EUROPEAN PATENT SPECIFICATION

SYSTEMS AND METHODS FOR SECURE COMMUNICATION

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).
Description

FIELD

[0001] The subject matter disclosed herein generally relates to systems and methods for secure wireless commu-
nication, and more particularly to secure wireless payment in a fuel dispensing environment.

BACKGROUND

[0002] A number of mobile payment systems have been developed in which a mobile device can be used to pay for
goods or services at a payment terminal. In some systems, the mobile device does not communicate directly with the
payment terminal. Rather, the transaction is conducted between a mobile device payment infrastructure and a merchant
payment infrastructure. Integrating these complex and widely-divergent infrastructures, however, can often be cost-
prohibitive.

[0003] Other systems involve direct communication between the mobile device and the payment terminal. In such
systems, sensitive user data such as payment and loyalty information is transmitted as cleartext, raising a number of
security issues. For example, the sensitive user data can be intercepted by unscrupulous third parties. This can be of
particular concern in fueling environments, where the payment
terminal is often disposed in an unmanned, outdoor setting where there is an elevated risk of snooping or tampering.
Users can be discouraged from using such systems for fear that the payment terminal may have been compromised.

[0004] While some secure communication schemes have been developed, they have not been applied in mobile
payment systems. Moreover, they typically involve runtime validation of digital certificates and a complex handshaking
procedure in which several rounds of large-payload data exchange occur. Such schemes thus introduce significant
delays, and are cumbersome and time consuming for the user.

[0005] Accordingly, a need exists for improved mobile payment systems.

[0006] EP 1653655 (Research In Motion Limited) relates to a system and method for verifying a digital signature on
a certificate, which may be used in the processing of encoded messages. In one embodiment, when a digital signature
is successfully verified in a signature verification operation, the public key used to verify that digital signature is cached.
When a subsequent attempt to verify the digital signature is made, the public key to be used to verify the digital signature
is compared to the cached key. If the keys match, the digital signature can be successfully verified without requiring that
a signature verification operation in which some data is decoded using the public key be performed.

[0007] US 2008/294894 (Microsoft Corporation) describe systems, methods, and/or techniques for binding content
licenses to portable storage devices. In connection with binding the content licenses to the portable storage devices, a
host may perform authentication protocols that include generating a nonce, sending the nonce to a store, and receiving
a session key from the store, with the session key being generated using the nonce. The store may perform authentication
protocols that include receiving the nonce from the host, generating a random session key based on the nonce, and
sending the session key to the host.

BRIEF DESCRIPTION

[0008] Fast and secure mobile communication can be achieved in some embodiments with systems and methods
that validate an authentication request based on one or more pre-validated cryptographic keys.

[0009] Systems and methods for providing secure communication between a payment terminal and a mobile device,
e.g., in a fueling environment, are disclosed herein. In some embodiments, the payment terminal and the mobile device
conduct a mutual authentication process that, if successful, produces a session key which can be used to encrypt
sensitive data to be exchanged between the payment terminal and the mobile device. The mutual authentication process
can be expedited, for example by transferring a public key in place of a complete certificate and/or by maintaining at
each device a database of pre-authenticated certificates indexed by a lookup table. The pre-authenticated certificates
can be superior in a trust hierarchy to unit-level certificates associated with a particular mobile device or payment terminal,
such that the amount of validation that must be performed at runtime is reduced.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] These and other features will be more readily understood from the following detailed description taken in
conjunction with the accompanying drawings, in which:

FIG. 1 is a schematic diagram of one exemplary embodiment of a fueling environment;
FIG. 2 is a schematic diagram of one exemplary embodiment of a computer system;

FIG. 3 is a schematic diagram of one exemplary embodiment of a payment terminal;

FIG. 4 is a schematic diagram of one exemplary embodiment of a certificate hierarchy;

FIG. 5 is a sequence diagram of one exemplary method of managing digital certificates during production of a payment terminal;

FIG. 6 is schematic diagram of one exemplary embodiment of a mobile device;

FIG. 7 is a sequence diagram of one exemplary embodiment of a mutual authentication method conducted by a payment terminal and a mobile device;

FIG. 8 is a flowchart that depicts the method of FIG. 7 from the perspective of the payment terminal; and

FIG. 9 is a flowchart that depicts the method of FIG. 7 from the perspective of the mobile device.

[0011] It is noted that the drawings are not necessarily to scale. The drawings are intended to depict only typical aspects of the subject matter disclosed herein, and therefore should not be considered as limiting the scope of the disclosure. In the drawings, like numbering represents like elements between the drawings.

DETAILED DESCRIPTION

[0012] Certain exemplary embodiments will now be described to provide an overall understanding of the principles of the structure, function, manufacture, and use of the devices, systems, and methods disclosed herein.

[0013] Systems and methods for providing secure communication between a payment terminal and a mobile device, e.g., in a fueling environment, are disclosed herein. In some embodiments, the payment terminal and the mobile device conduct a mutual authentication process that, if successful, produces a session key which can be used to encrypt sensitive data to be exchanged between the payment terminal and the mobile device. The mutual authentication process can be expedited, for example by transferring a public key in place of a complete certificate and/or by maintaining at each device a database of pre-authenticated certificates indexed by a lookup table. The pre-authenticated certificates can be superior in a trust hierarchy to unit-level certificates associated with a particular mobile device or payment terminal, such that the amount of validation that must be performed at runtime is reduced.

FUELING ENVIRONMENT

[0014] FIG. 1 illustrates an exemplary embodiment of a fueling environment 100 in which one or more of the systems and methods disclosed herein can be implemented. The fueling environment 100 generally includes a payment terminal 102 and a mobile device 104 associated with a user (e.g., a customer seeking to purchase fuel or service personnel seeking service access to the payment terminal).

[0015] The payment terminal 102 can be integrated with a fuel dispenser 106, which can include various features well understood by those skilled in the art such as a nozzle, a pump, buttons for selecting fuel grade, a display screen, and so forth. The payment terminal 102 can include a computer system, as described below. The payment terminal 102 can be coupled to a back end server 108, which can be configured to communicate with various networks, such as a fueling loyalty network 110 for maintaining, checking, and updating customer loyalty information and a fueling payment network 112 for processing fuel purchase and other transactions. Together, the back end server 108, the fueling loyalty network 110, and the fueling payment network 112 form a fueling payment infrastructure.

[0016] The mobile device 104 can also include a computer system, as described below. The mobile device 104 can be configured to communicate with various networks, such as a mobile loyalty cloud 114 for maintaining, checking, and updating customer loyalty information and a mobile payment cloud 116 for processing purchases and other transactions executed using the mobile device 104. The mobile loyalty cloud 114 and the mobile payment cloud 116 together form a mobile payment infrastructure. The mobile device 104 can be or can include any device that is configured to exchange data over a communications network, such as a mobile phone, tablet computer, laptop computer, digital wallet, and so forth. The mobile device can be held by a user or integrated with a movable object.

[0017] The payment terminal 102 and the mobile device 104 can mutually authenticate one another to facilitate secure communication of payment or other information directly between the payment terminal 102 and the mobile device 104. A secure communication channel between the payment terminal 102 and the mobile device 104 can allow for secure
mobile payment without requiring the fueling payment infrastructure and the mobile payment infrastructure to be changed or integrated.

[0018] Although a fueling environment is shown in FIG. 1, it will be appreciated that the systems and methods disclosed herein can be readily applied in other settings, e.g., any setting in which a mobile device is used to conduct a transaction with a terminal. Transactions can include payment transactions, refund transactions, service transactions, control transactions, or any other transaction that requires communication. Terminals can include payment terminals, kiosks, and so forth, and/or can be part of a dispenser (e.g., a fuel dispenser, a snack or beverage dispenser, a cash dispenser, etc.).

COMPUTER SYSTEM

[0019] FIG. 2 illustrates an exemplary architecture of a computer system 200 which can be used to implement the payment terminal 102 or mobile device 104 of FIG. 1. Although an exemplary computer system 200 is depicted and described herein, it will be appreciated that this is for sake of generality and convenience. In other embodiments, the computer system may differ in architecture and operation from that shown and described here.

