Скрипт добавления пакета открытых ключей в скрипт подписи deb-пакетов

Рекомендуется к deb пакетам с программным обеспечением, имеющим цифровую подпись, добавлять в зависимость пакет с открытым ключом, обеспечивающим работу ПО с цифровой подписью в режиме замкнутой программной среды.

Принцип хранения пакетов открытых ключей в скрипте подписи пакетов основан на использовании строки-маркера последней строки скрипта вида "`# Script EOF`".

Примеры deb пакетов открытых ключей

Добавление пакетов открытых ключей из директорий keyring-1.* выполняется с помощью скрипта update-sign-script.sh:

```
./update-sign-script.sh sign-deb-package.sh
```

Удаление пакетов открытых ключей из скрипта подписи выполняется с помощью скрипта clean-sign-script.sh:

```
./clean-sign-script.sh sign-deb-package.sh
```

Для извлечения из своего тела необходимого пакета в скрипте подписи sign-deb-package.sh используется команда:

```
sed -e '1,/^# Script EOF/d' < $0 | tar --strip-components=1 -zxv -C ${DIR_SIGNED} "${key_package}"
```

Она обеспечивает передачу на вход tar тела скрипта после строки "`# Script EOF`" с последующим извлечением данных из соответствующей директории в архиве с учетом удаления первого компонента пути из имени извлеченного файла. Таким образом, при формировании подписи в ОС версии 1.4 приведенный пример скрипта выполнит извлечение файла-пакета с открытым ключом из директории keyring-1.4 архива `tar.gz` из состава скрипта в директорию подписанных пакетов.

Для задания в скрипте подписи идентификаторов (отпечатков) используемых закрытых ключей используется переменная `key_id`. Директория пакета открытого ключа из встроенного в скрипт архива определяется переменной `key_package`. См. блок кода:

```
case "${os_release}" in
            "SE 1.4 (smolensk)")
                    key_id="12345678"
                    key_package="keyring-1.4"
                    ;;
            "SE 1.5 (smolensk)")
                    key_id="87654321"
                    key_package="keyring-1.5"
                    ;;
            *)      key_id="'unknown'"
                    echo "Unsupported OS release ('${os_release}')."
                    exit 1
                    ;;
    esac
```

sign-deb-package.sh

update-sign-script.sh

clean-sign-script.sh

Примеры deb пакетов открытых ключей:

keyring-1.4.tar.gz

keyring-1.5.tar.gz