NTT
NIPPON TELEGRAPH AND TELEPHONE CORPORATION

NEWS RELEASE

April 25, 2001

The Development of Japan's First Electronic Bidding System Capable of Proving the Authenticity of a Transaction to Third Parties

- To be adopted by Yokosuka City as first electronic bidding system in Japanese local govermants -

Nippon Telegraph And Telephone Corporation (NTT) have developed an electronic bidding system capable of proving the authenticity (or falsification) of bidding transactions even to third parties. The system, developed by NTT Service Integration Laboratories (NTT-SI Labs.), incorporates the electronic notary system developed by NTT Information Sharing Platform Laboratories (NTT-PF Labs.). It is the first development in Japan of an electronic bidding system capable of proving the fairness of the bidding process on the Internet. Yokosuka City will adopt the new system this September.

In response to the "Electronic Government" initiative, the national and local government will introduce electronic bidding for procurements and public works. Because the process of handling bidding was time-consuming and costly, some electronic systems have already been announced, but they only attempted to streamline the process by using the Internet and fell short of allowing verification of fairness of the bidding process.

In the new system, an electronic notary system (server) stands between the bidders and the orderer and, like a notary public, records and stores the bidding information exchanged between them - a feature that distinguishes the system from other similar systems. After bid opening, the information stored in the electronic notary server can be made public so that even third parties can verify the fairness of the bidding process.

The new system also uses a hash system developed by NTT, instead of encryption, for the electronic bidding protocol --equivalent to an envelope in conventional form of bidding - to assure confidentiality of bidding information up to bid opening. This eliminates the cumbersome management of encryption keys.

Starting with Yokosuka City, this system will be sold as a product by NTT operating companies.

< Main Features > [See Figure 1]

1) Features as an electronic bidding system

Since the complete bidding process flow from invitation of tender, bidding to bid opening can be performed on the Internet (through a browser), both the bidders and the orderer benefit from greatly increased efficiency. Furthermore, since the only technical requirement is the capability to access the Internet, more bidders can participate in bid invitations thereby deterring people from bid-rigging.

2) Verification of the fairness through an electronic notary system

Since an electronic notary system (notary server) obtains and maintains all bid records (bid application form, bidding form, etc.) between the bidders and the orderer, the notary server itself can serve as a "Trusted Third Party (TTP)" and provide proof similar to content-certified mail or delivery-certified mail.
Therefore, unlike conventional paper-based bidding or other electronic bidding systems, in which all one can do is blindly trust the information made public by the orderer, even third parties can determine the fairness of the bidding process from the records stored in the notary server.

3) Electronic bidding protocol eliminates the need for operation and management of encryption keys

Other electronic bidding systems use encryption involving the distributed management of common keys in their electronic bidding protocol. Such management requires the generation and management of encryption and decryption keys for individual bidders and constitutes a considerable management load.

The new bidding system uses the Public Hash-Value Electronic Bidding Protocol (described later) developed by NTT that eliminates the need for key management, resulting in the ease of using the system.

< **Technical points** > [See Figure 2]

The Public Hash-Value Electronic Bidding Protocol, authentication system (Trust-CANP *1), and notary system (Trust-CYNOS *2) adopted in this system are all methods or products developed in NTT-PF Labs.

In particular, the Public Hash-Value Electronic Bidding Protocol is one of the key technologies in the verification of the authenticity of bids.

(What is hash?)

Hash technology compresses electronic data into a certain size by using a special algorithm (calculation). If the original electronic data is considered plain text, the specific-length message digest (hash value) derived by hash calculation is equivalent to an encrypted text.

The hash used in the latest encryption technology meets two requirements: it does not allow the original electronic data to be reconstructed from the hash value; nor does it allow the same hash value to be generated from different data (i.e., any alteration will change the hash value).

(What is the Public Hash-Value Electronic Bidding Protocol?)

NTT developed this protocol by applying the hash technology to the electronic bidding protocol.

Specifically, the electronic bidding procedure is as follows:

1) A bidder enters its bid price through the electronic bidding program (browser) of this system. The price is automatically calculated into a hash value. Since, in practice, the price data is too short, it is multiplied by a random number before a hash calculation is made. This random number is automatically generated and stored in the electronic bidding program. It is impossible to reconstruct the original data of bid price or the random number from the hash value.

2) The bidder sends the hash value to the orderer through the notary server.

3) The orderer posts the hash value in a Web page publicizing bidding information. At this point, the bidder's application number is published instead of the bidder's name. Its bid price is not published on the Web page. People browsing the Web page can only see the number of bids (i.e., someone has entered the bidding).

4) At the time of bid opening, all bidders are requested to send their bid price as well as the random number in a plain text, instead of the opening of the envelopes or decryption of coded data. The bid prices collected in plain text are compared electronically and the successful bidder is selected. Next, it is necessary to verify that the price in the plain text is the same as the bid price entered at the time of bid application. To do so, the bid price and random number sent from the bidder are computed into a hash value by the electronic bidding program, and the resulting value is compared with the hash value submitted earlier.

5) The contract price, the application number, and the random number are posted on the orderer's Web page. Third parties can make a hash calculation on the electronic bidding program available on the page to verify that the bid price is authentic.

< Glossary >

*1 Trust-CANP
An electronic authentication system developed in NTT-PF Labs. Electronic authentication systems issue public key certificates (equivalent to a certificate of seal impression in the real world) used for authentication of a person on the network. The electronic authentication system developed in NTT supports a number of encryption algorithms, including the ones domestically developed, and is characterized by its ability for real-time validation of certificates.

*2 Trust-CYNOS
An electronic notary system developed in NTT-PF Labs. Electronic notary systems are used for proof provided by a third party on the facts of electronic transactions in order to avoid such problems as alteration, masquerading, or repudiation. The service they provide is therefore equivalent to notary offices or content-certified mail in the real world. The electronic notary system developed by NTT features strict user authentication and proof of facts achieved through working with the electronic authentication system.

- (Figure 1) Use of Notary to prove facts
- (Figure 2) Electronic Bidding Protocol Using Hash

For inquiries related to this matter:
NTT Information Sharing Laboratory Group
Planning Department, Public Relations: Kurashima, Sano, Ikeda
TEL: 0422-59-3663
E-mail: koho@mail.rdc.ntt.co.jp

NTT NEWS RELEASE