(19) DANMARK

(10) DK/EP 3243310 T3

Patent- og Varemærkestyrelsen

(12) Oversættelse af europæisk patentskrift

(51) Int.Cl.: *G 06 F 21/33 (2013.01)* *F 03 D 7/04 (2006.01)* *H 04 L 9/32 (2006.01)* *H 04 L 29/06 (2006.01)*

(45) Oversættelsen bekendtgjort den: **2020-04-14**

(80) Dato for Den Europæiske Patentmyndigheds bekendtgørelse om meddelelse af patentet: **2020-01-08**

(86) Europæisk ansøgning nr.: **15816467.3**

(86) Europæisk indleveringsdag: **2015-12-21**

(87) Den europæiske ansøgnings publiceringsdag: **2017-11-15**

(86) International ansøgning nr.: **EP2015080736**

(87) Internationalt publikationsnr.: **WO2016110405**

(30) Prioritet: **2015-01-09 DE 102015200209**

(84) Designerede stater: **AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR**

(73) Patenthaver: **Wobben Properties GmbH, Borsigstrasse 26, 26607 Aurich, Tyskland**

(72) Opfinder: **JAKOBS, Thorsten, Moosweg 7, 26529 Leezdorf, Tyskland**
GIERTZ, Helge, Kolberger Straße 46, 26789 Leer, Tyskland
DEMUTH, Simon, Kastanienallee 9, 26524 Hage, Tyskland

(74) Fuldmægtig i Danmark: **Zacco Denmark A/S, Arne Jacobsens Allé 15, 2300 København S, Danmark**

(54) Benævnelse: **Fremgangsmåde til autorisering af styreadgange til vindenergianlæg og grænseflade af vindenergianlæg og certificeringssted**

(56) Fremdragne publikationer:
WO-A2-2009/131656
GB-A- 2 487 049
JP-A- 2011 524 559

Description

The invention relates to a method for authorizing users for control accesses to at least one wind turbine or at least one wind farm, and relates to an interface for at least one wind turbine or for at least one wind farm, to a certification centre and to a system comprising a certification centre and an interface for at least one wind turbine or for at least one wind farm.

According to the prior art, control accesses and read accesses to a wind turbine or a plurality of wind turbines organized as a wind farm are possible. Control accesses and read accesses to wind farms are implemented, for instance, by read accesses and control accesses to a wind farm controller. With a read access, a user can read, for instance, live operating data such as the power currently being fed into the power grid. Thus read accesses are all accesses for which there is no intervention in the operation of the wind turbine, so the user has in particular no influence on the operating parameters.

Unlike a read access, a control access has a direct or indirect effect on the operation of the wind turbine, for instance by a change to operating parameters. Operating parameters are e.g. control variables and the like. A control access can also be used, for example, to start up or shut down one or more wind turbines or to vary the amount of power, and the voltage or frequency of the power, that is fed into a power grid.

According to the prior art, a user is authenticated with a wind turbine or a wind farm by transferring a tuple of password and user identifier so that the user can identify himself with the wind farm as regards his identity. On the basis of this transfer to the wind turbine or the wind farm, the user is then permitted control accesses and/or read accesses, where the access type i.e. the read-access type or control-access type, of different users can be restricted differently by the wind turbine

or wind farm concerned. Such restrictions are stored in the wind farm or wind turbine together with the user identifier and password.

At the very least, at least one user also has the authority to perform system-critical control-access types which include e.g. switching on or shutting down the wind turbine or wind farm. Thus if the access data of this user is known, namely the tuple consisting of user name and password, the wind turbine or wind farm can be accessed by critical control-access types.

Under a threat scenario resulting from human error and insider sabotage, if the access data is known for a plurality of wind farms in a region, it is hence possible to shut down these wind farms. Thus a power grid or electricity grid in this region could completely fail because, as a result of a simultaneous shutdown of a plurality of wind farms, consumers are demanding more energy than the energy sources can provide. It is therefore the object of the present invention to take measures that make control accesses, and in particular critical control accesses, to wind turbines and wind farms more secure.

In the priority application for the present application, the German Patent and Trademark Office researched the following prior art: DE 10 2010 044 517 A1, EP 1 598 729 A2, WO 2011/015414 A1. Further, GB 2487049 A discloses the possibility to perform an authorization of a user for a wind turbine or a wind farm by means of a previously issued certificate.

The present invention achieves this object by a method according to Claim 1 for authorizing users for control accesses to at least one wind turbine or at least one wind farm, by a certification centre according to Claim 7 and by a system according to Claim 9 comprising a certification centre and at least one interface of at least one wind turbine or of at least one wind farm.

According to the invention, the following steps are performed for the purpose of authorizing users for control accesses to at least one wind turbine, i.e. to one or more wind turbines, or even to one or more wind farms formed in each case by a network of wind turbines.

First, a user who authenticates himself with a certification centre is authenticated by the certification centre. In this process, a user transfers to a certification centre for the purpose of authentication e.g. a tuple consisting of password and user name, password and user identifier, an electronic certificate, a combination of password, user name and certificate or the like, thereby providing evidence of the personal identity of the user. If the access data is correct, i.e. the user name and password are correct and/or the certificate is correct, the user is then authenticated by the certification centre, i.e. an access permission is confirmed. Hence the user is thereby authenticated with the certification centre by the certification centre.

In the next step, the certification centre accepts one or more control-access types from the authenticated user, said control-access types being transferred to the certification centre in particular by the user e.g. using input means and/or a graphical user interface.

