(19) Евразийское патентное ведомство

(11) 043360 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2023.05.17

(21) Номер заявки
201691100

(22) Дата подачи заявки
2014.11.28

(51) Int. Cl. ***H04L 9/32*** (2006.01)
G06Q 20/38 (2012.01)

(54) СПОСОБ АУТЕНТИФИКАЦИИ И/ИЛИ ИДЕНТИФИКАЦИИ В СЕТИ СВЯЗИ

(31) **10 2013 019 870.4**
(32) **2013.11.28**
(33) **DE**
(43) **2016.09.30**
(86) **PCT/EP2014/076016**
(87) **WO 2015/079045 2015.06.04**

(71)(72)(73) Заявитель, изобретатель и патентовладелец:
КИСТЕРС ФРИДРИХ (CH)

(74) Представитель:
Медведев В.Н. (RU)

(56) GB-A-2387999
US-A-5060263
US-A1-2013054474

(57) Изобретение относится к способу аутентификации и/или идентификации устройства, услуги, лица и/или денежного средства в сети связи, состоящей из первого устройства связи и другого устройства связи, например центральной базы данных, между которыми выполняется запрос аутентификации. Для этого сначала предоставляется первый ключ в устройстве связи, который содержит по меньшей мере одну последовательность символов из отдельного или нескольких локально изменяемых символов, которые динамически изменяются в зависимости от измеряемого параметра или зависимого от измеряемого параметра алгоритма, правила и/или инструкции в устройстве связи между двумя моментами времени аутентификации. Кроме того, предоставляется второй ключ в центральной базе данных или другом абоненте связи, который содержит последовательность символов, состоящую из централизованно изменяемых символов и, при необходимости, неизменяемых символов. На последующем этапе осуществляется передача и сопоставление ключей, сохраненных в центральной базе данных и устройстве связи.

043360 B1

043360 B1

Область техники

Изобретение относится к способу аутентификации и/или идентификации устройства, услуги, лица и/или денежного средства в сети связи, состоящей из устройства связи и центральной базы данных, между которыми выполняется запрос аутентификации.

Предшествующий уровень техники

Известны различные способы обеспечения защиты для выполнения обмена данными в сети между различными абонентами сети. Например, в WO 2013/116019 A1 описан способ обеспечения защиты, в котором так называемый динамический защитный код криптографически идентифицирует мобильное устройство связи пользователя в сети. При этом динамика кода состоит в замене защитного элемента после каждой выполненной аутентификации. В этом способе, таким образом, речь идет о динамически следующих друг за другом статических защитных кодах. Сами коды остаются статическими и не изменяются непрерывно, а полностью заменяются, то есть заново вычисляются и выдаются. При этом различные запросы подтверждения безопасности могут выполняться между поставщиком услуг и пользователем или его устройством.

US 2007/0260544 A1 описывает способ и систему для динамической аутентификации вместо статического PIN-кода, который изменяется перед каждой новой транзакцией. Таким образом, транзакция должна быть авторизована через сеть транзакций. Таким образом, и здесь речь идет о динамически следующих друг за другом статических защитных кодах, которые изменяются только в случае транзакции и допускают однократное применение.

В EP 1804418 A1 описан способ, который применяет динамический пароль, в который вставляется ключ, который генерируется посредством некоторого алгоритма. При этом параметр инициализации хранится в коммуникационной карте памяти. И здесь динамический код описан как однократно используемый код, который динамически генерируется для каждой аутентификации. При этом сам код не изменяется, но каждый раз заново вычисляется и заменяется. В соответствии с этим он хотя и генерируется динамически, однако в остальном является статическим, так как он из-за вычисления заново не проходит через процесс изменения.

В US 7106845 B1 раскрывает систему безопасности с различными уровнями защиты, которые могут выбираться для конкретного пользователя. При этом один уровень может использовать алгоритм, который изменяет определенные значения, причем алгоритм известен пользователям. Например, алгоритм может состоять из последовательности символов, которая включает в себя, например, время суток или дату. Зависимый от времени код изменялся бы при этом таким же образом. Другой уровень защиты отправляет случайную часть пользователю (например, с помощью мобильного телефона). При этом профиль пользователя хранится в базе данных. Динамический код вычисляется в этом способе через динамические факторы при аутентификации, но затем является статическим и поэтому может использоваться только однократно. И в данном случае код хотя и генерируется динамически, но затем остается статическим, так как он после своей генерации больше не проходит процесс изменения, а должен каждый раз генерироваться заново.

Существуют способы для генерации "цифрового денежного средства" или цифровой банкноты, которая может быть использована для оплаты. Такой способ описан, например, в WO 2013/131560, в нем физические и/или численные параметры существующей банкноты сначала собираются, а затем посредством алгоритмов переводятся в электронную форму.

Кроме того, в WO 2013/1244991 A1 описан способ выполнения транзакций с цифровыми банкнотами, причем способ предусматривает идентификацию, валидацию (проверку действительности) и авторизацию для цифровой банкноты.

Многие известные способы защиты предусматривают жестко установленные запросы касательно защиты, например, запрос паролей или PIN-кодов. Наряду с этим существуют способы, которые работают с динамическим кодом, который изменяется периодически или в соответствии с алгоритмом, причем динамической является только его генерация. После динамической генерации код остается статическим и поэтому может применяться только однократно. Таким образом, он вычисляется заново при каждой последующей аутентификации. Такие способы могут быть преодолены злоумышленником, если он противозаконно получает доступ к соответствующей базе данных или алгоритму. Поэтому часто для идентификации используются биометрические признаки, которые, однако, подвержены подделке и копированию.

Так в EP 0996928 D1 описан способ аутентификации, в котором код состоит из случайной части и неслучайной части (например, идентификационного номера). При этом как случайная часть, так и неслучайная часть кода являются статическими, т.е. код сам по себе статически не изменяется далее. Применение случайного кода должно повысить уровень защиты. Аналогичный способ описан также в US 4,998,279 A, где описан статический код, который состоит из динамических переменных (например, даты или времени). Динамическое изменение этих переменных, которое не является предсказуемым, не раскрыто в данной публикации.

DE 102011101711 A1 описывает способ аутентификации, в котором предусмотрены статический компонент и динамический компонент. Для формирования динамического компонента предусмотрено

правило формирования. На одном этапе способа генерируется код аутентификации за счет того, что обрабатываются информации аутентификации статического компонента, правило формирования для определения динамического компонента, а также параметр состояния в форме значения состояния. Параметр состояния может, например, представлять собой время суток. И в данном случае не имеется индивидуального локального параметра для формирования динамического, непредсказуемого компонента.

В DE 102011085538 A1 описан способ, в котором последовательность символов имеет предопределенный набор символов. С помощью средств генератора случайных чисел осуществляется выбор по меньшей мере одного символа из предопределенного набора символов, чтобы заменить этот символ. При этом несколько символов могут быть выбраны из предопределенного набора символов посредством генератора случайных чисел. Затем выбранный символ или символы отображаются на устройстве отображения. На последующем этапе осуществляется прием третьей последовательности символов. И, наконец, проверяется, совпадает ли третья последовательность символов с второй последовательностью символов.

В US 6636973 B1 описан способ, в котором динамически изменяемый пароль пользователя используется при идентификации в компьютерной сети. Сначала для этого регистрируется биометрический признак пользователя и преобразуется в код. Этот код ассоциирован с паролем пользователя, который изменяется при регистрации в сети. Вновь созданный пароль хранится в базе данных пользователя. Таким образом, происходит динамическое изменение, как только пользователь регистрируется в сети. Передача динамически изменяющегося кода и перекрестная проверка не предусмотрена.

Эти способы не обеспечивают достаточный уровень защиты, если злоумышленник противоправно использует доступ к локальному или центральному устройству связи, например, серверу для выполнения услуг, например, финансовых транзакций. Поэтому была бы желательна система защиты, которая является устойчивой к несанкционированному доступу к центральной или локальной базе данных и могла бы использоваться человеком, устройством, а также абстрактно для авторизации услуг или денежных средств.

Сущность изобретения

Исходя из этих предпосылок, задачей настоящего изобретения является создание усовершенствованного способа аутентификации и/или идентификации устройства, услуги, лица и/или денежного средства в сети связи, в котором проверка базируется на применении непредсказуемых динамических компонентов.

Эта задача решается описываемым здесь способом, соответствующим изобретению.

Соответствующие изобретению способы пригодны для аутентификации и/или идентификации устройства, услуги, лица и/или денежного средства. В принципе, конкретные предметы, лица, услуги Интернет-провайдера (например, финансовые услуги, Интернет-транзакции, медиа-предложения) или денежные средства могут регистрироваться способом, соответствующим изобретению. При этом исходят из сети связи (например, проводной или беспроводной сети общего пользования, такой как Интернет или внутренняя сеть или интранет), которая состоит из одного или нескольких абонентов. При этом имеются локальные абоненты и/или центральная база данных, в которой сохранены информации об устройстве, услуге, лице и/или денежном средстве абонентов. Однако способ также функционирует среди абонентов, причем "центральная база данных" соответствует одному или нескольким абонентам. Соответствующий изобретению способ обеспечивает возможность аутентификации и/или идентификации абонента, его устройства, а также может идентифицировать или аутентифицировать для использования средство платежа или услугу, которую абонент хотел бы использовать. Термин "центральная база данных" должен толковаться широко в контексте настоящего изобретения и может относиться не только к базе данных системы обработки данных. Этот термин включает, например, систему обработки данных, аппаратный сервер или другое стационарное, мобильное или портативное устройство связи.

