# КАРТОЧКА ЭЛЕКТРОННОГО ДОКУМЕНТА

## Концепция совершенствования применения ЭЦП.pdf

**Дата и время формирования**
2021.01.01 13:45:00 UTC+6

**Информационная система или сервис**
Шаблон карточки ЭД

**Содержание:**



**Перечень вложенных файлов:**

| | | |
|---|---|---|
| 1. | Концепция совершенствования применения ЭЦП.pdf | Подлинник электронного документа |
| 2. | 1.cms | ЭЦП, БЕРИКОВ АЛИМЖАН |
| 3. | 2.cms | ЭЦП, ПЕТРЕНКО СЕРГЕЙ |

*При формировании карточки электронного документа была автоматически выполнена процедура проверки ЭЦП в соответствии с положениями Приказа Министра по инвестициям и развитию Республики Казахстан «Об утверждении Правил проверки подлинности электронной цифровой подписи».*

*Карточка электронного документа — это файл в формате PDF, состоящий из визуально отображаемой части и вложенных файлов.*

*Визуально отображаемая часть карточки электронного документа носит исключительно информативный характер и не обладает юридической значимостью.*

*Многие программы для просмотра PDF поддерживают вложенные файлы, позволяют просматривать их и сохранять как обычные файлы. Среди них Adobe Acrobat Reader и браузер Firefox.*

*В соответствии с Законом Республики Казахстан «Об электронном документе и электронной цифровой подписи», подлинник электронного документа обладает юридической значимостью в том случае, если он подписан ЭЦП и были выполнены проверки подписи в соответствии с утвержденными правилами.*

*Это шаблон карточки электронного документа, все данные в карточке синтетические, в том числе ФИО, реквизиты и цифровые подписи.*

*ВНИМАНИЕ! Остерегайтесь мошенников! При получении электронных документов, обязательно выполняйте проверку подписей! Злоумышленники могут пробовать подделывать или менять визуально отображаемую часть карточки, так как она не защищена от изменения цифровой подписью.*

# Концепция совершенствования применения ЭЦП

С каждым годом в нашу жизнь всё больше проникают электронные документы — документы, в которых информация представлена в электронно-цифровой форме и удостоверена посредством электронной цифровой подписи. Однако, имеется ряд препятствий, сдерживающих этот процесс. Ниже представлено описание некоторых из них, а также предложены варианты их устранения.



## Квитанция метки времени (TSP)

Согласно подпункту 6 пункта 6 Правил проверки подлинности электронной цифровой подписи, утверждённых Приказом Министра по инвестициям и развитию Республики Казахстан от 9 декабря 2015 года №1187, проверка квитанции метки времени осуществляется для электронных документов долговременного хранения.

К сожалению, в законодательстве РК нами не было обнаружено определение термина «электронный документ долговременного хранения». Анализ показал, что чаще всего под долговременным хранением документов в нормативных правовых актах нашей страны понимается срок, превышающий 10 лет.

Вместе с тем, срок действия регистрационных свидетельств, содержащих ключи электронной цифровой подписи составляет 1 год для незащищённых (файловых) носителей и 3 года для защищённых носителей.

Кроме того, известны случаи, когда подписание электронного документа выполнялось за несколько дней до истечения срока действия ключей ЭЦП.

В соответствии с подпунктом 1 пункта 6 вышеуказанных Правил, необходима проверка срока действия регистрационного свидетельства. Таким образом, если на момент проверки ЭЦП срок действия регистрационного свидетельства истёк и при подписании не была сформирована квитанция метки времени, будет определён отрицательный результат проверки ЭЦП и регистрационного свидетельства.

Исходя из вышеизложенного, принимая во внимание всё большее проникновение электронных документов в повседневную жизнь, считаем необходимым внести изменения в вышеуказанные Правила, определив формирование и проверку квитанции метки времени обязательной для всех электронных документов.

## Возможность скачивания электронных документов из информационной системы

В настоящее время пользователям судебного кабинета при скачивании судебных актов в электронном виде и портала электронного правительства при скачивании результата оказания услуги «Электронные обращения» (ответов на обращение) не предоставляется возможность скачать вышеуказанные файлы в виде электронного документа. Т.е. в скачиваемых данных отсутствует электронная цифровая подпись. Это не позволяет проверить техническими средствами подлинность электронного документа.

Таким образом, в случае изменения или удаления файла в информационной системе (ошибочного или намеренного), нет возможности доказать, что скачанный ранее файл является подлинником электронного документа, который был подписан ЭЦП. Это, при определённых ситуациях, может создавать элементы коррупционной составляющей.

