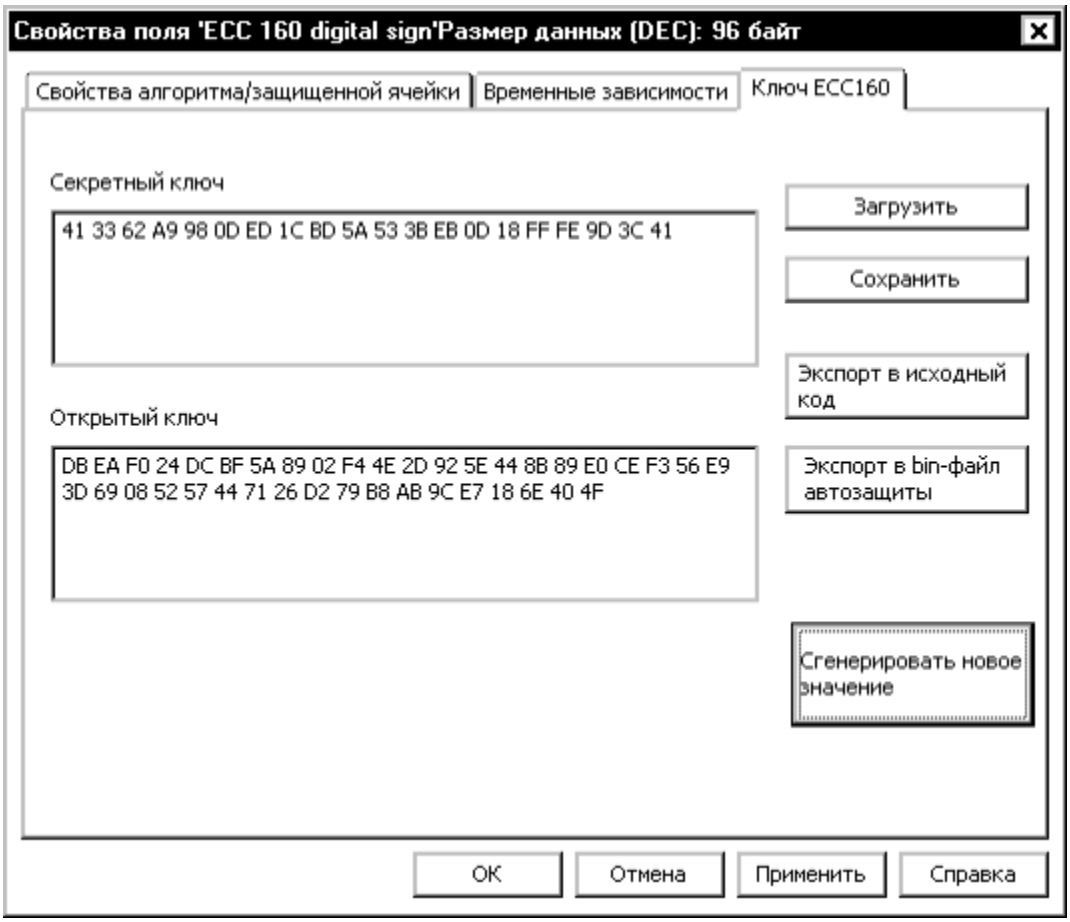
Цифровая подпись ECC160

При создании (редактировании) асимметричного алгоритма цифровой подписи **ECC160** место диалога **Определитель алгоритма** занимает **Ключ ECC160**.

Диалог **Ключ ECC160** служит для генерации ключевой пары алгоритма цифровой подписи ECC160.

В верхней части диалога отображается секретный ключ алгоритма, в нижней – открытый. Справа располагаются кнопки, позволяющие выполнять сервисные действия с ключевой парой.



По умолчанию при создании алгоритма **ECC160** генерируется ключевая пара из случайных чисел. Ключевую пару можно изменить, автоматически создав новую (кнопка **[Сгенерировать новое значение]**).

Кнопка **[Сохранить]** позволяет сохранить ключевую пару во внешнем файле (***.ecc).** По нажатию кнопки **[Загрузить]** произойдет загрузка ранее сохраненной ключевой пары из файла **(*.ecc).**

Чтобы использовать алгоритм **ECC160** при автозащите (опция установки типа ключа**)** необходимо указывать в качестве параметра опции файл с открытым ключом. Кнопка **[Экспорт в bin-файл автозащиты]** позволяет сохранить открытый ключ в файле (имя по умолчанию – **PublicKey.bin).**

Кнопка **[Экспорт в исходный код]** сохраняет ключевую пару в заголовочном файле на C++ (имя по умолчанию – **EccKeySource.h).**

***

После редактирования определителя (или ключа **ECC160** для одноименного алгоритма) и нажатия на кнопку **[Завершить]** диалог создания алгоритма закрывается, и новый алгоритм появляется в списке полей образа. При этом **GrdUtil.exe** автоматически присваивает алгоритму числовое имя (порядковый номер) *(для защищенных ячеек и аппаратных алгоритмов действует единая нумерация)* и корректирует границу аппаратных запретов с учетом добавленного алгоритма.

Теперь остается записать образ в ключ, и созданный аппаратный алгоритм можно будет использовать.