Анализ кода продукта Microsoft Windows

Коршунов Владимир Геннадьевич, ООО «ИнфоБиС»

В последнее время значению кода продукта Microsoft Windows (product ID), отображаемому, в том числе, в окне «Свойства системы», уделяется особое внимание. Связано это в первую очередь с процедурой проверки контрафактности установленного экземпляра операционной системы Windows. В статье мы подробно рассмотрим различные аспекты формирования значения Product ID и его анализа.

Необходимо заметить, что приведенная информация получена опытно-аналитическим путем и постоянно уточняется. Любые свои отзывы и комментарии присылайте на электронный адрес com@infobis.ru.

Формат отображения значения Product ID Microsoft Windows

Как выглядит значение Product ID Windows 2000/XP/2003 ? Как символьная последовательность длиной 20 символов:

XXXXX-YYY-*ZZZZZZZ*-ZZZZZ, где

XXXXX – это код продукта Microsoft (Microsoft Product Code – MPC).

Полный список кодов всех своих продуктов официально фирмой Microsoft не опубликован, но, например, для Windows Server 2003 коды продукта приведены в статье «Как определить канал покупки Вашей копии Windows Server 2003»[1].

Примеры значений MPC:

51873 – Windows 2000 Professional English,
55034 – Windows XP Professional English,
55681 – Windows XP Home Edition Russian,
55683 – Windows XP Professional Russian,
69712 – Windows Server 2003 Standard Edition 32-bit English,
69890 – Windows Server 2003 Standard Edition 32-bit Russian.

Разные локализации Windows XP имеют разные MPC, однако для Windows Vista Microsoft выделила всего несколько MPC, которые имеют следующие собственные значения только для разных редакций Vista:

89572 – Windows Vista Home Basic,
89576 – Windows Vista Business,
89578 – Windows Vista Home Premium,
89580 – Windows Vista Ultimate.

Код MPC определяет не конкретный продукт семейства Windows, а указывает на некоторое подмножество продуктов. Для дальнейшего уточнения информации о продукте необходимо воспользоваться составляющими Product ID. И, напротив, для некоторых наименований продуктов выделено несколько кодов MPC, которые, по-видимому, отличаются разными каналами или условиями поставки.

Рассмотрим сначала существующие на момент подготовки статьи каналы или условия поставки продуктов Microsoft.

- **Коробочные продукты** (Retail или Full Package Product – FPP). Т.е. продукты, продаваемые за полную цену, с полным комплектом сопровождающих материалов и предназначенные для продажи через розничную торговлю конечным покупателям. Техническую поддержку коробочных продуктов осуществляет сама Microsoft.
- **OEM** (Original Equipment Manufacturer) – продукты, предназначенные для включения их Поставщиками Вычислительной Техники (ПВТ) (в новой редакции лицензионного соглашения – Сборщиками Систем (System Builders)), в свои готовые изделия. Если

[1] http://support.microsoft.com/kb/889713

отвлечься от продуктов Microsoft, то термин OEM применяется обычно к тем товарам, которые производятся не для конечных потребителей, а для использования в следующем цикле производства. Такие товары, само собой, не комплектуются красочными упаковками или инструкциями, имеют ограниченную гарантию, при этом их цена гораздо ниже. Microsoft OEM продукты могут быть проданы только поставщикам и продаются они также по более низким ценам, чем продукты FPP, однако именно на сборщиков систем возлагается техническая поддержка конечных пользователей. Также OEM продукты, согласно лицензионному соглашению, не могут быть установлены на другой компьютер. Каналами поставки OEM продуктов могут быть:

- **OEM SYSTEM BUILDER** – продукты, устанавливаемые обычными OEM партнерами (маленькими OEM, System Builder), и требующие помещения сертификата подлинности (Certificate of Authentication или COA) на корпус системного блока компьютера. В указанном случае ПВТ покупают у дистрибьюторов Microsoft комплекты, включающие компакт диски и наклейки COA. Для каждого экземпляра программы вводится свой ключ продукта, указанный на COA.
- **OEM SLP.** Крупные производители (Royalty OEM, Direct OEM, Large Computer Manufacturer), которые имеют специальные соглашения с Microsoft, устанавливают и активируют операционную систему без обращения в Microsoft, но это предполагает наличие определенных данных в BIOS компьютера или определенной модели материнской платы. Таким образом, фактически осуществлена «привязка» операционной системы к аппаратной составляющей конкретного производителя (System Locked Preinstallation). Интересным фактом является то, что при установке каждый Roalty OEM использует один общий ключ продукта, однако на наклейке COA напечатан совершенно другой ключ, который конечный пользователь может использовать при повторной установке системы. Таким образом, в случае OEM SLP хранящееся в системном реестре значение ключа продукта заведомо **не совпадает** со значением ключа на наклейке COA, если такая переустановка операционной системы не проводилась**!**