Чтобы иметь возможность использовать, например, определенную услугу поставщика услуг, сначала лицо и/или устройство должно быть идентифицировано, чтобы пользователь или его устройство могло получить доступ к услуге. С этим может быть связана, например, также платежная система, которая позволяет пользователю оплачивать используемую услугу надежно и безналичным способом. Это может, например, осуществляться посредством зашифрованной внутри устройства суммы кредита или внутренне сохраненного "цифрового кредитного билета", который после выполненной транзакции полностью или частично стирается или становится недействительным, или заново назначается.

В качестве релевантного для защиты элемента в соответствующем изобретению способе используются "ключи" нового типа, которые соотнесены с каждым абонентом сети и/или одной или несколькими центральными базами данных. "Ключи" состоят из последовательностей символов или символов, которые могут быть либо изменяемыми, либо статическими, причем один партнер либо не знает точные состояния динамических символов или последовательностей символов другого, либо знает лишь частично. Последовательность символов состоит из нескольких символов, причем символы могут быть расположены предпочтительно последовательно или разветвленно по отношению друг к другу. Кроме того, несколько последовательностей символов могут быть взаимосвязаны друг с другом, при этом установленное перед этим расположение последовательностей символов в ключе, наряду с изменчивостью отдельных символов или целых последовательностей символов, может представлять собой особенный защит-

ный признак.

Сгенерированный в соответствии с изобретением ключ может временно храниться в центральной базе данных, чтобы идентифицировать абонентов в сети связи или их устройства, а также авторизовать использование услуг. Отдельные ключи состоят из по меньшей мере одной последовательности чисел, состоящей из по меньшей мере 5, 10, 20, 50, 70, 100, 200 или более символов. Предпочтительно, также может быть предусмотрено несколько последовательностей символов с изменяемыми и/или неизменяемыми символами. При этом ключи могут содержать специфические для лиц, услуги, устройств информации или параметры, например, идентификационный номер пользователя, сетевой номер устройства, дату, физические параметры, денежную стоимость или также суммы цифр чисел или контрольные суммы этих параметров, которые обеспечивают возможность однозначной идентификации или соотнесения лица или устройства в сети связи.

Изобретение по существу базируется на двух базах данных, которые в целях различения обозначаются как локальная и центральная база данных. Локальная база данных сохранена, например, в устройстве связи, таком как портативный персональный компьютер (PC), планшет или смартфон. Термин "локальный" означает, например, мобильный телефон или портативное устройство связи, термин "центральный" означает устройство обработки данных (сервер) или другое мобильное или портативное устройство связи. Термины "локальный" или "центральный" поэтому служат лишь для дифференцирования/различения.

Особенность настоящего изобретения заключается в том, что как в устройстве связи, так и в центральной базе данных сохранен по меньшей мере один ключ, который состоит из по меньшей мере одной последовательности символов, и каждая последовательность символов в соответствующем ключе состоит из изменяемых и/или неизменяемых символов, причем изменение символов осуществляется локально или централизованно и/или в обоих местах. При этом предпочтительно может быть предусмотрено, что изменяемые символы могут изменяться только локально, только централизованно или в обоих местах, в то время как неизменяемые символы могут изменяться, например, только в центральной базе данных, но не в устройстве связи. Термины "изменяемый" или "неизменяемый" поэтому всегда следует рассматривать с точки зрения соответствующей базы данных и момента времени аутентификации. Определенные символы остаются неизменяемыми во время или между двумя моментами времени аутентификации, однако изменяются снова при аутентификации, например, заменяются другими символами или возвращается в исходное состояние.

В предпочтительном варианте выполнения изменяемые символы являются динамически изменяемыми, т.е. локально динамически изменяемыми или централизованно динамически изменяемыми. В случае локально динамически изменяемых символов центральная база данных не "знает", на какой основе базируются эти изменения. Напротив, динамические централизованные изменения локальной базы данных в устройстве связи, таком как мобильный телефон или смартфон, не известны.

Динамические изменения, которые, например, осуществляются локально на устройстве связи, не являются предсказуемыми для центральной базы данных и, следовательно, не могут также быть взломаны хакером. С другой стороны, динамические изменения в центральной базе данных известны только ей, поскольку соответствующие правила или инструкции не сохранены в локальном устройстве связи. Наряду с этим имеются статические символы, то есть символы, которые не изменяются между двумя моментами времени аутентификации и только при запросе аутентификации могут изменяться (но не должны, например, путем возврата в исходное состояние или замены вновь сгенерированным символом). При этом вновь сгенерированный символ может предпочтительно происходить из динамически изменяемой последовательности символов. Числа изменяемой последовательности символов были бы тогда косвенно частью статической последовательности символов. Например, может быть предусмотрено, что центральная база данных содержит динамически изменяемые символы, которые непрерывно изменяются на основе только локально доступных факторов, которые не могут быть вычислены заранее (без того, чтобы эти изменения стали известны устройству связи). При аутентификации, дополнительно определенные символы (например, любые или, например, дата или время суток) могли бы служить в качестве основы для статических символов, которые при запросе передаются от центральной базы данных на устройство связи. Кроме того, определяющие идентичность символы (=уникальный идентификатор (ID)), пароль или код могут быть частью последовательности символов, которая не изменяется.

В соответствии с этим для изменяемых символов различают динамически изменяемые символы, которые изменяются либо локально, либо централизованно, и символы, которые изменяются только при запросе аутентификации, а также, при необходимости, символы, которые никогда не изменяются. Неизменяемые символы представляют собой символы, которые по меньшей мере между двумя запросами аутентификации остаются статическими или неизменными.

При этом целые последовательности символов или также отдельные символы в пределах последовательности символов могут изменяться, причем изменяемые символы или изменяемая последовательность символов не известны соответствующему другому абоненту связи. С другой стороны, неизменяемые символы не обязательно известны другому абоненту связи. Если имеются, например, символы, которые изменяются только локально в устройстве связи, то центральная база данных не распознает, какие

символы изменяются локально в устройстве связи, и на каких воздействиях основано это изменение. Она также не распознает, как составляются изменения, и какова причина этих изменений. Соответствующие правила, которые определяют характер и степень изменений в последовательности символов, в этом случае были бы известны только устройству связи, но не центральной базе данных. В зависимости от случая применения, это, конечно, может также применяться к обратной ситуации, т.е. изменения централизованно изменяемых символов или всей последовательности символов центральной базы данных известны только последней, но не устройству связи. Поскольку эти изменения сохраняются после каждой аутентификации в соответствующей другой базе данных в качестве нового состояния, с одной стороны, не представляется возможным регистрироваться с ранее выполненной копией, которая отображает еще предыдущее состояние, а с другой стороны, не представляется возможным копировать новое состояние в изменяющейся базе данных, так как оно не остаются неизменным, а непрерывно изменяется в дальнейшем. Поэтому противоправное применение обнаруживается самое позднее при последующем использовании корректной последовательности символов, если это использование уже было сделано, то противоправное применение немедленно обнаруживается.

Отдельные или несколько локально изменяемых символов изменяются в соответствии с изобретением в зависимости от измеряемого параметра, например, физически или химически определяемого параметра. Для этой цели предпочтительно используются датчики или измерительные устройства, которые определяют параметр состояния в устройстве связи или вне его. Примером может служить измерение температуры процессора внутри или внешней температуры. На основе определенного измеренного параметра на последующем этапе изменяемые символы или последовательность символов могут изменяться непредсказуемым образом. Определение измеренного значения обеспечивает, таким образом, определенное числовое значение, которое используется для динамического изменения защитного кода. Кроме того, также возможно, что определенный измеряемый параметр оказывает воздействие на существующий алгоритм, правило и/или инструкцию, либо в устройстве связи, либо в центральной базе данных. Возможны, например, внешние или внутренние воздействия, которые приводят к изменению динамического кода. Внешние или внутренние воздействия предпочтительно основаны на физических или химических свойствах или процессах. Внутреннее воздействие включает в себя, например, состояние батареи, температуру процессора, таймер, момент времени последней(их) аутентификации(й), разницу между двумя значениями времени, импульс или алгоритм, зависящий от параметров, специальную конфигурацию (например, версию операционной системы, загруженный мобильный пакет программного обеспечения (APP), используемые приложения или открытые приложения). Кроме того, воздействия могут также включать в себя индивидуальную модификацию (например, дополнительная SD-карта, обновление RAM) или специфические для приложения или зависящие от пользователя признаки (например, типовая загрузка процессора, рабочая температура). Внешнее воздействие включает в себя, например, локальное, внешнее изменение температуры, изменение давления, количество или интенсивность вибраций, изменение положения движущегося абонента, типичные или характеристики режима работы и управления пользователя (например, количество параллельных контактов с другими пользователями, контакты за временной интервал, какие контакты=группе контактов, причем она может существенно изменяться в зависимости от времени суток), частоту использования, также в зависимости от времени суток/временного интервала, громкость речи, другие предпочтения, такие как любимая музыка, предпочтительные APP, предпочтительные слова и сокращения слов. Правило включает в себя, например, применение основного правила вычисления, обратный отсчет или прямой отсчет значения или числа, общий алгоритм или также колебание в определенных пределах и смещение позиции счета. Инструкция включает в себя, например, увеличение или уменьшение суммы кредита на определенную величину, расходование суммы кредита, установленное изменение последовательности символов или присвоение значения. Например, последовательность символов может включать в себя денежную сумму, которая полностью используется в качестве средства оплаты, причем последовательность символов после транзакции частично или полностью аннулируется.

