Findings and Recommendations of the Industry/Government FPKI Think Tank

Bethesda, MD
September 6, 2007

Table of Contents

1 Introduction

On September 6, 2007, Dr. Peter Alterman, Chair of the Federal Public Key Infrastructure Policy Authority (FPKIPA), hosted a group of PKI experts from government and industry to determine:

1. The strategic direction for the FPKI;
2. Short-term actions in support of that FPKI strategic direction; and
3. Long-term actions in support of that FPKI strategic direction

The results of this "Think Tank" are summarized in this paper, which is designed to encourage further discussion, exploration, and study by the FPKI.

1.1 Attendees

Name	Organization
Alterman, Peter	NIH (Chair, FPKIPA) altermap@mail.nih.gov
Ellison, Carl	Microsoft cme@microsoft.com
Fincher, Judy	Enspier Technologies (FPKIPA Support) Judith.fincher@enspier.com
Hallam-Baker, Phillip	VeriSign Principal Scientist pbaker@verisign.com
King, Matt	Enspier Technologies (FPKIPA Support) matt.king@enspier.com
Louden, Chris	Enspier Technologies Chris.louden@enspier.com
Moore, Gary	Chief Architect Cygnacom Solutions gary.moore@cygnacom.com
Pinegar, Tim	Enspier Technologies (FPKIPA Support) tim.pinegar@enspier.com
Spencer Judy	GSA (FICC Chair, SSPWG Chair) Judith.spencer@gsa.gov
Weiser, Russ	Verizon Security Business Systems russ.weiser@cybertrust.com

2 Meeting Summary

The Federal government has always been concerned with security, but is now also committed to Electronic Commerce (E-Commerce). The commitment to E-Commerce drives the FPKIPA to:

- Promote PKI for securely accessing government E-Commerce applications; and
- Encourage commercial entities to support PKI in a government E-Commerce context

The members of the Think Tank acknowledged that the current FPKI is a major accomplishment, but it is not perfect and there are issues. Some of the issues were identified during the meeting, but the list is not exhaustive. Visions for the future of the FPKI were then discussed, as well as areas where the FPKIPA should focus to achieve the most benefit to the government.

The FPKIPA will use this meeting summary as one input into the development of a long-term FPKI strategic plan.

2.1 FPKI Strategic Direction

The Think Tank discussed a variety of issues related to today's PKI Implementations. The discussion included identification of some issues and some potential solutions were also offered. These issues are discussed in the following sections, grouped into lists that can be addressed in the short- and long-term. The discussions held were not necessarily FPKI-specific and the resulting information should not be considered to be comprehensive. Rather, the issues identified should be used as a starting point to developing an overall strategic direction for the FPKI to improve the way it and other PKIs are deployed and operated.

2.1.1 Short Term

The Think Tank identified the following issues that can be addressed in the short-term (i.e., less than five years) and should be considered when constructing the FPKI Strategic Direction. The list is not exhaustive. The FPKIPA may identify and address other short-term issues.

2.1.1.1 No Need for Directory Chaining

- There was extensive discussion about directory chaining.
- The Think Tank concluded that directory chaining is unnecessary and discussed the elimination of X.500 directories. Lightweight Directory Access Protocol (LDAP) is the industry consensus directory standard, is easier and cheaper to implement, and supports all the necessary operations that X.500 supports today. Every X.500 directory can support LDAP, but not every LDAP directory supports X.500. Therefore, the impact to each Certification Authority (CA) currently cross-certified with the Federal Bridge Certification Authority (FBCA) would be minimal if X.500 directories were no longer used.

- The Think Tank suggested that it would be important to understand the number of Relying Party applications that could be impacted if the FPKIPA eliminated directory chaining.
- ***Recommendation:***
    - Eliminate X.500 Directory Chaining as soon as possible and do away with X.500 Directories over time. One approach to consider is transitioning from X.500 directory use within the border architectures to LDAP referrals. The resulting architecture would make use of LDAP referrals as the only supported communications channel.
    - Create a Transition Plan to identify and address issues that may arise for existing PKIs or Relying Parties that depend on chaining.

2.1.1.2 PKI Complexity

- The Think Tank discussed the importance of simplifying PKI and making it less complex to manage and use.
- One way to simplify PKI is to add application layers (e.g., a client) to shield them from PKI complexity and risk. However, adding new layers would add new vulnerability points.
- Other ways to simplify PKI are to use web services (e.g., XKMS, WS-Trust) and to train staff and end users about secure PKI use.
- ***Recommendation***:
    - Initiate a study to identify ways to reduce PKI complexity (for systems and users).

