Условия использования сертификатов сертифицированной услуги Smart-ID

Перевод оригинального документа "Terms and Conditions for Use of Certificates of Qualified Smart-ID" осуществлен Удостоверяющим центром SK ID Solutions AS.

Действительны с 01.01.2018

Определения и сокращения

Термин/Сокращение	**Определение**
Аутентификация	Уникальная идентификация личности человека путем проверки его/ее заявленных идентификационных данных.
Сертификат аутентификации	Сертификат предназначен аутентификации.
CA	Certificate Authority - организация, отвечающая за распределение сертификатов
Сертификат	Открытый ключ, вместе с дополнительной информацией, указанный в профиле сертификата, исключающий возможность подделки посредством шифрования с использованием закрытого ключа организации, отвечающей за распределение сертификатов, которая его выдала.
Certificate Authority (CA)	Часть структуры SK, ответственная за выдачу и проверку электронных сертификатов и списков аннулированных сертификатов с электронной подписью.
CP	SK ID Solutions AS - Политика применения сертификата для сертифицированной услуги Smart-ID.
CPS	SK ID Solutions AS – Стандартная практика сертификации EID-SK.
Пункт Обслуживания клиентов	Пункт обслуживания клиентов принимает заявления на Сертификаты Q Smart-ID и передает запросы на Сертификаты в SK. Пункт обслуживания клиентов также принимает заявления аннулирования Сертификатов и передает их в SK.

Горячая линия Пункта обслуживания клиентов	Горячая линия управляется Пунктом обслуживания клиентов. Горячая линия пункта обслуживания клиентов принимает запросы об аннулировании Сертификатов Q Smart-ID от Подписчиков, кто получили Q Smart-ID через Пункт Обслуживания клиентов.
eIDAS	Постановление (ЕС) № 910/2014 Европейского Парламента и Совета от 23.07.2014 относительно электронной идентификации и трастовых услуг для электронных сделок/операций на внутреннем рынке и отменяющая Директива 1999/93/ЕС.
Поставщик электронной услуги	Третье лицо, которое использует услуги, предоставляемые системой Smart-ID для аутентификации Подписчиков, а также в целях предоставления Подписчикам разрешения электронным образом подписывать документы или сделки.
Поставщик идентификационной услуги	Организация, предоставляющая средства электронной аутентификации, ответственная за создание электронной идентификационной информации, которая используется для выдачи сертификатов Q Smart-ID. Поставщик идентификационной услуги проверен поставщиком услуги Smart-ID относительно соблюдения Требований, действующих в отношении поставщиков идентификационной услуги для квалифицированных сертификатов.
Служба помощи	Служба помощи предоставляет пользователям поддержку для решения проблем, связанных с использованием услуги Q Smart-ID. Служба помощи принимает запросы на аннулирование сертификатов услуги Q Smart-ID от Подписчиков.
OCSP	Интернет-протокол для проверки статуса сертификата
OID	Идентификатор, используемый для уникального наименования объекта.
PIN-код	Код активации для закрытого ключа.
Закрытый ключ	Ключ в паре ключей, который должен храниться в секрете владельцем пары ключей, используемый для создания электронных подписей и/или расшифровки электронных записей или файлов, которые были зашифрованы при помощи соответствующего открытого ключа. В системе Smart-ID значение самого "закрытого ключа" никогда не генерируется, и "закрытый ключ" существует только лишь в виде его компонентов.

Открытый ключ	Ключ в паре ключей, который владелец соответствующего закрытого ключа может публично разглашать, используемый проверяющими сторонами для проверки электронных подписей, создаваемых при помощи соответствующего закрытого ключа владельца, и/или для зашифровки сообщений, чтобы их можно было расшифровать только при помощи соответствующего закрытого ключа владельца.
Q Smart-ID	Smart-ID, содержащая одну пару Сертификатов, которая состоит из Сертификата аутентификации и Сертификата квалифицированной электронной подписи и соответствующих закрытых ключей.
Квалифицированная электронная подпись	Квалифицированная электронная подпись согласно постановлению eIDAS.
Проверяющая сторона	Лицо/организация, которые используют информацию, содержащуюся в сертификате.
SK	SK ID Solutions AS, поставщик сертификационной услуги.
SK PS	SK ID Solutions AS, Стандартная практика оказания трастовых услуг.
SLA	Договор о сервисном обслуживании
Smart-ID	Smart-ID - это новое поколение электронной идентификации, которое обеспечивает Подписчиков способами электронной аутентификации и проставления квалифицированной электронной подписи.
Портал Smart-ID	Точка взаимодействия с системой Smart-ID для Подписчика, к которой можно получить доступ через веб-браузер. Портал обеспечивает доступ к функциям регистрации и управления учетной записью Smart-ID.
Поставщик услуги Smart-ID	Организация, которая несет законную ответственность за систему Smart-ID. SK ID Solutions AS является поставщиком Smart-ID.

