Outline

• Review TWG Mission Statement
• Provide project updates
• Suggest potential new work areas
TWG Mission Statement

To provide a vendor neutral environment where PKI vendors and users can advance PKI technology and multi-vendor interoperability. The TWG will develop white papers, implementation guidelines, multi-vendor product interoperability demonstrations, and collaborate with industry- and government-led initiatives.
Project Status Matrices

- Project status matrices available on-line (see TWG home home page)
- Project information divided into four categories:
  - Active
  - Completed
  - On Hold
  - Proposed
- Can be used as a tool to find:
  - Project leader’s name
  - High-level purpose of the project
  - Pointer to project plan or final deliverable
AKID/SKID Implementation Guideline

Purpose:
- To document a PKI Forum endorsed solution that will prevent mismatches between the AKID/SKID populated in self-signed certificates and the SKID populated in cross-certificates

Project Leader:
- Steve Lloyd (PKI Forum)

Status:
- Completed

Deliverable:
- Implementation Guideline (see http://www.pkiforum.org/resources.html)
Certification Path Construction

• Purpose:
  – To document issues and recommendations associated with building certification paths

• Project Leader:
  – Steve Lloyd (PKI Forum)

• Status:
  – Completed
  – Paper was presented during the RSA Security Conference Conference in Paris: October 2002

• Deliverable:
  – White Paper (see http://www.pkiforum.org/resources.html)
CA and User Certificate Profiles

• Purpose:
  – To provide CA and user certificate implementation guidance based on lessons learned from the CESG-sponsored interoperability initiatives

• Project Leaders:
  – Richard Lampard/Andrew Watson (CESG), S. Lloyd (PKIF)

• Status:
  – Original drafts submitted to PKI Forum by CESG on 30 May 2001
  – Drafts updated by S. Lloyd and submitted to TWG for review on 29 October 2002

• Deliverable:
  – Implementation Guidelines
CA Certificate Profile
User Certificate Profile
PKI Enablement Questionnaire

• Purpose:
  – To document a list of questions that potential customers can use to help evaluate PKI vendor products.

• Project Leader:
  – Rich Guida (Johnson & Johnson)

• Status:
  – Final draft submitted for final review 18 September 2002
  – Next step is to submit for board approval

• Deliverable:
  – PKI Enablement Questionnaire
Draft Questionnaire
Additional Projects

- Token Interoperability and Portability - Andrew Nash Nash (RSA Security)
- PKI Application Library - Anthony Starks (Merck)
- XKMS Interoperability - Ulrich Brell (Baltimore)
- Others…
Potential New Work Items?

- Certification Path *Validation* White Paper?
- Canadian Treasury Board Interoperability Proposal?
- PKI/SAML Integration/Interoperability?
- CRL Profile?
Questions?