17

Auctioning by Satellite using Trusted Third Party Security Services

P. Sanders [a], S. Rhodes [b] and A. Patel [c]

[a,b] Network Research Group, University of Plymouth,
Drake Circus, Plymouth, PL4 8AA, UK. email: psanders@soc.plym.ac.uk

[c] University College Dublin, Belfield, Dublin 4, Ireland.

1. Abstract.

Auctioning of livestock by satellite broadcast is a new and rapidly expanding service within Europe. The concept has enormous potential for further expansion into other agricultural commodities and other areas, such as marine equipment, fine art, large machinery, vehicles, etc. It updates the age-old method of competitive buying and selling, by incorporating forms of teleworking and electronic commerce into a system that reduces the amount of travelling and movement of goods, especially important when operating on a larger scale.

Such a potentially pan-European open service, presents a number of security problems to both the users and service operators. The need to ensure the real-time integrity of data and purchaser decisions, the anonymity of authenticated potential purchasers, with complete non-repudiation of their activities, results in perhaps a unique combination of security requirements for a single application service. It is considered that these requirements can be solved efficiently and effectively by the use of Electronic Signatures (ES) and Trusted Third Party (TTP) security services technology.

The paper describes the application service to set the scene, the perceived threats and vulnerabilities of the system when operating on a large scale, and the general design and use of the TTP services, with smart card operation, that meets the security requirements of the auctioning activities for local and pan-European operations.

It incorporates a hierarchical logical network of TTP centres, based on the X509 recommendations, that is suitable for many other types of business applications and suggests the use of EDI and EFT services with multimedia cataloguing for the auction previews. It concludes with the necessity for the early implementation of such a general network and TTP services.

J. H. P. Eloff et al. (eds.), *Information Security — the Next Decade*

2. Introduction.

The advent of satellite communication systems for business use has created the opportunity for a wide range of commodities and services to be traded by auction on a pan-European or global basis. Selling by satellite enables high value products, that can remain in situ, to be presented to a wider market place through a diverse, increased purchaser base, that is able to participate, without leaving their own locality, through the use of satellite transmitted television and the public telephone network.

In addition to auctions a variety of other applications are possible, which range from the operation of inter-state lotteries and general trading. However, whatever the commodity traded, to enable the vendors, buyers and auction houses to participate with complete confidence, the operation of a secure system in the areas of authentication, non-repudiation of contract and settlement of accounts, with corresponding levels of integrity and general confidentiality is required.

One of the operators of satellite systems is Central Livestock Auction Satellite Sales, CLASS, which provides the only livestock auctioning system in operation in Europe at the present time. Trading since October 1992 it brings to the market place a range of cattle, sheep and pigs, for slaughter as well as for rearing purposes. Both the buyers and vendors of the livestock find this innovative form of electronic auctioning very acceptable and effective, as they can actually see what is being bought as well as taking part in the normal live auction activities.

The system allows livestock vendors to achieve the best prices from a standard competitive, dead-weight or live-weight auction whilst keeping their costs down and minimising the stress and potential health risks that may be incurred by stock when travelling to, and being sold in, a traditional livestock market. Buyers also benefit as any amount of stock may be purchased quickly and cost effectively, (up to 90 lots per hour are sold) in large sized lots, from an office or at home merely by using a telephone and a television equipped with a satellite receiver.

A network of Primary Centres, (twenty at present), located around auctioneers, livestock corporations and large farmers have been set up to provide a local service throughout the UK and in parts of Ireland, with future expansion planned for much of Northern Europe. The concept of large-scale auctioning by satellite is now being broadened into other commodity areas.

