МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 61708
от "22" декабря 2020

ПРИКАЗ

19.11.2020 № 603

Москва

Об утверждении требований к порядку действий аккредитованного удостоверяющего центра при возникновении обоснованных сомнений относительно лица, давшего поручение на использование хранимых ключей электронной подписи, а также при приостановлении (прекращении) технической возможности использования хранимых ключей электронной подписи, включая информирование владельцев квалифицированных сертификатов ключей проверки электронной подписи о событиях, вызвавших приостановление (прекращение) технической возможности использования хранимых ключей электронной подписи, об их причинах и последствиях

Во исполнение положений пункта 6 части 4 статьи 8 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (Собрание законодательства, 2011, № 15, ст. 2036; 2019, № 52, ст. 7794)[1]

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые требования к порядку действий аккредитованного удостоверяющего центра при возникновении обоснованных сомнений относительно лица, давшего поручение на использование хранимых ключей электронной подписи, а также при приостановлении (прекращении) технической возможности использования хранимых ключей электронной подписи, включая информирование владельцев квалифицированных сертификатов ключей проверки электронной подписи о событиях, вызвавших приостановление (прекращение) технической возможности использования хранимых ключей электронной подписи, об их причинах и последствиях.

2. Направить настоящий приказ на государственную регистрацию в Министерство юстиции Российской Федерации.

3. Настоящий приказ вступает в силу с 1 января 2021 г. и действует до 1 января 2027 г.

Министр М.И. Шадаев

[1] Пункт 1 Положения о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 2 июня 2008 г. № 418 (Собрание законодательства Российской Федерации, 2008, № 23, ст. 2708; 2020, № 38, ст. 5870)

УТВЕРЖДЕНЫ
приказом Министерства цифрового
развития, связи и массовых
коммуникаций
Российской Федерации
от 19.11. 2020 г. № 603

ТРЕБОВАНИЯ
к порядку действий аккредитованного удостоверяющего центра при возникновении обоснованных сомнений относительно лица, давшего поручение на использование хранимых ключей электронной подписи, а также при приостановлении (прекращении) технической возможности использования хранимых ключей электронной подписи, включая информирование владельцев квалифицированных сертификатов ключей проверки электронной подписи о событиях, вызвавших приостановление (прекращение) технической возможности использования хранимых ключей электронной подписи, об их причинах и последствиях

1. Настоящие Требования устанавливают порядок действий аккредитованного удостоверяющего центра при возникновении обоснованных сомнений относительно лица, давшего поручение на использование хранимых ключей электронной подписи (далее – сомнения), а также при приостановлении (прекращении) технической возможности использования хранимых ключей электронной подписи, включая информирование владельцев квалифицированных сертификатов ключей проверки электронной подписи о событиях, вызвавших приостановление (прекращение) технической возможности использования хранимых ключей электронной подписи, об их причинах и последствиях.

2. При возникновении сомнений аккредитованный удостоверяющий центр обязан осуществить идентификацию и аутентификацию лица, давшего поручение, путем получения и (или) подтверждения достоверности сведений о нем с использованием единой системы идентификации и аутентификации либо иными способами, предусмотренными пунктом 1 части 1 статьи 18 Федерального закона от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (далее – идентификация).

В случае сохранения сомнений после проведенной идентификации аккредитованный удостоверяющий центр осуществляет процедуру дополнительной аутентификации владельца квалифицированного сертификата путем предоставления сведений из единой системы идентификации и аутентификации и информации о степени соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в единой информационной системе персональных данных, обеспечивающей обработку, сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации.

В целях осуществления указанной в абзаце втором настоящего пункта процедуры дополнительной аутентификации аккредитованный удостоверяющий центр получает из единой системы идентификации и аутентификации следующие сведения о владельце квалифицированного сертификата:

в отношении физических лиц – фамилию, имя, отчество (при наличии), страховой номер индивидуального лицевого счета застрахованного лица в системе персонифицированного учета Пенсионного фонда Российской Федерации (СНИЛС), реквизиты основного документа, удостоверяющего личность гражданина (серия, номер, дата выдачи), идентификационный номер налогоплательщика (при наличии данных сведений в единой системе идентификации и аутентификации), основной государственный регистрационный номер индивидуального предпринимателя (для физического лица, являющегося индивидуальным предпринимателем);

в отношении юридических лиц – наименование, организационно-правовую форму, адрес в пределах места нахождения, основной государственный регистрационный номер, идентификационный номер налогоплательщика.

3. В случае если после осуществления действий, указанных в пункте 2 настоящих Требований, сомнения относительно лица, давшего поручение на использование хранимых ключей электронной подписи, продолжают существовать, аккредитованный удостоверяющий центр обязан незамедлительно прекратить создание при помощи указанных ключей подписи по поручению владельца квалифицированного сертификата и уведомить об этом владельца данного квалифицированного сертификата с указанием причин.

Такое уведомление направляется посредством телефонной связи через СМС-сообщение и (или) на электронную почту (при наличии) по адресу, указанному в поручении на хранение ключа электронной подписи, ключ проверки которой содержится в квалифицированном сертификате.

4. При приостановлении (прекращении) технической возможности использования хранимых ключей электронной подписи аккредитованный удостоверяющий центр обязан сообщить об этом владельцам ключей электронной подписи, в том числе проинформировав о событиях, вызвавших приостановление (прекращение) технической возможности использования хранимых ключей электронной подписи, об их причинах и последствиях.

Указанное сообщение должно быть направлено посредством телефонной связи посредством СМС-сообщений и (или) на электронную почту (при наличии) по адресу, указанному в поручении на хранение ключа электронной подписи, ключ проверки которой содержится в квалифицированном сертификате, в срок, не превышающий один день, с момента приостановления (прекращения) технической возможности использования хранимых ключей электронной подписи.

5. Уведомление и сообщение посредством СМС-сообщения осуществляется только с разрешения владельца квалифицированного сертификата. Факт разрешения на получение СМС-извещения подтверждается согласием владельца квалифицированного сертификата на уведомление таким способом, а также подтверждением отсутствия блокировки на получение сообщений.

6. В случае отсутствия возможности устранения событий, вызвавших приостановление (прекращение) технической возможности использования хранимых ключей электронной подписи, в срок до 30 календарных дней, аккредитованный удостоверяющий центр обязан повторно сообщить об этом владельцам ключей электронной подписи с последующим уничтожением указанных ключей.