- **Корпоративные лицензии.** Для крупных организаций предусмотрены специальные программы, в рамках которых, по прямому соглашению с Microsoft, приобретается соответствующее число лицензий и, при необходимости, лицензионный носитель. Эти программы разработаны отдельно для коммерческих, правительственных и образовательных организаций, и имеют отличия в механизмах оплаты (обычная оплата, аренда ПО, страховка апгрейда и пр.) Для установки системы на все компьютеры используется один ключ, называемый Volume License Key (VLK), активация таких ключей в Microsoft не требуется. В Windows Vista/Server 2008 на смену ключам VLK пришли ключи Multiple Activation Keys (MAK) и Key Management Server (KMS), которые тем или иным способом требуют активации.
- **Продукты, предназначенные для легализации установленной ОС**, т.е. для использования на ПК с ранее установленным контрафактным («пиратским», полученным или используемым незаконным способом) экземпляром операционной системы Windows. На данный момент таким продуктом является Get Genuine Kit (GGK), легализующий версию Windows XP Professional. Необходимо заметить, что хотя GGK и разрешается продавать конечным пользователям, но по лицензионному соглашению GGK является OEM продуктом, что не дает права применять его для легализации количества контрафактных экземпляров программы, отличающегося от количества экземпляров, указанного при покупке.

YYY – код, в преимущественной степени определяющий способ поставки продукта (Channel

ID или CID). Несмотря на мнения, широко представленные в различных источниках, на наш взгляд, не совсем корректно использовать только значение CID для точного определения канала поставки. Тем не менее, приведем некоторые примеры значений CID[2]:

- **OEM** – однозначно определяет OEM продукты (причем по CID невозможно отличить OEM SYSTEM BUILDER от OEM SLP);
- **640**, **641** и другие 6xx – корпоративные, образовательные и прочие лицензии с ключом многократной установки;
- **073** – пакет легализации Get Genuine Kit;
- **007** и многие другие значения – коробочные продукты.

Прежде чем перейти к интерпретации следующей группы символов ProductID, необходимо рассказать о том, что представляет собой ключ установки (ключ продукта, ключ активации, CD Key, Product Key), который Windows запрашивает при установке. Данный ключ (без разделителей) состоит из 25 символов, которые должны входить в алфавит «BCDFGHJKMPQRTVWXY2346789», включающий 24 символа. Максимальное количество информации, которое может содержаться в ключе – 114 бит. Как интерпретируется значение этого ключа?

Часть данных представлена в явном виде. Например для OEM продуктов первые 30 бит – это уникальный номер, который, по видимому, является серийным номером конкретного экземпляра программы. Часть данных содержится в компонентах ключа в зашифрованном с помощью эллиптической криптографии виде[3]. Это асимметричная криптография, т.е. для того, чтобы зашифровать сообщение, нужен один закрытый (секретный) ключ, а для того, чтобы расшифровать его, нужен другой, открытый (публичный) ключ. Само собой, закрытый ключ шифрования известен только Microsoft, а вот открытые ключи хранятся в различных системных исполняемых файлах, в частности в библиотеке pidgen.dll. Валидными (признаваемыми системой корректными) ключами продукта являются те, в которых информация, полученная после расшифровки, совпадает с информацией из открытой части в ключе.

Для разных продуктов предусмотрены различающиеся ключи шифрования, поскольку если бы они были совпадающими, то один ключ подходил бы ко всем продуктам Microsoft. Как уже говорилось выше, открытые ключи хранятся в ресурсах библиотеки pidgen.dll. Данные ресурсы имеют тип BINK, что, по-видимому, является сокращением от BINary Key. Таких ресурсов в библиотеке может быть несколько, например pidgen.dll для Server 2003 R2 содержит четыре разных ключа, а библиотеки для Windows XP содержат только два, причем второй в основном предназначен для OEM продуктов. Таким образом, зная криптографический ключ можно идентифицировать конкретный продукт. Каким образом это сделать?

