PKIX WG Meeting 3/20/03

Edited by Steve Kent

Chairs: Stephen Kent <kent@bbn.com>, Tim Polk <tim.polk@nist.gov>

The PKIX WG met once during the 56th IETF. A total of approximately 76 individuals participated in the meeting.

Agenda review and document status - Tim Polk (NIST)

There are about 19 WG documents in various stages in the process, some of which fell through the cracks due to process glitches. Also, IDs are no longer automatically timed-out and must be explicitly removed by WG chair action, which accounts for some of the backlog. Of special interest is the interoperability testing in support of progression of RFC 3280. NIST is working on this task. CA testing is going well but they need examples for DH, ECC, DSA parameter inheritance, and delta CRLs. Please get in touch if your implementation supports these. Several attendees indicated that they would do so. Testing of path validation implementations will start next month. [slides]

DPD/DPV standard selection process– Tim Polk (NIST)

First the WG developed RFC 3371 as a requirements basis. The WG chairs developed a compliance matrix and each protocol was rated relative to this matrix. A straw poll was conducted and SCVP received a majority (not just a plurality) of the votes. An independent review of the compliance matrix confirmed that SCVP was very close to compliance, requiring minimal changes/enhancements. [slides]

SCVP Discussion – Trevor Freemen (Microsoft)

Working to meet few remaining mandatory requirements for 3379, and to reach consensus on optional features. Adding MAC (in addition to signature) support for request authentication. Will define “standard” policies as default. Target end of May for publication of next draft. Intent is to move to WG last call before Vienna meeting. [slides]

Proxy Certificates Von Welch (Argonne Labs)

Document is also being worked on in Global Grid Forum. X.509 EE certificates that are issued by other EEs, not CAs. Contain critical extension marking it as a proxy certificate. Facility to represent delegation of full or limited rights (capability model) to the proxy, by the EE. Major change from last meeting is to describe additions to path validation to accommodate proxy certificates, i.e., hand off proxy certificate to the extended additional validation code. This is consistent with the way these certificates are currently processed by modified software in the Global Grid context. This ID is ready for WG last call. [slides]

Signature Algorithms & Key Usage – Jim Schaad (Soaring Hawk Consulting)

Often public key data (for use with signatures) could in principle, be used with more than one algorithm, e.g., RSA PSS/OAEP or DH/DSA. Today we bind signature validation keys to a pair of algorithms, via a single OID. One question is how to express that one key could be used with multiple algorithms, e.g., a mix of hash algorithms or even different public key algorithms, to avoid redundant certificate issuance, but still retain ability to express current notion of restrictive use. Analogous issues arise in validation of signatures, i.e., processing signature fields and matching against data from the certificate used to validate a signature. We could do nothing, or we could include additional data to facilitate more general use of the key bits, e.g., by creating an extension. There was disagreement over whether there is a security concern that is addressed by the proposed change. [slides]

Trusted Archive Protocol (TAP)– Carl Wallace (Cygnacom)

New protocol defining a service for trusted archive of data, in support of NR. Simple transaction protocol for timely refresh of timestamps, certificates, CRLs, etc. Requests support submission of data for archive, and a limited search/retrieval capability. Extensions to TAP allow a server to constrain the types of data accepted, to verify TAP tokens, sent by a client, etc. RFC 3161 timestamp tokens are employed. Optional services include trust anchor retrieval, relative to a prior point in time. CMS format used for TSP messages. A straw poll of the meeting attendees did not show significant support for this to become a new WG work item. The WG chairs will raise the question on the list, and ask what interest exists re implementation support, if this were to become a WG item. [slides]

Qualified Certificates Profile - Stefan Santesson (RetroSpekt)

The author is ready to update the document and is asking whether the update should address the scope of the document, i.e., should this be viewed as a (non-exclusive) profile for user identity certificates (for use with digital signature) more generally, vs. only for qualified certificates. And if so, would that result in changes to the substance of the document, e.g., the KeyUsage text might be changed to be less restrictive. A minor issue is the fact that PostalAddress is called for here, but RFC 3280 does not mandate support of that attribute. We need to be sensitive to changes that we make here, since ETSI relies on it in their standards. [slides]

Liaison Report: LDAP/X.500 alignment – Skip Slone (Lockheed-Martin)

ITU work, will show up in 5th edition of X.500. Major topics of interest for PKIX: semi-colon binary matching, string matching, enhanced matching, domain component names, NR bit. Proposal is to rename the NR bit as “content commitment” to defuse the long running debate about the name and semantics.[slides]

Subject Identification Method - Park Jong-Wook – (KISA)

Goal is to provide a way to represent a personal ID value (e.g., national ID number) in a certificate (e.g., in a subject altname) in a way that does not disclose its value, for privacy reasons. The proposal also includes a protocol for transferring this data to the CA. There will be some terminology changes, based on WG feedback. There is overlap here with our permanent identifier work, as the national ID number that motivates this work is a PI, and this overlap needs to be better described in the ID. Also, more example will be provided in the ID. The author requests more feedback from the WG. [slides]

Liaison Report: EESSI – Riccardo Genghini (Studio Notarile Genghini)

Presentation on European Electronic Signature Standardization Initiative. Includes brief review of relevant EU digital signature standards, and discussion of various EU-based committees and working groups in this area. Suggestion that EESSI and PKIX WG attendees might get together after Vienna meeting. [slides]

Liaison Report: JNSA Challenge PKI 2002 Status Report - Ryu Inada (JNSA)

A status report on the interoperability testing activities in Japan. The results of testing are useful for uncovering specification problems with PKIX standards and of products vs. these standards. Test environment includes CAs and VAs capable of generating data for test cases, some of which intentionally do not conform to PKIX standards. They provided a short demo of their test technology. [slides]

LDAP PKI Issues – David Chadwick (University of Salford)

Problem is that we cannot search for certificates and CRLs in LDAP based on anything attribute other than a Subject DN, given current LDAP search limitations. But we would like to locate these data in an LDAP server based on other attributes. The component matching solution was selected by the LDAPext WG as the preferred solution to this problem, but so far it has not received LDAP vendor support. This approach requires changes to both clients and servers. Another approach is attribute extraction, generating new attributes for directory entries by extracting them from certificates and CRLs. This can be effected by having a front end that does the processing for populating directory entries. But this strategy significantly increases storage space for each entry that holds certificates/CRLs, and the front end must be updated whenever the set of attributes to be matched against changes. This approach requires client changes, and the addition of front ends to servers, but no changes to servers per se. The Security AD has emphasized the need to have only one solution. A quick straw poll indicates that the attendees favor component matching, but the number of attendees voting was very small, thus it was decided to take this discussion to the list. [slides]