PKI 102. Toward a Mature, Globally Interoperable Public Key Infrastructure.

Gene. McDowell, NOAA
Chair, Federal PKI Legal & Policy Working Group
April 29, 2003

I announce today a project to produce a book, PKI 102. Toward a Mature, Globally Interoperable Public Key Infrastructure, to be published on-line at the Federal PKI Steering Committee web site. It will be published (and revised) serially, as each section is ready, with a goal of publishing the first two parts, each with four or more chapters, by the end of December 2003. Three more parts are planned for completion in 2004.

The purpose of this book is (Part I) to advance a view of how a mature, globally interoperable PKI will be structured and will operate, (Part II) to examine the current state of implementation of critical parts of that end-in-view, and identify the gap between the current state and that objective, (Part III) to assess criticisms of PKI and how well those criticisms are now answered, (Part IV) to assist organizations in making their case for use of PKI in their business applications, and (Part V) to develop and articulate plans for getting from here to there. Briefly, the purpose is to contribute direction and impetus to push along the development and adoption of PKI.

The book will be edited by me (Eugene.C.McDowell@noaa.gov), and I invite you to collaborate in this project. My own knowledge of PKI comes primarily from my work with the Federal Bridge CA (FBCA), so my views tend to be FBCA-centric. I will depend on collaborators to broaden the perspective. I have begun work on the chapters of Part I, and will circulate drafts prior to publishing the chapters on this web site. You are welcome to work on all five parts in 2003, and to submit sections as they become ready for publication (as well as to make your interest known early in the process, and to circulate drafts). A listserv will be established to facilitate the collaboration. Material in this book is in the public domain (not subject to copyright), but references (and links) to copyrighted materials may be included in this book. Before a section is published it will be peer reviewed to help assure accuracy of factual information and soundness of argument for views and proposals.

The authors assume the reader's general familiarity with PKI – what it is and does. For those lacking this familiarity, the following documents are suitable for background: The Evolving Federal Public Key Infrastructure, http://www.cio.gov/fpkisc/library/pki_brochure.pdf ; PKI 101, which will also be placed here at the FpkiSC site.

The current outline follows.

Preface

PART I. Concept and Policy

Chapter 1. A Mature, Globally Interoperable PKI

Chapter 2. Authentication and Validation as PKI Fundamentals

Chapter 3. Entities, End Entities, Relying Parties, and Parties Relied Upon

Chapter 4. Topology and Polity

Chapter 5. Outline for an Architecture of Liability in a Mature, Globally Interoperable PKI

PART II. Implementation: State of the Art, and What's Missing

Chapter 1. Subjects Dealt With Elsewhere

Chapter 2. Identity Proofing

Chapter 3. Private Key Protection

Chapter 4. SSL/TLS Implementation

Chapter 5. The User Interface and the User Experience

PART III. Criticisms, Doubts, Misconceptions, and True Weaknesses of PKI

PART IV. The Business Case for Use of PKI

PART V. Prospectus: How Do We Get There?

Glossary

Index

Chapter numbering is subject to change as chapters are added or deleted. For example, if SSL/TLS Implementation is adequately treated somewhere else (such as in a NIST document as a follow-on to the work reported by Burr and Fanto at the Fpki TWG meeting of June 20, 2002), then Part II Chapter 4 as shown above would be removed in favor of a section in Part II Chapter 1, where a brief summary of the current status would be given, along with a link to the NIST document). As a chapter, or a section of a chapter, is updated, the latest revision date will be indicated, and the revision date of the whole book will be the date of the latest revision of any of its sections. Authorship will be shown by chapter or section, as appropriate. References will be

listed at the end of each chapter or section.

Some other subjects that might be included are:

1. PKI-enablement of applications, and middleware for that function;
2. Validation, validation services, validation service providers;
3. Repository issues and solutions, directory interoperability;
4. Time-stamping: standards, products, services;
5. PKI Records management policy, technology and services (Policy guidance for PKI administrative records is about to be published by the CIO Council and NARA; guidance is needed for PKI transaction records.);
6. Mapping of assurance levels to risk assessments of applications/data (A policy guidance document on this is being prepared by OMB.);
7. Privacy;
8. Anonymous and Pseudonymous certificates;
9. Separate authentication and signing certificates;
10. Policy Mapping (if there are interesting issues);
11. Risks in PKI implementation: operational, legal, economic

Now let's look at the outline in more detail. PART I is about Concept and Policy. You can think of it as analogous to a Target Architecture.

Chapter 1 explains my concept of A Mature, Globally Interoperable PKI. The function of PKI is to provide strong security services upon which various parties can justifiably rely with a level of confidence appropriate to the risk of a business process, the value of a transaction, or the sensitivity of the information to be protected. To this end, the PKI itself must be secure. It must be robust against accidental dysfunction and against malevolent compromise. It must be designed and implemented so it's easy for users and the PKI's administrators to do the right thing and hard for them to do the wrong thing.

In PKI, as in any area of security, policy goes hand in hand with threat assessment (which determines in part what we need or want to do) and with technology (which determines in part what we can do).

The "I" in PKI is Infrastructure: the technology, hardware, software, policy, procedures and people – all working together to support the application of public key cryptography for trust in digital transactions. Since people are part of this infrastructure – both as users and as administrators – people's behaviors are an important element of the system. In very broad terms: policy, technology and behavior are the elements of PKI.

