A brief summary of the various versions of the Security Descriptor Definition Language (SDDL)

devblogs.microsoft.com/oldnewthing/20220510-00

May 10, 2022

Raymond Chen

The Security Descriptor Definition Language (SDDL) was introduced in Windows 2000 to provide a textual representation for security descriptors. Prior to its introduction, security descriptors were typically represented as hex bytes, which was not particularly readable or editable.

Although the only defined revision number is 1, there have actually been quite a few revisions to the Security Descriptor Definition Language, which makes you wonder what that version number was for. The fact that the version number hasn't changed when the language changed means that if you call `ConvertSecurityDescriptorToStringSecurity-Descriptor`, you will get a string security descriptor that works on the version of Windows that generated it, but it may not work on older versions of Windows, because the older versions may not support some of the newer features.

Oops.

Okay, so here's a history of the Security Descriptor Definition Language, in table form.

SDDL Component Tags

Code	Meaning Symbol	Introduced

O	Owner
	`SDDL_OWNER`
	`OWNER_SECURITY_INFORMATION`
		Windows 2000

G	Group
	`SDDL_GROUP`
	`GROUP_SECURITY_INFORMATION`	

D	DACL
	`SDDL_DACL`
	`DACL_SECURITY_INFORMATION`	

S	SACL
	`SDDL_SACL`
	`SACL_SECURITY_INFORMATION`	

SDDL Security Descriptor Controls

Code	Meaning	Introduced

P	Protected
	`SDDL_PROTECTED`
	`SE_DACL_PROTECTED`
	`SE_SACL_PROTECTED`
		Windows 2000

AR	Auto inherit request
	`SDDL_AUTO_INHERIT_REQ`
	`SE_DACL_AUTO_INHERIT_REQ`
	`SE_SACL_AUTO_INHERIT_REQ`	

AI	Auto inherited
	`SDDL_AUTO_INHERITED`
	`SE_DACL_AUTO_INHERITED`
	`SE_SACL_AUTO_INHERITED`	

NO_ACCESS_CONTROL	Null ACL `SDDL_NULL_ACL`	Windows 7

SDDL ACE Types

Code	Meaning	Introduced

A	Access allowed
	`SDDL_ACCESS_ALLOWED`
	`ACCESS_ALLOWED_ACE_TYPE`
		Windows 2000

D	Access denied
	`SDDL_ACCESS_DENIED`
	`ACCESS_DENIED_ACE_TYPE`	

OA	Object access allowed
	`SDDL_OBJECT_ACCESS_ALLOWED`
	`ACCESS_ALLOWED_OBJECT_ACE_TYPE`	

OD	Object access denied
	`SDDL_OBJECT_ACCESS_DENIED`
	`ACCESS_DENIED_OBJECT_ACE_TYPE`	

AU	Audit
	`SDDL_AUDIT`
	`SYSTEM_AUDIT_ACE_TYPE`	

AL	Alarm
	`SDDL_ALARM`
	`SYSTEM_ALARM_ACE_TYPE`	

OU	Object audit
	`SDDL_OBJECT_AUDIT`
	`SYSTEM_AUDIT_OBJECT_ACE_TYPE`	

OL	Object alarm
	`SDDL_OBJECT_ALARM`
	`SYSTEM_ALARM_OBJECT_ACE_TYPE`	

ML	Integrity label
	`SDDL_MANDATORY_LABEL`
	`SYSTEM_MANDATORY_LABEL_ACE_TYPE`
		Windows Vista

XA	Callback access allowed
	`SDDL_CALLBACK_ACCESS_ALLOWED`
	`ACCESS_ALLOWED_CALLBACK_ACE_TYPE`
		Windows 7

XD	Callback access denied
	`SDDL_CALLBACK_ACCESS_DENIED`
	`ACCESS_DENIED_CALLBACK_ACE_TYPE`	

RA	Resource attribute
	`SDDL_RESOURCE_ATTRIBUTE`
	`SYSTEM_RESOURCE_ATTRIBUTE_ACE_TYPE`
		Windows 8

SP	Scoped policy
	`SDDL_SCOPED_POLICY_ID`
	`SYSTEM_SCOPED_POLICY_ID_ACE_TYPE`	

XU	Callback audit
	`SDDL_CALLBACK_AUDIT`
	`SYSTEM_AUDIT_CALLBACK_ACE_TYPE`	

ZA	Callback object access allowed
	`SDDL_CALLBACK_OBJECT_ACCESS_ALLOWED`
	`ACCESS_ALLOWED_CALLBACK_OBJECT_ACE_TYPE`	