При соблюдении требований законодательства, в вышеуказанных информационных системах уже должны храниться электронные документы (т.е. документы, подписанные ЭЦП). Предоставление возможности скачивать информацию в виде электронного документа (т.е. с ЭЦП), позволит увеличить прозрачность отправления правосудия и взаимоотношений физических и юридических лиц с государственными органами.

Аналогичный подход предлагается применять для всех информационных систем, где допускается скачивание электронных документов. Например, системы электронного документооборота, enbek.kz (трудовые договоры).

Это позволит осуществлять обмен электронными документами без участия информационных систем, в которых данные документы хранились изначально. При этом, сохранятся все свойства и преимущества электронных документов.

## Возможность загрузки в информационную систему ранее подписанного электронного документа

В настоящее время, при взаимодействии с информационной системой, предполагающей подписание электронных документов, подписание происходит непосредственно перед загрузкой электронного документа в информационную систему. При этом, подписант не контролирует, что именно он подписывает. Т.е. подписанту может быть показан один документ, а отправлен на подпись совсем другой, как в ситуации с АО «Отбасы Банк».

В определённых случаях такой подход может иметь серьёзные негативные последствия для подписанта.

Данную ситуацию можно решить разрешив загружать на стороне информационной системы ранее подписанные электронные документы. Т.е. сначала подписант локально подписывает электронный документ (без взаимодействия с информационной системой), а только потом загружает уже подписанный электронный документ.

## Подписание и проверка ЭЦП средствами NCALayer без взаимодействия с информационной системой

ПО, находящееся в составе NCALayer, позволяет формировать и проверять электронную цифровую подпись. Однако, в настоящее время, отсутствует функционал делать это непосредственно в интерфейсе NCALayer, без взаимодействия в браузере с информационной системой, и сохранять подписанный электронный документ локально, на компьютере подписанта.

Предлагается реализовать данный функционал в NCALayer и добавить соответствующие пункты в имеющееся всплывающее меню.

## Карточка электронного документа

Данная спецификация описывает **карточку электронного документа** — ориентированный на людей композитный формат хранения подлинников электронных документов и ЭЦП под ними, основанный на стандартизованном и широко используемом формате файлов PDF, а так же распространённом в Республике Казахстан формате упаковки цифровых подписей CMS (CAdES).

Отличительные особенности формата **карточки электронного документа**:
- один файл включает в себя все необходимые данные для долгосрочного хранения электронных документов;
- содержит в себе достаточный объём информации для проверки цифровых подписей под электронным документом в любой момент времени без необходимости взаимодействовать с какими-либо информационными системами, сервисами, в том числе с сервисами УЦ;
- визуально отображаемая часть может включать в себя визуализацию подписанного электронного документа и визуализацию цифровых подписей.

Спецификация разрабатывалась с учётом следующих принципов, которые также должны служить основным ориентиром при разработке следующих версий спецификации:
- **удобство для людей** — нельзя ущемлять права участников информационного взаимодействия,

отправителей и получателей электронных документов, не являющихся специалистами в области информационных технологий, поэтому технические средства, в том числе и форматы хранения данных, следует разрабатывать так, чтобы они были информативны, наглядны и понятны;
- **прозрачность** — люди имеют право знать что именно было подписано ЭЦП, то есть что именно является электронным документом в терминологии Закона РК «Об электронном документе и электронной цифровой подписи»;
- **целостность** — необходимо сохранять всю информацию, необходимую для полноценной проверки ЭЦП в любой момент времени после подписания электронного документа;
- **открытость и доступность** — при разработке спецификации следует отдавать предпочтение тем технологиям, стандартам, спецификациям и программному обеспечению, которые общедоступны, общеприняты и не ставят участников информационного взаимодействия в зависимость от закрытых проприетарных разработок.

Спецификация **карточки электронного документа** разработана с прицелом на такие сценарии обработки и хранения электронных документов, в которых участвуют люди и которые не привязаны к конкретным информационным системам, к примеру:
- экспорт электронных документов из информационных систем;
- обмен электронными документами людьми без применения информационных систем, к примеру, по электронной почте, с использованием мессенджеров или через корпоративное облачное хранилище;
- импорт электронных документов в информационные системы;
- архивное хранение электронных документов вне информационных систем.

Информационные системы, реализующие данную спецификацию, образуют единое информационное пространство с общим форматом передачи данных, участвовать в котором могут не только машины, но и обычные люди.

## Формат хранения данных

**Карточка электронного документа** — это основной файл (PDF, версия спецификации не ниже 1.4), логически состоящий из двух компонент:
- визуально отображаемая часть;
- вложенные файлы.