2.1.1.3 Role Based Access Control Gap

- If the gap between Role Based Access Control (RBAC) and PKI could be closed, it would support real world application needs.
- When academic, commercial, and government applications engage in "real business," what they really need is access control rather than just authentication that can be provided with PKI – the access control solutions for these applications could be enhanced with exchange of more attribute information.
- Exchange of more attribute information would provide tremendous benefit to the applications and using PKI to drive this exchange of information would benefit the PKI industry.
- The Think Tank discussed creating an RBAC chain with PKI certificates instead of Kerberos or a chain *initiated* with PKI. Kerberos has a model in which cooperating domains are assumed to be part of the same organization. If there were a generally accessible mapping between a Kerberos Domain ID and a public key, it would promote exchange of attribute information using Kerberos.
- The Think Tank discussed PKI as the method to link attributes to an ID (a PKI cert), which would support the authentication of individuals within their domain or across domains. Today, membership is identified relative to the domain. A move to identification of membership in the domain relative to a Root key would provide greater interoperability and allow easier exchange of attribute information.

- The Think Tank discussed how to drive convergence of PKI and SAML. If the PKI community could drive the convergence of PKI and SAML, it would help address the issue of linking attributes to identities, which would facilitate RBAC.
    - Discussion was then held about how to uniquely identify people such that their identity credentials could be linked to their attributes.
    - Discussion then addressed how exchange of attributes would be managed. Backend Attribute Exchange (BAE) is a model that would support the solution to the problem, but there are many questions to be answered, including who certifies? Who issues keys? How are attributes and Identities correlated? How do agencies and security officers accept the attribute information?
    - A participant broached the idea of an ID Attribute Issuance Infrastructure. The infrastructure would present a common data structure for common protocols. The example used was the many ways to provide information on the age of an individual (e.g., State Drivers License, Locality Birth Certificate or School ID). The Relying Party, however, decides which type of credential to trust.
- ***Recommendation***:
    - Investigate methods for using a combination of PKI and SAML to support access control, as recommended in the *Rich Attribute Exchange with PKI Certificates* document on the FPKIPA website.
    - Consider the FICC Working Group *Backend Attribute Exchange Architecture and Interface Specification.*

2.1.1.4 Lack of Naming Authority

- Since there is no authoritative Naming Authority, nothing prevents name collisions across organizations. It's possible that an organization could use a name space already in use by another organization, since an individual CA chooses names.
- For example, Treasury and other agencies use name constraints that exclude certificates from being trusted if issued within the Treasury name space by a CA not subordinated to the Treasury Root. In this case, a server that has been issued a server certificate from a CA under the Treasury-root would not trust a General Services Administration (GSA) Managed Service Office (MSO) certificate issued to a Treasury user using the National Institute of Standards and Technology Special Publication (NIST SP) 800-87 name specification. In this scenario, it is possible for Treasury to issue a certificate to a server, and when a user tried to access that server, access would be denied due to name constraints. Other agencies will face the same issue in the coming months.
- Without an authoritative Naming Authority to guarantee name uniqueness, an organization must trust that everybody else is doing things properly. Otherwise, constraints, such as naming constraints, are required to protect the individual organizations. Use of constraints is detrimental to initiatives such as the GSA MSO where a centralized service runs in parallel to individual PKIs because the constraints would deny access when, in fact, it should be allowed.
- It is not clear that it would be possible or desirable to institute a Naming Authority at this stage.

- Names are meant to be interpreted by human beings and there is a limit to the size of namespace a human can retain in memory and access correctly. This implies a need for small namespaces that is apparently at odds with the need for non-collision, which implies a single, large namespace.
- ***Recommendation***:
    - Conduct a study to evaluate what actions, if any, should be taken to address the problems presented by the lack of a naming authority.

2.1.1.5 CardAuth Deficiencies

- Currently, the PIV specifications allow for the CardAuth credential that does not require a Personal Identification Number (PIN) for use. The specifications for what types of certificates could be used for CardAuth are fairly flexible. This credential was designed for local, contactless, physical access (e.g., swipe cards), but now there is a critical mass user base (~2-3M) within the Federal government (equivalent to 1% of US population). As the PIV cards have become more widely used, there has been a desire to use these cards in inter-agency applications (i.e., not just local access). Because the specifications are not strict in how CardAuth is implemented, interoperability across agencies is inhibited and not guaranteed. Fixing the CardAuth piece is important to encourage proper use of the CardAuth credential.
- The Think Tank noted that some agencies are suggesting that PIV cards be used for more than just government use (e.g., two-factor authentication provided by PIV cards issued by banks).
- As PIV credentials are becoming more popular, states want to build compatible credentials, and large commercial entities (and bridges) want to implement the federal standard for their enterprises.
- ***Recommendation***:
    - Work to further educate PIV implementers about CardAuth usage, including potential use case descriptions of when to use CardAuth and when to use PIVAuth and coordinate with the NIST team that is working on 800-116 and who may be addressing this issue.

