US 20160344727A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2016/0344727 A1**

Brockhaus et al. (43) **Pub. Date: Nov. 24, 2016**

(54) **CHARACTERIZING A CLIENT APPARATUS ON AT LEAST ONE SERVER APPARATUS**

(71) Applicant: **SIEMENS AKTIENGESELLSCHAFT**, München (DE)

(72) Inventors: **Hendrik Brockhaus**, Unterbiberg (DE); **Jens-Uwe Bußer**, Neubiberg (DE); **Steffen Fries**, Baldham (DE); **David von Oheimb**, Heimstetten (DE)

(21) Appl. No.: **15/034,570**

(22) PCT Filed: **Oct. 2, 2014**

(86) PCT No.: **PCT/EP2014/071132**

§ 371 (c)(1),
(2) Date: **May 5, 2016**

(30) **Foreign Application Priority Data**

Nov. 6, 2013 (DE) 10 2013 222 503.2

Publication Classification

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)

(52) **U.S. Cl.**
CPC ***H04L 63/0823*** (2013.01); ***H04L 9/3263*** (2013.01); *H04L 63/10* (2013.01)

(57) **ABSTRACT**

Systems and methods for characterizing a client apparatus on at least one server apparatus are provided. A first certificate is received in the event of a first request for a connection set-up from a server apparatus in a client apparatus. One or more predefined certificate parameters of the first certificate are stored as a set of characterization parameters in the client apparatus. Each further certificate from a server apparatus is checked that is received in the client apparatus in the event of a request for a further connection set-up, against the stored characterization parameter set. A request for a further connection set-up is accepted only if all of the predefined certificate parameters of the further certificate match all characterization parameters of the characterization parameter set.

