Updating ASN.1 modules for PKIX and CMS

Paul Hoffman, VPN Consortium

Jim Schaad, Soaring Hawk Consulting

Why do this?

- Current modules are based on ASN.1 of 1988
- However, ASN.1 1998 and 2002 do not allow “ANY”, which appears in many of the modules
- Newer ASN.1 has features that allow compilers to do automatic checking
- No bits-on-the-wire changes at all

What is changing?

- All ANYs are replaced with new objects
- New objects are being created to allow automated constraint checking
  - Algorithm structures
  - Binding OIDs to the structures that call them
- Where useful, new parameterization
  - For example, bounds checking in DirectoryString
- No bits-on-the-wire changes at all

Where is this being done?

- draft-hoffman-cms-new-asn1
- draft-hoffman-pkix-new-asn1
- The drafts cross-reference each other, and so do many of the modules
- No need to make these WG items (both WGs need to die sometime...), but we want as much review as we can get

What is the status?

- We got some good corrections on the -00
- -01 will include many more modules from more standards-track RFCs and RFCs-to-be
- Modules will have more objects added
- No bits-on-the-wire changes at all

Do you have questions?

- Do we have answers?