[0020] The computer system 200 can include a processor 202 which controls the operation of the computer system 200, for example by executing an operating system (OS), device drivers, application programs, and so forth. The processor 202 can include any type of microprocessor or central processing unit (CPU), including programmable general-purpose or special-purpose microprocessors and/or any of a variety of proprietary or commercially-available single or multi-processor systems.

[0021] The computer system 200 can also include a memory 204, which provides temporary or permanent storage for code to be executed by the processor 202 or for data that is processed by the processor 202. The memory 204 can include read-only memory (ROM), flash memory, one or more varieties of random access memory (RAM), and/or a combination of memory technologies.

[0022] The various elements of the computer system 200 can be coupled to one another. For example, the processor 202 can be coupled to the memory 204. The various elements of the computer system 200 can be directly coupled to one another or can be coupled to one another via one or more intermediate components. In the illustrated embodiment, the various elements of the computer system 200 are coupled to a bus system 206. The illustrated bus system 206 is an abstraction that represents any one or more separate physical busses, communication lines/interfaces, and/or multi-drop or point-to-point connections, connected by appropriate bridges, adapters, and/or controllers.

[0023] The computer system 200 can also include a network interface 208 which enables the computer system 200 to communicate with remote devices (e.g., other computer systems) over a network. In the case of the payment terminal 102, the network interface can facilitate communication with the back end server 108, the fueling loyalty network 110, and the fueling payment network 112. In the case of the mobile device 104, the network interface can facilitate communication with the mobile loyalty cloud 114 and the mobile payment cloud 116, for example via Wi-Fi or a cellular data network.

[0024] The computer system 200 can also include an input/output (I/O) interface 210 which facilitates communication between one or more input devices, one or more output devices, and the various other components of the computer system 200. Exemplary input and output devices include keypads, touchscreens, buttons, magnetic-stripe card readers, lights, speakers, and so forth.

[0025] The computer system 200 can also include a storage device 212, which can include any conventional medium for storing data in a non-volatile and/or non-transient manner. The storage device 212 can thus hold data and/or instructions in a persistent state (i.e., the value is retained despite interruption of power to the computer system 200). The storage device 212 can include one or more hard disk drives, flash drives, USB drives, optical drives, various media disks or cards, and/or any combination thereof and can be directly connected to the other components of the computer system 200 or remotely connected thereto, such as over a network.

[0026] The computer system 200 can also include a display controller 214 which can include a video processor and a video memory, and can generate images to be displayed on one or more displays in accordance with instructions received from the processor 202.

[0027] The computer system 200 can also include a secure element 216. The secure element 216 can be a tamper-resistant platform (e.g., a one-chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (e.g., key management) in accordance with the rules and security requirements set forth by a set of well-identified trusted authorities. The secure element 216 can be capable of providing random number generation, generating device-specific public/private key pairs, and executing a security algorithm. Known examples of security algorithms include, but are not limited to: Hash, TDES, AES, RSA, etc. Exemplary secure elements 216 include Universal Integrated Circuit Cards (UIICC), embedded secure elements, and micro secure digital (microSD) cards.

[0028] The computer system 200 can also include a secure communication interface 218 through which the computer system 200 can conduct mutual authentication procedures and communicate with other computer systems. The secure
The various functions performed by the payment terminal 102 and the mobile device 104 can be logically described as being performed by one or more modules. It will be appreciated that such modules can be implemented in hardware, software, or a combination thereof. It will further be appreciated that, when implemented in software, modules can be part of a single program or one or more separate programs, and can be implemented in a variety of contexts (e.g., as part of an operating system, a device driver, a standalone application, and/or combinations thereof). In addition, software embodying one or more modules can be stored as an executable program on one or more non-transitory computer-readable storage mediums. Functions disclosed herein as being performed by a particular module can also be performed by any other module or combination of modules, and the payment terminal 102 and the mobile device 104 can include fewer or more modules than what is shown and described herein.

Figure 3 is a schematic diagram of the modules of one exemplary embodiment of the payment terminal 102. As shown, the payment terminal 102 can include a certificate module 302, an authentication request receiving module 304, an authentication module 306, a session key generation module 308, an authentication response transmitting module 310, and a secure information receiving module 312.

The certificate module 302 can maintain a repository 316 of one or more digital certificates and an associated lookup table 314. Figure 4 illustrates an exemplary certificate hierarchy 400 which can be maintained by the certificate module 302.

As shown, the hierarchy can include a root certificate 402 that identifies an industry-standard Root Certificate Authority (Root CA). Exemplary Root CAs include VeriSign, GlobalSign, DigiCert, and the like. The root certificate 402 forms the trust root for the certificate hierarchy 400, and can be an unsigned public key certificate or a self-signed certificate. Trustworthiness of the root certificate 402 can be established by secure physical distribution, e.g., during production of the payment terminal 102 as discussed in further detail below. For convenience of description, the root certificate 402 is referred to herein as a level 1 or "L1" certificate. It will be appreciated that the hierarchy 400 can include a plurality of L1 certificates, e.g., issued from a plurality of different Root CAs. Each L1 certificate, or the public key contained therein, can be associated with a unique identifier (a "Level1ID"). The Level1ID can be an industry unique number assignment similar to a MAC address, a hash of the entire L1 certificate, or some other unique code, string, number, etc. Each L1 certificate or its public key and the corresponding unique identifier can be associated with one another in the lookup table 314 such that, when a unique identifier is provided, the associated certificate(s) or public key(s) can be quickly retrieved from the certificate repository 316.

The certificate hierarchy can also include one or more levels of subordinate certificates which are signed by a superior certificate authority and thereby inherit the trustworthiness of the superior certificate authority. In the illustrated embodiment, for example, the hierarchy 400 includes one or more payment terminal network certificates 404 issued from payment networks such as card-issuing banks, acquirers, or other payment processors. The illustrated hierarchy 400 also includes one or more mobile carrier certificates 406 issued from mobile carriers. For convenience of description, the payment terminal network certificates 404 and the mobile carrier certificates 406 are referred to herein as level 2 or "L2" certificates. Each L2 certificate can be stored in the certificate repository 316 and the certificate or its public key can be associated in the lookup table 314 with a unique identifier (a "Level2ID"), as described above. The L2 certificates are immediately-subordinate to the L1 certificates, and can therefore be signed by the Root CA to inherit the Root CA’s trustworthiness. Each L2 public key can thus be indexed in the lookup table 314 by a unique identifier that specifies the L2 public key and its superior L1 public key (e.g., Level2ID + Level1ID).

The hierarchy can also include certificates which are subordinate to the L2 certificates. In the illustrated embodiment, for example, the hierarchy 400 includes one or more payment terminal vendor certificates 408 issued from manufacturers or distributors of payment terminals. The hierarchy 400 can also include one or more mobile device vendor certificates 410 issued from manufacturers or distributors of mobile devices. For convenience of description, the payment terminal vendor certificates 408 and the mobile device vendor certificates 410 are referred to herein as level 3 or "L3" certificates. Each L3 certificate can be stored in the certificate repository 316 and the certificate or its public key can be associated in the lookup table 314 with a unique identifier (a "Level3ID"), as described above. The L3 certificates are immediately-subordinate to the L2 certificates, and can therefore be signed by a L2 certificate authority to inherit the L2 certificate authority’s trustworthiness. Each L3 public key can thus be indexed in the lookup table 314 by a unique identifier that specifies the L3 public key and its superior L2 public key (e.g., Level3ID + Level2ID).
by a unique identifier that specifies the L3 public key and its superior L2 and L1 public keys (e.g., Level3ID + Level2ID + Level1ID).

[0036] The hierarchy 400 can also include a device-specific certificate 412 unique to the individual payment terminal 102. For convenience of description, the device-specific certificate 412 is referred to herein as a level4 or "L4" certificate. The L4 certificate can be signed by a L3 certificate authority to inherit the L3 certificate authority's trustworthiness.