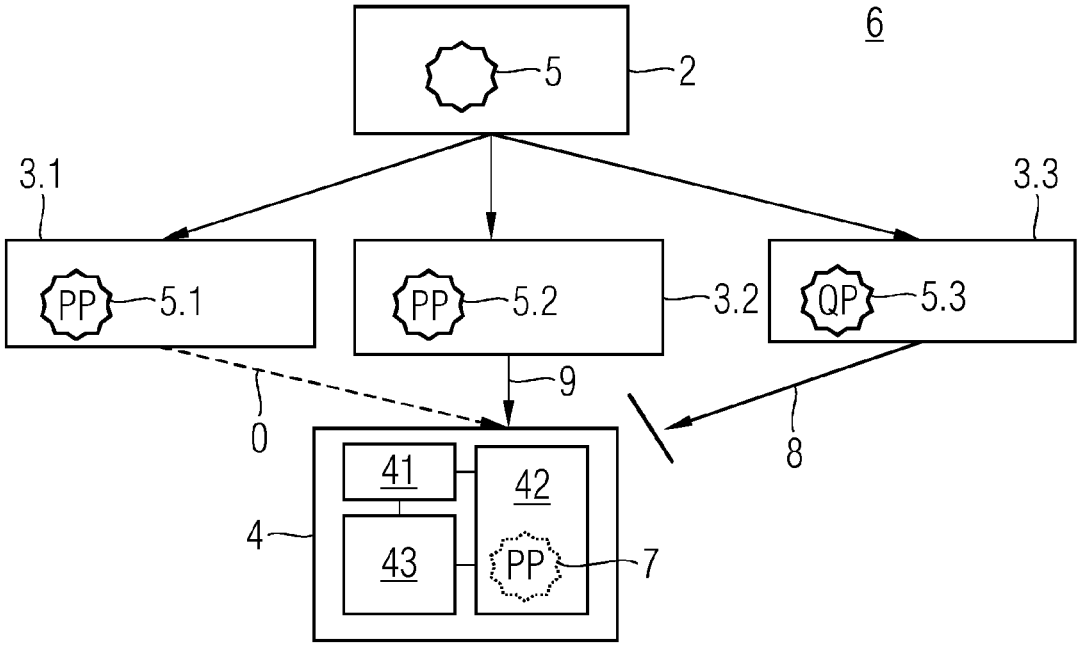


FIG 1

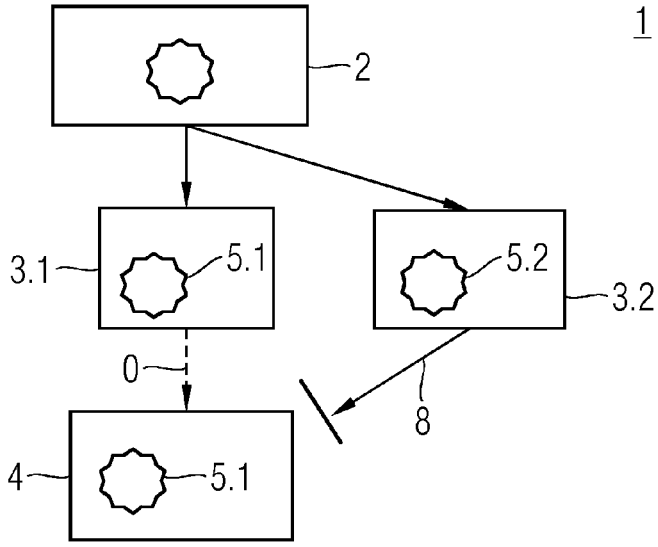


FIG 2

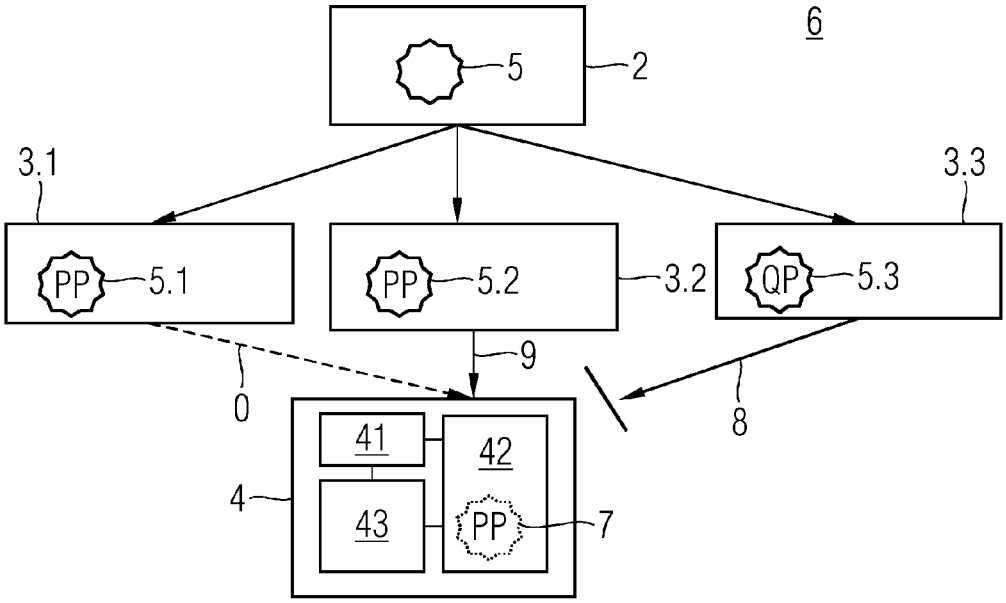


FIG 3

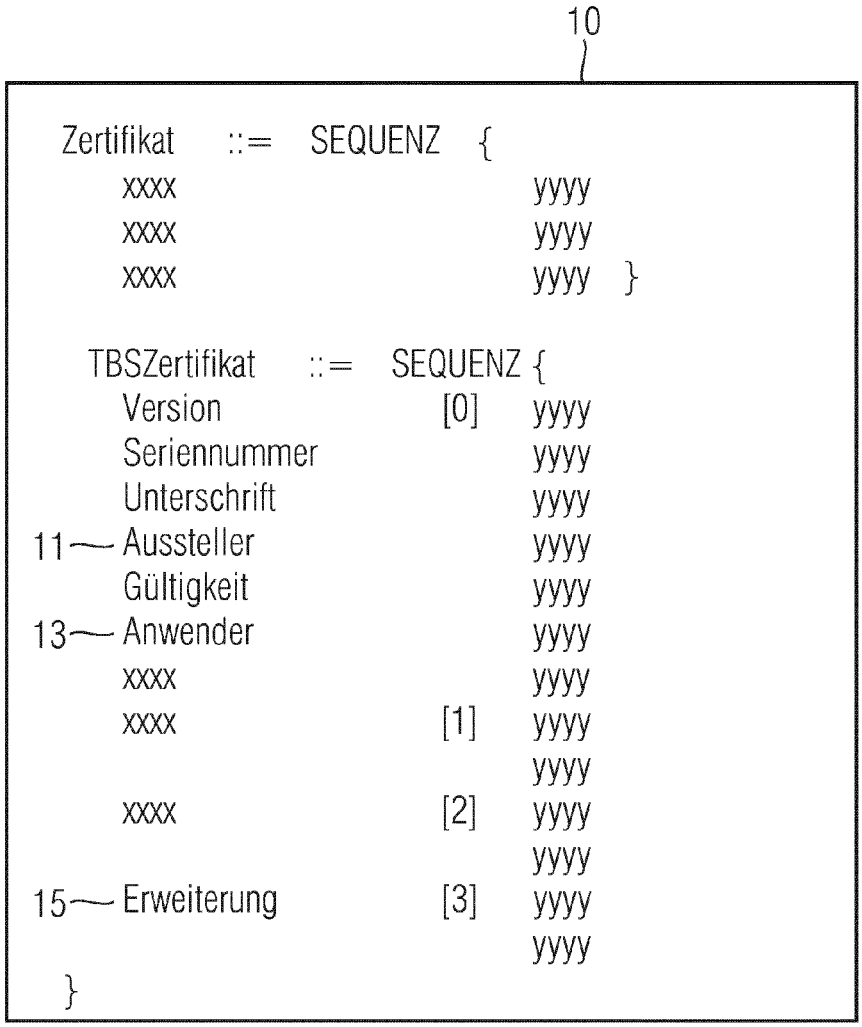

10
Zertifikat ::= SEQUENZ {
xxxx yyyy
xxxx yyyy
xxxx yyyy }
TBSZertifikat ::= SEQUENZ {
Version [0] yyyy
Seriennummer yyyy
Unterschrift yyyy
11 Aussteller yyyy
Gültigkeit yyyy
13 Anwender yyyy
xxxx yyyy
