Условия пользования If Mobile

Содержание

Настоящим подтверждаю, что:

- я прочел и согласен с правилами использования If Mobile;
- буду держать код безопасности (PIN-код) If Mobile в своем единоличном контроле и немедленно изменю его, если он может стать или станет известен другому лицу.

Краткое описание

В настоящем документе приведены условия пользования If Mobile, ограничения на использование, права и обязанности сторон, порядок предоставления услуг и меры безопасности.

Идентификация документа

Идентификатором объекта настоящего документа (OID) является: 1.3.6.1.4.1.51321.1.1.1.2

2022.03.31

Версия 02

Описание идентификатора:

1.3.6.1.4.1.51321.x.y.z.q

1.3.6.1.4.1.51321 – идентификатор организации – If P&C Insurance AS;

x – идентификатор государства, возможные значения – .1 – Эстония, .2 – Латвия, .3 – Литва;

y – идентификатор продукта, возможные значения – .1 – If Mobile;

z – идентификатор документа, .1 – условия пользования, .2 – профиль сертификата;

q – порядковый номер версии документа.

1. Понятия

eIDAS – Регламент Европейского парламента и совета ЕС от 23 июля 2014 года № 910/2014 об электронной идентификации и удостоверительных услугах для электронных транзакций на внутреннем рынке и об отмене директивы 1999/93/EC.

Пользователь – дееспособное физическое лицо, пользующееся услугами If Mobile.

Электронная подпись – электронные данные, прилагаемые к электронному документу или логически связанные с ним, и которые подписывающее лицо использует для подписания документа.

Расширенная электронная подпись – электронная подпись, соответствующая требованиям, изложенным в статье 26 eIDAS.

Сертификат – открытый ключ вместе с дополнительной информацией, определенной в профиле сертификата. Подлинность сертификата невозможно подделать благодаря шифрованию с использованием персонального ключа, выданного органом по сертификации.

Данные идентификации личности – совокупность данных, позволяющих идентифицировать физическое или юридическое лицо.

Электронная идентификация – процесс использования электронных данных идентификации, позволяющий уникальным способом установить физическое или юридическое лицо.

Аутентификация – электронный процесс, позволяющий идентифицировать физическое или юридическое лицо.

Сертификат аутентификации – электронное подтверждение, сертификат, используемый для аутентификации или шифрования.

Сертификат электронной подписи – сертификат, связывающий данные валидации электронной подписи с физическим лицом и удостоверяющий, по меньшей мере, имя данного лица.

Подписывающее лицо – физическое лицо, создающее электронную подпись.

Электронный документ – любое содержание, которое сохраняется в электронном формате, в частности, в виде текстовой, звуковой, визуальной или аудиовизуальной записи.

Валидация – верификация (проверка) и подтверждение действительности электронной подписи.

Устройство для создания электронной подписи – сконфигурированное программное или аппаратное обеспечение, используемое для создания электронной подписи – защищенная часть в памяти мобильного устройства, защищенная от несанкционированного доступа и дублирования.

Орган по сертификации – Latvijas Valsts radio un televīzijas centrs VAS (Латвийский государственный центр радио и телевидения, ГАО), рег. № 40003011203, выдающий сертификаты для использования в приложении If Mobile и обеспечивающий верификацию и аннулирование выданных сертификатов.

Политика сертификации – документ органа по сертификации, определяющий требования относительно процедур и деятельности органа по сертификации, которые орган по сертификации выполняет при выдаче и управлении сертификатами If Mobile.

If Mobile – предлагаемый и управляемый If пакет программного обеспечения, предназначенный для использования в мобильных устройствах и предоставляющий пользователю возможность осуществлять связанные со страховыми услугами процедуры аутентификации, шифрования и подписания электронных документов расширенной электронной подписью.

Поставщик услуг идентификации – организация, предлагающая возможность электронной аутентификации и несущая ответственность за установление реальной идентичности лица, за создание электронной идентичности лица и ее удостоверение для регистрирующего органа, например, кредитного учреждения.

OCSP – протокол статуса сетевого сертификата.

PIN-код – код активации для персонального ключа, соответствующего сертификату аутентификации, и для персонального ключа, соответствующего сертификату электронной подписи.

Персональный ключ – ключ из пары ключей, который пользователь обязан хранить в тайне, и который используется для создания электронных подписей и/или дешифровки электронных данных или файлов, зашифрованных при помощи соответствующего открытого ключа.