TL	Process trust label
	`SDDL_PROCESS_TRUST_LABEL`
	`SYSTEM_PROCESS_TRUST_LABEL_ACE_TYPE`
		Windows 8.1

FL	Access filter
	`SDDL_ACCESS_FILTER`
	`SYSTEM_ACCESS_FILTER_ACE_TYPE`
		Windows 10 Version 1703

SDDL Resource attribute ACE data types

Code	Meaning	Introduced

TI	Signed integer
	`SDDL_INT`
	`CLAIM_SECURITY_ATTRIBUTE_TYPE_INT64`
		Windows 8

TU	Unsigned integer
	`SDDL_UINT`
	`CLAIM_SECURITY_ATTRIBUTE_TYPE_UINT64`	

TS	Wide string
	`SDDL_WSTRING`
	`CLAIM_SECURITY_ATTRIBUTE_TYPE_STRING`	

TD	SID
	`SDDL_SID`
	`CLAIM_SECURITY_ATTRIBUTE_TYPE_SID`	

TX	Octet string
	`SDDL_BLOB`
	`CLAIM_SECURITY_ATTRIBUTE_TYPE_OCTET_STRING`	

TB	Boolean
	`SDDL_BOOLEAN`
	`CLAIM_SECURITY_ATTRIBUTE_TYPE_BOOLEAN`	

SDDL ACE flags

Code	Meaning	Introduced

CI	Container inherit
	`SDDL_CONTAINER_INHERIT`
	`CONTAINER_INHERIT_ACE`
		Windows 2000

OI	Object inherit
	`SDDL_OBJECT_INHERIT`
	`OBJECT_INHERIT_ACE`	

NP	Inherit no propagate
	`SDDL_NO_PROPAGATE`
	`NO_PROPAGATE_INHERIT_ACE`	

IO	Inherit only
	`SDDL_INHERIT_ONLY`
	`INHERIT_ONLY_ACE`	

ID	Inherited
	`SDDL_INHERITED`
	`INHERITED_ACE`	

SA	Audit success
	`SDDL_AUDIT_SUCCESS`
	`SUCCESSFUL_ACCESS_ACE_FLAG`	

FA	Audit failure
	`SDDL_AUDIT_FAILURE`
	`FAILED_ACCESS_ACE_FLAG`	

TP	Trust protected filter
	`SDDL_TRUST_PROTECTED_FILTER`
	`TRUST_PROTECTED_FILTER_ACE_FLAG`
		Windows 10 Version 1703

CR	Critical
	`SDDL_CRITICAL`
	`CRITICAL_ACE_FLAG`
		Windows 10 Version 1809

SDDL access rights

Code	Meaning	Applies to	Introduced
RP	`ACTRL_DS_READ_PROP` `SDDL_READ_PROPERTY`	Directory services	Windows 2000
WP	`ACTRL_DS_WRITE_PROP` `SDDL_WRITE_PROPERTY`		
CC	`ACTRL_DS_CREATE_CHILD` `SDDL_CREATE_CHILD`		
DC	`ACTRL_DS_DELETE_CHILD` `SDDL_DELETE_CHILD`		
LC	`ACTRL_DS_LIST` `SDDL_LIST_CHILDREN`		
SW	`ACTRL_DS_SELF` `SDDL_SELF_WRITE`		
LO	`ACTRL_DS_LIST_OBJECT` `SDDL_LIST_OBJECT`		
DT	`ACTRL_DS_DELETE_TREE` `SDDL_DELETE_TREE`		
CR	`ACTRL_DS_CONTROL_ACCESS` `SDDL_CONTROL_ACCESS`		
RC	`READ_CONTROL` `SDDL_READ_CONTROL`	Anything	
WD	`WRITE_DAC` `SDDL_WRITE_DAC`		
WO	`WRITE_OWNER` `SDDL_WRITE_OWNER`		