xxxx [1] yyyy
yyyy
xxxx [2] yyyy
yyyy
15 Erweiterung [3] yyyy
yyyy
}

FIG 4

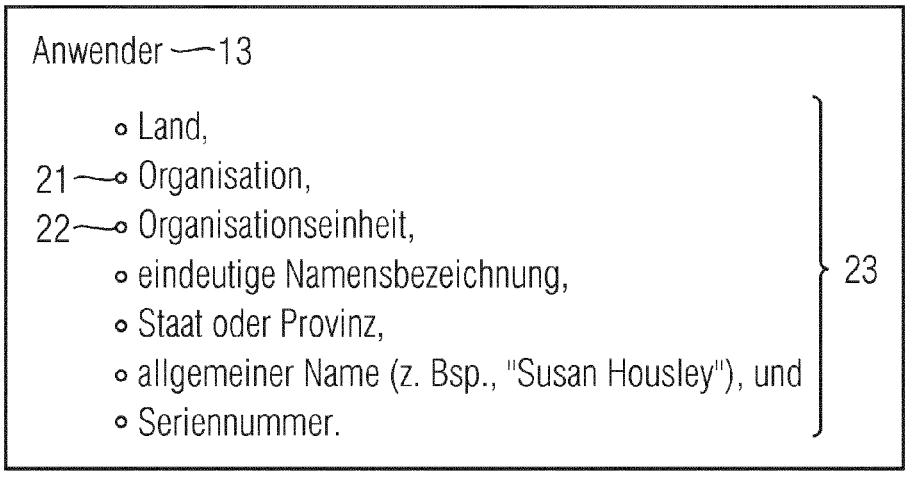

Anwender 13
Land,
21 Organisation,
22 Organisationseinheit,
eindeutige Namensbezeichnung,
Staat oder Provinz,
allgemeiner Name (z. Bsp., "Susan Housley"), und
Seriennummer.
23

FIG 5

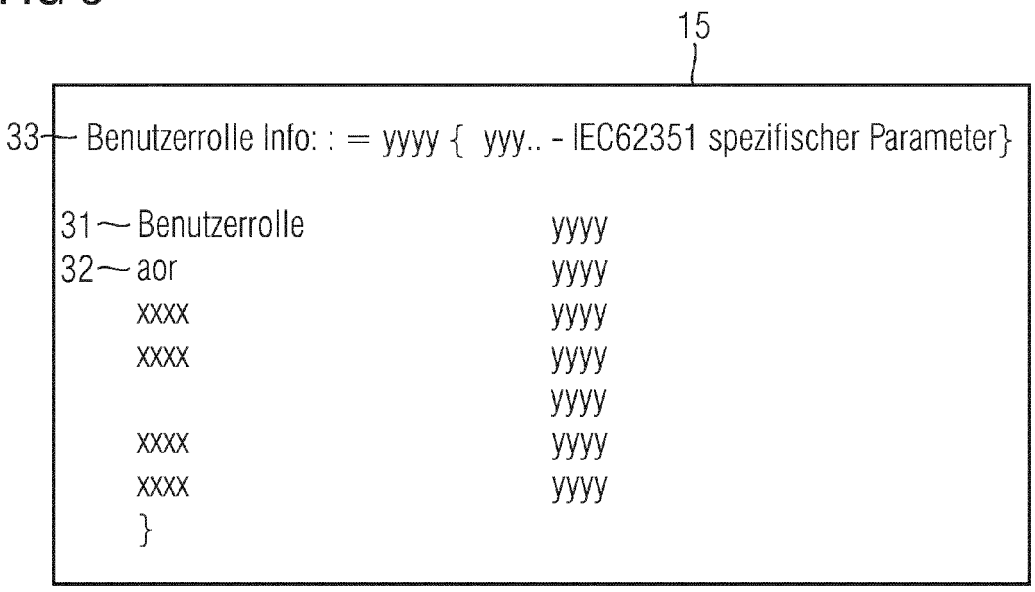
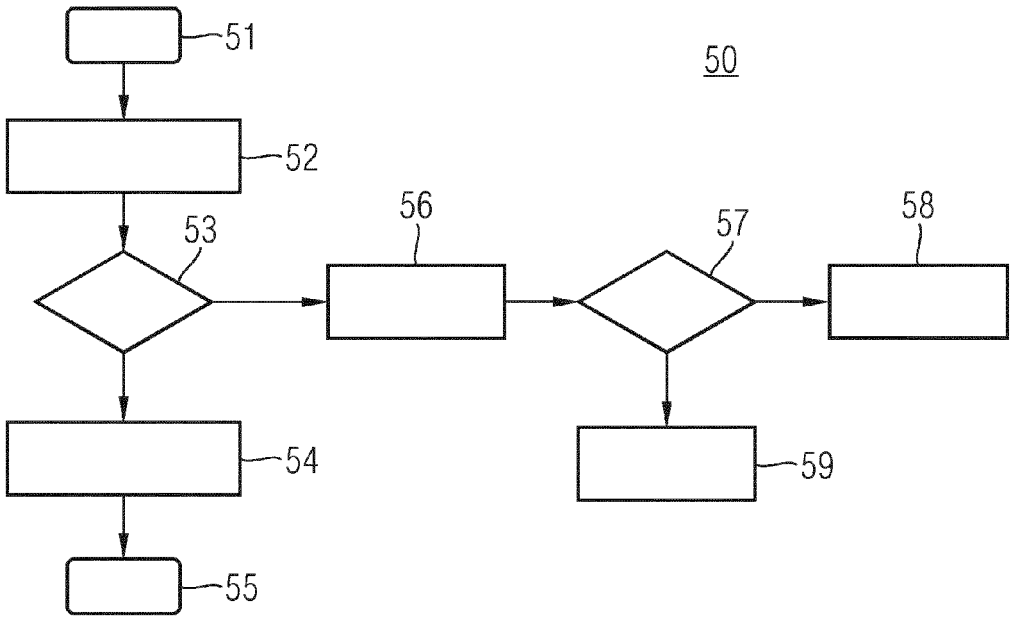

