Method for Access to an Electronic Device by a Data Terminal

Description

This invention pertains to a method for accessing an electronic device by a data terminal as well as a computer program product, an electronic device and a data terminal.

Methods for electronically storing data under cryptographic protection are already well-known from the state of the art. One form of protected storage, which has found broad acceptance over the last two decades, is electronic chip cards, which are standardized by ISO 7816 Sections 1 through 4. One of the most important application areas for chip

card technology in the future is the introduction of machine-readable travel documents. Anticipated benefits of this include an increase in security as well as efficiency in checking passengers, particularly when it comes to global air travel. Over the last several years, the International Civil Aviation Organization ICAO has provided standards for machine-readable travel documents.

Seen alongside the secure storage of personal data in machine-readable travel documents is the goal of simplifying security checks by the largest possible number of governmental and non-governmental organizations and the extent to which personal data is worthy of protection from being read without authorization. A suitable balance between both requirements must allow for both differences in the method of legal data protection and varying extents to which individual data objects are worthy of protection.

A system is known from US 2005/0097320A1 which enables communication between a user and an institution, such as a bank. Communication takes place via a network. A "transaction risk assessment" occurs each time the user accesses the institution's system, which determines the risk of the current transaction.

A similar system is known from US 2002/0087894 A1, where the user himself selects the security level for the data transfer.

According to the invention, a method is provided for a data terminal to access one of a number of data objects stored in an electronic device, whereby the electronic device features an allocation table in which a cryptographic protocol of a different security level is assigned to different data objects. The data terminal first transmits a request to the electronic device for a particular one of the data objects. With the aid of the allocation table, the electronic device specifies a cryptographic protocol for that one data object. The electronic device and the data terminal implement the cryptographic protocol. Assuming successful implementation, the electronic device transmits that one data object to the data terminal.

The present invention has a particular advantage in that it enables data objects classified as worthy of different levels of protection, which are stored together in an electronic device serving as a data carrier, to be protected to different degrees and in

this way comply flexibly with conflicting demands for accessibility to the stored data objects.

According to one embodiment of the invention, the electronic device features a software application which contains the allocation table. With the aid of the allocation table, the software application determines the cryptographic protocol, implements the specific cryptographic protocol with the data terminal and the software application and, assuming it is successful, sends the one data object to the data terminal. Consequently, all of the procedural steps of the electronic device are implemented by the software application, which has the advantage that the electronic device is built using standardized, cost-effectively produced hardware and the level of cryptographic protection of the data objects can be easily adapted to individual requirements.

According to one embodiment of the invention, the electronic device features an operating system that prevents unauthorized alteration or removal of the software application and only permits access to the data objects via the software application. This function of the operating system ensures that the protection of the data objects implemented by the software application cannot be circumvented or broken by an unauthorized party. Preferably, however, the operating system allows alteration or removal of the software application after authentication as an administrator of the electronic device. This is particularly advantageous because the allocation of individual data objects to cryptographic protocols or the cryptographic protocols themselves can be changed, for example, without having to replace the electronic device. In a preferred but unlimited manner, the invention pertains to a software application implementing the method for a chip card, in particular a Java-Applet for a chip card with an operating system that includes a virtual Java machine.

According to one embodiment of the invention, the electronic device is integrated into an identity document. Identity documents can include, for example, chip cards in check card format, or documents of other formats such as passports or visas, in which the electronic device is embedded. In particular, the identity document can pertain to a machine-readable travel document in accordance with the ePassport standardizations of the International Civil Aviation Organization, ICAO. The ICAO defines a file system conforming to the chip card standard ISO 7816-4 for machine-readable travel

documents carrying the designation Logical Data Structure (LDS) as well as an interoperable structure of the data stored in the file system.

According to one embodiment of the invention, at least one of the data objects includes personal biometric data. In the case of a machine-readable travel document in accordance with ePassport standardizations, the path names and file formats of personal – and also biometric – data are laid down by the LDS. In particular, the storing of a photograph, fingerprints and iris data of the holder of the identity document is standardized. The embodiment is of particular advantage, since for example a different, perhaps lower level of being worthy of protection and thus a cryptographic protocol of a lower security level can be assigned to the photograph than to the fingerprints or iris data.

