

Правда об идентификаторах безопасности

Иван Коробко

Для многих идентификатор безопасности – это темный лес. На самом деле все гораздо проще. Эта статья поможет превратить его в прекрасную цветущую поляну.

В настоящее время в Windows повсюду используются идентификаторы безопасности: в правах доступа, в реестре, в Active Directory. Понимать, откуда берутся эти идентификационные номера, очень важно, поскольку это значительно облегчит жизнь как системным администраторам, так и специалистам системной поддержки.

В Windows широко используется несколько видов различных иденти-

фикаторов безопасности: GUID, SID, UUID (CLSID).

Виды идентификаторов безопасности

■ **GUID (Globally Unique Identifier)** – представляет собой уникальный 128-битный идентификатор. Его главная особенность – уникальность. Общее количество уникальных ключей настолько велико (2^{128} или $3,4028 \times 10^{38}$), что веро-

ятность генерации двух совпадающих ключей ничтожно мала. GUID – это частная реализация (компанией Microsoft) стандарта, имеющего название Universally Unique Identifier (UUID).

■ **SID (Security Identifier)** – уникальная бинарная структура данных переменной длины, однозначно идентифицирующая объект: учетную запись пользователя, группы, домена, компьютера и т. д.

■ **UUID (Universally Unique Identifier)** – это стандарт идентификации, используемый в создании программного обеспечения, стандартизированный Фондом свободного программного обеспечения (FSF). UUID описан в RFC1422 «A Universally Unique Identifier (UUID) URN Namespace».

Рассмотрим каждый тип идентификаторов безопасности подробнее.

Идентификатор безопасности GUID

GUID нашел широкое применение в Active Directory. Совместно с другим идентификатором безопасности, о котором речь пойдет позже (SID), он однозначно определяет объект.

При создании новой учетной записи пользователя или группы в Active Directory новому объекту присваивается уникальный в глобальном масштабе идентификатор (GUID) не только в домене, но и во всем мире. Кроме объектов-пользователей и объектов-групп, GUID есть у всех объектов, создающихся в Active Directory. Значение GUID хранится в бинарном виде в параметре ObjectGUID (см. **рис. 1**).

Структура GUID

GUID – это 16-байтный (128-битный) идентификатор, описанный в стандарте «A Universally Unique Identifier (UUID) URN Namespace» (RFC 1422). Условно идентификатор разбивают на 4 части (см. **таблицу 1**), а при записи в текстовом виде последнюю часть разбивают дополнительно еще на две. Это делается для упрощения определения типа идентификатора: первый байт последнего, 64-битного раздела (в текстовом виде это как раз 4 символа) определяет тип GUID (см. **таблицу 2**). В текстовом виде GUID записывается следующим образом: d50b151a-02c0-4dd0-a59e-f1fb61614d6b.

Определение типа GUID

В настоящее время существует 5 версий GUID (см. **таблицу 3**). Номер версии GUID – первое число третьей части GUID: c9802770-e0af-11dc-95ff-0016368d1a02. Как видно из **таблицы 3** – этот GUID сгенерирован на основе временного штампа. Зная тип идентификатора, легко определить,

Таблица 1. Структура GUID

Бит	Байт	Часть	Количество символов в блоке
32	4	1	8
16	2	2	4
16	2	3	4
64	8	4	4
			12

Таблица 2. Расшифровка значения первого байта последнего блока GUID

Значение	Описание
0	NCS Совместимость с Networking Computing System
10	Стандарт
110	Microsoft COM. Сюда также относится очень важный GUID – unknown-устройства
111	Зарезервировано

objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=msk,DC=prosv,DC=ru	text attribute	58
objectClass	top	text attribute	3
objectClass	person	text attribute	6
objectClass	organizationalPerson	text attribute	20
objectClass	user	text attribute	4
objectGUID	EB BE E8 EC 4F 52 F6 42 96 3C 99 B6 23 E7 D7 73	binary attribute	16
objectSid	01 05 00 00 00 00 00 05 15 00 00 00 2C 8F EC FB	binary attribute	28

Рисунок 1. GUID в Active Directory

является ли он стандартным или сгенерирован каким-либо программным обеспечением. Подводя итог, перечислим особенности глобального идентификатора (GUID):

- генерируемое значение GUID уникально во всем мире;
- идентификатор не изменяется на протяжении всего времени существования объекта.

Генерация GUID

Для генерации GUID можно воспользоваться либо одним из on-line-генераторов в Сети, либо встроенной в Windows стандартной библиотекой с помощью сценариев (см. **ЛИСТИНГ 1**).

