Приложение№ 2

к Приказу Генерального секретаря

Правительства № 130-А

от 26 марта 2015 г.

**ПРАВИЛА**

**о порядке интеграции бенефициаров услуги МРаssс правительственной электронной услугой**аутентификации и контроля доступа**(MPass)**

## Глава I. Общие положения

1. Правила о порядке интеграции бенефициаров с правительственной электронной услугой аутентификации и контроля доступа(MPass) (в дальнейшем– Правила) разработаны с целью обеспечения внедрения положений Постановления Правительства № 1090 от 31 декабря 2013 г. «О правительственной электронной услуге аутентификации и контроля доступа (MPass)» в части, касающейся интеграции бенефициаров с услугой MPass.
2. Правила устанавливают комплекс организационных, административных и технических мер, которые необходимо принять для реализации интеграции правительственной электронной услуги аутентификации и контроля доступа(в дальнейшем– услуга MPass) в технико-технологическую инфраструктуру бенефициаров услуги MPass, а также регулируют всю совокупность отношений между владельцем услуги MPass и бенефициарами этой услуги, установленных в рамках процесса интеграции.

## Глава II. Термины и определения

1. Для целейнастоящих Правил используются термины и определения, установленные п. 2 Положения о правительственной электронной услуге аутентификации и контроля доступа (MPass), утвержденного Постановлением Правительства № 1090 от 31 декабря 2013 г.

## Глава III. Участники процесса интеграции

1. Участниками процесса интеграции бенефициаров с услугой MPass являются:
2. владелец услуги MPass (в дальнейшем – Владелец) –лицо, назначенное постановлением Правительства;
3. бенефициар услуги MPass (в дальнейшем – Бенефициар) – поставщики публичных услуг и поставщики услуг из частного сектора, обладатели информационных систем, интегрированных с услугой MPass;
4. технико-технологический оператор услуги MPass –лицо, назначенное Постановлением Правительства;
5. администратор услуги MPass – лицо, назначенное Владельцем услуги, которое имеет неограниченный доступ ко всем разделам системы в целях полного управления услугой MPass;
6. администратор доступа – лицо, назначенное бенефициарами услуги MPass, которое уполномочено предоставлять аутентифицированным идентичностям права в информационных системах, интегрированных с услугой MPass;
7. пользователь услуги MPass – лицо, у которого есть собственный профиль в рамках услуги MPass.