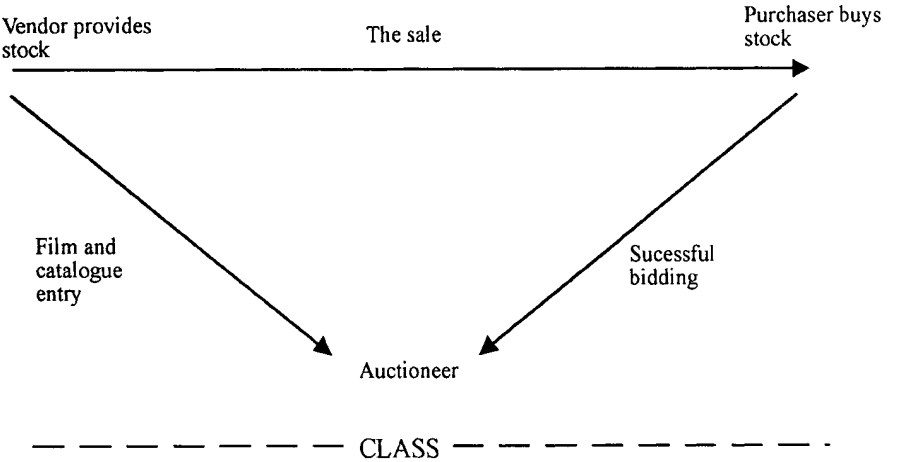

Figure 1. The auction process.

The auction process and associated activities can be conveniently divided into three stages:- pre-auction, the auction itself, and post-auction.

2. The Existing Satellite Auctioning System.

2.1 Pre-Auction.

Before the auctioning process can take place, a number of activities and prior arrangements must be carried out. All potential purchasers of stock who wish to use the auctioning service and take part in future auctions must be registered within the CLASS system. This is achieved by obtaining a credit rating for the interested party, which is used to determine the credit limit that is allowed at individual Primary Centres, in association with the management that operates that Centre. The potential purchaser is then issued with a buyer reference number that allows access to the auction catalogue as well as the actual auction itself.

A potential vendor of stock who wishes to sell his animals using the satellite system, instigates a visit by a Fieldsman, usually from their local Primary Centre, who films the livestock in appropriate groups, and completes a livestock (cattle) entry form (CEF) which sets out details of the stock. This is signed by the vendor as being correct, as well as indicating the intention of placing those animals for auction. The effective identification of livestock by ear tag reference numbers is a very important issue at present within the EU, relating to their traceability for possible subsidy fraud and disease.

The Fieldsman sends the film and CEF to the CLASS headquarters and provides a copy for his Primary Centre. Primary Centres are allocated the same block of lot numbers in the auction each week to help potential purchasers quickly locate stock in their district, and to allow the Centres to make up the lots from their set of CEFs for the catalogue. Access to the catalogue central computer is provided by individual PINs for the Primary Centres, and for all registered potential purchasers on the system. The software allows the potential purchasers to enter their own particular stock requirements for a search and identification of all lots that meet their criteria, and for printing out of their own personal catalogues.

At CLASS headquarters the individual films are edited to the required transmission length, combined, and graphics added, detailing the lot number, the number of animals in the lot, the breed and average weight. The integrated film is transmitted by satellite at a pre-advertsed time prior to the auction, as a preview programme, complete with a full descriptive commentary on each lot.

