IEEE Software Taggant System Public Key Infrastructure RFP
Frequently Asked Questions

Version 1.0

1. **Does IEEE plan to create a dedicated Certificate Policy (CP) and/or Certificate Practice Statement (CPS) for the IEEE Taggant PKI, or is PKI vendor expected to either create a dedicated CPS or incorporate Taggant certificates into standard CPS?**

   It's best if the CA created these documents as part of the deliverables. If any IEEE input is required, we will provide it.

2. **Securing end user private keys: Does IEEE prefer a standard solution to implement cryptographic hardware protection of end user keys?**

   Any standard method of securing the root and SPV keys is acceptable as long as it exceeds the average expected requirements for the industry. For the end user keys, no hardware protection is planned. Occasional compromises are expected (e.g. due to malware and attackers having remote access to the user key) and that is what black-listing (CRL) of user certificates will be handling.

3. **About how many SPVs and end users does IEEE expect to participate in service?**

   We can expect up to 100 SPVs with on average at most 10,000 users each.

4. **Is it expected that a single Timestamping Authority for all SPV end user certificates will be utilized?**

   Yes.

5. **Does IEEE have any estimates on the amount of Online Certificate Status Protocol (OCSP) requests that will be sent to the PKI service by all relying parties?**

   This is an operation that happens only on the security vendor's backend. It is not something that each end user performs. That would limit the number of requestors at any point in time to approximately 100. Each security vendor's polling would be done periodically, at most every minute.

6. **Will the SPVs act as an approver for certificate requests coming from users?**

Yes. IEEE approves SPVs (registered, established vendors with some history and traceability). SPVs approve their users once payments or other arrangements are made for the use of their software (i.e. only registered customers).

7. **IEEE would provide the PKI service with a list of approved SPVs. Does this list contain some form of credential (e.g. OTP) that can be used during enrollment of the SPV certificate?**

   This concerns the method of delivering updates (SPV list or updates to it) to the CA. Yes, once a new SPV is approved they will be provided interface login credentials to log into the CA. These will be communicated from IEEE manually to both the approved SPV and the CA.

8. **Would it be appropriate for SPVs to manually approve certificate requests by Users? Or would it be a requirement to have the issuance of User certificates completely automated, perhaps through an API?**

   SPVs may wish to make use of a user-friendly HTTPS page or communicate via some more automation-friendly method (e.g. SOAP). Support for both would be preferable.

9. **What SLAs (uptime and performance) does IEEE expect of each PKI service component (CA, RA, OCSP, CRL distribution, Time Stamping)?**

   Above industry average.

10. **Does the PKI need to use a major security vendor's product (Microsoft, Entrust, etc)? Would you be open to a custom-built CA using open-source tools (e.g., openssl + database + scripts + API + web interface)?**

    The main requirements are: Security - All components of the system must be protected from attack; and Availability - The system must operate with little to no downtime. Any solution that meets these requirements will be acceptable.