

VIRGINIA TECH PKI POLICY MANAGEMENT AUTHORITY

Scope of PMA

The primary purpose of the Virginia Tech Public Key Infrastructure Policy Management Authority (VTPKI-PMA) is to approve policies/standards of the Virginia Tech Public Key Infrastructure (PKI) and the related Certificate Authority (CA) operating within it. The PMA should be the point of contact for subscribers in its PKI as well as relying parties and other external entities, i.e. other PKI-PMA's, new subscribers, etc. Relying parties in particular need a forum to raise issues such as application, certificate usages, certificate roles, and security concerns.

Membership

The initial membership of the PMA shall be comprised of 6-10 senior managers within the Information Technology organization and 1-2 senior managers external to the IT organization. The chairman of the PMA will be designated by the VP for Information Technology. New members or expansion of the PMA shall be approved by existing members through a voting process.

The initial membership is:

Randy Pelt Chairman
Mary Dunker
Mike Naff
Randy Marchany
Pat Rodgers
Susan Brooker-Gross
James Powell
Alan Moeller
Phil Benchoff
Bill Plymale
Tommy Regan

Responsibilities

The PMA is responsible for approving all policies, procedures and other operating documents (and subsequent revisions) of the Virginia Tech CA and PKI. The PKI may make changes and the following areas may require adjustment in policies and procedures in the near future:

- Certificate validation infrastructure
- Authority information extensions

VIRGINIA TECH PKI POLICY MANAGEMENT AUTHORITY

- Key sizes
- Special purpose servers and web services
- Certificate profiles and extensions
- Key generation/storage

The PMA is a policy management authority, not an operations unit. It does not manage day-to-day activities of the CA. However, the PMA is responsible for ensuring that the CA and PKI are operated in accordance with their governing documents. The PMA is encouraged to provide recommendations for improved operating procedures and any needed technical assistance.

Activities

The PMA should meet initially to approve the PMA charter/by-laws and meet periodically when approval for amendments are needed for CA and PKI governing documents, or to resolve questions/complaints made by users. When possible, questions, amendments submission, and other items under consideration should be submitted to members of the PMA prior to meetings to allow a review period. Agendas should be posted by the chairman in advance of these meetings.

The PMA should create a web site and/or other public forms as needed to provide point of contact information. Users should have the ability to contact the PMA for questions, concerns, or to bring forth complaints pertaining to the operation of the CA and PKI. The PMA should address these issues and ensure that any problem areas are addressed and proper resolution is made.

The PMA should ensure that an annual audit is performed of the VT PKI by an independent party...i.e. Internal Audit, Auditor of Public Accounts, etc.