Depending on the embodiment of the invention, the repertoire of the cryptographic protocols available to the electronic device and the data terminal can comprise different protocols and the allocation of the individual data objects stored in the electronic device can be defined in different ways for the individual cryptographic protocols available. According to the invention, read access can be freely granted, linked to the implementation of a cryptographic protocol, linked to the implementation of one of several cryptographic protocols made available for choosing or linked to the mandatory implementation of several cryptographic protocols. Preferably, free access is assigned to at least one of the number of data objects in the allocation table without a mandatory cryptographic protocol.

According to one embodiment of the invention, a cryptographic protocol of elevated security level is assigned to at least one data object, which requires authentication of the data terminal to the electronic device by means of a Challenge-Response procedure, which is based on a symmetrical cryptographic algorithm. A device-specific key is used here, which the data terminal must derive from machine-readable printed data associated with the electronic device. A general key that must be known to the electronic device and data terminal may also be required to derive the device-specific key.

According to one embodiment of the invention, a cryptographic protocol of a higher security level is assigned to at least one data object, which requires authentication of the data terminal with respect to the electronic device by means of a Challenge-Response procedure based on an asymmetrical cryptographic algorithm. The data terminal has both a public key and a private key in this case. The data terminal sends the electronic device its public key, which is preferably provided with a digital signature that can be verified by the electronic device via a certificate chain. The data terminal subsequently proves to the electronic device in a Challenge-Response sequence, that it is also in possession of the associated private key. Preferably, the implementation of the cryptographic protocol of a higher security level is required in addition to the protocol of an elevated security level.

According to one embodiment of the invention, communication between the data terminal and the electronic device is contactless, preferably via a contactless interface corresponding to the norms ISO/IEC 14443 Parts 1 through 4, as stipulated by the ICAO in the case of machine-readable travel documents. To prevent unauthorized monitoring of the contactless communication by third parties, it is preferable to also assign an encryption protocol of a different security level to [the] different data objects in the allocation table, according to which the data terminal and electronic device communicate in an encrypted manner. In this way, the data terminal and electronic device preferably exchange a session key in a safe manner.

In other respects, preferred embodiments of the invention are explained in more detail with reference to the drawings. These include:

Figure 1 a block diagram of an embodiment of the data terminal according to the invention and the electronic device according to the invention,

Figure 2 a flow chart of the method according to the invention,

Figure 3 a flow chart of the procedural steps implemented by one embodiment of the electronic device according to the invention and

Figure 4 a flow chart of the procedural steps implemented by one embodiment of the data terminal according to the invention.

Figure 1 shows a block diagram of one embodiment of data terminal 100 and of electronic device 102, which is integrated into an identity document 114. The identifying document is presented as a passport in a schematic, perspective view and features a zone with machine-readable printed data 116. Integration of the electronic device into the identity document can be done, for example, by embedding it into the cover page or the main page of a passport.

Both electronic device 102 and data terminal 100 can have a contactless interface 142 or 142', which is connected to both a transmitter 130 or 130' and a receiver 128 or 128' and facilitates the contactless communication between data terminal and electronic device. Electronic device 102 can feature a memory 126 for a number of data objects 104. Personal biometric data such as a photograph, fingerprints, or iris data of the owner of identity document 114 can be stored in one or more of data objects 104. Storage of data objects 104 in memory 126 may follow the standard series 9303 "Machine-readable Travel Documents" of the International Civil Aviation Organization, ICAO. Under the designation "Logical Data Structure" (LDS), the ICAO defines a file system that conforms to the chip card standard ISO 7816-4 as well as an interoperable structure of the data objects stored in this file system.

Data terminal 100 can be programmed with computer-executable instructions 124', which allow it to read access data objects 104 stored in memory 126 of electronic device 102 via contactless interfaces 142' and 142. To protect the personal biometric data, in particular, from unauthorized readout, electronic device 102 has program instructions 124, which can link read access to data objects 104 to the successful implementation of a cryptographic protocol with data terminal 100. One such measure is recommended by the ICAO, which mentions the support of a number of data protection options as a mandatory requirement for the standardized LDS.

