

第3回 PKI R&D ワークショップ参加報告

古賀 聡† 菊池 浩明††

† 九州大学大学院システム情報科学府 〒 812-8581 福岡市東区箱崎 6-10-1

†† 東海大学電子情報学部情報メディア学科 〒 259-1292 神奈川県平塚市北金目 1117

E-mail: †satoshi@itslab.csce.kyushu-u.ac.jp, ††kikn@tokai.ac.jp

あらまし 2004 年 4 月 12 日から 14 日まで、アメリカの NIST において開催された 3rd Annual PKI R&D Workshop の開催概要について報告する。(URL : <http://middleware.internet2.edu/pki04/>)

キーワード PKI R&D ワークショップ, 参加報告

A Report on the 3rd Annual PKI R&D Workshop

Satoshi KOGA† and Hiroaki KIKUCHI††

† Graduate School of Information Science and Electrical Engineering, Kyushu University

Hakozaki 6-10-1, Higashi-ku, Fukuoka, 812-8581 Japan

†† Department of Information Media Technology, School of Information Technology and Electronics, Tokai

University Kitakaname 1117, Hiratsuka, Kanagawa, 259-1292 Japan

E-mail: †satoshi@itslab.csce.kyushu-u.ac.jp, ††kikn@tokai.ac.jp

Abstract This paper reports the 3rd annual PKI R&D workshop, held on April 12-14, 2004 at NIST.
(URL : <http://middleware.internet2.edu/pki04/>)

1. はじめに

2004 年 4 月 12 日から 14 日まで、米国メリーランド州にある国家標準技術局 (National Institute of Standards and Technology, NIST) において開催された 3rd Annual PKI R&D Workshop [3] について報告する。本ワークショップは、2002 年に第一回ワークショップ [1] が開催されて以来、公開鍵認証基盤 (Public Key Infrastructure, PKI) に関する研究ワークショップとして毎年 NIST にて開催されている。第二回ワークショップも、NIST にて 2003 年 4 月 28 日から 29 日にかけて開催された [2]。第二回 PKI 研究ワークショップの概要については、文献 [6] を参照のこと。

本ワークショップの内容として、PKI 技術だけでなくウェブ・サービス、グリッド技術、認証システム等の技術的課題や、PKI の運用、実装等にも焦点を当てている。本ワークショップの目的は、PKI における技術的課題や PKI を運用する上での課題等を、産学官における PKI 関連の専門家間で共有し討議を行うことである。

今回のワークショップの参加者は 100 名ほどであり、米国からの参加者が大半であった。他国からは、カナダ 3 名、ウガンダ 1 名、英国 1 名、トルコ 1 名、モーリシャス 1 名であり、日本からは著者らが参加した。大学の研究者以外にも、政府や企

業のセキュリティ専門家等が多数参加していた。11 件の論文発表に加え、基調講演やパネルディスカッションも行われた。論文の内容としては、技術的な論文発表だけでなく、PKI 技術に関する調査論文や今後の PKI 動向に関する内容の発表もあった。

また、次回の第 4 回 PKI R&D ワークショップは 2005 年 4 月 19 日から 21 日にかけて、今までと同様に NIST にて開催される予定である [4]。

2. プログラム

プログラム委員

Peter Alterman (NIH)
Bill Burr (NIST)
Yassir Elley (Sun Microsystems)
Carl Ellison (Microsoft)
Stephen Farrell (Trinity College Dublin)
Richard Guida (Johnson & Johnson)
Peter Honeyman (University of Michigan)
Russ Housley (Vigil Security LLC)
Ken Klingenstein (University of Colorado)
Olga Kornievskaja (University of Michigan)
Neal McBurnett (Internet2)
Clifford Neuman (USC)

Eric Norman (University of Wisconsin)
 Tim Polk (NIST)
 Ravi Sandhu (George Mason University: NSD Security)
 Krishna Sankar (Cisco Systems – program chair)
 Jeff Schiller (MIT)
 Frank Siebenlist (Argonne National Laboratory)
 Sean Smith (Dartmouth College)
 Michael Wiener (Cryptographic Clarity)

Rea, Deb Blanchard
 12:15 - 12:45 : Trusted Archiving, Santosh Chokhani
 12:45 – 14:00 Lunch - NIST Cafeteria
 14:00 - 15:00 Panel: Document Signatures, Randy Sabett,
 John Landwehr, Ron Usher
 15:00 - 15:30 PKI: Ten Years Later, Carlisle Adams

3. プログラム

2004 年 4 月 12 日 (月)