15
33
Benutzerrolle Info: : = yyyy { yyy.. - IEC62351 spezifischer Parameter}
31
Benutzerrolle
yyyy
32
aor
yyyy
xxxx
yyyy
xxxx
yyyy
yyyy
xxxx
yyyy
xxxx
yyyy
}

FIG 6


51
50
52
53
56
57
58
54
59
55

CHARACTERIZING A CLIENT APPARATUS ON AT LEAST ONE SERVER APPARATUS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present patent document is a §371 nationalization of PCT Application Serial Number PCT/EP2014/071132, filed Oct. 2, 2014, designating the United States, which is hereby incorporated by reference, and this patent document also claims the benefit of DE 10 2013 222503.2, filed on Nov. 6, 2013, which is also hereby incorporated by reference.

TECHNICAL FIELD

[0002] Embodiments relate to a client apparatus and a method for characterizing a client apparatus on at least one server apparatus using a first certificate.

BACKGROUND

[0003] For a secure first start-up of devices, it is often necessary to generate or set up key material for the security functions of the device. It is similarly necessary to establish specific security associations. One example is the characterization of one client apparatus on a specific other server apparatus with which a connection may successfully be set up. In the case of a secure connection, the characterization may be based on a certificate of the remote station. The aim of the characterization is to restrict the communication partners from the perspective of the client apparatus to one server apparatus or one specific group of server apparatuses. Client apparatuses may be for example a field device, an intelligent meter such as a smart meter or a smart metering gateway, an automation station or a client apparatus of a time synchronization protocol (NTP). Corresponding server apparatuses are for example, a substation control unit, a data concentrator, a power transformer operating system server or an NTP server.

[0004] A known characterization method, for example of an RFID tag on an RFID reader, is carried out by moving the RFID tag toward the RFID reader, so that the RFID tag is recognized via near field communication (NFC) by the RFID reader and vice versa. Both the tag and the reader then store the communication partner and verify the communication partner during the next connection set-up. In a further known characterization method, for example in the setting up of a virtual LAN, a fixed address or a fixed identifier of the server apparatus with which a communication is permitted is specified administratively to a client apparatus. In a third known example of a characterization method, in the case of a communication via an encrypted network connection that is set up using a Secure Shell Protocol SSH, a fingerprint of the certificate of the first connection is stored in the client apparatus. The fingerprint of a certificate is, for example, a checksum that is formed over the entire certificate. In the event of further connection set-up requests, a check is carried out via a comparison of the fingerprint of the received further certificate with the stored fingerprint of the first certificate to determine whether the same certificate is involved.

[0005] If the validity of the certificate expires or if the secret key of a server apparatus is compromised, the certificate is then replaced. Certificates may be updated or renewed, for example, by an operating system update. On the other hand, root certificates, for example, are exchanged, for example via a Trust Anchor Management Protocol (TAMP) or via a local device management. All settings and stored data may also be deleted and therefore stored certificates may also be deleted and therefore the characterization may be cancelled, for example by a manual pressing of a button on the client apparatus.

