「PKI アクションプラン」

OASIS PKI TC

著者：Steve Hanna Hanna (Sun Microsystems, Inc.)

日付：2003 年 11 月 24 日

バージョン：0.4

ドラフト

目次

1. はじめに

公開鍵インフラストラクチャ（PKI）は 20 年以上も前に考案され、現在、多くの重要な標準やプロトコル（たとえば、SSL/TLS、IPSEC 等）で使われている。毎日、数百万というユーザがショッピングやバンキングの目的でセキュアな Web サイトを訪れ、PKI はその接続をセキュアにするために使用されている。

しかし、PKI が持つすべての潜在能力に到達しているとはいえない。PKI はユーザ認証に使用でき、大量の PIN とパスワードを記憶する必要性を取り除く。また、PKI は、商用トランザクションをセキュアにしたり、電子メールや電話での会話のプライバシーを保護するために使用できる。しかし、アプリケーションの不足、高いコスト、PKI の理解不足、および相互運用可能性の問題等、数々の障害により、PKI の使用が制限されているのが現状である。

OASIS 公開鍵インフラストラクチャ技術委員会（PKI TC）は、デジタル証明書の導入に関する問題を克服するという共通の任務を持つ PKI ユーザ、ベンダー、および専門家で構成されるグループである。PKI TC の最初のミーティングで、TC の重要な役割とは、PKI の導入と利用に対する障害を認識し、これらの障害を克服することであると、メンバー間で意見が一致した。このトピックについて、2 つの調査が実施された。調査結果（セクション 2 で概説）により、PKI の導入と利用に対する 5 つの大きな障害が明らかになり、これらの障害を克服するためのいくつかの推奨事項も提案された。

調査結果に基づいて、PKI TC は、障害を克服するために一致した取り組みを呼びかける「PKI アクションプラン」を構築した。これらの取り組みによってコストの削減とセキュリティの強化がもたらされ、PKI ユーザ、将来のユーザ、ソフトウェアベンダなどのすべての団体にとって有益なものになるであろう。ただし、すべての団体による一致した取り組みが不可欠である。PKI TC は連携を保つためだけの、つまり調整役としての役割を果たすだけである。

このため、OASIS PKI TC は、すべての PKI 関係者（ユーザ、ベンダー、標準化グループ、および専門家）に「PKI アクションプラン」のレビュー、コメント、およびサポートを依頼している。そして、2004 年 2 月に、多くのサポータとともにアクションプランを発表し、発表と同時にプランの実行を開始する予定である。PKI TC は、すべての団体による真剣な取り組みによってプランが遂行され、大幅な改善がもたらされるものと確信している。

2. 調査結果

最初の調査は 2003 年 6 月に実施され、回答者は PKI の導入と利用の妨げになっている主な要因を明確にするよう求められた。この調査は高レベルの多くの回答者を得られたという点で成功し、いくつかの特定の障害が明らかになった。これに続いて 2003 年 8 月に第 2 回目の調査が実施され、PKI TC は障害の認識をよりいっそう深めた。これらの調査結果は、「http://www.oasis-open.org/committees/pki/pkiobstaclesjune2003surveyreport.pdf」と「http://www.oasis-open.org/committees/pki/pkiobstaclesaugust2003surveyreport.pdf」で参照できる。

これらのレポートを読み、調査の回答者によって明らかにされた障害を完全に理解することが必要である。しかし、「PKI アクションプラン」の段階を設定するために、ここではその概要を示すことにする。

PKI TC 調査には、200 名以上の回答者が参加した。これらの回答者はさまざまなバックグラウンドを持ち、IT 管理者とスタッフも数多く含まれている。注目すべき点として、回答者の 90%が PKI の導入または PKI 関連ソフトウェアの開発を経験している。

調査の結果、PKI の導入と利用をはばむ障害のトップ 5 が次のように明らかになった。

1. ソフトウェアアプリケーションが PKI をサポートしていない
2. コストが高すぎる
3. PKI の理解不足
4. あまりに技術に注目し過ぎており、十分にニーズに応えていない
5. 相互運用可能性が貧弱である