Control-access types here refer to different forms of control access, where a control access denotes all accesses which can have an effect on functions and operation, and which therefore can result in effects on current and future operating statuses of the wind turbine or of the wind farm. Thus a control-access type describes one or more possible control accesses such as e.g. parameterization, the start-up and/or shutdown of one or more or all wind turbines, etc.

Thus according to the method, the user transfers one or more control-access types to the certification centre, in particular the user transfers the control-access type(s) that are intended to be used later to access a wind turbine or a wind farm.

If the certification centre accepts the control-access type from the authenticated user then a digital certificate is generated by the certification centre according to the accepted control-access type and/or according to stored access permissions of the authenticated user. Hence in particular the accepted control-access type(s) are also stored in the certificate, and therefore this certificate generated by the certification centre can also be referred to as a token.

A certificate, also called a digital certificate, is a digital data record which is used to verify certain properties of people by means of cryptographic techniques for the purpose of authorizing the person. In addition to user-specific data such as access data, further data such as e.g. said control-access type is also stored in the certificate in an essentially tamperproof manner, which data can be read by the wind turbine(s) or by the wind farm(s). Thus a certificate is also a form of token, so for instance is equivalent to an electronic key, which is essentially tamperproof and on which further data is also stored in addition to the data for authorizing a user.

In the next step, the certificate is used to perform an authentication with the wind turbine or the wind farm for the purpose of implementing the control-access type(s) previously transferred by the user and accepted by the certification centre. In addition, according to an alternative embodiment, it is also necessary for the purpose of authentication to transfer in addition to the certificate generated by the certification centre additionally user-access data such as e.g. user identifier and password.

Thus a central certification centre is advantageously provided, which is used to coordinate control-access types of users. Direct control access by a user to a wind turbine or a wind farm without the step via the certification centre is hence not possible. It can hence be guaranteed that coordination of the permitted control accesses is possible in the certification centre, thereby counteracting error and sabotage. The certification centre is thus designed to restrict the awarding of certificates such that

control-access types to a plurality of wind turbines or wind farms which are requested by one or more users, i.e. accepted by the certification centre, and which may for example result in a mains failure, can be inhibited.

Here and below, a user is a person, e.g. a member of maintenance staff, or else also an electronic system of a power company or of a direct seller. If the user is an electronic system, the user is authenticated automatically e.g. by transferring a certificate.

According to one embodiment, read accesses to wind turbines and wind farms, so for instance to the wind-farm control system, is possible by certificate-independent authentication of users, in particular by means of a tuple consisting of user identifier and password. In other words, a user needs to request or apply for the certificate from the certification centre only for control accesses to a wind turbine and wind farm. A read access is still possible by means of a direct authentication using a user name and password. Thus a read access can be performed very easily and quickly by a user, and because read accesses are non-critical, the digital certificate from the certification centre can be dispensed with in this case.

According to another embodiment, the certification centre uses an issuing interface to issue the certificate, in particular to a processing unit of the user, with the result that the external processing unit, which is e.g. a portable computer or another mobile device similar to a computer, can be used to perform authentication independently of the certification centre.

This has the advantage that when there is no data connection to the certification centre, a control access can be performed using the control-access type contained in the certificate. In remote areas in which a certificate cannot be requested from the certification centre, the certificate can hence be "pre-generated" and the issued certificate can then be used locally at the wind turbine or wind farm to perform a control access even without a data connection.

According to another embodiment, the control accesses are performed directly by the certification centre. For this purpose, the certification centre comprises e.g. a user interface, by means of which a user transfers control accesses directly to the certification centre, and the certification centre then authenticates the user together with the certificate at the wind turbine or wind farm, so that control accesses from the user received by the certification centre are also forwarded to the wind turbine or wind farm or prohibited.

According to this embodiment, users in the form of power companies actually have the facility to restrict output from wind farms and to modify other operating parameters that relate to power feed-in, if grid stability makes this necessary.

After successful authentication, it is possible to perform control accesses, such as wind-farm output restrictions, for individual wind farms by a power company addressing a central interface of the system, namely the certification centre, and the necessary parameters of the control access being transferred. Then the certification centre generates internally on behalf of the power company a certificate for the desired action and sends the control command together with certificate (token) to the wind farm. Finally, feedback on the success of the action is given to the power company.

For safety reasons, the described interface can have a redundant design according to various embodiments, and can be implemented as various protocols such as, for example, SOAP, IEC 60870-5-104, DNP3 TCP or even Modbus TCP.

The advantage over the prior art is that the power company no longer needs to service and maintain a dedicated connection for each wind farm. Furthermore, it is also possible via this interface to provide the power company with more operating parameters (current setpoint values, possible power output etc.) of the wind farm. This form of central control is made possible for the first time by the certificate-

based or token-based communication with the wind farm, because by conventional means the potential risks would be untenable.

If the users are direct sellers, the certification centre can also be used by these direct sellers in order to regulate the feed-in power directly or indirectly according to economic considerations, for instance on the basis of what are known as schedules. According to the present state of the art, direct sellers have a direct connection to each individual wind farm.

The process runs in a similar way to the power company interface. The advantages are that a direct seller no longer needs to set up and maintain a multiplicity of connections. Furthermore, this method increases security.

