Приложение № 10

к Регламенту Поставщика сертификационных услуг

в области применения усиленной квалифицированной

электронной подписи

**Технологические характеристики**

**программно-технического комплекса Поставщика сертификации высшего уровня**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Критерий** | **Технологические характеристики** |
|  | Способы сертификации | Сетевая, иерархическая |
|  | Множественные службы сертификации | Без ограничений |
|  | Множественные службы регистрации | Без ограничений |
|  | Масштабируемость | Количество выпущенных сертификатов без ограничений |
|  | Формат сертификата и списка отозванных сертификатов | В соответствии с IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profil, ETF RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profil и IETF RFC 3739 Qualified Certificates Profile, ITU-T X.509, версия 2, стандарту SM ISO CEI 9594-8:2014 Информационные технологии. Взаимодействии открытых систем. Направляющие линии. Структура сертификата открытых ключей и атрибута или рекомендации IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profil, ETF RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profil и IETF RFC 3739 Qualified Certificates Profile. |
|  | Дополнения сертификата | Х.509 v 3, PKIX, FPKX, Web, SET, VPN, определяемые пользователем |
|  | Формат сертификата ограниченного использования | В соответствии с RFC 3039 |
|  | Формат атрибутного сертификата для авторизации | В соответствии с RFC 3281 |
|  | Политика применения сертификата и структура регламента | В соответствии с RFC 2527 Certificate Policy and Certification Practices FrameworkIETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework |
|  | Протоколы управления сертификатами | В соответствии с RFC 2510 Certificate Management Protocols (CMP) |
|  | Запрос на сертификацию | В соответствии с RFC 2986 Certification Request Syntax Specification |
|  | Протокол определения статуса сертификата | В соответствии с RFC 2560 Online Certificate Status Protocol (OCSP) |
|  | Методы отзыва сертификата | Посредством распространения списков отозванных сертификатов, протокол OCSP |
|  | Получение из реестра сертификатов и списка отозванных сертификатов | В соответствии с RFC 2585 HTTP/FTP OperationsАвтоматическая рассылка списков отозванных сертификатов по электронной почте |
|  | Управление сертификатами на базе сообщений управления сертификатами | В соответствии с RFC 2797 Certificate Management Messages over CMS (CM3) |
|  | Алгоритмы и идентификаторы для профилей сертификатов и списка отозванных сертификатов CAC PKIX | В соответствии с RFC 3279 (бывший RFC 2528) Algorithms and Identifiers for Internet X.509 Public Key Infrastructure Certificate and CRL Profile |
|  | Поддерживаемые алгоритмы электронной подписи | RFC3447 – Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1;  |
|  | Поддерживаемые алгоритмы функции хеширования | RFC3174 – US Secure Hash Algorithm 1 (SHA1) |
|  | Протоколы сервера сертификации и проверки достоверности данных | В соответствии с RFC 3029 Data Validation and Certification Server Protocols |
|  | Эксплуатационные протоколы инфраструктуры открытых ключей | В соответствии с RFC 2559 LDAP v2 |
|  | Схема поддержки PKIX в среде LDAP v2 | В соответствии с RFC 2587 LDAP v2 Schema |
|  | Коммуникации с клиентом (подсистемы получения сертификатов) | PKCS#10/7, PKCS#12, посредством считывания PIN-кода, по электронной почте, SSL, PKIX-CMP |
|  | Коммуникации между подсистемами сертификации и регистрации | Подписанные сообщения, PKIX-CMP |
|  | Механизмы регистрации | Личное присутствие пользователя, посредством Web, электронная почта, VPN соединение |
|  | Поддержка каталогов | Собственный каталог или поддержка любого каталога LDAP v2 и v3 |
|  | Поддержка смарт-карт | Стандарты: ISO 7816-1/2/3, PKCS#11, PC/SC, другие распространенные стандарты смарт-карт |
|  | Восстановление ключей | Возможность резервирования администраторских и пользовательских ключей |
|  | Протоколы проставления меток времени | В соответствии с IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) , RFC 5816 ESSCertIDv2 Update for RFC 3161 |
|  | Управление безопасностью жизненного цикла сертификации | Отказоустойчивость при проверке статуса сертификатаГарантированность обслуживания пользователейСоздание системы контроля над всеми действиями администратора с сертификатом, контроль целостности сертификата |
|  | Обеспечение целостности баз данных сертификатов, владельцев сертификатов и др. | Использование концепции надежной компьютерной базы, дискреционное и мандатное управление доступом, метки, повторное использование объекта, достоверный маршрут; создание системы резервного копирования |
|  | Обеспечение безопасности закрытых ключей | Безопасное создание, хранение, использование, многофакторная система аутентификации |
|  | Контроль безопасности  | Регистрация и контроль событий в подсистемахВедение, обработка и проверка контрольных журналовОбеспечение защиты контрольных журналов от несанкционированных изменений и уничтожения |