Приложение 1

к Политике применения атрибутных сертификатов

Удостоверяющего центра

ОАО «Белорусская универсальная товарная биржа»

**Профиль формата атрибутного сертификата,**

**издаваемого центром атрибутных сертификатов ОАО «Белорусская универсальная товарная биржа» для участников процедур закупок, проводимых в электронном формате**

**(набор обязательных полей входящих в состав атрибутного сертификата)**

Атрибутный сертификат в соответствии с СТБ 34.101.67-2014 состоит из трех базовых компонентов:

**AttributeCertificate ::= SEQUENCE {**

**attrCertifnfo AttributeCertificateInfo;**

**signatureAlgorithm AlgorithmIdentifier;**

**signatureValue BIT STRING}**

1. Состав базового компонента **attrCertifnfo**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Поле (компонент) | OID | Описание поля (компонента) | Тип поля | Постоянные значения | |
| **version** |  | Версия формата сертификата по x.509.  В текущей локализации используется Version3 | постоянное | ***1*** | |
| **holder** |  |  |  |  | |
| baseCertificateID |  | Содержит:  issuerName (имя эмитента);  serialNumber (серийный номер СОК, для которого выпущен АС) | *изменяемое* |  | |
| **issure** |  |  |  |  | |
| Набор полей и их значений совпадает с набором и значениями полей компонента **subject** в СОК ЦАС, издавшем данный атрибутный сертификат | | | | | |
| **signature** |  |  |  | |  |
| algorithm |  | Идентификатор алгоритма, который УЦ использовал для выработки ЭЦП для данного сертификата, в данном профиле **bign-with-hbelt** согласно СТБ 34.101.45-2013 | постоянное | | ***1.2.112.0.2.0.34.101.45.12*** |
| parameters |  | Параметры алгоритма. Значение поля ***NULL*** | постоянное | | ***NULL\*\**** |
| **serialNumber** | 2.5.4.5  id-at-serialNumber | Серийный номер, который однозначно определяет АС среди всех сертификатов, выпущенных ЦАС, присваивается ЦАС, является уникальным | *изменяемое* | |  |
| **attrCertValidityPeriod** |  |  |  | |  |
| notBeforeTime |  | Дата начала срока действия СОК  тип – GeneralizedTime | *изменяемое* | |  |
| afterBeforeTime |  | Дата окончания срока действия СОК  тип – GeneralizedTime | *изменяемое* | |  |
| **attributes** |  |  |  | |  |
| organizationName | 2.5.4.10  id-at-organizationName | Наименование организации – для юридических лиц, наименование ИП – для ИП. | *изменяемое* | |  |
|  | 2.5.4.3 | Краткое наименование организации – для юридических лиц, наименование ИП – для ИП. | *изменяемое* | |  |
| organizationUnitName | 2.5.4.11  id-at-organizationalUnitName | Наименование структурного подразделения | *изменяемое* | |  |
| title | 2.5.4.12 | Должность | *изменяемое* | |  |
|  | 2.5.4.6 | Страна | *изменяемое* | |  |
| stateOrProvincename | 2.5.4.8 | Наименование области | *изменяемое* | |  |
| localityName | 2.5.4.7 | Название населенного пункта | *изменяемое* | |  |
| streetAddress | 2.5.4.9 | Информация о юридическом адресе организации | *изменяемое* | |  |
| УНП (регистрационный номер) | 1.3.6.1.4.1.12656.104.3 | Учетный номер плательщика (УНП), присвоенный юридическому лицу МНС РБ | *изменяемое* | |  |
| Неструктурированное поле | 2.5.4.45 | Неструктурированное поле  Для юридического лица: UNP=УНП/OKPO=ОКПО/EGR=ЕГР  Для индивидуального предпринимателя: UNP=УНП | *изменяемое* | |  |
|  | 2.5.4.4 | Фамилия владельца сертификата | *изменяемое* | |  |
|  | 2.5.4.41 | Имя и Отчество владельца сертификата | *изменяемое* | |  |
|  | 1.3.6.1.4.1.12656.5.3 | Личный номер (данные из документа, удостоверяющего личность) | *изменяемое* | |  |
|  | 1.2.840.113549.1.9.1 | Электронная почта | *изменяемое* | |  |
|  |  |  |  | |  |
|  | 1.2.643.6.3.1.1 | Использование на электронных площадках отобранных для проведения аукционов в электронной форме | *изменяемое* | |  |
|  | 1.2.643.6.3.1.3.1 | Участник размещения заказа | *изменяемое* | |  |
|  | 1.2.643.6.3.1.2.1 | Юридическое лицо | *изменяемое* | |  |
|  | 1.2.643.6.3.1.2.3 | Индивидуальный предприниматель | *изменяемое* | |  |
|  | 1.2.643.6.3.1.4.3 | Специалист с правом подписи контракта | *изменяемое* | |  |
|  | 1.2.643.6.3.1.4.1 | Администратор организации | *изменяемое* | |  |
|  | 1.2.643.6.3.1.4.2 | Уполномоченный специалист | *изменяемое* | |  |
| **extensions** |  |  |  | |  |
| authorityKeyIdentifier | 2.5.29.35 | Уникальный идентификатор открытого ключа ЦАС (представляет хэш-значение **SHA-1**  **20 байт**  согласно 1) п. 6.2.1.2 СТБ 34.101.19-2012) | *изменяемое* | |  |
| CRLDistributionPoints | 2.5.29.31 | Точка распространения СОС | *изменяемое* | |  |
| acceptablePrvilegePolicies | 2.5.29.57 | Политика применения АС.  (п. 9.2.6 СТБ 34.101.67-2014) | *изменяемое* | | 1.2.112.1.2.1.1.1.3.2.3 |
| AuthorityInfoAccess | 1.3.6.1.5.5.7.1.1 | Доступ к информации ЦАС |  | |  |
| caIssuers | 1.3.6.1.5.5.7.48.2 | Содержит URL-адрес сертификата УЦ | *изменяемое* | |  |

2. Состав базового компонента **signatureAlgorithm**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Поле (компонент) | OID | Описание поля (компонента) | Тип поля | Постоянные значения |
| **signatureAlgorithm** |  |  |  |  |
| **algorithm** |  | Идентификатор алгоритма, который ЦАС использовал для подписи сертификата, в данном профиле **bign-with-hbelt** согласно СТБ 34.101.45-2013 | постоянное | ***1.2.112.0.2.0.34.101.45.12*** |
| **parameters** |  | Параметры алгоритма. Значение поля ***NULL\*\**** | постоянное | ***NULL\*\**** |

3. Состав базового компонента **signatureValue**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Поле (компонент) | OID | Описание поля (компонента) | Тип поля | Постоянные значения |
| **signatureValue** |  | Значение электронной цифровой подписи, вычисленное ЦАС |  |  |

\* – поле не обязательно для заполнения

\*\* – соответствуют требованиям СТБ 34.101.45-2013