PROCEDURE AND SYSTEM FOR RELIABLE AND SAFE IDENTIFICATION OF A CONTRACTING PARTY

FIELD OF THE INVENTION

The present invention relates to a procedure as defined in the preamble of claim 1 and to a system as defined in the preamble of claim 7 for reliable and safe identification of a contracting party in various contracts, deeds, offers, and deals requiring authentication by a notary and in other corresponding applications.

BACKGROUND OF THE INVENTION

In the making of certain agreements between two juridical persons, it is necessary to ascertain the identity of the contracting parties. In real estate deals, offers and various other agreements requiring authentication by a notary, the parties are identified by a notary public, notary or other authorised person. For this, it is generally necessary for the contracting parties to be simultaneously present at a meeting with a third person in order to be identified by the latter. This involves practical problems because either the contracting parties have to go e.g. to a notary themselves or a notary must visit the contracting parties. In any case, confirming an agreement by this method is difficult and time consuming.

In other words, a notariate, notary public or a corresponding functionary verifies that the contracting party really is the person he/she purports to be and in whose name he/she is signing the agreement. There is no known identification method based on an electronic signature. However, identifying a person on the basis of an electronic signature would make things considerably easier because in this case the electronic signature could be sent over a telecommunica-

tion network to a notariate, a notary public or a reliable third party for verification.

BRIEF DESCRIPTION OF THE INVENTION

The object of the present invention is to eliminate or at least to significantly reduce the problems described above.

A specific object of the present invention is to disclose a new type of method and procedure for reliable and safe identification of contracting parties. A further object of the invention is to disclose a system for reliably and acceptably implementing the identification of contracting parties as stipulated by law by making use of a telecommunication network.

As for the features characteristic of the invention, reference is made to the claims.

In the procedure of the invention for reliable and safe identification of contracting parties via a telecommunication network, the telecommunication network used may be a mobile communication network, public telephone network, data network or a combination of these. Correspondingly, the terminals used in the procedure may be any terminal devices compatible with the telecommunication network.

According to the invention, a first contracting party is authenticated by means of a first terminal. The authentication may be accomplished using any method. The essential point is that the authentication is implemented in conformity with the standards applying to electronic signature. After authentication, a verification request is sent to a reliable third party for verification of the identity of the first contracting party. The verification request is preferably sent via the first terminal, which is also used for the authentication. Finally, the identity of the first party is confirmed for a second party by sending the

second party an identification message given by the reliable third party.

The invention makes it possible to implement a service corresponding to a notarial service in a flexible and advantageous manner.

Moreover, the invention allows easy introduction of electronic signature in conjunction with the use of mobile telephones and other suitable terminal devices. This makes it possible to use a mobile telephone as an instrument of payment, as a credit card or equivalent.

The second party, e.g. in the case of a real estate deal, is identified in the same way as the first party. The second party is also authenticated by means of a second terminal. However, if desirable, in some cases the second party may use the first party's first terminal for his/her own identification. In this case, the second party uses his/her own subscription or other information individualising the second party in conjunction with the first terminal. Another possibility is to establish separate service points provided with terminal equipment for subscriber identification, which is utilised by both contracting parties for giving an electronic sample signature and for identification of the other party.

In a preferred embodiment, the second contracting party is identified after the second party has received an identification and verification message concerning the first contracting party. Identifying the second party is useless unless the first party can be reliably identified.

To allow the contract to be confirmed and the identification inquiries regarding the parties to be verified and traced, the verification request is saved to a verification database. This verification database may be a database server managed by a reliable party, such as a public authority. The record in question

preferably contains information indicating the party who sent the verification request, the party to whom the verification and identification message is sent, the matter or contract to which the verification is related and the point of time of the event. The same information is preferably comprised in the verification requests sent by the first and second contracting parties.

The system of the invention for reliable and safe identification of contracting parties comprises a telecommunication network and a terminal device connected to it and compatible with it. The telecommunication network may be a combination of a mobile communication network and a telephone network and the terminal device may be a mobile telephone. The telecommunication network may also be a data network, in which case the terminal device is preferably a computer or other terminal compatible with the data network. According to the invention, the system comprises means connected to a first terminal for authentication of a first contracting party. The system also comprises a reliable database apparatus or a corresponding application server, to which the verification request of the first contracting party is sent. This server or database may be under the management of a third party known to be reliable, and it may be connected e.g. via a data-secure link to the telecommunication network used for the operations. The database or server in question preferably comprises means for sending a verification and identification message to the second contracting party on the basis of identification by the reliable third party.

Correspondingly, the system can be used to identify and verify the second contracting party's identity for the first contracting party. It is also possible for each contracting party to be identified by a different reliable third party. This may be pos-

sible in cases where the contracting parties are citizens of different countries or otherwise have established their identification data with different third parties.

As to the advantages of the system of the invention, reference is made to the advantages of the procedure of the invention.

In a preferred embodiment of the present invention, the system comprises a verification database server connected to an identification database server of a reliable third party. In this case, a record concerning the verification request and verification can be saved by the identification database server to allow examination and tracing at a later time.

In the following, the invention will be described by the aid of a few examples of its preferred embodiments with reference to the attached drawing, wherein

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 represents a preferred system according to the present invention; and

Fig. 2 presents a block diagram representing an embodiment of the procedure of the invention.