11:00 – 12:00 Registration
 12:00 – 12:15 Opening Remarks
 12:15 – 13:15 KEYNOTE ADDRESS : Non-Intrusive
 Cross-Domain Identity Management, Stefan Brands

13:15 – 14:00 Break

14:00 – 14:30 Role Sharing in Password-Enabled PKI,
 Xunhua Wang
 14:30 – 15:00 Greenpass: Decentralized, PKI-based Au-
 thorization for Wireless LANs, Nicholas C. Goffee
 15:00 – 15:30 X.509 Proxy Certificates for Dynamic Dele-
 gation, Von Welch

15:30 – 16:00 Break

16:00 - 17:30 Panel: Controlled and Dynamic Delegation
 of Rights, Frank Siebenlist, Carl Ellison, Kent E. Seamons,
 Ravi Pandya, Von Welch

18:15 – 20:00 Social Gathering and Workshop Dinner

2004 年 4 月 13 日 (火)

8:30 – 9:00 Continental Breakfast

9:00 - 10:00 KEYNOTE ADDRESS: How to build a PKI
 that works, Peter Gutmann
 10:00 - 10:30 Experiences of establishing trust in a dis-
 tributed system operated by mutually distrusting parties,
 David Chadwick

10:30 – 11:00 Break

11:00 - 12:15 Panel: NIH-EDUCAUSE PKI Interoperability
 Project: Phase Three, Peter Alterman, Russ Weiser, Scott

15:00 – 15:30 Break

16:00 - 16:30 An Examination of Asserted PKI Issues and
 Proposed Alternatives, John Linn
 16:30 - 17:30 Panel: Which PKI Approach for Which
 Application Domain?, Peter Alterman, Carl Ellison, Russ
 Weiser

2004 年 4 月 14 日 (水)

8:30 – 9:00 Continental Breakfast

9:00 - 10:00 KEYNOTE ADDRESS: A New and Improved
 Unified Field Theory of Trust, Ken Klingenstein
 10:00 - 10:30 Private Revocation Test using Oblivious
 Membership Evaluation Protocol, Hiroaki Kikuchi

10:30 – 11:00 Break

11:00 - 11:30 “Dynamic Bridge” Concept Paper, Ken
 Stillson

11:30 - 12:45 Panel: Approaches to Certificate Path Dis-
 covery, Peter Hesse, Steve Hanna, Matt Cooper, Ken Stillson

12:45 – 14:00 Lunch - NIST Cafeteria

14:00 – 14:30 Johnson & Johnson Use of Public Key Tech-
 nology, Rich Guida

14:30 – 15:00 Identifying and Overcoming Obstacles to
 PKI Deployment and Usage, Jean Pawluk

15:00 – 15:30 Break

15:30 – 16:30 Panel: The PKI Action Plan: Will it make a
 difference?, Steve Hanna, Sean Smith, John Linn, Lieutenant
 Commander, Tim Polk, and Jean Pawluk

16:30 – 17:00 Wrapup Session

4. 発表の概要

KEYNOTE ADDRESS: Non-Intrusive Cross-Domain Identity Management, Stefan Brands

異なるドメイン間の Identity Management に関する講演。ユーザの属性と公開鍵の結び付きを保証するデジタル・クレデンシャルを利用した方式を提案している。提案方式は、属性証明書を利用する場合は異なり、デジタル・クレデンシャル所有者は開示する属性を選ぶ事ができる特徴がある。そのため、ユーザのプライバシーを保護する事が可能となる。

Role Sharing in Password-Enabled PKI, Xunhua Wang

Password-Enabled PKI では、秘密鍵をユーザ自身が保持するのではなく、オンラインサーバ上に保管しパスワードを用いて利用する。現在までに、virtual soft token と virtual smartcard の二つの方式が提案されている。virtual soft token PKI では、パスワードは秘密鍵の暗号化に用いられ、それはサーバ上に格納される。ユーザは、パスワードを用いてサーバとセッション鍵を確立し、暗号化された秘密鍵をダウンロードする。それをパスワードにより復号化する事で秘密鍵を入手する。もう一つの方法である virtual smartcard PKI では、秘密鍵は二つに分割される。一つはユーザがパスワードとして保持し、もう一つはサーバ上に格納する方式である。しかし、これらの Password-Enabled PKI 方式では、一人のユーザが一つの秘密鍵を持つモデル (single user-oriented) を利用したものであり、複数のユーザが一つの秘密鍵を共有するモデル (role sharing) については考慮されていなかった。

