**V.6. Изменения, связанные с актуализацией версии сертифицированного средства криптографической защиты информации**

**Приложение № 5.6**

|  |  |  |
| --- | --- | --- |
| **Инициатор:** АО «АТС».  **Обоснование:** актуализация версии сертифицированного средства криптографической защиты информации (СКЗИ) «КриптоПро CSP».  **Дата вступления в силу:** 1 августа 2018 года. |  |  |

**Предложения по изменениям и дополнениям в** СОГЛАШЕНИЕ О ПРИМЕНЕНИИ ЭЛЕКТРОННОЙ ПОДПИСИ В ТОРГОВОЙ СИСТЕМЕ ОПТОВОГО РЫНКА (Приложение № Д 7 **к Договору о присоединении к торговой системе оптового рынка)**

|  |  |  |
| --- | --- | --- |
| **№**  **пункта** | **Редакция, действующая на момент**  **вступления в силу изменений** | **Предлагаемая редакция**  (изменения выделены цветом) |
| **1.10** | **Средство электронной подписи** – сертифицированное средство криптографической защиты информации (СКЗИ) «КриптоПро CSP» версии 3.6 и выше, обеспечивающее реализацию следующих функций: создание электронной подписи, проверку электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи. | **Средство электронной подписи** – сертифицированное средство криптографической защиты информации (СКЗИ) «КриптоПро CSP», обеспечивающее реализацию следующих функций: создание электронной подписи, проверку электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи. |
| **5.1** | Стороны принимают в качестве средства электронной подписи при выполнении функций создания ЭП в электронном документе с использованием ключа ЭП, подтверждения с использованием ключа проверки ЭП подлинности ЭП в электронном документе, создания ключей ЭП и ключей проверки ЭП использовать средство криптографической защиты информации «КриптоПро CSP» версии 3.6 и выше (далее по тексту – СКЗИ). | Стороны принимают в качестве средства электронной подписи при выполнении функций создания ЭП в электронном документе с использованием ключа ЭП, подтверждения с использованием ключа проверки ЭП подлинности ЭП в электронном документе, создания ключей ЭП и ключей проверки ЭП использовать сертифицированное средство криптографической защиты информации «КриптоПро CSP» версии 4.0 и выше (далее по тексту – СКЗИ). |
| **5.3** | Стороны обязуются использовать копии СКЗИ версии 3.6 и выше, полученные законным путем. | Стороны обязуются использовать копии сертифицированных СКЗИ, полученные законным путем. |

**Предложения по изменениям и дополнениям в** СОГЛАШЕНИЕ О ПРИМЕНЕНИИ ЭЛЕКТРОННОЙ ПОДПИСИ В ТОРГОВОЙ СИСТЕМЕ ОПТОВОГО РЫНКА (Приложение № Д 7 **к Договору о присоединении к торговой системе оптового рынка)**

**Действующая редакция**

*Приложение 4*

*к Правилам ЭДО СЭД КО*

1. **Версии программного обеспечения используемого в электронном документообороте коммерческого оператора**

|  |  |  |
| --- | --- | --- |
|  | **Программное обеспечение** | **версии/спецификации/стандарты** |
| 1. | Программное средство криптографической защиты информации «КриптоПро CSP» | Версии 3.6 и выше |
| 2. | **HTTP/1.1** (*HyperText Transfer Protocol* ) — протокол прикладного уровня передачи данных | RFC 2616 |
| 3. | **HTTPS** (Hypertext Transfer Protocol Secure) – расширение протокола HTTP, поддерживающее шифрование | RFC 2818 |
| 4. | **SNTP** (*Simple Network Time Protocol*) – протокол синхронизации времени по компьютерной сети | RFC 2030 «Simple Network Time Protocol (SNTP) Version 4». |
| 5. | **SMTP** (*Simple Mail Transfer Protocol*) – это сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP | RFC 2821 |
| 6. | Обмен почтовыми сообщениями | RFC 822 «Standard for the format of arpa internet text messages» |
| 7. | Формирование текста электронного сообщения | RFC 1341 - MIME (Multipurpose Internet Mail Extensions): Mechanisms for Specifying and Describing the Format of Internet Message Bodies» |
| 8. | Формирование ЭП электронного сообщения | «RFC 2311 - S/MIME Version 2 Message Specification» |
| 9. | Формирование ЭП в виде отдельных файлов | PKCS#7 Cryptographic Message Syntax Standard |
| 10. | Microsoft Notepad | Версии 6.1 или более поздней |
| 11. | Adobe Reader | Версии 6.0 или более поздней |
| 12 | Microsoft Word | Microsoft Office 2007 или более поздней версии Microsoft Office |
| 13. | Microsoft Excel | Microsoft Office 2007 или более поздней версии Microsoft Office |
| 14. | WinRAR | Версии 3.71 или более поздней |
| 15. | Windows Internet Explorer | Версии 11 |

**Предлагаемая редакция**

*Приложение 4*

*к Правилам ЭДО СЭД КО*

1. **Версии программного обеспечения используемого в электронном документообороте коммерческого оператора**

|  |  |  |
| --- | --- | --- |
|  | **Программное обеспечение** | **версии/спецификации/стандарты** |
| 1. | Сертифицированное программное средство криптографической защиты информации «КриптоПро CSP» | Версии 4.0 и выше |
| 2. | **HTTP/1.1** (*HyperText Transfer Protocol* ) — протокол прикладного уровня передачи данных | RFC 2616 |
| 3. | **HTTPS** (Hypertext Transfer Protocol Secure) – расширение протокола HTTP, поддерживающее шифрование | RFC 2818 |
| 4. | **SNTP** (*Simple Network Time Protocol*) – протокол синхронизации времени по компьютерной сети | RFC 2030 «Simple Network Time Protocol (SNTP) Version 4». |
| 5. | **SMTP** (*Simple Mail Transfer Protocol*) – это сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP | RFC 2821 |
| 6. | Обмен почтовыми сообщениями | RFC 822 «Standard for the format of arpa internet text messages» |
| 7. | Формирование текста электронного сообщения | RFC 1341 - MIME (Multipurpose Internet Mail Extensions): Mechanisms for Specifying and Describing the Format of Internet Message Bodies» |
| 8. | Формирование ЭП электронного сообщения | «RFC 2311 - S/MIME Version 2 Message Specification» |
| 9. | Формирование ЭП в виде отдельных файлов | PKCS#7 Cryptographic Message Syntax Standard |
| 10. | Microsoft Notepad | Версии 6.1 или более поздней |
| 11. | Adobe Reader | Версии 6.0 или более поздней |
| 12 | Microsoft Word | Microsoft Office 2007 или более поздней версии Microsoft Office |
| 13. | Microsoft Excel | Microsoft Office 2007 или более поздней версии Microsoft Office |
| 14. | WinRAR | Версии 3.71 или более поздней |
| 15. | Windows Internet Explorer | Версии 11 |