## Глава IV. Полномочия участников

1. В процессе интеграции Владелец осуществляет следующие полномочия:
2. рассматривает заявки на интеграцию услуги MPass раньше, чем поставщики публичных услуг и поставщики услуг из частного сектора, отвечает им в соответствии с положениями настоящих правил;
3. назначает контактное лицо, ответственное за координацию процесса интеграции;
4. разрабатывает, утверждает и предоставлет, по требованию, поставщикам публичных услуг и поставщикам услуг из частного сектора техническую документацию по интеграции;
5. регистрирует поставщиков публичных услуг и, при необходимости, поставщиков услуг из частного сектора в качестве бенефициаров услуги MPass в тестовой среде и производственной среде услуги MPass;
6. предоставляет функцию администратора доступа ответственному лицу, назначенному Бенефициаром;
7. обеспечивает предоставление технической помощи по интеграции поставщикам публичных услуг и поставщикам услуг из частного сектора или, в случае необходимости, бенефициарам;
8. утверждает соответствие технологического решения по интеграции бенефициаров;
9. может делегировать свои полномочия администратору услугиMPass;
10. заключает с Бенефициаром соглашение или, при необходимости, договор о предоставлении услуг по подтверждению идентичности и/или по поставке идентификационных сведений.
11. В процессе интеграции Бенефициар осуществляет следующие полномочия:
12. запрашивает у Владельца интеграцию услуг по подтверждению идентичности и по поставке идентификационных сведений с собственными информационными системами;
13. назначает администратора доступа для собственных информационных систем;
14. назначает контактное лицо, ответственное за координацию процесса интеграции;
15. обеспечивает из собственных финансовых ресурсов проведение технико-технологических мероприятий по интеграции услуги MPass в свои информационные системы, в том числе проверяет соответствие технического решения по интеграции;
16. получает и обеспечивает безопасность закрытого ключа и актуальность используемых сертификатов открытых ключей;
17. запрашивает у Владельца техническую помощь в урегулировании технических трудностей, возникших в процессе интеграции;
18. В процессе интеграции Технико-технологический оператор услуги MPassобеспечивает, по запросу Владельца, техническую помощь, необходимую для процесса интеграции, включая работы по реконфигурации технической инфраструктуры с целью обеспечения доступа или безопасности решения.
19. В процессе интеграции Администратор услуги MPassосуществляет следующие полномочия:
20. обеспечивает, по запросу Владельца, предоставление технической помощи, необходимой для процесса интеграции, в том числе выполнение работ;
21. выполняет другие полномочия, делегированные Владельцем.
22. Администратор доступа осуществляет следующие полномочия:
23. присваивает функции конечным пользователям электронной интегрированной услуги Бенефициара в соответствии с его запросами;
24. актуализирует регистрационные атрибуты электронных интегрированных услуг Бенефициара.
25. Участники процесса интеграции должны принять организационные и технические меры, необходимые для защиты персональных данных от уничтожения, изменения, блокирования, копирования, распространения, а также от других незаконных действий, меры, призванные обеспечить адекватный уровень безопасности и конфиденциальности относительно рисков, связанных с обработкой и характером обработанных данных, в соответствии с требованиями законодательства о защите персональных данных.

## Глава V. Процесс интеграции

1. Процесс интеграции услуги MPass включает следующие действия в нижеуказанном порядке:
2. Поставщик услуг подает Владельцу запрос об интеграции в соответствии с положениями главы VIнастоящих Правил.
3. Владелец проверяет подлинность документов, представленных поставщиком публичных услуг или, в зависимости от случая, поставщиком услуг из частного сектора, и регистрирует его в качестве Бенефициара тестовой среды. С этого момента поставщик публичных услуг или, в зависимости от случая, поставщик услуг из частного сектораполучает статус Бенефициара услуги MPass.
4. Владелец предоставляет Бенефициару техническую документацию по интеграции. Техническая документация,описанная в главе VII настоящих Правил детализирует технический процесс аутентификации и авторизации конечных пользователей.
5. Владелец присваивает функцию Администратора доступа лицу, назначенному Бенефициаром. Этот атрибут идентичности обеспечивает доступ к функции администрирования профиля Бенефициара в тестовой среде услуги MPass.
6. Бенефициар инициирует техническую, административную и организационную подготовкуинтеграции. Владелец и технико-технологический оператор услуги MPass предоставляют техническую помощь, необходимую для интеграции.
7. Бенефициар предпринимает технические меры по интеграции услуги MPass, включая экспериментальную эксплуатацию и утверждение соответствия собственной интегрированной услуги в соответствии с главой IX настоящих Правил.
8. Бенефициар тестирует соответствие интегрированного решения и передает Владельцу результаты тестирования в соответствии с главой IXнастоящих Правил. Владелец утверждает соответствие внедрения и подтверждает его правильность.
9. Владелец регистрирует Бенефициара в производственной среде услуги MPass и предоставляет необходимые реквизиты для производственной интеграции.
10. Бенефициар конфигурирует свое техническое решение в рамках своей производственной среды для интеграции с производственной средой услуги MPass и запускает в производство свою услугу, интегрированную с услугой MPass.