According to another embodiment, a control system, e.g. a dynamic set of rules or a control database, in which each of a plurality of registered users, in particular every registered user, can be allocated or is allocated at least one allowed and/or one unallowed control-access type, is stored in the certification centre. According to this embodiment, the certification centre generates for authenticated users certificates containing the control-access type accepted from the user only if the control-access type transferred by the user is allowed for the user in the control system. Hence the control system is like a set of permission rules, which can be static or is changed dynamically according to various factors.

Different control-access types can hence be allocated centrally in the certification centre to different users of different wind farms, so that access permissions can be administered centrally for a multiplicity of wind farms or wind turbines.

According to another embodiment, each of the certificates generated by the certification centre has a validity period, also known as a timestamp. After a designated validity period, an electronic certificate thereby loses the permission to authenticate a user for a control access to a wind turbine or a wind farm.

A validity period is stored, for example in the control database, individually for each user and/or each control-access type, or a general validity period is designated for all the certificates in the certification centre and is used to generate the certificates.

This simplifies the coordination of the control-access types currently allocated by the certification centre, because the validity periods of the currently issued certificates can be stored in the certification centre. The certification centre thus always knows which control-access types and how many are currently possible. Hence a certificate does not need to be returned after use to the certification centre by the user, but expires "automatically".

According to another embodiment, a maximum total number or a maximum number per predefined region is stored in the control system for each control-access type and/or for all control-access types. Certificates are generated or awarded for a control-access type only in such a number that the number, or total number, of awarded certificates that are currently valid on the basis of their validity period lies below the maximum total number or the maximum number for the given region.

This ensures that for control-access types and in particular critical control-access types such as e.g. shutting down wind turbines, only so many certificates are generated as to keep the power grid stable, in particular in specific regions. This avoids the risk of permitting so many control accesses having a critical control-access type in one region or in total as to cause the power grid to collapse.

According to another embodiment, the certification centre generates the certificate also according to at least one ascertained current or predicted parameter, in particular according to a grid status parameter, the weather and/or the status of the wind turbines or other wind turbines. It is thus possible, for instance, to adjust the maximum total number or the maximum number per predefined region according to a grid parameter such as e.g. a grid status parameter. In regions in which a weak grid, for instance, is detected from the current ascertained parameters, then a complete

shutdown or a reduction in the power feed-in of any wind turbine is not permitted, or is only permitted for very few wind turbines. Hence the certification centre limits or restricts for this region the number of control-access types.

The control system is hence dynamically adjusted, for instance by external parameters.

The invention also includes an interface for at least one wind turbine, i.e. one or more wind turbines, in particular in a wind farm. The interface is designed to receive an electronic digital certificate which has been generated by a certification centre and to allow on the basis of the electronic certificate, in particular on the basis of the information stored in the certificate, control accesses of the control-access type(s) stored in the certificate. Control accesses to a wind turbine or a wind farm are hence possible only by means of a pre-generated certificate that was generated by the certification centre.

According to one embodiment, the interface of the wind turbine or of the wind farm is also designed to allow a validity period stored in the certificate to be read, and to allow control accesses only if a validity period is valid.

Thus by checking a validity period of the certificate, certificates that have already expired can be classified so that a user using such a certificate is not allowed to perform a control access.

According to another embodiment, the interface of the wind turbine or of the wind farm is designed to read a turbine identifier, which is stored in the certificate, and to allow control accesses only for a turbine identifier that matches the turbine identifier of the wind turbine to which access is required.

Checking a turbine identifier in the certificate means that it is possible to allow a user access only to wind turbines cleared by the certification centre.

In addition, the invention includes a certification centre for authenticating users for control accesses to at least one wind turbine. The certification centre comprises an interface for authenticating users with the certification centre, which interface is also designed to accept a control-access type from the user to the certification centre.

The certification centre is also designed to generate an electronic digital certificate according to the transferred control-access type, i.e. the control-access type accepted by the certification centre, and/or according to stored access permissions of the authenticated user. The interface is also used to issue the generated certificate.

Thus the certification centre can be used for awarding centrally the access permissions of the control accesses to a multiplicity of wind turbines or wind farms, with the result that critical control-access types can be controlled.

According to one embodiment, the certification centre is designed to generate the certificate such that it contains a validity period and/or one or more turbine identifiers, said validity period and/or turbine identifier(s) being stored in the certificate.

Hence using the certificate, a user is allowed to perform control accesses having the control-access type stored in the certificate only on wind turbines that are cleared by the certification centre and have corresponding turbine identifiers and/or only for a time period specified by the validity period.

According to another embodiment, the certification centre comprises a control system, by means of which control system at least one registered user or each of a plurality of registered users, in particular every registered user, can be allocated or is allocated at least one allowed and/or un-allowed control-access type. The certification centre is designed to generate electronic, i.e. digital, certificates for pre-authenticated users if the control-access type transferred by the user concerned is designated in the control database as allowed.

An access-permission administration system can hence be stored in a single control database in the certification centre, and can be used for central administration of the user permissions.

According to another embodiment, the certification centre is designed to allocate a validity period to the certificates, i.e. to store a validity period in the certificate.

According to another embodiment, a maximum total number or a maximum number per predefined region is stored for each control-access type in the control database. The certification centre is also designed such that certificates are generated for a control-access type only if the number of the electronic certificates containing this control-access type that have already been awarded and are currently valid remains below the maximum total number or the maximum number for the region. Hence only as many certificates for e.g. critical control-access types are awarded or generated that will continue to ensure a stable grid.

According to another embodiment, the interface of the certification centre is designed to accept from the authenticated user also turbine identifiers in addition to control-access types, which turbine identifiers uniquely identify one or more wind turbines or one or more wind farms.