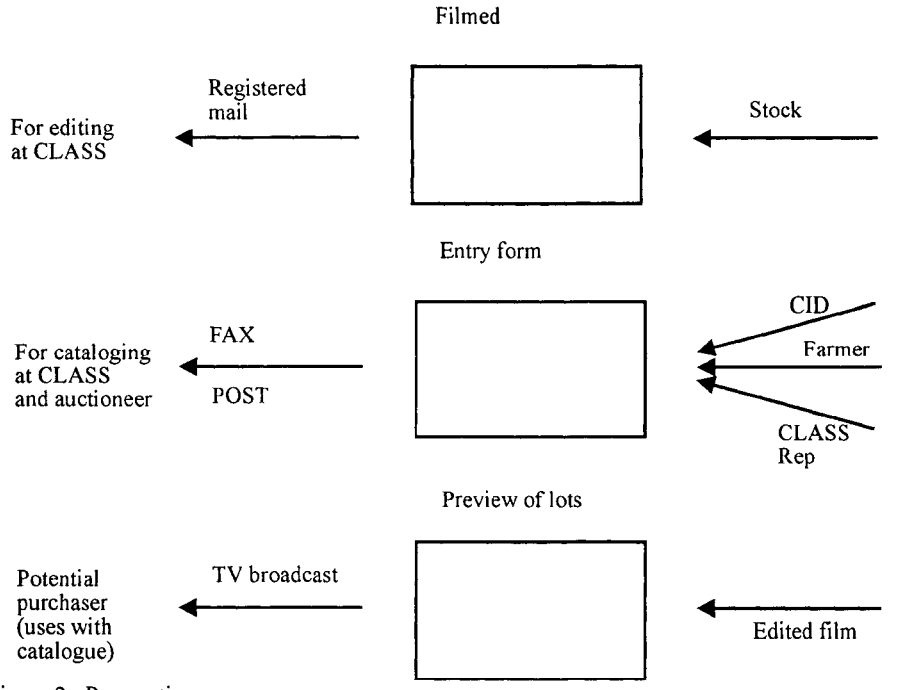

Figure 2. Pre-auction.

2.2 The auction.

A potential purchaser telephones the studio at the beginning or during the auction period and is answered by one of the numbered bid relayers. His buyer reference number and

PIN are checked against a current list of registered buyers, and when the relayer is satisfied, an auction buyer number is allocated to the potential purchaser for that session with that relayer. The potential purchaser informs his bid relayer each time he wishes to bid for a particular lot. The bottom third of the television screen shows the bid relayers, and as they are constantly on screen, the potential purchasers know, by watching the bid relayers raise their arms when instructed, that they are reacting to their instructions, thereby enabling the potential purchaser to bid with total confidence. As each bid is accepted the new bid price is displayed on the screen, and the number of the bid relayer with the final bid is announced by the auctioneer prior to the hammer falling. As each prospective purchaser drops out their final bid is entered by their bid relayer on a Responders Bid List (RBL) with an indication if the bid was successful. These records are used to arbitrate any dispute after the auction has ended. A clerk in the studio enters the prices onto the screen as the bidding takes place and records the final purchase price of the lot together with the buyer weekly reference number of the successful purchaser.

Registered purchasers can enter the auction session from any physical location as long as they have access to the PSTN. Generally access is made from farms, abattoirs, Primary Centres and hotels. Remote auctioneer relayers or sub-auctioneers at some of the Primary Centres are used to convey bids from farmers within auction rooms to the bid relayers at the studio. The sub-auctioneer is then held responsible for his relaying activities at these Centres.

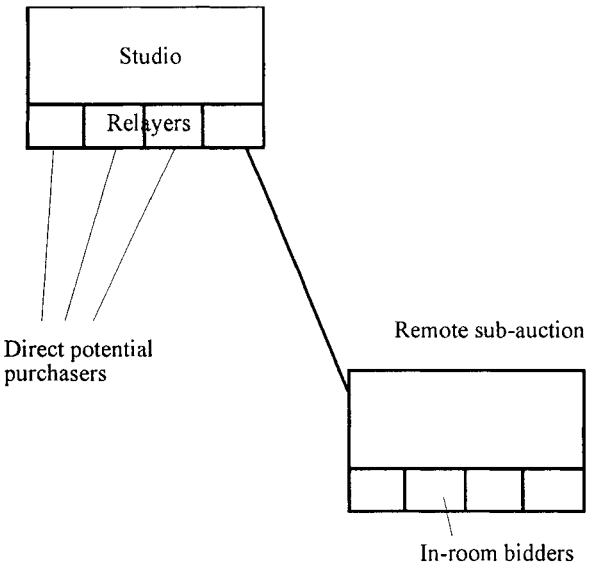

Figure 3. The sub-auction.

2.3 Post auction.

At the end of the auction, CLASS headquarters send out an invoice pro-forma to each successful purchaser indicating the lots purchased at that auction session, with the bid price per kilo for the live or dead-weight stock.

For live-weight stock, the animals are either weighed at a convenient public weighbridge or at a Collection Centre, en route to their destination. The dead-weight carcass weights are produced by the abattoirs, which are certified by the Meat & Livestock Commission, after the animals are killed and 'dressed' to the required standard. The weightsheets are used to produce invoices that show the weights of the animals, the bid price and the final amount due. The Title to the animals is transferred at the drop of the hammer, but the vendor retains responsibility for the welfare of the animals until they are collected.

