The IETF PKIX Working Group

The PKIX Working Group was established in the Fall of 1995 to develop Internet standards needed to support an X.509-based PKI. Since PKI has evolved considerably since hten, the PKIX workgroup has expanded its tasks. Today, the PKIX group profiles ITU PKI standards and develops new standards through the normal Internet RFC process to enable consistent use of X.509-based PKIs on the Internet.

IETF Simple PKI – SPKI -- Working Group:

Many Internet protocols and applications which use the Internet employ public key technology for security purposes and require a public key infrastructure to manage public keys.

The IEFT SPKI working group was convened to develop Internet standards for an IETF sponsored public key certificate format, associated signature and other formats, and key acquisition protocols. The key certificate format and associated protocols are simple to understand, implement, and use. For purposes of the working group, the resulting formats and protocols are known as the Simple Public Key Infrastructure, or SPKI.

The SPKI sought to provide mechanisms to support security in a wide range of internet applications, including IPSEC protocols, encrypted electronic mail and WWW documents, payment protocols, and any other application which requires the use of public key certificates and the ability to access them. It is intended that the Simple Public Key Infrastructure could support a range of trust models. The SPKI working group developed two RFC's, which are:

SPKI Requirements -RFC 2692, http://www.ietf.org/rfc/rfc2692.txt and
SPKI Certificate Theory RFC 2693, http://www.ietf.org/rfc/rfc2693.txt

After these two protocols, there has been no further development of this concept, and the SPKI working group is currently suspended as the output of the working group is now complete.

Early RFC's Produced by the PKIX Working Group

The PKIX has produced several informational and standards track documents. The important early documents produced are:

1. RFC 2459, http://www.ietf.org/rfc/rfc2459.txt, which profiled X.509 version 3 certificates and version 2 CRLs for use in the Internet. Profiles for the use of Attribute Certificates,

2. RFC 2587, http://www.ietf.org/rfc/rfc2587.txt, which dealt with Internet X.509 Public Key Infrastructure and the LDAPv2 Schema.
3. RFC 3039, http://www.ietf.org/rfc/rfc3039.txt, which dealt with Internet X.509 Public Key Infrastructure Qualified Certificates Profile, and
4. RFC 2527, http://www.ietf.org/rfc/rfc2527.txt, which dealt with Certificate Policy and Certification Practices Framework.

Ongoing work has produced the following topical RFC's

5. RFC 2510, http://www.ietf.org/rfc/rfc2510.txt, which deals with the Certificate Management Protocol (CMP)
6. RFC 2560, http://www.ietf.org/rfc/rfc2560.txt, which deals with the Online Certificate Status Protocol (OCSP)
7. RFC 2511, http://www.ietf.org/rfc/rfc2511.txt, which deals with the Certificate Management Request Format (CRMF)
8. RFC 3161, http://www.ietf.org/rfc/rfc3161.txt, which deals with the X.509 PKI Time Stamp Protocols
9. RFC 2797, http://www.ietf.org/rfc/rfc2797.txt, which deals with Certificate Management Messages over CMS, and
10. RFC 2585, http://www.ietf.org/rfc/rfc2585.txt, which deals with the use of FTP and HTTP for transport of PKI operations.

A roadmap, providing a guide to the growing set of PKIX document, also has been developed as an informational RFC.

Some New PKIX Projects

Some new PKIX projects include:

1. Producing a requirements RFC for delegated path discovery and path validation protocols (DPD/DPV) and subsequent production of RFCs for protocols that satisfy the requirements,
2. Developing a logotype extension for certificates,
3. Developing a proxy certificate extension and associated processing rules, and
4. Developing an informational document on PKI disaster recovery.

PKIX Goals and Milestones:

TimeLine	Item to be Worked on
Done	Complete approval of CMC, and qualified certificates documents
Done	Complete time stamping document

TimeLine	Item to be Worked on
Done	Continue attribute certificate profile work
Done	Complete data certification document
Done	Complete work on attribute certificate profile
Done	Standard RFCs for public key and attribute certificate profiles, CMP, OCSP, CMC, CRMF, TSP, Qualified Certificates, LDAP v2 schema, use of FTP/HTTP, Diffie-Hellman POP
Done	INFORMATIONAL RFCs for X.509 PKI policies and practices, use of KEA
Done	Experimental RFC for Data Validation and Certification Server Protocols
Done	Production certificate and CRL syntax and processing RFC (son-of-2459)
Done	DPD/DVP Requirements RFC
Done	Certificate Policy & CPS Informational RFC (revision)
Done	Logotype Extension RFC
Done	Proxy Certificate RFC
Done	Cert Path Building approved as Informational RFC
Done	CRMFbis approved as PROPOSED Standard RFC
Done	CMPbis approved as PROPOSED Standard RFC
Done	Principal Identifier approved as PROPOSED Standard RFC
Done	Warranty Extensions approved as Informational RFC
Done	Certificate Store approved as Informational RFC
Sep 2005	OCSPv2 Extensions approved as PROPOSED Standard RFC
Dec 2005	PKIX Repository approved as Informational RFC
Jan 2006	Progression of CRMF, CMP, and CMP Transport to DRAFT Standard
Jan 2006	Progression of SCVP to Draft Standard
Jan 2006	Subject Identification Method as Informational RFC
Mar 2006	Progression of Time Stamp Protocols RFC to DRAFT Standard
Apr 2006	Progression of Qualified Certificates Profile RFC to DRAFT Standard
Apr 2006	Progression of Certificate & CRL Profile RFC to DRAFT Standard
Apr 2006	Progression of Logotype RFC to DRAFT Standard
Apr 2006	Progression of Proxy Certificate RFC to DRAFT Standard
Apr 2006	Progression of Attribute Certificate Profile RFC to DRAFT standard
Apr 2006	SCVP approved as PROPOSED Standard RFC
Apr 2006	ECC Algorithms approved as PROPOSED Standard RFC
Aug 2006	Progression of CMC RFCs to DRAFT Standard