Hence the authenticated user supplies to the certification centre via the interface of the certification centre not only at least one control-access type but also at least one turbine identifier. The certification centre is then designed to generate the electronic certificate according to the turbine identifier. The transferred turbine identifier is accordingly stored in the certificate. Hence access is possible only to the wind turbines or the wind farm for which the turbine identifier is valid.

It is thereby possible to restrict the control accesses to wind turbines previously established with the certification centre.

According to another embodiment, the certification centre comprises a further interface in order to receive parameters such as e.g. prevailing weather data, weather forecasts, current grid statuses and/or grid-status predictions, and to adjust the control database according to these parameters.

This hence provides a dynamic control system, which is updated or changed on the basis of received parameters. In particular, it is possible to use these parameters to adjust, for example, the maximum total number or the maximum number per defined region. Thus in a region in which a weak power grid exists already, safeguards can be made against control accesses that would degrade this grid status further. For this purpose, for example, the maximum total number of control-access types and a maximum number of permitted wind turbines would be reduced.

The invention also includes a system comprising an interface of a wind turbine or of a wind farm according to any of the above-mentioned embodiments and a certification centre according to any of the above-mentioned embodiments, in particular for implementing a method according to any of the above-mentioned embodiments.

The invention is determined by the appended claims.

The invention is described in greater detail below using exemplary embodiments with reference to the accompanying drawings, in which:

Fig. 1 shows a wind turbine;

Fig. 2 shows a wind farm;

Fig. 3 shows an exemplary embodiment of the system according to the invention and

Fig. 4 shows a flow sequence of an exemplary embodiment of the method according to the invention.

Fig. 1 shows a schematic diagram of a wind turbine according to the invention. The wind turbine 100 comprises a tower 102 and a nacelle 104 on the tower 102. An aerodynamic rotor 106 having three rotor blades 108 and a spinner 110 is provided on the nacelle 104. During operation of the wind turbine, the wind causes the aerodynamic rotor 106 to rotate, which hence also turns a generator rotor that is coupled directly or indirectly to the aerodynamic rotor 106. The electric generator is arranged in the nacelle 104 and generates electrical energy. The pitch angle of the rotor blades 108 can be varied by pitch motors on the rotor-blade roots 108b of the respective rotor blades 108.

Fig. 2 shows a wind farm 112 comprising by way of example three wind turbines 100, which may be identical or different. The three wind turbines 100 are hence representative of in principle any number of wind turbines in a wind farm 112. The wind turbines 100 provide their power, specifically the generated electrical current, via an electrical wind-farm network 114. The current or power generated by each of the wind turbines 100 is summated in this network, and a transformer 116 which steps up the voltage in the wind farm is usually provided in order to feed into the power grid 120 at the point of common coupling (PCC) 118. Fig. 2 is just a simplified representation of a wind farm 112, which does not show a controller for instance, although obviously a controller exists. The wind-farm network 114, for example, can also have a different design, for instance a design in which a transformer is present at the output of each wind turbine 100, to name just one different exemplary embodiment.

Fig. 3 shows an exemplary embodiment of the system according to the invention, which comprises in particular a certification centre 10 and an interface 12 of a wind farm 112. The interface 12 of the wind farm 112 is e.g. the interface of a SCADA system, where SCADA stands for Supervisory Control And Data Acquisition.

The figure also shows a mobile device 16 of a user 18. The user 18 makes a connection via the mobile device 16 to an interface 20 of the certification centre 10. For

the purpose of authenticating the user 18, the mobile device 16 transmits to the interface 20 a user name and a password of the user 18. In addition, the user 18 transmits a control-access type and a turbine identifier to the interface 20 by means of the mobile device 16. The turbine identifier specifies to which wind farm the user 18 wishes to make a control access having the transmitted control-access type.

The interface 20 transmits the transferred data to a processor 22, which first checks using a control system 24 whether the authenticated user 18 is permitted to perform the requested control-access type on the wind farm specified by the turbine identifier.

In addition, the processor 22 checks using the control

system 24 whether a maximum number of control accesses of the requested control-access type is already exceeded. If this number is not exceeded, then the processor 22 generates a certificate. The certificate contains a validity period, which is created by a date-and-time source 26. The date-and-time signal is here determined e.g. from a GPS signal, and transmitted to the processor. Then, in the processor 22, the validity period is stored in the certificate for a time period, which in particular is predefined by the control system 24. Examples of validity periods are, for instance, two hours, eight hours, one day or five days.

The certificate that was generated by the processor 22 also contains the control-access type transferred by the user 18 to the interface 20 using the mobile device 16, the turbine identifier and further cryptographic parameters for verifying the authenticity of the certificate.

The certificate 28 is transmitted via the interface 20 to the mobile device 16. By entering his user name and password, the user 18 can initiate a read access to the wind farm 112 and can read data from the wind farm 112 via a further data connection 30 between the mobile device 16 and the interface 12 of the wind farm 112. If,

however, the user wants to make a write access, which in this context corresponds to the control access, to the wind farm 112, then the certificate 28 is transferred via the further data connection 30 to the interface 12 of the wind farm 112. In the wind farm 112 or in a controller (not shown here) of the wind farm 112, the certificate which has been imported via the interface 12 of the windfarm 112, is then checked for authenticity.

