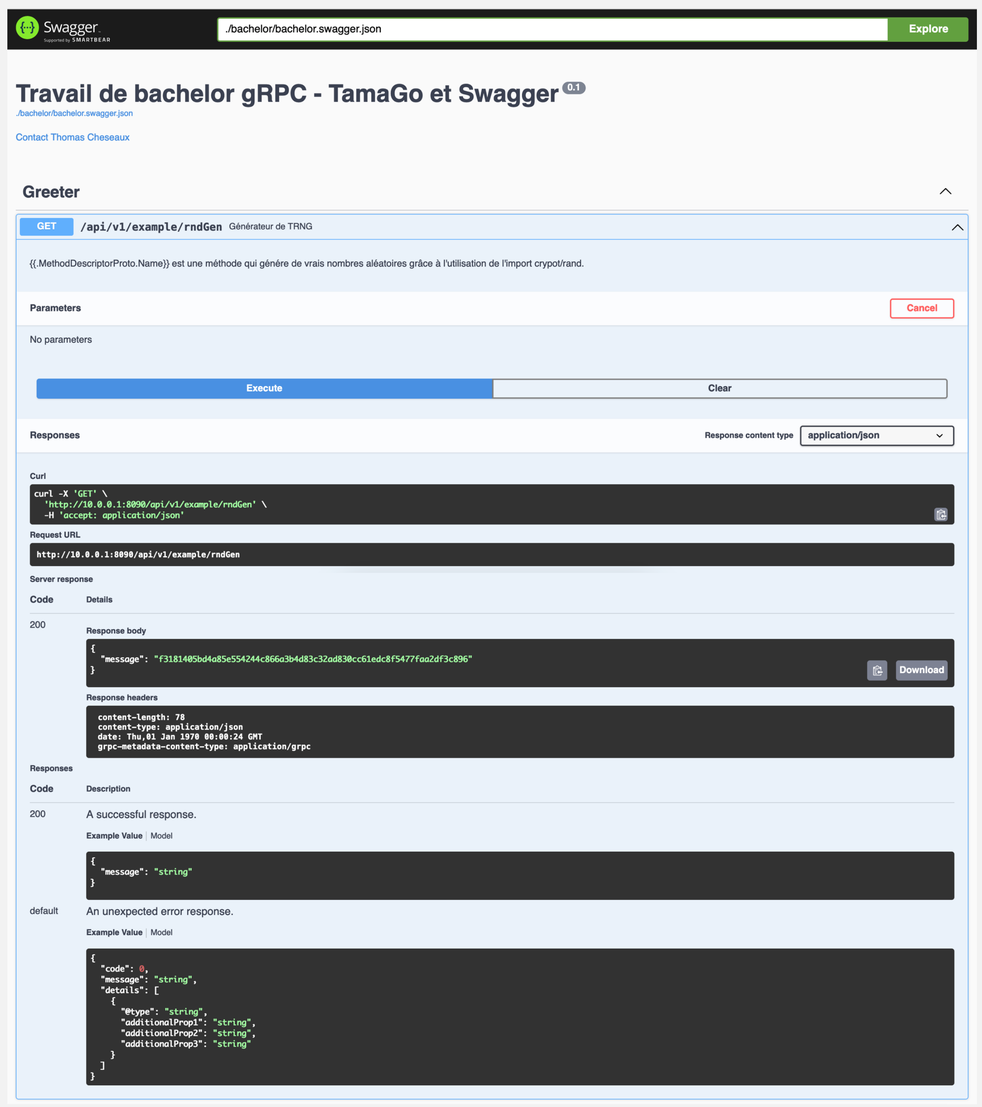
- La gestion des clés cryptographiques est une tâche complexe. Cette gestion nécessite le choix d'une méthode de génération des clés et d'une réflexion sur le cycle de vie.
- Dans notre cas, les clés de chiffrement sont stockées en plusieurs parts dans des hébergements en ligne distincts. Les opérations de chiffrement, de déchiffrement ou de signature sont effectuées sans reconstruire la clé cryptographique en un point unique.
- **L'objectif à moyen terme serait d'utiliser notre travail pour stocker une part des clés de chiffrement sur une clé USB sécurisée en complément des hébergements en ligne**.
- **Pour ce faire, notre travail considérera et analysera l'utilisation de l'Armory Mk II en tant que dispositif de sécurité complémentaire des clés cryptographiques.**
- TamaGo est un framework basé sur le langage Go. Ce cadre de développement offre la possibilité d'exécuter et de compiler sur des systèmes embarqués de type ARM ou RISC-V sans l'aide d'un OS.

Méthodes

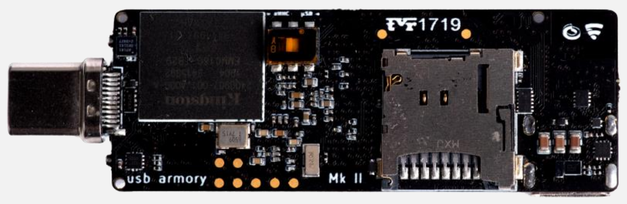
1. Compréhension des concepts et technologies (MPC, HSM, clé USB Armory Mk II, True Random Number Generator).
2. Recherche de frameworks existants.
3. Développement d'une application de démonstration sur l'ordinateur comprenant un serveur gRPC avec OpenApi.
4. Mise en œuvre de la communication entre la clé USB Armory Mk II et l'ordinateur.
5. Adaptation de l'application de démonstration pour une exécution bare metal sur le périphérique USB et affichage du serveur gRPC.

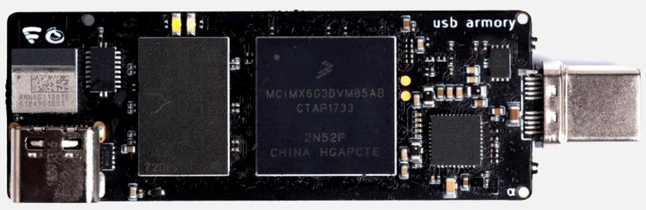
Résultat

Affichage du service gRPC-Gateway avec OpenApi



Outils





Conclusions

- L'application de démonstration permet d'afficher de vrais nombres aléatoires à travers l'interface visuelle Swagger GUI.
- Notre travail établit l'Armory Mk II en tant que dispositif complémentaire, susceptible d'améliorer la gestion future des clés de chiffrement mais aussi comme une potentielle alternative aux HSM selon l'emploi et le niveau de sécurité requis.

HES-SO Valais-Wallis • rte de la Plaine 2 • CP 80 • 3960 Sierre
+41 58 606 93 11 • info@hevs.ch • www.hevs.ch/ig

Contact and more informations:
http://www.hevs.ch/ig