Various types of personal biometric data which are worthy of protection at various levels can be stored in different data objects 104. For example, only slight sensitivity can be attributed to a photograph, while fingerprints or iris data are worthy of a higher level of

protection. The various assessments of being worthy of protection of different data objects 104 are coded by allocation table 106 of electronic device 102. Each data object 104 in the allocation table is assigned a cryptographic protocol 108 of a different security level. The allocation table can assign free access without the mandatory implementation of a cryptographic protocol to one or a number of data objects 104.

In operation, electronic device 102 receives a request for one of the data objects 104 from data terminal 100 via receiver 128 and contactless interface 142. Thereupon, using allocation table 106, the electronic device specifies a cryptographic protocol 108, the successful execution of which is set as a condition for read access of the data terminal to one of the data objects. The electronic device and the data terminal carry out the cryptographic protocol and, if successful, the electronic device transmits the one data object to the data terminal.

Electronic device 102 may feature a software application 110, which includes allocation table 106. Cryptographic protocol 108 is thus specified by the software application, the cryptographic protocol is carried out by the data terminal and the software application, and the one data object is transmitted by the software application. The electronic device can feature an operating system 112, which, working together with the hardware of the electronic device, prevents any unauthorized alteration or removal of the software application and only allows access to data objects 104 via the software application. In this way it is possible to implement electronic device 102 on the basis of mass-produced, standardized hardware, while at the same time the specifications of the cryptographic protocols which are being used and the coded allocation of data objects 104 in allocation table 126 can be adapted to cryptographic protocols of varying requirements. The electronic device can be a Java card with a virtual Java machine, on which software application 110 is installed in the form of a Java Applet.

Operating system 112 can protect software application 110 including allocation table 126 from unauthorized alteration or removal, while at the same time feature an administrator function 140, which allows alteration or removal of the software application following authentication as administrator of electronic device 102. The administrator function is especially advantageous because the electronic device can be adapted to revised requirements instead of being replaced by a new electronic device. Revised

requirements can pertain, for example, to improved cryptographic protocols 108 or a revised classification of worthiness of protection of different data objects 104.

Various encryption protocols 109 can also be assigned to different data objects in allocation table 106, according to which electronic device 102 and data terminal 100 can encrypt their communication. Encryption is particularly advantageous, since it allows third parties to be prevented from monitoring the contactless communication between the electronic device and the data terminal.

Electronic device 102 and data terminal 100 may have suitable cryptographic keys 118, 120 and 146, which are used in carrying out various cryptographic protocols.

Data terminal 100 can derive another device-specific key for electronic device 102 from machine-readable printed data 116. To this end, the data terminal may feature an optical sensor to read printed data 116 visually. A symmetrical key for communicating with electronic device 102 can thus be obtained from the data so recorded. In one embodiment, data 116 is used as a symmetrical key. This symmetrical key can be stored in unprotected or protected form in electronic device 102. Alternatively, electronic device 102 is designed in such a way that, if needed, it can generate this symmetrical key from data 116 also electronically stored in electronic device 102.

A general key 146 or 146' can also be used, which is familiar to both the electronic device and data terminal 100. The data terminal may also feature an asymmetrical pair of keys from public 118 and private 120 keys, whereby it transmits its public key to the electronic device as part of a cryptographic protocol. The public key can be provided with a digital signature 122, which allows it to verify the authenticity of the key 118 by means of a certificate chain.

General key 146' can be used from data terminal 100, for example, in order to generate the additional symmetrical key from optically recorded data 116. To this end, general key 146' and data 116 are linked together.

Figure 2 is a flow diagram which shows the method according to the invention for the data terminal to access one of the data objects stored in the electronic device. In step

216, the data terminal transmits a request to the electronic device for the one particular data object. In step 218 the electronic device uses its allocation table to specify a cryptographic protocol. In step 222 the electronic device and the data terminal carry out the cryptographic protocol. In step 220 the electronic device transmits the one data object to the data terminal.