**Визуально отображаемая часть** — это текстовая и графическая информация в PDF-файле. Она предназначена для того, чтобы любой человек, получивший **карточку электронного документа**, мог быстро ознакомиться с содержимым документа используя стандартные средства, имеющиеся в большинстве потребительских информационно-вычислительных устройств, таких как компьютеры, ноутбуки, смартфоны, планшеты и электронные книги. Визуально отображаемая часть **предназначена только для поверхностного ознакомления** и **не обладает юридической значимостью**, так как она не защищена техническими средствами от изменения или искажения злоумышленниками.

**Вложенные файлы** — это подлинник электронного документа и электронные цифровые подписи под ним. Можно утверждать что подлинник электронного документа обладает юридической значимостью в соответствии с законодательством РК после того, как была удостоверена его целостность путём выполнения проверок ЭЦП под ним. Для выполнения проверок ЭЦП

требуются специальные технические средства. В настоящее время разработаны библиотека с открытым исходным кодом и прототип ПО на основе этой библиотеки, позволяющий формировать **карточку электронного документа** и осуществлять проверку. Предполагается, что по мере принятия спецификации всё большим количеством организаций и информационных систем, будет появляться всё больше различных инструментов, позволяющих выполнять проверки подписей.

## Требования к ЭЦП

Данная спецификация определяет набор требований к электронным цифровым подписям для того, чтобы упростить процедуру импорта электронных документов в информационные системы.

Спецификация допускает исключительно те цифровые подписи, которые могут считаться равнозначными собственноручным подписям в соответствии с законодательством Республики Казахстан. В частности, это означает что подписи должны быть сформированы с применением сертификатов (регистрационных свидетельств), выпущенных аккредитованными удостоверяющими центрами Республики Казахстан.

Дополнительные требования к ЭЦП:
- цифровые подписи должны быть упакованы в формат CMS (RFC 5652) — один поддерживаемый формат упростит анализ криптографических структур и снизит вероятность ошибок, а, следовательно, и уязвимостей;
- в каждом CMS, в поле `certificates` структуры `SignedData` должен быть приведён сертификат (регистрационное свидетельство) подписавшей стороны, то есть тот, открытый ключ в котором соответствует закрытому ключу, использованному для подписания;
- подписанные данные не должны быть включены в CMS ( `external signatures` в терминах RFC 5652), то есть поле `eContent` должно отсутствовать в `EncapsulatedContentInfo` — подписанные данные включены в карточку электронного документа в виде отдельного файла;
- метка времени TSP (RFC 3161) должна быть встроена в CMS в виде неподписанного атрибута `1.2.840.113549.1.9.16.2.14` (RFC 3161, APPENDIX A — Signature Time-stamp attribute using CMS);
- подтверждение валидного статуса сертификата, использованного при подписании, должно быть предоставлено одним из следующих образов:
- в виде ответа OCSP (RFC 6960), с успешным статусом проверки сертификата, который должен быть встроен в CMS в виде неподписанного атрибута `1.2.840.113549.1.9.16.2.24` (RFC 5126, 6.3.4. revocation-values Attribute Definition), в этом случае разница между меткой времени TSP и моментом формирования OCSP ответа не должна превышать 5 (пять) минут;
- в виде списка отозванных сертификатов CRL (RFC 5280), подтверждающего статус сертификата, который должен быть встроен в CMS в виде неподписанного атрибута `1.2.840.113549.1.9.16.2.24` (RFC 5126, 6.3.4. revocation-values Attribute Definition), в этом случае метка времени TSP должна находиться в промежутке между значениями из `thisUpdate` и `nextUpdate`. В случае, если УЦ, выпустивший сертификат, поддерживает разностные CRL (RFC 5280, 5 CRL and CRL Extensions Profile), то, помимо базового CRL, обязательно должен быть предоставлен и разностный CRL.

Для снижения объёмов передаваемых и хранимых данных, настоятельно рекомендуется предоставлять подтверждение валидности статусов сертификатов в виде OCSP ответов.

## Визуально отображаемая часть

Визуально отображаемая часть служит для быстрого ознакомления с содержимым электронного документа и ЭЦП под ним. Она состоит из блоков, размещённых в следующей последовательности:
- информационный блок (обязательно);
- визуализация электронного документа (опционально);
- визуализация всех имеющихся ЭЦП под электронным документом (опционально).

Общие требования к визуально отображаемой части:
- формат страницы A4, рекомендуется портретная ориентация;
- отступы слева 30 мм, сверху 20 мм, справа 10 мм, снизу 20 мм;
- рекомендуется использовать легко читаемые свободно распространяемые шрифты;
- рекомендуется придерживаться диапазона размеров шрифтов 8–14 для основных данных;
- нумерация страниц начинается с первой страницы, порядковый номер страницы и общее количество страниц отображается в нижнем колонтитуле справа, начиная со второй страницы;
- начиная со второй страницы, нижний колонтитул слева должен содержать слова `Карточка электронного документа`.

