ユビキタス環境におけるハードウェア認証基盤ソフトウェアの開発
～ IC チップを利用した機器指向の認証フレームワーク ～

開発代表者： 平野 学 （豊田工業高等専門学校 情報工学科 助手）

1. 背景

近い将来、様々な情報機器がインターネットにつながる真のユビキタス社会が実現すると、一人のユーザが多数のハードウェア機器をインターネットに接続し、目的に応じて機器を連携させて操作する利用形態が具体化すると考えられる。その際にネットワーク経由で接続している機器が、本当に信頼できる環境を提供しているかを確認することがセキュリティ上、非常に重要な課題となる。

2. 目的

本プロジェクトの目的は、従来の「人間」を対象とした認証ではなく、「機器」を対象とした認証を実現する為の、IC チップで動作するソフトウェアを開発することである。図1に本提案の概念図を示す。新たに提案する IC チップのソフトウェアは HAAC(Hardware Authentication and Authorization Chip の略)と名付けて開発を進めるものとする。本プロジェクトを実施することにより、従来の人間を対象とした認証ではなく、機器を対象とした認証の枠組みを提案し、実際に利用可能な IC チップソフトウェアを開発する。本プロジェクトでは、HAAC IC チップの処理を効率化して高速に動作させるための改良も実施する。さらに、IC チップと連携する管理アプリケーションを開発、周辺ソフトウェアを充実させることにより、機器指向の認証フレームワークを普及させることを目指すものとする。

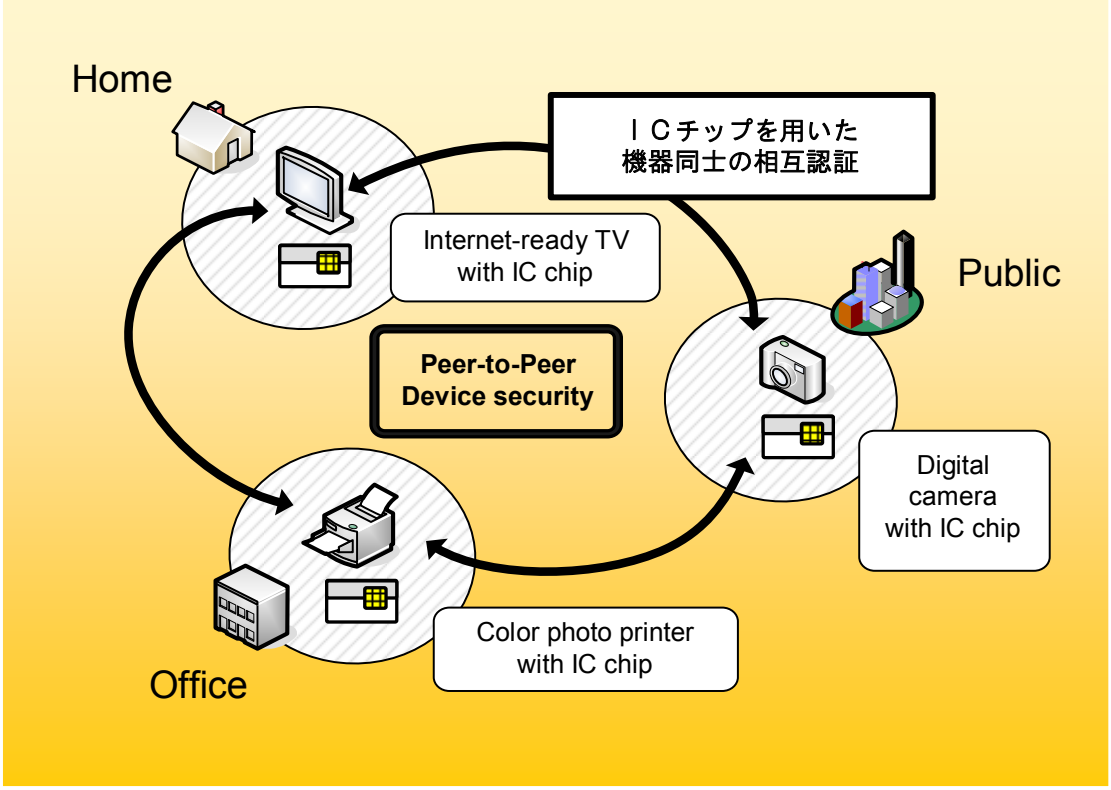

図1 提案するICチップを利用した機器指向のセキュリティ機能

3. 開発の内容

本プロジェクトでは、機器指向の認証・アクセス制御を実現する IC チップで動作するソフトウェア、並びに IC チップを初期化、パーソナライズするための管理アプリケーションの開発を実施した。なお、本プロジェクトで開発するソフトウェアは、原則として IC チップのソフトウェアも含め、全てオープンソースの枠組みの中で実現した。

本プロジェクトでは、IC チップ(スマートカード)として大日本印刷株式会社の製造する Standard-J T3.2、及び松下電器産業株式会社の製造する ZU-9PS スマートカードリーダを用いて開発を実施した。開発した IC チップソフトウェアは Standard-J T3.2 で動作し、管理アプリケーションは Linux オペレーティングシステムの稼動しているPCで動作する。以降に開発したソフトウェアの詳細を示すものとする。

3. 1 HAAC ICチップソフトウェア

本プロジェクトでは IC チップで動作するソフトウェアを Sun Microsystems 社の提供する Java Card ™ API 2.1 を用いて開発した。ICチップソフトウェアは、主として、次に示す機能をアプリケーションに提供するものとして開発した。