Листинг 1. Генерация GUID (V-Script)

```
Set TypeLib = .  
CreateObject("Scriptlet.TypeLib")  
wscript.Echo TypeLib.Guid  
Set TypeLib = Nothing
```

Идентификатор безопасности SID

Этот идентификатор широко известен не только опытным системным администраторам и специалистам системной поддержки, но и обычным пользователям, настраивающим доступ к папке между двумя компьютерами. Открыв вкладку «Безопасность» свойств обычной папки (см. **рис. 2**), пользователь видит объекты: группы и пользователи, которым назначен индивидуальный набор прав. На самом деле там указаны SID, а для упрощения восприятия отображаются понятные всем имена объектов. SID имеет сложную структуру, которая будет рассмотрена позже.

SID присваивается пользователю при создании учетной записи пользователя или группы в Active Directory.

Значение SID в бинарном виде хранится в параметре ObjectSID.

Особенности SID

Идентификатор имеет несколько очень важных особенностей:

Таблица 3. Версии GUID

Версия	Описание
1	GUID созданный на основе временного штампа (time based GUID)
2	DCE Security version (with POSIX UIDs)
3	GUID основанный на имени (MD5 hash)
4	Произвольный GUID
5	GUID основанный на имени(SHA-1 hash)

Таблица 4. Расшифровка значений параметра «уровень идентификации» SID

Идентификатор	Значение
SECURITY_NULL_SID_AUTHORITY	0
SECURITY_WORLD_SID_AUTHORITY	1
SECURITY_LOCAL_SID_AUTHORITY	2
SECURITY_CREATOR_SID_AUTHORITY	3
SECURITY_NON_UNIQUE_AUTHORITY	4
SECURITY_NT_AUTHORITY	5

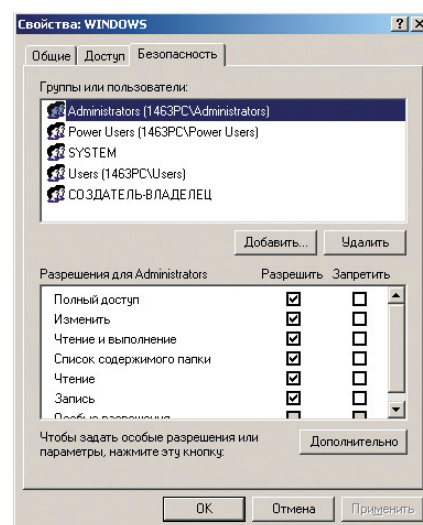


Рисунок 2. Параметры безопасности объекта

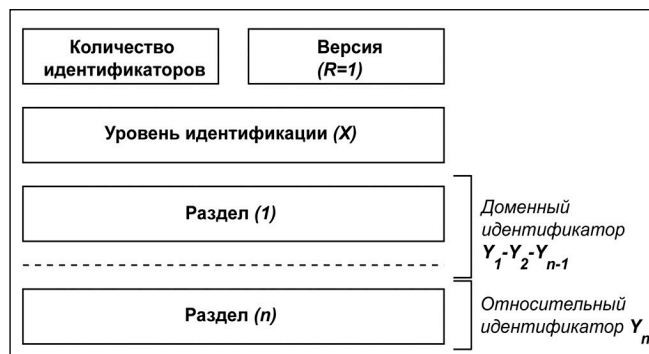


Рисунок 3. Структура SID

- Каждый объект (группа безопасности или пользователь) имеет персональный идентификатор.
- Изменить SID объекта в пределах одного домена невозможно. При переходе в другой домен пользователь получает дополнительный SID.
- Идентификаторы удаленных объектов никогда более не используются.
- SID в учетных записях домена или Windows одни и те же, вне зависимости от версии продукта (см. **таблицу 6**).
- Если контроллер домена по какой-либо причине недоступен, то имя объекта не подставляется и отображается его SID. Второй причиной, по которой может отображаться, – некорректное удаление объекта.

Таблица 5. Поэтапное преобразование SID

Бинарный вид	Канонический (строковый) вид	Положение в бинарной записи	Комментарий
01	S-1	1-й байт (1 байт)	К идентификатору добавляется признак SID – S
05	5 разделов (5=0x5)	2-й байт (1 байт)	Не участвует в формуле SID. Несет информационную нагрузку о количестве идентификационных групп
00 00 00 00 00 05	05 (0x00000005)	3-8 байты (6 байт)	Смотри таблицу 6 . Расшифровка значений параметра «уровень идентификации» SID
15 00 00 00	21 (0x00000015)	9-12 байты (4 байта)	Перед преобразованием из 16-ричной системы записывают байты в обратном порядке
2C 8F EC FB	4226584364 (0xFBEC8F2C)	13-16 байты (4 байта)	
E5 F2 48 01	21557989 (0x0148F2E5)	17-20 байты (4 байта)	
35 A6 99 55	1436132917 (0x5599A635)	21-24 байты (4 байта)	
26 1B 00 00	6950 (0x00001B26)	25-28 байты (4 байта)	