DETAILED DESCRIPTION THE DRAWINGS

The system presented in Fig. 1 comprises a telecommunication network 1, which in this example is a combination of a mobile telephone network and the public telephone network. In addition, the system involves the use of two terminals TE1, TE2, which are mobile stations and connected to a mobile communication network GSM and further to the public telephone network PSTN. The mobile stations are consistent with the current GSM standard, but, as is obvious to the skilled person, other applicable mobile stations can

also be used. Furthermore, connected to the telecommunication network 1 is an identification and verification system TTP of a reliable third party. This identification and verification system comprises a first verification server TTP1 and a second verification server TTP2. These servers are connected via a suitable link to the telecommunication network, over which they communicate with the terminals TE1, TE2. Moreover, the verification servers TTP1 and TTP2 are connected to a central storage server TTP3, to which the verification servers write records concerning the verification and identification actions they have carried out.

Next, referring to Fig. 2, a preferred embodiment of the procedure of the invention will be described. In this example, a first and a second contracting party are making a deal which requires verification of the identity of the contracting parties by a notary public. In the procedure of the invention, the first contracting party is first authenticated using his/her electronic signature, which may consist of e.g. a PIN code in a mobile station. The PIN code must be entered when the mobile station TE1 is activated. Therefore, upon receiving the correct PIN code, a mobile station belonging to a subscriber can send an electronic signature message to an address selected by the subscriber. Authentication is represented by block 21. Next, the first contracting party sends a verification request to a verification server TTP1, block 22. The verification server receives the subscriber's request and checks the validity of the electronic signature supplied by the subscriber by comparing it with its own information about the subscriber, block 23. When the verification server discovers the subscriber's identity and finds that the identification was successful, it sends an identification and verification message to the second contracting party to a

subscriber number or terminal device indicated by the first contracting party in his/her verification request message. If it is detected in block 23 that the subscriber's electronic signature is wrong or the subscriber is not identified, the procedure goes on to block 24 and the identification process is ended. After the verification and identification message, block 25, has been sent to the other party, a record of the identification event is saved to a storage database TTP3, block 26.

Once the second contracting party has received a confirmation of the identity of the first contracting party, a verification procedure for establishing the identity of the second contracting party is started. First, the second party is authenticated, whereupon he/she sends a confirmation and verification request to his/her own reliable third party, in this example to verification server TTP2, block 27. Next, verification server TTP2 verifies the identity of the second contracting party, block 28, and if the identity is found to be right, then an identification message is sent to the first contracting party, block 29. If the identification of the second contracting party in block 28 fails, then the procedure goes on to block 29 and the identification process is ended. After the identification message has been sent to the first contracting party, a record concerning the identification of the second party is added to the storage database, block 30. Both parties have now been reliably identified, and both parties are informed about the fact. In addition, stored in the storage database is information regarding the identification of the parties and generally also information regarding the event to which the identification is related. This makes it possible to verify and ascertain the identity of the parties at a later time, and also to ascertain that it

has been verified in conjunction with the signing of the deed.

The invention is not restricted to the embodiments described above, but many variations are possible within the scope of protection of the claims.

* C L M S *

CLAIMS

1. Procedure for reliable and safe identification of contracting parties via a telecommunication network, characterised in that

a first contracting party is authenticated by means of a first terminal;

a verification request is sent to a third party for verification of the identity of the first contracting party by means of the first terminal; and

a confirmation of the identity of the first contracting party is sent to a second party on the basis of identification by the third party.

2. Procedure as defined in claim 1, characterised in that

the second contracting party is authenticated by means of a second terminal;

a verification request is sent to a third party for verification of the identity of the second contracting party by means of the second terminal; and

a confirmation of the identity of the second contracting party is sent to the first contracting party on the basis of identification by the third party.

3. Procedure as defined in claim 1, characterised in that a procedure for identification of the second party is started after the second party has received the confirmation of the identity of the first party.

4. Procedure as defined in any one of claims 1 - 3, characterised in that, after a confirmation message regarding the identity of a contracting party has been sent, a record is written to a verification database.

5. Procedure as defined in any one of claims 1 - 4, characterised in that the verification request sent by a contracting party to a third party contains information indicating the party to

THIS SHEET HAS BEEN REPLACED

whom the identification message is sent, the matter or contract to which the verification is related and the point of time of the verification.

6. Procedure as defined in any one of claims 1 - 5, characterised in that the record written to the verification database, which is managed by a reliable third party, contains information indicating the party to whom the verification message has been sent, the matter or contract to which the verification is related and the point of time of the verification.

7. System for reliable and safe identification of contracting parties in a telecommunication network comprising a mobile communication network, a public telephone or data network and at least one terminal device (TE1), characterised in that the system comprises

means for authentication of a first contracting party;

a verification database (TTP1) which is managed by a third party and by means of which the identity of the first contracting party is verified; and that

the verification database comprises means for sending a verification message to a second contracting party on the basis of identification by the third party.

8. System as defined in claim 7, characterised in that the system comprises a second verification database (TTP2) managed by the third party for verification of the identity of the second contracting party.

9. System as defined in claim 7 or 8, characterised in that the system comprises a storage database (TTP3), which is connected to the first and second verification databases (TTP1, TTP2)

THIS SHEET HAS BEEN REPLACED

to receive verification records and which is managed by a reliable third party.

10. System as defined in any one of claims 7 - 9, characterised in that the first and second verification databases (TTP1, TTP2) are managed by a reliable third party.



THIS SHEET HAS BEEN REPLACED