cpl.thalesgroup.com

THALES

フリービット株式会社：ブロックチェーンとThales Luna Network HSMを組み合わせて、革新的なデジタルキー基盤を構築

サマリ

利便性の高いネットワーク社会に不可欠な要素として、「デジタルキー」の需要が高まっています。普及の最前線は、自動車業界と住宅・ホテル業界です。

フリービット株式会社（以下、フリービット）は、ブロックチェーンを用いたデジタルキー基盤を、アルプスアルパイン株式会社と共同開発。さらに、ブロックチェーンを用いて、証跡ログなどシステム運用情報の改ざんリスク対策ソリューション「The Log」を共同開発して自社利用を開始しました。

ブロックチェーンのシステムにおいて、セキュリティの要となるのが、秘密鍵の管理です。フリービットはタレスのLuna Network HSMを採用することで、FIPS 140-2[1] Level 3準拠の最高レベルの秘密鍵管理のしくみを構築し、セキュリティと汎用性・拡張性を兼ね備えた、革新的なブロックチェーンの基盤構築に成功しました。

選定のポイント

CASE[2]、MaaS[3]などのトレンド・キーワードが示すとおり、自動車業界は大きな変革期に直面しています。

フリービットは、ISP、MVNO事業者向け支援、法人向けクラウドサービス及びモバイル通信サービス等の各種インフラサービスから、教育・医薬・住宅業界へのソリューションサービス提供まで、マルチレイヤで事業展開してきましたが、自動車業界に向けては、カーエレクトロニクス製品のトップメーカーであるアルプスアルパイン社と包括的に提携。「CASE/MaaS時代のシームレスカーライフ実現に向けたCaaS[4]」をコンセプトに、共同開発に取り組んでいます。

第1弾として2019年1月に発表したのが、車の鍵発行、権利の移転といった鍵管理プロセスをシンプルかつ低コストにカバーするデジタルキーシステムです。同年7月には第2弾として、あらゆるインターネット/IoTインフラにおけるシステム運用情報の改ざんリスク対策ソリューション「The Log」を発表。フリービットが展開するクラウドサービス基盤に順次「The Log」を導入しています。また、アルプスアルパイン社と共同開発しているデジタルキーにも導入していく予定で進んでいます。

freebit

> “ HSMを使って、接続性・汎用性の高いブロックチェーン基盤を作ることができました。今後は、ログ以外の重要データを保管するプラットフォームなど、様々な分野へ応用展開していきます。ブロックチェーンはIoT時代に不可欠な優れた技術であり、HSMと組み合わせることで適用領域をさらに大きく広げていけると考えています。”
>
> – フリービット株式会社　クラウドインフラ事業部 事業部長
> 玉野井 智洋氏

1 FIPS（Federal Information Processing Standard：米国連邦情報処理規格）140-2は、暗号化ハードウェアの有効性を検証するためのベンチマーク。製品がFIPS 140-2認定の場合、その製品が米国政府とカナダ政府によってテストされ、正式に検証されていることを示している。

2 CASE：コネクテッド、自動運転、シェアリング、電動化の略

3 MaaS：Mobility as a Service

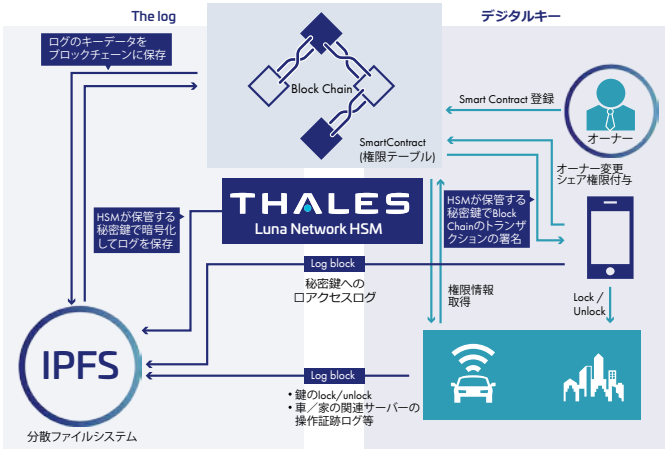
4 CaaS：Car as a Service

デジタルキーおよびログ管理システムの革新に用いたのが、ブロックチェーンです。権限のない人はデータを書き換えられない強固なセキュリティのしくみと、新車から中古車に至るまでの長いライフサイクルをパブリックシステムで効率よくカバーできるという特長を活かしました。