2.1.1.6 Barriers to PKI Deployment

- The Think Tank cited the difficulty of deploying PKI as a major problem. Few smaller entities (academic, commercial, government) can afford to implement and operate a PKI.
- Currently, the majority of PKIs are used for very high value transactions.
- In the United States, credit card companies have not adopted PKI. However, in the European Union (EU) for example, a business model has been implemented such that Merchant Acquiring Banks benefit and the Card Issuing Banks have to pay for PKI. The only fraud in EU is when legacy channels are used for initial deployment.
- The success of Chip and PIN in the EU will likely lead to demands for similar technology in the US, as implemented in the EU or in a more advanced form (e.g. wireless smartcards).
- The major barrier to US PKI deployment is the economics and composition of the US banking industry, which is highly asymmetric with tens of thousands of Card Issuing Banks and far fewer Merchant Acquiring Banks. Consequently, it is difficult to

negotiate the allocation of security measures where costs and benefits fall disproportionately on Issuers and Acquirers. Furthermore, US federal anti-trust laws arguably make it impossible to negotiate terms.

- The EU has fewer overall banks, the majority of which have an approximate balance between their Card Issuing banks and Merchant Acquiring businesses. Consequently, it is much easier in the EU to negotiate the allocation of security measures where costs and benefits do not fall disproportionately on issuers and acquirers.
- What is needed is the ubiquitous use of PKI such that people use the same credential for personal and business use.
- ***Recommendation***:
    - Investigate means of aligning benefits and risks in Financial Services industry to encourage deployment of PKI for strong authentication.

2.1.1.7 High Cost of Merging IT Systems

- IT systems are often merged, and the integration and "harmonization" process is typically costly (e.g., every time one company acquires another, the systems must be harmonized).
- The Think Tank referred back to the earlier discussion about the use of Kerberos. Today, membership is identified relative to the domain. A move to identification of membership in the domain relative to a Root key would provide greater interoperability and allow easier exchange of attribute information. The group discussed generalizing the domain in the Microsoft Windows model to be Root Key / Distinguished Name, instead of the current Distinguished Name / Root Key model. This change would result in tokens that define group membership.
- The Think Tank discussed replacing the "single root key" concept with a "quorum" concept, which could address both the fault tolerance and political problems in applications where control of the root by one entity is unacceptable. For example, mapping of the Bridge CA concept to the United Nations to create an intergovernmental PKI is unlikely to be politically acceptable to certain stakeholders.
- The Think Tank also discussed Semantic Web Technologies, which uses a secure token service to create groups. Semantic Web requires a common approach to identifying the level of assurance of an Authorization Provider.
- ***Recommendation***:
    - Further study to understand how FPKI could support various concepts that could reduce the cost of or make it easier to merge IT systems from various entities.

2.1.1.8 DNS Attacks

- The Domain Name Service (DNS) is the third major directory system in the world. The others are the postal system and telephone system.
- Currently, Internet Service Providers (ISPs) do not have an incentive to address approximately 500 billion malicious DNS hits per hour (50% of one trillion DNS hits per hour are malicious).
- "Core DNS" addresses DNS problems, such as attacks.

- If ISPs paid for the Core DNS Service, much of the ISP cost of running DNS would be eliminated since 99% of DNS costs are due to (1) mis-configured clients, and (2) malice (i.e., continuous denial of service attacks).
- Another technology that could address the issue is including a DNS lookup throttle in residential internet gateways that could turn off nodes that were violating the throttle limits.
- This issue is driven more by economics than technology.
- ***Recommendation***:
    - Determine what role the FPKIPA could play in encouraging a paradigm shift where ISPs pay for Core DNS Services and the use of DNS throttles on residential internet gateways.

2.1.2 Long Term

The Think Tank identified the following strategic direction issues that can be addressed in the longer-term (i.e., greater than five years). The list is not exhaustive. The FPKIPA may identify and address other longer-term issues.

2.1.2.1 Reducing the PKI Burden on End Points

- The Think Tank discussed the idea of reducing the burden of PKI for end points. An end point is any entity that must have PKI integrated into it (e.g., Relying Party system). The goal is to make end point PKI processing as simple and "lightweight" as possible, such that any end point, even an unintelligent device such as an electric light switch, could readily, easily, and cost effectively benefit from the use of PKI.
- If there were a way to validate credentials that was not cumbersome, it would facilitate simplicity. One idea is to move from X.500 and Certificate Revocation Lists (CRLs) to Online Certificate Status Protocol (OCSP). The following additional points were made:
    - A scenario was presented where a user calls the IT department, and provides the MAC address of a new computer. The IT department is able to tell the user's computer to connect to a specific network and be automatically configured – the key to this concept is having some intelligence in the end point with most of the intelligence in the "service."
    - It was also suggested that the XML Key Management Specification (XKMS) might help move PKI complexity away from the end points, to the service. Simple Certificate Validation Protocol (SCVP) was also mentioned but did not appear to be a viable alternative. An analogy was provided suggesting that XKMS tells someone what to do (or provides the answer) and SCVP is like sending someone to Harvard and educating them on how to approach the problem. It was also suggested that XKMS may not be moving forward as broadly as needed and that it is not possible to do provisioning with a protocol. An initial bootstrap is needed – cable companies are doing this today with "FireWire".
    - WS* is another approach. WS* is very feature rich, but there was concern that its implementation would simply result in spending more consulting dollars.