A copy of the invoice is sent to the appropriate Primary Centre, from where the lot originated and payment is made by this Centre to the vendor within 7 days of the stock collection. On payment to CLASS by the purchaser, the Primary Centre is reimbursed for its initial vendor outlay. There are no problems with the purchaser payment, as the money is guaranteed by a credit scheme.

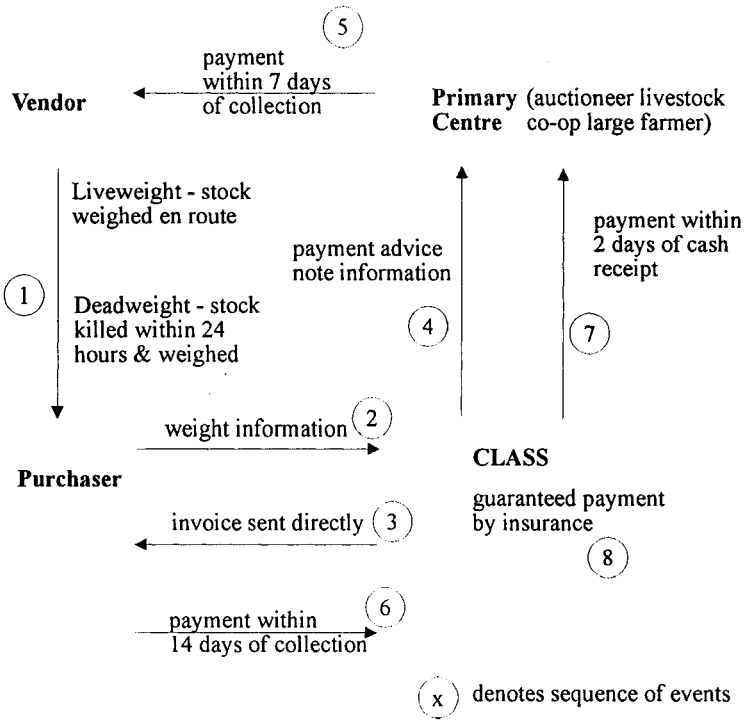

Figure 4. Information flows.

3. Security Requirements.

A basic risk analysis investigation of the auctioning system and discussions with a comprehensive selection of people involved in the auctioning operations, allowed the security requirements of the existing system and the proposed extended system to be determined.

A relatively simple blocking attack by competitors during an auction, and to a lesser extent on the catalogue, could considerably affect customer confidence. The probability of such attacks occurring increases as the system grows. The adequate authentication of all users of the system, plus access limitation with appropriate privileges to the catalogue and to the auction itself, with high integrity of much of the data used was considered essential. The non-repudiation of the actual sale transaction was deemed paramount. There is an inherent operational anonymity in the auctioning process by the employment of bid-relayers which satisfied the vendors and purchasers.

The identification and ownership of the stock, as well as the correctness of the sale information and its operation was particularly important to the Primary Centres. The main requirements of the users were for a simple system that was reliable and operated correctly. As at present, many users wish to enter the system and within one or two minutes, take part in the auctioning process. A fast response, real-time system was considered very important and the use of smart card electronic signature (ES) systems was deemed acceptable.

At present the system is limited mainly to Primary Centres and purchasers in the UK and Ireland, but they have a few vendors in France and Holland. The system operates very satisfactorily with no major security problems to date, but there is a substantial amount of personal knowledge and familiarity with the users of the system.

Operating within a pan-European or global environment with a range of commodities and other subject areas raises the strong possibility of dealing with unknown parties. All parties to a transaction must be fully authenticated for the application service provider and users to have confidence in the system. This lends itself to the transaction services being certified by an 'un-connected' third party to provide a level playing field irrespective of the location, size or reputation of the parties involved. In an auction environment this scenario is likely to be more common than in other trading situations and thus the ability to be able to trade immediately, but securely, with 'unknown' parties via a mutually trusted third party (TTP) is a paramount requirement. The standing of this third party will be dependant on, in the main, the quality of self regulatory practices, including the monitoring and audit control procedures of technical practices as is operated within a legal framework backed by appropriate statutes.