Первые 4 байта в ресурсе BINK содержат так называемый BINKID – идентифицирующий ключ шифрования. Рассмотрим наиболее распространенные BINKID (во второй колонке значения представлены в десятичной системе исчисления):

BINKID 16-ричный	BINKID 10-ричный	Версия Windows
0x28	40	Windows XP Evaluation
0x2A	42	Windows XP Home Retail Для CID 337-359 - Tablet PC Edition
0x2B	43	Windows XP Home OEM для CID 120-169, 400-665, 667-699, 700-754 - Retail
0x2C	44	Windows XP Professional Retail

[2] http://ru.wikipedia.org/wiki/Product_ID

[3] http://en.wikipedia.org/wiki/Elliptic_curve_cryptography

		Для CID 337- 359, 360-369 - Tablet PC Edition
0x2D	45	Windows XP Professional OEM Для CID не равных 119 - Retail
0x2E	46	Windows XP Professional VOLUME
0x30	48	Windows XP Tablet PC Edition
0x31	49	Windows XP Home OEM Для CID не равных 119 - Retail
0x32	50	Windows XP Tablet PC Edition
0x33	51	Windows XP Professional OEM Для CID не равных 119 - Retail
0x54	84	Windows Server 2003 Retail (для некоторых CID — Windows Home Server)
0x55	85	Windows Server 2003 OEM (для некоторых CID - Retail)
0x56	86	Windows Server 2003 Evaluation
0x58	88	Windows Server 2003 R2 Retail (для некоторых CID — Windows Home Server)
0x59	89	Windows Server 2003 R2 OEM (для некоторых CID - Retail)
0x5A	90	Windows Server 2003 VOLUME
0x8E	142	Vista RTL и VOL
0x90	144	Vista OEM COA
0x92	146	Vista OEM (SLP и SYSTEM BUILDER)

Анализируя значения, представленные в таблице, можно сделать обоснованный вывод о том, что по комбинации BINKID и кода канала поставки можно определить и наименование продукта, и канал поставки. Каким образом определить значение BINKID, использованное в исследуемом программном продукте? Для этого вернемся к рассмотрению значений последних групп символов в ProductID.

Для ключа OEM-продукта, соответствующего наклейке COA, значение последних групп символов в ProductID представляет собой серийный номер данного экземпляра Windows, формат которого следующий:

001234*X*-**56789**, где *X* – значение контрольной суммы.

Приведенный в качестве примера серийный номер продукта 12345689 указан на всех компонентах упаковки OEM продукта. На этикетке COA под штрих кодом должна располагаться последовательность символов 000DD-123-456-789, где DD – это значение того самого BINKID, который мы рассматривали ранее. Например, для Windows XP Professional OEM значение BinkID будет равным 51. На упаковочной коробке под штрих кодом COA Barcodes должна быть указана последовательность символов 000DD123456789.

Для OEM ключей **SLP** последние группы символов обычно имеют следующий вид:

00119**ZZ-XXXXX**, где

119 – это значение, используемое Microsoft для OEM канала, т.е. данное значение является дополнительным подтверждением того, что программный продукт является OEM-продуктом.

Группа цифр **XXXXX** идентифицирует производителя, причем для каждого региона

производителю присвоен уникальный код. Например:

Производитель	XP Home/Pro	XP Media Center	XP Tablet Edition
Acer	00100/00577/01807	00865	00303
Asus	00109/00584/01814	00935	
Dell	00102/00581/01811	00825	
Fujitsu-Siemens	00117/00583/01810	00854	00309
Hewlett-Packard	00106/00570/01801	00803/00800	00302
Toshiba	00111/00573	00817	00305
Sony	00110/00572/01800	00826	

Для всех остальных типов ключей соблюдается следующий формат:

***ZZZZZZZ*-DDYYY**,

где ***ZZZZZZZ*** – уникальный номер,
DD – значение BINKID, деленное на два,
YYY – случайное число, полученное при генерации ключа.

Таким образом, для всех «не-OEM» продуктов значение BINKID можно получить «напрямую» из ProductID, для OEM продуктов это невозможно, и в этом случае необходимо воспользоваться DigitalProductID или DigitalProductID4, о формате и назначении которых мы расскажем в следующей статье.

Для **Retail** и **Volume** продуктов, не удалось определить, чему соответствует код *ZZZZZZZ*. Автор не исключает того, что для Volume лицензий этот код является значением хэш-функции от номера соглашения.

Пакет легализации **Get Genuine Kit** является гибридным продуктом, поскольку он, с одной стороны, может продаваться конечному пользователю и идентифицируется при помощи BinkID и CID как Retail продукт, а с другой стороны, он сопровождается наклейкой COA и не может использоваться для легализации количества контрафактных экземпляров программы, отличающегося от количества экземпляров, указанного при покупке пакета легализации. Видимо поэтому штрих-код наклейки COA для GGK отличается от обычных OEM. Если последние группы символов кода продукта имеют вид 123456X-QQRRR, где X – значение контрольной суммы, а QQ – это значение BinkID, деленное на два, то на наклейке COA под штрих кодом должна быть следующая последовательность символов: 000DD-CID-132-456, где DD – значение BinkID, CID – значение Channel ID.

Продолжение статьи читайте в журнале "Компьютерно-техническая экспертиза" №3 (4) за 2008 год. Раздел "Техническая документация".