Открытый ключ – ключ из пары ключей, который пользователь соответствующего персонального ключа может сделать общедоступным и который третьи лица используют для верификации электронных подписей, созданных при помощи соответствующего персонального ключа пользователя, и/или для шифрования сообщений таким образом, чтобы их мог дешифровать только пользователь при помощи соответствующего персонального ключа.

Третье лицо – лицо, деятельность которого основывается на содержащейся в сертификате информации, в том числе, электронных подписях и электронной идентификации личности.

If – If P&C Insurance AS (АО If P&C Insurance), зарегистрированное в Коммерческом регистре Эстонской Республики под регистрационным номером 10100168, и его филиалы в Латвии и Литве: If P&C Insurance AS Latvian branch (Латвийский филиал АО If P&C Insurance), единый регистрационный номер в Коммерческом регистре Латвийской Республики 40103201449 и If P&C Insurance AS filialas (филиал АО If P&C Insurance), регистрационный номер 4302279548 в Государственном регистре предприятий Литовской Республики.

If Group – все вместе или каждое по отдельности – If P&C Insurance AS (Эстония, рег. № 10100168) и его филиалы, If Skadeförsäkring Holding AB (publ) (Швеция, рег. № 5562417559) и его филиалы, If Skadeförsäkring AB (publ) (Швеция, рег. № 5164018102) и его филиалы.

Учетная запись If Mobile – учетная запись, которую пользователь регистрирует в приложении If Mobile. Учетная запись необходима для пользования услугами If Mobile, и она связывает пользование приложением If Mobile с идентичностью пользователя. При регистрации учетной записи If Mobile пользователь подтверждает If свою идентичность посредством поставщика услуг идентификации и на основании запроса сертификата, направленного If органу по сертификации, подтверждает связь между данной идентичностью и парой ключей пользователя. Учетная запись If Mobile имеет пару ключей расширенной электронной подписи и пару ключей аутентификации.

Услуга If Mobile – услуга аутентификации, услуга расширенной электронной подписи, страховая услуга или иная связанная со страхованием услуга, предлагаемая пользователю посредством If Mobile.

Сертификаты If Mobile – сертификаты аутентификации и расширенной электронной подписи, которые генерируются для пользователя в результате регистрации учетной записи If Mobile.

Профиль сертификата – требования, касающиеся содержания сертификата.

Регистрирующий орган – организация, несущая ответственность за проверку, регистрацию и администрирование идентичностью пользователя в соответствии со следующими документами:

ETSI EN 319 412-1 v1.1.1 (2016-02), Электронные подписи и инфраструктуры (ESI). Профили сертификатов. Часть 1. Основные положения и общие структуры данных.
и
RFC 3647 (ноябрь 2003 г.), Инфраструктура открытых ключей Internet X.509. Политика сертификации и концепция практики сертификации.

2. Версии документа

История версий
Дата – 2021.03.31
Версия– 01
Изменения – первоначальная версия

Дата – 2022.03.31
Версия – 02
Изменения - редакционные изменения

3. Общие условия

3.1. Настоящими условиями регулируется предоставление пользователю услуг If Mobile, а также порядок пользования соответствующими услугами, и они составляют юридически обязывающей частью договора между пользователем и If.

3.2. Для пользователя предварительным условием использования услугами If Mobile является необходимость ознакомиться с настоящими условиями и выразить свое согласие с ними. Заявка на получение сертификата считается согласием пользователя с условиями и подтверждением заключения договора.

3.3. If вправе в одностороннем порядке в любое время менять условия, публикуя их в If Mobile. Если пользователь не согласен с соответствующими изменениями, он вправе в одностороннем порядке расторгнуть договор на использование If Mobile. Измененные условия являются обязывающими для пользователя до момента расторжения договора на использование If Mobile со стороны пользователя. If публикует действующую версию настоящих условий на домашней странице If и в приложении If Mobile.

3.4. Пользователь может подать заявление на If Mobile только лично. Создание учетной записи If Mobile представителем не допускается.

3.5. Электронная подпись If Mobile соответствует изложенным в статье 26 eIDAS требованиям к расширенной электронной подписи:

3.5.1. Электронная подпись If Mobile уникальным образом связана с подписывающим лицом;

3.5.2. Электронная подпись If Mobile способна установить личность подписывающего лица;

3.5.3. Электронная подпись If Mobile проставляется при помощи данных, необходимых для проставления электронной подписи, которые при высоком уровне секретности может использовать исключительно подписывающее лицо;

3.5.4. Электронная подпись If Mobile связана с подписанными данными таким образом, что все последующие изменения данных возможно идентифицировать.

4. Идентификация

4.1. If проверяет личность пользователя и подтверждает, что запрос на сертификат является точным, авторизованным и полным для подтверждения подлинности личности пользователя.