### Информационный блок

Информационный блок следует размещать в начале **карточки электронного документа**, он должен содержать следующие данные:
- строку `Карточка электронного документа`;
- наименование электронного документа;
- (опционально) краткое описание электронного документа;
- дату формирования данной карточки электронного документа;
- время формирования данной карточки электронного документа с обязательным указанием часового пояса. Рекомендуется приводить время к часовому поясу UTC+6 (часовой пояс города Нур-Султан);
- наименование информационной системы или сервиса, в котором была сформирована данная карточка электронного документа;
- содержание визуально отображаемой части карточки с указанием страниц;
- перечень вложенных файлов с указанием имен файлов и примечаний;
- упоминание о том, что в процессе формирования данной карточки информационная система выполнила проверки подписей и проверила целостность подписанных данных;
- пояснение о том, что такое карточка электронного документа;
- пояснение о том, что такое подлинник электронного документа;
- пояснение о том, как выполнить проверку подписи с использованием той информационной системы или сервиса, в котором была сформирована карточка;
- предостережение о том, что визуально отображаемая часть не защищена от модификаций и не имеет юридической значимости.

Информационный блок может занимать одну или более страниц в зависимости от детализации содержания и количества вложенных файлов.

### Визуализация электронного документа

**Карточка электронного документа** может включать в себя визуализацию электронного документа. Решение о том, включать визуализацию электронного документа в карточку или нет, рекомендуется предоставлять пользователю, запрашивающему формирование карточки. Визуализацию следует размещать на отдельных страницах.

Визуализация электронного документа должна отображать фактическое содержимое электронного документа, так как она предназначена не для того, чтобы пояснить, разъяснить или дополнить содержимое электронного документа, а для того, чтобы предоставить человеку возможность ознакомиться с фактическим содержимым электронного документа. К примеру:
- визуализация офисных документов (DOC, DOCX, ODT, XLS, XLSX, ODS и т.п.) не должна существенно отличаться от того, как эти документы отображают такие приложения, как MS Office, LibreOffice и OpenOffice и подобные;
- визуализация PDF файлов не должна существенно отличаться от того, как эти файлы отображают такие программы, как Adobe Acrobat Reader, Chrome, Firefox и подобные;
- визуализация простых тестовых документов (TXT, XML, JSON, YAML и т.п.) должна представлять из себя текст этих документов, разрешено добавлять переносы каретки для того, чтобы длинные строки не вылезали за края страницы;
- визуализацию HTML документа со встроенными таблицами стилей CSS рекомендуется выполнять в таком виде, как этот документ отобразили бы широко распространенные браузеры Chrome, Firefox или Safari.

Запрещается формировать визуализацию таким образом, чтобы она существенно отличалась от содержимого электронного документа, отображаемое стандартными (распространенными) программами для просмотра и редактирования этого типа данных. К примеру:
- запрещено выполнять визуализацию XML файла путем наполнения шаблона оформления данными из XML файла в том случае, если шаблон содержит уточняющую информацию (пояснения, человекочитаемые наименования полей, какую-либо интерпретацию значений из XML файла), так как подобная визуализация не будет соответствовать содержимому подлинника электронного документа, а будет являться его субъективной интерпретацией и в значительной степени зависеть от того, какой шаблон использовался.

Верхний колонтитул каждой страницы визуализации электронного должен содержать слова `Визуализация электронного документа`.

Поверх визуализации электронного документа на каждой странице визуализации необходимо разместить хорошо читаемый водяной знак `Копия электронного документа`.

### Визуализация ЭЦП под электронным документом

**Карточка электронного документа** может включать в себя визуализации подписей. Следует либо включать визуализации всех вложенных подписей, либо не включать их вовсе. Не допустимо приводить визуализации тех подписей, которые не вложены в карточку. Решение о

том, включать визуализации подписей в карточку или нет, рекомендуется предоставлять пользователю, запрашивающему формирование карточки.

Визуализацию каждой подписи следует размещать на отдельной странице.