In addition, the interface 12 of the wind farm checks whether the certificate 28 is still valid, i.e. the validity period has not elapsed yet, and whether the turbine identifier stored in the certificate matches the turbine identifier of the windfarm. Given a valid validity period, a matching turbine identifier and an authentic certificate, the user 18 is then allowed control accesses to the windfarm 112 that relate to the control-access types stored in the certificate 28. The user 18 can thereby make a control access to the wind farm 112 via the mobile device 16.

If the power grid 32 to which the windfarm 112 is connected via a transformer 116 and a point of common coupling 118 is weak or unstable, for instance because all the electrical power generators connected to this grid are currently feeding only a small amount of power into the network, this is detected by the certification centre 10 by means of externally supplied parameters 36. A parameter 36 can be ascertained, for instance, by a system measurement or frequency measurement 38 of the power grid 32 to which the windfarm 112 is connected.

In addition, a weather database 39 is provided, from which the prevailing and forecast weather data is transferred to the certification centre and/or retrieved by the certification centre. According to other exemplary embodiments, the weather database 39 is a complete weather system for weather recording and forecasting.

If a user 18 now transfers a control-access type, which might be critical for the grid network 32, to the interface 20 for certificate generation in the processor 22, then a

critical control-access type of this kind is prohibited, because the control database 24 has been dynamically updated previously by the parameter 32 and as a result of which, critical control-access types that relate to the windfarms 112 in the region of the power grid 32 are identified categorically as prohibited.

In this last-mentioned case, the interface 20 does not issue the certificate 28 to the mobile device 16. Instead, the interface 20 issues a message to the mobile device 16 that such a control-access type is currently not possible.

Fig. 4 shows the sequence flow of an exemplary embodiment of the method. In the first step 40, a password, a user name, a required control-access type and a turbine identifier are transferred to an interface 20 of a certification centre 10. In the next step 42, the user, if registered in the certification centre 10 and the password and user name are correct, is authenticated and hence authorized for further communication with the certification centre 10. If an incorrect user name or an incorrect password has been entered, then access terminates in the step 44.

If user name and password agree with stored data in the control system 24, then in a next step 46, a check is made as to whether the control-access type is allowed for the authenticated user to the wind turbine 100 having the transferred turbine identifier. If the control-access type is not allowed for the user then the method terminates again in the step 44. If the control-access type and the selected wind turbine 100 is allowed for the user, then in a next step 46, the certification centre checks on the basis of the number of currently valid requested control accesses to wind farms in the same region, whether the requested control-access type is allowed. If this control-access type is not allowed, then the method terminates again in the step 44.

If the control-access type is currently allowed, then a certificate 28 is generated in a step 48, which certificate 28 comprises the user name, the turbine identifier, the

control-access type and a timestamp or validity period. The certificate 28 is then issued to a mobile device 16 of the user 18 in a step 50.

In the next step 52, the user authenticates himself with a wind turbine 100 using the mobile device 16, re-entering for this purpose a password and a user name via an interface 12 of a wind turbine 100. If the transferred user name and transferred password match the user name and password stored in the wind turbine, the user 18 is then authorized for read accesses. Otherwise the method terminates again in the step 44.

After successful authorization of the user 18 for read accesses, the mobile device 16 transfers the certificate 28 to the interface 12 of the wind turbine 100 in the step 54, and the user is authorized for the control accesses stored in the certificate if the turbine identifier in the certificate matches the turbine identifier of the wind turbine 100 and if the validity period has not expired yet.

In the step 56, the user is then allowed control accesses according to the control-access type(s) stored in the certificate 28, and the user 18 can then perform a control action. Once the control accesses have been performed, the method terminates in the step 44.

Patentkrav

1. Fremgangsmåde til autorisering af brugere (18) til styreadgange til mindst et vindenergianlæg (100) eller mindst en vindpark, omfattende trinnene:

- at autentisere og autentificere en bruger (18) ved hjælp af et certificeringssted (10),
- at overtage mindst en styreadgangstype ved hjælp af certificeringsstedet (10) fra den autentificerede bruger (18),
- at generere et elektronisk certifikat (28) med styreadgangstypen ved hjælp af certificeringsstedet (10) afhængigt af den overtagede styreadgangstype og/eller afhængigt af gemte adgangsrettigheder af den autentificerede bruger (18) til autentisering af styreadgange med styreadgangstypen på det mindst ene vindenergianlæg eller den mindst ene vindpark og
- at autentisere ved det mindst ene vindenergianlæg (100) eller den mindst ene vindpark med certifikatet (28) til udførelse af styreadgange med styreadgangstypen,

hvor

a) certifikatet (28) genereres med en gyldighedsperiode, og

et maksimalt samlet antal gemmes med et styresystem (24) til hver styreadgangstype, og

certifikater (28) kun genereres til en styreadgangstype, når antallet af de allerede tildelte certifikater (28), der på nuværende tidspunkt er gyldige på grund af deres gyldighedsperiode, ligger under det maksimale samlede antal eller

b) certifikatet (28) genereres med en gyldighedsperiode, og

et maksimalt antal pr. på forhånd defineret region gemmes med et styresystem (24) til hver styreadgangstype, og

certifikater (28) kun genereres til en styreadgangstype, når antallet af de til den region allerede tildelte certifikater (28), der på nuværende tidspunkt er gyldige på grund af deres gyldighedsperiode, ligger under det maksimale antal pr. på forhånd defineret region.

2. Fremgangsmåde ifølge krav 1, hvor certificeringsstedet (10) endvidere afhængigt af mindst et fastslået aktuelt eller prognosticeret parameter (32), omfattende en nettilstand, vejret eller et eller flere vindenergianlægs tilstand, genererer et certifikat (28).