4.2. Перед выдачей сертификата пользователю If собирает, проверяет и сохраняет доказательства идентичности пользователя из соответствующих авторизованных источников и включает соответствующие доказательства или ссылки на них в сертификат пользователя. If сохраняет соответствующие доказательства в течение всего срока действия сертификата и на протяжении 5-ти лет после истечения его срока действия или аннулирования сертификата.

4.2.1. Идентичность пользователя подтверждается также на основании информации, полученной от поставщика услуг идентификации, и это позволяет однозначно распознать пользователя из числа других лиц.

4.3. If подтверждает и дополняет сертификат следующими касающимися пользователя данными:

4.3.1. имя и фамилия пользователя;

4.3.2. личный код пользователя;

4.3.3. указанный пользователем и проверенный им номер мобильного телефона.

5. Получение сертификата

5.1. If выполняет функции регистрирующего органа.

5.2. Пользователь подает заявку на сертификат посредством If, используя приложение If Mobile.

5.3. If проверяет подлинность личности пользователя следующим образом:

5.3.1. If проверяет подлинность личности пользователя на основании результатов аутентификации пользователя, полученных от поставщика услуг идентификации;

5.3.2. пользователь подает заявку на сертификат только после аутентификации, успешно проведенной у поставщика услуг идентификации с использованием приложения If Mobile;

5.3.3. If проверяет, доступен ли пользователь по указанному номеру мобильного телефона, отправив код однократного использования и с ограниченным сроком действия, который пользователь должен ввести в приложение If Mobile в процессе регистрации;

5.4. После успешного проведения всех проверок в процессе регистрации необходимо выполнить следующие действия:

5.4.1. Пользователь должен подтвердить свое согласие с условиями пользования If Mobile.

5.4.2. Сертификаты пользователя If Mobile выдаются только на основании профиля сертификата If Mobile, составленного в соответствии с запросами If, отправленными органу по сертификации.

5.4.3. Процесс регистрации гарантирует, что персональный ключ, соответствующий используемому в заявке на сертификат открытому ключу, контролирует только пользователь.

5.4.4. Орган по сертификации принимает поступающие только от If заявки, соответствующие профилю сертификата If Mobile.

5.4.5. Орган по сертификации выдает сертификат пользователя только в том случае, если запрос на сертификат соответствует техническим условиям, определённым в профиле сертификата If Mobile, и в договоре, заключенном между If и органом по сертификации.

5.4.6. Сертификат If Mobile генерируется для пользователя в соответствии с описанием, содержащимся в профиле сертификата If Mobile.

5.4.7. По получении нового сертификата If Mobile аннулируются ранее выданные пользователю сертификаты If Mobile.

5.4.8. Орган по сертификации уведомляет If о выдаче сертификата пользователя или об отказе в его выдаче.

5.4.9. If уведомляет пользователя об ответе органа по сертификации. Уведомление о выдаче подтверждает выдачу сертификата пользователю. Уведомление об отказе в выдаче подтверждает, что сертификат не был выдан пользователю.

6. Тип сертификата и его использование

Тип сертификата и его использование

Сертификат на электронную подпись If Mobile применяется для создания соответствующих eIDAS расширенных электронных подписей.

Применяемая и опубликованная политика сертификации

Политика сертификации поставщика сертификатов расширенной электронной подписи, опубликована по адресу:

https://www.eparaksts.lv/repository,
OID: 1.3.6.1.4.1.32061.2.4.1

Тип сертификата и его применение

Сертификат аутентификации If Mobile применяется для аутентификации и шифрования.

Применяемая и опубликованная политика сертификации

Политика сертификации поставщика сертификатов аутентификации опубликована по адресу:

https://www.eparaksts.lv/repository,
OID: 1.3.6.1.4.1.32061.2.4.1

6.1. Использование сертификатов If Mobile разрешено исключительно для:

- подписания электронных документов при помощи расширенной электронной подписи в соответствии с eIDAS (только сертификат электронной подписи),
- аутентификации (только сертификат аутентификации),
- шифрования (только сертификат аутентификации),

с целью пользования страховыми услугами If Group, пользования связанными со страхованием услугами If Group или партнеров (определенных со стороны If) или для оказания услуг группе If Group.