Визуализация каждой подписи должна включать в себя следующую информацию в текстовом человекочитаемом виде:
- ФИО подписавшего;
- ИИН подписавшего, либо другой государственный идентификатор;
- (для сертификатов юридических лиц) наименование организации, сотрудником которой является подписавший;
- (для сертификатов юридических лиц) БИН организации, либо другой государственный идентификатор;
- содержимое поля subject в текстовом виде в соответствии с RFC 4514 (опционально);
- серийный номер сертификата (регистрационного свидетельства);
- дата и время начала и окончания срока действия сертификата (регистрационного свидетельства), рекомендуется использовать тот же самый часовой пояс, что был указан на первой **странице** информационного блока карточки электронного документа;
- шаблон, на основании которого был выпущен сертификат (регистрационное свидетельство) в человекочитаемом виде и в виде OID;
- информация о разрешённых использованиях ключа (keyUsage) в человекочитаемом виде;
- информация о разрешённых расширенных использованиях ключа (extendedKeyUsage) в человекочитаемом виде и в виде OID;
- информация об организации, выпустившей сертификат (регистрационное свидетельство) — содержимое поля `issuer` в текстовом виде в соответствии с RFC 4514;
- дату и время формирования подписи с указанием часового пояса (за момент формирования цифровой подписи следует принимать момент, приведенный в метке времени TSP), рекомендуется использовать тот же самый часовой пояс, что был указан на первой странице информационного блока карточки электронного документа;
- информация о наличии метки времени TSP:
- дата и время формирования метки времени с указанием часового пояса, рекомендуется использовать тот же самый часовой пояс, что был указан на первой странице информационного блока карточки электронного документа;
- серийный номер сертификата (регистрационного свидетельства), использованного для подписания метки времени;
- содержимое поля `subject` сертификата (регистрационного свидетельства), использованного для подписания метки времени, в текстовом виде в соответствии с RFC 4514;
- содержимое поля `issuer` сертификата (регистрационного свидетельства), использованного для подписания метки времени, в текстовом виде в соответствии с RFC 4514;
- (если подтверждением статуса сертификата является OCSP ответ) информация об OCSP ответе:
- дата и время формирования OCSP ответа;
- статус сертификата `CertStatus` из OCSP ответа;
- серийный номер сертификата (регистрационного свидетельства), использованного для подписания OCSP ответа;
- содержимое поля `subject` сертификата (регистрационного свидетельства), использованного для подписания OCSP ответа, в текстовом виде в соответствии с RFC 4514;

- содержимое поля `issuer` сертификата (регистрационного свидетельства), использованного для подписания OCSP ответа, в текстовом виде в соответствии с RFC 4514;
- (если подтверждением статуса сертификата является CRL) информация из базового CRL:
- дата и время формирования CRL, `thisUpdate` ;
- дата и время окончания срока действия CRL, `nextUpdate` ;
- информация об отсутствии, либо наличии серийного номера сертификата в CRL;
- серийный номер сертификата (регистрационного свидетельства), использованного для подписания CRL;
- содержимое поля `subject` сертификата (регистрационного свидетельства), использованного для подписания CRL, в текстовом виде в соответствии с RFC 4514;
- содержимое поля `issuer` сертификата (регистрационного свидетельства), использованного для подписания CRL, в текстовом виде в соответствии с RFC 4514;
- (если подтверждением статуса сертификата является CRL и УЦ поддерживает разностные CRL) информация из разностного CRL:
- дата и время формирования CRL, `thisUpdate` ;
- дата и время окончания срока действия CRL, `nextUpdate` ;
- информация об отсутствии серийного номера сертификата в CRL, либо уведомление о том, что он присутствует там с кодом причины `removeFromCRL` ;
- серийный номер сертификата (регистрационного свидетельства), использованного для подписания CRL;
- содержимое поля `subject` сертификата (регистрационного свидетельства), использованного для подписания CRL, в текстовом виде в соответствии с RFC 4514;
- содержимое поля `issuer` сертификата (регистрационного свидетельства), использованного для подписания CRL, в текстовом виде в соответствии с RFC 4514.

Визуализация подписи может включать в себя подпись, закодированную в виде набора QR кодов. Решение о том, включать QR коды в визуализацию подписи или нет, рекомендуется предоставлять пользователю, запрашивающему формирование карточки.

Каждый QR код из набора должен кодировать JSON структуру содержащую, как минимум, следующие данные (переносы каретки и отступы не обязательны, приведены в описании для наглядности):

```
{
  "signId": 9,
  "total": 7,
  "index": 1,
  "data": ""
}
```

- `signId` — идентификатор подписи, необходим для того, чтобы можно было однозначно определить к какой подписи относится данный QR код в том случае, если документ включает в себя QR коды нескольких подписей;
- `total` — общее количество QR кодов, кодирующих данную подпись, позволит удостовериться в том, что все QR коды из набора считаны успешно;
- `index` — номер данного QR в наборе QR кодов, кодирующих данную подпись, необходим

для восстановления корректного порядка частей;
- `data` — часть строки `Base64` с данными.