Для соответствующего изобретению способа требуется в одном варианте стационарный сервер и устройство мобильной связи, такое как компьютер, ноутбук, мобильный телефон, планшет или смартфон и центральную базу данных, причем между устройством связи и центральной базой данных выполняется запрос аутентификации. Как правило, центральная база данных находится на стационарной серверной системе. Однако также возможно место хранения на другом устройстве связи или сервере (стационарном или мобильном). В рамках запроса аутентификации, устройство, услуга, лицо и/или денежное средство аутентифицируется и/или идентифицируется.

На первом этапе, сначала в устройстве связи предоставляется первый ключ, который включает в себя по меньшей мере одну локально сохраненную последовательность символов. Термин "локально" здесь означает сохранение в устройстве связи, термин "централизованно" означает сохранение не в локальной базе данных. Сохраненная локально в устройстве связи последовательность символов предпочтительно состоит из отдельных или нескольких локально изменяемых символов, которые динамически изменяются в зависимости от физического параметра, т.е. внутреннего или внешнего воздействия, зависимого от измеренного параметра алгоритма, правила и/или инструкции в устройстве связи между двумя момента-

ми времени аутентификации. Это динамическое, прогрессивное изменение происходит, в одной форме выполнения, только в символах или последовательности символов устройства связи. Центральная база данных не "знает" эти изменения в символах или последовательности символов устройства связи. Таким образом, центральная база данных также не знает правила или воздействия, лежащие в основе этих изменений.

Динамическая изменчивость включает в себя обмен, удаление, дополнение или другие изменения отдельных или многих символов или целых последовательностей символов. Предпочтительно, например, изменяемые символы могут изменяться в последовательности символов с разными скоростями. Например, можно предусмотреть правило, что числовое значение изменяется в соответствии с временным тактом либо вверх, либо вниз. Для других символов в последовательности символов могут быть предусмотрены более быстрые изменения с другим временным тактом, например, отсчет в секундах вверх или вниз перед установленными символами или последовательностями символов. Эта задержка или ускорение временного такта динамического изменения (например, временной последовательности, частоты изменения, интервала) также может находиться под воздействием локально имеющих место физических или химических параметров, которые также могут быть частью локально сохраненной динамической последовательности символов и, тем самым, устанавливать переменное соотношение с возможностью изменения других динамических символов. Таким образом, локальный фактор может непосредственно оказывать воздействие на возможность изменения.

Локально сохраненная последовательность символов в ключе устройства связи состоит в одной форме выполнения из отдельных или нескольких локально неизменных символов, в этой или любой другой локально сохраненной последовательности символов, которые между двумя моментами времени аутентификации остаются статическими в устройстве связи. Таким образом, также имеется ситуация, когда ключ состоит из локально изменяемых символов и локально неизменяемых символов. Локально изменяемые символы, как описано выше, изменяются, например, в соответствии с локально доступным измеренным значением, сохраненным правилом или инструкцией, в то время как неизменяемые символы между двумя моментами времени аутентификации, то есть моментами времени, в которые осуществляется запрос и сопоставление между устройством связи и центральной базой данных в сети связи, остаются неизменными.

В соответствии с изобретением, предусмотрен второй ключ, который хранится в центральной базе данных. Этот второй ключ также включает в себя последовательность символов, которая состоит из централизованно изменяемых и централизованно не изменяемых символов или последовательностей символов. Сохраненный в центральной базе данных второй ключ состоит из отдельных или нескольких символов, которые соответствуют таковым из локально изменяемых символов устройства связи в последний момент времени аутентификации. Централизованно неизменяемые символы в момент времени запроса соответствовали бы состоянию локально изменяемых символов при последнем запросе. Другими словами, локально изменяемые при последнем запросе аутентификации символы или последовательность символов устройства связи передаются в центральную базу данных и актуализируют соответствующие централизованно неизменяемые символы или последовательность символов в центральной базе данных. Эти символы предпочтительно не изменяются в центральной базе данных до следующего запроса аутентификации и остаются статическими. Централизованно изменяемые символы, в свою очередь, соответствовали бы локально неизменяемым символам. Посредством сравнения с последним состоянием изменяемых символов можно установить, совпадает ли переданная последовательность символов с сохраненной последовательностью символов, то есть, имеет ли место однозначная аутентификация. В случае противоправной аутентификации, последовательность символов использовалась бы между двумя моментами времени аутентификации, так что два различных пользователя должны существовать под одинаковым идентификатором, из которых один аутентифицировался противоправно.

Конечно, также может быть предусмотрено, что централизованно неизменяемые (или также локально неизменяемые) символы периодически изменяются (и, таким образом, становятся изменяемыми символами) или не изменяются между двумя моментами времени запроса. Также изменяемые символы могут быть преобразованы в неизменяемые символы. В связи с этим ключ, соответствующий изобретению, является гибким. Однако предпосылкой является состав динамических и статических символов. На основе такого состава, последовательности символов могут взаимно проверять друг друга и гарантировать целостность аутентификации.

Предпочтительно, однако, локально неизменяемые символы или последовательности символов при запросе аутентификации с помощью централизованной базы данных централизованно изменяются. Если бы эти символы в последующем запросе аутентификации не изменились, то можно было бы быстро установить, что устройство связи используется неправомерным лицом.

Второй ключ центральной базы данных предпочтительно состоит из отдельных или нескольких централизованно изменяемых символов в данной или другой последовательности символов, которые соответствуют локально неизменяемым символам или последовательности символов устройства связи в последний момент времени аутентификации. Централизованно неизменяемые символы центральной базы данных при запросе аутентификации передаются на устройство связи и актуализируют соответст-

вующие локально изменяемые символы или последовательности символов. Если бы эти символы были по меньшей мере частично изменены или подделаны, то можно было бы установить попытку несанкционированного доступа к ним неправомочного лица. Только центральная база данных "знает" централизованно изменяемые символы, которые сохранены в ключе. И наоборот, только устройство связи (то есть, локальная база данных) "знает" локально изменяемые символы. Централизованно неизменяемые символы хранятся в базе данных и соответствуют символам последнего момент времени аутентификации.

На следующем этапе способа осуществляется передача и сопоставление сохраненного в устройстве связи ключа с ключом, сохраненным в центральной базе данных в последний момент времени аутентификации. В соответствии с изобретением положительная аутентификация и/или идентификация устройства, услуги, лица и/или денежного средства в момент времени аутентификации осуществляется тогда, когда выполняются по меньшей мере следующие признаки:

i) по меньшей мере частичное совпадение локально неизменяемых символов или последовательности символов в ключе устройства связи с соответствующими локально изменяемыми символами или последовательностью символов в последнем ключе центральной базы данных;

ii) по меньшей мере частичное несовпадение локально изменяемых символов или последовательности символов в ключе устройства связи с соответствующими централизованно неизменяемыми символами или последовательностью символов в ключе центральной базы данных.

Предпочтительно, может устанавливаться полное совпадение или несовпадение. Локально изменяемые символы или последовательность символов между двумя моментами времени аутентификации в соответствии с изобретением могут изменяться только в устройстве связи, но не в центральной базе данных, и централизованно изменяемые символы или последовательность символов могут изменяться только в центральной базе данных, но не в устройстве связи. В соответствии с изобретением далее предусмотрено, что при успешной аутентификации локально неизменяемые символы или последовательность символов в ключе центральной базы данных сбрасываются или изменяются. Таким образом, локально сохраненные в устройстве связи неизменяемые символы или последовательность символов соответствуют централизованно изменяемым символам или последовательности символов в ключе центральной базы данных, если произошло сопоставление.

При сбросе или изменении централизованно изменяемых (=локально неизменяемых) символов или последовательности символов в ключе центральной базы данных устройство связи получает в момент времени аутентификации в этом варианте осуществления дополнительно разработанный "набор символов". В этом случае, этот централизованно изменяемый набор символов может также содержать новую информацию, например, актуализированную денежную сумму, дату или разницу между двумя моментами времени запроса. В соответствии с изобретением, либо отдельные символы, последовательности символов полностью или полный ключ могут передаваться между центральной базой данных и устройством связи (и обратно). Этот новый набор данных изменяется теперь между моментами времени аутентификации динамически в зависимости от локально присутствующих факторов, таких как температура окружающей среды, что эффективно предотвращает его копирование.

