z/OS 2.4 IBM Education Assistant (IEA)

Solution (Epic) Name: PKCS#7 Signed Data Detach Signature Creation Support

Element(s)/Component(s): System SSL

IBM LinuxONE™

Agenda

- Trademarks
- Session Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Installation
- Session Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.

Session Objectives

- At the end of this presentation, you should have an understanding of the System SSL – PKCS #7 Signed Data Detach Signature creation support
- A PKCS#7 detached signature means the customer data, for example a PDF, is used to create the signature and hash data but is not saved inside the final message.

Overview

- Who (Audience)
  - Need the ability to create a PKCS#7 Signed data message with a detached signature so that both the data and signature do not need to be together.
- What (Solution)
  - Update the gsk_make_signed_data_content_extended() and gsk_make_signed_data_msg_extended() routines to accept a new option flag (create_detached_signature) to indicate the created PKCS #7 Signed Data message is to be of type detached signature.
  - APAR OA54821 – V2R1, V2R2 and V2R3. Base of V2R4
- Wow (Benefit / Value, Need Addressed)
  - A much smaller PKCS#7 signed data message is created.
  - PKCS#7 signed data message can be provided along with the original data

Usage & Invocation

- Modified System SSL routines:
  - gsk_make_signed_data_msg_extended (
    gsk_process_option *option_flag*, **int** *version*,
    x509_algorithm_type *digest_algorithm*, **gsk_boolean** *include_certificates*,
    pkcs_cert_keys * *signer_certificates*, **pkcs_certificates *** *ca_certificates*,
    gsk_buffer * *data*, **gsk_attributes_signers *** *attributes_signers*,
    gsk_buffer * *stream*)
  - gsk_make_signed_data_content_extended (
    gsk_process_option *option_flag*, **int** *version*,
    x509_algorithm_type *digest_algorithm*, **gsk_boolean** *include_certificates*,
    pkcs_cert_keys * *signer_certificates*, **pkcs_certificates *** *ca_certificates*,
    pkcs_content_info * *content_data*, **gsk_attributes_signers *** *attributes_signers*,
    pkcs_content_info * *content_info*)
- System SSL header file gskcms.h has been updated with the addition of a new create_detached_signature flag in gsk_process_option

```
typedef struct _gsk_process_option       {
    unsigned int  enforce_keyusage : 1;         /* enforce key usage          */
    unsigned int  enforce_content_length : 1;   /* enforce non-zero content   */
    unsigned int  enforce_keyparity : 1;        /* enforce key odd parity     */
    unsigned int  create_detached_signature : 1;  /* create detached signature*/
} gsk_process_option;
```

Usage & Invocation

- *option_flag*
  - Specifies process options to customize process behavior.
  - Enforce signing certificate has digital signing capabilities. That is, the purpose of the certificate key as reflected by the key usage extension must indicate digitalSignature.
  - Do not allow zero-length content data
  - Create detached (external) signature content data. The passed in data is included in the data being digitally signed, but is not included in the returned SignedData content. This flag is only supported when version 500, 501, 502 or 503 is specified. It is ignored when version 0, 1, 2 or 3 is specified.

Usage & Invocation

- *version* – new values
  - Specify 500 to create SignedData content as described in PKCS #7 Version 1.4 This version encodes the *IssuerAndSerialNumber* as the *signerIdentifier*.
  - Specify 501 to create SignedData content as described in PKCS #7 Version 1.5. This version encodes the *IssuerAndSerialNumber* as the *signerIdentifier*.
  - Specify 502 to create SignedData content as described in PKCS #7 Version 1.6. This version encodes the *IssuerAndSerialNumber* as the *signerIdentifier*.
  - Specify 503 to create Signed Data content as described in PKCS #7 RFC 3852. This version encodes the *SubjectKeyIdentifier* as the *signerIdentifier*.

Interactions & Dependencies

- To exploit this item, all systems in the Plex must be at the new z/OS level: No

- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - z/OS Print

Installation

- APAR OA54821
  - V2R2 PTFs: UA96100 and UA96101
  - V2R3 PTFs: UA96089 and UA96092

Session Summary

- You should now be able to:
  - Understand the updates made to System SSL routines gsk_make_signed_data_content_extended() and gsk_make_signed_data_msg_extended() to allow one to create a PKCS#7 Detached Signature

Appendix

- z/OS Cryptographic Services System Secure Sockets Layer Programming
- RFC 3852