[0006] It may similarly occur that a server apparatus suddenly fails and is replaced by a different server apparatus. Similarly, a changeover of a client apparatus between two domains of an operator may be required, for example to connect a conspicuous client apparatus from a server apparatus in a live system to a server apparatus in a test system for maintenance.

SUMMARY AND DESCRIPTION

[0007] The scope of the present invention is defined solely by the appended claims and is not affected to any degree by the statements within this summary. The present embodiments may obviate one or more of the drawbacks or limitations in the related art.

[0008] The object of the embodiments is to devise a method enabling a client apparatus to set up a connection to a different server apparatus reliably and without manual or other complex measures, even following the characterization.

[0009] The method according to an embodiment for characterizing a client apparatus on at least one server apparatus includes receiving of a first certificate in the event of a first request for a connection set-up from a server apparatus in a client apparatus. One or more predefined certificate parameters of the first certificate are stored as a set of characterization parameters in the client apparatus. The method further includes checking of each further certificate from a server apparatus that is received in the client apparatus in the event of a request for a further connection set-up against the stored characterization parameter set. The method further includes accepting of a request for a further connection set-up only if all of the predefined certificate parameters of the further certificate match all characterization parameters of the characterization parameter set.

[0010] A client apparatus is thereby advantageously not exclusively characterized on an individual certificate, as would be the case, for example, by storing and checking an entire certificate with all certificate parameters or a fingerprint of a certificate. A client apparatus may be characterized through the characterization on specific, prescribed parameters that form a set of characterization parameters on a group of certificates with common characteristics. In one advantageous embodiment, at least the value of one sub-parameter of a certificate parameter of the first certificate is stored as a characterization parameter.

[0011] As a result, for example, the structure of a certificate is utilized and a group of server apparatuses that satisfies a specific characteristic of the certificate parameter defined by the sub-parameters is permitted to communicate.

[0012] In a further embodiment, at least the value of one parameter or sub-parameter of an extension element of the first certificate is stored as a characterization parameter.

[0013] Using already defined extension elements of a certificate structured according to the X.509 standard, a role-based access control, for example, may be defined or

server apparatuses may be represented via alternative subject designations, referred to as subjectAltNames, by DNS names or email addresses.

[0014] In a further embodiment, at least the value of one parameter or sub-parameter of an attribute certificate of a first certificate is stored as a characterization parameter.

[0015] Attribute certificates indicate further parameters or characteristics and thus allow further possibilities for the characterization on a group of server apparatuses with the aforementioned parameters or sub-parameters of the attribute certificate.

[0016] In one embodiment, at least one issuer of the first certificate is used as a characterization parameter.

[0017] In one embodiment, a further certificate that is received in the event of a request for a further connection set-up from a server apparatus is checked against the stored characterization parameter, bit-by-bit. The embodiment represents a simple comparison method that is simply and economically available in simple client apparatuses also.

[0018] In one embodiment, the predefined certificate parameters that are intended to be stored by a client apparatus on receiving a first certificate as a characterization parameter are notified to the client apparatus in a first certificate. The embodiment allows a highly flexible allocation of characterization parameters to a client apparatus, such as, for example, an application protocol. Different application protocols may thus be characterized on different characterization parameters.

[0019] In a further embodiment, the predefined certificate parameters to be stored as characterization parameters are indicated in at least one extension element of the first certificate. For example, the extension elements standardized by the X.509 standard for certificates are already available and may simply be used as carriers for the definition of the characterization parameters predefined for the client apparatus.

[0020] In an alternative embodiment, the predefined certificate parameters that are intended to be used as characterization parameters by a client apparatus on receiving a first certificate are predefined by an application of the client apparatus. The embodiment offers the advantage that no additional information relating to the characterization parameters needs to be transported between the client apparatus and the server apparatus. The embodiment reduces the data quantity to be exchanged and furthermore rules out a manipulation of the information transmission.

[0021] In a further embodiment, the predefined certificate parameters that are intended to be stored as characterization parameters by a client apparatus on receiving a first certificate are preconfigured in the client apparatus. The embodiment offers the advantage that the client apparatus determines and stores only the predefined and permanently specified certificate parameters that are intended to be used as characterization parameters in the certificate received in the first connection request.

[0022] A client apparatus according to an embodiment includes a receiving unit, a characterizing unit and a checking unit. The receiving unit is designed to receive a first certificate from a server apparatus in the event of a first request for a connection set-up. The characterizing unit is designed to store values of one or more predefined certificate parameters of the first certificate as a set of characterization parameters. The checking unit is designed to check each further certificate that is received from a server apparatus in the event of a request for a further connection set-up against the stored characterization parameter set and to accept the request for a further connection set-up only if all of the predefined certificate parameters of the further certificate match all characterization parameters of the characterization parameter set.

[0023] In the case of, for example, an expired certificate on which characterization has been effected, or in the event of a failure of one server apparatus, an embodiment offers the advantage of communicating with another server apparatus without manual measures having to be undertaken. Example embodiments of the method and a client apparatus according to an embodiment are shown by way of example and are explained in detail in the description below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0024] FIG. **1** depicts prior art of a schematic representation of a client-server system with a characterization of a client apparatus on a single dedicated server apparatus.