6.2. Не допускается использование сертификатов пользователя в иных целях, в том числе для:

6.2.1. осуществления противоправной деятельности (в том числе, кибератак и попыток изменить сертификат If Mobile);

6.2.2. выдачи новых или производных сертификатов, а также информации, касающейся действительности сертификата;

6.2.3. тестов и испытаний, которые могут повлечь за собой последствия для пользователя и других лиц;

6.2.4. автоматизированного использования сертификатов, в том числе, при выполнении действий по подписанию, аутентификации и дешифровке без участия соответствующих лиц;

6.3. Запрещено использование сертификатов пользователя, если персональный ключ попал в распоряжение другого лица или был передан другому лицу.

6.4. Не разрешено использование сертификата аутентификации пользователя для генерирования расширенных электронных подписей, соответствующих eIDAS.

7. Срок действия сертификата

7.1. Сертификат выдается со сроком действия три года.

7.2. Действие сертификата вступает в силу с указанного в сертификате числа и времени, которое пользователь может проверить в приложении If Mobile.

7.3. Действие сертификата заканчивается в последний день указанного в сертификате срока действия или в случае аннулирования сертификата.

7.4. Журналы аудита хранятся не менее 7 лет после окончания срока действия сертификата или после аннулирования сертификата. Физические или цифровые архивные записи, содержащие заявки на сертификаты, информацию о регистрации и заявки на получение информации или заявки на аннулирование хранятся в течение не менее 7 лет после окончания срока действия соответствующего сертификата.

8. Отмена действия сертификата

8.1. В течение срока действия сертификата пользователь имеет право в любое время в одностороннем порядке аннулировать свой сертификат, удалив свой профиль в приложении If Mobile или направив письменное заявление в If.

8.2. Аннулирование одного выданного пользователю сертификата автоматически применяется ко всем сертификатам If Mobile, выданным пользователю в том же устройстве.

8.3. If аннулирует сертификат не позднее, чем в течение 3-х рабочих дней после получения заявления об аннулировании сертификата.

8.4. Действие аннулированного сертификата не подлежит восстановлению. Для продолжения работы с If Mobile пользователь должен подать заявление на получение нового сертификата.

8.5. If вправе аннулировать сертификат пользователя в следующих случаях:

8.5.1. пользователь подал заявление об аннулировании сертификата;

8.5.2. пользователь заблокировал его, введя 5 раз подряд неверный PIN-код;

8.5.3. В If поступила информация о том, что пользователь утратил контроль над персональными ключами или PIN-кодами своего приложения If Mobile;

8.5.4. If получил доказательства того, что персональный ключ пользователя, соответствующий используемому в сертификате открытому ключу, поврежден или более не соответствует требованиям;

8.5.5. If получил доказательства того, что сертификат не использовался в предназначенных для него целях;

8.5.6. В If поступила информация о том, что пользователь нарушил настоящие условия пользования If Mobile;

8.5.7. В If поступила информация об изменениях в части фактов содержащейся в сертификате информации;

8.5.8. В If поступила информация о том, что сертификат был выдан в нарушение политики сертификации, профиля сертификата If Mobile или настоящих условий пользования If Mobile;

8.5.9. If выяснил, что содержащаяся в сертификате информация является неточной или вводящей в заблуждение;

8.5.10. If прекращает оказание услуги If Mobile, и орган по сертификации не оказывает услугу по аннулированию сертификатов;

8.5.11. Право If на выдачу сертификатов приостановлено или аннулировано, за исключением случаев, когда If продолжает обеспечивать функционирование хранилища OCSP или CRL;

8.5.12. В If поступила информация о том, что нарушен персональный ключ, используемый органом по сертификации для выдачи сертификата;

8.5.13. В If поступила информация о том, что пользователь скончался или утратил дееспособность;

8.5.14. Политикой сертификации предусмотрена необходимость аннулирования;

8.5.15. Техническое содержание или формат сертификата представляет собой существенную угрозу для пользователя, If или любого третьего лица;

8.5.16. If более не пользуется имеющимися в приложении If Mobile услугами поставщика идентификации, которые предоставляли информацию на основании того, какой сертификат был выдан.

9. Прочие связанные с сертификатом действия

9.1. Не разрешены следующие действия в отношении сертификата пользователя:

9.1.1. изменение содержащейся в сертификате информации;

9.1.2. исправление ошибок в содержащейся в сертификате информации;

9.1.3. временное приостановление действия сертификата с целью его позднейшего восстановления;

9.1.4. изменение пары связанных с ним ключей.

Если необходимо осуществить какие-либо из перечисленных выше действий, то пользователь обязан аннулировать действующий сертификат и подать заявку на получение нового.

