ＰＫＩ の 信 頼 性

Web やスーパーコンピュータなどの情報リソースを利用するために、われわれは ID を使います。われわれの大部分は、ID を使うシーンにもっぱら係わっていればよく、それがどのように発行され、管理されているかについては、あまり気を使わなくても良いようになっています。しかし、この「発行」や「管理」のコストは結構大きなものです。本人性確認について強力な枠組を提供する PKI ならなおさらです。ここでは、情報基盤センターの PKI プロジェクトが検討を進めている「信頼するに足る CA の構築」について、背景説明をしてみたいと思います。

1.PKI とその応用

PKI の枠組において、一般利用者（エンド・エンティティ）は公開鍵と証明書を公開し、さらに私有鍵を秘密にして、本人以外がアクセスできないようにしておきます。これを利用すると、公開鍵と証明書の情報を持っているサーバ側と、私有鍵の情報を持っている利用者側の間でやりとりを行って認証を行うことができます。やりとりのプロトコルの例として、公開鍵認証やチャレンジーレスポンス認証が知られています。

認証は対人間には限りません。HTTPS を使った通信ではサーバの認証が入ります。これに使われるのがいわゆる「サーバ証明書」です。

また、相手の公開鍵でメッセージを暗号化してメールで送り、送られた側は私有鍵で復号する S/MIME も PKI の重要な応用です。この場合、鍵は暗号化/復号に使われます。

公開情報と秘密情報の分離は大きな発明であり、現在 PKI が、セキュリティの強度と、スケーラビリティに優れているシステムであるといわれる理由になっています。利用者どうしがお互いに秘密情報を持つ（共通鍵）システムでは、全体の体制が大きくなると、運用が難しくなると指摘されています。

2.PKI の「信頼性」

このような便利な枠組を提供する PKI ですが、その利便性を享受するには、PKI が安定して運用されなければなりません。特に、証明書と公開鍵、私有鍵がどのように生成、配布、管理されるのかのライフサイクル管理を定めることが重要になります。この中心にあるのが、PKI の管理部門です。管理部門はいくつかの機能があり、しばしば独立した局として運営されます。証明書や鍵を発行する発行局(IA)と利用者の情報を登録する登録局(RA)は、認証局(CA)として、管理部門の中核を担うものです。さらに証明書と失効情報を公開するリポジトリの運用が重要になります。

3.CA とその「信頼」

そういうわけで、利用者が「CA を信頼する」ことが重要です。PKI の文脈では、「利用者（エンドエンティティ）が CA を信頼する」とは、「証明書が発行されるエンティティの本人性を正確に表現すると、エンドエンティティが思うこと」になります。たとえば、発行に関してずさんな管理をしていて、誰に発行したのかの正確な管理ができていなかったり、証明書が失効したのにそれを公開しなかったりとか、ということが疑われると、それだけでアウトです。ある程度いいかげんな管理を許す研究室レベルのサーバでは、いつのまにか知らない人のアカウントが、一人の管理者の独断で作成されることは今までよくありましたが、PKI では、そのような管理は許されません。

4.CA 運用のいろいろな解

CA の運用は、そういうわけで必然的にお役所的になります。しかも、利用者からの信頼を得るためには、物理的なセキュリティの確保も重要になります。それら（大学レベル・規模の CA を運用するため）にかかるコストがどうなるかの積算は、実はわれわれのプロジェクトの重要な検討テーマになっています。先行して PKI を運用する組織では、おおよそ 3 つの解を持っています。すなわち、1. アウトソースする、2. 内部で構築、運用する、3. アプリケーションを限定して、セキュリティに関して弱いところを認識して、それを納得ずくで使うことにする、です。1. については、いろいろなベンダーが証明書発行業務を請け負っています。セキュリティ的にも、申し分ない管理をしています（管理の基準としては、アメリカ公認会計士協会の Web Trust for CA、日本では特定認証業務に係る基準が有名です）。その代わり、コストはそれなりのものを見なければなりません。3. については、無線 LAN や、Grid などでの取り組みが知られています。

5.本センターでの取り組み

われわれは、すでに、学生証/職員証といったメディアを持っているわけで、それらに後付けで PKI を実現し、なおかつ柔軟性を持った CA の運用を可能にするためにどのくらいのコストがかかるかの検討からはじめることにしました。また、いきなりアウトソースするのではわれわれの意識もスキルも上がらないと考え、2. の「内部で構築、運用する」ことを選びました。実際に作ったのは、申請から発行までの PKI 管理業務をつかさどるためのソフトウェアシステムです。

問題なのは「信頼」されると同時に、発行する側のコストの削減、発行される側の利便性を満たさなければならないことです。「信頼」については、運用についてある一人の悪意のある独走を許さないソフトウェアシステムの構築をすることで、テストを始めようとしています。さらに、上であげたような厳しい基準を参考にして、運用管理モデルを構築しました。また、発行する側についても、少人数での最低限度の作業で業務が回るようなモデルの構築をし、実際にテスト的に運用しようとしています。さらに、管理の手間の削減と並び、証明書を申請した利用者がオンラインで安全に証明書を受け取れるようなソフトウェアシステムを構築しました。

現在は、プロトタイプの構築が終了し、これを用いてテストと、コスト検討を始めようとしているところです。また、デモンストレーション用のパッケージを作成しました。今後は、協力していただけるところを探して、「信頼」されるに足る CA の熟成をはかっていきたいと思います。

（佐藤周行）