In this context, the coded information in the allocation table of the electronic device, whose cryptographic protocol is assigned to the one data object, may already be known to the data terminal even before transmitting 216 the request. For example, the allocation table currently existing in the electronic device may contain content specified by a standard, which the data terminal also has a copy of. Alternatively, the electronic device may transmit a specification of the cryptographic protocol to the data terminal before its implementation 222, whereby the specification must correspond to one cryptographic protocol out of a repertoire of several, which the data terminal is able to implement. As another alternative, the electronic device can transmit the specification of several cryptographic protocols to the data terminal, from which the data terminal can select any desired protocol which it is able to implement.

Figure 3 shows a flow chart of the procedural steps implemented by a preferred embodiment of the electronic device according to the invention. After the electronic device has received a request for a data object from the data terminal in step 216, it specifies in step 218, with the aid of the allocation table, a cryptographic protocol (CP), the mandatory implementation of which the read access is supposed to be linked to by the data terminal. Presented as examples are three possible arrangements, including linking to a cryptographic protocol of an elevated security level beginning with step 200, linking to a cryptographic protocol of a higher security level beginning with step 210, and free access without linking to a cryptographic protocol.

When specifying the cryptographic protocol of elevated security level for the data object, the data terminal must authenticate itself to the electronic device in a Challenge-Response procedure based on in a symmetrical cryptographic algorithm such as the 3DES or AES encryption algorithm. To this end, the electronic device sends a request (the challenge) to the data terminal in step 200, which must correctly answer the request and send the response back o the electronic device. In step 204 the electronic

device receives the response of the data terminal and makes sure of its accuracy. And vice versa, in step 206 the electronic device can receive a request from the data terminal, which it answers in step 208 to authenticate itself vis-à-vis the data terminal. This respective one-sided authentication can also take place in one step in the form of a mutual authentication.

When specifying the cryptographic protocol of a higher security level for the data object, the data terminal must authenticate itself to the electronic device in a Challenge-Response procedure based on an asymmetrical cryptographic algorithm such as the RSA or elliptical curve cryptosystem. To this end the electronic device receives the public key of the data terminal in step 210. This can be provided with a digital signature, which the electronic device verifies in step 300. The verification can also be based on a certificate chain, at the end of which must be a topmost certification authority, whose public key is available in the electronic device. If the electronic device is integrated into an identity document, the topmost certification authority can be the issuing national authority or an international organization. In step 212 the electronic device sends a request to the data terminal which is based on the public key received, and through the answering of which the data terminal must prove that it is also in possession of the associated private key. In step 214 the electronic device receives the response from the data terminal and is therefore assured of its accuracy.

In step 302 with the aid of the allocation table, the electronic device can specify an encryption protocol according to which the data terminal and the electronic device communicate in encrypted form. Possible arrangements which are presented as examples include both the encryption of the communication with a session key, which is exchanged in step 304, and a free, unencrypted communication which circumvents step 304. Thus the Diffie-Hellman key exchange or a similar procedure is used in step 304, which allows the electronic device and the data terminal to derive a session key of high-level magnitude in a safe manner.

Figure 4 shows a flow chart of the procedural steps implemented by a preferred embodiment of the data terminal according to the invention. After the data terminal has requested a data object from the electronic device in step 216, it follows the cryptographic protocol at branch 218, upon whose mandatory implementation the

electronic device links read access to the data object. Similar to Figure 3, three possible arrangements show examples of linking to a cryptographic protocol of elevated security level beginning with step 200, linking to a cryptographic protocol of higher security level beginning with step 210, and free access without linking to a cryptographic protocol.

When specifying the cryptographic protocol of elevated security level for the data object, the data terminal must authenticate itself to the electronic device in a Challenge-Response procedure based on a symmetrical cryptographic algorithm such as the 3DES or AES encryption algorithm. In step 200 the data terminal receives a request from the electronic device. The device-specific key, which the data terminal must derive from the machine-readable printed data of the electronic device to respond to the request in step 202, can be used for the symmetrical cryptographic algorithm. The data terminal thereby proves that it was visibly presented with a passport, for example, in which the electronic device is integrated. A general key may also be needed to derive the device-specific key from the machine-readable printed data. In step 204 the data terminal sends the response to the electronic device. Inversely, in step 206, a data terminal can send a request to the electronic device and receive the response in step 208.