10. Права и обязанности пользователя

10.1. Пользователь имеет право:

10.1.1. подавать заявку на выдачу сертификата If Mobile для использования в приложении If Mobile;

10.1.2. использовать сертификат для получения указанных в пункте 6.1 услуг;

10.1.3. ходатайствовать о том, чтобы If аннулировал сертификат на основании заявления пользователя в изложенных в настоящих условиях случаях;

10.2. На пользователя возлагаются следующие обязанности:

10.2.1. соблюдать настоящие условия;

10.2.2. пользоваться своим персональным ключом и сертификатом в соответствии с настоящими условиями, в том числе, с применимыми документами,

перечисленными в пункте 16 и действующему законодательству Эстонской Республики;

10.2.3. обеспечить невозможность попадания персонального ключа пользователя в распоряжение других лиц, в том числе и при попадании мобильного устройства и PIN-кодов в распоряжение других лиц;

10.2.4. незамедлительно уведомлять If о возможных случаях несанкционированного использования персонального ключа и аннулировать свой сертификат, в том числе в случаях, когда пользователь утратил контроль над своим персональным ключом или PIN-кодом;

10.2.5. предоставлять в приложении If Mobile точную и достоверную информацию;

10.2.6. уведомлять If об изменениях личных данных, аннулируя сертификат с недействительными данными и подавая заявление на сертификат с обновленными данными;

10.2.7. не использовать If Mobile в устройствах, если игнорируются инструкции, ограничения и меры безопасности, установленные производителем устройства, в том числе в устройствах, освобожденных от ограничений со стороны производителя (т.н. «jailbroken» – разблокированных или «rooted» – рутованных).

11. Права и обязанности If

11.1. На If возлагаются следующие обязанности:

11.1.1. Предложение услуги сертификации в соответствии с настоящими условиями, требованиями eIDAS, касающимися расширенной электронной подписи, политикой сертификации, а также действующими в Эстонской Республике законами.

11.1.2. Принимая во внимание уровень развития технологии, расходы на внедрение и характер объем, контекст и цели обработки данных, а также все связанные с правами и свободами физических лиц риски с различной степенью вероятности и серьезности, которые могут возникать в процессе предоставления услуг If Mobile, If применяет соответствующие технические и организационные меры с целью обеспечить безопасность данных при предоставлении услуг If Mobile.

11.1.3. Не сохранять PIN-коды, введенные пользователем в любую контролируемую If среду, в том числе и введенные в приложение If Mobile.

11.1.4. Гарантировать активизацию ключей сертификации, используемых для предоставления услуг сертификации, на основании разделенного контроля.

11.1.5. Обеспечить возможность проверки действительности сертификатов, привлекая для этого орган по сертификации.

11.1.6. Гарантировать соответствие выдаваемого сертификата профилю сертификата, используя информацию, предоставленную пользователем и поставщиком услуг идентификации.

11.1.7. Выполнять процедуру генерирования и сохранения ключей в соответствии с политикой сертификации и изложенными в eIDAS требованиями относительно расширенной электронной подписи.

11.1.8. Оценивать качество касающейся идентичности лица информации, предоставленной поставщиком услуг идентификации, и убедиться в её достаточности для пользования приложением If Mobile в предусмотренных целях.

11.2. If имеет право:

11.2.1. Прекращать использование предоставленной поставщиком услуг идентификации информации, касающейся идентичности в приложении If Mobile, если качество данной информации является недостаточным.

11.2.2. Аннулировать сертификаты в предусмотренных в настоящих условиях случаях.

11.2.3. Не допускать использование услуги If Mobile в устройствах пользователя, если игнорируются инструкции, ограничения и меры безопасности, установленные производителем устройства, в том числе использование If Mobile в устройствах, освобожденных от ограничений со стороны производителя (т.н. «jailbroken» – разблокированных или «rooted» – рутованных).

12. Права и обязанности третьих лиц в связи с проверкой статуса сертификата

12.1. Третьи лица имеют право проверять действительность сертификата:

12.1.1. 12.1.1.используя для проверки статуса сертификата услугу OCSP;

12.1.2. направляя в орган по сертификации письменное заявление;

12.1.3. если справка о действительности сертификата прилагается к сертификату или если электронная

подпись не является достаточной, третье лицо проверяет действие сертификата на основании услуг валидации сертификата, которые If предлагает во время использования сертификата или проставления электронной подписи.

12.2. Третье лицо обязано соблюдать установленные в сертификате ограничения и проверять соответствие подтвержденной сделки настоящим условиям и политике сертификации.

12.3. Третье лицо обязано валидировать идентичность из сертификата If Mobile на основании известных третьему лицу личных данных.

12.4. Третьему лицу не разрешается при оказании своих услуг предоставлять несовершеннолетним возможность использования If Mobile.

