

Claims

1. A method for addressing, authentication and secure data storage in computer systems comprising at least one first, at least one second and/or at least one third computer system (1, 1a, 1a1, 1a2, 1b) each having at least one network interface (11) and at least one telephony interface (12) and at least one storage space (2) for administrative information, in particular for at least one authorized call number and/or at least one subscriber PIN in such a way that the computer systems (1) are programmed with a program reproducing a control logic for controlling the interaction of the aforementioned interfaces, wherein the method comprises the following steps:
 - a) transmitting the connection information for the network interface (11) of at least one first computer system (1, 1a, 1a1, 1a2) via the telephony interface (12) to at least one second and/or third computer system (1, 1a, 1a1, 1a2, 1b);
 - b) automatically checking a call number of the first computer system (1, 1a, 1a1) with the call numbers stored in the storage space (2) in the second computer system (1b) and, if the outcome of the check is positive, automatically transmitting the connection information for the network interface (11) of the second and/or third computer system (1, 1a1, 1a2, 1b) via the telephony interface (12) to the first computer system (1, 1a, 1a1) and activating the network interface (11) of the second and/or third computer system (1, 1a1, 1a2, 1b), in order to accept connections (104) on the basis of the connection information of the first computer system (1, 1a, 1a1);
 - c) checking the call number of the second and/or third computer system (1, 1a1, 1a2, 1b) with the call numbers stored in the storage space (2) in the first computer system (1, 1a1, 1a) and, if the outcome of the check is positive, activating the network interface (11) of the first computer system (1, 1a1, 1a), in order to establish a connection (101, 102, 103, 104) on the basis of the connection information of the second and/or third computer system (1, 1a1, 1a2, 1b);
 - d) only allowing connections (104) with the connection information of the first computer system (1a) by the network interface (11) of the second computer system (1, 1a1, 1a2, 1b), and

e) only allowing connections (104) with the connection information of the second computer system (1, 1a1, 1a2, 1b) by the network interface (11) of the first computer system (1a), and wherein

f) the network interfaces (11) of the first and second computer system (1a, 1b) only allow connection attempts, in particular for between 1 and 10, preferably between 2 and 7, in particular preferably between 3 and 5 seconds, with the respective connection information, and after the connection is established or after the predetermined time period has elapsed without a connection being established these network interfaces are not recognizable or reachable for other computer systems.

2. The method according to claim 1, characterized in that at least in each case the first and the second computer system (1, 1a1, 1a2) are already connected to the at least one third computer system (1b), and the first and second computer system (1a1, 1a2) in each case by means of the control logic (10) in the one third computer system (1b) establish a direct connection (203) via the network interface (11), and the method comprises the following further steps:

g) transmitting to the second computer system (1a2) the connection information for the telephony interface (12) and network interface (11) of the first computer system (1a1) with a system message (201) via the existing connection (200) to the third computer system (1b);

h) checking a call number of the first computer system (1a1) with call numbers stored in the storage space (2) of the second computer system (1a2) and, if the outcome of the check is positive, transmitting to the first computer system (1a1) the connection information (202) for the telephony interface (12) and network interface (11) of the second computer system (1a2) via the existing connection (200) to the third computer system (1b), and activating the network interface (11) of the second computer system (1a2), in order to accept connections (203) on the basis of the connection information of the first computer system (1a1); and

i) checking the call number of the second computer system (1a2) with the call numbers stored in the storage space (2) in the first computer system (1a1) and, if the outcome of the check is positive, activating the network interface (11) of the first

computer system (1a1), in order to establish connections (203) on the basis of the connection information of the second computer system (1a2); wherein

- j) the network interface (11) of the second computer system (1a2) only allows connections (203) with the connection information of the first computer system (1a1);
- k) the network interface (11) of the first computer system (1a1) only allows connections (203) with the connection information of the second computer system (1a2), and
- l) the network interfaces (11) of the first and second computer system (1a1, 1a2) only allow connection attempts, in particular between 1 and 15, preferably between 2 and 12, in particular preferably between 3 and 10 connection attempts with the respective connection information for a short predetermined time period, in particular for between 1 and 10, preferably between 2 and 7, in particular preferably between 3 and 5 seconds, and after the connection is established or after the predetermined time period has elapsed without a connection being established these network interfaces are not recognizable or reachable for other computer systems.

3. The method according to one of claims 1 or 2, characterized in that in step b) and/or h) the network interface (11) of the second computer system (1b, 1a2) is activated in order to establish connections on the basis of the connection information of the first computer system (1a, 1a1), and that in step c) and/or i) the network interface (11) of the first computer system (1a, 1a1) is activated in order to accept connections (103) on the basis of the connection information of the second computer system (1b, 1a2).