Система Smart-ID	Техническая и организационная среда, которая позволяет осуществлять электронную аутентификацию и ставить электронные подписи в электронной среде. Система Smart-ID предоставляет услуги, которые позволяют Подписчикам (владельцам учетной записи) подтверждать подлинность их личности для поставщиков электронных услуг, ставить электронные подписи и управлять своими учетными записями в системе Smart-ID.
Подписчик	Физическое лицо, которому выдаются сертификаты для использования услуги Q Smart-ID.
Условия	Настоящий документ, в котором содержится описание обязательств и сфер ответственности Подписчика при использовании сертификатов.

1. **Общие условия**
   1.1. В настоящих условиях содержится описание основных принципов и практики, которых придерживается SK, перечисленных в CP для услуги Q Smart-ID, CPS и SK PS (например, заявление о разглашении информации).
   1.2. Настоящие условия регулируют использование Подписчиками Сертификатов и представляют собой договор между Подписчиком и SK, имеющий обязательную юридическую силу.
   1.3. Подписчик должен ознакомиться с Условиями и согласиться с ними.
   1.4. SK имеет право в любое время вносить поправки в Условия, если у SK появится обоснованная необходимость внесения таких поправок. Информация относительно поправок будет публиковаться на Интернет-странице https://sk.ee/en.
   1.5. Подписчик ходатайствует о регистрации Q Smart-ID аккаунта самолично, за исключением несовершеннолетнних подписчиков, которые должны ходатайствовать о регистрации Q Smart-ID через его/её законного представителя. Q Smart-ID не выдается представителю.

2. **Получение сертификата**
   2.1. После предоставления ходатайства о выдаче сертификата Q Smart-ID, Подписчик подтверждает, что он/она прочитали и согласились с Условиями. Соответствующее подтверждение считается получением сертификата Q Smart-ID.
   2.2. В случае ввода нового ключа сертификатов, Подписчик подтверждает, что он/она прочитали и согласились с Условиями.

3. **Тип сертификата, процедура проверки и использование сертификатов**

Тип сертификата	Использование	Применимая и опубликованная политика сертификации	OID	Краткое содержание
Сертификаты для Smart-ID	Сертификат на квалифицированную электронную подпись предназначен для: создания квалифицированных электронных подписей, соответствующих eIDAS.	SK ID Solutions AS – политика сертификации для сертифицированной услуги Smart-ID, опубликована на https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.17.2	онлайн-атрибут (1.3.6.1) атрибут частного юридического лица (4) атрибут зарегистрированного предприятия, присвоенный менеджером частного предприятия IANA(1) атрибут SK в регистре IANA (10015) атрибут сертификационной услуги (17.2)
		ETSI EN 319 411-2 Policy: QCP-n	0.4.0.194112.1.0	itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1)qcp-natural(0)
	Сертификат аутентификации предназначен для: аутентификации	SK ID Solutions AS – политика сертификации для сертифицированной услуги Smart-ID, опубликована на https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.17.2	онлайн-атрибут (1.3.6.1) атрибут частного юридического лица (4) атрибут зарегистрированного предприятия, присвоенный менеджером частного предприятия IANA(1) атрибут SK в регистре IANA (10015) атрибут сертификационной услуги (17.2)
		ETSI EN 319 411-1 Policy: NCP+	0.4.0.2042.1.2	itu-t(0) identified-Organisation(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)

3.1. Использование сертификатов Подписчика запрещено в перечисленных ниже целях:

3.1.1. незаконная деятельность (в т.ч. кибератаки и попытки взломать сертификат системы Smart-ID);
3.1.2. выдача новых сертификатов и информации, касающейся срока действия сертификата;
3.1.3. предоставление возможности другим сторонам использовать закрытый ключ Подписчика;
3.1.4. предоставление возможности использования сертификата, выданного для проставления электронной подписи, автоматическим способом;
3.1.5. использование сертификата, выданного для проставления электронной подписи, для подписи документов, которая может повлечь за собой нежелательные последствия (в т.ч. подпись таких документов в целях тестирования).