12.5. If обеспечивает доступность пользования услугами статуса сертификата 24 часа в сутки, 7 дней в неделю, с общей доступностью услуг не менее 99% в год, при этом плановое время неисправности не должно превышать 1% в год.

12.6. If предлагает услугу OCSP для верификации статуса сертификата, выданного органом по сертификации. Услуга доступна для использования посредством протокола HTTP.

12.7. If предлагает OCSP вместе со следующими возможностями проверки:

12.7.1. Услуга OCSP является бесплатной и она публично доступна на веб-сайте: http://ocsp.eparaksts.lv;

12.7.2. В соответствии с профилем сертификата адрес услуги OCSP содержится в поле сертификата «Authority Information Access» (AIA).

13. Партнеры

13.1. Партнером является третье лицо или учреждение, подписавшее с If договор на пользование If Mobile для достижения одной или нескольких из нижеследующих целей (далее «цели»):

- Аутентификация пользователя
- Предоставление услуг пользователю
- Шифрование информации пользователя

13.2. If обеспечивает использование партнерами If Mobile исключительно в установленных настоящими условиями целях в соответствии с предусмотренными в пункте 6.1 ограничениями.

14. Требования, предъявляемые к органу по сертификации

14.1. If гарантирует, что орган по сертификации и его деятельность соответствуют следующим требованиям:

14.1.1. Место, где происходит генерирование и аннулирование сертификатов, защищено от несанкционированного и незарегистрированного физического доступа;

14.1.2. Используемые для генерирования и аннулирования сертификатов устройства защищены от негативного воздействия физических обстоятельств – пожара, потопа, отключений подачи электричества, перебоев со связью, кражи, злонамеренного или случайного уничтожения, стихийных бедствий, кражи с взломом;

14.1.3. Применяются меры, предупреждающие несанкционированное выключение и изъятие из защищённой зоны устройств, информации, носителей информации и программного обеспечения;

14.1.4. Обеспечивает резервное копирование такой информации и систем, которые необходимы для его деятельности в качестве органа по сертификации и восстановления своей деятельности; регулярное сохранение резервных копий, безопасность хранения и возможность использования копий для возобновления деятельности. Для данной работы привлекаются уполномоченные и доверенные работники;

14.1.5. План бесперебойной деятельности предприятия разработан, внедрен и управляется таким образом, что он позволяет восстановить деятельность органа по сертификации в том случае, если его персональные ключи утеряны, повреждены или потенциально могут быть повреждены. План должен включать следующие связанные с данным инцидентом действия:

14.1.5.1. возможность аннулировать все сертификаты пользователя;

14.1.5.2. возможность уведомлять всех пользователей и If о произошедшем инциденте;

14.1.5.3. возможность аннулировать все выданные органом по сертификации сертификаты, которые подчиняются обусловившему инцидент сертификату;

14.1.6. Орган по сертификации генерирует свои персональные ключи в безопасной среде и сохраняет их конфиденциальность:

14.1.6.1. Генерирование персональных ключей в физически защищенной среде и в сетевой среде с высокой степенью защиты осуществляют доверенные и наделенные соответствующими полномочиями работники, количество которых соответствует минимально требуемому, но не менее двух лиц, которым разрешено вместе генерировать ключи. Каждое лицо, участвующее в генерировании ключей органа по сертификации, использует для данной деятельности многофазовую аутентификацию;

14.1.6.2. Ключи генерируются с использованием алгоритмов, которые подходят с учетом данных рисков безопасности, и гарантируют выполнение проистекающих из eIDAS требований, касающихся расширенных электронных подписей;

14.1.6.3. До истечения срока действия сертификатов органа по сертификации, использующихся для генерирования сертификатов пользователя, орган по сертификации обязан генерировать и ввести в действие новый сертификат, который будет использоваться для генерирования сертификатов пользователя с целью обеспечения бесперебойного выполнения функций органа по сертификации. О данных действиях необходимо своевременно уведомить If, и эти действия следует осуществлять с достаточным запасом времени, чтобы предоставить If и другим сторонам возможность адаптировать свою деятельность и информационные системы к соответствующим изменениям и тем самым обеспечить продолжение предоставления пользователям оказываемых услуг.