[0025] FIG. **2** depicts a schematic representation of a client-server system with characterization of a client apparatus on a group of server apparatuses according to an embodiment.

[0026] FIG. **3** depicts a certificate according to an X.509 standard with certificate parameters according to an embodiment.

[0027] FIG. **4** depicts a certificate parameter with sub-parameters according to an embodiment.

[0028] FIG. **5** depicts an extension element according to an embodiment.

[0029] FIG. **6** depicts a flow diagram of the method according to an embodiment.

[0030] Parts corresponding to one another are denoted with the same reference numbers in all figures.

DETAILED DESCRIPTION

[0031] FIG. **1** depicts by way of example a client-server system **1** with a characterization, not corresponding to an embodiment, of a client apparatus **4**. The client apparatus **4** checks a certificate **5.1** received from the server apparatus **3.1** during the first connection set-up **0** and imports the entire content of the certificate **5.1** into a security association list of the client apparatus **4**. The server apparatus **3.1** is uniquely identified by the issuer and the serial number of the certificate **5.1**. If the client apparatus **4** receives a further certificate **5.2** that differs from the stored certificate **5.1** from a further server apparatus **3.2** in the event of a subsequent request for a connection set-up **8**, the connection set-up is refused by the client apparatus **4**. A certificate is normally issued for each server apparatus **3.1**, **3.2** by a certification body **2** based on a trustworthy root certification body. Instead of a check of the certificate **5.1** and **5.2**, fingerprints of the respective certificate **5.1** and **5.2** may also be compared with one another. A fingerprint of a certificate may normally be, for example, the hash value for the respective certificate.

[0032] The client apparatus **4** is thus dedicated and characterized exclusively on one server apparatus **3.1** and accepts no communication with another server apparatus **3.2**. If, for example, the validity of the certificate **5.1** expires, or if the secret key of the server apparatus **3.1** is compromised, the certificate **5.1** is replaced. Communication may then take place between the client apparatus **4** and another

server **3.2** only through special interventions, for example an update of the operating system or a manual factory reset.

[0033] FIG. **2** depicts a client-server system **6** with a characterization using the method according to an embodiment. Each server apparatus **3.1**, **3.2**, **3.3** in each case includes one certificate **5.1**, **5.2**, **5.3** that was issued and notified by the certification body **2** at the request of the server apparatus **3.1**, **3.2**, **3.3**. If the client apparatus **4** then receives a certificate **5.1** following the start-up in the event of a first request for a connection set-up from a server apparatus **3.1**, the client apparatus **4** does not use the entire certificate **5.1**, but only the values PP of one or more predefined certificate parameters of the certificate **5.1** subsequently as a set of characterization parameters **7**. In the event of a further request **8** for a further connection set-up from a server apparatus **3.3**, the transmitted further certificate **5.3** is checked against the stored set of characterization parameters **7**. If all values of the predefined certificate parameters of the further certificate **5.3**, here QP, match the values of all characterization parameters of the characterization parameter set **7**, the request **8** is accepted by the client apparatus **4**. If, as in the example depicted, the values QP of the predefined certificate parameters of the further server apparatus **3.3** differ from the set of characterization parameters PP, the connection set-up is refused.

[0034] If the client apparatus **4** receives a certificate in the event of a request for a connection set-up **9** from a server apparatus **3.2**, and if the predefined certificate parameters of the certificate **5.2** have the same values, here PP, as the set of characterization parameters **7** in the client apparatus **4**, similarly PP, the client apparatus **4** accepts the connection set-up request **9** and allows the set-up of a connection to the further server apparatus **3.2**.

[0035] A characterization of the client apparatus **4** on a plurality of server apparatuses **3.1**, **3.2** may thus be effected in a simple manner. A changeover, for example, of the client apparatus **4**, for example a smart meter, from a live server apparatus **3.1** to a test server apparatus **3.2** in order to carry out a check may thus take place without a manual intervention in the client apparatus **4**. In the same way, the client apparatus **4**, following the check on the test server apparatus **3.2** may resume the connection to the live server apparatus **3.1**.

[0036] Certificate parameters, for example, that identify the issuer of the certificate or the subject, for example, the server apparatus or the application for which certificate was issued, are suitable as predefined certificate parameters that are stored as characterization parameters. It is assumed here that the issuer of the certificate may be, but not exclusively, a sub-certification body under the root certification body.

