Условия использования сертификатов несертифицированной услуги Smart-ID

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

Действительны с 09.02.2017

Определения и сокращения

Термин	**Определение**
Усовершенствованная электронная подпись	Электронная подпись, которая соответствует требованиям, перечисленным в статье 26 eIDAS.
Аутентификация	Уникальная идентификация личности человека путем проверки его/ее заявленной идентификации.
Сертификат аутентификации	Сертификат предназначен для проверки подлинности.
SK ID Solutions AS, Стандартная практика предоставления доверительных услуг (SK PS)	Стандартная практика, используемая SK в ходе предоставления доверительн услуг.
Сертификат	Открытый ключ, вместе с дополнительной информацией, указанный в профиле сертификата. Считается, что открытый ключ исключает возможность подделки посредством шифрования, используя закрытый ключ организации, отвечающей за распределение сертификатов, которая их выдала.
CA (Certificate Authority; организация, отвечающая за распределение сертификатов)	Часть структуры SK, ответственная за выдачу и проверку электронных сертификатов с электронной подписью.
Certificate Policy (CP)	Политика применения сертификата для несертифицированной услуги Smart-ID.
Профиль сертификата	Профиль сертификата и OCSP для Smart-ID.
Стандартная практика сертификации (CPS)	SK ID Solutions AS - Стандартная практика сертификации NQ-SK
eIDAS	Постановление (ЕС) № 910/2014 Европейского Парламента и Совета от 23.07.2014 относительно электронной идентификации и доверительныхуслуг для электронных сделок/операций на внутреннем рынке и отменяющая Директива 1999/93/ЕС.
Поставщик идентификационной услуги	Организация, предоставляющая средства электронной аутентификации, ответственная за создание электронной идентификационной информации, которая используется для выдачи сертификатов NQ Smart-ID. Поставщик идентификационной услуги, проверенный поставщиком услуги Smart-ID относительно соблюдения требований, действующих в отношении поставщиков идентификационной услуги для несертифицированных сертификатов.
Сертификат несертифицированной электронной подписи	Электронная аттестация, которая устанавливает связь между контрольными данными электронной подписи и физическим лицом и подтверждает по меньшей мере имя этого лица.
NQ Smart-ID	Smart-ID, которая содержит одну пару Сертификатов, состоящих из Сертификата аутентификации и Сертификата несертифицированной электронной подписи и соответствующие закрытые ключи.

Идентификатор объекта	Идентификатор, используемый для уникального наименования объекта (OID).
OCSP	Интернет-протокол для проверки статуса сертификата
PIN-код	Код активации для закрытого ключа, который соответствует Сертификату аутентификации, и для закрытого ключа, который соответствует Сертификату электронной подписи
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.
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.

Проверяющая сторона	Лицо/организация, которые используют информацию, содержащуюся в сертификате.
SK	SK ID Solutions AS, поставщик сертификационных услуг.
SK PS	SK ID Solutions AS, Стандартная практика предоставления доверительных услуг.
SLA	Договор о сервисном обслуживании
Smart-ID	Smart-ID - это новое поколение электронной идентификации, которое обеспечивает Подписчиков способами электронной аутентификации и проставления электронной подписи.
Учетная запись Smart-ID	Подписчик должен зарегистрировать учетную запись Smart-ID для использования услуг, предоставляемых системой Smart-ID. Учетная запись Smart-ID устанавливает связь между экземпляром приложения Smart-ID и личностью Подписчика в системе Smart-ID. В ходе создания и регистрации учетной записи Smart-ID личность владельца учетной записи Smart-ID (Подписчик) подтверждается регистрирующим органом, а связь между личностью владельца и парой ключей проверяется организацией, отвечающей за распределение сертификатов. Учетная запись Smart-ID имеет ключ усовершенствованной электронной записи и ключ аутентификации.
Поставщик услуги Smart-ID	Организация, которая несет предусмотренную законом ответственность за систему Smart-ID. SK является поставщиком Smart-ID.
Приложение Smart-ID	Технический компонент системы Smart-ID. Мобильное приложение Smart-ID, установленное в мобильном устройстве Подписчика,предоставляет доступ к несертифицированной услуге 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 (владельцы учетной записи Smart-ID) подтверждать подлинность их личности для поставщиков электронных услуг, проставлять электронные записи и управлять их учетными записями Smart-ID.
Подписчик	Физическое лицо, которому выдаются сертификаты NQ Smart-ID.
Условия	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 NQ 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 может только лично ходатайствовать об использовании услуги NQ Smart-ID. NQ Smart-ID не выдается представителю.