- Another idea to reduce the burden on end-points is to have a huge network of OCSP servers support Secure Sockets Layer (SSL) transactions without individual certificates, as is supported in XKMS. For example, a client could request a session with PayPal.com, and the OCSP service would tell the client which key to use. There was concern among the participants about the lack of broad use of XKMS today.
- One final idea discussed was the implementation of policies that govern how packets traverse a network (i.e., a packet is not allowed to go across a network unless a policy specifically allows it).

o ***Recommendation***:
  - Initiate a study, perhaps in conjunction with other industry groups, to explore options for reducing the complexity of PKI at the end points thereby encouraging wider use of PKI.

2.1.2.2 Accountability vs. Access Control

- The Think Tank discussed the relationship between access control and accountability. In current PKI implementations, Relying Parties trust that credentials are issued according to a specific assurance level, which allows Relying Parties to determine what credentials it should trust. However, that approach focuses on punishing a person if they misbehave (i.e., a person is accountable for their actions, which serves as a deterrent to bad behavior), which is different from access control that prevents the bad actions from occurring at all. This model is essentially "allow = accountability" vs. "deny = access control" – so the problem becomes a question of how it is possible to tie accountability of an ID + attributes to access control.
- It was suggested that several players will converge into "Identity 3.0", which is a concept where both outbound and inbound authentication are handled. It was also suggested that some type of referral model could be created by combining PKI with these concepts and common points of trust.
- ***Recommendation***:
  - Initiate a study to prepare for and possibly influence the development of a model that ties identity credentials with attributes for the purposes of access control.

3 Conclusions and Next Steps

The discussions held during this FPKI Think Tank session show that while PKI has come a long way, there are still many areas that could be improved. The FPKI Think Tank suggests the following next steps:

1. The FPKIPA should further refine the list of specific issues identified in this paper;
2. The FPKIPA should prioritize the list of issues in order to understand which issues are fundamental to the widespread deployment of PKI and critical for the FPKI strategic direction
3. Once steps 1 and 2 are completed (or nearly completed), a FPKI Vision for the Future should be developed;
4. A resolution/action plan should be created and executed to identify what activities the FPKIPA should engage in to address both short and long term goals and make progress towards the vision

The table below summarizes the issues and recommendations presented in the previous sections and can be used as a starting point for a more complex action tracking list to support the FPKI Future Vision.

Table 3-1: Issues and Recommendations Summary

Issue	Recommendation
No Need for Directory Chaining	➢ Eliminate X.500 Directory Chaining as soon as possible and do away with X.500 Directories over time. One approach to consider is transitioning from X.500 directory use within the border architectures to LDAP referrals. The resulting architecture would make use of LDAP referrals as the only supported communications channel. ➢ Create a Transition Plan to identify and address issues that may arise for existing PKIs or Relying Parties that depend on chaining.
PKI Complexity	➢ Initiate a study to identify ways to reduce PKI complexity (for systems and users).
RBAC Gap	➢ Investigate methods for using a combination of PKI and SAML to support access control, as recommended in the Rich Attribute Exchange with PKI Certificates. ➢ Consider the FICC Working Group Backend Attribute Exchange Architecture and Interface Specification.
Lack of Naming Authority	➢ Conduct a study to evaluate what actions, if any, should be taken to address the problems presented by the lack of a naming authority.
CardAuth Deficiencies	➢ Work to further educate PIV implementers about CardAuth usage, including potential use case descriptions of when to use CardAuth and when to use PIVAuth.
Barriers to PKI Deployment	➢ Investigate means of aligning benefits and risks in Financial Services industry to encourage deployment of PKI for strong authentication.
High Cost of Merging IT Systems	➢ Further study to understand how FPKI could support various concepts that could reduce the cost of or make it easier to merge IT systems from various entities.
DNS Attacks	➢ Determine what role the FPKIPA could play in encouraging a paradigm shift where ISPs pay for Core DNS Services and the use of DNS throttles on residential internet gateways.
Reducing the PKI Burden on End Points	➢ Initiate a study, perhaps in conjunction with other industry groups, to explore options for reducing the complexity of PKI at the end points thereby encouraging wider use of PKI.
Accountability vs. Access Control	➢ Initiate a study to prepare for and possibly influence the development of a model that ties identity credentials with attributes for the purposes of access control.