[0037] The client apparatus **4** includes a receiving unit **41**, a characterizing unit **42** and a checking unit **43** that are in each case interconnected. The receiving unit **41** includes, for example, an interface to an Internet cable or a receiving unit for a radio link that receives a first certificate **5.1** in the event of a first request for a connection set-up from a server apparatus **3.1**. At least the value PP of the one or more predefined certificate parameters of the first certificate **5.1** is stored as a characterization parameter set **7** in the characterizing unit **42**. In the event of a request **9** for a further connection set-up, the certificate **5.2** also supplied by a server apparatus, for example the server apparatus **3.2**, is received in the receiving unit **41** and is checked in the checking unit **43** against the characterization parameter set **7** stored in the characterizing unit **42**. If all values PP of the predefined certificate parameters of the further certificate **5.2** match all characterization parameters of the characterization parameter set **7**, the checking unit **43** accepts the request and sets up the connection to the server apparatus **3.2**. If the values QP of the predefined certificate parameters of the further certificate **5.3** received, for example, from the server apparatus **3.3** do not match all characterization parameters of PP of the characterization parameter set **7** in the event of a request **8**, the checking unit **43** refuses the request. Alternatively or additionally, the information may be stored in a logging file and/or may be transmitted to a, for example, preconfigured logging server.

[0038] FIG. **3** depicts an example of a certificate **10** that is structured according to the X.509 standard of the International Telecommunication Union ITU-T. Certificate parameters are the different entries specified under the "TBS Certificate" heading. The "issuer" **11** and "subject" **13** parameters that may, for example, have a sub-structure **23** with sub-parameters are particularly suitable for the characterization. A sub-structure **23** is shown by way of example in FIG. **4** for the certificate parameter **13**. The "organization" **21** sub-parameters or an "organizational unit" **22** parameter indicating a sub-unit, for example, are suitable for the characterization of a client apparatus **4** on a group of server apparatuses.

[0039] Parameters or sub-parameters of an extension element, see FIG. **3**, referred to as "extensions" **15**, may also be used.

[0040] FIG. **5** depicts by way of example an extension element **15**. A certificate may be extended by role information "UserRoleInfo" **33**. The client apparatus **4** may be characterized via the "userRole" **31** parameters, for example on the "authorization server" role. The "aor" **32** parameter that indicates an area of responsibility may also be stored as a characterization parameter in the client apparatus **4**. Each server apparatus **3.1**, **3.2** with the same value PP of the characterization parameter set **7** is then permitted by the client apparatus **4** as a communication partner.

[0041] Parameters from attribute certificates that are allocated to a certificate may furthermore be stored as characterization parameters. As a result, it is therefore possible not to characterize a client apparatus **4** on a dedicated server, but instead to enable the communication and therefore the connection set-up on a group of server apparatuses **3.1**, **3.2**. The changeover of the certificates **5.1**, **5.2** within the group of server apparatuses that have the same characterization parameters is therefore also enabled. However, the unwanted changeover to a server apparatus **5.3** that does not have the corresponding characterization parameters may still be prevented.

[0042] Certificates **5**, **5.1**, **5.2**, **5.3**, etc., from commercial certificate issuers such as, for example, Verisign or Telekom, may be used. Certificates **5**, **5.1**, **5.2**, **5.3**, etc., that are used may comply with the X.509 standard. However, non-standardized certificates that have a logical structure of the certificate parameters, for example the subject, e.g. the application or the server appliance, may also be used.

[0043] FIG. **6** depicts the method according to an embodiment for characterizing a client apparatus on server apparatuses in the form of a flow diagram **50**. Starting from the initial state **51**, a certificate is received at act **52** in a client apparatus in the event of the first request to set up a connection from a server apparatus **3**. At act **53**, the client

apparatus checks whether a certificate or characterization parameters are already stored. If not, the client apparatus selects predefined certificate parameters as a set of characterization parameters and stores the certificate or at least these characterization parameters. The characterization, see act **55**, of the client apparatus is performed on server apparatuses whose certificates have the same values in the predefined certificate parameters as the characterization parameters.

[0044] The predefined certificate parameters **11**, **12** or sub-parameters **21**, **22** or parameters or sub-parameters **31**, **32** of an extension element **15** that are intended to be stored by a client apparatus as a set of characterization parameters **7** on receiving a first certificate **5.1** may be notified to the client apparatus **4** in the first certificate **5.1**. An extension element of the first certificate, for example, is suitable for the purpose. However, the predefined certificate parameters may also be predefined in an application in a client apparatus **4** itself. The application selects the certificate parameters predefined for the application in the event of a first connection set-up and stores these as characterization parameters. Alternatively, the predefined certificate parameters may be preconfigured in the client apparatus **4**.

[0045] If the client apparatus **4** establishes in the check **53** that a set of characterization parameters **7** is already stored in the client apparatus **4**, the client apparatus **4** checks the received further certificate in act **56** against the stored characterization parameter set **7**. If all of the predefined certificate parameters of the further certificate match all characterization parameters of the characterization parameter set **7**, the connection request is accepted and a connection is set up to the further server apparatus, see act **58**. If at least one of the predefined certificate parameters did not match the characterization parameter set **7**, the connection request is refused, see act **59**.

[0046] The check of the predefined certificate parameters against the characterization parameter set may be carried out, for example, bit-by-bit. The check simplifies a corresponding check routine, since the certificate parameters do not have to be evaluated in a dedicated manner.