Допустимо дополнять структуру дополнительными данными.

Генерацию набора QR кодов следует осуществлять следующим образом:
- каждая подпись должна иметь уникальный идентификатор (уникальный, как минимум, в контексте формируемой карточки электронного документа);
- выбрать версию QR кода и уровень коррекции ошибок (https://www.qrcode.com/en/about/version.html), рекомендуется использовать версию `25` и уровень коррекции ошибок `M`;
- определить максимальную длину строки, которую можно закодировать в QR код с выбранными параметрами;
- сформировать оценочную JSON структуру, заполнив поле `signId` корректными данными, поля `total` и `index` установив в `0`, поле `data` в `""`;
- определить длину строки оценочной JSON структуры;
- вычислить максимальную длину подстроки с данными по формуле `"максимальная длина строки" – "длина строки оценочной JSON структуры" – 10`, где 10 символов зарезервированы под значения полей `total` и `index`;
- байты подписи упаковать как файл в ZIP архив методом DEFLATE, для формирования имени архивируемого файла использовать формат `signId.cms`, где `signId` — это уникальный идентификатор подписи;
- закодировать полученный ZIP архив в строку `Base64`;
- разбить строку `Base64` на подстроки в соответствии с определенной ранее максимальной длинной подстроки с данными;
- для каждой подстроки сформировать JSON структуру;
- текстовое представление каждой JSON структуры закодировать в изображение QR кода, рекомендуется использовать формат PNG, под каждую клетку QR кода выделять не менее 2-х пикселей.

## Вложенные файлы

Вложенные файлы следует встраивать в основной PDF файл как встроенные потоки файлов (`Embedded File Streams` в терминологии спецификации PDF), которые были добавлены в версии 1.4 в 2001 году. Для встраивания следует использовать элементы `EmbeddedFiles` словаря `Name Dictionary`, ассоциирующие вложенный файл со всем документом. Данный подход выбран исходя из соображений его полной поддержки популярными приложениями для просмотра PDF-файлов (например, Adobe Acrobat Reader, браузер Firefox).

Так как встроенные потоки файлов в основном PDF-файле записаны один после другого, то можно говорить о последовательности вложенных файлов. Первым вложенным файлом всегда должен быть подлинник электронного документа. За ним должны следовать цифровые подписи в последовательности их формирования. За момент формирования цифровой подписи следует принимать момент, приведённый в метке времени TSP.

Все вложенные файлы должны быть адекватно именованы, то есть должны иметь читаемое имя файла. Настоятельно рекомендуется указывать расширение для упрощения идентификации типов файлов программным обеспечением и пользователями. Это необходимо для того, чтобы пользователи всегда имели возможность беспрепятственно сохранять вложенные файлы на файловые системы своих устройств. Допустимо не указывать расширения файлов только в тех случаях, когда это нарушает сложившиеся практики или противоречит стандартам, но нужно иметь в виду, что отсутствие расширения у файла усложняет идентификацию типа файла и противоречит принципу **удобство для людей**.

Имена файлов должны быть в кодировке UTF–8. Не допускается использование других кодировок (таких как Windows–1251), так как это может вызывать проблемы при сохранении вложенных файлов на файловую систему в некоторых операционных системах.

Вложенные файлы не должны быть исполняемыми файлами (https://helpx.adobe.com/acrobat/using/attachments-security-risks-reader-acrobat.html#attachments_as_security_risks_in_reader_and_acrobat).

Настоятельно рекомендуется выполнять проверку вкладываемых файлов на наличие вирусов и других угроз в процессе формирования карточки.

## Проверка подписей и целостности данных в карточке электронного документа

При получении **карточки электронного документа** информационная система должна удостовериться в целостности подлинника электронного документа путём проверки всех вложенных подписей под ним. Эту процедуру информационной системе следует выполнять при каждом случае получения карточки из внешнего источника, в том числе:
- при импорте карточки полученной от пользователя;
- при получении карточки из сторонней информационной системы;
- при запросе проверки карточки пользователем или информационной системой.

Разработчикам информационных систем важно помнить о том, что достоверной можно считать информацию исключительно во вложенных файлах и только после проверки цифровых подписей.

Подготовительные шаги перед выполнением проверки подписей:
- удостовериться в том, что в качестве карточки электронного документа был передан PDF-файл;
- извлечь первый вложенный файл, считать его электронным документом;
- в том случае, если в качестве электронного документа был передан исполняемый файл, рекомендуется прекратить проверку с ошибкой;
- рекомендуется проверить электронный документ на наличие вирусов и вредоносного программного обеспечения;
- извлечь все остальные вложенные файлы, считать их файлами цифровых подписей.