За счет объединения локально изменяемых и локально неизменяемых символов или централизованно изменяемых или централизованно неизменяемых символов (или последовательностей символов) в центральной базе данных достигается высокий уровень защиты для аутентификации и/или идентификации устройства, услуги, лица или денежного средства. Если бы неправомочное лицо получило доступ к центральной базе данных, оно не смогло бы завладеть правилами, которые определяют изменение символов в локальной базе данных, так как эти правила находятся под воздействием или дополняются локально измененными измеренными значениями. Поэтому при аутентификации не может фальсифицироваться ни подделанная центральная база данных, ни подделанная локальная база данных. Фальсификатор не знает обстоятельств, факторов и особенно локальных динамических значений, которые могут оказывать воздействие на динамические изменения. Даже если бы фальсификатор имел одновременный доступ к центральной и локальной базе данных, он не смог бы быть успешно аутентифицирован и был бы раскрыт самое позднее при запросе правомерного пользователя, так как вызванные им изменения в центральной базе данных (инициированные проведенной аутентификацией) больше не соответствовали бы таковым в локальной базе данных правомерного пользователя. Если эта защита от фальсификации связывается с биометрическим признаком, то фальсификатор теряет всякую возможность незаметно подделать идентификацию другого лица.

Способ также работает в обратном направлении, то есть динамически изменяемые символы или последовательность символов сохранены в центральной базе данных. Кроме того, последовательности символов могут содержать символы, которые изменяются динамически только в устройстве связи, и/или символы, которые динамически изменяются только в центральной базе данных. Таким образом, динамика согласно настоящему изобретению может использоваться на различных стадиях (только локально, только централизованно или локально-централизованно).

Если принципы, описанные выше для устройства связи, реализуются для центральной базы данных, то ключ центральной базы данных включает в себя динамически изменяемые символы. Повышению защиты в конечном счете способствуют динамические символы, в то время как статические, как правило, служат для более легкого распознавания. В варианте способа они также могут быть опущены.

В соответствии с изобретением, способ включает в себя следующие этапы:

предоставление первого ключа в центральной базе данных, который содержит по меньшей мере одну последовательность символов, состоящую из

отдельного или нескольких централизованно изменяемых символов, которые динамически изменяются в зависимости от измеряемого параметра, зависимого от измеряемого параметра алгоритма, правила и/или инструкции в центральной базе данных между двумя моментами времени аутентификации,

отдельного или нескольких централизованно неизменяемых символов в этой или другой централизованно сохраненной последовательности символов, которые остаются статическими в центральной базе данных между двумя моментами времени аутентификации;

предоставление второго ключа в устройстве связи, который содержит последовательность символов, состоящую из

отдельного или нескольких локально изменяемых символов в этой или другой последовательности символов, которые соответствуют централизованно неизменяемым символам или последовательности символов центральной базы данных в последний момент времени аутентификации,

отдельного или нескольких локально неизменяемых символов, которые соответствуют централизованно изменяемым символам или последовательности символов центральной базы данных в последний момент времени аутентификации;

передача и сопоставление ключей, сохраненных в центральной базе данных и устройстве связи.

При этом положительная аутентификация и/или идентификация устройства, услуги, лица и/или денежного средства в момент времени аутентификации осуществляется тогда, когда выполняются по меньшей мере следующие критерии:

i) по меньшей мере частичное совпадение централизованно неизменяемых символов или последовательности символов в ключе центральной базы данных с соответствующими локально изменяемыми символами или последовательностью символов в ключе устройства связи;

ii) по меньшей мере частичное несовпадение централизованно изменяемых символов или последовательности символов в ключе центральной базы данных с соответствующими локально неизменяемыми символами или последовательностью символов в последнем ключе устройства связи,

причем централизованно изменяемые символы или последовательность символов между двумя моментами времени аутентификации могут изменяться только в центральной базе данных, но не в устройстве связи, и локально изменяемые символы или последовательность символов могут изменяться только в устройстве связи, но не в центральной базе данных.

Предпочтительным образом может быть предусмотрено, что изменяемые символы при аутентификации преобразуются в неизменяемые, статические символы и затем интегрируются в последовательность символов, подлежащую передаче в партнерскую базу данных, или присоединяются к ней. В этом случае статическая последовательность символов содержала бы переданные изменяемые символы последнего момента времени аутентификации.

Предпочтительным образом в другом варианте осуществления предусмотрено, что описанные выше принципы первого локального ключа устройства связи и второго центрального ключа центральной базы данных по смыслу переставляются для первого центрального ключа центральной базы данных и второго локального ключа устройства связи. Это означает, что (в дополнение или в качестве альтернативы) центральная база данных включает в себя динамически изменяемые символы или последовательность символов, которые/ая могут (может) непрерывно изменяться на основе вышеописанных воздействий. Централизованно изменяемый ключ в соответствии с этим был бы изменяемым динамически всегда, а не только между двумя моментами времени аутентификации.

В соответствии с изобретением может, кроме того, предусматриваться, что локально или централизованно сохраненный ключ в устройстве связи состоит из нескольких последовательностей символов, причем одна последовательность символов состоит исключительно из изменяемых символов, в то время как другая последовательность символов состоит только из неизменяемых символов, и третья последовательность символов удерживает состояние изменяемых символов соответствующей другой базы данных на момент времени последней аутентификации. В качестве альтернативы, может также предусматриваться последовательность символов, в которой один или несколько символов являются изменяемыми, в то время как другие символы в этой последовательности символов являются неизменяемыми. В качестве альтернативы, можно полностью отказаться от статических символов и использовать для аутентификации только динамические символы. Различные комбинации также возможны.

В предпочтительной форме выполнения, при успешной аутентификации, локально неизменяемые символы или последовательности символов в ключе устройства связи и/или центральной базе данных сбрасываются или изменяются и затем передаются в устройство связи или базу данных. При этом передаваемые символы или последовательности символов в устройстве связи или центральной базе данных в зависимости от направления передачи полностью или частично заменяются или стираются.

В еще одном предпочтительном варианте осуществления устройство связи и/или центральная база данных могут также включать в себя множество ключей с изменяемыми и/или неизменяемыми последовательностями чисел, чтобы выполнять "перекрестную защиту". Это означает, что сброс или изменение

статических символов может осуществляться как локально, так и централизованно. С другой стороны, центральная база данных также может включать в себя динамические символы или последовательности символов, которые непрерывно изменяются между двумя моментами временами аутентификации, при этом устройство связи или локальная база данных не "знает" это правило или воздействия на это правило. Та же система может быть применена к центральной базе данных. Таким образом, перекрываются все возможности и комбинации, чтобы реализовать способы обеспечения защиты в соответствии с изобретением, как на устройстве связи, так и в центральной базе данных. Конечно, этот способ также работает между двумя устройствами связи или между двумя центральными базами данных. Ключ может храниться в стационарных, мобильных или портативных устройствах и получать назначение в качестве "локального" или "центрального" ключа. При этом, однако, важно, что новые динамические изменения не известны соответствующему другому партнеру.

В предпочтительной форме выполнения первый ключ в устройстве связи и второй ключ в центральной базе данных включают в себя дополнительные определяющие идентификацию символы или последовательность символов, с помощью которых устройство, услуга, лицо или денежное средство могут однозначно идентифицироваться, причем идентификация для момента времени аутентификации осуществляется тем, что сохраненные в устройстве связи символы или последовательность(и) символов идентификации по меньшей мере частично совпадают с сохраненными в центральной базе данных символами или последовательностью(ями) символов идентификации.

В качестве альтернативы, в варианте способа, посредством описанного ниже двойного квитирования можно полностью отказаться от частичного совпадения сохраненных символов или последовательности(ей) символов идентификации, так что в случае ключей (DSC) используются только динамически изменяемые символы. В одном варианте, было бы достаточно, что, например, только состояние заряда энергии или другое измеренное значение передается в качестве динамического кода к другому абоненту связи.

Предпочтительным образом, изменения в изменяемой последовательности символов выполняются с временным управлением, с импульсным управлением, в зависимости от движения, в зависимости от местоположения, в зависимости от времени, в зависимости от температуры, в зависимости от вибрации, в зависимости от значений и/или в соответствии с другими, специфическими для услуги инструкциями. Например, данные о местоположении могут с помощью датчика GPS сохраняться в последовательности символов в виде кода. Кроме того, также момент времени аутентификации устройства связи может сохраняться в центральной базе данных, или временные разности последних моментов времени аутентификации могут сохраняться в изменяемой последовательности символов. Датчики вибрации могут также представлять данные измерения и формировать суммы цифр числа или средние значения, которые приводят к численному значению, которое, в свою очередь, может сохраняться в изменяемой последовательности символов. В платежной системе может также выполняться зависимое от стоимости изменение последовательности символов, например, изменяемая последовательность символов может содержать числовое значение для валюты, с которой может выполняться платежная операция. Разница для приобретенных товаров или предоставленных услуг затем вычитается из этого числового значения и сохраняется в качестве измененного значения в последовательности символов. Кроме того, также возможно, что в изменяемой или неизменяемой последовательности символов устанавливается значение платежного средства. Например, можно использовать числовой код с "сохраненной" в нем денежной стоимостью для безналичных платежей. В этом случае, каждый код может соответствовать "цифровой банкноте". Сдача вновь осуществлялась бы посредством другой цифровой банкноты путем передачи соответствующих зависимых от стоимости последовательностей символов. Кроме того, валюта может автоматически пересчитываться и согласовываться в зависимости от географического положения.