3.2. Принадлежащие Подписчику сертификаты аутентификации нельзя использовать для создания квалифицированных электронных подписей, соответствующих eIDAS.

4. Доверительные пределы

4.1. Сертификат вступает в силу в дату, указанную в сертификате.
4.2. Сертификат теряет силу в дату, указанную в сертификате, или после аннулирования сертификата.
4.3. Журналы аудита сохраняются локально в течение не менее 10 лет. Физические или цифровые архивные записи, касающиеся сертификатов, регистрационной информации и запросов или ходатайств относительно аннулирования, хранятся не менее 10 лет после истечения срока действия соответствующего сертификата.

5. Права и обязанности Подписчика

5.1. Подписчик имеет право на подачу ходатайства о выдаче сертификата Q Smart-ID.
5.2. Подписчик обязан:
5.2.1. согласиться с Условиями;
5.2.2. соблюдать требования, установленные SK;
5.2.3. использовать свой закрытый ключ и сертификат в соответствии с Условиями, в т.ч. с действующими соглашениями, перечисленными в ст. 10, а также с законами Эстонской Республики и Европейского союза;
5.2.4. убедиться в том, что закрытый ключ Подписчика используется под его/ее наблюдением;
5.2.5. предоставить в систему Smart-ID правдивую и достоверную информацию;
5.2.6. оповещать поставщика услуги Smart-ID о достоверной информации в течение разумного срока в случае изменения его/ее личной информации;
5.2.7. незамедлительно сообщать в SK о возможности неправомочного использования его/ее закрытого ключа и аннулировать сертификаты;

5.2.8. незамедлительно аннулировать сертификаты, если Подписчик утратил контроль над своим закрытым ключом.

6. Права и обязанности SK

6.1. SK обязан:

6.1.1. предоставлять сертификационную услугу в соответствии с действующими соглашениями, перечисленными в ст. 10, и соответствующим законодательством;

6.1.2. вести учет выданных сертификатов и их сроков действия;

6.1.3. обеспечивать безопасность внутренних процедур;

6.1.4. предоставлять возможность проверки срока действия сертификатов 24 часа в сутки;

6.1.5. ключи сертификатов защищены модулями аппаратной защиты (т.е. HSM) и находятся под исключительным контролем SK;

6.1.6. ключи сертификатов, используемые в ходе предоставления сертификационной услуги, активируются на базе совместного управления.

7. Обязательство проверяющих сторон проверки статуса сертификата

7.1. Проверяющая сторона изучает риски и обязательства, связанные с получением сертификата. Риски и обязательства перечислены в CPS и в CP.

7.2. Если к сертификату или к электронной подписи прилагается недостаточно доказательств относительно срока действия сертификата, Проверяющая сторона проверяет срок действия сертификата на основании услуг по проверке сертификатов, предлагаемых SK в момент использования сертификата или проставления квалифицированной электронной подписи.

7.3. Проверяющая сторона соблюдает ограничения, указанные в сертификате, и должна убедиться в том, что сделка/операция, подлежащая приемке, соответствует CPS и CP.

7.4. SK гарантирует доступность услуг, связанных с проверкой статусов сертификатов, 24 часа в сутки, 7 дней в неделю, с минимальным уровнем доступности 99.44% в год с запланированным простоем системы, не превышающим 0,28% ежегодно.

7.5. SK предлагает услуги OCSP для проверки статуса сертификата. Доступ к услуге осуществляется посредством HTTP протокола.

7.6. Проверяющая сторона проверяет срок действия сертификата посредством проверки срока действия сертификатов относительно OCSP. SK предлагает OCSP со следующими возможностями проверки:

7.6.1. Услуга OCSP является бесплатной и общедоступной на сайте http://aia.sk.ee/eid2016;

7.6.2. SK предлагает услугу OCSP с улучшенным SLA согласно соглашению и прейскуранту.

7.6.3. Электронный адрес (URL) услуги OCSP включен в сертификат в поле AIA (Доступ к информации об УЦ) в соответствии с профилем сертификата.