他の障害も指摘されているが、この 5 つが他よりも上位に位置付けられる。

調査の回答者は、最も重要なアプリケーションは、ドキュメント署名、セキュア電子メール、電子商取引、およびシングルサインオンであると指摘した。ドキュメント署名は、フォームへの署名、契約への署名、配布前の文書への署名に細分化されるが、これらの 3 つのサブカテゴリはほぼ等分の関心がもたれている。

調査の回答者は、これらの障害の原因と、PKI TC または他の人々がこれらの障害を克服するためにできることを、各自の言葉で書くよう求められた。多くの回答者によって繰り返し述べられたテーマは次のとおりである。

- PKI のサポートが不統一である。アプリケーションやオペレーティングシステムにこれが欠落しているケースもある。存在する場合でも、サポートされる内容が大幅に異なる。これによって、コストと複雑さが大幅に高められ、相互運用可能性を確保することは至難である。
- 現在の PKI 標準は不十分である。場合によっては（証明書管理のように）標準が多すぎる。また（スマートカードのように)、標準が少なすぎることもある。存在する場合でも、標準が柔軟かつ複雑すぎる。つまり、あまりにも柔軟で複雑なので、異なるベンダーによる実装間ではほとんど相互運用可能性がない。
- 標準をどのように使用すべきかを示す特定のプロファイルまたはガイドラインを作成する。ガイドラインは、ベンダーとカスタマが正しく実装し、PKI の相互運用可能性を確保できるよう、簡潔で明快なものにすること。場合によっては、標準を作成、統合、または改善することも必要。
- 相互運用可能性のテストおよび相互運用可能性を改善するテストイベントを実施する。
- シンプルな PKI を構築するための、クックブック方式の簡単な手順を提供する。もちろん、より高度な PKI にはカスタマイズが必要である。
- 低コストまたは無料でテスト用の PKI を構築できるようなフリーソフトウェアと CA を提供する。このフリーソフトウェアは低い保証しか提供しないが、テスト用として、また PKI を開始するきっかけを人々に与えるものとして役に立つ。

PKI TC はこれらの提案を慎重に検討し、PKI TC のメンバーの経験を加味して「PKI アクションプラン」を準備した。

これらのアイテムの中には、すでに他の人によって進行中のものもある。調査の回答は、これらの優れた取り組みを奨励する必要がある。PKI TC はこれらの人々に単に指針を与えるだけであろう。

3. PKI アクションプラン

PKI TC は、このアクションプランの策定と実装を単独で行うことはできないことを認識している。PKI には、カスタマとユーザ、CA 運用者、ソフトウェア開発者（アプリケーション、PKI コンポーネント、プラットフォーム、およびライブラリ）、業界と標準化グループ、法律家、監査者、セキュリティエキスパートなど、多くの団体が関わっている。これらのすべての団体によるサポートなしには、PKI アクションプランは完遂しえない。

PKI TC は、これらのすべての団体に相談し、プランに対するフィードバックとサポートを開始前に得るつもりである（現在、2004 年 2 月の開始予定）。コメントは http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pki にある「Send a Comment」ボタンを使用して送信する必要がある。

また、PKI TC は、これらのほとんどのアクションは、PKI TC ではなく、他の人々（ベンダー、標準化グループ、ユーザなど）によって行われるべきであることを認識している。PKI TC は、主にコーディネータ、つまり調整役として動くことを目的としている。その意味で、このドキュメントは業界へのアクションの呼び掛けといえる。このような呼び掛けを行うのは傲慢ともとられかねないが､TC はその調査を介して数百の PKI ユーザおよびカスタマから得られた要求を単に渡すだけである。TC は、このドキュメントを全員の賛意を得たコンセンサスプランとするべく、プランの発表前に関連団体と協議する予定である。

すべての PKI 関係者は、OASIS PKI TC への参加と、デジタル証明書の利用を成功に導くためのこの取り組みへの参加を望まれている。詳細については、「http://www.oasis-open.org/join」を参照されたい。