[0047] All described and/or characterized features may be combined with one another within the scope of the invention. The invention is not limited to the example embodiments described.

[0048] It is to be understood that the elements and features recited in the appended claims may be combined in different ways to produce new claims that likewise fall within the scope of the present invention. Thus, whereas the dependent claims appended below depend from only a single independent or dependent claim, it is to be understood that these dependent claims may, alternatively, be made to depend in the alternative from any preceding or following claim, whether independent or dependent, and that such new combinations are to be understood as forming a part of the present specification.

[0049] While the present invention has been described above by reference to various embodiments, it may be understood that many changes and modifications may be made to the described embodiments. It is therefore intended that the foregoing description be regarded as illustrative rather than limiting, and that it be understood that all equivalents and/or combinations of embodiments are intended to be included in this description.

1. A method for characterizing a client apparatus on at least one server apparatus, with the method comprising:

receiving a first certificate from the at least one server apparatus in the client apparatus in the event of a first request for a connection set-up;

storing values of one or more predefined certificate parameters of the first certificate as a set of characterization parameters in the client apparatus;

checking each further certificate from a server apparatus that is received in the client apparatus in the event of a further request for a connection set-up, against the stored characterization parameter set; and

accepting the further request for a connection set-up only when all predefined certificate parameters of the further certificate match all characterization parameters of the characterization parameter set.

2. The method of claim **1**, wherein at least one value of a sub-parameter of one of the certificate parameters of the first certificate is used as one of the characterization parameters.

3. The method of claim **1**, wherein at least one value of a parameter or sub-parameter of an extension element of the first certificate is used as one of the characterization parameters parameter.

4. The method of claim **1**, wherein at least one value of a parameter or sub-parameter of an attribute certificate of the first certificate is used as one of the characterization parameters.

5. The method of claim **1**, wherein at least one issuer of the first certificate is used as one of the characterization parameters parameter.

6. The method of claim **1**, wherein the checking of a further certificate that is received from the server apparatus in the event of the further request for the connection set-up against the stored characterization parameter set is carried out bit-by-bit.

7. The method of claim **1**, wherein the predefined certificate parameters that are intended to be stored as characterization parameters by the client apparatus on receiving the first certificate are notified to the client apparatus in the first certificate.

8. The method of claim **7**, wherein the predefined certificate parameters that are to be stored as characterization parameters are indicated in at least one extension element of the first certificate.

9. The method of claim **1**, wherein the predefined certificate parameters that are intended to be stored as characterization parameters by the client apparatus on receiving the first certificate are predefined by an application of the client apparatus.

10. The method of claim **1**, wherein the predefined certificate parameters that are intended to be stored as characterization parameters by the client apparatus on receiving the first certificate are preconfigured in the client apparatus.

11. A client apparatus, comprising

a receiving unit;

a characterizing unit; and

a checking unit,

wherein the receiving unit is configured to receive a first certificate from a server apparatus in the event of a first request for a connection set-up;

wherein the characterizing unit is configured to store the values of one or more predefined certificate parameters of the first certificate as a set of characterization parameters;

wherein the checking unit is configured to check each further certificate that is received from the server apparatus in the event of a request for a further connection set-up against the stored characterization parameter set and to accept the request for the further connection set-up only when the values of all of the predefined certificate parameters of the further certificate match all values of the characterization parameters of the characterization parameter set.

12. (canceled)

13. (canceled)

14. (canceled)

15. The client apparatus as claimed in claim **11**, wherein at least one value of a sub-parameter of one of the certificate parameters of the first certificate is used as one of the characterization parameters.

16. The client apparatus as claimed in claim **11**, wherein at least one value of a parameter or sub-parameter of an extension element of the first certificate is used as one of the characterization parameters.

17. The client apparatus as claimed in claim **11**, wherein at least one value of a parameter or sub-parameter of an attribute certificate of the first certificate is used as one of the characterization parameters.

18. The client apparatus as claimed in claim **11**, wherein at least one issuer of the first certificate is used as one of the characterization parameters.

19. The client apparatus as claimed in claim **11**, wherein the checking of a further certificate is carried out bit-by-bit.

20. The client apparatus as claimed in claim **11**, wherein the predefined certificate parameters that are intended to be stored as characterization parameters by the client apparatus on receiving the first certificate are notified to the client apparatus in the first certificate.

21. The client apparatus as claimed in claim **20**, wherein the predefined certificate parameters that are to be stored as characterization parameters are indicated in at least one extension element of the first certificate.

22. The client apparatus as claimed in claim **11**, wherein the predefined certificate parameters that are intended to be stored as characterization parameters by the client apparatus on receiving the first certificate are predefined by an application of the client apparatus.

23. The client apparatus as claimed in claim **11**, wherein the predefined certificate parameters that are intended to be stored as characterization parameters by the client apparatus on receiving the first certificate are preconfigured in the client apparatus.

* * * * *