SD	`DELETE` `SDDL_STANDARD_DELETE`		
GA	`GENERIC_ALL` `SDDL_GENERIC_ALL`		
GR	`GENERIC_READ` `SDDL_GENERIC_READ`		
GW	`GENERIC_WRITE` `SDDL_GENERIC_WRITE`		
GX	`GENERIC_EXECUTE` `SDDL_GENERIC_EXECUTE`		
FA	`FILE_ALL_ACCESS` `SDDL_FILE_ALL`	Files and folders	
FR	`FILE_GENERIC_READ` `SDDL_FILE_READ`		
FW	`FILE_GENERIC_WRITE` `SDDL_FILE_WRITE`		
FX	`FILE_GENERIC_EXECUTE` `SDDL_FILE_EXECUTE`		
KA	`KEY_ALL_ACCESS` `SDDL_KEY_ALL`	Registry keys	
KR	`KEY_READ` `SDDL_KEY_READ`		
KW	`KEY_WRITE` `SDDL_KEY_WRITE`		
KX	`KEY_EXECUTE` `SDDL_KEY_EXECUTE`		
NW	`SYSTEM_MANDATORY_LABEL_NO_WRITE_UP` `SDDL_NO_WRITE_UP`	Mandatory label ACE	Windows 7
NR	`SYSTEM_MANDATORY_LABEL_NO_READ_UP` `SDDL_NO_READ_UP`		
NX	`SYSTEM_MANDATORY_LABEL_NO_EXECUTE_UP` `SDDL_NO_EXECUTE_UP`		

SDDL users and groups

Tag	Meaning	Introduced

DA	Domain admins
	`SDDL_DOMAIN_ADMINISTRATORS`
	`DOMAIN_GROUP_RID_ADMINS`
		Windows 2000

DG	Domain guests
	`SDDL_DOMAIN_GUESTS`
	`DOMAIN_GROUP_RID_GUESTS`	

DU	Domain users
	`SDDL_DOMAIN_USERS`
	`DOMAIN_GROUP_RID_USERS`	

ED	Enterprise domain controllers
	`SDDL_ENTERPRISE_DOMAIN_CONTROLLERS`
	`SECURITY_SERVER_LOGON_RID`	

DD	Domain domain controllers
	`SDDL_DOMAIN_DOMAIN_CONTROLLERS`
	`DOMAIN_GROUP_RID_CONTROLLERS`	

DC	Domain computers
	`SDDL_DOMAIN_COMPUTERS`
	`DOMAIN_GROUP_RID_COMPUTERS`	

BA	Local administrators
	`SDDL_BUILTIN_ADMINISTRATORS`
	`DOMAIN_ALIAS_RID_ADMINS`	

BG	Local guests
	`SDDL_BUILTIN_GUESTS`
	`DOMAIN_ALIAS_RID_GUESTS`	

BU	Local users
	`SDDL_BUILTIN_USERS`
	`DOMAIN_ALIAS_RID_USERS`	

LA	Local administrator account
	`SDDL_LOCAL_ADMIN`
	`DOMAIN_USER_RID_ADMIN`	

LG	Local guest account
	`SDDL_LOCAL_GUEST`
	`DOMAIN_USER_RID_GUEST`	

AO	Account operators
	`SDDL_ACCOUNT_OPERATORS`
	`DOMAIN_ALIAS_RID_ACCOUNT_OPS`	

BO	Backup operators
	`SDDL_BACKUP_OPERATORS`
	`DOMAIN_ALIAS_RID_BACKUP_OPS`	

PO	Printer operators
	`SDDL_PRINTER_OPERATORS`
	`DOMAIN_ALIAS_RID_PRINT_OPS`	

SO	Server operators
	`SDDL_SERVER_OPERATORS`
	`DOMAIN_ALIAS_RID_SYSTEM_OPS`

AU	Authenticated users
	`SDDL_AUTHENTICATED_USERS`
	`SECURITY_AUTHENTICATED_USER_RID`