3. Fremgangsmåde ifølge krav 1 eller 2, hvor en autorisering til en læseadgang af en bruger (18) sker ved certifikatuafhængig autentisering af en bruger (18) ved en grænseflade (12) af et vindenergianlæg (100) eller en vindpark.

4. Fremgangsmåde ifølge et af de foregående krav, hvor certifikatet (28) udlæses fra certificeringsstedet (10) til en computerenhed (16) med en grænseflade (20), og autentiseringen udføres med computerenheden (16) ved vindenergianlæggets (100) grænseflade (12) eller ved vindparken, og styreadgange til vindenergianlægget (100) eller vindparken udføres uafhængigt af certificeringsstedet (10).

5. Fremgangsmåde ifølge et af de foregående krav, hvor autentiseringen udføres med certificeringsstedet (10) ved vindenergianlæggets (100) grænseflade (12) eller ved vindparken og styreadgange til vindenergianlægget (100) eller vindparken.

6. Fremgangsmåde ifølge et af de foregående krav, hvor
certificeringsstedet (10) omfatter et styresystem (24), hvormed der er tilordnet hver især mindst en tilladt og/eller ikke tilladt styreadgangstype til en, flere eller alle registrerede brugere (18), og
certifikater (28) af en autentificeret bruger (18) med den overtagede styreadgangstype udelukkende genereres med certificeringsstedet (10) i det tilfælde, at den overtagede styreadgangstype er tilordnet i styresystemet (24) som tilladt for brugeren.

7. Certificeringssted til autorisering af brugere til styreadgange til mindst et vindenergianlæg eller mindst en vindpark, omfattende:
- en grænseflade (20) til autentisering og autentificering af en bruger (18) ved certificeringsstedet (10) og til overføring af mindst en styreadgangstype til certificeringsstedet (10) fra den autentificerede bruger (18),
- hvor certificeringsstedet (10) er indrettet til at generere et certifikat (28) med styreadgangstypen afhængigt af styreadgangstypen og/eller afhængigt af gemte adgangsrettigheder af den autentificerede bruger (18) til autentisering af styreadgange med styreadgangstypen på det mindst ene vindenergianlæg eller den mindst ene vindpark og
- hvor grænsefladen (20) er indrettet til at udlæse det elektroniske certifikat (28),
hvor
a) certificeringsstedet (10) er indrettet til at tildele en gyldighedsperiode til certifikaterne (28), og

et maksimalt samlet antal er gemt i et styresystem (24) for hver styreadgangstype, og

certificeringsstedet (10) er indrettet til kun at generere certifikater (28) til en styreadgangstype, når antallet af de tildelte certifikater (28) af denne styreadgangstype, der er gyldig på nuværende tidspunkt, ligger under det maksimale samlede antal, eller

b) certificeringsstedet (10) er indrettet til at tildele en gyldighedsperiode til certifikaterne (28), og

et maksimalt antal pr. på forhånd defineret region er gemt i styresystemet (24) for hver styreadgangstype, og

certificeringsstedet (10) er indrettet til kun at generere certifikater (28) til en styreadgangstype, når antallet af de tildelte certifikater (28) af denne styreadgangstype, der er gyldig for regionen på nuværende tidspunkt, ligger under regionens maksimale antal.

8. Certificeringssted ifølge krav 7, hvor certificeringsstedet (10) omfatter en yderligere grænseflade for at modtage parametre (36), omfattende aktuelle vejrdata og vejrprognoser eller aktuelle nettilstande og nettilstandsprognoser og tilpasse styresystemet (24) afhængigt af disse parametre (36).

9. Certificeringssted ifølge krav 7 eller 8, hvor

certificeringsstedet (10) omfatter styresystemet (24), og der med styresystemet (24) er tilordnet hver især mindst en tilladt og/eller ikke tilladt styreadgangstype til en, flere eller alle registrerede brugere (18), og

certificeringsstedet (10) er indrettet til at generere certifikater (28) af en autentificeret bruger (18) i det tilfælde, at den af brugeren (18) overtagede styreadgangstype er tilordnet i styresystemet (24) som tilladt for brugeren (18).

10. Certificeringssted ifølge et af kravene 7 til 9, hvor

certificeringsstedets (10) grænseflade (20) er indrettet til udover styreadgangstypen at overtage mindst en anlægsidentifikator af mindst et vindenergianlæg (100), der skal styres, eller mindst en vindpark, der skal styres, ved hjælp af grænsefladen (20), og

certificeringsstedet (10) er indrettet til at generere det elektroniske certifikat (28)

med certificeringsstedet (10) afhængigt af styreadgangstypen og anlægsidentifikatoren og/eller gemte adgangsrettigheder af den autentificerede bruger (18).

11. System med en grænseflade til mindst et vindenergianlæg (100) eller mindst en vindpark, hvor
grænsefladen (12) er indrettet til at modtage et certifikat (28) og afhængigt af certifikatet (28) at tillade mindst en styreadgang af en styreadgangstype, eller
grænsefladen (12) er indrettet til at udlæse en styreadgangstype af certifikatet (28), der er gemt i certifikatet (28), og kun tillade styreadgange med den gemte styreadgangstype og
et certificeringssted ifølge et af kravene 7 til 10.