論文では、複数のユーザが一つの秘密鍵を共有しているモデル (図 1) における Password-Enabled PKI について検討を行っており、 (t, n) 閾値法を用いた Threshold password-enabled role sharing PKI を提案している。各ユーザに割り当てられた分散情報 (share) は、パスワードにより暗号化されてオンラインサーバ上に保管される。 (t, n) 閾値法を利用している場合は、 t 人以上の協力がないと共有した role の実行 (秘密鍵による処理) ができない。

Greenpass: Decentralized, PKI-based Authorization for Wireless LANs, Nicholas C. Goffee

Greenpass は、権限が付与されたユーザのみが内部のワイヤレスネットワークに接続でき、さらに外部のゲストに内部ネットワークへのアクセス権限委任ができる事を目的とした、Dartmouth 大学のプロジェクトである。ワイヤレスネットワークにおけるセキュリティについては、権限付与されたユーザを識別するために SPKI/SDSI (Simple Public Key Infrastructure/Simple Distributed Security Infrastructure) の権限証明書を利用している。SPKI/SDSI では、本人認証だけでなく権限を他人に委任する機能を持つ。

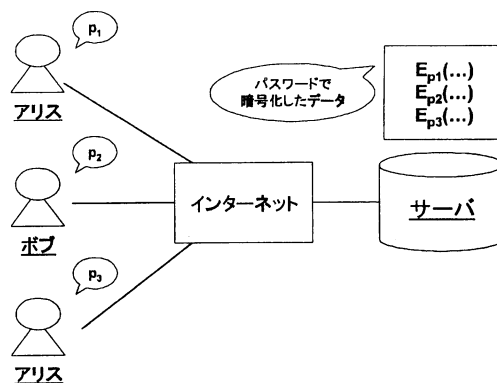


図 1 Password-Enabled Role Sharing

X.509 Proxy Certificates for Dynamic Delegation, Von Welch

代理証明書 (Proxy certificate) は、公開鍵証明書を所有するエンティティが、他のエンティティに権限を委譲するために利用される証明書である。公開鍵証明書と異なる点としては、認証局ではなく、公開鍵証明書もしくは他の代理証明書の所有者が代理証明書の発行者となる。代理証明書を発行する際には、公開鍵証明書の発行プロセスのような厳密な認証が必要ないため、動的かつ柔軟に発行することが可能である。また、大きく異なる点として代理証明書発行者の持つ全ての権限を代理証明書所有者に委任するポリシーを設定する事ができる。

グリッド・コンピューティングのセキュリティ基盤である Grid Security Infrastructure (GSI) では、認証と暗号化を実現するために、X.509 公開鍵証明書、SSL/TLS プロトコルに加えて X.509 代理証明書も利用可能となっている。論文では代理証明書をを用いた、動的な権限委任方式やシングル・サイン・オンについて検討している。

KEYNOTE ADDRESS: How to build a PKI that works, Peter Gutmann

発表者は、以下のような PKI における課題を指摘し、その解決案を提案した。

(1) Key lookup

1976 年に、Diffie と Hellman により “Public File” が提案されたが、30 年たった今でも公開鍵の検索は困難である。発表者は解決案として、Web を利用する方法を提案している。Google のような検索エンジンを用いて簡単に公開鍵を取ってくる事ができる。

(2) Enrolment

証明書を発行してもらう際の最初の登録作業は、ユーザにとって非常に面倒で時間のかかる作業である。そこで、DHCP のように ID と PIN だけで、自動的に鍵生成と証明書発行を行う方式を提案している。

(3) Validity checking

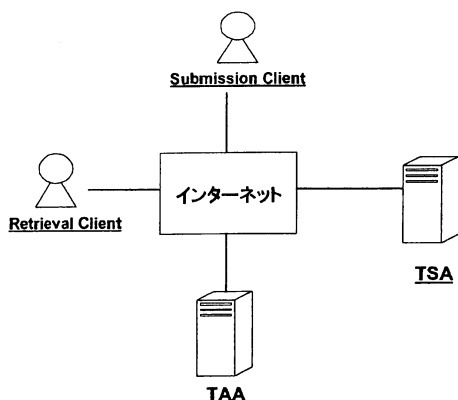


図 2 Trusted archive system

オンライン・バンキング等では、リアルタイムで有効性検証が必要である。このリアルタイム性を実現するため、リクエストに対して Yes/no の応答を返す検証システムを提案している。

Trusted Archiving, Santosh Chokhani

PKI の整備が進み、電子商取引におけるデジタル署名の利用が今後ますます普及していく事が予想される。しかし、公開鍵証明書には有効期限があるため、期限切れや失効した後も、長期間にデジタル署名文書を保存できるシステムが必要とされている。本論文では、電子文書を長期間安全に保管するためのアーカイブシステムについて論じている。