[0037] The root certificates 402, payment terminal network certificates 404, payment terminal vendor certificates 408, and the payment terminal certificate 412 can be referred to as "terminal-side" certificates. The root certificates 402, mobile carrier certificates 406, mobile device vendor certificates 410, and a mobile device certificate 414 (discussed further below) can be referred to as "mobile-side" certificates. Certificates can be referred to as "superior certificates," "more-superior certificates," "inferior certificates," "more-inferior certificates," and so forth based on their position within the hierarchy 400 and the certificate whose perspective is being described. For example, from the perspective of a L4 certificate, a L3 certificate can be referred to as a superior certificate and a L2 certificate can be referred to as a more-superior certificate. Likewise, from the perspective of a L4 certificate, a L2 certificate can be referred to as a superior certificate and a L1 certificate can be referred to as a more-superior certificate.

[0038] While a four-level certificate hierarchy 400 is shown and described herein, it will be appreciated that the hierarchy can include any number of levels. For example, a two-level hierarchy can be used in which device-specific certificates are signed directly by a Root CA. A three-level hierarchy can also be used in which device-specific certificates are signed by a sub-CA whose certificate is in turn signed by a Root CA. Hierarchies in which three or more intermediate certificate authorities exist in the chain of trust between the device-specific certificate and a Root CA can also be used. In addition, the level in the hierarchy at which a particular entity or class of certificates resides can vary from what is shown and described herein. For example, mobile carrier certificates can be subordinate to mobile device vendor certificates. In some embodiments, the repository 316 can be configured, for one or more certificates in the hierarchy 400, to store only the encrypted public key portion of said certificate(s) (e.g., the L3 and L4 certificates).

[0039] In some embodiments, the certificate hierarchy 400 can be part of a public key infrastructure (PKI), for example according to the X.509 industry standard. A PKI uses public key / private key pairs to securely encrypt and decrypt information. A public key can be freely distributed and can be used to encrypt the information. To decrypt the information, however, a party must possess a private key associated with the public key. All exemplary public key/private key encryption algorithms are the RSA cryptography system. A digital certificate can include a public key and a digital signature. The digital signature is created using a party's private key, such that anyone with access to the party's public key can prove that the signer had access to the party's private key and therefore that the signature is authentic.

[0040] Thus, in the example above, the Root CA stores a private key in a highly-secure location. The root certificate 402 stored in the certificate repository 316 includes the public key that corresponds to the private key and a digital signature signed by the Root CA using the private key. A known-good root certificate 402 can be installed in a controlled environment (e.g., during manufacture) such that the certificate can be trusted. Other certificates in the repository 316 can be trusted or authenticated based on a hierarchical system of cryptographic keys and digital signatures that traces back to the root certificate, as will be appreciated by those skilled in the art.

[0041] FIG. 5 illustrates an exemplary sequence diagram for pre-loading the certificate repository 316 during manufacture or production of the payment terminal 102. Referring now to FIGS. 3, 4, and 5, first, the payment terminal 102 self-generates a device-specific L4 key pair. The private key is stored in a secure location within the payment terminal 102, e.g., the secure element 216. The public key is delivered to a production security management system 500 with a request for encryption. The production security management system 500 encrypts the device-specific L4 public key using its own private key (e.g., a L3 payment terminal vendor private key). The resulting public key certificate (signed by the L3 sub-CA) is then returned to the payment terminal 102. The other public key certificates in the chain of trust for this particular payment terminal (e.g., the L1 root certificate 402, the L2 payment terminal network certificate 404, and the L3 payment terminal vendor certificate 408) are also sent to the payment terminal 102, along with their corresponding unique identifiers (Level3ID, Level2ID, and Level1ID). Because the production security management system 500 is a controlled environment, known-good certificates can be pre-loaded into the certificate repository 316 of the payment terminal 102.

[0042] The production security management system 500 can also pre-load in the certificate repository 316 a plurality of mobile-side certificates and their corresponding unique identifiers. Alternatively, or in addition, one or more of the mobile-side certificates can be loaded into the certificate repository 316 in the field, for example via a network such as the fueling payment network 112. Thus, when it becomes necessary for the payment terminal 102 to authenticate a mobile device 104, the payment terminal can have pre-installed one or more certificates in the mobile device's chain of trust.

[0043] Once the mobile-side certificates are loaded in the certificate repository 316, they can be pre-authenticated. For example, a L3 mobile-side certificate (e.g., a mobile device vendor certificate 410) can be pre-authenticated by the certificate module 302 against its corresponding L2 and L1 certificates such that the given L3 public key can be used directly at run-time without requiring a time-consuming L3 certificate authentication process to be executed at run-time.
If the pre-authentication is successful, the now-trusted L1, L2, and L3 public keys can be stored in the certificate repository with a corresponding unique identifier being added to the lookup table. In some embodiments, the unique identifier can be a concatenation of the Level1ID, the Level2ID, and the Level3ID. The following pseudo code demonstrates the process of pre-authenticating a L3 certificate and indexing its public key in the lookup table according to its chain of trust:

```plaintext
Level1PubKey = RetrievePublicKeyFromCertificate(Level1);
AddIntoLevel1PublicKeylookup (Level1PubKey, Level1ID);
Level2PubKey = DecryptPublicKeyFromCertificate (Level2, Level1PubKey);
AddIntoLevel2PublicKeylookup (Level2PubKey, Level1ID, Level2ID);
Level3PubKey = DecryptPublicKeyFromCertificate (Level3, Level2PubKey);
AddIntoLevel3PublicKeylookup (Level3PubKey, Level1ID, Level2ID, Level3ID);
```

The certificate module can thus be configured to pre-authenticate one or more mobile-side certificates to expedite run-time authentication of a mobile device.

The authentication request receiving module can be configured to receive an authentication request from a device seeking authentication (e.g., a mobile device). The authentication request can include a variety of information. In some embodiments, the authentication request can include a device-specific public key (e.g., a L4 public key) of the mobile device. The request can also include one or more superior public keys in the mobile-side certificate hierarchy. While the request can include the entire certificate(s), in some embodiments, only the public key portion of the certificate is included, thereby reducing the data payload and speeding transaction time. The request can also include identification information for specifying the chain of trust by which the mobile device traces back to a mutual trusted root certificate. For example, the request can include a concatenation of unique identifiers associated with each certificate (or public key thereof) in the chain of trust. The request can also include information used as a precursor to a session key which ultimately can be used to encrypt sensitive data once mutual authentication is complete. For example, the precursor can be or can include a random number generated by the mobile device.

The authentication module can be configured to validate public keys received in the authentication request. In particular, the authentication module can use the identification information in the request to determine from the lookup table the set of pre-authenticated public keys required to decrypt the device-specific public key included in the request. The authentication module can also be configured to request any certificates in the chain that may be missing from the certificate repository, e.g., from the mobile device or from the fueling payment network.

The session key generation module can be configured to generate a session key when the authentication request is successfully validated. For example, the session key generation module can combine a session key precursor generated by the payment terminal (e.g., a random number) with the session key precursor included in the request to produce a final session key. The session key can be used by two mutually-authenticated devices to encrypt and decrypt information communicated between the devices. The session key generation module can also be configured to generate a checksum for use by a mutually-authenticated party to validate the session key.

The authentication response transmitting module can be configured to transmit an authentication response to the mobile device. The authentication response can include a variety of information. In some embodiments, the authentication response can include a device-specific public key (e.g., a L4 public key) of the payment terminal. The response can also include one or more superior public keys in the terminal-side certificate hierarchy. While the response can include the entire certificate(s), in some embodiments, only the public key portion of the certificate is included, thereby reducing the payload and speeding transaction time. The response can also include identification information for specifying the chain of trust by which the payment terminal traces back to a mutual root certificate. For example, the response can include a concatenation of unique identifiers associated with each certificate (or public key thereof) in the chain of trust. The response can also include the encrypted session key and checksum.

The secure information receiving module can be configured to receive secure information from an authenticated device and to decrypt the information using the session key. In particular, a user’s payment or loyalty information can be encrypted by the mobile device using the session key and received by the secure information receiving module. The secure information receiving module can then decrypt the information using the session key such that the payment terminal can complete the transaction.
MOBILE DEVICE MODULES

[0050] FIG. 6 is a schematic diagram of the modules of one exemplary embodiment of the mobile device 104. As shown, the mobile device 104 can include a certificate module 602, an authentication request transmitting module 604, an authentication response receiving module 606, an authentication module 608, a session key validation module 610, and a secure information transmitting module 612. The mobile device 104 can also include a lookup table 614 and a certificate repository 616.