Whilst the number of transactions may be low, in a comparative sense, the potential high value of each transaction brings a commensurate need for high authentication and integrity. The primary service of the TTP in this respect is the preparatory authorisations prior to the auction, i.e. prior to the transaction, authorised entry into, and participation during, the auction and verification of the transaction, i.e. the actual completed sale. Therefore, included within the services provided by the TTP in an auction situation will be a need for authentication of entry, certification and authorisation of participants plus certification of correctness, time-stamping and transaction copy services, the latter three being of particular interest when linked to the recording of the auction, which will form part of the record keeping and information storage system.

4. The ES / TTP service requirements.

The auctioning application presents four main areas where ES / N-TTP services are directly required:

- The authentication of the vendor and fieldsman, and the signing of the cattle entry form (CEF) as the intention of selling by the auctioning process.

- The authentication with access control for writing to and reading from the auction catalogue.

- The authentication with access control to the actual auction itself.

- The signing of the sale contract using the electronic signature on individual lots and so ensuring non-repudiation in a court of law.

Other potential areas, such as EDI, EFT and animal registration services, that can indirectly make use of the proposed security features. The actual individual services required from the ES / N-TTP in the above areas, can be defined as:

- NAME REFERRAL - Referral of local TTP Distinguished Names, DNs.

- CERTIFICATE CREATION - Creation and certification (signing) of X.500 User Certificates, UCs.

- CERTIFICATION DISTRIBUTION - Distribution and management (including distribution of revocation lists) of X.500 UCs.

- TRANSACTION LOGGING - Arbitrated Digital Signature, ADS service to provide record of, and increase confidence in, user transactions.

These can be provided on a European scale from existing COST products, with a few modifications to meet the particular interface requirements of the auctioning application. All the necessary security services provided by these products are based on smart card technology and a hierarchical infrastructure of TTPs operating at national and international levels. A full and thorough explanation of the TTP infrastructure, its operations and the services provided is given in Refs. 2 and 3.

5. The Enhanced Auctioning System.

In order to provide this level of security to all parties using the system, additional services must be built into the application and supported by the TTP network. The following describes the suggested modifications to the existing arrangement to meet the requirements. The studio and satellite aspects are not affected, but additional equipment is required by other participants in order to take part in the enhanced auctioning system. All potential purchasers require a standard PC with smart card reader, and access to an international data network as well as to the PSTN. The mode of access to the data network will depend on the availability of local services. In this respect, the use of the ISDN system seems ideally appropriate where it is available, otherwise modem access must be used with a separate line or channel on the PSTN.

An access unit, AU, (front-end security server) at the studio provides for the automatic authentication of all users, access control, distribution of telephone and session identification numbers, the sale confirmation, and ensures non-repudiation of transactions using the TTP infrastructure. The basic arrangement is shown in Figure 5. With the increased size of the overall system, it is assumed that an increasing use of remote sub-auctioneers will be required in a hierarchical arrangement to limit the number of relayers in the studio and to provide facilities for limited auctioning in regions and areas of individual countries, as shown in Figure 6.

5.1 Overview.

Each system user, including potential purchasers, major vendors, sub-auctioneers and fieldsmen must have their own individual smart card, containing their RSA secret key, and their X.500 Distinguished Name, DN, which uniquely identifies them. The DN indicates which TTP, within the TTP network, that user has been registered with, and hence the location of the public key which is contained in the user's X.500 User Certificate, UC.

Each user terminal (ISDN or modem based) must be supplied with the relevant software that allows the smart card to be used with the appropriate operational protocols for the enhanced system. The workstation is initialised with the Distinguished Name, DN of its 'local TTP' (a preferential order of DNs are likely for a backup facility) to provide access into the TTP network. This arrangement of TTP 'domains of operation' for both the cards and workstations, independently of each other, allows for flexibility within the system and makes user mobility a relatively simple issue. The following provides the basic sequence of events, for operation of the system with the TTP infrastructure.