4. The method according to one of the preceding claims, characterized in that after a connection is established the second computer system (1b, 1a2) requests an identification of the first computer system (1a, 1a1), compares it with the identification tag stored in the storage space (2) of the second computer system (1b, 1a2), and if the outcome of the check is positive the connection remains activated and if the outcome of the check is negative the connection is closed and in particular an alarm notification is output.

5. The method according to claim 4, characterized in that after a predetermined number, in particular after between 1 and 15, preferably between 2 and 12, in particular preferably between 3 and 10 negative identification attempts, the call number of the first computer system (1a, 1a1) in the storage space (2) of the second computer system (1b, 1a2) is marked as blocked by the control logic and no more connection information is accepted for the first computer system (1a, 1a1) with this call number.

6. The method according to claim 4, characterized in that the identification tag is a text, a biometric tag, an electronic key or a mechanical key, of which the key information is read by a reading device on the first, second and/or third computer system (1a, 1a1, 1b).

7. The method according to one of the according to one of the preceding claims, characterized in that the first computer system (1a, 1a1) supplies a security token with the connection information to the second and/or third computer system (1b, 1a2), and this security token is transmitted when the connection is established via the network interface (11) and is checked by the control logic (10) in the first computer system (1a, 1a1), and if the outcome of the check is positive the connection remains activated and if the outcome of the check is negative the connection is closed and in particular an alarm notification is output.

8. The method according to claim 7, characterized in that after a predetermined number, in particular after between 1 and 15, preferably between 2 and 12, in particular preferably between 3 and 10 negative connection attempts, the call number of the second computer system (1b, 1a1) in the storage space (2) of the first computer system (1a, 1a2) is marked as blocked by the control logic (10) and no more connection attempts are accepted for the second computer system (1b, 1a2) with this call number.

9. The method according to claim 2, characterized in that at least the first and the second computer systems (1a1, 1a2), which in each case are already connected to a common third computer system (1b) and have established a direct connection (203), are only authenticated reciprocally via the common third computer system (1b), and the method comprises the following further steps:

- m) the first computer system (1a1) requests a security token from the third computer system (1b) via the connection (200) and sends this on to the second computer system (1a2) via the direct connection (203);
- n) the second computer system (1a2) passes on the security token to the third computer system (1b) via the connection (200);
- o) the third computer system (1b) compares the two security tokens and in each case sends a system message with the result of the comparison to the first and/or the second computer systems (1a1, 1a2), and
- p) the control logic (10) of the first and/or the second computer system (1a1, 1a2) checks the system message with the result of the comparison and when the outcome of the check is positive it leaves the connection (203) open and when the outcome of the check is negative it closes the direct connection (203) and outputs an alarm message.

10. The method according to claim 2 or claim 9, characterized in that a first and a second computer system with the addition of a third computer system (1b) carry out a payment process, and the method comprises the following further steps:

- q) the control logic (10) in the first computer system (1, 1a1), in particular the computer system of a vendor, generates a security token, and the second computer system (1a2), in particular the computer system of a purchaser, obtains the security token together with the payment information from the first computer system (1, 1a1), in particular the purchaser's computer system, via the direct connection (203);
- r) the first computer system (1, 1a1), in particular the vendor's computer system, passes on the payment information via the connection (200) together with the security token to the third computer system (1b), in particular the computer system (1b) of a payment service (1b);
- s) the second computer system (1a2), in particular the purchaser's computer system, passes on the payment information via the connection (200) together with the security token to the third computer system (1b), in particular the computer

system (1b) of the payment service;

t) the second computer system (1a2), in particular the purchaser's computer system, authorizes the payment process via the connection (200) in the third computer system (1b), in particular the computer system (1b) of the payment service, with a PIN, and

u) a control logic (10) in the third computer system (1b), in particular the computer system (1b) of the payment service, compares the security token from the first computer system (1, 1a1), in particular the vendor's computer system, and the second computer system (1a2), in particular the purchaser's computer system, and validates the PIN of the second computer system (1a2), in particular the purchaser's computer system (1a2), and concludes the payment process and sends back a positive system message to the first computer system (1a2), in particular the vendor's computer system, and to the second computer system (1a2), in particular the purchaser's computer system, when the outcome of the check is positive, and sends back a negative system message to the first computer system (1a2), in particular the vendor's computer system, and the second computer system (1a2), in particular the purchaser's computer system, when the outcome of the check is negative.

11. The method according to claim 10, characterized in that for the payment process between the first computer system (1a2), in particular the vendor's computer system, and the second computer system (1a2), in particular the purchaser's computer system, preferably in a shop the connection (203) is established via NFC, Bluetooth, wireless LAN or wired LAN.

