РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2008 104 627** (13) **A**

(51) МПК
H04L 29/06 (2006.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21), (22) Заявка: **2008104627/09, 07.07.2005**

(43) Дата публикации заявки: **20.08.2009** Бюл. № **23**

(85) Дата перевода заявки PCT на национальную фазу: **07.02.2008**

(86) Заявка PCT:
SE 2005/001128 (07.07.2005)

(87) Публикация PCT:
WO 2007/008120 (18.01.2007)

Адрес для переписки:
129090, Москва, ул. Б.Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Ю.Д.Кузнецову, рег.№ 595

(71) Заявитель(и):
ТЕЛЕФОНАКТИЕБОЛАГЕТ ЛМ ЭРИКССОН (ПАБЛ) (SE)

(72) Автор(ы):
БАРРИГА Луис (SE),
КАСТЕЛЬЯНОС-САМОРА Давид (ES)

(54) СПОСОБ И УСТРОЙСТВО ДЛЯ АУТЕНТИФИКАЦИИ И КОНФИДЕНЦИАЛЬНОСТИ

(57) Формула изобретения

1. Способ в сети связи, которая реализует OAA/OAH3 (обобщенную архитектуру аутентификации/обобщенную архитектуру начальной загрузки), и в которой сетевой узел (120) ФСН3 (функции сервера начальной загрузки) выполняет начальные этапы, по меньшей мере содержащие авторизацию пользовательского объекта ОП (140) и установление по меньшей мере одного ключа защиты, совместно используемого с ОП, содержащего первый ключ Ks и связанный с ним идентификатор B_TID ключа, и по меньшей мере один второй ключ Ks_NAF, полученный из Ks и связанный по меньшей мере с одной функцией сетевого приложения ФСП (130), для улучшенной защиты конфиденциальности и поддержки аутентификации, содержит этапы

дополнительного генерирования сетевым узлом ФСН3 ваучера аутентификации, объявляющего, что ОП было аутентифицировано;

генерирования по меньшей мере одного идентификатора B_TID_NAF ключа, связанного с упомянутым по меньшей мере одним вторым полученным ключом, причем идентификатор ключа является уникальным для каждой ФСП;

посылки сетевым узлом ФСН3 идентификаторов B_TID и по меньшей мере одного идентификатора B_TID_NAF на ОП;

предоставления функцией сетевого приложения ФСП в ответ на обращение ОП за услугами, включающее в себя по меньшей мере один идентификатор B_TID_NAF, по меньшей мере, упомянутого идентификатора B_TID_NAF для ФСН3;

RU 2008104627 A

RU 2008104627 A

идентификации сетевым узлом ФСНЗ в ответ на упомянутый идентификатор B_TID_NAF ваучера аутентификации ОП для возможности установления статуса аутентификации ОП.

2. Способ по п.1, в котором пользовательский объект ОП идентифицируется по интерфейсу Ub между ФСНЗ-ОП упомянутым идентификатором B_TID.

3. Способ по п.1, в котором этап посылки идентификатора B_TID ключа и по меньшей мере одного идентификатора B_TID_NAF с ФСНЗ на ОП дополнительно содержит шифрование идентификаторов, используя ключ Ks.

4. Способ по п.1, в котором ваучер аутентификации является уникальным для каждой ФСП и идентифицируется упомянутым по меньшей мере одним идентификатором B_TID_NAF.

5. Способ по п.1, в котором этап предоставления дополнительно включает в себя предоставление подписи B_TID_NAF, причем подпись создается при помощи ОП, используя ключ Ks, и включается в упомянутое обращение за услугами.

6. Способ по п.5, в котором подпись включает в себя признак обновленности.

7. Способ по п.5, дополнительно содержащий этап проверки ФСНЗ подписи B_TID_NAF.

8. Способ по любому из пп.1-5, дополнительно содержащий этап установления ФСП статуса аутентификации посредством запроса ваучера аутентификации с сетевого узла ФСНЗ.

9. Способ по любому из пп.1-5, дополнительно содержащий этап установления ФСНЗ статуса аутентификации посредством анализа ваучера аутентификации.

10. Способ по любому из пп.1-5, в котором ФСП при упомянутом предоставлении дополнительно включает в себя запрос ключа Ks_NAF.

11. Способ по любому из пп.1-5, в котором ваучер аутентификации включает в себя информацию о, по меньшей мере, одном из: времени достоверности, времени для аутентификации и способа аутентификации.

12. Способ по п.8, дополнительно содержащий этапы

представления ФСП для сетевого узла ФСНЗ дополнительных требований для подтверждения достоверности авторизации;

проверки ФСНЗ для ФСП, какие из дополнительных требований выполнены.

13. Способ по любому из пп.1-3, дополнительно содержащий этап посылки ФСНЗ на ОП ваучера аутентификации совместно с посылкой идентификаторов или отдельно от них.

14. Способ по п.13, в котором ваучер аутентификации выполнен уникальным для каждой ФСП и идентифицируется упомянутым по меньшей мере одним идентификатором B_TID_NAF.