2 **Получение сертификата**

2.1 Подписчик подтверждает выдачу сертификата NQ Smart-ID в приложении Smart-ID. Соответствующее подтверждение считается получением сертификата NQ Smart-ID.

2.2 В случае ввода нового ключа сертификатов Подписчик подтверждает выдачу сертификата в приложении Smart-ID.

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

Сертификат Тип	Использование	Применимая и опубликованная политика сертификации	OID	Краткое содержание
Сертификаты для Smart-ID	Сертификат на электронную подпись предназначен для: создания усовершенствованных электронных подписей, соответствующих eIDAS	SK ID Solutions AS – политика сертификации для несертифицированных Smart-ID, опубликована на https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.17.1	internet attribute(1.3.6.1) private entity attribute(4) registered business attribute given by private business manager IANA(1) SK attribute in IANA register(10015) Certification service attribute(17.1)
		ETSI EN 319 411-1 Policy: NCP	0.4.0.2042.1.1	itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp(1)
	Сертификат аутентификации предназначен для: аутентификац	SK ID Solutions AS – политика сертификации для несертифицированных Smart-ID, опубликована на https://sk.ee/en/repository/CP/	1.3.6.1.4.1.10015.17.1	internet attribute(1.3.6.1) private entity attribute(4) registered business attribute given by private business manager IANA(1) SK attribute in IANA register(10015) Certification service attribute(17.1)

	ии.	ETSI EN 319 411-1 Policy: NCP	0.4.0.2042.1.1	itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp(1)

3.1 Использование сертификатов Подписчика запрещено в перечисленных ниже целях:
3.1.1 незаконная деятельность (в т.ч. кибератаки и попытки взломать сертификат NQ 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 испытательных целях).
3.2 Принадлежащие Подписчику сертификаты аутентификации нельзя использовать для создания усовершенствованных 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 не менее 10 лет.. Физические или цифровые архивные записи, касающиеся сертификатов, регистрационной информации и запросов или ходатайств относительно приостановки действия, прекращения приостановки и 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 NQ 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. 9, 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 подозревает, что он утратил контроль над своим закрытым ключом;
5.2.9 незамедлительно аннулировать сертификаты или ходатайствовать о выдаче новой NQ Smart-ID, если Подписчик утратил контроль над своими PIN-кодами.

6 Права и обязанности SK

6.1 SK обязан:
6.2 предоставлять сертификационную услугу в соответствии с действующими соглашениями, перечисленными в ст. 9, и соответствующим законодательством;
6.3 вести учет выданных сертификатов и их сроков действия;
6.4 обеспечивать безопасность внутренних процедур;
6.5 предоставлять возможность проверки срока действия сертификатов 24 часа в сутки;
6.6 обеспечивать защиту ключей сертификатов модулями аппаратной защиты (т.е. HSM) и и их пребывание под исключительным контролем SK;
6.7 обеспечивать активизацию ключей сертификатов, используемых в ходе предоставления сертификационной услуги, 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 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 Проверяющая сторона проверяет личность в сертификате NQ Smart-ID относительно личной информации, известной поставщику идентификационной услуги, в ходе первой аутентификации этого Подписчика в системе.
7.5 Проверяющая сторона обязана:
7.5.1 не создавать новые личности на основе информации, которая содержится в сертификатах NQ Smart-ID;
7.5.2 иметь необходимые разрешения от законных представителей, позволяющие несовершеннолетним лицам использовать NQ Smart-ID в их услугах;
7.5.3 инициировать изменение имени Подписчика в базе данных, если имя в Сертификате и в базе данных поставщика идентификационной услуги не совпадают.
7.6 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.
7.7 SK предлагает услуги OCSP для проверки статуса сертификата. Доступ к услуге осуществляется посредством HTTP протокола.
7.8 Проверяющая сторона проверяет срок действия сертификата посредством проверки срока действия сертификатов относительно OCSP. SK предлагает OCSP со следующими возможностями проверки:
7.8.1 Услуга OCSP является бесплатной и находится в общественном доступе на сайте http://aia.sk.ee/nq2016;
7.8.2 SK предлагает услугу OCSP с улучшенным SLA согласно соглашению и прейскуранту;
7.8.3 URL услуги OCSP включен в сертификат в поле Authority Information Access (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 она соответствует основным процедурам генерирования и хранения данных, которые находятся в ее распоряжении, и описание которых приведено в CPS;