[0051] The certificate module 602, lookup table 614, and certificate repository 616 of the mobile device 104 are substantially identical to those of the payment terminal 102, with a few exceptions as discussed below. One difference is that the L4 certificate 414 in the certificate module 602 corresponds to the mobile device 104 instead of the payment terminal 102. The mobile device 104 is pre-loaded with certificates installed during manufacture and production of the mobile device 104, or the certificates can be downloaded via the mobile payment cloud 116 or the mobile loyalty cloud 114. The certificate hierarchy of the mobile device 104 is the same as that described above, with the mobile device 104 including the certificates in its own chain of trust as well as one or more pre-authenticated terminal-side certificates.

[0052] The authentication request transmitting module 604 is configured to assemble the authentication request described above and to send the request to the payment terminal 102 when triggered by a user (e.g., when the user places the mobile device 104 in proximity to the payment terminal, when the user launches an application on the mobile device, or when the user actuates a user interface element on the mobile device).

[0053] The authentication response receiving module 606 is configured to receive the authentication response described above from the payment terminal 102.

[0054] The authentication module 608 is configured to authenticate the L4 public key received from the payment terminal 102 using an authentication system as described above with respect to the authentication module 306 of the payment terminal 102.

[0055] The session key validation module 610 is configured to decrypt the session key received from the payment terminal 102 using the payment terminal's L4 public key and to validate the session key using the checksum received from the payment terminal.

[0056] The secure information transmitting module 612 is configured to encrypt secure information using the session key and to transmit the encrypted secure information to the payment terminal 102 to complete a transaction.

OPERATION

[0057] An exemplary method of conducting a mutually-authenticated transaction is illustrated schematically in FIGS. 7, 8, and 9. While various methods disclosed herein may be shown in relation to flowcharts or sequence diagrams, it should be noted that any ordering of method steps implied by such flowcharts, sequence diagrams, or the description thereof is not to be construed as limiting the method to performing the steps in that order. Rather, the various steps of each of the methods disclosed herein can be performed in any of a variety of sequences. In addition, as the illustrated flowcharts and sequence diagrams are merely exemplary embodiments, various other methods that include additional steps or include fewer steps than illustrated are also within the scope of the present disclosure.

[0058] FIG. 7 is a sequence diagram of the mutually-authenticated transaction. The mutual authentication process can, in some embodiments, involve only a single exchange between the payment terminal 102 and the mobile device 104 (e.g., an authentication request transmitted from the mobile device 104 to the payment terminal 102 and an authentication response transmitted from the payment terminal 102 to the mobile device 104). Completing the authentication process in a single exchange can advantageously decrease the amount of time required to complete a transaction, increasing user convenience. Initially, the payment terminal 102 is in a ready state waiting for a mobile device 104 to initiate a transaction. The payment terminal 102 can display a message requesting that the user initiate a transaction using their mobile device 104.

[0059] To begin the transaction, the mobile device 104 sends an authentication request to the payment terminal 102. For example, the authentication request transmitting module 604 of the mobile device 104 can transmit an authentication request to the authentication request receiving module 304 of the payment terminal 102. The authentication request can include:

1. the device-specific (e.g., L4) public key of the mobile device 104, which is encrypted by a mobile-side L3 private key,
2. the mobile-side L3 public key, encrypted by a mobile-side L2 private key,
3. a unique identifier that specifies the chain of public keys required to decrypt the L4 public key of the mobile device 104 (e.g., Level1ID + Level2ID + Level3ID), and
A random number $R_1$ generated by the mobile device 104 and encrypted by the mobile device's L4 private key.

(4) Upon receipt of the authentication request, the payment terminal 102 can attempt to authenticate the received L4 public key using the lookup table 314 and certificate repository 316. In particular, the authentication module 306 of the payment terminal 102 can use the received unique identifier (Level1ID + Level2ID + Level3ID) to locate the pre-authenticated L3 public key that can decrypt the L4 public key of the mobile device 104. If the L3 public key is present in the payment terminal 102, the received L4 public key can be decrypted and then used to decrypt the random number $R_1$.

[0061] In some instances, the L3 public key that can decrypt the L4 public key of the mobile device 104 may not be pre-loaded in the payment terminal 102. For example, the mobile-side L3 certificate may not yet be available for download through the fueling payment network 112, e.g., if the mobile device 104 is of a particular brand, model, or carrier that is new. In such cases, the authentication module 306 can use the received unique identifier without the Level3ID (i.e., Level1ID + Level2ID) to locate the pre-authenticated L2 public key that can decrypt the L3 public key of the mobile device 104. If the L2 public key is present in the payment terminal 102, the received L3 public key can be decrypted and then used, as described above, to decrypt the L4 public key which in turn decrypts the random number $R_1$. The newly-decrypted L3 public key can then be stored in the certificate repository 316 for future use and its corresponding unique identifier (Level1ID + Level2ID + Level3ID) can be added to the lookup table 314.

[0062] If the L2 public key is not present in the payment terminal 102, the payment terminal can attempt to locate the L2 public key over a network, request the public key from the mobile device 104, or deny the transaction.

[0063] After the random number $R_1$ is decrypted, the session key generation module 308 of the payment terminal 102 can generate a session key $S_1$ to be used in carrying out the transaction. In some embodiments, the session key generation module 308 can generate its own random number $R_2$ and create the session key $S_1$ based on a combination of the mobile device's random number $R_1$ and the payment terminal's random number $R_2$. For example, the session key $S_1$ can be defined by the exclusive or of $R_1$ and $R_2$:

$$S_1 = \text{XOR} (R_1, R_2)$$

[0064] The session key generation module 308 can also generate a checksum $\text{CHKS1}$ of the session key $S_1$, for example by calculating a hash of the session key:

$$\text{CHKS1} = \text{Hash} (S_1)$$

[0065] The session key generation module 308 can then encrypt the session key $S_1$ using the mobile device's L4 public key, such that only the private key stored in the mobile device's secure element 216 can be used to decrypt and obtain the session key $S_1$. The checksum $\text{CHKS1}$ can be encrypted using the payment terminal's own L4 private key.

[0066] The following pseudo code demonstrates the process of authenticating the mobile device 104 and generating the session key $S_1$ and session key checksum $\text{CHKS1}$:

```plaintext
PubKey = Lookup(MobileDevicelevel1ID + MobileDevicelevel2ID + MobileDevicelevel3ID)
If (PubKey == null)
    {Level2PubKey = Lookup (MobileDevicelevel1ID + MobileDevicelevel2ID);
     If (Level2PubKey != null)
        
        PubKey = DecryptPubKey (Encrypted Level3 PubKey, Level2PubKey);
        NewCertificateAvailable=true;
    }
If (PubKey !=null)
    {
        Level4PubKey=Decrypt (Given Encrypted Level4 Pub Key, PubKey);
        R1 = Decrypt (Given Encrypted R1, Level4PubKey);
        R2 = RandomGeneration();
        S1 = R1 XOR R2;
        EncryptedS1 = Encrypt (S1, Level4PubKey);
        EncryptedCHKS1 = Encrypt (Hash(S1), MyPrivateKey);
    }
```

[0067] As noted above, if the mobile-side L2 public key is not available at the payment terminal 102, it can be obtained
in some instances from the fueling payment network 112, the fueling loyalty network 110, the mobile device 104, or some other source. An exemplary process for obtaining and decrypting the mobile-side L2 public key is demonstrated by the following pseudo code:

If (Levei2PubKey == null)
{
    Obtainlevei2Certificate (*Given Level2);
    Level1PubKey = Lookup (Given MobileDevicelevei11D);
    If (Level1PubKey == null)
        Throw Exception of "No Pre-stored Trusted Level1 Root CA"
    Level2PubKey = DecryptPubKeyFromCertificate (Level2, Level1PubKey);
    PubKey = DecryptPubKey (Encrypted Level3 PubKey, Levei2PubKey);
    NewCertificateAvailable = true;
}

As also noted above, the payment terminal 102 can be configured to store new certificates obtained at runtime (e.g., from the mobile device 104) and to add them to the lookup table 314 to facilitate faster processing in the future. An exemplary process for storing a new certificate and adding it to the lookup table 314 is demonstrated by the following pseudo code:

If (NewCertificateAvailable ==true)
{
    if (CanStoreAdditionalPubKeyIntolookupTable() ==true)
    {
        AddIntolevei3LookupTable (PubKey, MobileDevicelevei11D, MobileDevicelevei21D, MobileDevicelevei31D);
        AddIntolevei2LookupTable (Levei2PubKey, MobileDevicelevei11D, MobileDevicelevei21D);
        ReportToMyNetwork();
    }
}

After generating the session key S1 and the session key checksum CHKS1, the payment terminal 102 can transmit an authentication response to the mobile device 104. In particular, the authentication response transmitting module 310 of the payment terminal 102 can transmit the authentication response to the authentication response receiving module 606 of the mobile device 104.