提案しているアーカイブシステムは、信頼のあるアーカイブ・オーソリティ(Trusted Archive Authority, TTA), タイムスタンプ・オーソリティ (Time Stamp Authority, TSA), 電子文書を提出するクライアント, 電子文書を検索するクライアントの 4 つのエンティティにより構成される (図 2)。

電子文書にデジタル署名が付与されている場合、提出者は電子文書に加えて、公開鍵証明書、認証パス上の証明書、CRL 等の検証に必要なデータも一緒に TAA に提出する。TAA は、送られてきた電子文書を TSA に送り、タイムスタンプを付与してもらう。TSA の公開鍵証明書の有効期限が切れると、タイムスタンプが付与された署名データの検証ができなため、提案システムではタイムスタンプの更新を行う。そのため、アーカイブ・レコードは過去に更新したデータの入れ子構造となっている。筆者らは、アーカイブシステムの標準化活動を行っており、Long-term Archive Service Requirements をウェブサイト [5] にて参照できる。

PKI: Ten Years Later, Carlisle Adams

論文では、PKI の歴史と進化について検討を行っており、初期の PKI の定義がどのように変遷してきたかを調査し、現在の定義との比較を行っている。10 年ほど前に PKI という言葉が生まれ、その当時はオーソリティとして認証局、失効検証として CRL のみだった。しかし、10 年間の研究開発を経た現

在では、様々なオーソリティ(登録局、属性認証局等)や失効検証方式(オンライン検証方式等)が提案されている。

また論文の中では、X.509, PGP (Pretty Good Privacy), AADS (Account Authority Digital Signature)/ANSI X9.59, SPKI について、証明書発行プロセスや、検証プロセスなどの観点から比較を行っている。筆者は、今後の PKI の展望として「理論から実践への移行 (Moving from theory to practice)」を強調していた。

An Examination of Asserted PKI Issues and Proposed Alternatives, John Linn

現在の PKI における問題点を整理し、既存の PKI に代わる拡張方式や新しい認証方式について論じている。PKI における問題点として、証明書検索や証明書検証処理のコストが増大になる事や、ドメイン間における信頼確立、プライバシー問題について取り上げている。

それらの問題点を解決するための PKI の代替案として、Identity-Based Encryption (関連研究として Certificateless Public Key Cryptography, Certificate-Based Encryption についても紹介している) や、オンライン第三者機関 (On-Line TTP) を用いた方式等を紹介している。

Panel: Which PKI Approach for Which Application Domain?, Peter Alterman, Carl Ellison, Russ Weiser

PKI をどのアプリケーション(文書署名、認証、暗号化等)で利用するのか、またどの産業(政府、金融等)で利用するのかによって、適用する PKI 技術とその効果について検討を行っている。また、電子メール暗号化のための技術 S/MIME、ネットワーク認証に利用されるシングルサインオン、通信路暗号化のための SSL/TLS 技術についての説明が行われた。

Private Revocation Test using Oblivious Membership Evaluation Protocol, Hiroaki Kikuchi

OCSF (Online Certificate Status Protocol) のようなオンライン証明書検証システムでは、ユーザは第三者機関(レスポンド、ディレクトリ)に証明書の失効情報に関するリクエストを送信する。この場合、第三者機関には誰がどの証明書の失効確認をしているかが分かってしまう。これがプライバシー問題に繋がる事が指摘されている。このプライバシー問題を改善するために、どの証明書について失効確認を行っているかを、問い合わせた第三者に匿名にできる PIR (Privacy Information Retrieval) 方式 (図 3) について検討を行っている。

筆者はリクエストのプライバシーに加えて、失効情報の信頼性と効率性(リクエストとレスポンスのサイズ、ユーザの計算コスト)を考慮した PIR 方式を提案している。

"Dynamic Bridge" Concept Paper, Ken Stillson

PKI では、証明書を検証する際に「認証パス構築」と「認証パス検証」の二つの処理が必要となる。認証パス構築では、検証対象となる証明書と検証者の信頼している認証局の間の認証

