5Q-03

SPKI (Simple Public Key Infrastructure) によるプライバシー重視の権限管理の提案と Java を用いた実装

梅澤 健太郎　齋藤 孝道　奥乃 博
東京理科大学 理工学部 情報科学科

SPKI（Simple Public Key Infrastructure）は, 公開鍵暗号を用いた権限管理の技術である. SPKIでは認証と権限管理を別に扱うことができるので, X.509 証明書を用いた場合よりもプライバシーを重視し, サービスが提供できると期待される. 本論文では, SPKIを用いた権限管理の Java による実装を行い, その応用の検証を行ったので報告する.

1. プライバシー重視のネットワークサービス

公開鍵暗号を用いた安全な通信のためのインフラストラクチャの構築の動きがあり, それは PKI (Public Key Infrastructure) と呼ばれ, その枠組みの一つとして, PKIX (PKI with X.509) が提案されている. PKIX は ID 証明書を発行する母体として認証局 CA (Certificate Authority) を使用し, 証明書としては X.509 を用いる. 元来, PKIX は認証の枠組みであるが以下のようにして権限管理に利用できる:

1) **認証**：公開鍵と ID の結びつきを保証する ID 証明書を用いて, 本人であることを示す.
2) **権限管理**：属性証明書 (一般的にはサーバの ACL) を確認し, ID の属性である権限を決定する.

ID と公開鍵, 及び, ID と権限の結びつきが前提となっていて, 認証 (authentication) と 権限 (authority, access rights) が一体化している. このように, 権限と公開鍵とを結び付けるのに ID が必要なので, PKIX による権限管理を用いた場合, 匿名サービスといったプライバシーを重視したネットワークサービスの実現は難しい.

本稿では, ID を介さず権限と公開鍵が直接結びついている SPKI (Simple Public Key Infrastructure) の権限証明書 (Authority Certificate) を利用し, プライバシー重視の権限管理, つまり, 認証と権限が分離した権限管理の枠組みを提案する. 具体的な権限証明書の様式は, 以下のような 5-tuple に発行者のディジタル署名を付加したものとなっている.

$$[I, S, D, A, V]$$

- I:Issuer. 権限証明書の発行者の公開鍵.
- S:Subject. 権限を行使する主体の公開鍵.
- D:Delegation. bool 値. S が更に権限を委譲することが可能かどうかを示している.
- A:Authorization. 権限を表現している.
- V:Validity. 証明書の有効期限.

なお, 一般に, 権限の生存時間は短かく種種の権限が存在するが, それらに対応した使い捨ての公開鍵を利用できる.

SPKI-based Access Control and Its Implementation
by Kentaro Umesawa, Takamichi Saito, Hiroshi G. Okuno
Dept. of Information Sciences, Science University of Tokyo
2461 Yamazaki, Noda, Chiba 274-8510

2. SPKI に基づいた権限管理の枠組

SPKI は, Carl Ellison の論文 [1] を切っ掛けに始まり, 現在, RFC2962, 2963 で規定されてている [2),3)]. RFC の中では, 名前空間に関する記述が多いが, 我々のアイデアは, SPKI 権限証明書が ID を含まないという事実に着目し, プライバシーを重視した権限管理の実現を目指したことにある.

以下, 具体的な応用を提示しながら, SPKI による権限管理について説明する.

2.1 SPKI による権限管理で登場する主体 (Entity)

1) **発行者 (Issuer)**：ユーザを認証して権限証明書を発行する.
2) **検証者 (Verifier)**：権限証明書の正当性を検証し, その権限に応じたサービスをユーザに対して提供する.
3) **委譲者 (Delegater)**：自らの権限の一部を, 他のユーザに与える為に権限証明書を発行する.
4) **ユーザ (User)**：権限証明書を獲得し, 権限を行使する主体. 委譲者にもなりうる.

2.2 権限管理の処理の概要

今回, 我々は, Web サーバが提供するコンテンツに関して SPKI による権限管理を行った. 以下では, **発行者**は権限証明書発行サーバ, **検証者**は Web サーバ, **権限**は "Web コンテンツにアクセスできる権利", である.
権限管理の処理は大きく権限証明書発行, 権限委譲, 権限証明書検証という 3 つに分かれる.

2.2.1 権限証明書発行

1) ユーザ $\mathcal{A}$ は, 発行者に自分の ID を渡す.
2) 発行者は, $\mathcal{A}$ の ID に対応する「権限」と「公開鍵」に, 自分の公開鍵, 証明書の有効期限, 及び権限委譲の可否を示す情報を付加して, 権限証明書 $Cert_1$ を作成する.
3) 発行者は, デジタル署名を $Cert_1$ に付け, $\mathcal{A}$ に発行する.

ここで, $Cert_1$ を受け取った $\mathcal{A}$ は, $Cert_1$ を検証者に提示することで $Cert_1$ の示す権限を行使できる. また $\mathcal{A}$ は, $Cert_1$ の権限委譲項目が可の場合, $Cert_1$ を基にして, $Cert_1$ にある権限の範囲内で別の権限証明書を発行することもできる.