When specifying the cryptographic protocol of a higher security level for the data object, the data terminal must authenticate itself to the electronic device in a Challenge-Response procedure based on an asymmetrical cryptographic algorithm such as the RSA or elliptical curve cryptosystem. To this end, the data terminal sends its public key to the electronic device in step 210. In step 212 the data terminal receives a request from the electronic device which is based on the transmitted public key and through the answering of which the data terminal, in step 214, proves that it is also in possession of the associated private key.

For example, let's assume the electronic device generates a random number. This is encrypted with the public key of the data terminal and the resulting cipher is transmitted to the data terminal by the electronic device. The data terminal decodes the cipher with its secret key and sends the result of the decoding [decryption] back to the electronic device. The electronic device then compares the originally generated random number

with the result of decoding received from the data terminal. If both agree, the data terminal is classified as authentic and authorized.

The electronic device may additionally link the transmission of the data object to the mandatory execution of the steps of the cryptographic protocol of a higher security level with the steps of the protocol of the elevated security level.

In step 302 the electronic device can specify, with the aid of the allocation table, an encryption protocol according to which the data terminal and electronic device can communicate in encrypted manner. Presented by way of example as possible arrangements are the encrypting of the communication with a session key, which is exchanged in step 304, and a free, unencrypted communication whereby step 304 is circumvented.

Reference Number List

100	Data terminal
102	Electronic device
104	Data objects
106	Allocation table
108	Cryptographic protocol
109	Encryption protocol
110	Software application
112	Operating system
114	Identity document
116	Machine-readable printed data
118	Public key
120	Private key
122	Digital signature
124, 124'	Computer-executable instructions
126	Memory [storage]
128, 128'	Receiver
130, 130'	Transmitter
140	Administrator function
142, 142'	Contactless interface
146, 146'	General key

Patent Claims

---

1. Method for a data terminal (100) to access one of a number of data objects (104), stored in an electronic device (102) whereby the electronic device features an allocation table (106), in which a cryptographic protocol (108) of a different security level is assigned to different data objects, with the following steps:
   - Transmission (216) of a request by the data terminal to the electronic device for a particular one of the data objects,
   - Specification (218) of a cryptographic protocol by the electronic device for the one data object with the aid of the allocation table,
   - Implementation (222) of the cryptographic protocol by the electronic device and the data terminal, and
   - Transmission (220) of the one data object by the electronic device.
2. Method of Claim 1, whereby electronic device (102) features a software application (110), whereby the software application contains allocation table (106), whereby cryptographic protocol (108) is specified by the software application, whereby the cryptographic protocol is implemented by the data terminal and the software application, and one of the data objects is transmitted by the software application.
3. Method of Claim 2, whereby electronic device (102) features an operating system (112), which prevents any unauthorized alteration or removal of software application (110) and only allows access to data objects (104) by means of the software application.
4. Method of Claim 3, whereby operating system (112), following authentication as an administrator of electronic device (102), allows an alteration or removal of the software application.
5. Method of one of the preceding claims, whereby electronic device (102) is integrated in an identity document (114).
6. Method of one of the preceding claims, whereby at least one of data objects (104) is comprised of personal biometric data.
7. Method of one of the preceding claims, whereby data terminal (100) and electronic device (102) communicate without contact.

8. Method of Claim 7, whereby in allocation table (106) an encryption protocol (109) of a different security level is also assigned to different data objects (104), according to which the data terminal and the electronic device communicate in encrypted manner.

9. Method of one of the preceding claims, whereby at least one of the number of data objects (104) in the allocation table is assigned free access without cryptographic protocol (108).

10. Method of Claim 9, whereby electronic device (102) features machine-readable printed data (116), whereby in allocation table (106) at least one of a number of data objects (104) is assigned a cryptographic protocol (108) of elevated security level, which comprises the following steps:

- Placement (200) of a request to data terminal (100) based on a symmetrical cryptographic algorithm, whereby a device-specific key (144) is used, which can be derived from the machine-readable printed data, by the electronic device,
- Derivation (202) of the device-specific key from the machine-readable printed data by the data terminal,
- Responding (204) to the request by the data terminal, to authenticate itself to the electronic device.