3.1. アクションアイテム

名称: PKI の利用についてのアプリケーションガイドラインを策定する

内容: 最も一般的な 3 つのアプリケーション（文書署名、セキュア電子メール、および電子商取引）において、このアプリケーションに対して標準をどのように使用するかを示す適切なガイドラインを策定する。これらのガイドラインは、ベンダとカスタマが正しく実装し、PKI の相互運用可能性を確保できるよう、簡潔で明快なものにする必要がある。

PKI TC のメンバーは、アプリケーションベンダ、業界グループ、および標準化グループと連絡を取り、このようなガイドラインがすでに存在するかどうか、存

在しない場合は、誰がガイドラインを作成できるまたは作成すべきなのかを決定する。場合によっては、標準を作成、統合、または改善することも必要である。アプリケーションのガイドラインがすでに存在する場合は、PKI TC は単にそれを示すだけである。

担当: PKI TC のメンバー、アプリケーションベンダ、業界グループ、標準化グループ

時期: 未定

名称: 相互運用可能性を向上させるための実験を増やす

内容: 相互運用可能性を改善するために、最も一般的な 3 つのアプリケーション（文書署名、セキュア電子メール、および電子商取引）に対し、適合テストのセット、相互運用可能性テスト、およびテストイベントを提供する。証明書管理プロトコルについても考慮する。ブランド設定および認定が望ましい。このような取り組みが既に行われている場合は、PKI TC は単にそれを示すだけである。行われていない場合は、作成を督励する。

担当: 業界グループ、標準化グループ（詳細は未定）

時期: 未定

名称: アプリケーション ベンダーに何が必要であるかを問う

内容: OASIS PKI TC のメンバーは、最も一般的な 3 つのアプリケーション（文書署名、セキュア電子メール、および電子商取引）のアプリケーションベンダに対し、よりよい PKI サポートを提供するためには、何が必要なのを問う。次に、これらの要件をどのような方法で満たすことができるのかを考慮する（たとえば、カスタマの要望の定量化や優秀なサポートライブラリなど）。

担当: PKI TC、アプリケーションベンダの社内（詳細は未定）

時期: 未定

名称: PKI についての教材を集めて提供する

内容: PKI の利点、価値、ROI、およびリスクマネジメント効果を技術用語を使用せずに説明する。特定の PKI アプリケーションの例を実際の利点と ROI をまじえて紹介する。また、PKI が最も適している（または適さない）状況を説明する。教材は、偏向せず、誰でも利用できるようにする。これらの教材が既に存在する場合は、PKI TC は単にそれを示すだけである。存在しない場合は、作成する。

担当: PKI TC、アプリケーションベンダの社内（詳細は未定）

時期: 未定

名称: コストを削減するための方策を追求する

内容: ソフトウェア開発コミュニティ（オープンソースコミュニティも含む）を督励し、組織がリーズナブルなコストで PKI を試用およびテストできるオプションを提供してもらう（実際に、コストが PKI の利用を阻む障害となっている）。もちろん、PKI 製品の運用には、ソフトウェアの購入以外にも多くのコストがかかるため、全世界での PKI 導入におけるコスト削減のベストプラクティスを収集し、配布することから取り組みを実行するとよい。

担当: PKI TC、開発コミュニティ、カスタマなど

時期: 未定

3.2. 次のステップ

2003 年の 11 月と 12 月に、このドラフト版のアクションプランが公開レビュー用に配布された。コメントは http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pki にある「Send a Comment」ボタンを使用して送信する必要がある。

2004 年 1 月に、PKI TC は最終版のアクションプランを準備し、そのサポートを集める予定。そして、2004 年 2 月、アクションプランを正式に発表し、実装が開始される予定である。

PKI TC は、将来、さらに調査を実施し、PKI の導入と利用の障害がどれぐらい解決されているかを測定する。「PKI アクションプラン」の開始後 2 年以内に測定可能な形で結果が現れることが期待されている。

「PKI アクションプラン」が成功すれば、他のアイテム（他のアプリケーションのアプリケーションガイドラインなど）も追加されるであろう。