

Руководителям организаций,  
участвующих в электронном  
обмене с Банком России  
(рассылка по списку)

О размещении ППИ СКЗИ на  
официальном сайте Банка России

Информационное сообщение ВН-16-4-6-1/9287 от 03.11.2023

Центр эксплуатации платежной системы Департамента информационных технологий Банка России (далее – ЦЭПС ДИТ) информирует участников обмена (далее - УО), о размещении на сайте Банка России [www.cbr.ru/development/mciris](http://www.cbr.ru/development/mciris) в подразделе «Прикладные программные интерфейсы СКЗИ» раздела «Информация о новых версиях программного обеспечения» обновленной версии прикладного программного интерфейса средства криптографической защиты информации (далее - ППИ СКЗИ):

- ППИ СКАД «Сигнатура» версия 6 для платформы Java («iface.6.rar»);
- ППИ СКЗИ «Янтарь» версия 6 на платформах Java (сборка 6.0.6.0) («iface.6.0.6.0.rar»)

Содержание изменений приведено в приложение к настоящему информационному сообщению.

ЦЭПС ДИТ обращает внимание УО, что в папке из архива «\*.rar» содержится файл «hash.txt» и архив «\*.zip». Файл «hash.txt» содержит список контролируемых файлов ППИ СКЗИ и хэш-код, рассчитанный по алгоритму вычисления хэш-функции в соответствии с ГОСТ Р 34.11-2012.

Архив создан с помощью программы WinRAR 6.23.

ЦЭПС ДИТ напоминает о том, что при тиражировании ППИ СКЗИ в адрес УО с использованием автоматизированной системы «Транспортный шлюз Банка России для обмена платежными и финансовыми сообщениями с клиентами Банка России (ТШ КБР)» будут направлены два информационных сообщения –

уведомительное (о тиражировании новых версий ППИ СКЗИ) и дополнительное, в котором будут даны рекомендации по проверке целостности ППИ СКЗИ.

Данное сообщение будет размещено на сайте Банка России [www.cbr.ru/development/mcirabis](http://www.cbr.ru/development/mcirabis) в подразделе «Прикладные программные интерфейсы СКЗИ» раздела «Информация о новых версиях программного обеспечения».

Контактные данные Единой службы поддержки пользователей Департамента информационных технологий:

многоканальный телефон - 8 (495) 957-80-01;

адрес электронной почты - [helpdeskmci@cbr.ru](mailto:helpdeskmci@cbr.ru).

Заместитель директора Департамента -  
директор Центра эксплуатации  
платежной системы Департамента  
информационных технологий

М.Н. Шашлов

Содержание изменений в ППИ СКАД «Сигнатура» версия 6 для платформы Java:

- типы всех полей классов, используемых для хранения значений времени в формате `time_t`, заменены на `int` на `long`;

- идентификаторы всех указанных выше полей классов заменены посредством добавления к ним суффикса `Ex`;

- описанные выше изменения касаются следующих классов и полей:

```
public static class certificate_t:
public long notBeforeEx;
public long notAfterEx;
public long notBeforePrivateEx;
public long notAfterPrivateEx;
public static class reycefb_t:
public long rpvertimeEx;
public static class crt t:
public long lastUpdateEx;
public long nextUpdateEx;
public static class verify_policy_param_t:
public long check_timeEx;
public static class sign_status_t:
public long timeEx;
public static class tsp_verify_result_t:
public long timeEx;
public static class omsp_verify_result_t:
public long revtimeEx;
public long thisupdEx;
public long nextupdEx;
public static class cms_siginf_t:
public long signingTimeEx;
public static class sign_info_t:
public long timeEx;
```

- описанные выше изменения приводят к тому, что плавный переход на обновленный Java API невозможен. Для внедрения обновленного Java API необходима доработка и пересборка прикладного программного обеспечения

## Содержание изменений в документации

В документе ВАМБ.00115-06 33 01 «Руководство программиста» изменено описание классов, используемых для хранения значений времени в формате `time_t` в подразделах 1.8, 1.9, п. 1.15.1, подразделе 1.20, пп. 1.24.1, 1.25.1, 1.26.1.

### Содержание изменений в ППИ СКЗИ «Янтарь» версия 6 на платформах

#### Java:

- типы всех полей классов, используемых для хранения значений времени в формате `time_t`, заменены на `int` на `long`;
- идентификаторы всех указанных выше полей классов заменены посредством добавления к ним суффикса `Ex`;
- описанные выше изменения касаются следующих классов и полей:

```
public static class certificated_t
public long notBeforeEx;
public long notAfterEx;
public long notBeforePrivateEx;
public long notAfterPrivateEx;
public static class revcert_t:
public long revtimeEx;
public static class crl_t:
public long lastUpdateEx;
public long nextUpdateEx;
public static class verify_policy_param_t:
public long check_timeEx;
public static class sign_status_t:
public long timeEx;
public static class tsp_verify_result_t:
public long timeEx;
public static class ocsp_verify_result_t:
public long revtimeEx;
public long thisupdEx;
public long nextupdEx;
public static class cms_signif_t:
public long signingTimeEx;
public static class sign_info_t:
public long timeEx;
```

- описанные выше изменения приводят к тому, что плавный переход на обновленный Java API невозможен. Для внедрения обновленного Java API необходима доработка и пересборка прикладного программного обеспечения

#### Содержание изменений в документации

В документе ВАМБ.00116-06 33 01 «Руководство программиста» изменено описание классов, используемых для хранения значений времени в формате `time_t` в подразделах 1.4.9 - 1.4.12.