**ОРГАНИЗАЦИЯ ОБЪЕДИНЕННЫХ НАЦИЙ**

**E**

**ЭКОНОМИЧЕСКИЙ И СОЦИАЛЬНЫЙ СОВЕТ**

Distr.
GENERAL

ECE/TRANS/WP.30/AC.2/2008/2
21 November 2007

RUSSIAN
Original: ENGLISH

**ЕВРОПЕЙСКАЯ ЭКОНОМИЧЕСКАЯ КОМИССИЯ**

Административный комитет Конвенции МДП 1975 года

Сорок пятая сессия
Женева, 31 января 2008 года
Пункт 4 a) iii) предварительной повестки дня

ДЕЯТЕЛЬНОСТЬ И АДМИНИСТРАТИВНЫЕ ФУНКЦИИ ИСПОЛНИТЕЛЬНОГО СОВЕТА МДП (ИСМДП)

Деятельность ИСМДП

# Онлайновый реестр устройства наложения таможенных пломб и таможенных печатей

Записка секретариата МДП

## I. КРАТКИЙ ОБЗОР

1. На своей сорок четвертой сессии Административный комитет МДП просил подготовить документ с общим описанием элементов безопасности в онлайновом реестре устройств наложения таможенных пломб и таможенных печатей ЕЭК ООН. В настоящем документе представлена краткая информация по каждому из элементов безопасности для электронного реестра ЕЭК ООН. Сочетание предлагаемых элементов обеспечивает удобство пользования для конечного потребителя и высокий уровень защиты данных на основе применяемой отраслью наилучшей практики в этой области.

## II. ИСТОРИЯ ВОПРОСА И МАНДАТ

2. Проект онлайнового реестра устройств наложения таможенных пломб и таможенных печатей ЕЭК ООН призван обеспечить наличие в онлайновом режиме информации, которая сейчас представлена в бумажном реестре. Секретариату МДП поручено вести и обновлять этот реестр. В настоящее время в реестре, имеющемся на английском, русском и французском языках, содержится описание устройств наложения таможенных пломб и таможенных печатей из 55 Договаривающихся сторон для использования таможенными координационными центрами МДП и сотрудниками таможен на местах. Цель этого электронного реестра состоит в том, чтобы повысить эффективность, сэкономить время и свести к минимуму потенциальные ошибки по сравнению с нынешней системой, основанной на бумажном носителе.

3. В феврале 2007 году на своей сорок третьей сессии Административный комитет принял к сведению сообщение[1] секретариата по этому проекту. Комитет счел проект полезным, но сослался на конфиденциальный характер информации и подчеркнул необходимость обеспечения целостности данных в этом реестре. Кроме того, для достижения согласия Договаривающихся сторон на сбор и онлайновое распространение информации об устройствах наложения таможенных пломб и таможенных печатей Комитет поручил секретариату направить письменный запрос всем Договаривающимся сторонам, применяющим Конвенцию, и сообщить об итогах этого запроса на его следующей сессии (ECE/TRANS/WP.30/AC.2/89, пункт 16).

4. На своей сорок четвертой сессии в сентябре 2007 года, ознакомившись с результатами вышеупомянутого запроса, Административный комитет поручил секретариату продолжать работу над усовершенствованием этого реестра. Комитет также просил секретариат представить на следующей сессии AC.2 документ с общим описанием элементов безопасности в предлагаемом онлайновом реестре (ECE/TRANS/WP.30/AC.2/91, пункт 11).

## III. ЭЛЕМЕНТЫ БЕЗОПАСНОСТИ В ОНЛАЙНОВОМ РЕЕСТРЕ УСТРОЙСТВ НАЛОЖЕНИЯ ТАМОЖЕННЫХ ПЛОМБ И ТАМОЖЕННЫХ ПЕЧАТЕЙ ЕЭК ООН

5. В настоящем документе приводится описание всех специальных средств защиты, предназначенных для онлайнового реестра ЕЭК ООН.