The authentication response can include:

1. the device-specific (e.g., L4) public key of the payment terminal 102, which is encrypted by a terminal-side L3 private key,

2. the terminal-side L3 public key, encrypted by a terminal-side L2 private key,

3. a unique identifier that specifies the chain of public keys required to decrypt the L4 public key of the payment terminal 102 (e.g., Level1iD + Level2ID + Level3ID),

4. the session key S1, encrypted by the mobile device’s L4 public key; and

5. the session key checksum CHKS1, encrypted by the payment terminal’s L4 private key.

Upon receipt of the authentication response, the mobile device 104 can attempt to authenticate the received L4 public key using the lookup table 614 and the certificate repository 616. In particular, the authentication module 608 of the mobile device 104 can use the received unique identifier (Level1iD + Level2ID + Level3ID) to locate the pre-authenticated L3 public key that can decrypt the L4 public key of the terminal 102. If the L3 public key is present in the mobile device 104, the received L4 public key can be decrypted.

In some instances, the L3 public key that can decrypt the L4 public key of the terminal 102 may not be pre-loaded in the mobile device 104. For example, the terminal-side L3 certificate may not yet be available for download through the mobile loyalty cloud 114 or the mobile payment cloud 116, e.g., if the payment terminal 102 is of a particular brand, model, or payment network that is new. In such cases, the authentication module 608 can use the received unique identifier without the Level3ID (i.e., Level1iD+ Level2ID) to locate the pre-authenticated L2 public key that can decrypt
the L3 public key of the payment terminal 102. If the L2 public key is present in the mobile device 104, the received L3 public key can be decrypted and then used, as described above, to decrypt the L4 public key. The newly-decrypted L3 public key can then be stored in the certificate repository 616 for future use and its corresponding unique identifier (Level1ID + Level2ID + Level3ID) can be added to the lookup table 614.

If the L2 public key is not present in the mobile device 104, the mobile device can attempt to locate the L2 public key over a network, request the public key from the payment terminal 102, or deny the transaction.

If authentication is successful, the session key validation module 610 can use the mobile device’s own L4 private key to decrypt the session key S1 and use the decrypted L4 public key of the payment terminal 102 to decrypt the session key checksum CHKS1. The session key validation module 610 can then check whether the checksum CHKS1 matches the session key S1. If a match is found, both the mobile device 104 and the payment terminal 102 are in possession of the agreed upon session key S1 and the mutual-authentication process is complete.

The session key S1 can then be used to encrypt and decrypt user data transmitted between the mobile device 104 and the payment terminal 102. For example, the secure information transmitting module 612 of the mobile device 104 can encrypt the user’s primary account number (PAN), credit card expiration date, and credit card security code (CVV) using the session key S1 and can transmit the encrypted data to the payment terminal 102. The secure information receiving module 312 of the payment terminal 102 can receive the encrypted payment information and decrypt it using the session key S1. User loyalty information can be communicated in a similar fashion.

The following pseudo code demonstrates the process of authenticating the payment terminal 102 and encrypting the payment information using the session key S1, as well as obtaining additional certificates and updating the lookup table 614 if necessary:

```pseudo
def PubKey = Lookup(PaymentTerminallevel1D + PaymentTerminallevel2D + PaymentTerminallevel3D)
If (PubKey == null)
    Level2PubKey = Lookup(PaymentTerminallevel1D + PaymentTerminallevel2D);
    If (Level2PubKey != null)
        PubKey = DecryptPubKey (Encrypted Level3 PubKey, Level2PubKey);
        NewCertificateAvailable = true;
    If (Level2PubKey == null)
        ObtainLevel2Certificate ("Given Level2");
        Level1PubKey = Lookup (Given PaymentTerminallevel1D);
        If (Level1 PubKey == null)
            Throw Exception of "No Pre-stored Trusted Level1 Root CA"
        Level2PubKey = DecryptPubKeyFromCertificate (Level2, Level1 PubKey);
        PubKey = DecryptPubKey (Encrypted Level3 PubKey, Level2PubKey);
        NewCertificateAvailable =true;
    If (PubKey != null)
        Level4PubKey = Decrypt (Given Encrypted Level4 Pub Key, PubKey);
        S1 = Decrypt (Given Encrypted S1, MyPrivateKey);
        CHK81 = Decrypt (Given Encrypted CHK81, Level4PubKey);
        If (Hash(S1) == CHK81)
            EncryptedCardData = EncryptCardData (PAN, Expiration, CVV, S1);
    If (NewCertificateAvailable ==true)
        If (CanStoreAdditionalPubKeyIntolookupTable() ==true)
            AddIntoLevel3LookupTable (PubKey, PaymentTerminallevel1D, PaymentTerminallevel2D, PaymentTerminallevel3D);
            AddIntoLevel2LookupTable (Level2PubKey, PaymentTerminallevel1D, PaymentTerminallevel2D);
```

11
Once received by the payment terminal 102, the payment and/or loyalty information can be processed through the fuel payment network 112 and fuel loyalty network 110 in the same manner as if the user had presented a traditional magnetic-stripe plastic card.

FIG. 8 provides an overview of the above-described method from the perspective of the payment terminal 102. Initially, in step S800, the payment terminal 102 is idle. In step S802, an incoming authentication request is received from a mobile device 104. In decision block D804, the payment terminal 102 determines whether a L3 public key capable of decrypting the received L4 public key of the mobile device 104 is available. If not, the payment terminal 102 determines at decision block D806 whether a L2 public key capable of decrypting the received L3 public key is available. If not, the L2 certificate is requested from the mobile device 104 in step S808, received in step S810, and assessed for trustworthiness in decision block D812. If the L2 certificate is not trusted, mutual authentication fails in step S814. If the L2 certificate is trusted or if the L2 public key is available in the payment terminal 102, the L3 public key is decrypted in step S816. If the L3 public key was decrypted in step S816 or was available in decision block D804, the received L4 public key and, in turn, the received random number R1 are decrypted in step S818. In step S820, the authentication response is delivered to the mobile device 104 for authentication and the payment terminal 102 waits for a response from the mobile device in step S822. If the mobile device 104 requests the terminal-side L2 certificate (yes in decision block D824), it is transmitted to the mobile device in step S826 and execution returns to step S822. If the mobile device 104 is able to authenticate the payment terminal 1 02, encrypted payment and/or loyalty information is received from the mobile device at step S828 and the payment is processed at step S830.

