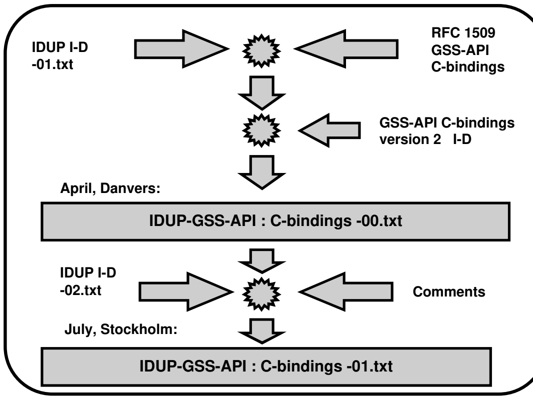
Independent Data Unit Protection GSS API : C-bindings

– draft-ietf-cat-idup-cbind-01.txt –

D. Grebovich
Bell-Northern Research

July 19, 1995
33rd Internet Engineering Task Force
Stockholm, Sweden



I-D Contents

- Introduction
- IDUP-GSS-API routines
- IDUP-GSS-API routine descriptions
- Example

Introduction

- 4 STAGES:
  - –acquiring a set of credentials
  - –establishing a security environment
  - –per-data-unit services:
    - » integrity
    - » data origin authentication
    - » confidentiality
  - –completion of a security environment

IDUP-GSS-API Calls

- CREDENTIAL MANAGEMENT
- ENVIRONMENT-LEVEL
- PER-IDU
- SUPPORT

IDUP-GSS Status Codes

MSB LSB

Calling Error	Routine Error	Supplementary Info

Bit 31 24 23 16 15 Bit 0

Calling Errors (identical to gss_api)

Routine Errors (identical to gss_api, some are not applicable) +

IDUP_S_BAD_TARG_INFO	(15)	IDUP_S_BAD_AI_KEY	(21)
IDUP_S_BAD_DIGEST_ALG	(16)	IDUP_S_BAD_KE_KEY	(22)
IDUP_S_BAD_CONF_ALG	(17)	IDUP_S_DEFECTIVE_CHECK	(23)
IDUP_S_BAD_ENC_IDU	(18)	IDUP_S_NO_MATCH	(24)
IDUP_S_NO_ENV	(19)	IDUP_S_EVIDENCE_UNAVAIL	(25)
IDUP_S_UNKNOWN_OPER_ID	(20)		

Supplementary Status Bits (identical to gss_api, some are not applicable) +

IDUP_S_RECEIPTS_UNAVAIL (6)

CREDENTIAL MANAGEMENT CALLS

- GSS_Acquire_cred()
- GSS_Release_cred()
- GSS_Inquire_cred()

IDENTICAL TO GSS-API

NO CHANGES

ENVIRONMENT-LEVEL CALLS

- IDUP_Establish_env()
- IDUP_Abolish_env()
- IDUP_Inquire_env()

NO CHANGES

PER-IDU CALLS

Calls		Set
IDUP_Start_Protection IDUP_Protect IDUP_End_protect		PROTECTION SET
IDUP_Start_Unprotect IDUP_Unprotect IDUP_End_Unprotect		UNPROTECTION SET
IDUP_Start_Generate_Receipt IDUP_Generate_Receipt IDUP_End_Generate_Receipt IDUP_Process_Receipt	*NEW *NEW *NEW	RECEIPT SET
IDUP_Generate_Evidence IDUP_Process_Evidence	*NEW *NEW	EVIDENCE SET (for non-repudiation)

SUPPORT CALLS

- GSS_Display
- GSS_Indicate_mechs
- GSS_Compare_name
- GSS_Display_name
- GSS_Import_name
- GSS_Release_name
- GSS_Release_buffer
- GSS_Release_oid_set

IDENTICAL TO GSS-API

NO CHANGES

- IDUP_Parse_token

TARGETS

- STANDARDS TRACK
- DATES