Приложение № 3
к Порядку дистанционного банковского обслуживания
юридических лиц и индивидуальных предпринимателей
в АО «Тагилбанк» с использованием доступа через
информационно-телекоммуникационную сеть Интернет

БЕЗОПАСНОСТЬ
дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Тагилбанк» с использованием доступа через Интернет

1. Система безопасности

1.1. Система безопасности включает в себя следование общим рекомендациям, систему ограничения доступа на рабочем месте участника Системы и систему обеспечения секретности и подлинности (защиты) информации, передаваемой по каналам связи.

2. Общие рекомендации

2.1. Не сохраняйте Ваш пароль в текстовых файлах на компьютере либо на других электронных носителях информации, т.к. при этом существует риск его кражи и компрометации.

2.2. При любых подозрениях компрометации пароля посторонними лицами (в т.ч. представившимися сотрудниками Банка), следует незамедлительно остановить работу и обратиться в Банк по любому из телефонов: +7(3435) 977-000, +7(3435) 977-616, +7(3435) 977-619.

2.3. Используйте современное антивирусное программное обеспечение и следите за его регулярным обновлением.

2.4. Регулярно выполняйте антивирусную проверку на своем компьютере для своевременного обнаружения вредоносных программ.

2.5. Своевременно устанавливайте обновления операционной системы своего компьютера, рекомендуемые компанией-производителем в целях устранения выявленных в нем уязвимостей.

2.6. Используйте дополнительное программное обеспечение, позволяющее повысить уровень защиты Вашего компьютера – персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от “спам”-рассылок и пр.

2.7. Исключайте на ПК, на которых осуществляется подготовка и отправка документов в Банк, неконтролируемое использование систем удаленного управления ПК. Не привлекайте для администрирования и обслуживания данного ПК ИТ-персонал на условиях предоставления ему неконтролируемого удаленного доступа.

2.8. Исключайте посещение с ПК, на которых осуществляется подготовка и отправка документов в Банк, сайтов сомнительного содержания и любых других интернет-ресурсов непроизводственного характера (социальные и пиринговые сети, конференции и чаты, телефонные сервисы и т.п.), чтение почты и открытие почтовых вложений от недоверенных источников, установку и обновление любого ПО не с сайтов производителей. Настройками сетевого оборудования, корпоративных и персональных сетевых экранов выход в сеть Интернет ограничивайте “белым списком” со всех рабочих мест, на которых осуществляется подготовка, подписание и отправка платежных документов. В “белый список” должны включаться исключительно доверенные сайты и хосты самой организации, банков, налоговой службы, других государственных органов, необходимых в производственном процессе, серверы обновлений системного и антивирусного ПО.

3. Система ограничения доступа

3.1. Доступ к информации на абонентском пункте Клиента ограничен системой паролей при обращении к программному обеспечению абонентского пункта Клиента. При этом каждый сотрудник Клиента имеет свой собственный пароль для входа в Систему и свой индивидуальный код, которым отмечаются все произведенные им действия.

3.2. Банк не несет ответственности за разглашение сотрудниками Клиента их паролей, равно как и за модификации данных на абонентском месте Клиента несистемными средствами.

3.3. При регистрации клиента на Сервере Банка по запросу Системы Клиент проставляет кодовое (блокировочное) слово, по которому без проведения дополнительного расследования производится блокировка работы Клиента в Системе. Блокировка работы Клиента в Системе производится по устному запросу Клиента с обязательным указанием кодового слова. Для

отмены блокировки Клиенту необходимо предоставить в Банк письменное заявление с указанием причин отмены блокировки.

4. Защита информации, передаваемой по каналам связи

4.1. Система защиты информации, передаваемой по каналам связи, включает в себя подсистему обеспечения секретности информации и подсистему обеспечения ее подлинности.

4.2. Конфиденциальность данных обеспечивается защитой всех данных, передаваемых по каналам связи. Для защиты данных используется протокол TLS.

4.3. Каждая из сторон имеет свой набор из двух ключей - открытый ключ и закрытый ключ. Клиент хранит свой закрытый ключ на своем абонентском месте и несет полную ответственность за его секретность и конфиденциальность. С помощью этого ключа Клиент формирует ЭП под электронными документами, отправляемыми в Банк.

5. Обеспечение подлинности данных. Группы подписей под документами

5.1. Для обеспечения подлинности данных применяется ЭП. Все передаваемые Банку Клиентом или принимаемые Клиентом от Банка электронные документы могут иметь ЭП одного или более уполномоченных лиц соответствующих сторон, определяемых при регистрации на Сервере Банка.

Количество уполномоченных лиц не должно превышать 8 (восьми) человек. При этом следует учесть, что количество ЭП под каждым электронным документом должно соответствовать количеству имеющих право подписи лиц, определенных при регистрации на Сервере Банка.

5.2. Для подписи документа уполномоченными лицами соответствующих сторон используется двухключевой алгоритм. Алгоритм использует два ключа: секретный ключ, с помощью которого ставится подпись под документом, и открытый ключ, с помощью которого проверяется подпись под документом.

Каждому секретному ключу соответствует ровно один открытый ключ и наоборот. Построить секретный ключ, соответствующий заданному открытому, зная только этот открытый ключ, невозможно.

Зная открытый ключ, можно проверить правильность уже поставленной под документом с помощью соответствующего секретного ключа подписи, но невозможно правильно эту подпись поставить.

5.3. Для подписи документа уполномоченное лицо каждой из сторон использует свою личную ЭП, хранящуюся на носителе (в файловом хранилище ключей или USB-токене). Данное лицо несет полную ответственность за подлинность и конфиденциальность своей ЭП. В частности, все документы, подпись под которыми при проверке действительным открытым ключом ЭП лица является правильной, считаются подписанными этим лицом, даже если ЭП была поставлена другим лицом, получившим каким-либо образом доступ к ЭП этого лица.

5.4. Открытые ключи ЭП лиц с правом подписи хранятся у противоположной стороны и используются для проверки подписи под документами. ЭП под документом считается правильной, если проверка ЭП с помощью действовавшего на момент ее простановки ключа дает положительный результат. Проверка ЭП производится с помощью соответствующей утилиты Системы.

5.5. Стороны признают используемые в настоящей Системе электронные документы с правильной цифровой ЭП уполномоченных лиц организации юридически эквивалентными (аутентичными) бумажным документам с рукописными подписями уполномоченных лиц и печатью организации.