FIG. 9 provides an overview of the above-described method from the perspective of the mobile device 104. Initially in step S900, the mobile device 104 receives an instruction to initiate a transaction, for example when a user launches a mobile payment application or actuates a button or other user interface element. In step S902, the mobile device 104 sends an authentication request to the payment terminal 102, and waits at step S904 for a response from the payment terminal. If the mobile device 104 receives a request from the payment terminal 102 for the mobile-side L2 certificate, (yes in decision block D906), the mobile device sends the certificate in step S908 and execution returns to step S904. Otherwise, the mobile device 104 processes the authentication response received from the payment terminal 102 and determines in decision block D910 whether a L3 public key capable of decrypting the L4 public key of the payment terminal is present in the mobile device. If not, the mobile device 104 determines at decision block D912 whether a L2 public key capable of decrypting the received L3 public key is available. If not, the L2 certificate is requested from the payment terminal in step S914, received in step S916, and assessed for trustworthiness in decision block D918. If the L2 certificate is not trusted, mutual authentication fails in step S920. If the L2 certificate is trusted or if the L2 public key is available in the mobile device 104, the L3 public key is decrypted in step S922. If the L3 public key was decrypted in step S922 or was available in decision block D910, the received L4 public key and, in turn, the received session key S1 are decrypted in step S924. Finally, in step S926, the mobile device 104 sends sensitive data encrypted by the session key S1 to the payment terminal 102.

In the above examples, the authentication request and the authentication response each include an encrypted L4 public key and an encrypted L3 public key. It will be appreciated, however, that more or fewer public keys can be included in the authentication request and/or the authentication response. For example, the request and/or the response can include only a single key (e.g., the encrypted L4 public key). By way of further example, the request and/or the response can include the encrypted L4 public key, the encrypted L3 public key, and one or more additional keys, such as an encrypted L2 public key.

The method of FIGS. 7, 8, and 9 can thus permit the payment terminal 102 and the mobile device 104 of FIG. 1 to engage in secure communication using a fast mutual authentication process. In particular, the payment terminal 102 can receive an authentication request from the mobile device 104 and, if the mobile device is authenticated, reply with an authentication response. After this single exchange, assuming authentication is successful, both parties possess a secure session key which can be used to encrypt sensitive information for wireless transmission. For example, the mobile device 104 can use the session key to encrypt customer payment or loyalty information and transmit the encrypted information to the payment terminal 102, which can decrypt the information using the session key and then process the information through normal channels.

SERVICE ACCESS

In some embodiments, the mobile device can be a service mobile device possessed by a user seeking to access the payment terminal, or a fuel dispenser or other system of which it is a part, for service purposes. In such cases, instead of transmitting payment or loyalty information upon completion of the mutual authentication process, the
service mobile device can be configured to transmit an instruction to open or unlock a service door, perform a diagnostic test, or perform other service-related functions. If the service mobile device is authenticated by the payment terminal, the payment terminal can respond to the service request by controlling an actuator to open or unlock the service door, etc. Accordingly, service personnel can be authenticated to prevent unauthorized access or unauthorized field service or troubleshooting operations, thereby providing improved security as compared with a traditional mechanical key model.

ADVANTAGES / TECHNICAL EFFECTS

[0083] The systems and methods disclosed herein can produce a number of advantages and/or technical effects.

[0084] For example, in some embodiments, digital certificates are pre-stored and pre-authenticated on the payment terminal and the mobile device, such that a reduced-size public key / identifier pair can be exchanged instead of a plurality of larger certificates, thus enabling rapid authentication and transaction execution. In some embodiments, the entire mutual authentication process can be completed in less than 500 ms, less than 250 ms, or less than 100 ms. In some embodiments, the authentication response transmitting module can be configured to transmit the authentication response less than 500 ms, less than 250 ms, or less than 100 ms after an authentication request is received by the authentication request receiving module.

[0085] By way of further example, in some embodiments, secure mutual authentication between two devices can be completed with only one transfer from the first device (e.g., a payment terminal) to the second device (e.g., a mobile device) and one transfer from the second device to the first device, thus enabling rapid authentication and transaction execution.

[0086] Further exemplary advantages and/or technical effects which may be produced by one or more of the systems and methods disclosed herein include: (1) secure, mutually-authenticated communication between a mobile device and a payment terminal without requiring extensive changes to or integration of existing fuel payment infrastructure and mobile payment infrastructure, (2) a secure NFC interface to allow a payment terminal to mutually authenticate with a mobile payment application to enable secure fast communication between the two, (3) no requirement for change in communication between a mobile payment cloud and a payment terminal cloud, and (4) improved security for service access.

[0087] This written description uses examples to disclose the invention, including the best mode, and also to enable any person skilled in the art to practice the invention, including making and using any devices or systems and performing any incorporated methods. The patentable scope of the invention is defined by the claims, and may include other examples that occur to those skilled in the art. Such other examples are intended to be within the scope of the claims if they have structural elements that do not differ from the literal language of the claims, or if they include equivalent structural elements with insubstantial differences from the literal languages of the claims.

Claims

1. A terminal (102), comprising
   a wireless transceiver (218) configured to communicate wirelessly with a mobile device (104);
   a secure element (216) configured to store one or more pre-validated cryptographic keys; and
   a processor (202) coupled to the secure element and the wireless transceiver, the processor being programmed to
      receive (S802), via the wireless transceiver, an authentication request from the mobile device, authenticate the mobile device by validating the authentication request based on the one or more pre-validated cryptographic keys stored in the secure element, generate a session key based on a random number received in the authentication request, transmit (S820), via the wireless transceiver, when the mobile device is successfully authenticated, an authentication response including the session key to the mobile device, and receive (S828) secure information from the mobile device, the secure information being encrypted by the session key.

2. The terminal of claim 1, wherein the terminal comprises at least one of a payment terminal, a kiosk, and a fuel dispenser.

3. The terminal of claim 1, wherein the transceiver comprises a near-field communication, NFC, transceiver.

4. The terminal of claim 1, wherein the authentication request comprises:
The terminal of claim 4, wherein the processor is configured to validate the authentication request by:

- using a lookup table (314) to determine whether a superior public key specified in the unique identifier is stored in the terminal and pre-validated; and
- if the superior public key is stored in the terminal and pre-validated, retrieving the superior public key and decrypting the first public key using the superior public key.

The terminal of claim 5, wherein the authentication request includes the superior public key and wherein the processor is configured to validate the authentication request by:

- if the superior public key is not stored in the terminal or not pre-validated, using the lookup table to determine whether a more-superior public key specified in the unique identifier is stored and pre-validated in the terminal, and
- if the more-superior public key is stored and pre-validated in the terminal, retrieving the more-superior public key and decrypting the superior public key using the more-superior public key; and
- if the more-superior public key is not stored in the terminal or not pre-validated, at least one of requesting the more-superior public key from the mobile device, obtaining the more-superior public key from a network, and rejecting the authentication request as originating from a non-authenticable mobile device.

The terminal of claim 4, wherein the session key comprises a combination of the random number R1 and a random number R2 generated by the terminal.

The terminal of claim 4, wherein the authentication response comprises:

- a second public key specific to the terminal, the second public key being encrypted by a terminal-side private key that is superior to the second public key in the certificate hierarchy;
- a terminal-side unique identifier that specifies the chain of public keys in the certificate hierarchy which ultimately decrypts the second public key;
- the session key, said session key being encrypted by the first public key of the mobile device; and
- a session key checksum generated by the processor, said session key checksum being encrypted by a private key corresponding to the second public key of the terminal.

The terminal of claim 8, wherein the authentication response comprises a terminal-side superior public key corresponding to the terminal-side superior private key.

The terminal of claim 1, wherein the terminal is configured to complete an authentication process with the mobile device in less than 500 ms.

The terminal of claim 1, wherein the terminal is configured to complete an authentication process with the mobile device in a single exchange.

The terminal of claim 1, wherein the secure information comprises payment information.

The terminal of claim 1, wherein the secure information comprises a service instruction to open a door of the terminal, and wherein the terminal is configured to open the door in response to the service instruction.

A secure communication method for execution by a terminal (102) that includes a wireless transceiver (218) configured to communicate wirelessly with a mobile device (104), a secure element (216) configured to store one or more pre-validated cryptographic keys, and a processor (202) coupled to the secure element and the wireless transceiver, the method comprising:

- receiving (S802), via the wireless transceiver, an authentication request from the mobile device;
- authenticating the mobile device by using the processor to validate the authentication request based on the
one or more pre-validated cryptographic keys stored in the secure element;
using the processor to generate a session key based on a random number received in the authentication request;
transmitting (S820), via the wireless transceiver, when the mobile device is successfully authenticated, an
authentication response including the session key to the mobile device; and
receiving (S828), via the wireless transceiver, secure information from the mobile device, the secure information
being encrypted by the session key.