8. **Обязанности других участников**

8.1. Поставщик услуги Smart-ID гарантирует, что:

8.1.1. он соблюдает процедуры генерирования и хранения ключей, которые находятся в его пользовании, описание которых приводится в CPS;

8.1.2. он соблюдает условия оплаты, описания которых приводится в CPS;

8.1.3. он предоставляет достоверные сертификаты и достверную информацию о статусах сертификатов.

8.2. Поставщик услуги Smart-ID имеет право лишить организацию статуса поставщика идентификационной услуги, если он получит доказательства того, что поставщик идентификационной услуги не соблюдает Требования, действующие в отношении поставщиков идентификационной услуги, для сертифицированных сертификатов.

8.3. Поставщик идентификационной услуги обеспечивает соответствие Требованиям, действующим в отношении поставщиков идентификационной услуги, для сертифицированных сертификатов.

9. **Ограниченная гарантия и оговорка об ограничении ответственности**

9.1. Подписчик несет единоличную ответственность за сохранность его/ее закрытого ключа.

9.2. Подписчик несет единоличную и полную ответственность за любые последствия цифровой идентификации и проставления цифровой подписи с использованием его/ее сертификатов как во время срока действия Сертификатов, так и после окончания их срока действия.

9.3. Подписчик несет единоличную ответственность за любой ущерб, причиненный вследствие неисполнения или ненадлежащего исполнения его/ее обязательств, указанных в условиях использования сертификатов и/или в законах Эстонской Республики.

9.4. Подписчик знает, что цифровые подписи , проставленные на основании сертификатов, срок действия которых истек или которые были аннулированы, недействительны.

9.5. SK гарантирует, что:

9.5.1. сертификационная услуга предоставляется в соответствии с CPS, CP и соответствующим законодательством Эстонской Республики и Европейского союза;

9.5.2. ключи сертификатов защищены модулями аппаратной защиты (т.е. HSM) и находятся под исключительным контролем SK;

9.5.3. ключи сертификатов используются для обеспечения активации сертификационной услуги на базе совместного управления;

9.5.4. SK имеет обязательные договоры страхования для всех услуг SK для обеспечения компенсации ущерба, причиненного нарушением SK своих обязательств;

9.5.5. SK информирует всех Подписчиков до того, как SK прекратит предоставление услуги выдачи сертификатов, и обязуется хранить документацию, связанную с прекращением услуги выдачи

сертификатов, и необходимую информацию в соответствии с описанием процесса, приведенного в CPS.

9.6. SK не несет ответственности за:

9.6.1. секретность закрытых ключей Подписчиков, любое злоупотребление сертификатами или ненадлежащие проверки сертификатов или неправильные решения Проверяющей стороны или любые последствия каких-либо ошибок или упущений в проверках сертификатов;

9.6.2. неисполнение своих обязательств, если такое неисполнение было вызвано ошибками или проблемами с безопасностью в контролирующем органе, в органе, осуществляющем наблюдение за охраной данных, списке доверенных сертификатов или каком-либо другом органе власти;

9.6.3. неисполнение своих обязательств, если неисполнение было вызвано форс-мажорными обстоятельствами.

10. Действующие соглашения, CPS, CP

10.1. Соответствующие соглашения, принципы и стандартные практики, связанные с Условиями использования сертификатов:

10.1.1. SK ID Solutions AS – политика сертификации для сертифицированной услуги Smart-ID, опубликована на https://sk.ee/en/repository/CP/;

10.1.2. SK ID Solutions AS – политика сертификации для EID-SK, опубликована на https://sk.ee/en/repository/CPS;

10.1.3. SK ID Solutions AS - Стандартная практика оказания доверительных услуг, опубликована на: https://sk.ee/en/repository/sk-ps/;

10.1.4. Профиль сертификатов и OCSP для Smart-ID, опубликован на: https://www.sk.ee/en/repository/profiles/;

10.1.5. Принципы защиты данных клиентов https://www.sk.ee/en/repository/data-protection/.

10.2. Текущие версии всех действующих документов имеются в открытом доступе в архиве SK https://www.sk.ee/en/repository/.

11. 10 Политика соблюдения конфиденциальности

11.1. SK соблюдает принципы защиты данных клиента, которые хранятся в архиве SK https://sk.ee/en/repository/data-protection/ и другие законодательные акты Эстонской Республики при обработке личной и регистрационной информации.