ブロックチェーンにおいて、権限を最終的に守るのは秘密鍵であり、秘密鍵の管理体制こそがシステム全体のセキュリティレベルの要となります。フリービットは、各種の暗号鍵管理ソリューションを比較検討したうえで、暗号鍵保護を目的として特別設計された専用ハードウェアの採用こそが最高レベルのセキュリティを確保できると判断。「Luna Network HSM」を導入しました。

ソリューション

開発の初期段階では、鍵管理/利用において多数の独自APIを提供、また仮想化アプライアンスモデルをクラウド環境にも提供する鍵管理プラットフォーム「KeySecure」を使う予定で、プログラム開発と動作検証を進めました。開発途中でSafeNet Luna Network HSMに切り替えたのは、FIPS 140-2 Level 3のハードウエアによるセキュリティ、秘密鍵は決してハードウェア外に出さない運用、楕円曲線や各種必要な暗号アルゴリズムという各種セキュリティ機能、1台のHSMを複数HSMに仮想的に分割して利用できる機能(パーティション分割)またフリービット社独自でファームウェアに近い機能を開発できる拡張性を重視したためです。Luna Network HSMの開発には暗号デバイスの標準インターフェースであるPKCS#11を利用することですでに開発を進めていたウォレット機能を含めて、短期間で移行が完了。当初予定どおりにサービスをカットオーバーすることができました。



ブロックチェーンとLuna Network HSMを組み合わせたセキュリティな基盤で、革新的なデジタルキーシステム、およびオフチェーンのログ保管システムを構築

タレスについて

皆様がプライバシー保護を信頼して任せている相手は、そのデータを保護するためにタレスに頼っています。データセキュリティに関しては、組織が直面する決定的な局面は次々と増え続けています。その局面が暗号化戦略の策定、クラウドへの移行、コンプライアンス要件の順守のいずれであっても、デジタルトランスフォーメーションを保護するためにタレスに頼ることができます。

決断の瞬間のための、確実なテクノロジー。

課題

- ブロックチェーンを用いた新しいデジタルキーのシステムでは、秘密鍵管理の強固なセキュリティが必須
- 秘密鍵を保管するだけでなく、Ethereum環境で、暗号化、デジタル署名サービス等を高速処理する先進性・信頼性・パフォーマンスも重要

ソリューション

- ブロックチェーンとLuna Network HSMを組み合わせて、強固な秘密鍵管理のしくみを開発
- ブロックチェーンとLuna Network HSMを組み合わせた基盤を使って、システム運用情報の改ざんリスク対策ソリューション「The Log」を開発。大規模なブロックチェーンシステムに不可欠なオフチェーン部分のログ管理についても、セキュリティレベルの高い新しいしくみを構築した

メリット

- 秘密鍵管理に最高レベルのセキュリティを確立して、革新的なデジタルキーシステムを実現した
  -ライフサイクルを通じて暗号鍵をハードウェアに保持するHSM
  -FIPS 140-2 Level 3準拠であり、利用者へのセキュリティレベル説明もわかりやすい
- 開発しやすく、汎用性、拡張性の高い技術基盤ができた.
  -業界標準インターフェースに対応して、Ethereum環境で、SmartContract、IPFS（InterPlanetary File System）サーバ等と高速連携
  -公開鍵インターフェースは業界標準のPKCS #11対応
  -処理性能が高く、ハイパフォーマンスを発揮
- 1台のHSMをパーティション分割して、本番／開発環境で効率よく並行利用.
  -最大 100 のパーティションに分割可能。複数サービスを同時に開発できる
- バックアップ、HA構成もセキュリティレベル高く構築
  -バックアップ専用ハードウェア「Luna バックアップHSM」を使って、セキュリティレベルを落とすことなくバックアップシステムを構築
  -HA構成もあらかじめ用意されており、設定に手間をかけることなく容易に構築
- 日本国内で安定したサポート
  -開発者向け資料が充実。特に、暗号化、SmartContract連携、電子署名などのソースコードはとても役に立った
  -Thalesはブロックチェーンについても高度な知見

> cpl.thalesgroup.com <

お問い合わせ先 – cpl.jpsales@thalesgroup.com

すべてのオフィスの所在地と連絡先情報につきましては 、cpl.thalesgroup.com/ja/contact-usをご覧ください。