PS	Personal self
	`SDDL_PERSONAL_SELF`
	`SECURITY_PRINCIPAL_SELF_RID`

CO	Creator owner
	`SDDL_CREATOR_OWNER`
	`SECURITY_CREATOR_OWNER_RID`

CG	Creator group
	`SDDL_CREATOR_GROUP`
	`SECURITY_CREATOR_GROUP_RID`

SY	Local system
	`SDDL_LOCAL_SYSTEM`
	`SECURITY_LOCAL_SYSTEM_RID`

PU	Power users
	`SDDL_POWER_USERS`
	`DOMAIN_ALIAS_RID_POWER_USERS`

WD	Everyone (World)
	`SDDL_EVERYONE`
	`SECURITY_WORLD_RID`

RE	Replicator
	`SDDL_REPLICATOR`
	`DOMAIN_ALIAS_RID_REPLICATOR`

IU	Interactive logon user
	`SDDL_INTERACTIVE`
	`SECURITY_INTERACTIVE_RID`

NU	Nework logon user
	`SDDL_NETWORK`
	`SECURITY_NETWORK_RID`

SU	Service logon user
	`SDDL_SERVICE`
	`SECURITY_SERVICE_RID`

RC	Restricted code
	`SDDL_RESTRICTED_CODE`
	`SECURITY_RESTRICTED_CODE_RID`

SA	Schema administrators
	`SDDL_SCHEMA_ADMINISTRATORS`
	`DOMAIN_GROUP_RID_SCHEMA_ADMINS`

CA	Certificate server administrators
	`SDDL_CERT_SERV_ADMINISTRATORS`
	`DOMAIN_GROUP_RID_CERT_ADMINS`	

RS	RAS servers group
	`SDDL_RAS_SERVERS`
	`DOMAIN_ALIAS_RID_RAS_SERVERS`	

EA	Enterprise administrators
	`SDDL_ENTERPRISE_ADMINS`
	`DOMAIN_GROUP_RID_ENTERPRISE_ADMINS`	

PA	Group Policy administrators
	`SDDL_GROUP_POLICY_ADMINS`
	`DOMAIN_GROUP_RID_POLICY_ADMINS`	

RU	Compatibility for pre-Windows 2000 accounts
	`SDDL_ALIAS_PREW2KCOMPACC`
	`DOMAIN_ALIAS_RID_PREW2KCOMPACCESS`	

AN	Anonymous logon
	`SDDL_ANONYMOUS`
	`SECURITY_ANONYMOUS_LOGON_RID`
		Windows XP

LS	Local service account
	`SDDL_LOCAL_SERVICE`
	`SECURITY_LOCAL_SERVICE_RID`	

NS	Network service account
	`SDDL_NETWORK_SERVICE`
	`SECURITY_NETWORK_SERVICE_RID`	

RD	Remote desktop users
	`SDDL_REMOTE_DESKTOP`
	`DOMAIN_ALIAS_RID_REMOTE_DESKTOP_USERS`	

NO	Network configuration operators
	`SDDL_NETWORK_CONFIGURATION_OPS`
	`DOMAIN_ALIAS_RID_NETWORK_CONFIGURATION_OPS`	

MU	Performance Monitor users
	`SDDL_PERFMON_USERS`
	`DOMAIN_ALIAS_RID_MONITORING_USERS`	

LU	Performance Log users
	`SDDL_PERFLOG_USERS`
	`DOMAIN_ALIAS_RID_LOGGING_USERS`	

WR	Write Restricted code
	`SDDL_WRITE_RESTRICTED_CODE`
	`SECURITY_WRITE_RESTRICTED_CODE_RID`
		Windows Vista

IS	Anonymous Internet users
	`SDDL_IIS_USERS`
	`DOMAIN_ALIAS_RID_IUSERS`	

CY	Crypto operators
	`SDDL_CRYPTO_OPERATORS`
	`DOMAIN_ALIAS_RID_CRYPTO_OPERATORS`	

OW	Owner Rights SID
	`SDDL_OWNER_RIGHTS`
	`SECURITY_CREATOR_OWNER_RIGHTS_RID`	

RM	RMS service operators
	`SDDL_RMS_SERVICE_OPERATORS`
	`DOMAIN_ALIAS_RID_RMS_SERVICE_OPERATORS`
		Windows Vista Removed in Win7

ER	Event log readers
	`SDDL_EVENT_LOG_READERS`
	`DOMAIN_ALIAS_RID_EVENT_LOG_READERS_GROUP`
		Windows 7

RO	Enterprise read-only domain controllers
	`SDDL_ENTERPRISE_RO_DCs`
	`DOMAIN_GROUP_RID_ENTERPRISE_READONLY_DOMAIN_CONTROLLERS`	

CD	Can connect to certification authorities using DCOM
	`SDDL_CERTSVC_DCOM_ACCESS`
	`DOMAIN_ALIAS_RID_CERTSVC_DCOM_ACCESS_GROUP`	

