Don’t Hate Your Users:

Best practices for applications using X.509 certificates.

David Woodhouse <dwmw2@infradead.org>
2023-07-26
Problem: Using keys securely is too hard

- Secure storage methods are often unsupported
- Configuration is baroque and inconsistent

Result:

- Users are less secure than they should be.
Key storage is complex

- System certificate stores
- PKCS#11 tokens
- Trusted Platform Module
- Files
  - PKCS#1 (and variants)
  - PKCS#8
  - PKCS#12
Passphrase handling is awful

• Character sets:
  − Unspecified charset for PKCS#8
  − Broken conversions even for PKCS#12

• Random availability of encryption algorithms
“How do I use the key in my USB token?”

“It depends…”

- Which application are you using?
- Which crypto library is it built against?
- Do you know the right incantation to identify which token to use and which certificate/key therein?
- Is your PKCS#11 provider installed correctly?
“How do I secure a key with my TPM?”

“It depends…”

- Which application are you using?
- Which crypto library is it built against?
- Does your application let you manually specify an OpenSSL “engine” or “provider”? 
“Can I use my OS’s secure cert store?”

“Maybe…”

- Which application are you using?
- Which crypto library is it built against?
- Do you know the right incantation for that?
“OK, I give up. Can I just use a file?”

“Well…”

- Which application are you using?
- Which crypto library is it built against?
- What kind of file is it? PEM or DER?
- What character set are you using locally?
Applications should make it easy!

- Support all reasonable file types, all sane PBES
- Recognise TPM wrapped files automatically
- Recognise RFC7512 PKCS#11 URIs automatically, find certs + keys consistently
- Support system certificate stores through uniform syntax
What can we do about it?

- Clearly set out expectations for user experience
- Encourage applications to improve
- Encourage crypto libraries to make it hard for applications to get it *wrong*
References / Thanks

- https://www.infradead.org/openconnect/
- https://www.hansenpartnership.com/draft-bottomley-tpm2-keys.html

Thanks to Nikos Mavrogiannopoulos for his support over the years on everything I didn’t understand about crypto, and James Bottomley for all things TPM.
References / Credits


- https://www.hansenpartnership.com/draft-bottomley-tpm2-keys.html