15. Способ по п.14, в котором ваучер аутентификации выполнен уникальным посредством шифрования его ФСНЗ, используя ключ Ks и выбранное случайное число (Rand), различное для каждой ФСП, по формуле Encr(Ks, ваучер, Rand), где Encr представляет собой функцию шифрования, и в котором упомянутый способ дополнительно содержит установление статуса аутентификации посредством

посылки зашифрованного ваучера аутентификации ФСНЗ;

расшифрования ФСНЗ ваучера аутентификации и проверки его достоверности;

выбора ФСНЗ нового случайного числа (Rand2) и повторного шифрования ваучера аутентификации во второй раз ключом Ks следующим образом: Encr(Ks, Encr(Ks, ваучер, Rand2));

возврата ФСНЗ повторно зашифрованного ваучера аутентификации на ОП через ФСП;

расшифрования ОП принятого ваучера аутентификации один раз для получения:

RU 2008104627 A

RU 2008104627 A

Encr(Ks, ваучер, Rand2);

использования ОП расшифрованного один раз ваучера аутентификации при последующем обращении к ФСП.

16. В сети связи, которая реализует архитектуру OAA/OAHЗ, сетевой узел ФСНЗ (120) выполняет аутентификацию пользовательского объекта ОП (140) и согласовывает совместно используемый ключ Ks с ОП (140), причем сетевой узел ФСНЗ (120) дополнительно содержит

средство (320) для генерирования идентификатора B_TID, связанного с Ks;

средство (320) для генерирования по меньшей мере одного полученного ключа Ks_NAF, связанного с по меньшей мере одной функцией сетевого приложения ФСП (130) и для генерирования по меньшей мере соответствующего идентификатора B_TID_NAF, причем идентификатор является уникальным для каждой ФСП (130);

средство (330) для генерирования ваучера аутентификации, объявляющего, что ОП было аутентифицировано;

средство (360) для хранения ключей, идентификаторов ключей и ваучера аутентификации и для связывания этих объектов с ОП;

средство (310) для посылки B_TID и по меньшей мере одного B_TID_NAF на ОП;

средство (360) для извлечения, в ответ на прием по меньшей мере одного идентификатора B_TID_NAF, относящегося к оборудованию пользователя ОП, соответствующего ваучера аутентификации для возможности установления статуса аутентификации ОП.

17. Сетевой узел по п.16, дополнительно содержащий средство (380) для шифрования с использованием ключа Ks и алгоритма шифрования (Encr).

18. Сетевой узел по п.17, содержащий средство (390) для генерирования случайного числа Rand, и в котором упомянутое средство (380) для шифрования используется для шифрования ваучера аутентификации в виде Encr(Ks, ваучер, Rand).

19. Сетевой узел по п.16, содержащий средство (310) для приема и ответа на запрос от ФСП, касающийся подробностей аутентификации пользовательского объекта ОП, полученных от средства (340), анализирующего ваучер аутентификации.

20. Сетевой узел по п.19, в котором упомнутый запрос касается любого или всех из времени для аутентификации, способа аутентификации или времени действия аутентификации.

21. Система обеспечения улучшенной защиты конфиденциальности и аутентификации в сети связи, реализующей инфраструктуру (100) OAA/OAHЗ, причем система содержит

функцию сервера начальной загрузки ФСНЗ (120), которая предоставляет ваучер аутентификации, объявляющий аутентификацию пользовательского объекта ОП (140), и идентификаторы B_TID_NAF ключей Ks_NAF, связанных с по меньшей мере одной функцией сетевого приложения ФСП, причем идентификаторы являются уникальными для каждой ФСП (130);

интерфейс Ub между ФСНЗ (130) и ОП (140), который дополнительно защищен посредством шифрования с использованием ключа Ks, совместно используемого ФСНЗ (130) и ОП (140);

интерфейс Ua между ОП (140) и ФСП (130), который дополнительно защищен от атак соединением с подстановкой посредством подписания сообщений, используя ключ Ks и признак обновленности;

по меньшей мере одну функцию сетевого приложения ФСП (130), предназначенную для связи с ФСНЗ (120) в отношении достоверности ваучера аутентификации так, чтобы предотвратить сговор нескольких ФСП (130) с целью отслеживания

RU 2008104627 A

RU 2008104627 A

пользовательского объекта ОП (140).

22. Система по п.21, в которой дополнительно содержится

средство (330) для ограничения информации в ваучере аутентификации только объявлением, что имела место аутентификация;

средство для предоставления ФСП (130) для задания дополнительных требований, относящихся к аутентификации пользователя, и средство (340) на ФСНЗ (130) для проверки выполнения каждого дополнительного требования.

23. Система по п.21, в которой дополнительно содержится средство (380) для шифрования ваучера аутентификации с использованием ключа Ks и в зависимости от случайного числа так, чтобы формировать уникальный ваучер аутентификации для каждой ФСП (130).

RU 2008104627 A