14.1.6.4. После внедрения органом по сертификации новых сертификатов орган по сертификации уведомляет If за подписью своего руководителя об успешном окончании процесса генерирования ключей органа по сертификации, подтверждая, что он был проведен в соответствии с предусмотренной процедурой, что его реализацией занимались исключительно доверенные и наделенные соответствующими полномочиями лица, что конфиденциальность и целостность пары ключей была гарантирована, что открытые ключи генерированных пар ключей находятся в открытом доступе, что персональные ключи генерированных пар ключей хранятся и используются в надежных устройствах шифрования, и они защищены техническими средствами, физическими и организационными мерами в соответствии с их уровнем риска, что все персональные ключи, ранее использовавшиеся органом по сертификации для генерирования сертификатов пользователя, были уничтожены.

14.1.7. Доступ к корневому персональному ключу органа по сертификации, который используется для подписания подчиненных органу по сертификации сертификатов, имеется лишь у доверенных и наделенных соответствующими полномочиями работников;

14.1.8. Орган по сертификации уведомляет всех пользователей и If, если какие-либо из используемых алгоритмов становятся неприменимыми для предусмотренных целей, и в сотрудничестве с If планирует аннулировать затронутые сертификаты;

14.1.9. Недопустимо единоличное подписание подчиненных органу по сертификации сертификатов одним лицом, проверку подписания проводят не менее двух доверенных и уполномоченных работников.

14.1.10. Все последующие связанные с выдачей и аннулированием сертификатов инциденты в сфере безопасности регистрируются: включение и выключение систем, нарушения функционирования, неисправности устройств, перебои со связью, запросы на регистрацию и аннулирование сертификатов, данные о таких запросах и о связанных с ними ответах, события жизненного цикла сертификатов пользователя, события жизненного цикла корневых ключей;

14.1.11. При получении и обработке данных пользователей гарантирована их конфиденциальность и целостность, эти данные используются только для выполнения функций органа по сертификации;

14.1.12. .Все предусмотренные для тестирования сертификаты содержат ясные и однозначно понимаемые примечания с указанием цели тестирования, например, от имени пользователя;

14.1.13. Орган по сертификации является независимым от других организаций в том, что касается выполнения функций органа по сертификации: генерирования, аннулирования и верификации сертификатов пользователя. При выполнении этих функций на орган по сертификации и его руководство не оказывается коммерческое, финансовое, политическое или иное давление, которое могло бы послужить основанием для сомнений в надежности предоставляемых им услуг.

15. Ответственность и её ограничения

15.1. Пользователь несет ответственность за сохранение, хранение и использование своего персонального ключа.

15.2. Пользователь несет полную ответственность за любые последствия аутентификации и использования электронной подписи при использовании своих сертификатов как во время срока их действия, так и после окончания срока их действия.

15.3. Пользователь несет ответственность за любые ущербы, причиненные в результате неисполнения изложенных в настоящих условиях обязанностей пользователя или за их ненадлежащее выполнение.

15.4. Пользователь осознает, что электронные подписи, выданные на основании сертификата, который недействителен или аннулирован, являются недействительными.

15.5. Пользователь несет ответственность за любые ущербы при использовании If Mobile в устройстве, если они обусловлены игнорированием инструкций, ограничений или мер безопасности, установленных производителем устройства, в том числе при использовании If Mobile в устройствах, освобожденных от ограничений со стороны производителя (т.н. «jailbroken» – разблокированных или «rooted» – рутованных).

15.6. Для заверения расширенной электронной подписи пользователь должен использовать только ему известный, им самим выбранный дополнительный PIN-код каждый раз, когда она присоединяется к электронным данным. Введение дополнительного и выданного для подтверждения действий PIN-кода считается согласием пользователя на соответствующее действие, и это необходимо для незамедлительного генерирования расширенной электронной подписи пользователя и её присоединения к отображаемым для пользователя электронным данным.

15.7. Если оказание услуг сертификации нарушено, If своевременно уведомляет всех пользователей и хранит связанные с нарушением услуг сертификации документы и информацию в течение не менее 7 лет после проявления нарушения услуг сертификации.

15.8. If не несет финансовую ответственность за содержащуюся в сертификатах If Mobile информацию. If в любом случае не несет ответственность за причиненный пользователю или третьим лицам косвенный ущерб, в том числе и за неполученный доход.

15.9. If не несет ответственность за причиненный пользователю или третьим лицам ущерб, который возник, проистекал или был связан со следующими обстоятельствами:

15.9.1. Конфиденциальность персональных ключей пользователя, неверное использование сертификатов или неверная верификация сертификатов или неверные решения третьих сторон или любые последствия, возникшие вследствие ошибок или недостатков, проявившихся в ходе проверки валидации сертификата;

15.9.2. Невыполнение If своих обязанностей, если причиной такого неисполнения являются ошибки или проблемы в системе безопасности надзорных учреждений, учреждений по защите данных или иных государственных ведомств;

15.9.3. Невозможность исполнять свои обязанности, если причиной этого являются обстоятельства непреодолимой силы.