8.1.2 она соответствует условиям оплаты, описание которых приводится в CPS;

8.1.3 она передает правильный сертификат и правильную информацию о статусе сертификата;

8.1.4 перед выдачей объекту статуса поставщика идентификационной услуги оценивается уровень качества идентификационных данных посредством проверки, соответствует ли объект требованиям, действующим в отношении поставщиков идентификационной услуги для несертифицированных сертификатов.

8.2 Поставщик услуги Smart-ID имеет право на отзыв статуса поставщика идентификационной услуги, если он получит доказательства того, что поставщик идентификационной услуги не соблюдает требования, действующие в отношении поставщиков идентификационной услуги для несертифицированных сертификатов.

8.3 Поставщик идентификационной услуги обязан проверять личность законных представителей, если несовершеннолетнее лицо ходатайствует об услуге NQ Smart-ID.

8.4 Поставщик идентификационной услуги гарантирует соблюдение требований, действующих в отношении поставщиков идентификационной услуги для несертифицированных 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 электронной 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 электронные подписи, проставленные на основании сертификатов, срок действия которых истек, которые были аннулированы или приостановлены, 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 материальную ответственность за информацию, которая содержится в сертификатах NQ Smart-ID.

9.7 SK не несет ответственности за:

9.7.1 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;

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

9.7.3 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 несертифицированной услуги Smart-ID, опубликована на https://sk.ee/en/repository/CP/;

10.1.2 SK ID Solutions AS – политика сертификации для NQ-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 **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 тем фактом, что в ходе использования сертификатов для удостоверения личности человеку, осуществляющему идентификацию, отправляется сертификат, который содержится в NQ 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 надлежащее хранение конфиденциальной информации и информации, предназначенной для внутреннего использования, и воздерживается от ее разглашения третьим сторонам путем применения различных контрольных мер безопасности.

11.5 SK имеет право на разглашение информации о Подписчике третьей стороне, которая, согласно соответствующим 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 Сертификационная услуга для NQ Smart-ID соответствует требованиям доверительных услуг согласно описанию в eIDAS.

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

13.4 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.

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

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

14 **Контактная информация**

14.1 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
Телефон +372 610 1880
Факс +372 610 1881
E-mail: info@sk.ee

14.2 Запросы об аннулировании сертификатов NQ Smart-ID принимаются 24/7 по телефону службы поддержки. Со службой поддержки можно связаться:
14.2.1 В Эстонии по телефону 9001807 или +372 715 1606;
14.2.2 В Латвии по телефону 1807 или +371 6766 5001;
14.2.3 В Литве по телефону 1807 или +370 6704 1807.

14.3 Ходатайства об аннулировании сертификатов NQ Smart-ID также принимаются через Интернет-портал самообслуживания и/или приложение NQ Smart-ID и/или пункты обслуживания клиентов.

14.4 Информация и контактные данные службы поддержки и Интернет-портала самообслуживания, а также пунктов обслуживания клиентов имеются на Интернет-странице SK https://www.sk.ee/en and https://www.smart-id.com/.