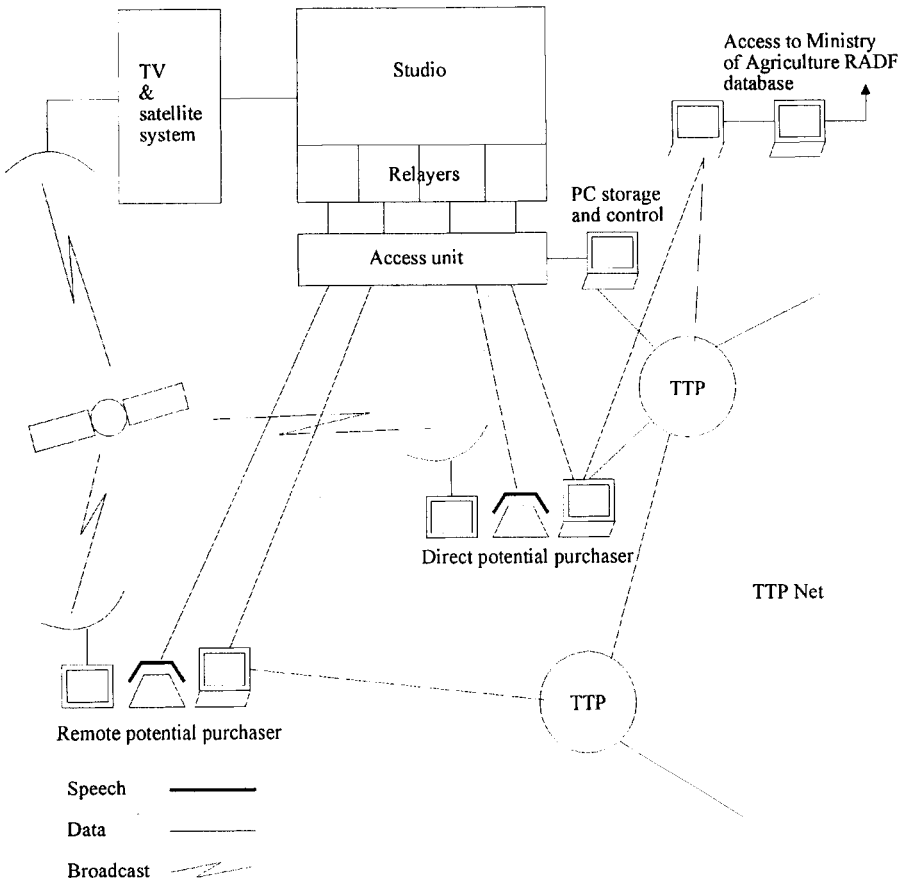

Figure 5. Arrangement of CLASS system with TTP network.

5.2 Pre-auction.

5.2.1 Initial registration of smart card users.

An initial registration must occur when each user is given their smart card. The smart card is personalised with the private key of the user, and the UC is generated and signed by the local TTP. Each user UC is then stored by CLASS for future use, i.e. verifying digital signatures, etc.

5.2.2 Entry of livestock to auction.

The fieldsman must verify the vendor's ownership of the livestock. This is achieved using the Cattle Identification Document, CID, and eartags on the animals. In future, it may

be possible to access the CID information directly on the Ministry of Agriculture, Fisheries and Food, MAFF database. (The Fieldsman's smart card could potentially be used for authentication in association with access control to this database, assuming that this allied application area was taking advantage of the ES / N-TTP services).

The details of the livestock must then entered onto the Cattle Entry Form, CEF. In the case of the occasional vendor the CEF will be paper-based, and will be manually signed by both parties as existing.

With smart card operation, the CEF details are entered into the Fieldsman's portable computer. At least the same level of legal assurance as for the paper CEF is required, and so both the vendor and fieldsman use their smart cards and sign to provide authenticity, integrity and non-repudiation of the transaction.