15. The method of claim 14, further comprising executing a payment transaction using the secure information and
dispensing fuel from a fuel dispenser operatively coupled to the terminal.

Patentansprüche

1. Endgerät. (102), umfassend
einen drahtlosen Sendeempfänger (218), welcher so konfiguriert ist, dass er drahtlos mit einer mobilen Vorrichtung
(104) kommuniziert, ein sicheres Element (216), welches so konfiguriert ist, dass es einen oder mehrere vorvalidierte
kryptographische Schlüssel speichert; und einen Prozessor (202), welcher mit dem sicheren Element und dem
drahtlosen Sendeempfänger verbunden ist, wobei der Prozessor programmiert ist zum
Empfangen (S802) einer Authentifizierungsanforderung von der mobilen Vorrichtung über den drahtlosen Sende-
empfänger, Authentifizieren der mobilen Vorrichtung durch Validieren der Authentifizierungsanforderung auf der
Grundlage des einen oder der mehreren vorvalidierten kryptographischen Schlüssel, die in dem sicheren Element
gepapnochicht sind,
Erzeugen eines Sitzungsschlüssels auf der Grundlage einer Zufallszahl, die in der Authentifizierungsanforderung
empfangen wird, Senden (S820) einer Authentifizierungsantwort, welche den Sitzungsschlüssel umfasst, über den
drahtlosen Sendeempfänger an die mobile Vorrichtung, wenn die mobile Vorrichtung erfolgreich authentifiziert ist,
und
Empfangen (S828) sicherer Informationen von der mobilen Vorrichtung, wobei die sicheren Informationen durch
den Sitzungsschlüssel verschlüsselt sind.

2. Endgerät nach Anspruch 1, wobei das Endgerät mindestens eines aus einem Bezahlterminal, einem Verkaufsau-
tomaten und einer Zapfsäule umfasst.

3. Endgerät nach Anspruch 1, wobei der Sendeempfänger einen Sendeempfänger für Nahfeldkommunikation, NFC,
umfasst.

4. Endgerät nach Anspruch 1, wobei die Authentifizierungsanforderung umfasst:
einen ersten öffentlichen Schlüssel, welcher für die mobile Vorrichtung spezifisch ist, wobei der erste öffentliche
Schlüssel durch einen privaten Schlüssel verschlüsselt ist, der dem ersten öffentlichen Schlüssel in einer Zer-
tifikathierarchie übergeordnet ist;
eine eindeutige Kennung, welche die Kette von öffentlichen Schlüsseln in der Zertifikathierarchie spezifiziert,
durch welche der erste öffentliche Schlüssel am Ende entschlüsselt wird; und
eine Zufallszahl R1, welche durch einen privaten Schlüssel verschlüsselt ist, der dem ersten öffentlichen Schlüs-
sel entspricht.

5. Endgerät nach Anspruch 4, wobei der Prozessor so konfiguriert ist, dass er die Authentifizierungsanforderung
validiert durch:
Verwenden einer Verweistabelle (314) zum Bestimmen, ob ein übergeordneter öffentlicher Schlüssel, der in
der eindeutigen Kennung spezifiziert ist, in dem Endgerät gespeichert und vorvalidiert ist; und
wenn der übergeordnete öffentliche Schlüssel in dem Endgerät gespeichert und vorvalidiert ist, Abrufen des
übergeordneten öffentlichen Schlüssels und Entschlüsseln des ersten öffentlichen Schlüssels unter Verwen-
dung des übergeordneten öffentlichen Schlüssels.

6. Endgerät nach Anspruch 5, wobei die Authentifizierungsanforderung den übergeordneten öffentlichen Schlüssel
umfasst und wobei der Prozessor so konfiguriert ist, dass er die Authentifizierungsanforderung validiert durch:

wenn der übergeordnete öffentliche Schlüssel nicht in dem Endgerät gespeichert ist oder nicht vorvalidiert ist,

7. Endgerät nach Anspruch 4, wobei der Sitzungsschlüssel eine Kombination der Zufallszahl R1 und einer Zufallszahl R2 umfasst, die durch das Endgerät erzeugt wird.

8. Endgerät nach Anspruch 4, wobei die Authentifizierungsantwort umfasst:
   einen zweiten öffentlichen Schlüssel, welcher für das Endgerät spezifisch ist, wobei der zweite öffentliche Schlüssel durch einen endgerätseitigen privaten Schlüssel verschlüsselt ist, welcher dem zweiten öffentlichen Schlüssel in der Zertifikathierarchie übergeordnet ist;
   eine endgerätseitige eindeutige Kennung, welche die Kette von öffentlichen Schlüsseln in der Zertifikathierarchie spezifiziert, durch welche der zweite öffentliche Schlüssel am Ende entschlüsselt wird;
   den Sitzungsschlüssel, wobei der Sitzungsschlüssel durch den ersten öffentlichen Schlüssel der mobilen Vorrichtung verschlüsselt ist; und eine von dem Prozessor erzeugte Sitzungsschlüssel-Prüfsumme, wobei die Sitzungsschlüssel-Prüfsumme durch einen privaten Schlüssel verschlüsselt ist, welcher dem zweiten öffentlichen Schlüssel des Endgeräts entspricht.

9. Endgerät nach Anspruch 8, wobei die Authentifizierungsantwort einen endgerätseitigen übergeordneten öffentlichen Schlüssel umfasst, welcher dem endgerätseitigen übergeordneten privaten Schlüssel entspricht.

10. Endgerät nach Anspruch 1, wobei das Endgerät so konfiguriert ist, dass es ein Authentifizierungsverfahren mit der mobilen Vorrichtung in weniger als 500 ms abschließt.

11. Endgerät nach Anspruch 1, wobei das Endgerät so konfiguriert ist, dass es ein Authentifizierungsverfahren mit der mobilen Vorrichtung in einem einzigen Austausch abschließt.

12. Endgerät nach Anspruch 1, wobei die sicheren Informationen Bezah lungsinformationen umfassen.

13. Endgerät nach Anspruch 1, wobei die sicheren Informationen einen Dienstbefehl zum Öffnen einer Tür des Endgeräts umfassen und wobei das Endgerät so konfiguriert ist, dass es die Tür in Reaktion auf den Dienstbefehl öffnet.

14. Sicheres Kommunikationsverfahren zur Ausführung durch ein Endgerät (102), welches einen drahtlosen Sendeempfänger (218), der so konfiguriert ist, dass er drahtlos mit einer mobilen Vorrichtung (104) kommuniziert, ein sicheres Element (216), das so konfiguriert ist, dass es einen oder mehrere vorvalidierte kryptographische Schlüssel speichert, und einen Prozessor (202) umfasst, der mit dem sicheren Element und dem drahtlosen Sendeempfänger verbunden ist, wobei das Verfahren umfasst:
   Empfangen (S802) einer Authentifizierungsanforderung von der mobilen Vorrichtung über den drahtlosen Sende empfänger;
   Authentifizieren der mobilen Vorrichtung unter Verwendung des Prozessors zum Validieren der Authentifizierungsanforderung auf der Grundlage des einen oder der mehreren vorvalidierten kryptographischen Schlüssel, die in dem sicheren Element gespeichert sind;
   Verwenden des Prozessors zum Erzeugen eines Sitzungsschlüssels auf der Grundlage einer Zufallszahl, die in der Authentifizierungsanforderung empfangen wird;
   Senden (S820) einer Authentifizierungsantwort, welche den Sitzungsschlüssel umfasst, über den drahtlosen Sendeempfänger an die mobile Vorrichtung, wenn die mobile Vorrichtung erfolgreich authentifiziert ist; und Empfangen (S828) sicherer Informationen von der mobilen Vorrichtung über den drahtlosen Sendeempfänger, wobei die sicheren Informationen durch den Sitzungsschlüssel verschlüsselt sind.

15. Verfahren nach Anspruch 14, ferner umfassend Ausführen einer Bezahlungstransaktion unter Verwendung der
sicheren Informationen und Abgeben von Treibstoff aus einer Zapfsäule, die operativ mit dem Endgerät verbunden ist.

