

Защита личного ключа абонента

1 Защита личного ключа абонента

Настоящий документ содержит руководство по созданию и хранению личного ключа абонента удостоверяющего центра ОИПИ НАН Беларуси на специализированных аппаратных криптографических устройствах, а также на компьютерах общего назначения, при условии строгого соблюдения физических мер обеспечения безопасности и регулярного исправления или нейтрализации ошибок в используемом программном обеспечении (установки обновлений безопасности). Пароли должны быть устойчивы к взлому и выбраны согласно лучшим современным практическим рекомендациям. Если в используемом программном обеспечении есть возможность контролировать соответствие паролей заданным требованиям сложности, то данная возможность должна быть задействована.

1.1 Создание ключевой пары

Ключевая пара, на основании которой выдается сертификат, должна создаваться исключительно одним из следующих способов:

1. Внутри специализированного аппаратного криптографического устройства.
2. На локальном компьютере, на котором абонент является единственным пользователем и администратором, и при выполнении следующего требования:
 - 2.1 Ключевая пара должна быть создана при помощи доверенного криптографического программного обеспечения (например, при помощи набора программ OpenSSL с установленными новейшими обновлениями безопасности).
3. На компьютере, который администрируется организацией, в которой работает абонент, и при выполнении следующих требований:
 - 3.1 Ключевая пара должна быть создана при помощи доверенного криптографического программного обеспечения (например, при помощи набора программ OpenSSL с установленными новейшими обновлениями безопасности).
 - 3.2 Доступ к компьютеру должен быть ограничен уполномоченным персоналом, который осведомлен о применяемых правилах конфиденциальности и профессиональных правилах поведения.
 - 3.3 Личный ключ нельзя отправлять открытым текстом (в незашифрованном виде) по сети.
 - 3.4 Пароль нельзя отправлять открытым текстом (в незашифрованном виде) по сети.
 - 3.5 Файл с зашифрованным личным ключом не следует отправлять по незащищенной сети. Защита передаваемых данных по сети может осуществляться посредством шифрования информации или физическим контролем сети в доверенной среде.
 - 3.6 Не следует оставлять в системе пароли и личные ключи в открытом тексте (в незашифрованном виде) более 24 часов, если только ключевая пара не используется исключительно для создания краткосрочных мандатов, т.е. соответствующий этой паре сертификат имеет срок действия менее 1 мегасекунды.
4. На компьютере, который администрируется организацией, в которой абонент не работает, и где выполняются следующие требования:
 - 4.1 Ключевая пара должна быть создана при помощи доверенного криптографического программного обеспечения (например при помощи набора программ OpenSSL с установленными новейшими обновлениями безопасности).

- 4.2 Доступ должен быть ограничен уполномоченным персоналом, который осведомлен о применяемых правилах конфиденциальности и профессиональных правилах поведения
- 4.3 Личный ключ нельзя отправлять открытым текстом (в незашифрованном виде) по сети.
- 4.4 Пароль нельзя отправлять открытым текстом (в незашифрованном виде) по сети.
- 4.5 Файл с зашифрованным личным ключом не следует отправлять по незащищенной сети. Защита передаваемых данных по сети может осуществляться посредством шифрования информации или физическим контролем сети в доверенной среде.
- 4.6 Ключевая пара должна быть создана только в результате собственноручных действий абонента.
- 4.7 В организации должны соблюдаться меры по обеспечения конфиденциальности.
- 4.8 Компьютер должен быть размещен в безопасной среде, где доступ контролируется и ограничен только уполномоченным персоналом.
- 4.9 Не следует оставлять в системе пароли и личные ключи в открытом тексте (в незашифрованном виде) более 24 часов, если только ключевая пара не используется исключительно для создания краткосрочных мандатов, т.е. соответствующий этой паре сертификат имеет срок действия менее 1 мегасекунды.

1.2 Хранение личного ключа

Личный ключ физического лица должен храниться:

1. Защищенный паролем на специализированном аппаратном криптографическом устройстве, из которого он не может быть извлечен.
2. На локальной файловой системе на компьютере, на котором абонент является единственным пользователем и администратором, и при выполнении следующего требования:
 - 3.1 Личный ключ должен храниться только в зашифрованном виде.
3. Защищенный паролем на локальной или сетевой файловой системе на компьютере, который администрируется организацией, в которой работает абонент, и где выполняются следующие требования:
 - 3.1 Личный ключ должен храниться только в зашифрованном виде.
 - 3.2 Системы и системные администраторы не должны хранить данные, которые необходимы, чтобы расшифровать или активировать личный ключ. Только абонент собственноручно использует эти данные во время работы в системе. Данные активации и расшифрованный личный ключ запрещается оставлять в системе по истечении 24 часов после прекращения использования GRID-служб и следует удалять, как только абонент прекращает использование GRID-служб.
 - 3.3 Доступ должен быть ограничен уполномоченным персоналом, который осведомлен о применяемых правилах конфиденциальности и профессиональных правилах поведения.
 - 3.4 Личный ключ нельзя отправлять открытым текстом (в незашифрованном виде) по сети.
 - 3.5 Пароль нельзя отправлять открытым текстом (в незашифрованном виде) по сети.
 - 3.6 Файл с зашифрованным личным ключом не следует отправлять по незащищенной сети. Защита передаваемых данных по сети может осуществляться посредством шифрования информации или физическим контролем сети в доверенной среде.
 - 3.7 Не следует оставлять в системе пароли и личные ключи в открытом тексте (в незашифрованном виде) более 24 часов, если только ключевая пара не используется исключительно для создания краткосрочных мандатов, т.е. соответствующий этой паре сертификат имеет срок действия менее 1 мегасекунды.

4. На локальной или сетевой файловой системе на компьютере, который администрируется организацией, в которой абонент не работает, и где выполняются следующие требования:
 - 4.1 Личный ключ должен храниться только в зашифрованном виде.
 - 4.2 Системы и системные администраторы не должны хранить данные, которые необходимы, чтобы расшифровать или активировать личный ключ. Только абонент собственноручно использует эти данные во время работы в системе. Данные активации и расшифрованный личный ключ запрещается оставлять в системе по истечении 24 часов после прекращения использования грид-служб и следует удалять, как только абонент прекращает использование грид-служб.
 - 4.3 Доступ должен быть ограничен уполномоченным персоналом, который осведомлен о применяемых правилах конфиденциальности и профессиональных правилах поведения
 - 4.4 В организации должны соблюдаться меры по обеспечения конфиденциальности.
 - 4.5 Компьютер должен быть размещен в безопасной среде, где доступ контролируется и ограничен только уполномоченным персоналом.
 - 4.6 Личный ключ нельзя отправлять открытым текстом (в незашифрованном виде) по сети.
 - 4.7 Пароль нельзя отправлять открытым текстом (в незашифрованном виде) по сети.
 - 4.8 Файл с зашифрованным личным ключом не следует отправлять по незащищенной сети. Защита передаваемых данных по сети может осуществляться посредством шифрования информации или физическим контролем сети в доверенной среде.