---

[1] <http://www.unece.org/trans/bcf/ac2/ac2-inf-documents.html>.

6. Глоссарий ОРССИ[2] (SAML - язык разметки, предусматривающий защиту данных), версия 2.0 от 15 марта 2005 года, определяет безопасность как "*комплекс защитных средств, обеспечивающих конфиденциальность информации, защиту систем или сетей, используемых для ее обработки, и контроль доступа к ним. Обычно понятие безопасности охватывает концепции секретности, конфиденциальности, целостности и доступности. Она призвана обеспечить устойчивость системы к потенциальным атакам*".

7. Элементы безопасности для онлайнового реестра устройств наложения таможенных пломб и таможенных печатей ЕЭК ООН предоставит Европейская экономическая комиссия Организации Объединенных Наций (ЕЭК ООН).

8. Онлайновый реестр ЕЭК ООН будет защищен межсетевыми экранами. Межсетевые экраны - это компьютерные устройства, которые регулируют компьютерный трафик внутри и за пределами сети. Межсетевой экран проверяет весь сетевой трафик и блокирует передачу сообщений, которые не отвечают установленным критериям безопасности, обеспечивая таким образом устойчивость системы к атакам типа отказ в обслуживании[3]. В этом смысле межсетевой экран можно сравнить с часовым на входе в замок.

9. Чувствительная информация для конечных пользователей (такая, как пароли) будет храниться в защищенной базе данных с использованием мощных односторонних криптографических функций хеширования (например, MD5[4] или SHA-1). Криптографическая функция хеширования - это функция преобразования входных данных в слово установленного размера в нечитаемом формате, которое называется значением хеш-функции.

10. Вся информация, которая может быть легко перехвачена компьютерными пиратами в процессе передачи через Интернет, будет шифроваться. Шифрование - это метод

---

[2] Организация по развитию стандартов структурированной информации.

[3] Атака типа отказ в обслуживании (DOS-атака - это попытка посторонних лиц взломать компьютерную систему или сервис, сделав их недоступными для конечных пользователей.

[4] MD5: алгоритм представления сообщений в краткой форме 5, SHA1: защищенный алгоритм хеширования 1.

кодирования данных, с тем чтобы их не могли прочитать неавторизованные лица. С его помощью обычный текст (информация в читаемой форме) преобразовывается в закодированный текст (в нечитаемом формате). Для связи между конечным пользователем и вебсервером, на который планируется поместить онлайновый реестр ЕЭК ООН, будет использоваться 128-битовый цифровой сертификат SSL (протокол безопасных соединений (ПБС)). Сегодня 128-битовое кодирование применяется в качестве стандарта для безопасной передачи данных через Интернет. Поэтому использование криптографии подразумевает, что передаваемая информация не может быть понята третьими лицами, что обеспечивает конфиденциальность, безопасность и целостность информации.

11. Система будет автоматически блокировать нарушителей. Например, это означает, что она будет игнорировать IP-адрес[5] любого лица, использовавшего определенное число попыток незаконного проникновения в систему. Подобный способ применяется для предупреждения криптоаналитических атак, т.е. попыток подсоединения методом подбора паролей для доступа в систему. Такая "блокировка" автоматически прекращается через заданный максимальный период времени.

12. Система будет автоматически закрывать все безопасные соединения, если конечный пользователь не задействует онлайновый реестр ЕЭК ООН в течение заданного периода времени (время ожидания сеанса).