AC	All applications running in an app package context
	`SDDL_ALL_APP_PACKAGES`
	`SECURITY_BUILTIN_PACKAGE_ANY_PACKAGE`
		Windows 8

RA	RDS remote access servers
	`SDDL_RDS_REMOTE_ACCESS_SERVERS`
	`DOMAIN_ALIAS_RID_RDS_REMOTE_ACCESS_SERVERS`	

ES	Endpoint servers
	`SDDL_RDS_ENDPOINT_SERVERS`
	`DOMAIN_ALIAS_RID_RDS_ENDPOINT_SERVERS`	

MS	Management servers
	`SDDL_RDS_MANAGEMENT_SERVERS`
	`DOMAIN_ALIAS_RID_RDS_MANAGEMENT_SERVERS`	

UD	User-mode driver
	`SDDL_USER_MODE_DRIVERS`
	`SECURITY_USERMODEDRIVERHOST_ID_BASE_RID`	

HA	Hyper-V administrators
	`SDDL_HYPER_V_ADMINS`
	`DOMAIN_ALIAS_RID_HYPER_V_ADMINS`	

CN	Domain controllers which may be cloned
	`SDDL_CLONEABLE_CONTROLLERS`
	`DOMAIN_GROUP_RID_CLONEABLE_CONTROLLERS`	

AA	Access control assistant operators
	`SDDL_ACCESS_CONTROL_ASSISTANCE_OPS`
	`DOMAIN_ALIAS_RID_ACCESS_CONTROL_ASSISTANCE_OPS`	

RM	Remote management users
	`SDDL_REMOTE_MANAGEMENT_USERS`
	`DOMAIN_ALIAS_RID_REMOTE_MANAGEMENT_USERS`	

AS	Authentication Authority Asserted
	`SDDL_AUTHORITY_ASSERTED`
	`SECURITY_AUTHENTICATION_AUTHORITY_ASSERTED_RID`	

SS	Authentication Service Asserted
	`SDDL_SERVICE_ASSERTED`
	`SECURITY_AUTHENTICATION_SERVICE_ASSERTED_RID`	

AP	Protected users
	`SDDL_PROTECTED_USERS`
	`DOMAIN_GROUP_RID_PROTECTED_USERS`
		Windows 8.1

KA	Domain key credential administrators
	`SDDL_KEY_ADMINS`
	`DOMAIN_GROUP_RID_KEY_ADMINS`
		Windows 10

EK	Enterprise key credential administrators
	`SDDL_ENTERPRISE_KEY_ADMINS`
	`DOMAIN_GROUP_RID_ENTERPRISE_KEY_ADMINS`	

"RM" is the only case I can find of something being *removed* from SDDL.

SDDL integrity labels

Code	Meaning	Introduced
LW	Low mandatory level `SECURITY_MANDATORY_LOW_RID`	Windows Vista
ME	Medium mandatory level `SECURITY_MANDATORY_MEDIUM_RID`	
MP	Medium Plus mandatory level `SECURITY_MANDATORY_MEDIUM_PLUS_RID`	Windows 7
HI	High mandatory level `SECURITY_MANDATORY_HIGH_RID`	Windows Vista
SI	System mandatory level `SECURITY_MANDATORY_SYSTEM_RID`	

SDDL syntax elements

Syntax	Meaning	Introduced
semicolon	Separates elements inside an ACE `SDDL_SEPERATOR`	Windows 2000
colon	Delimits SD components `SDDL_DELIMINATOR`	

parentheses	Enclose an ACE
	`SDDL_ACE_BEGIN`
	`SDDL_ACE_END`	

parentheses	Enclose a conditional ACE expression
	`SDDL_ACE_COND_BEGIN`
	`SDDL_ACE_COND_END`
		Windows 7

curly braces	Enclose a comma-separated list of SIDs
	`SDDL_ACE_COND_COMPOSITEVALUE_BEGIN`
	`SDDL_ACE_COND_COMPOSITEVALUE_SEPERATOR`
	`SDDL_ACE_COND_COMPOSITEVALUE_END`	

number sign	Hexadecimal byte data `SDDL_ACE_COND_BLOB_PREFIX`	

parentheses	Enclose a string SID in a SID list
	`SDDL_ACE_COND_SID_BEGIN`
	`SDDL_ACE_COND_SID_END`	

I like how “separator” and “delimiter” are misspelled.

Raymond Chen

Follow