11.2. Подписчик знает и соглашается с фактом, что в ходе использования сертификатов для цифровой идентификации, человеку, осуществляющему идентификацию, отправляется сертификат, который содержится в документе Q Smart-ID Подписчика и содержит имя и личный код Подписчика.

11.3. Вся информация, которая стала известна сторонам в ходе предоставления услуг, и которая не предназначена для разглашения (например, информация, которая была известна SK по причине оказания

доверительных услуг), является конфиденциальной. Подписчик имеет право на получение информации от SK о нем/о ней согласно закону.

11.4. SK обеспечивает защиту конфиденциальных данных и информации, предназначенной для внутреннего использования, от несанкционированного разглашения и воздерживается от разглашения такой информации третьим лицам посредством осуществления различных мер контроля за безопасностью.

11.5. SK имеет право разглашать информацию о Подписчике третьему лицу, которое, согласно применимым законам и законодательным актам, имеет право на получение такой информации.

11.6. Кроме того, неперсонализированные статистические данные об услугах SK также считаются общедоступной информацией. SK может публиковать неперсонализированные статистические данные о своих услугах.

12. Условия возмещения

12.1. SK рассматривает ходатайства о возмещении в индивидуальном порядке.

13. Применимое законодательство, жалобы и решение споров

13.1. Сертификационная услуга регулируется юрисдикцией Эстонии и Европейского союза в местоположении, где SK зарегистрирован в качестве CA.

13.2. Все споры между сторонами подлежат разрешению путем переговоров. Если сторонам не удается прийти к дружескому соглашению, спор подлежит разрешению в суде по местоположению SK.

13.3. Другие стороны будут проинформированы о любой претензии или жалобе не позднее, чем в течение 30 календарных дней с момента выяснения основания для претензии, если законом не установлено иное.

13.4. Подписчик или другая сторона могут отправить свою претензию или жалобу по следующему адресу: info@sk.ee.

13.5. Все запросы о разрешении споров следует отправлять с использованием контактной информации, указанной в Условиях.

14. SK и архивные лицензии, трастовые отметки и аудит

14.1. Сертификационная услуга для Q Smart-ID имеет квалификационный статус в Списке доверительных сертификатов Эстонии: https://sr.riik.ee/en/tl.html. Обязательным условием для регистрации является соответствие требованиям действующих постановлений и стандартов.

14.2. Орган, занимающийся оценкой соответствия, аккредитуется согласно Постановлению (ЕС) № 765/2008 в качестве компетентного органа на проведение оценки соответствия квалифицированного поставщика доверительной услуги и квалифицированных доверительных услуг, которые он поставляет.

14.3. Заключения аудиторских проверок или сертификаты, основанные на результатах аудита, т.е. проверки соответствия, проведенной в

соответствии с постановлением eIDAS, а также соответствующее законодательство и стандарты опубликованы на Интернет-странице SK https://www.sk.ee/en/repository/.

15. **Контактная информация**

15.1. Поставщик доверительной услуги

SK ID Solutions AS
Регистрационный код 10747013
Пярну мнт. 141, 11314
Таллинн, ЭСТОНИЯ
(Пн-пт 9.00 - 18.00, восточноевропейское время)
http://www.sk.ee/en
Phone +372 610 1880
Fax +372 610 1881
E-mail: info@sk.ee

15.2. Заявления аннулирования сертификатов Q Smart-ID принимаются 24/7 по следующим контактным данным службы поддержки:

15.2.1. В Эстонии по номеру 9001807 или +372 715 1606;
15.2.2. В Латвии по номеру 1807 или +371 6766 5001;
15.2.3. В Литве по номеру 1807 или +370 6704 1807.

15.3. Заявления аннулирования сертификатов Q Smart-ID принимаются 24/7 по следующим контактным данным горячей линии Пункта обслуживания клиентов:

15.3.1. В Эстонии по номеру +372 6 310 310 (24/7);
15.3.2. В Латвии по номеру +371 67 444 444 (24/7);
15.3.3. В Литве по номеру 1884 или +370 5 268 4444 (понедельник-пятница 8.00 - 20:00, в субботу 9.00 -16:00).

15.4. Заявления аннулирования сертификатов NQ Smart-ID также принимаются через Интернет-портал самообслуживания и/или приложение NQ Smart-ID и/или пункты обслуживания клиентов.

15.5. Информация и контактные данные службы поддержки и портала Smart-ID имеются на Интернет-странице SK https://www.sk.ee/en и https://www.smart-id.com/.