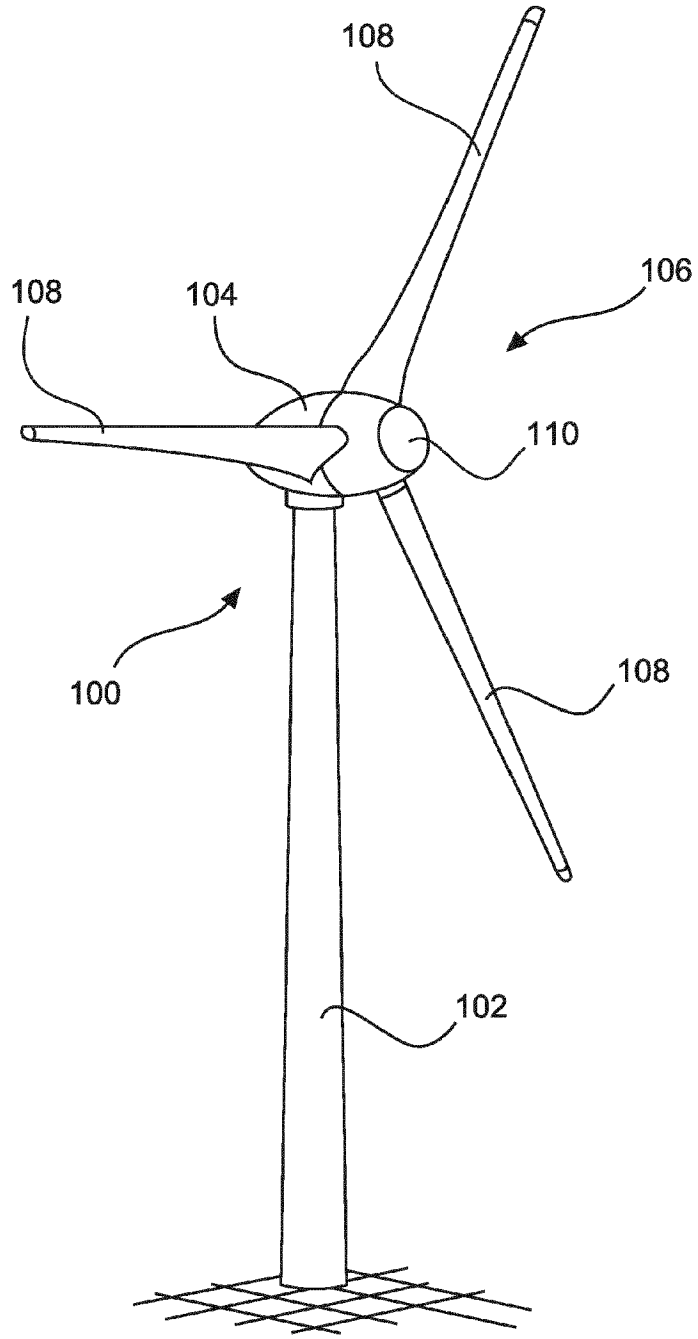

Fig. 1

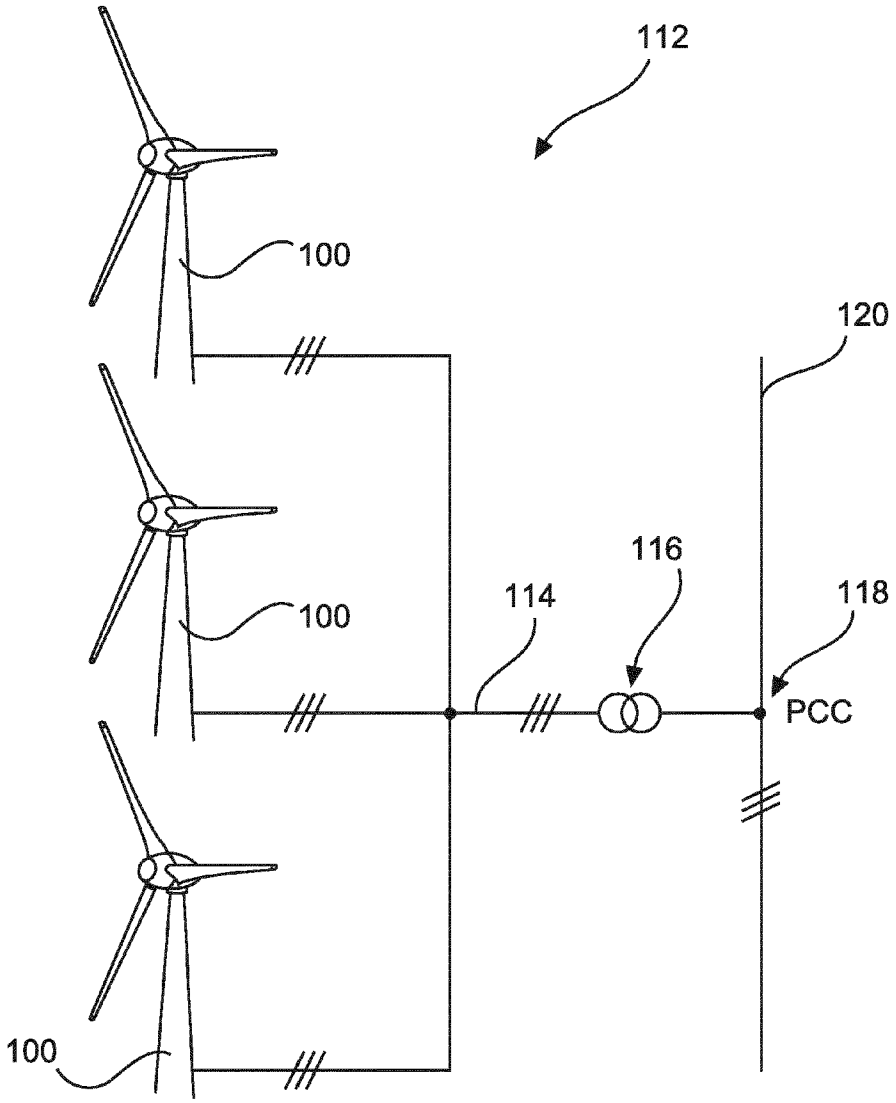

Fig. 2

