z/OS V2.5 IBM Education Assistant

Solution Name: PBKDF2 (Password-Based Key Derivation Function 2)

Solution Element(s): ICSF

Agenda

- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

Objectives

- Discuss new function enhancements and benefits.

Overview

- Who (Audience)
  - Potential exploiters of PBKDF2 (standard key derivation function)
    - PKCS #5 v2.0 (also published as IETF RFC 2898) defines PBKDF2. RFC 8018 (PKCS #5 v2.1) continues to recommend it.
- What (Solution)
  - Ability to derive key material from a password (really a passphrase) using PBKDF2.
- Wow (Benefit / Value, Need Addressed)
  - PBKDF2 is an industry-wide capability that should be supported in a cryptographic provider on z/OS (ICSF is ideal).

Usage & Invocation

- PKCS #11 function C_GenerateKey and the underlying ICSF service PKCS #11 Generate secret key (CSFPGSK and CSFPGSK6) are enhanced to receive the PBKDF2 structure to derive key material.
  - For C_GenerateKey, the structure is CK_PKCS5_PBKD2_PARAMS2 and is used with the mechanism CKM_PKCS5_PBKD2.

```
typedef struct CK_PKCS5_PBKD2_PARAMS2 {
        CK_PKCS5_PBKDF2_SALT_SOURCE_TYPE saltSource;
        CK_VOID_PTR pSaltSourceData;
        CK_ULONG ulSaltSourceDataLen;
        CK_ULONG iterations;
        CK_PKCS5_PBKD2_PSEUDO_RANDOM_FUNCTION_TYPE prf;
        CK_VOID_PTR pPrfData;
        CK_ULONG ulPrfDataLen;
        CK_UTF8CHAR_PTR pPassword;
        CK_ULONG ulPasswordLen;
} CK_PKCS5_PBKD2_PARAMS2;
```

  - As always for PKCS #11 implementations, C_GetMechanismList and C_GetMechanismInfo are updated to reflect that CKM_PKCS5_PBKD2 is available.

Usage & Invocation

- PKCS #11 function C_GenerateKey and the underlying ICSF service PKCS #11 Generate secret key (CSFPGSK and CSFPGSK6) are enhanced to receive the PBKDF2 structure to derive key material.
  - For CSFPGSK, we use a flattened version of the PKCS #11 structure CK_PKCS5_PBKD2_PARAMS2 with a rule of PBKDF2.

Table xxx. parms_list parameter format for PBKDF2 mechanism

Offset	Length in bytes	Direction	Description
0	4	input	source of the salt value; currently, this must be X'00000001' (CKZ_SALT_SPECIFIED)
4	4	input	number of iterations to perform when generating each block of random data (n), where 1 <= n <= 65,536
8	4	input	pseudo-random function to use to generate the key (PRF); supported values are: X'00000001' (CKP_PKCS5_PBKD2_HMAC_SHA1) X'00000003' (CKP_PKCS5_PBKD2_HMAC_SHA224) X'00000004' (CKP_PKCS5_PBKD2_HMAC_SHA256) X'00000005' (CKP_PKCS5_PBKD2_HMAC_SHA384) X'00000006' (CKP_PKCS5_PBKD2_HMAC_SHA512) X'00000007' (CKP_PKCS5_PBKD2_HMAC_SHA512_224) X'00000008' (CKP_PKCS5_PBKD2_HMAC_SHA512_256)
12	2	input	length of the salt source input, in bytes (s), where 1 <= s <= 128
14	2	input	length of the input data for the PRF, in bytes (d); currently, d must be 0
16	2	input	length of the password, in bytes (p), where 1 <= p <= 128
18	s	input	salt data
18+s	d	input	PRF data (empty since d must be 0)
18+s+d	p	input	password

Interactions & Dependencies

- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - IBM HTTP Server (IHS)

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Sysplex must be at the new z/OS level: No
- No upgrade actions associated.

Installation & Configuration

- No changes to installation or configuration are required.

Summary

- PKCS #11 mechanism CKM_PKCS5_PBKD2 is now available for C_GenerateKey
- ICSF service CSFPGSK is updated to support PBKDF2. This service is what C_GenerateKey calls to do the actual key derivation.

Appendix

- Publications updated
  - Cryptographic Services Integrated Cryptographic Service Facility Application Programmer's Guide
  - Cryptographic Services Integrated Cryptographic Service Facility Writing PKCS #11 Applications