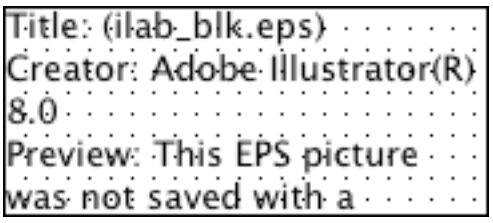


# References and Resources on Public Key Infrastructure

PKI has a lot of terms and technologies in it. The list below gives some hardcopy resources and web sites which we've found helpful in learning more about PKI ourselves.

### *Background/Technology*

**Applied Cryptography: Protocols, Algorithms, and Source Code** (2nd edition), by Bruce Schneier (ISBN: 041117099)

This is considered by many network managers and programmers to be the best description and discussion ever written on this subject. To understand the tools which make up PKI, *Applied Cryptography* is a must.

**Network Security: Private Communication in a Public World**, by Charlie Kaufman, Radia Perlman, and Mike Speciner (ISBN: 013061461)

An outstanding discussion of technologies behind PKI, but taken a few hundred feet up from Schneier's book. Kaufman, Perlman, and Speciner draw things together with a little more application-oriented discussion. You can often use *Network Security* as a first point of reference, turning to *Applied Cryptography* when you need the nuts-and-bolts.

**SSL and TLS: Designing and Building Secure Systems**, by Eric Rescorla (ISBN: 0201615983)

Because SSL was the first widely adopted application (in the form of secure web pages) to use PKI, SSL is the first exposure most of us will have to PKI. Rescorla discusses how SSL works in the first part of his book, and how it can be deployed in the second.

**PKI: A Wiley Tech Brief** by Thomas Austin (ISBN: 0471353809)

This small volume is a compendium of articles which give a more high-level overview of PKI and PKI deployment issues and strategies. It's a good introduction if you know nothing about PKI or cryptography.

**Ipsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks** by Naganand Doraswamy and Dan Harkins (ISBN: 0130118982)

The first technically accurate discussion of IPSec VPN technology, written by the people who helped to write the RFCs. If you're using PKI and VPNs, you'll want to have this on your shelf to help figure out how it all works together.

### iLabs Participating Companies

A number of key vendors in the PKI and PKI-enabling world have chosen to participate in the iLabs here. You can learn more about their products and services on the Internet.

| | | |
|---|---|---|
| Baltimore | PKI | http://www.baltimore.com/ |
| Check Point | Firewall, VPN | http://www.checkpoint.com/ |
| Datakey | Smart Card readers | http://www.datakey.com/ |
| iPlanet | Messaging,PKI,LDAP | http://www.iplanet.com/ |
| Litronic | Smart Card readers | http://ww.litronic.com/ |
| NetScreen | VPN | http://www.netscreen.com/ |
| Nokia | Firewall platform | http://www.nokia.com/ |
| Rainbow | USB tokens | http://www.rainbow.com/ |
| Secure Computing | AAA | http://www.securecomputing.com/ |

### White Papers on PKI

One of the PKI vendors has established a large repository of white papers on PKI and PKI-related issues. Although some of them are sales-oriented, many are vendor-neutral and can serve as resources for further exploration. See these at
`http://www.entrust.com/resourcecenter/whitepapers.htm`

### PKI Vendors

A number of companies provide PKI solutions. Some of them include:

| | |
|---|---|
| IPlanet (Netscape/Sun) | `http://www.iplanet.com/products/iplanet_certificate/` |
| Baltimore | `http://www.baltimore.com/unicert/` |
| Entrust | `http://www.entrust.com/entrust/` |
| Verisign | `http://www.verisign.com/products/onsite/` |
| RSA Data Security | `http://www.rsa.com/products/keon/` |
| Certicom | `http://www.certicom.com/products/trustpoint.html` |
| Microsoft | `http://www.microsoft.com/windows2000/server/` |

### Smart Cards

In our demonstrations, we show smart cards and smart card-related technology (such as the Rainbow iKey) quite a bit. You can learn more about smart cards (and find many more resource lists) at the following vendor-neutral sites:

`http://www.smartcardalliance.com/`
`http://www.smartcardcentral.com/`
`http://www.pcscworkgroup.com/`

### Public Certification Authorities

Netscape maintains a list of public certification authorities which can be helpful if you're looking for a CA to issue certificates

`http://certs.netscape.com/`