5.2.3 Registration of potential purchasers for each auction.

In the ISDN scenario, the potential purchaser uses their smart card and selects the option to register for a specific auction. A request message is created and signed and sent to the AU. In order to verify the signature, and hence the authenticity of the potential purchaser, the AU needs the potential purchaser's UC. This should be available locally as it was stored in the AU database during initial registration. However, the UC may be out of date, or revoked, in which case the AU would have to request the UC from its local TTP. Once the message has been authenticated, the AU sends a signed confirmation to the potential purchaser which contains the session identifier and telephone number to be used for the auction proper. This information is held at the potential purchaser's ISDN terminal.

Where an ISDN service is not available, the potential purchaser uses a modem via a PSTN line for data communication, and a separate mobile (or fixed) telephone for speech communication. Here the sequence is logically the same as for the ISDN case, except that the session identifier and telephone number returned in the confirmation from the AU are visible to the potential purchaser.

5.2.4 Access to catalogue.

Access to the catalogue, with the appropriate read/write capabilities, is provided to the registered potential purchasers and Primary Centres after the authentication of their requests that have been signed by their smart cards. The need to obtain certificates from the TTP is a requirement in this respect.

If the Primary Centre / Fieldsman / potential purchaser is at a remote location and is not within the TTP domain covering CLASS headquarters then the certificates of the respective parties are passed over the TTP network. For a user that is not within the domain of their local TTP, their DN will indicate the location of the required certificate.

5.3 Auction.

5.3.1 Admission of registered potential purchasers to the auction.

For ISDN access, the potential purchaser inserts their smart card and selects the option to join the auction. The ISDN terminal creates a message containing the potential purchaser's session identifier and signs it. It automatically dials the AU and sends the signed message. The AU verifies the authenticity of the potential purchaser from his digital signature and then compares the session identifier with its database of current valid session identifiers. Once verified, the AU automatically selects a bid-relayer and routes the call to him/her. The session identifier of the potential purchaser is automatically displayed on the screen of the bid-relayer they are connected to and the potential purchaser then places bids on lots.

When the potential purchaser makes a successful bid, the auctioneer's hammer falls and a signed sale request is sent to the local TTP. The TTP verifies the AU signature, and passes on the request to the potential purchaser. They must confirm their acceptance of the bid price by selecting the 'Confirm Sale' option on their terminal. This instigates a signed confirmation of the sale which is sent to the local TTP. The TTP verifies the potential purchaser's signature and passes the confirmation to the AU. This service is called Arbitrated Digital Signature, ADS. When the AU receives the confirmation, bidding may proceed on the next auction lot.

When the modem and telephone are being used, the potential purchaser manually dials the auction number and is allocated a bid-relayer who immediately requests him to authenticate. The potential purchaser must manually select the option to authenticate, and this results in a signed message being sent to the auction AU. The AU verifies the potential purchaser's signature and the relevant valid session identifier from the database which is then displayed on the bid-relayer's screen. The bid-relayer then asks the potential purchaser for his session number and if the two numbers match the authentication is successful. The potential purchaser may then bid on auction lots via the telephone. Similarly, when the potential purchaser makes a successful bid, they must confirm the bid by initiating the digital contract with CLASS, via the TTP, as described previously.

5.3.2 Admission of registered sub-auctioneer(s) to auction.

This procedure is logically similar to that for admitting the potential purchasers. Again, two routes are possible, depending on whether the sub-auctioneer has an ISDN terminal or telephone and modem access.

At present, the bidding actions of the sub-auctioneer are very rapid with negligible additional delay produced on a successful purchase. The countersigning arrangements must be such as to maintain this status quo.

