# z/OS V2.5 IBM Education Assistant

Solution Name:  ICSF RSA-PSS Performance enhancements

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 enchantments
  - Performance benefits
  - Usage

# Overview

- Who (Audience)
  - Users of PKCS#11 PSS functions using clear RSA keys
- What (Solution)
  - ICSF will offload Clear PKCS#11 RSA-PSS requests to an accelerator or CCA coprocessor if present
- Wow (Benefit / Value, Need Addressed)
  - Significant performance improvement over doing the equivalent function in software.

# Usage & Invocation

PKCS#11 RSA-PSS function driven through CSFPOWH callable service

## CSFPOWH rexx Sign example

```
OWH_Handle = Priv_Handle (Clear RSA Private key object)
OWH_Rule_Array = 'SHA-256 SIGN-PSS';
OWH_Rule_Count = '00000002'x;
OWH_Text = copies('FF'x,128);
OWH_Text_Length = D2C(Length(OWH_Text),44)
OWH_Chain_Length  = '00000080'x ;
OWH_Chain_Data = copies('00'x,c2d(OWH_Chain_Length));
OWH_Chain_Data = CKM_SHA256 || CKG_MGF1_SHA256 ||
'00000020'x
OWH_Hash_Length  = '00000D26’x
OWH_Hash = copies('00'x,c2d(OWH_Hash_Length));
```

## CSFPOWH rexx Verify example

```
OWH_Handle = Pub_Handle (Clear RSA Public key object)
OWH_Rule_Array = 'SHA-256 VER-PSS';
OWH_Rule_Count = '00000002'x;
OWH_Text = copies('FF'x,128);
OWH_Text_Length = D2C(Length(OWH_Text),44)
OWH_Chain_Length  = '00000080'x ;
OWH_Chain_Data =
copies('00'x,c2d(OWH_Chain_Length));
OWH_Chain_Data = CKM_SHA256 || CKG_MGF1_SHA256
|| '00000020'x
OWH_Hash_Length  = '00000D26’x
OWH_Hash = copies('00'x,c2d(OWH_Hash_Length));
```

# Interactions & Dependencies

- Software Dependencies
  - V2R5 ( ICSF HCR77D2)
- Hardware Dependencies
  - CCA RSA-PSS support requires CCA 5.3 or later
- Exploiters
  - System SSL

# Upgrade & Coexistence Considerations

- N/A

# Installation & Configuration

- N/A

# Summary

- No changes needed to CSFPOWH API to utilize HW offload for accelerators or CCA coprocs.
- ICSF will send request to accelerator first if available.
- If no accelerator present, ICSF will try the CCA coprocessor.
- If neither is available, request will be done in SW as done today.

# Appendix

- PSS - Probabilistic signature scheme