PKCS #9 Amendment for PTDs

PKCS Workshop 2002

Magnus

Motivation

- Currently, there's:
  - No way to indicate suggested MIME type (if not given MIME message)
  - No way to indicate device's display/presentation capabilities
- So, an attacker could:
  - Disguise a message using a bogus Content-Type and/or character set
  - Take advantage of a particular device's deficiencies

Proposal

- PKCS #9 attributes for PTD to be included in the signed message
  - Alleged Content-Type
  - Presentation Capabilities
- Syntax & Value set:
  - Alleged Content-Type
    - UTF8String, value provided in CKM_CMS_SIG mechanism parameters
  - Presentation Capabilities
    - CC/PP, UAProf, something else? Or just make & model?

Problems

- Especially for the presentation capabilities
  - Change of display
  - Use of external speakers
  - Abuse of owner
- Workaround
  - Just an open format string?