13. Система будет создавать файлы регистрации, которые будут анализироваться и просматриваться секретариатом МДП. Этот механизм позволит осуществлять регулярный мониторинг информационного потока в онлайновом реестре ЕЭК ООН и динамики операций, что поможет обнаруживать вторжение. Механизм регистрации даст возможность отслеживать действия конечных пользователей на вебсервере. Такой режим регистрации позволит выявлять и анализировать любые злоупотребления и будет дополнять механизм аутентификации. Определить причину злоупотребления без регистрационных журналов операций в системе крайне трудно. По каждому конечному пользователю эти журналы будут регистрировать:

---

[5] Каждый компьютер, подсоединенный к Интернету, идентифицируется с помощью IP-адреса, который представляет собой заданное число. В этом смысле IP-адреса сопоставимы с телефонными номерами.

a) все индивидуальные доступы конечного пользователя;

b) все осуществленные консультации (идентификация или название соответствующей страны);

c) ошибочные попытки логического доступа.

14. Регистрационные журналы будут сохраняться в течение не менее трех лет.

15. Компьютерные пираты и исследователи постоянно выявляют уязвимые стороны и слабые места с точки зрения безопасности, которые появляются в системах по мере введения нового программного обеспечения. Известные уязвимые стороны и слабые места можно устранять с помощью корректировок[6] от изготовителя программных средств[7]. ЕЭК ООН будет обеспечивать установку новых корректирующих программ по мере необходимости.

16. Управление данными в онлайновом реестре ЕЭК ООН будет осуществлять секретариат МДП.

## IV. ЭЛЕМЕНТЫ АУТЕНТИФИКАЦИИ В ОНЛАЙНОВОМ РЕЕСТРЕ УСТРОЙСТВ НАЛОЖЕНИЯ ТАМОЖЕННЫХ ПЛОМБ И ТАМОЖЕННЫХ ПЕЧАТЕЙ ЕЭК ООН

17. Секретариат рекомендует применять средства строгой аутентификации, представляющие собой комбинацию двух факторов аутентификации. В этом случае конечному пользователю будет предложено ввести учетные данные двух типов:

---

[6] Корректировка - программный продукт, предназначенный для обновления, корректирования или устранения ошибки в программном обеспечении, используемом в компьютерах или серверах.

[7] Изготовитель операционной системы или вебсервера и т.д.

a) то, что известно (*первый фактор*): имя пользователя и пароль;

b) то, что имеется (*второй фактор*): одноразовый пароль (OTP)[8].

18. Такая технология используется, например, финансовыми учреждениями для защиты своих систем трансфертных платежей и каналов связи между клиентами.

19. Использование двух факторов аутентификации, основанной на механизме одноразового пароля, обеспечивает высокий уровень надежности аутентификации (см. рис. 1). Банки входят в число основных инвесторов, вкладывающих большие средства в системы онлайновой аутентификации, причем тенденция к более широкому применению двухфакторной аутентификации для обеспечения надежности онлайновых приложений усиливается. Комбинация первого и второго факторов увеличивает надежность механизма аутентификации. Поскольку каждому фактору присущи свои слабые стороны, использование двух факторов значительно повышает устойчивость к атакам.

---

[8] OTP: одноразовый пароль. Система безопасности, которая требует указания нового пароля каждый раз, когда конечный пользователь вводит свои учетные данные для регистрации, и которая таким образом защищает от повторного использования нарушителем перехваченного пароля.

OOB: аутентификация по внешнему каналу. Данный метод предполагает использование отдельной сети/канала для передачи удостоверяющей информации конечному пользователю, например с помощью системы передачи коротких сообщений (СМС).