Для подтверждения юридической значимости электронного документа, проверку подписей под ним следует выполнять в соответствии с законодательством РК, в частности, с Правилами проверки подлинности электронной цифровой подписи, утверждёнными Приказом Министра по

инвестициям и развитию Республики Казахстан «Об утверждении Правил проверки подлинности электронной цифровой подписи».

Дополнительно, следует выполнять следующие проверки, невыполнение любой из которых должно помечать подпись как не прошедшую проверку:
- удостовериться в том, что подписи упакованы в CMS;
- удостовериться в том, что в подписях присутствуют метки времени в соответствии с разделом «Требования к ЭЦП»;
- в каждой метке времени проверить подпись сервиса, сформировавшего ее, построить и проверить цепочку сертификатов от сертификата сервиса до одного из доверенных сертификатов УЦ;
- удостовериться в том, что для каждой подписи присутствует доказательство валидного статуса сертификата (регистрационного свидетельства) в соответствии с разделом «Требования к ЭЦП»;
- в том случае, если в качестве доказательства приведен CRL, проверить, выпускает ли УЦ, выпустивший сертификат, использованный для подписания электронного документа, разностные CRL, в том случае, если выпускает, удостовериться в наличии разностного CRL;
- проверить подписи соответствующих сервисов под ответами OCSP и CRL, построить и проверить цепочки сертификатов от сертификатов сервисов до одного из доверенных сертификатов УЦ;
- удостовериться в том, что доказательство валидного статуса сертификата приведено на момент времени, указанный в приведенной метке времени, то есть:
- в том случае, если в качестве доказательства приведен ответ OCSP, разница между меткой времени TSP и моментом формирования OCSP ответа не должна превышать 5 (пять) минут;
- в том случае, если в качестве доказательства приведен CRL, метка времени TSP должна находиться в промежутке между значениями из `thisUpdate` и `nextUpdate`.

В том случае, если хотя бы одна из вложенных подписей не прошла проверку, следует считать все данные в карточке недостоверными.

**Подпись №1**

Дата формирования подписи:
**19.05.2021 01:01:51 UTC+6**

Подписал(а):
**БЕРИКОВ АЛИМЖАН, ИИН 009988776655**

Шаблон:
**Юридическое лицо (1.2.398.3.3.2.1)**

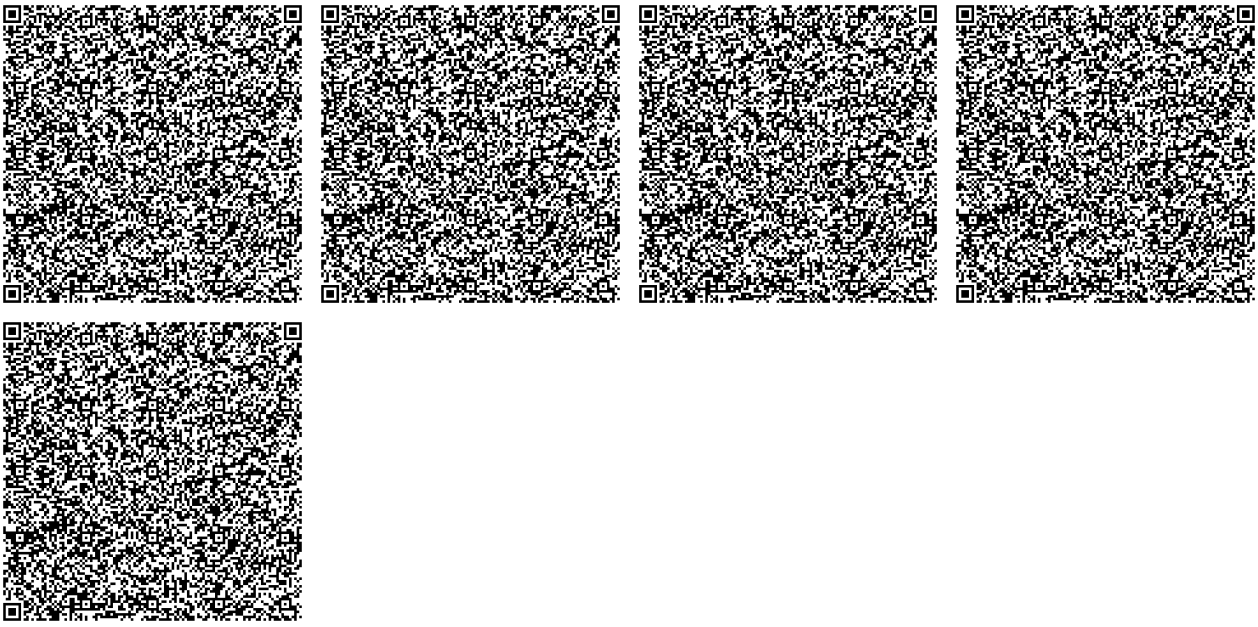
Представляет организацию:
**ТОВАРИЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "Компания", БИН 112233445566**