Revendications

1. Terminal (102), comprenant :

   un émetteur-récepteur sans fil (218) configuré pour communiquer sans fil avec un dispositif mobile (104) ;
   un élément sécurisé (216) configuré pour stocker une ou plusieurs clés cryptographiques pré-validées ; et
   un processeur (202) couplé à l’élément sécurisé et l’émetteur-récepteur sans fil, le processeur étant programmé
   pour recevoir (S802), via l’émetteur-récepteur sans fil, une demande d’authentification du dispositif mobile,
   authentifier le dispositif mobile en validant la demande d’authentification sur la base de cette ou ces clés
   cryptographiques pré-validées stockées dans l’élément sécurisé,
   générer une clé de session sur la base d’un nombre aléatoire reçu dans la demande d’authentification,
   envoyer (S820), via l’émetteur-récepteur sans fil, lorsque le dispositif mobile est authentifié avec succès, une
   réponse d’authentification comprenant la clé de session au dispositif mobile, et
   recevoir (S828) de l’information sécurisée du dispositif mobile, l’information sécurisée étant cryptée par la clé
   de session.

2. Terminal selon la revendication 1, dans lequel le terminal comprend au moins l’un parmi un terminal de paiement,
   un kiosque, et un distributeur de carburant.

3. Terminal selon la revendication 1, dans lequel l’émetteur-récepteur comprend un émetteur-récepteur de communi-
   cation en champ proche, NFC.

4. Terminal selon la revendication 1, dans lequel la demande d’authentification comprend :

   une première clé publique spécifique au dispositif mobile, la première clé publique étant cryptée par une clé
   privée qui est supérieure à la première clé publique dans une hiérarchie de certification;
   un identifiant unique qui spécifie la chaîne de clés publiques dans la hiérarchie de certification qui décrypte
   finalement la première clé publique ; et
   un nombre aléatoire RI crypté par une clé privée correspondant à la première clé publique.

5. Terminal selon la revendication 4, dans lequel le processeur est configuré pour valider la demande d’authentification
   grâce à :

   l’utilisation d’une table de consultation (314) pour déterminer si une clé publique supérieure spécifiée dans
   l’identifiant unique est stockée dans le terminal et est pré-validée ; et
   si la clé publique supérieure est stockée dans le terminal et pré-validée, la récupération de la clé publique
   supérieure et le décryptage de la première clé publique en utilisant la clé publique supérieure.

6. Terminal selon la revendication 5, dans lequel la demande d’authentification comprend la clé publique supérieure,
   et dans lequel le processeur est configuré pour valider la demande d’authentification grâce à :

   si la clé publique supérieure n’est pas stockée dans le terminal ou pré-validée, l’utilisation de la table de con-
   sultation pour déterminer si une clé publique davantage supérieure spécifiée dans l’identifiant unique est stockée
   et pré-validée dans le terminal, et
   si la clé publique davantage supérieure est stockée et pré-validée dans le terminal, la récupération de la clé
   publique davantage supérieure et le décryptage de la clé publique supérieure en utilisant la clé publique da-
   vantage supérieure ; et
   si la clé publique davantage supérieure n’est pas stockée dans le terminal ou non pré-validée, au moins l’une
   parmi une demande de la clé publique davantage supérieure au dispositif mobile, une obtention de la clé
   publique davantage supérieure d’un réseau, et le rejet de la demande d’authentification en tant que provenant
   d’un dispositif mobile non authentifiable.

7. Terminal selon la revendication 4, dans lequel la clé de session comprend une combinaison entre le nombre aléatoire
   R1 et un nombre aléatoire R2 généra par le terminal.
8. Terminal selon la revendication 4, dans lequel la réponse d’authentification comprend :

- une deuxième clé publique spécifique au terminal, la deuxième clé publique étant cryptée par une clé privée côté terminal qui est supérieure à la deuxième clé publique dans la hiérarchie de certification ;
- un identifiant unique côté terminal qui spécifie la chaîne de clés publiques dans la hiérarchie de certification qui décrypte finalement la deuxième clé publique ;
- la clé de session, ladite clé de session étant cryptée par la première clé publique du dispositif mobile ; et
- une somme de contrôle de clé de session générée par le processeur, ladite somme de contrôle de clé de session étant cryptée par une clé privée correspondant à la deuxième clé publique du terminal.

9. Terminal selon la revendication 8, dans lequel la réponse d’authentification comprend une clé publique supérieure côté terminal correspondant à la clé privée supérieure côté terminal.

10. Terminal selon la revendication 1, dans lequel le terminal est configuré pour achever un processus d’authentification avec le dispositif mobile en moins de 500 ms.

11. Terminal selon la revendication 1, dans lequel le terminal est configuré pour achever un processus d’authentification avec le dispositif mobile en un seul échange.

12. Terminal selon la revendication 1, dans lequel l’information sécurisée comprend de l’information de paiement.

13. Terminal selon la revendication 1, dans lequel l’information sécurisée comprend une instruction de service pour ouvrir une porte du terminal, et dans lequel le terminal est configuré pour ouvrir la porte en réponse à l’instruction de service.

14. Procédé de communication sécurisée pour l’exécution par un terminal (102) qui comprend un émetteur-récepteur sans fil (218) configuré pour communiquer sans fil avec un dispositif mobile (104), un élément sécurisé (216) configuré pour stocker une ou plusieurs clés cryptographiques pré-validées, et un processeur (202) couplé à l’élément sécurisé et l’émetteur-récepteur sans fil, le procédé comprenant :

- la réception (S802), via l’émetteur-récepteur sans fil, d’une demande d’authentification du dispositif mobile ;
- l’authentification du dispositif mobile en utilisant le processeur pour valider la demande d’authentification sur la base de cette ou ces clés cryptographiques pré-validées stockées dans l’élément sécurisé ;
- l’utilisation du processeur pour générer une clé de session sur la base d’un nombre aléatoire reçu dans la demande d’authentification ;
- l’envoi (S820), via l’émetteur-récepteur sans fil, lorsqu le dispositif mobile est authentifié avec succès, d’une réponse d’authentification comprenant la clé de session au dispositif mobile ; et
- la réception (S828), via l’émetteur-récepteur sans fil, de l’information sécurisée du dispositif mobile, l’information sécurisée étant cryptée par la clé de session.

15. Procédé selon la revendication 14, comprenant en outre l’exécution d’une transaction de paiement en utilisant l’information sécurisée et la distribution de carburant à partir d’un distributeur de carburant couplé de manière fonctionnelle au terminal.
Fig. 2
Payment Terminal 102

- PAYMENT TERMINAL IS READY TO ACCEPT DATA FROM MOBILE DEVICE

Mobile Device 104

- USER LAUNCHES MOBILE APPLICATION & ENABLES APPLICATION TO SEND DATA TO PAYMENT TERMINAL

DATA DELIVERED: ENCRYPTED OWN L4 PUBLIC KEY, MOBILE-SIDE ENCRYPTED L3 PUBLIC KEY, IDENTIFIERS FOR MOBILE-SIDE L1, L2, and L3, AND ENCRYPTED RANDOM NUMBER

1. AUTHENTICATE THE RECEIVED L4 PUBLIC KEY THROUGH LOOKUP PROCESS
2. GENERATE SESSION KEY

DATA DELIVERED: ENCRYPTED OWN L4 PUBLIC KEY, PAYMENT-SIDE ENCRYPTED L3 PUBLIC KEY, IDENTIFIERS FOR PAYMENT-SIDE L1, L2 AND L3, AND ENCRYPTED SESSION KEY AND CHECK VALUE

1. AUTHENTICATE THE RECEIVED L4 PUBLIC KEY THROUGH LOOKUP PROCESS
2. DECRYPT AND VALIDATE THE SESSION KEY
3. ENCRYPT SENSITIVE DATA (CARD DATA OR SERVICE COMMANDS)

ASK USER TO REMOVE MOBILE DEVICE

DATA DELIVERED: ENCRYPTED SENSITIVE DATA (CARD DATA OR SERVICE COMMANDS)

Fig. 7
REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- EP 1653655 A [0006]
- US 2008294894 A [0007]