16. Применимые документы

16.1. Использование If Mobile регулируют следующие документы:

16.1.1. [1] Политика сертификации, опубликованная на сайте по адресу: https://www.eparaksts.lv/repository;

16.1.2. [2] Профиль сертификата If Mobile, опубликован на сайте по адресу: https://www.if.ee/if-mobile#dokumendid;

16.1.3. [3] Настоящие условия;

16.1.4. [4] ETSI EN 319 412-1 v1.1.1 (2016-02), Электронные подписи и инфраструктуры (ESI). Профили сертификатов. Часть 1. Основные положения и общие структуры данных;

16.1.5. [5] RFC 3647 (ноябрь 2003 г.), Инфраструктура открытых ключей Internet X.509. Политика сертификации и концепция практики сертификации.

16.1.6. [6] Регламент Европейского парламента и совета ЕС от 23 июля 2014 года № 910/2014 об электронной идентификации и удостоверительных услугах для электронных транзакций на внутреннем рынке и об отмене директивы 1999/93/ЕС;

16.1.7. [7] Регламент (ЕС) 2016/679 Европейского парламента и Совета (от 27 апреля 2016 года) о защите физических лиц в отношении обработки персональных данных и о свободном обращении таких данных и отмене Директивы 95/46/ЕС (Общий регламент по защите данных) (Документ относится к ЕЭЗ);

16.1.8. [8] Принципы обработки личных данных If kindlustus, https://www.if. ee/isikuandmed;

16.1.9. Прочие правовые акты.

17. Защита информации и неприкосновенности частной жизни

17.1. При обработке личных данных и информации о регистрации If соблюдает общий регламент по защите данных и прочие действующие в Эстонской Республике законы.

17.2. Пользователь проинформирован и согласен с тем, что его личные данные, определенные в профиле сертификата If Mobile, будут переданы органу по сертификации для включения в сертификат

пользователя, а также для администрирования настоящего сертификата в соответствии с настоящими условиями использования If Mobile.

17.3. Пользователь проинформирован и согласен с тем, что во время аутентификации или шифрования стороне, осуществляющей идентификацию или шифрование, отправляется сертификат аутентификации пользователя, включенный в If Mobile пользователя, и содержащий имена, фамилию, личный код и номер мобильного телефона пользователя.

17.4. Пользователь проинформирован и согласен с тем, что сертификат электронной подписи If Mobile пользователя присоединяется к подписанным им документам, неотделимо связан с ними, включает имена, фамилию, личный код, номер мобильного телефона пользователя, а также с тем, что данная информация становится доступной для получателя подписанного документа.

17.5. If вправе использовать полученную информацию для предложения и предоставления услуг страхования If Group или определенных If связанных со страхованием услуг партнеров, а также для пользования услугами.

17.6. Вся информация, которая стала известной при предоставлении услуг и не была предусмотрена для разглашения (например, информация, ставшая известной в результате управления и предоставления услуг сертификации If Mobile), является конфиденциальной. Пользователь вправе получать от If информацию о себе в соответствии с законом.

17.7. If защищает конфиденциальную информацию и информацию, предусмотренную для внутреннего пользования, от компрометации и не допускает ее нарушения и разглашения третьим лицам, применяя разумные и соразмерные технические и организационные меры безопасности.

17.8. If вправе раскрывать касающуюся пользователя информацию третьим лицам, которые в соответствии с законом имеют право получать такую информацию.

18. Применимое законодательство и разрешение споров

18.1. If предоставляет услуги If Mobile в соответствии с действующим законодательством Эстонской Республики.

18.2. Услуга сертификации If Mobile в части расширенной электронной подписи соответствует требованиям, установленным eIDAS в отношении удостоверительных услуг.

18.3. Все споры между сторонами разрешаются путем переговоров. Если стороны не могут достичь договоренности, спор разрешается в суде Эстонской Республики.

18.4. Пользователь или иное лицо может предъявить свое требование или подать жалобу по следующему адресу электронной почты: info@if.ee

19. Контактная информация

19.1. Услуги If Mobile в Эстонии предоставляет If P&C Insurance AS (Эстония, рег. № 10100168): KMKR EE100305320

Юридический адрес и адрес главного офиса:
Лыытса 8A, Таллинн 11415

Номер телефона (работает 24/7): +372 7771211
адрес электронной почты: info@if.ee
Домашняя страница If и интернет-портал If: www.if.ee