Multi-factor Authentication for Higher Education

The "Higher Education MFA website"

During the course of the MFA Cohortium activities, a process for "promotion/release" of various documents and project artifacts to a public MFA web site will be established and followed. By the time the formal lifetime of the Cohortium ends, the intent is that this "Higher Education MFA website" will contain answers, samples and examples for all of the following questions and artifact categories:

- What use cases drove the decision to adopt MFA for authentication?
- What are the costs, both one-time and ongoing?
- What cost/benefit/risk analysis was done to justify the use of MFA for those use cases?
- Risk assessment – what functions/activities do various institutions believe require MFA?
- What MFA technologies/approaches mesh most easily with which Single-Signon frameworks and/or services and applications?
- Which MFA technologies are being deployed and used by institutions for which applications/environments/use cases?
- The same question, but the other side of it – which combinations have caused difficulties, and if those were overcome, how and at what cost?
- Were any new roles (or modification of current roles) determined to be needed?
- What special training is required? What audiences did/are you training, and how often?
- Samples/examples of any and all of the following kinds of documents and artifacts related to MFA:
    - use cases
    - requirements
    - RFP/specifications document
    - risk/cost analysis
    - cost analysis for full lifecycle of support of MFA, including any comparison analysis of various MFA technologies
    - technology choice(s), system architecture
    - project charter, project plan, Work Breakdown Structure
    - policy & procedure for
        - token request (or registration) process
        - replacing tokens
        - recovery of tokens when no longer needed
        - roles & process document
        - support process document
    - documentation of roles
    - user documentation
    - training materials
    - support materials – FAQs, KnowledgeBase articles, web pages, etc.
    - public awareness efforts, press releases, campaigns, advertising
    - Costs
        - Initial costs to implement (with whatever breakdown is available)
        - Ongoing licensing/maintenance costs
        - Ongoing user support costs
        - Service Level Agreement(s)
        - Other costs?
- What are the most frequent questions/problems encountered? And how were/are they solved?
- What are the approaches to the distribution/delivery of token/extra factor devices?
- Where/when in the on boarding/IdM workflow does MFA device registration/issuance occur?
- What are the best practices for supporting the users and the MFA deployment and operation?
- Are you happy with your MFA choice(s)? If you had it do to over again, would you use the same technology? If not, why not?
- What do you know now that you wish you knew before you started?
- What did you worry about that turned out not to actually be a problem/concern?
- Business policies, procedures, processes that support request, initial deployment, maintenance, infrastructure, and replacement of the tokens
    - what happens when a token breaks?
    - what happens when I forget it at home?
    - what about replacing lost tokens?
- How long did training take?
- Which units/roles did you have involved in your MFA deployment project, and at what points in the project timeline? How about for ongoing operations and support?
- What was your timeline – how long from "start to finish" (project initiation to pilot/production operational status)?
- What did you underestimate? What did you overestimate? What did you forget to estimate at all?