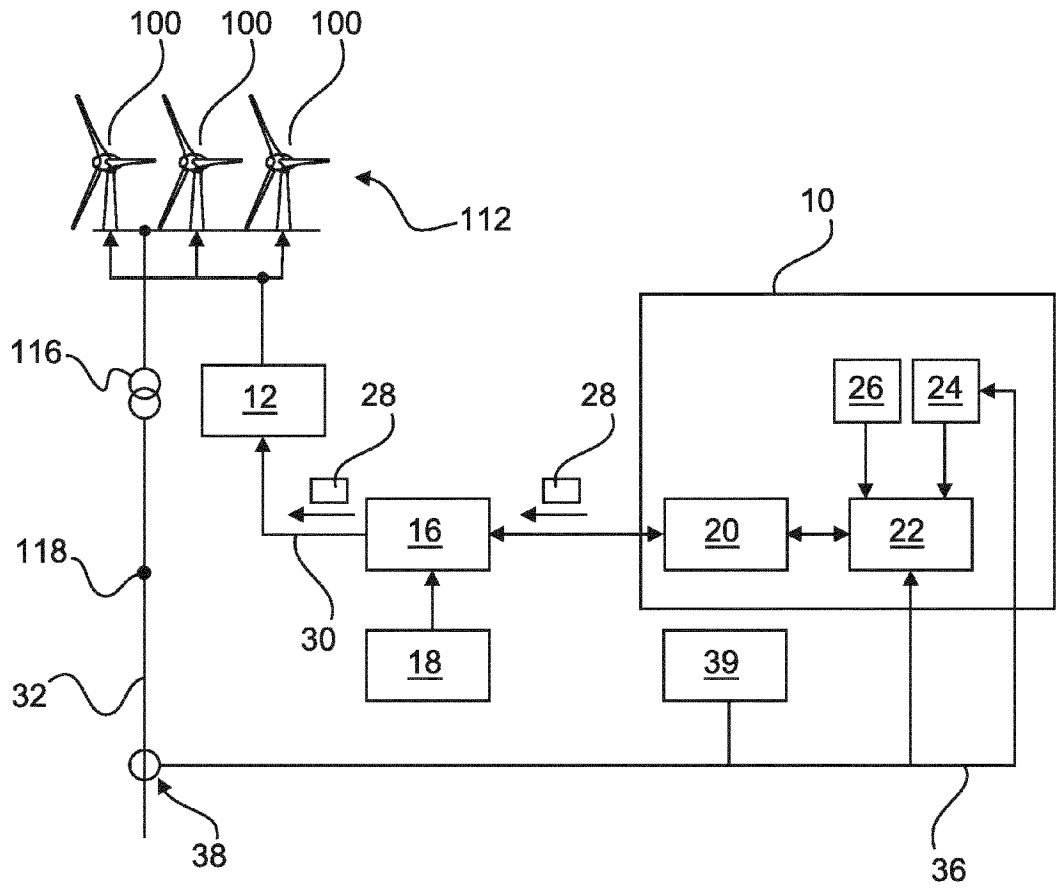

Fig. 3

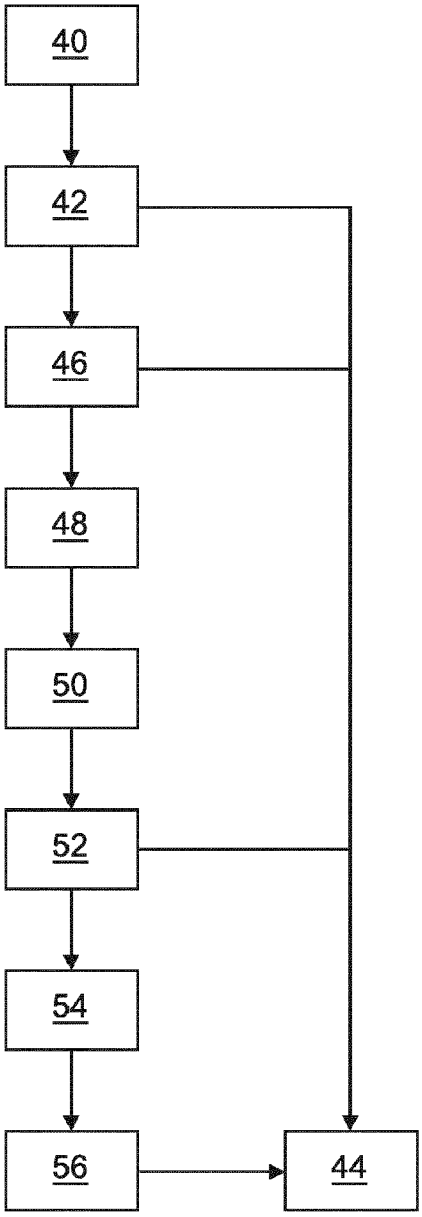

Fig. 4