Соответствующая изобретению центральная база данных может встраиваться в любую структуру или устройство. Ключ устройства связи предпочтительно хранится в локальной базе данных. Предпочтительным образом, ключ криптографически кодируется.

Предпочтительным образом, соответствующие изобретению последовательности символов включают в себя буквы, числа, знаки, изображения и/или символы. Изображения включают в себя, например, графики, цветовые схемы, чертежи или шаблоны, которые в качестве символов или последовательности символов в соответствующем ключе могут быть сохранены в центральной базе данных или устройстве связи и могут быть сопоставлены с значениями. Так шаблоны или цветовые схемы могут динамически изменяться в пределах последовательности символов. Также вся последовательность символов может быть представлена в виде шаблона и по меньшей мере частично подвергаться динамическому изменению в смысле настоящего изобретения.

Чтобы исключить подделку или имитацию, насколько это возможно, в предпочтительном варианте предусмотрено, что локально изменяемая последовательность символов или символы в устройстве связи и/или центральной базе данных включают в себя символы, которые изменяются с различными скоростями. Таким образом, отдельные символы или целые последовательности символов могут включать в себя изменяющиеся числовые значения, которые изменяются каждую секунду. Кроме того, отдельные символы или все последовательности символов могут изменяться ежеминутно или ежечасно, ежедневно или

еженедельно. Соответствующие правила или алгоритмы могут определяться соответствующим поставщиком услуг. При этом правила могут также быть число случайными. При этом предпочтительно может быть предусмотрено, что в устройстве связи и/или в центральной базе данных дополнительно сохранены алгоритм, правило и/или инструкция, которые устанавливают, должна ли и каким образом непрерывно изменяется последовательность символов между двумя моментами времени аутентификации. При этом могут, например, определяться установленные в последовательности символов значения и/или значения, колеблющиеся между двумя предельными значениями, и/или восходящие или нисходящие последовательности.

В предпочтительной форме выполнения, кроме того, также может быть предусмотрено, что изменяемая последовательность символов включает в себя последний момент времени аутентификации, стоимость денежного средства, физическое значение, указание позиции, дату, значение времени, сумму цифр числа и/или контрольную сумму. Кроме того, может быть предусмотрено, что также сохраняется разница во времени между двумя моментами времени запроса между устройством связи и центральной базой данных в качестве значения разницы во времени. Кроме того, значения изменяемых символов к последнему моменту времени аутентификации могут быть закодированы с использованием алгоритма. Этот алгоритм может основываться, например, на динамических факторах, указанных выше, и, таким образом, приводить к индивидуальным зашифрованным последовательностям символов в центральной базе данных и/или локальной базе данных. При запросе аутентификации, дата и/или время могут совместно передаваться, так что момент времени последней аутентификации для устройства связи и/или центральной базы данных становятся частью последовательности символов.

Сброс или изменение локально неизменяемых символов центральной базы данных или централизованно неизменяемых символов в устройстве связи предпочтительно осуществляется в момент времени аутентификации посредством централизованно или локально сохраненного правила, инструкции, в зависимости от значений, алгоритма и/или посредством иных специфических для услуги инструкций. Кроме того, в предпочтительном варианте может быть предусмотрено, что локальный ключ устройства связи после выполненной передачи в центральную базу данных частично или полностью удаляется или аннулируется.

Предпочтительным образом, локально сохраненная последовательность символов содержит определяющую идентичность последовательность символов, с помощью которой может однозначно идентифицироваться устройство, услуга, лицо и/или денежное средство. Эта определяющая идентичность последовательность символов может при запросе аутентификации дополняться посредством дополнительной новой последовательности символов, посредством которой может идентифицироваться независимое от этого устройство, услуга, лицо или денежное средство. Например, таким образом денежная стоимость может быть соотнесена с определенным лицом, если оно регистрируется в системе в момент времени аутентификации. Таким образом, с некоторым лицом могут соотноситься функции, услуги или денежные суммы в иерархическом порядке. Также возможно иерархически регистрировать семьи и другие группы лиц и соотносить, например, с идентификацией страны.

Соответствующий изобретению способ препятствует тому, что копия данных локального устройства связи и/или центральная база данных может быть использована незаконно. Динамические, изменяемые символы изменяются в зависимости от варианта выполнения в центральной базе данных и/или устройстве связи, причем также могут быть предусмотрены различные символы или последовательности символов, которые различным образом изменяются в соответствующих устройствах, за счет чего защита дополнительно увеличивается. Как правило, устройство связи также будет содержать базу данных, в которой хранится ключ.

Только в момент времени аутентификации изменяемые символы или последовательность(и) символов в этой последовательности символов или другой, отдельной последовательности символов передаются в центральную базу данных и там сравниваются с последними сохраненными символами или последовательностью(ями) символов. При этом локально неизменяемые символы известны только центральной базе данных. Если изменение этих символов или последовательностей символов, например, должно осуществляться в локальной базе данных, то это указывало бы на несанкционированный доступ или манипулирование. Неизменяемые символы или последовательность символов могут, в принципе, оставаться статичными. Однако защита дополнительно повышается, когда локально неизменяемые символы центральной базы данных после каждого процесса считывания сбрасываются и/или полностью или частично заменяются. Как уже отмечалось выше, также возможно, что централизованно неизменяемые символы устройством связи после процесса считывания или в момент времени аутентификации сбрасываются, изменяются или остаются неизменными.

В предпочтительном варианте осуществления, кроме того, может быть предусмотрено, что неизменяемые символы или последовательность символов локально обрабатываются как изменяемые символы, то есть изменяются, заменяются или удаляются, но в момент времени аутентификации затем посредством центральной базы данных снова сбрасываются или снова изменяются.

Наряду с этим, передачи более раннего момента времени аутентификации неизменяемых символов, которые по неосведомленности были изменены локальным устройством связи или его базой данных,

могут быть сохранены централизованно и, при необходимости, дополнительные могут сравниваться с вновь переданными символами или последовательностью символов, чтобы гарантировать, что вновь переданные символы или последовательность символов не могут быть копией более раннего состояния. В качестве альтернативы, неизменяемые символы в каждый момент времени запроса посредством некоторого алгоритма могут заменяться в центральной базе данных новыми неизменяемыми символами. В предпочтительном варианте осуществления предусмотрено, что эти символы или последовательность символов остаются сохраненными до следующего запроса в центральной базе данных. Локальные изменения этих символов при каждом запросе перезаписываются новыми записями центральной базы данных. Комбинация из изменяемых/неизменяемых символов или последовательности символов обеспечивает максимально возможную гибкость с точки зрения присвоения значения в пределах определенной последовательности символов. Так, например, дата, указание значения, физические параметры или также другая информация могут быть включены в последовательность символов. Эти информации, в зависимости от типа, могут быть либо интегрированы в локально изменяемые или локально неизменяемые или в централизованно изменяемые или в централизованно неизменяемые символы или последовательности символов. В соответствии с этим, последовательность символов может изменить встроенное в нее значение, например, когда поступления или платежи соотносятся с пользователем, даже без того, что последний идентифицируется или регистрируется.

В одном варианте может быть предусмотрено, что статические символы центральной базы данных (или, по смыслу, устройства связи) при запросе аутентификации ведут себя по-разному. Таким образом, символы при запросе могут оставаться неизменными, сбрасываться либо заменяться на новый символ, в результате чего статические символы могут быть разделены на различные подгруппы. Это будет пояснено на следующем примере:

Локальная переменная последовательность символов состоит из: **1** 2 **3** 4 5 **6** 7, где цифры 1, 3 и 6 используются при аутентификации. Централизованно изменяемая последовательность символов состоит из: 5 **2** 7 3 **4** 0 **9**, причем цифры 2, 4 и 9 используются для аутентификации. При аутентификации теперь генерируется новый код, состоящий из динамически изменяемых цифр устройства связи и центральной базы данных, то есть 1 2 3 4 6 9. Эта последовательность символов, как неизменяемые статические последовательности между двумя запросами аутентификации сохраняется в центральной базе данных и локальном устройстве связи. Динамически изменяемые символы будут изменяться непрерывно, в то время как эти статические символы остаются неизменными. Если, например, устройство связи используется противоправно, то при следующем запросе эта неизменяемая статическая последовательность символов была бы заменена новой, вновь составленной из динамических символов устройства связи и динамических символов центральной базы данных. Законный пользователь при его попытке аутентификации сразу заметил бы, что кто-то незаконно осуществляет запрос, так как он больше не может аутентифицироваться - ключ тем временем изменился в центральной базе данных. Защита обеспечивается в данном случае за счет того, что только центральная база данных "знает" статические символы последнего момента времени аутентификации. Последующая попытка аутентификации будет немедленно обнаружена.