Допустимое использование:
**Цифровая подпись (digitalSignature)**
**Неотказуемость (nonRepudiation)**
**Защищенная электронная почта (ЭЦП) (1.3.6.1.5.5.7.3.4)**
**Юридическое лицо (1.2.398.3.3.4.1.2)**
**Первый руководитель (1.2.398.3.3.4.1.2.1)**

Субъект: CN=БЕРИКОВ АЛИМЖАН,SURNAME=БЕРИКОВ,SERIALNUMBER=IIN009988776655,C=KZ,L=АЛМАТЫ,ST=АЛМАТЫ,O=ТОВАРИЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "Компания",OU=BIN112233445566,GIVENNAME=СЕРИКОВИЧ,E=SUBJECT@MAIL.KZ
Серийный номер: 182ed2cc442dc0addde8831ec3cb94253115e6d9
С: 01.01.2021 01:01:51 UTC+6
По: 01.01.2022 01:01:51 UTC+6
Издатель: C=KZ,CN=ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST)

Метка времени: 19.05.2021 01:01:51 UTC+6
Субъект: CN=TSA SERVICE,SERIALNUMBER=IIN761231300313,C=KZ,L=НУР-СУЛТАН,ST=НУР-СУЛТАН,O=АКЦИОНЕРНОЕ ОБЩЕСТВО "НАЦИОНАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ",OU=BIN000740000728
Серийный номер: 3d9de56d5f279c5d06ec7d8b83aa50bdeb437d34
Издатель: C=KZ,CN=ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA)

OCSP: good
Сформирован: 19.05.2021 01:01:52 UTC+6
Субъект: CN=OCSP RESPONDER,SERIALNUMBER=IIN761231300313,C=KZ,L=НУР-СУЛТАН,ST=НУР-СУЛТАН,O=АКЦИОНЕРНОЕ ОБЩЕСТВО "НАЦИОНАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ",OU=BIN000740000728
Серийный номер: 48bfe5df76c4a094ad7dc7ad2b8293103c08e433
Издатель: C=KZ,CN=ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST)



**Подпись №2**

Дата формирования подписи:
**19.05.2021 02:01:51 UTC+6**

Подписал(а):
**ПЕТРЕНКО СЕРГЕЙ, ИИН 009988776655**

Шаблон:
**Физическое лицо (1.2.398.3.3.2.3)**

Допустимое использование:
**Цифровая подпись (digitalSignature)**
**Неотказуемость (nonRepudiation)**
**Защищенная электронная почта (ЭЦП) (1.3.6.1.5.5.7.3.4)**
**Физическое лицо (1.2.398.3.3.4.1.1)**

Субъект: CN=ПЕТРЕНКО СЕРГЕЙ,SURNAME=ПЕТРЕНКО,SERIALNUMBER=IIN009988776655,C=KZ,L=АЛМАТЫ,ST=АЛМАТЫ,GIVENNAME=ГРИГОРЬЕВИЧ
Серийный номер: 1a9d886d5f27977d06ec7d8b44aa50bdeb436634
С: 01.01.2021 01:01:51 UTC+6
По: 01.01.2022 01:01:51 UTC+6
Издатель: C=KZ, CN=ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA)

Метка времени: 19.05.2021 02:01:51 UTC+6
Субъект: CN=TSA SERVICE,SERIALNUMBER=IIN761231300313,C=KZ,L=НУР-СУЛТАН,ST=НУР-СУЛТАН,O=АКЦИОНЕРНОЕ ОБЩЕСТВО "НАЦИОНАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ",OU=BIN000740000728
Серийный номер: 3d9de56d5f279c5d06ec7d8b83aa50bdeb437d34
Издатель: C=KZ,CN=ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA)

OCSP: good
Сформирован: 19.05.2021 02:01:50 UTC+6
Субъект: CN=OCSP RESPONDER,SERIALNUMBER=IIN761231300313,C=KZ,L=НУР-СУЛТАН,ST=НУР-СУЛТАН,O=АКЦИОНЕРНОЕ ОБЩЕСТВО "НАЦИОНАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ",OU=BIN000740000728
Серийный номер: 48bfe5df76c4a094ad7dc7ad2b8293103c08e433
Издатель: C=KZ,CN=ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (RSA)