- ✓ 管理アプリケーションとの連携API
  - 公開鍵証明書、アクセス制御リストの格納と取り出し
  - 信頼するルート証明書の格納
- ✓ 機器の認証API
  - 機器の鍵ペア生成
  - 機器の秘密鍵を用いた電子署名
  - 公開鍵証明書、および属性証明書の正当性の検証
- ✓ 機器のアクセス制御API
  - 属性証明書と公開鍵証明書の関連性検証
  - アクセス制御リストに基づく認可判定

信頼できる実行環境(ICチップ)の内部で、これらのセキュリティ機能を実行させることにより、安全性を要求されるプログラムコードの改竄やリバースエンジニアリングを防ぐことが可能となる。また、機器の認証情報を安全に格納することが可能となる。

3. 2 ICチップ初期化アプリケーション

本プロジェクトでは IC チップを初期化するための管理アプリケーションを開発した。本ソフトウェアによって、機器の製造業者は、機器の製造番号、及び製造業者の識別情報をICチップに書き込むことができるようになる。開発したICチップ初期化アプリケーションを図2に示す。本アプリケーションには認証局(CA, Certificate Authority)の機能が組み込んであり、本ソフトウェア単独で機器の公開鍵証明書を発行し、ICチップへの格納までを実行することができる。

3. 3 ICチップ パーソナライズアプリケーション

本プロジェクトでは IC チップをパーソナライズするための管理アプリケーションを開発した(図3)。本ソフトウェアを用いることで、機器を購入したユーザは、所有者情報と機器用のアクセス制御リストをICチップに書き込むことができる。本アプリケーションには属性証明書の発行局(AA, Attribute Authority)の機能が組み込んであり、本ソフトウェア単独で機器所有者の属性証明書を発行し、ICチップへ格納できるようになっている。

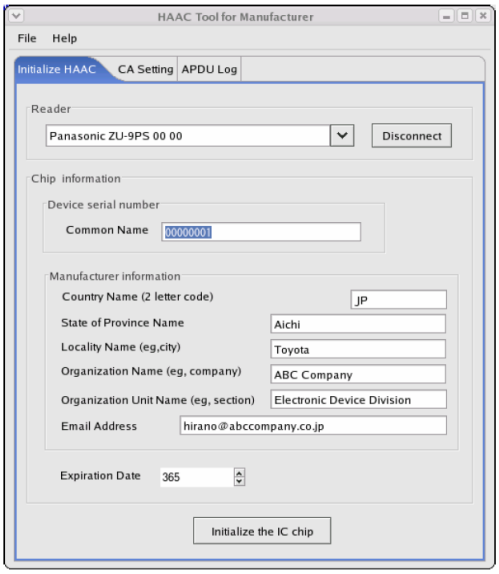

図2　ICチップ初期化アプリケーション

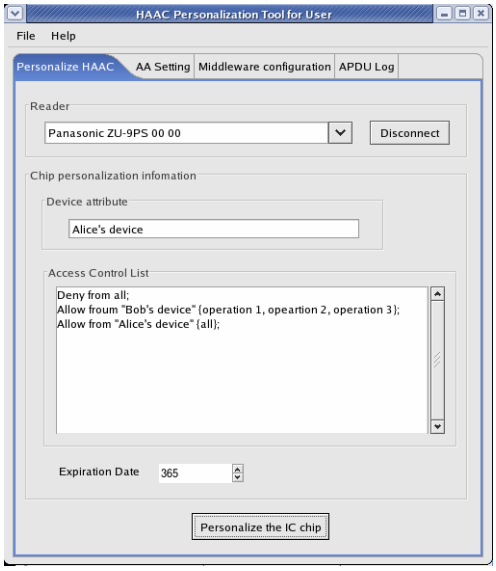

図3　ICチップパーソナライズアプリケーション

4. 従来の技術（または機能）との相違

本プロジェクトでは、機器指向の認証およびアクセス制御のAPIを提供するICチップソフトウェアを開発した。ICチップを用いて「人間」を認証する規格（PKCS#11　等）は国際標準化が進められているが、機器の正当性を検証するための規格は未だ研究段階にある。本研究の新規性は、機器指向のセキュリティ機能を実現するソフトウェアをICチップ上に実装したこと、そして、それらのソフトウェアをオープンソースとして公開可能な状態で開発したことである。

5. 期待される効果

本プロジェクトで提案、開発した機器指向の認証・アクセス制御のフレームワークは、家庭向け電化製品のネットワーク化に伴い必要不可欠となるセキュリティ機能の一手段として利用可能であると考えられる。ネットワーク対応の家電製品の本格的な普及に伴い、それに付随する情報提供サービスなどの新規産業が今後更に活性化していくものと考えられる。

6. 普及（または活用）の見通し

今後、開発したICチップを小型システム（Linux搭載のマイクロサーバや組み込みLinuxシステム）へ対応させ、実際に家庭向けの電化製品をネットワーク経由で安全に認証・アクセス制御させるシステムの開発を行っていく。オープンソースでの開発と並行して、学会や論文誌での成果発表を実施し、産学連携での本ソフトウェアの普及を積極的に進めていく。

7. 開発者名（所属）

開発代表者：　平野　学　（豊田工業高等専門学校　情報工学科　助手）

（参考）　プロジェクトホームページ　http://133.85.142.2/haac/