GitHub - gentilkiwi/kekeo: A little toolbox to play with Microsoft Kerberos in C

By gentilkiwi

Archived: 2026-04-05 23:36:03 UTC

`kekeo` is a little toolbox I have started to manipulate Microsoft Kerberos in C (and for fun)

ASN.1 library

In `kekeo`, I use an external commercial library to deal with Kerberos ASN.1 structures: **OSS ASN.1/C** (http://www.oss.com/asn1/products/asn1-c/asn1-c.html)
It was the **only** code generator/library that I've found to work easily with Microsoft C project.

- works without a lots of dependencies;
- magical documentation;
- wonderful support for my stupid questions;
- had a binary that work only few hours after started my project...

They were kind enough to offer me a 1-year licence.
With this one, I'm able to let you download binaries that run in your environment.
So don't forget to thank them (http://www.oss.com/company/contact-us.html / https://twitter.com/OSSNokalva)

Limitations

- Binaries will work until December 21, 2017 (yeah, 1 year licence ;));
- You must buy a licence from **OSS ASN.1/C** (*or download a trial version*) to build `kekeo` solution/adapt it.
  - http://www.oss.com/asn1/products/asn1-c/asn1-c.html
  - When you register for a free trial, don't forget to refer me in the description field ;) (`kekeo` or `gentilkiwi`)

Building `kekeo` with ASN.1/C

You **can't** build `kekeo` out-of-the-box, you'have to generate C files and link with OSS libraries.

After downloading and installing a commercial/trial version of **OSS ASN.1/C**, `Win32` and/or `x64` :

1. Open a command prompt in `($kekeo)\modules\asn1`
2. Adapt the `ASN1C` variable to your ASN.1/C configuration (architecture & version)

```
set ASN1C="C:\Program Files\OSS Nokalva\ossasn1\winx64\10.4.0"
```

3. Depending on the targeted lib architecture:

   - `Win32`

     ```
     %ASN1C%\bin\asn1.exe ^
      %ASN1C%\asn1dflt\asn1dflt.ms.zp4 ^
      KerberosV5Spec2.asn KerberosV5-PK-INIT-SPEC.asn PKIX1Explicit88.asn PKINIT.asn MS-SFU-KILE.asn ^
      -noSampleCode -der -root -CStyleComments -externalName kekeo_asn1 -messageFormat msvc -verbose ^
      -headerFile kull_m_kerberos_oss_asn1_internal.h -soedFile kull_m_kerberos_oss_asn1_internal_Win
     ```

   - `x64`

     ```
     %ASN1C%\bin\asn1.exe ^
      %ASN1C%\asn1dflt\asn1dflt.msx64.zp8 ^
      KerberosV5Spec2.asn KerberosV5-PK-INIT-SPEC.asn PKIX1Explicit88.asn PKINIT.asn MS-SFU-KILE.asn ^
      -noSampleCode -der -root -CStyleComments -externalName kekeo_asn1 -messageFormat msvc -verbose ^
      -headerFile kull_m_kerberos_oss_asn1_internal.h -soedFile kull_m_kerberos_oss_asn1_internal_x64
     ```

   Header file `kull_m_kerberos_oss_asn1_internal.h` is the same for both architecture.

4. Copy from **OSS ASN.1/C** install dir (eg: `C:\Program Files\OSS Nokalva\ossasn1\winx64\10.4.0`)

   - `include\ossasn1.h` to `($kekeo)\inc`
   - `include\osstype.h` to `($kekeo)\inc`
   - `lib\soeddefa.lib` to `($kekeo)\lib\{Win32 or x64}`
   - `lib\ossiphlp.lib` to `($kekeo)\lib\{Win32 or x64}`

You can now build the `kekeo` solution in **Visual Studio**

Licence

CC BY-NC-SA 4.0 licence - https://creativecommons.org/licenses/by-nc-sa/4.0/

Acknowledgements

- Tom Maddock - Qualcomm - @ubernerdom - MS14-068 - https://www.qualcomm.com/
- Sylvain Monné - Solucom - @BiDOrD - Author of `PyKek` - https://github.com/bidord/pykek
- Tal Be'ery - Aorato / Microsoft - @TalBeerySec - http://www.aorato.com/blog/active-directory-vulnerability-disclosure-weak-encryption-enables-attacker-change-victims-password-without-logged/
- Grace Sigona - OSS - @OSSNokalva - http://www.oss.com/
- Taylor Swift - @SwiftOnSecurity - https://twitter.com/SwiftOnSecurity/status/767788634904735745
- Seth Moore - Microsoft - @robododo - https://datatracker.ietf.org/doc/draft-ietf-kitten-pkinit-freshness/

- Alberto Solino - Core Security / Impacket - @agsolino - https://github.com/CoreSecurity/impacket
- Laurent Gaffié - @PythonResponder / @lgandx - https://github.com/lgandx/Responder / https://g-laurent.blogspot.com/

Author

Benjamin DELPY `gentilkiwi`, you can contact me on Twitter (@gentilkiwi) or by mail (benjamin [at] gentilkiwi.com)

This is a **personal** development, please respect its philosophy and don't use it for bad things!