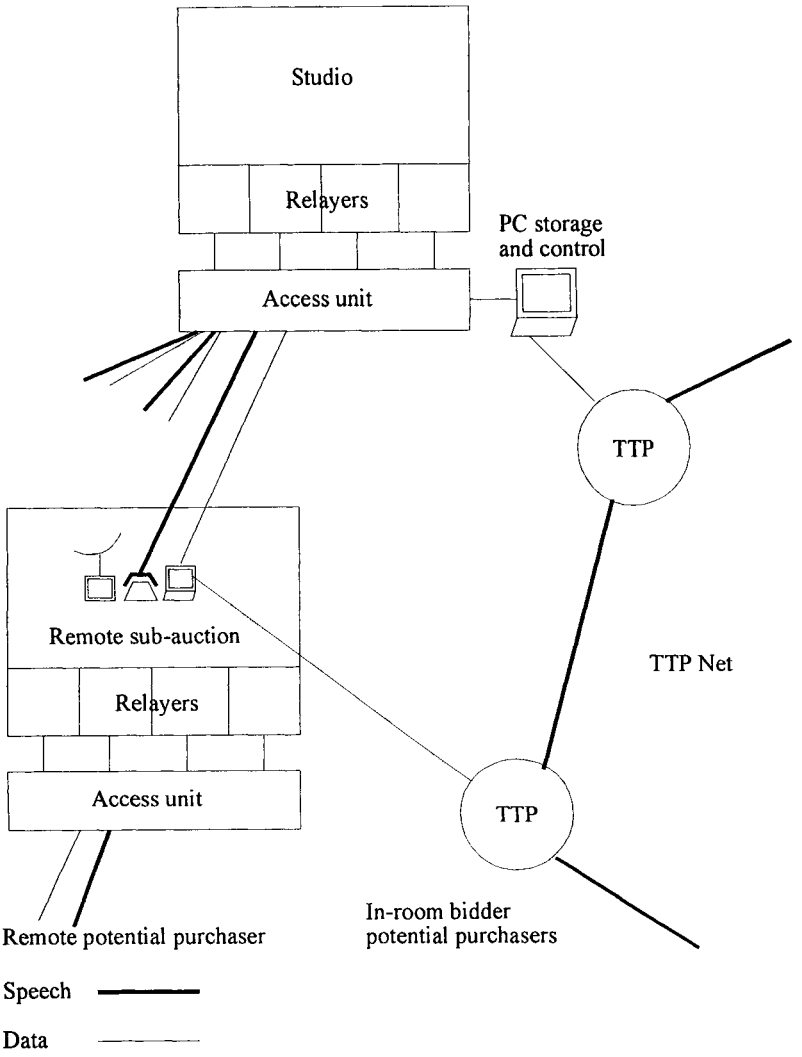

Figure 6. Sub-auction arrangement with TTP network.

5.4 Post-auction.

The procedures in this enhanced system will operate as existing from when the animal weights are determined from the abattoirs or purchaser. As the purchaser now has a PC as part of his standard system, he is ideally suited for EDI transfer of invoice details and EFT for providing rapid payment to CLASS! Similarly invoice notes to the Primary Centres can be

sent by EDI with payment to vendors by EFT, if all use these latest services. These activities will of course involve further TTP access and services.

6. Conclusions.

The auctioning by satellite, multimedia application forms an ideal scenario for the testing and further development of Electronic Signature / Trusted Third Party services. It provides the requirements for a wide range of security services that can be met by a TTP infrastructure, that will be needed to allow the application to expand over a wider geographical area and into other commodity areas. The use of a new, European-wide product that has only recently been marketed can allow an effective pilot scheme to be rapidly developed and evaluated in a commercial environment. The arrangement also provides the necessary facilities with which further development can be made to incorporate EFT and EDI services.

Acknowledgements.

The above paper was based on a feasibility study carried out for the European Union on an INFOSEC programme designed to investigate applications that could benefit from European-wide ES / TTP services. The authors fully acknowledge the support and contributions provided by the other partners of the consortium, namely *CLASS*, *COST AB* (Stockholm) and *KYROS* (Athens).

References.

1. "Identification of Common Interest Group (CIG) Requirements", S2203, CEC, INFOSEC '94 Programme.

2. "Electronic Signatures and Trusted Third Party specifications", S2203, CEC, INFOSEC '94 Programme.

3. "Business Electronic Transactions Architecture", COST Computer Security Technologies AB, Sweden.

4. CCITT X.500 International Standard (IS).