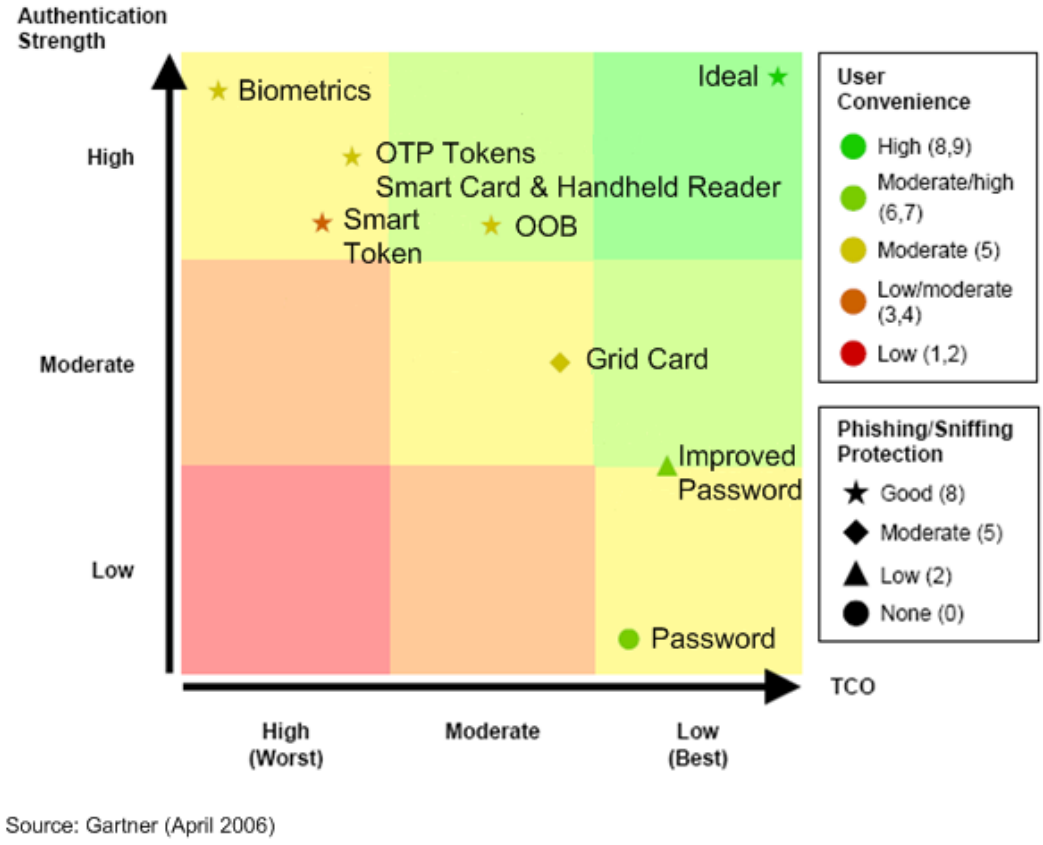


**Рис. 1: Сопоставление методов онлайновой аутентификации (только на английском языке)**


Рис. 2: Ключ безопасности

20. На рис. 1 приводится качественное сопоставление методов аутентификации. Степень надежности аутентификации отмечена на графике на вертикальной оси. Общая стоимость обладания (TCO) указана на горизонтальной оси и уменьшается слева направо. TCO включает стоимость лицензий, ключей безопасности[9], подключение к системе поддержки и т.д. Степень удобства для конечного пользователя показана цветом символов на шкале, где "low" (низкое значение) означает наихудшую степень, а "high" (высокое) наилучшую.

[9] Ключ безопасности - средство аутентификации для конечного пользователя (см. рис. 2).

Устойчивость метода к фишинг-мошенничеству[10] или снифинг-мошенничеству[11] отмечена формой символов: чем больше у символа сторон, тем выше уровень устойчивости. Кружками отмечен наихудший вариант, а звездочками наилучший. Более подробную информацию и разъяснения по поводу рис. 1 см. в приложении.

21. Сочетание всех вышеупомянутых средств защиты позволяет конечному пользователю задействовать современную технологию безопасности. В то же время конечным пользователям следует иметь в виду, что они также несут ответственность за обеспечение безопасности реестра. Речь идет о регулярном обновлении их программных средств безопасности и неразглашении имен пользователей, паролей (первый фактор) и ключей для системы двухфакторной аутентификации (второй фактор).

22. Контроль онлайнового реестра будет осуществлять независимая компания, с тем чтобы удостовериться в правильности применения всех вышеупомянутых мер.