12. The method according to claim 10 or 11, characterized in that for the payment process between the first computer system (1a2), in particular the vendor's computer system, and the second computer system (1a2), in particular the purchaser's computer system, preferably in a shop or an online shop, the payment information is not transmitted via a direct connection (203) but via an optical signal (for example Q/R code, barcode, character strings or the like), an acoustic signal (for example modem tones, speech, or the like) or by manual input, in particular bidirectionally, in particular wherein in this case, for an online purchase, a second device which forms or provides the second computer system (1a2) is used, in particular a smartphone for

receiving and transmitting the payment information from a first device which forms or provides the first computer system (1a1), in particular a PC or notebook, wherein the first device is preferably provided as a terminal of the first computer system (1a2), in particular the vendor's computer system.

13. The method according to one of the preceding claims, characterized in that the control logic (10) can transmit the data for the payment process between the first computer system (1a2), in particular the vendor's computer system, and the third computer system (1b), in particular the computer system of the payment service, or the second computer system (1a1), in particular the purchaser's computer system, and the third computer system (1b), in particular the computer system of the payment service, via other network connections, in particular different network connections from those defined in claims 1 or 2.

14. The method according to one of the preceding claims, characterized in that a text, a biometric tag, an electronic key or a mechanical key, of which the key information is read for example by a reading device in the computer systems (1a, 1b, 1a1, 1a2), are used for the encryption, identification by PIN, security token and authorization.

15. The method according to one of the preceding claims, characterized in that for small quantities of data, in particular for a payment process, the control logic (10) transmits at least a part of the data captured in the preceding steps via the telephony interface (12).

16. The method according to one of the preceding claims, characterized in that upon activation of a predetermined signal the control logic (10) passes on data, in particular email, SMS and fax to computer systems 1 without the aid of other internet services such as in particular DNS and DynDNS.

17. The method according to one of the preceding claims, characterized in that the control logic (10) carries out an automatic check as to whether the displayed call number corresponds to the actual subscriber connection.

18. The method according to one of the preceding claims, characterized in that

connection requests from the first computer systems (1a, 1a1) are distributed by the control logic (10) in a second and/or third computer system (1b, 1a2) to different second and/or third computer systems (1b, 1a2) according to a predetermined criterion, in particular to a number of connections and/or a utilization and/or an availability of the second and/or third computer systems (1b, 1a2) and/or a call number and/or a geographical location.

19. The method according to one of the preceding claims, characterized in that a first computer system (1a, 1a1) in a server role in the network processes connection requests or requests for name resolution (for example DNS requests or the like) from computer systems in the network through the control logic (10), and the control logic (10) of the first computer system (1a, 1a1) carries out the exchange of the connection information with a second and/or third computer system (1b, 1a2) as defined in the preceding claims and then produces the connection or sends back the connection parameters (for example IP address, port number, or the like) to the requesting computer systems.

20. The method according to one of the preceding claims, characterized in that the control logic (10) of at least one computer system (1) also passes on the determined connection parameters, as defined in the preceding claims, to at least one further computer system, in particular a server system such as for example a firewall, and this then allows the connections of the first computer system (1) or the further computer systems from the network with these connection parameters.

21. The method according to one of the preceding claims, characterized in that the control logic (10) of the second and/or third computer system (1b, 1a2) automatically passes on or makes available information and control data to the first computer system (1a, 1a1) as a function of the connection information.

22. The method according to one of the preceding claims, characterized in that the call number of the second and/or third computer system (1b) is used for another or an existing telephony service, in particular a fax service and/or an answering machine, and the control logic (10) of at least the second and/or third computer system (1b) compares the call number of at least the first computer system (1a) with the call numbers stored in the storage space (2) of the second and/or third computer

system (1b) and in the event of conformity it does not activate the telephony service, but transmits the connection data for the second and/or third computer system (1b) to the first computer system (1a).

23. The method according to one of the preceding claims, characterized in that for computer systems (1, 1a, 1a1, 1a2, 1b) which lie geographically close together the connection information for the network interface (11) can then be transmitted alternatively, in particular bidirectionally, by means of signals, preferably replacing the telephony interface (12), (for example Q/R code, barcode, character strings or the like), acoustic signals (for example modem tones, speech, or the like), by manual inputs and/or by secure connections previously produced in another way (for example NFC, Bluetooth, WLAN, USB, or the like) between the computer systems (1, 1a, 1a1, 1a2, 1b).

24. Use of the method according to one of the preceding claims with protocols of other connection-orientated interfaces, in particular with NFC, Bluetooth and WLAN protocols.