Чтобы предотвратить использование украденного устройства связи, предпочтительно используются биометрические признаки абонента. Они включают в себя отпечатки пальцев, радужную оболочку или структуру вен, голос или определенное специфическое для лица поведение. Наряду с этим также могут иметься специфические для объекта признаки, в случае которых можно идентифицировать устройство через специфические признаки. Например, могут быть образованы суммы цифр числа или средние значения из измеренных физических параметров. Среди них могли бы, например, использоваться сумма измеренных температур, сумма цифр числа для последних выполненных запросов или сумма вибраций, зарегистрированных датчиком вибрации. Образованные на этой основе численные значения могут заменять централизованно сохраненную последовательность символов частично или полностью. Кроме того, предпочтительным образом могут использоваться высокозащищенные от подделки статические и динамические защитные элементы, как, например, кракелированный узор, если они соотнесены с биометрическим защитным признаком пользователя.

Правила, представленные здесь, также могут объединяться или меняться местами, это означает, что изменяемые символы между двумя моментами времени аутентификации изменяются не локально, а изменяются централизованно. Кроме того, может быть предусмотрено несколько ключей, в которых комбинация между изменяемыми символами и неизменяемыми символами выполняется произвольно часто и в различных комбинациях. Кроме того, можно ранее изменяемые символы переводить в неизменяемые символы и наоборот. И, наконец, запросы аутентификации, описанные здесь, также могут быть выполнены несколько раз на разных уровнях, в результате чего получают дополнительные меры защиты.

Как было описано выше, в случае неизменяемых символов имеются такие, которые известны партнерской базе данных, и такие, которые неизвестны партнерской базе данных. В качестве "партнерской базы данных" обозначается либо центральная база данных, либо локальная база данных в устройстве связи.

Предпочтительно, неизменяемые символы можно разделить на две подгруппы:

1) символы, которые не могут быть изменены ни в какой момент времени. В этом случае партнерская база данных информируется об их неизменности;

2) символы, которые могут быть изменены партнерской базой данных, так как она не информирована об их неизменяемости.

Вторая группа, которая не известна партнерской базе данных как неизменяемая, может быть изменена ею при неосведомленности о неизменяемости и в рамках динамического изменения последовательности символов. В этом случае символы этой подгруппы делятся на три дополнительные подгруппы символов:

a) символы, которые на основе запроса аутентификации будут сброшены снова в исходное значение;

b) символы, которые по случаю запроса аутентификации получают новое значение, причем для них может быть использовано измененное в партнерской базе данных значение для вычисления нового значения, а также другие факторы, например, такие, которые в принципе используются для динамического изменения последовательности символов;

c) символы, которые по случаю процесса аутентификации принимают изменение, выполненное в партнерской базе данных, то есть переходят в него.

После того как неизменяемые символы, ввиду неосведомленности, подвергаются динамическому процессу изменений в партнерской базе данных, рекомендуется к переданной последовательности символов присоединить исходную последовательность символов непосредственно после последней аутентификации или интегрировать в нее, прежде чем она будет динамически изменена. Эта процедура обеспечивает возможность четкого сравнения вместо нечеткого сравнения и не представляет угрозу безопасности, поскольку первоначально выданная последовательность символов остается только частью всей последовательности символов, которая за счет также интегрированного в нее динамического процесса изменения эффективно защищена от любого типа копирования.

Чтобы полностью исключить попытки аутентификации с, возможно, изготовленными копиями или подделками динамической последовательности символов, в предпочтительной форме выполнения процесс аутентификации дополняется предварительной аутентификацией. Она может быть инициирована, в случае запроса аутентификации запрашивающей базы данных, партнерской базой данных, что приводит к немедленному изменению динамического кода в исходной запрашивающей базе данных, а также в партнерской базе данных. Однако это не имеет места при, возможно, запрашивающей подделке или копии, потому что к ней со стороны исходной партнерской базы данных нет существующего соединения. Обмен информацией происходит затем автоматически к исходной, видимым образом запрашивающей базе данных, а не к собственно запрашивающей подделке. Это приводит к изменению последовательности символов или отдельных символов, из-за чего фальсификация становится устаревшей и, таким образом, не имеющей значения. Таким образом, никакая успешная попытка аутентификации не может выполняться с фальсифицированной последовательностью символов. На основании предварительной аутентификации можно, в качестве альтернативы, полностью отказаться от статических последовательностей символов.

В соответствии с этим отыскивается контакт к последней аутентифицированной партнерской базе данных, причем фальсификация и копия за счет предварительной аутентификации может распознаваться уже при первой фактической попытке аутентификации. Если последняя аутентифицированная партнерская база данных была недоступна в момент времени предварительной аутентификации, выдается соответствующее предупреждение, и процесс аутентификации либо не выполняется, либо выполняется только кажущимся образом, например, с целью определения места расположения фальсификатора. Запрос через недостижимую базу данных достаточен, чтобы установить возможную атаку подделки.

В предпочтительном варианте осуществления настоящее изобретение включает в себя способ аутентификации и/или идентификации устройства, услуги, лица и/или денежного средства в сети связи, состоящей из первого устройства связи и другого устройства связи, такого как центральный сервер. Между первым устройством связи и другим устройством связи, таким как центральный сервер, выполняется запрос аутентификации. В этом варианте, сначала в устройстве связи обеспечивается первый ключ, который включает в себя по меньшей мере одну последовательность символов, состоящую из отдельного или нескольких локально изменяемых символов, которые динамически изменяются в зависимости от измеряемого техническим средством параметра, зависимого от него алгоритма, правила и/или инструкции в устройстве связи между двумя моментами времени аутентификации. Ключ представляет собой, например, код, значение или последовательность символов. Предпочтительно, ключ дополнительно может включать в себя один или нескольких локально неизменяемых символов в этой или другой локально сохраненной последовательности символов, которые между двумя моментами времени аутентификации остаются неизменными в устройстве связи.

Затем этот первый ключ устройства связи, который соответствует динамическому коду, передается на центральный сервер через канал связи. Предпочтительно, передача осуществляется в зашифрованном виде. От центрального сервера обеспечивается второй ключ (центральный ключ сервера), причем ключ включает в себя последовательность символов, состоящую из отдельного или нескольких централизованно изменяемых символов, которые динамически изменяются в зависимости от измеряемого параметра, зависимого от него алгоритма, правила и/или инструкции в устройстве связи между двумя моментами

времени аутентификации. В предпочтительном варианте осуществления второй ключ может дополнительно включать в себя один или несколько централизованно неизменяемых символов в этой или другой локально сохраненной последовательности символов, которые остаются статическими между двумя моментами времени аутентификации в устройстве связи.

Измеренный параметр (например, температура, давление воздуха, данные GPS, состояние заряда батареи), который используется для изменения динамического символа, предпочтительно определяется на соответствующем устройстве, в котором есть динамический код (DSC), либо на мобильном устройстве, центральном сервере или на мобильном устройстве другого абонента с соответствующим техническим оборудованием. При этом может, например, использоваться устройство измерения температуры, устройство измерения давления воздуха, GPS-устройство определения местоположения, датчик заряда, оптика и т.д.

На следующем этапе принятый центральным сервером первый ключ устройства связи и второй ключ центрального сервера через канал связи передаются на устройство связи. Переданный от центрального сервера динамический код включает в себя, таким образом, ключ первого устройство связи и ключ центрального сервера базы данных. В устройстве связи затем проверяется, совпадает ли полученный от центрального сервера первый ключ устройства связи с ранее переданным ключом. Если проверка проходит положительно, первый ключ устройства связи, полученный от центрального сервера, и второй ключ центрального сервера снова передаются устройством связи через канал связи на центральный сервер. Там проверяется, совпадают ли первый ключ устройства связи и второй центральный ключ центрального сервера с ключом, переданным на втором этапе. Если и этот запрос проходит положительно, первый ключ устройства связи и второй ключ центрального сервера посылаются вместе с кодом операции через канал связи обратно к устройству связи. Каждый код операции соотнесен с определенной операцией. На основании кода операции аутентифицированный пользователь может выполнить операцию, например, осуществить перевод или заказать услугу. При этом при необходимости может еще использоваться подтверждение посредством дополнительного защитного признака, например, биометрического признака. Это предпочтительно происходит в фоновом режиме на мобильном устройстве, так что пользователю не нужно выполнять никаких сложных вводов. При этом может быть предусмотрено, что пользователь еще раз намеренно подтверждает операцию.

Передача символов или последовательности символов может осуществляться через сеть или вручную. Например, последовательность символов может также вводиться вручную (например, с помощью цифровой клавиатуры или голосового устройства) или считываться посредством сканера.