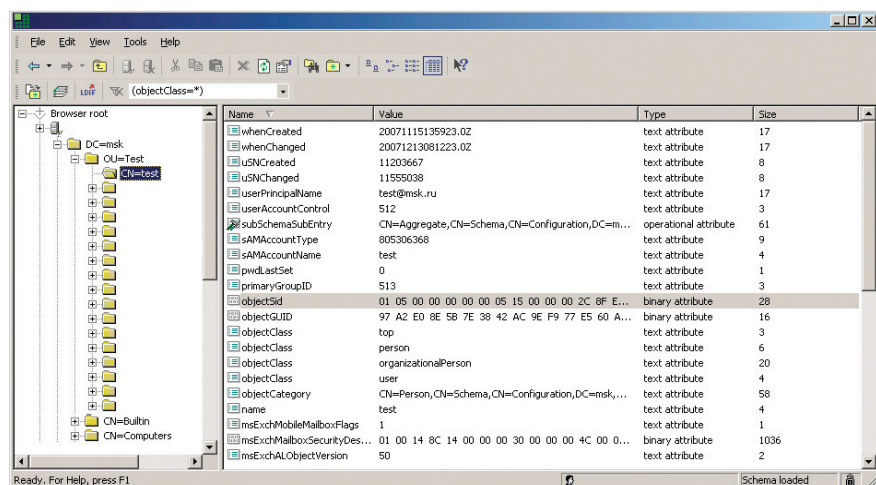


Рисунок 4. SID в Active Directory

При взаимодействии между объектами в Active Directory и Windows идентификация объектов осуществляется с помощью SID.

При переименовании объекта идентификатор безопасности остается прежним. При создании объекта ему присваивается новый SID.

Таким образом, если созданная доменная учетная запись пользователя User1 переименована в User2, то с точки зрения Active Directory у объекта изменено только свойство, поскольку SID остался неизменным.

Если же пользователь был удален, а затем создан заново с тем же именем, то с точки зрения Active Directory появился новый объект. Старый безвозвратно удален.

Если же учетная запись была удалена, а затем восстановлена из резервной копии Active Directory, то SID учетной записи пользователя после восстановления будет прежним

Структура SID

SID состоит из нескольких частей (см. **рис. 3**). Выражение SID можно записать формулой:

$$S-R-X-Y1-Y2-...-Yn-1-Yn \quad (1)$$

Каждая из букв несет в себе смысловую нагрузку:

- **S** – идентифицирует SID. Идентификатор всегда начинается с этой буквы.
- **R** – указывает на версию структуры идентификатора. Поскольку SID никогда не может быть изменен, этот параметр всегда равен 1.
- **X** – показывает наивысший уровень идентификации, которым обладает созданный объект. Значение этого параметра варьируется от 0 до 5 (см. **таблицу 4**). Например, параметр X в SID любой группы безопасности или учетной записи пользователя в домене имеет значение 5, а группа Everyone (все) – 0.
- **Y1-Y2-Yn-1** – идентификатор домена.
- **Yn** – относительный идентификатор (RID, relative IDs), который показывает порядковый номер объекта с момента создания Active Directory. Для встроенных объектов зарезервирован диапазон RID от 0 до 999. Например, для администратора – 500, для гостя – 501. Первой учетной записи, созданной в любой локальной системе или домене NT/2k, присваивается RID 1000, а каждому последующему объекту – следующий за ним порядковый номер (1001, 1002, 1003 и т. д.), причем при удалении объекта его номер уже никогда не используется при создании новых объектов.

S - 1 - 5 - 21 - 4226584364 - 21557989 -
1436132917 - 6950

(6)

Определение SID пользователя с помощью утилиты GetSID

Чтобы узнать SID пользователя, можно воспользоваться утилитой GetSID, входящей в состав Windows 2000 Resource Kit Tools. Утилиту можно загрузить с сайта Microsoft: <http://download.microsoft.com/download/win2000platform/GetSID/1.0/NT5/EN-US/getsid.exe>. В первую очередь GetSID.exe предназначена для сравнения SID разных пользователей, однако она может с успехом использоваться для получения SID конкретного пользователя. После завершения работы мастера утилиту и сопутствующую документацию можно найти в каталоге C:\Program Files\Resource Kit.

Утилита GetSID.exe запускается из командной строки и имеет следующий синтаксис:

```
GetSID.exe \\server1 account \\server2 account
```

Для определения SID рекомендуется задать две одинаковые пары параметров: сервер и имя учетной записи в сети. Если необходимо определить SID доменной учетной записи, то в качестве сервера необходимо указать либо имя контроллера домена, либо имя домена в сокращенной форме. Например, необходимо определить SID пользователя test в домене MSK. Для этого выполним команду:

```
GetSID.exe \\MSK test \\MSK test
```

В результате выполнения этой команды на экран будет выведено сообщение, показанное на **рис. 5**.