## Глава VI. Регистрация бенефициаров

1. Поставщик услуг заранее обеспечивает регистрацию электронной идентичности в рамках услуги MPass для руководства и администратора доступа Бенефициара.
2. Бенефициар должен обладать сертификатами открытого ключа для тестирования и оперирования каждой услугой, которая будет интегрирована с MPass.
3. Поставщик публичных услуг и поставщик услуг из частного сектора регистрируются как Бенефициар услуги MPass путем подачи заявки на интеграцию и подписания с Владельцем соглашения или, при необходимости, договора о предоставлении услуг по аутентификации и авторизации посредствомправительственной электронной услугиаутентификации  и контроля доступа (MPass). Владелец рассматривает запрос и отвечает поставщику публичных услуг или, при необходимости, поставщику услуг из частного сектора в течение 10 рабочих дней.
4. После одобрения запроса Владелец подписывает с Бенефициаром соглашение или, при необходимости, договор о предоставлении услуг по аутентификации и авторизации посредствомправительственной электронной услугиаутентификации  и контроля доступа (MPass).
5. Для интеграции своей информационной системы с услугой MPass Бенефициар представляет Владельцу следующие атрибуты информационной системы:
6. название и описание информационной системы;
7. сертификат открытого ключа информационной системы;
8. список атрибутов идентичности, включая характерные для информационной системы, которые будут предоставлены со стороны услуги MPass в результате аутентификации.
9. Информация об информационной системе будет отображаться конечным пользователям после их первой аутентификации вданной информационной системе или после изменения этой информации.
10. Конечный пользователь знакомится с информацией, указанной в пункте 16 настоящих Правил, и дает согласие на то, чтобы его персональные данные передавались в информационную систему,интегрированнуюс услугой MPass.
11. Бенефициар должен обеспечить загрузку сертификатов открытого ключа в профили собственных информационных систем из услуги MPass и правильно конфигурировать эти профили в собственной инфраструктуре.
12. Услуга MPass автоматически генерирует по одному единому идентификатору для каждой интегрированной информационной системы и извещает об этом едином идентификаторе Бенефициару.Бенефициар обеспечивает конфигурацию этого идентификатора в соответствующей информационной системе, которая служит впоследствии для идентификации информационной системы во взаимодействии с услугой MPass.
13. Бенефициар обеспечивает целостность и безопасность закрытых ключей, используемых в своих информационных системах. Во избежание компрометации сертификатов открытого ключа в тестовой среде и в производственной среде используются разные сертификаты.

## Глава VII. Аутентификация и авторизация пользователей

1. Аутентификация и авторизация в услуге MPass основана на открытых технологических стандартах/протоколах, подробно описанных в технической документации по интеграции, предоставленной Владельцем.
2. Бенефициар должен гарантировать, что информационная система передает аутентифицированному пользователюинформацию об аутентификации.

## Глава VIII. Интеграция новых электронных услуг одного и того же Бенефициара

1. Владелец обеспечивает Бенефициару возможность интегрировать несколько информационных систем.
2. Бенефициары должны зарегeстрировать каждую свою новую электронную услугу с услугой MPass. Недопустимо оперировать несколькими специфическими услугами под одной регистрацией в услуге MPass.

## Глава IX. Утверждение соответствия интеграции

1. Владелец обеспечивает внятное описание процедуры утверждения соответствия интеграции как части технической документации.
2. Бенефициар проверяет соответствие интегрированного решенияс процедурой утверждения в период экспериментальной эксплуатации. Бенефициару необходимо устранить все обнаруженные несоответствия.
3. Владелец может оценить результаты тестирования соответствия, представленные Бенефициаром,а может самостоятельно воспроизвести шаги процедуры утверждения. При обнаружении несоответствия Владелец сообщает о них Бенефициару и требует их устранения.

## Глава X. Выделение атрибутов авторизации для услуг Бенефициара

1. Владелец обеспечивает возможность выделения или отзыва атрибутов авторизации для пользователей на основе их единого идентификатора.
2. Администратор доступа Бенефициара авторизует или отзывает атрибуты авторизации для конечных пользователей. При следующей аутентификацииинтегрированные информационные системы получат актуализированный список атрибутов авторизации аутентифицированной идентичности для соответствующей авторизации.

## Глава XI. Заключительные положения

1. Владелец не обеспечивает оснащение конечных пользователей техническими средствами идентификации для использования в услуге MPass.