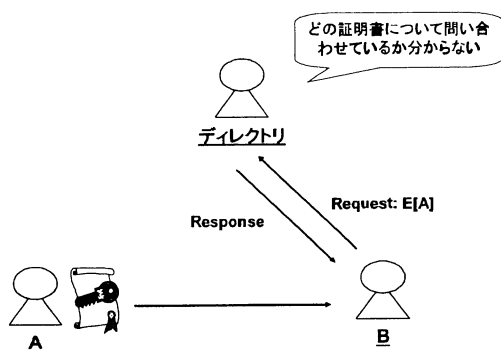


図 3 Private CRL Testing

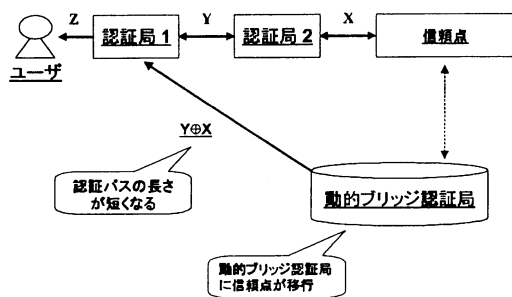


図 4 Dynamic Bridge CA

パスを発見し、認証パス上の証明書を入手する。認証パス構築が終わると、入手した証明書についてそれぞれ失効情報の確認、発行者の署名の検証等の処理を行う（認証パス検証処理）。

メッシュモデルやブリッジ認証局モデルのように、多くの相互認証証明書が用いられている PKI 信頼モデルにおいては、認証パスが何通りも存在するため、望ましい認証パスを決定するためにグラフ理論に基づくパス発見アルゴリズムを使用する必要がある。そのため、認証パス構築処理は非常に複雑で時間がかかる処理となる。また、認証パスが長くなると検証する証明書の数が大きくなり、認証パス検証処理にも時間がかかる。

論文では、認証パス構築、検証処理の効率化を目的として、動的ブリッジ認証局という概念を提案している。図 4 に動的ブリッジ認証局の概観を示す。検証者は動的ブリッジ認証局を信頼点とする。動的ブリッジ認証局は、証明書チェーンを一つに圧縮した証明書 $Y \oplus X$ を発行する役割を持つ。これにより、証明書 Z を検証する際に、既存の場合では証明書 X と証明書 Y について検証しなければならなかったが、証明書 $Y \oplus X$ を検証するだけでよいため、認証パスを短くする事が可能となる。

Panel: Approaches to Certificate Path Discovery,
Peter Hesse, Steve Hanna, Matt Cooper, Ken Stillson

証明書を検証する際は、証明書から信頼している認証局（信頼点）までの認証パスを構築する必要がある。特に、ブリッジ認証局モデルやメッシュモデル等、相互認証証明書を利用して

いる PKI 信頼モデルを採用した場合、この認証パス構築は複雑な処理となる。

認証パス構築方法は、ルート認証局から証明書までを辿る検索方式（Forward 検索）と証明書からルート認証局を辿る方式（Reverse 検索）があるが、パネリストらは、階層型モデルでは、Forward 検索、メッシュモデルでは Reverse 検索、ブリッジモデルでは両方を採用する方法が良いと主張していた。また、認証パス構築の高速化手法は、もはやグラフ理論に基づくパス発見アルゴリズムだけでは解決できず、認証パスを検証サーバにキャッシュするなどの工夫が必要であることを強調していた。

Johnson & Johnson Use of Public Key Technology,
Rich Guida

Johnson & Johnson 社では、6 万人もの遠隔ユーザの認証として PKI を利用している。その経験からいくつかの事例を取り上げている。例えば、証明書失効リストの肥大化（1 メガバイト）等の問題点を指摘している。

Identifying and Overcoming Obstacles to PKI Deployment and Usage, Jean Pawluk

PKI の普及が何故遅れているのかについて、その原因を探るため PKI 専門家へアンケートを実施し、その結果について報告している。PKI 普及の障害となっている原因として、ソフトウェアが PKI をサポートしていない、コストが大きい、PKI について理解が足りない等のアンケート結果が出た。PKI 普及促進のために、PKI 実装・運用方法について明確で分かりやすいガイドラインの作成が必要である事を筆者は主張していた。

5. おわりに

本論文では、第三回 PKI R&D ワークショップの開催概要について報告した。ワークショップ参加者には論文を掲載した予稿集が配布されたが、論文及び発表資料はワークショップのホームページ [3] 上に公開されている。

文 献

- [1] 1st Annual PKI Research Workshop
<http://www.cs.dartmouth.edu/pki02/>
- [2] 2nd Annual PKI Research Workshop
<http://middleware.internet2.edu/pki03/>
- [3] 3rd Annual PKI R&D Workshop
<http://middleware.internet2.edu/pki04/>
- [4] 4th Annual PKI R&D Workshop
<http://middleware.internet2.edu/pki05/>
- [5] Long-Term Archive and Notary Services
<http://www.imc.org/ietf-itsans>
- [6] 古賀、櫻井, “第 2 回 PKI 研究ワークショップ参加報告”, 情報セキュリティ研究会 (ISEC), 信学技報 Vol.103 No.196, Jul. 2003.