2.2.2 権限委譲

$\mathcal{A}$は, 委譲者となり, $Cert_1$を基にして, 権限を委譲する相手$\mathcal{B}$の公開鍵, $\mathcal{B}$に委譲する権限, 有効期限などの情報から権限証明書$Cert_2$を作成する. そして$\mathcal{A}$は$\mathcal{B}$に$Cert_1$, $Cert_2$を渡す. ここで, $Cert_1$, $Cert_2$を受け取った$\mathcal{B}$は, $\mathcal{A}$と同様に, $Cert_1$, $Cert_2$をVerifierに提示することで$Cert_2$の示す権限を行使できる. また$\mathcal{B}$は, $Cert_2$の権限委譲項目が可の場合, $Cert_2$で指定された権限の範囲内で別の権限証明書を発行することもできる.

2.2.3 権限証明書検証

1) ユーザは, 自分が持つ権限証明書のうち, 行使する権限に関連したすべての証明書を, 検証者に渡す.
2) 検証者は, 与えられた権限証明書の正当性を検証する. 正当と判断された場合, 検証者はユーザに対して権限に応じたサービスを提供する.

以上である. ここで, ユーザに対するサービスの提供は, ユーザが提示した権限証明書に含まれるユーザ自身の公開鍵を用いて, 暗号化できる.

3. Javaによる実装法

3.1 クラスの分類

実装においては処理系を三種類に分類した. その分類と, そこに属するクラスは以下のようになっている (図1) .

(1) **SPKI Tools**: SPKIによる権限管理に必要で, 固有のサービスに依存しないもの
- ISSUE: 権限証明書の生成用メソッド群
- VERIFY: 権限証明書の検証用メソッド群
- DELEGATER: 権限を他人に委譲するための権限証明書を生成する
- CreatePK: 公開鍵・秘密鍵の生成を行う

(2) **UI**: (1) のUI (User Interface) を提供するもの. Servletを使用.
- VERIFIER: 検証者のUIを提供するServlet
- ISSUER: 発行者のUIを提供するServlet

(3) **AuthorityServer**: 権限に応じたサービスを提供する為のもの
- AuthorityManager: 提供するWebコンテンツの決定を行う

提供するサービス毎に**AuthorityServer**を用意することで, 様々な権限を管理することが可能となる.

3.2 実装の考察

今回の実装において, 我々の考えるプライバシーが重視された状態とは, 権限発行, 行使, 及び委譲に際して, Webサーバが ID 情報を得る手段をもたないということである. この条件が充たされていることを以下で示す.

- **証明書の発行**: 発行者は, IDと公開鍵, 及びIDと権限の対応を記したホストの設定ファイルを参照している. しかし, 今回の実装において証明書発行サーバは, Webサーバと別の組織の運営によるチケット発行センターのようなものと考えている. したがって, 発行の際ユーザが提示したIDについて, Webサーバが直接知るすべはない.
- **権限の委譲**: 権限証明書自体には, ID 情報が含まれていないので, WebサーバへのID情報の流出はない.
- **権限行使**: 検証者は, ID情報を含まない権限証明書を検証する. その為ID情報は必要とされない.

以上より, この枠組みにおいて, WebサーバがID情報を得ることはない.

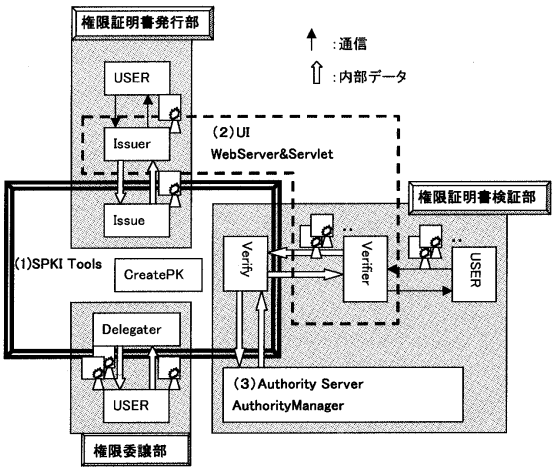

図1 各クラスの相関図

4. まとめ

本稿ではSPKIを用いた権限管理の枠組みを与え, Webサーバのコンテンツの権限管理という実装例について述べた. この手法は権限管理の対象となる組織において, 構成員のID, ひいてはプライバシーを重視する方法である. 本稿においてはあまり触れなかったが, PKIXと比較した場合のSPKIの利点[4)5)]として, 証明書の発行, 及び権限管理などを自分のポリシーに基づいた形で実現できるという点もある. なお, Webサーバへのコンテンツアクセス管理システムは研究室内で運用中である.

参考文献

1) C. Ellison: Establishing Idetity Without Certification Authority, *Proc. of USENIX Security Symp.*, '96.
2) C. Ellison, *et al.*: SPKI Certificate Theory, RFC2693, May 1999.
3) C.Ellison: SPKI Requirements, RFC2692, Sep. 1999.
4) T. Saito, K. Umesawa, *et al.*: Access Control by SPKI Certificate, *JW-ISC, to appear*, 沖縄, Jan. 2000.
5) 菊池, 川倉: SPKI/SDSIの承認証明書のフレームワークを利用した電子学生割引証, コンピュータセキュリティ研究会, 1999/5/21