## V. ДОПОЛНИТЕЛЬНЫЕ СООБРАЖЕНИЯ

23. Административный комитет, возможно, пожелает одобрить элементы безопасности, предлагаемые секретариатом для онлайнового реестра, и принять решение о типе требуемой аутентификации. В свете такого решения Административный комитет, возможно, пожелает рассмотреть вопрос об уровне конфиденциальности информации, содержащейся в онлайновом реестре устройств наложения таможенных пломб и таможенных печатей ЕЭК ООН.

24. Кроме того, Административный комитет, возможно, пожелает принять к сведению, что уровень безопасности, который сегодня считается достаточным, в будущем может таковым не оказаться. Поэтому важно регулярно усиливать элементы безопасности для поддержания высокого уровня безопасности. Использование в будущем аппаратных ключей для одноразовых паролей может стать следующим шагом в деле повышения безопасности. Вместе с тем такие меры по укреплению безопасности следует сопровождать контролями безопасности для обеспечения постоянного соблюдения стандартов в данной области. Исходя из этого, Административный комитет, возможно, пожелает также рассмотреть вопрос о выделении надлежащих финансовых средств на такие задачи в будущих бюджетах ИСМДП.

---

[10] Фишинг - кража личных конфиденциальных данных, таких, как имя пользователя и пароли доступа, через подставные сайты, копирующие интерфейсы легальных сервисов.

[11] Снифинг - перехват личных конфиденциальных данных, передаваемых в сети.

## Приложение

### Дополнительная информация о сопоставлении методов аутентификации

1. На рис. 1 проиллюстрированы методы однофакторной аутентификации, такие, как пароли и усовершенствованные пароли. Пароли в сочетании с именем пользователя являются базовой формой аутентификации. Усовершенствованные пароли - это пароли, в которых обязательно комбинируются буквы, цифры или специальные знаки.

2. Числа матричных карт - это серии цифр, отображенных таким образом, чтобы к ним можно было получить доступ с помощью регистрационных данных. Аутентификация по внешнему каналу (OOB) аутентифицирует конечного пользователя посредством передачи ему одноразового пароля (OTP) не на его ПК. Для этого применяется другой канал/другая сеть, например, одноразовый пароль может быть отослан через систему передачи коротких сообщений (СМС) на мобильный телефон конечного пользователя и затем введен через веббраузер для аутентификации. Смарт-ключ - это устройство (гибкий диск, КД-ПЗУ, обычно карта памяти USB), содержащее персональные данные, защищенные персональным идентификационным номером (ПИН), например цифровой сертификат. Ключи для одноразовых паролей - это персональные аппаратные устройства, выдающие случайные числа через установленный интервал времени, которые конечный пользователь передает через браузер для аутентификации. Смарт-карта - карта с чипом (например, кредитная карточка с чипом). Учетные данные конечного пользователя хранятся на чипе карты и могут считываться с помощью ручного считывающего устройства. Карточный чип защищен с помощью ПИН. Матричная карта, OOB, смарт-ключ, смарт-карта и ключи для одноразовых паролей являются методами двухфакторной аутентификации. Механизм биометрической аутентификации предполагает использование какой-либо биологической характеристики человека (например, физической характеристики, такой, как отпечатки пальцев, называемой биометрической характеристикой). Биометрия зачастую ассоциируется с дополнительным, третьим фактором аутентификации[12]; в этом случае конечный пользователь знает пароль (первый фактор) и располагает физическим ключом (второй фактор), используемым в сочетании с биометрическими данными (третий фактор). Матричная карта и ключи для одноразовых паролей представляют собой систему с одноразовым паролем, когда конечному пользователю выдается пароль, который может быть задействован только один раз и который меняется через установленный интервал времени. Метод двухфакторной аутентификации на основе ключей для одноразовых паролей обеспечивает средний уровень удобства для конечного пользователя и хорошую защиту от фишинг/снифинг-атак (см. рис. 1).

---

[12] Называется трехфакторной аутентификацией и обычно используется в армии, а также специальными и секретными службами.