Вместе с динамическим защитным кодом могут также передаваться дополнительные данные или пакеты данных. При этом в одном варианте предусмотрено, что отдельные фрагменты данных подобно головоломке - хранятся в разных местах, что дополнительно повышает защиту. Динамические символы могут быть преобразованы в статические символы или наоборот.

Таким образом, представленный здесь динамический код (DSC) использует локальные параметры, которые постоянно изменяются, например, в мобильном устройстве. В мобильном телефоне уровень заряда батареи может быть использован в качестве локального фактора. Соответствующее действительное значение никогда не может быть вычислено заранее, даже если алгоритм известен как таковой.

Сеть связи работает предпочтительно зашифрованным образом и гарантирует, что запрос исходит от правомочного лица. В предпочтительном варианте, также сам защитный код может зашифровываться и передаваться по защищенным каналам связи.

Настоящее изобретение далее иллюстрируется следующими чертежами.

Пути осуществления изобретения и промышленная применимость

На фиг. 1 приведен пример применения, в котором локальная база данных и центральная база данных используются в сети связи. Локальная база данных может, например, быть составной частью устройства связи, такого как мобильный телефон. Центральная база данных может находиться на сервере или другом устройстве связи (например, мобильном устройстве). В локальной базе данных сохранена последовательность символов, которая состоит из нескольких динамических символов. Эти символы могут изменяться локально и поэтому гибким образом в локальной базе данных. В центральной базе данных эти локально динамические символы являются, однако, статическими, то есть в центральной базе данных сохраняются символы последнего запроса аутентификации. Локальная база данных не "знает" изменяемые локально в центральной базе символы. Наряду с этим в локальной базе данных имеются локально неизменяемые символы, копия которых хранится в центральной базе данных. Там, однако, они при запросе аутентификации могут сбрасываться или изменяться как централизованно изменяемые символы. Локальная база данных не знает последний статус сохраненных в центральной базе данных локально неизменяемых или централизованно изменяемых символов. Если бы ключ устройства связи был, например, украден и использован для попытки аутентификации, то затем сразу же состояние сохраненных в центральной базе данных локально неизменяемых или централизованно изменяемых символов и, таким образом, центральный ключ изменится. Противоправное использование было бы установлено исходной базой данных при следующем запросе. Посредством предварительной аутентификации противоправный запрос аутентификации также может быстро распознаваться за счет того, что она вызывает па-

раллельные динамические изменения в обеих базах данных, которые не может предусмотреть фальсификация.

Сопоставление данных локальной базы данных и центральной базы данных осуществляется, как правило, в момент времени аутентификации. Только когда предварительная аутентификация и/или аутентификации и/или идентификации пройдены успешно, осуществляется актуализация статических символов.

На фиг. 2 показан пример способа в соответствии с изобретением. Устройство связи содержит ключ в форме последовательности символов, состоящей из чисел 1, 2, 3, 4, 5, 6. Выделенные жирным шрифтом числа устройства связи 2, 3, 6 соответствуют локально неизменяемым символам, в то время как числа 1, 4, 5 соответствуют локально изменяемым символам. Локально изменяемые символы должны изменяться в соответствии с правилами или инструкциями, установленными в устройстве связи, непрерывно динамическим образом, в то время как локально неизменяемые символы остаются статическими. В момент времени аутентификации (первой аутентификации) ключ передается в центральную базу данных и сравнивается с сохраненным там ключом. В центральной базе данных также сохранена последовательность символов, состоящая из чисел 1, 2, 3, 4, 5, 6. При этом цифры 2, 3, 6 являются централизованно изменяемыми, в то время как цифры 1, 4, 5 являются централизованно неизменяемыми.

При или после аутентификации централизованно изменяемые символы либо остаются, как есть, либо, как показано в этом примере, сбрасываются. Централизованно изменяемые символы признаки 2, 3, 6, таким образом, здесь сбрасываются или выбираются заново. В качестве примера, числовые значения 2, 3, 6, например, заменяются цифрой 0, так что получается вновь созданная числовая последовательность 1, 0, 0, 4, 5, 0. Она передается как локально неизменяемая последовательность символов в устройство связи и сохраняется в нем. При этом числа 1, 4, 5 непрерывно изменялись бы динамически в устройстве связи, в то время как цифры 0, 0, 0 остаются локально неизменяемыми. Между моментами времени аутентификации, таким образом, локально изменяемые символы изменялись бы в устройстве связи, то есть из цифр 1, 4, 5 получились, например, цифры 3, 6, 7. Во второй момент времени аутентификации вся последовательность символов снова передается и сравнивается с сохраненной в центральной базе данных последовательностью символов последнего момента времени аутентификации. Для успешной аутентификации и/или идентификации локально изменяемые символы 1, 4, 5, которые хранятся в центральной базе данных с последнего момента времени аутентификации, должны измениться. Если эти числа не изменены, то аутентификация была бы безуспешной. Кроме того, для успешной аутентификации было бы необходимо, чтобы локально неизменяемые символы 0, 0, 0 в центральной базе данных соответствовали защитной копии централизованно изменяемых символов 0, 0, 0 перед их изменением. В зависимости от варианта и профиля защиты может также требоваться только или дополнительно частичное совпадение или несовпадение может потребоваться с централизованно изменяемыми символами, т.е., сопоставление может быть осуществлено нечетким образом. Если какой-либо из этих символов также изменился, то это могло бы указывать на неправомерную попытку аутентификации. Изменение могло бы указывать на то, что локальная база данных, при неосведомленности, какие числа для нее являются неизменяемыми, изменила некоторые из них случайным образом, что, однако, было бы некритичным и было бы вновь устранено за счет сброса.

На фиг. 3 показан пример предварительной аутентификации между двумя пользователями A, C и центральной базой данных B. Здесь A обозначает оригинал, C - противоправную копию и B - центральную базу данных. В рамках предварительной аутентификации осуществляется запрос от C к B, в результате чего событие предварительной аутентификации запускается между A и B. В ходе предварительной аутентификации, измененный код (ключ) передается из центральной базы данных B к пользователю A. Тем самым A получает ключ, актуализированный посредством B. Однако поскольку ключ в C не изменился, C не получает во время собственно аутентификации доступа к B, потому что там уже имеется актуализированный ключ предварительной аутентификации.

На фиг. 4 показан другой пример способа согласно настоящему изобретению и его реализация в сети связи. На первом этапе осуществляется отправка динамического защитного кода, который состоит из локально изменяемых символов и, при необходимости, статических символов, от мобильного устройства на сервер. Динамическая часть кода может, например, быть зависимой от состояния заряда аккумулятора мобильного устройства. Определение состояния заряда осуществляется с помощью сенсорного устройства. Полученный параметр состояния служит в качестве базы для генерации динамического кода.

На втором этапе код отправляется обратно с сервера на мобильное устройство, причем защитный код состоит из переданного на этапе 1 защитного кода мобильного устройства (DSC_Mobil) и кода, сгенерированного сервером (DSC_Server). Код сервера также состоит из динамических символов и, при необходимости, статических символов. Статические символы могут включать в себя, например, идентификационный номер, чтобы идентифицировать устройство или лицо. На третьем этапе мобильное устройство снова устанавливает соединение связи с сервером и передает свой собственный защитный код (DSC_Mobil) и принятый от сервера защитный код (DSC_Server) на сервер. На четвертом этапе сервер сравнивает принятые защитные коды с защитными кодами, принятыми на первом этапе. На четвертом этапе сервер отправляет код операции вместе с двумя защитными кодами (DSC_Mobil и DSC_Server)

обратно в мобильное устройство. Оно сравнивает защитные коды с принятыми на этапе 2 защитными кодами. Код операции соотнесен с определенной операцией и позволяет пользователю мобильного устройства предпринимать операцию, такое как выполнение платежа или заказ услуги. В принципе, этот способ работает как "двойное квитирование", при котором динамические DSC абонентов многократно передаются по различным каналам связи и сравниваются, причем каждый DSC содержит изменяемый компонент, который может изменяться либо только локально, либо только централизованно, на основе определенного измененного параметра (например, температуры, давления воздуха, GPS-данных, состояния заряда батареи).