11. Method of Claim 10, whereby to derive device-specific key (144) from machine-readable printed data (116), a general key (146) is required, which is known to electronic device (102) and data terminal (100).

12. Method of Claim 10 or 11, whereby cryptographic protocol (108) of elevated security level also comprises the following steps:

- Placement (206) of a request by data terminal (100) to electronic device (102) based on a symmetrical cryptographic algorithm, whereby the device-specific key is used,
- Responding (208) to the request by the electronic device, to authenticate itself to the data terminal.

13. Method according to Claims 9 through 12, whereby data terminal (100) features a public key (118) and a private key (120), whereby in allocation table (106) at least one of a number of data objects is assigned a

cryptographic protocol (108) of a higher security level, which comprises the following steps:

- Transmission (210) of the public key to electronic device (102) by the data terminal,
- Placement (212) of a request to the data terminal by the electronic device using the public key, for which the private key is needed to make a reply, by the electronic device
- Responding (214) to the request for authentication with respect to the electronic device by the data terminal.

14. Method of Claim 13, whereby public key (118) is characterized by a digital signature (122) and the electronic device verifies (300) the digital signature.

15. Computer program product, in particular a digital storage medium, with an allocation table (106), in which different data objects (104) are assigned a cryptographic protocol (108) of a different security level and computer-executable instructions for

- Receiving a request for one of a number of data objects (104) from a data terminal (100),
- Specifying a cryptographic protocol for the one particular data object with the aid of the allocation table,
- Implementing the cryptographic protocol with the data terminal,
- Sending the one particular data object to the data terminal.

16. Computer program product of Claim 15, whereby allocation table (106) and computer-executable instructions (124) can be installed into an electronic device with an operating system in such a way that the operating system prevents any unauthorized alteration or removal of the allocation table or the computer-executable instructions.

17. Computer program product of Claim 16, which also comprises computer-executable instructions (124) and where access to data objects (104) is only possible via the computer-executable instructions.

18. Electronic device (102) with

- A memory (126) for a number of data objects (104),
- A receiver (128) for receiving a request for one of the data objects from a data terminal (100),

- An allocation table (106), in which different data objects are assigned a cryptographic protocol (108) of a different security level,
- Program instructions (124) for specifying a cryptographic protocol for the one particular data object with the aid of the allocation table.
- Program instructions (124) for implementing the cryptographic protocol with the data terminal,
- A transmitter (130) for sending the one particular data object to the data terminal.

19. Electronic device (102) of Claim 18, which features a software application (110), whereby the software application contains allocation table (106), whereby cryptographic protocol (108) can be selected by the software application, whereby the cryptographic protocol can be executed by data terminal (100) and the software application, and the one particular data object (104) can be transmitted by the software application.

20. Electronic device (102) of Claim 19, which features an operating system (112), whereby the operating system is designed to prevent unauthorized alteration or removal of software application (110) and to prevent access to data objects (104) by circumventing the software application.

21. Electronic device (102) of Claim 20, whereby operating system (112) features an administrator function (140) for authenticating as administrator, whereby after authenticating the electronic device as administrator, alteration or removal of software application (110) is possible.

22. Electronic device (102) according to one of Claims 18 to 21, whereby the electronic device is integrated into an identity document (114).

23. Electronic device (102) according to one of Claims 18 to 22, whereby at least one of data objects (104) comprises personal biometric data.

24. Electronic device (102) according to one of Claims 18 to 23, which features an interface (142) for contactless communication with data terminal (100).

25. Electronic device (102) of Claim 24, whereby an encryption protocol (109) of a different security level is also assigned to different data objects in allocation table (106), according to which data terminal (100) and the electronic device can communicate in encrypted manner.

26. Electronic device (102) according to one of Claims 18 to 25, whereby in allocation table (106) at least one of a number of data objects (104) is assigned free access without cryptographic protocol (108).