Широко известные идентификаторы SID

Под хорошо известными SID понимают группу идентификаторов безопасности, идентифицирующую общих пользователей и общие группы безопасности. Их значения одинаковы во всех операционных системах.

Идентификатор безопасности UUID

Универсальный уникальный идентификатор активно используется для создания программного обеспечения. Все объекты Windows имеют свой уникальный идентификатор – UUID. Перечень всех идентификаторов, используемых

Таблица 7. Некоторые стандартизованные UUID

UUID	Объект
{4e1-3957-11d2-a40b-0c5020524153}	Administrative Tools
{85bbd920-42a0-1069-a2e4-08002b30309d}	Briefcase
{21ec2020-3aea-1069-a2dd-08002b30309d}	Control Panel
{d20ea4e1-3957-11d2-a40b-0c5020524152}	Fonts
{ff393560-c2a7-11cf-bff4-444553540000}	History
{00020d75-0000-0000-c000-000000000046}	Inbox
{00028b00-0000-0000-c000-000000000046}	Microsoft Network
{20d04fe0-3aea-1069-a2d8-08002b30309d}	My Computer
{450d8fba-ad25-11d0-98a8-0800361b1103}	My Documents
{208d2c60-3aea-1069-a2d7-08002b30309d}	My Network Places
{1f4de370-d627-11d1-ba4f-00a0c91eedba}	Network Computers
{7007acc7-3202-11d1-aad2-00805fc1270e}	Network Connections
{2227a280-3aea-1069-a2de-08002b30309d}	Printers and Faxes
{7be9d83c-a729-4d97-b5a7-1b7313c39e0a}	Programs Folder
{645ff040-5081-101b-9f08-00aa002f954e}	Recycle Bin
{e211b736-43fd-11d1-9efb-0000f8757fcd}	Scanners and Cameras
{d6277990-4c6a-11cf-8d87-00aa0060f5bf}	Scheduled Tasks
{48e7caab-b918-4e58-a94d-505519c795dc}	Start Menu Folder
{7bd29e00-76c1-11cf-9dd0-00a0c9034933}	Temporary Internet Files
{bdeadf00-c265-11d0-bced-00a0c90ab50f}	Web Folders

мых в данном компьютере, можно найти в реестре в ветви HKEY_CLASSES_ROOT\CLSID (см. **рис. 6**).

Каждая UUID-папка имеет внутреннюю структуру, в которой находятся параметры, определяющие местоположение объекта, контекстное меню, значок объекта и другие свойства. В **таблице 7** приведены стандартизованные UUID объектов, которые во всех версиях Windows одинаковы.

Генерация UUID

При создании какого-либо приложения с помощью Microsoft Visual Studio .NET, GUID объектов формируется автоматически. Если необходимо сгенерировать идентификаторы явным образом воспользовавшись одним из on-line генераторов: <http://www.famkruihof.net/uuid/uuidgen>.

Заключение

В заключение хочется сказать: несмотря на то, что предложенные знания не являются самыми необходимыми, они важны. Понимание процесса образования SID и других идентификаторов безопасности поможет решить множество проблем, возникающих в процессе эксплуатации сети. Многие «чудеса» станут вполне объяснимыми.

1. KB 288900 «How To Use Visual Basic to Construct a Well-Known SID».
2. RFC 4122 «A Universally Unique Identifier (UUID) URN Namespace».
3. CLSID List. Windows Class Identifiers – <http://www.autohotkey.com/docs/misc/CLSID-List.htm>.

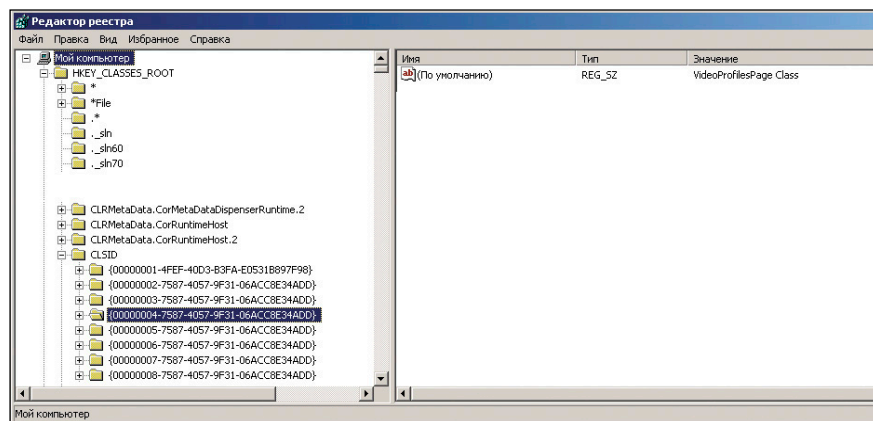


Рисунок 6. Папка CLSID