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ аутентификации и/или идентификации абонента связи в сети связи, состоящей из устройства связи и сервера, между которыми выполняют запрос аутентификации, включающий в себя следующие этапы:

генерирование и сохранение первого ключа в устройстве связи, причем первый ключ содержит

первую последовательность символов устройства связи, содержащую по меньшей мере один изменяемый в устройстве связи символ, и

набор неизменяемых в устройстве связи символов, причем набор неизменяемых в устройстве связи символов содержит по меньшей мере один неизменяемый символ в первой последовательности символов устройства связи и статическую последовательность символов устройства связи,

генерирование и сохранение второго ключа в сервере, причем второй ключ содержит

набор изменяемых в сервере символов, совпадающих с набором неизменяемых в устройстве связи символов первого ключа;

первую последовательность символов в сервере, содержащую по меньшей мере один неизменяемый в сервере символ, причем упомянутый по меньшей мере один неизменяемый в сервере символ совпадает по меньшей мере с одним изменяемым в устройстве связи символом первой последовательности символов устройства связи;

передача первого ключа, сохраненного в устройстве связи, на сервер и

сопоставление второго ключа, сохраненного в сервере, с первым ключом, сохраненным в устройстве связи, для определения положительной аутентификации и/или идентификации абонента связи,

при этом упомянутая положительная аутентификация и/или идентификация содержит:

i) по меньшей мере, частичное совпадение набора неизменяемых в устройстве связи символов первого ключа, сохраненного в устройстве связи, с набором изменяемых в сервере символов второго ключа, сохраненного в сервере,

ii) по меньшей мере, частичное совпадение по меньшей мере одного изменяемого в устройстве связи символа первой последовательности символов устройства связи по меньшей мере с одним неизменяемым в сервере символом первой последовательности символов сервера,

динамическое изменение по меньшей мере одного изменяемого в устройстве связи символа первой последовательности символов устройства связи, после определения упомянутой положительной аутентификации и/или идентификации, на основании по меньшей мере одного из: измеряемого датчиками физического или химического параметра; зависимого от упомянутого параметра алгоритма,

поддержание в качестве статического - набора неизменяемых в устройстве связи символов первого ключа, после определения упомянутой положительной аутентификации и/или идентификации.

2. Способ по п.1, дополнительно содержащий этап, на котором при успешной аутентификации неизменяемые в устройстве связи между двумя моментами времени аутентификации символы или последовательность символов в ключе сервера сбрасывают или изменяют и затем передают в устройство связи, в то время как переданные изменяемые в устройстве связи символы или последовательность символов устройства связи заменяют соответствующие неизменяемые в сервере символы или последовательность символов в ключе сервера.

3. Способ по п.1 или 2, отличающийся тем, что первый ключ в устройстве связи и второй ключ в сервере содержит дополнительную, определяющую идентичность последовательность символов, с помощью которой абонент связи может быть однозначно идентифицирован, причем идентификацию к моменту времени аутентификации осуществляют тем, что идентифицирующая последовательность символов, сохраненная в идентифицирующей последовательности символов устройства связи, по меньшей мере, частично совпадает с идентифицирующей последовательностью символов, сохраненной в сервере.

4. Способ по одному из пп.1-3, отличающийся тем, что часть переданных изменяемых символов устройства связи в момент времени аутентификации преобразуют в неизменяемые символы сервера за счет того, что отдельные символы или последовательность символов интегрируют или присоединяют к ключу сервера.

5. Способ по одному из пп.1-4, отличающийся тем, что изменение в устройстве связи выполняют с управлением по времени, импульсным управлением, в зависимости от движения, в зависимости от местоположения, в зависимости от времени, в зависимости от температуры, в зависимости от вибрации, в зависимости от значений и/или в соответствии с другими специфическими для услуги инструкциями.

6. Способ по одному из пп.1-5, отличающийся тем, что сохраненная в устройстве последовательность символов включает в себя буквы, числа, знаки, изображения и/или символы, которые изменяются с различной скоростью или интенсивностью.

7. Способ по одному из пп.1-6, отличающийся тем, что динамически изменяемые символы устройства связи включают в себя символы, которыми управляют только в устройстве связи, и/или символы, которыми управляют только на сервере, причем между двумя моментами времени аутентификации статические символы устройства связи и/или сервера при запросе аутентификации либо остаются неизменными, сбрасываются, либо заново предоставляются сервером.

8. Способ по одному из пп.1-7, отличающийся тем, что в устройстве связи дополнительно сохранен алгоритм, который устанавливает, изменяется ли непрерывно и каким образом непрерывно изменяется последовательность символов между двумя моментами времени аутентификации, причем в последовательности символов установлены или изменяются некоторое значение, значение, колеблющееся между двумя предельными значениями, и/или восходящие или нисходящие последовательности символов.

9. Способ по одному из пп.1-8, отличающийся тем, что изменяемая в сервере и переданная на устройство связи последовательность символов включает в себя момент времени последней аутентификации, стоимость денежного средства, физическое значение, указание положения, дату, разностное значение, временное значение, сумму цифр числа и/или контрольную сумму.

10. Способ по одному из пп.1-9, отличающийся тем, что ключ устройства связи после выполненной передачи на сервер частично или полностью изменяют, стирают или аннулируют.

11. Способ по одному из пп.1-10, отличающийся тем, что сохраненная в устройстве связи последовательность символов содержит определяющую идентичность последовательность символов, с помощью которой абонент связи может быть однозначно идентифицирован, и которую при запросе аутентификации дополняют другой новой последовательностью символов, с помощью которой может идентифицироваться независимый от этого абонент связи.

12. Способ аутентификации и/или идентификации абонента связи в сети связи, состоящей из устройства связи и сервера, между которыми выполняют запрос аутентификации, включающий в себя следующие этапы:

a) генерирование и сохранение первого ключа в сервере, причем первый ключ содержит

первую последовательность символов сервера, содержащую по меньшей мере один изменяемый в сервере символ, и набор неизменяемых в сервере символов, причем набор неизменяемых в сервере символов содержит по меньшей мере один неизменяемый символ в первой последовательности символов сервера и статическую последовательность символов сервера,

b) генерирование и сохранение второго ключа в устройстве связи, причем второй ключ содержит

набор изменяемых в устройстве связи символов, совпадающих с набором неизменяемых в сервере символов первого ключа,

первую последовательность символов устройства связи, содержащую по меньшей мере один неизменяемый в устройстве связи символ, причем упомянутый по меньшей мере один неизменяемый в устройстве связи символ совпадает по меньшей мере с одним изменяемым в сервере символом первой последовательности символов сервера,

c) передача второго ключа, сохраненного в устройстве связи, на сервер и

сопоставление первого ключа, сохраненного в сервере, со вторым ключом, сохраненным в устройстве связи, для определения положительной аутентификации и/или идентификации абонента связи,

при этом упомянутая положительная аутентификация и/или идентификация содержит:

i) по меньшей мере, частичное совпадение набора неизменяемых в сервере символов первого ключа, сохранённого в сервере, с набором изменяемых в устройстве связи символов второго ключа, сохранённого в устройстве связи,

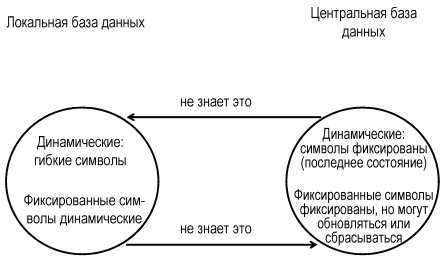
ii) по меньшей мере, частичное совпадение по меньшей мере одного изменяемого в сервере символа первой последовательности символов сервера по меньшей мере с одним неизменяемым в устройстве связи символом первой последовательностью символов устройства связи,

e) динамическое изменение по меньшей мере одного изменяемого в сервере символа первой последовательности символов сервера, после определения упомянутой положительной аутентификации и/или идентификации, на основании по меньшей мере одного из: измеряемого датчиками физического или химического параметра; зависимого от упомянутого параметра алгоритма,

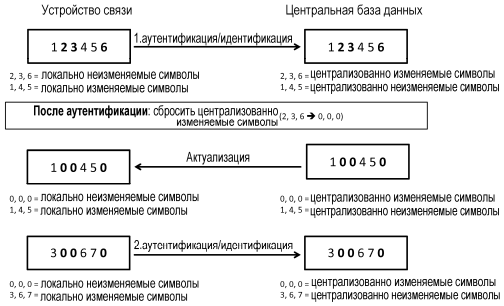
f) поддержание в качестве статического - набора неизменяемых в сервере символов первого ключа, после определения упомянутой положительной аутентификации и/или идентификации.

13. Способ по п.12, отличающийся тем, что принципы первого ключа устройства связи и второго ключа сервера в соответствии с пп.1-11 по аналогии реализуются для первого ключа сервера и второго ключа устройства связи по п.12.

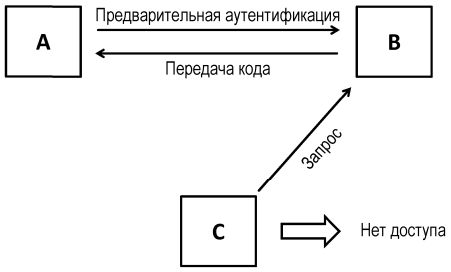
14. Способ по одному из пп.1 или 12, отличающийся тем, что перед запросом аутентификации выполняют предварительную аутентификацию, которую инициируют посредством соответствующей партнерской базы данных и которая приводит к изменению динамической последовательности символов.



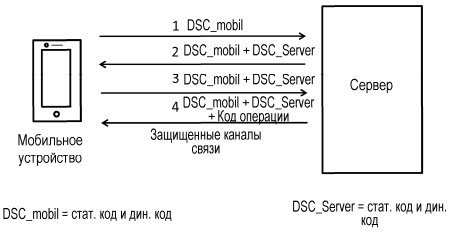
Фиг. 1



Фиг. 2



Фиг. 3



Фиг. 4