Interoperability is needed because PKI is implemented in separate trust domains – each defined

by a root CA (in a hierarchy) or defined by a mesh of CAs. To allow trusted transactions among separate trust domains, those domains must establish technical and policy means of interoperating while preserving trust.
Global interoperability is the linking of trust domains into a system of systems, just as the Internet is a network of networks, so any Relying Party can justifiably rely on PKI services in transactions with any PKI user, anywhere, anytime.

A mature PKI is one in which technology and policy shoulder almost all of the burden of making PKI work securely and smoothly, so its complexities are hidden from the user and so the behavioral element is minimized.

Chapter 2 is about the three fundamental roles of authentication in PKI, and about their relation to validation of a credential. It shows the logic by which these authentication roles are related one to another and to validation. It shows how the integrity of PKI depends on these.

Chapter 3 is about the entities in a PKI domain or a collection of interoperating domains, and about the policies and agreements that allow one entity to justifiably rely upon others.

Chapter 4 is about how the topology of a PKI domain (or collection of interoperating domains) affects who owns and enforces a policy, and it suggests the types of agreements that are suitable in the different topologies.

Chapter 5 is an outline for an architecture of liability in a mature, globally interoperable PKI. It begins by showing how certain entities in a globally interoperable PKI relate to one another. It proceeds to examine what functions are implied in those relations, infers what responsibilities one entity has to another, and suggests what potential liabilities follow from those responsibilities.

PART II is about Implementation – the State of the Art, and What's Missing. You can think of it as analogous to a Baseline Architecture and Gap Analysis. Its aim is to identify what problems have been solved, what the most important solutions are, what further work is needed, and some promising approaches.

Chapter 1, called Subjects Dealt With Elsewhere, is a place to collect subjects that are relevant to Part II but that don't need a chapter here because they have already been adequately treated in other publications. For each of these subjects, a brief summary will be included here, along with a reference to the publication.

Chapter 2, discusses Identity Proofing in the context of threat (including error and potential attacks) and in the context of levels of assurance (relating to the risk of a business process, the value of a transaction, or the sensitivity of the information to be protected). It lists the types of entity to be identity proofed: persons and various sponsored entities. The latter includes

organizations, among other types. Identity proofing methods for persons, organizations and other sponsored entities are discussed and evaluated. An approach to measuring the reliability of an identity proofing method is proposed. The essential role of technology in identity proofing is explained.

Chapter 3 describes the forms of Private Key Protection, and suggests how they rank in strength. Some methods included are camouflage of private keys stored on disk, and smart cards with biometric access control (either via a card reader or imbedded entirely within the card).

Chapter 4, about secure web implementation, is conceived as a follow-on to the SSL/TLS implementation work reported at the Fpki TWG meeting of June 20, 2002. That presentation showed, based on work done up to that time, that web security was often configured in an unnecessarily weak way, and that web server and client products were less than ideal in negotiation procedure and in configurability. Since web security is one of the most widely adopted uses of PKI, the gap between its current state and ideal state is an important opportunity for improvements with a real security payoff.

Chapter 5, on The User Interface and the User Experience, is aimed at making the user experience easy, intuitive and attractive. Think of how email, made interoperable across the Internet, has become popular. Think of how the web has transformed the way we work. To achieve widespread adoption of the security services that PKI provides, those services must be easy to use. When the user is digitally signing a document, he must be aware that he is doing so, and must understand what he is signing, just as is the case with a wet signature, because the signer's intent must be demonstrable in a law court. And when the user is communicating securely, she must be able to verify that at a glance. But as exemplified by secure web sites, the mechanics must be transparent. There is much progress in this already, but more is needed. This chapter is a place to assess what improvements can be made, to make PKI attractive to users who have no reason to care about the underlying details.

PART III is to evaluate Criticisms and Doubts, and to identify Misconceptions and True Weaknesses of PKI. Some examples of criticisms might be those that have been made by Greenleaf and Clarke (1997), Ellison and Schneier (2000), and Clarke (2000). The chapter will state a criticism, offer an answer based on current technology and policy, and follow that with a reply by the author of the criticism. If the present author wishes to make a counter-reply, that will be followed by the critic's response to that. Either way, the critic will be offered the opportunity to have the last word. This procedure will be followed for each criticism included in the chapter.

PART IV is about developing the Business Case for Use of PKI. PKI has a wide following of people who perceive it as being the best approach for the provision of strongly authenticated identification, verifiable data integrity, bilateral non-repudiation of transactions, and confidentiality of communications. But its adoption has been slow in coming. One reason is that

PKI, done right, is a complex infrastructure and it has a substantial cost for implementation and operation. Many organizations that are potential users of PKI have no killer application that alone will justify a PKI. Instead, the benefits of PKI would be spread over many applications, and they are hard to assess. The benefits would be accrued over a long period of time, and likely would appear in ways that aren't now anticipated by the organization. PKI vendors have had a hard time making a profit, and considerable consolidation has taken place in the industry. Making the business case for a potential user organization is a key to the success of PKI, yet it is a sticking point for many such organizations. The purpose of this Part IV is to focus interest on this topic, and in this way to help us progress on it.

PART V, about how to achieve a mature, globally interoperable PKI, is analogous to a Migration Plan. Having articulated a goal in Part I, and having assessed where we are and where we need to go next, we confront the question: What will be our plan for attaining this goal?

To answer this question, join the project. Contribute your knowledge and wisdom. Offer your answers and your questions. Look for us from time to time, here at the Federal PKI Steering Committee web site, http://www.cio.gov/fpkisc/ .