27. Electronic device (102) of Claim 26, whereby the electronic device features machine-readable printed data (116), whereby in allocation table (106) at least one of a number of data objects is assigned a cryptographic protocol (108) of elevated security level, which comprises the following steps:

- Placement (200) of a request to data terminal (100) based on a symmetrical cryptographic algorithm, whereby a device-specific key (144) is used, which can be derived from the machine-readable printed data, by the electronic device,
- Derivation (202) of the device-specific key from the machine-readable printed data by the data terminal,
- Responding (204) to the request, in order to authenticate itself to the electronic device, by the data terminal.

28. Electronic device (102) of Claim 27, whereby a general key (146) which is known to the electronic device and data terminal (100) is required to derive the device-specific key from machine-readable printed data (116).

29. Electronic device (102) of Claim 27 or 28, whereby cryptographic protocol (108) of elevated security level also comprises the following steps:

- Placement (206) of a request by data terminal (100) to the electronic device based on a symmetrical cryptographic algorithm, whereby device-specific key (144) is used.
- Responding (208) to the request by the electronic device in order to authenticate itself to data terminal (100).

30. Electronic device (102) according to one of Claims 26 to 29, whereby data terminal (100) features a public key (118) and a private key (118), whereby in allocation table (106) at least one of a number of data objects (104) is assigned a cryptographic protocol (108) of higher security level, which comprises the following steps:

- Transmission (210) of the public key to the electronic device by the data terminal,

- Placement (212) of a request to the data terminal by the electronic device using the public key, for which the private key is required to answer, by the electronic device
- Responding (214) to the request for authentication with respect to the electronic device by the data terminal.

31. Electronic device (102) of Claim 30, whereby public key (118) is characterized by a digital signature (122) and electronic device (102) verifies the digital signature.

32. Data terminal (100) with

- A transmitter (130) for transmitting a request for a data object (104) to an electronic device in which a number of data objects (104) are stored,
- A receiver (104) for receiving a specification of a cryptographic protocol for the requested data object from the electronic device,
- Program instructions (124) for implementing the cryptographic protocol, and
- A receiver (128) for receiving the data object.

33. Data terminal (100) of Claim 32, which features an interface (142') for contactless communication with electronic device (102).

34. Data terminal (100) of Claim 33, whereby receiver (128) is also designed to receive a specification of an encryption protocol (109), and the data terminal features a means for communication with electronic device (102) according to the encryption protocol.

35. Data terminal (100) according to one of Claims 32 to 34, whereby electronic device (102) features machine-readable printed data (116), whereby receiver (128) receives the specification of a cryptographic protocol (108) of elevated security level, which comprises the following steps:

- Placement (200) of a request to data terminal (100) based on a symmetrical cryptographic algorithm, whereby a device-specific key (144) is used, which can be derived from the machine-readable printed data, by the electronic device,
- Derivation (202) of the first cryptographic key from the machine-readable printed data by the data terminal,

- Responding (204) to the request by the data terminal in order to authenticate itself to electronic device.

36. Data terminal (100) of Claim 35, whereby a second cryptographic key, which is known to electronic device (102) and the data terminal, is required to derive device-specific key (144) from machine-readable printed data (116).

37. Data terminal (100) of Claim 35 or 36, whereby cryptographic protocol (108) of elevated security level also comprises the following steps:

- Placement (206) of a request to electronic device (102) by the data terminal based on a symmetrical cryptographic algorithm, whereby the device-specific key is used,
- Responding (208) to the request by the electronic device in order to authenticate itself to the data terminal.

38. Data terminal (100) according to one of Claims 32 to 37, whereby the data terminal features a public key (118) and a private key (120), whereby receiver (128) can receive the specification of a cryptographic protocol (108) of higher security level, which comprises the following steps:

- Transmission of the public key to electronic device (102) by the data terminal,
- Placement of a request to the data terminal by the electronic device using the public key, for which the private key is needed to reply, by the electronic device,
- Responding to the request for authentication with respect to the electronic device by the data terminal.

39. Data terminal (100) of Claim 38, whereby public key (118) is characterized by a digital signature (122) and electronic device (102) verifies the digital signature.