BEYOND IDENTITY: Warranty-based Digital Signature Transactions

Yair Frankel[*], David W. Kravitz [**], Charles T. Montgomery[*], Moti Yung[*]

Abstract. We distinguish between two types of digital-signature based transactions: *identity-based* and *warranty-granting.* In the relatively static (and traditional) offline "identity-based" transaction, a Certification Authority (CA) vouches for validity and veracity of data in a user's certificate. Whereas, in the more dynamic "warranty-granting" case, which we identify in this paper, a third-party entity vouches for a user on a per-transaction basis while considering the user's history and characteristics. Here, we provide a modeling for a warranty-granting transactions system and demonstrate its importance in the banking/financial/commercial setting. Warranty-granting systems can be implemented in one of several configurations based on the type of transaction and which party pays for the service (of acquiring the warranty). We discuss the primary configurations and then give a detailed specification for one of the discussed configurations.

1 Introduction

The development of public-key and modern cryptography has given us the notion of "digital signature". The role of digital signature is to replace real-life signatures and allow a user in an "electronic world" to have a mechanism for signing documents. The digital signature identifies the signer and unequivocally associates the signer with the document signed. It provides non-repudiation of the sender and enables transitive passing of authenticated messages.

Let us note first that in order to achieve scalability of digital signature, a mere personal digital signature scheme is not enough. In a crude form every user must have the "signature verification key" of every other user. Therefore, the notion and architecture of "Certification Authority" (CA) has been suggested. In fact, a CA is an entity that vouches for the correctness of very specific messages, each of which establishes the association of "user identity" with the user's "signature verification key". Thus, a CA architecture is in fact a bootstrapping of the notion of digital signature. The individual users now do not have to have the verification key of each user, instead they can be presented with a signature and a "certificate" where the CA signs the standard message associating a user with a verification key. To this end there are various schemes (e.g., [X509]).

In a basic CA-based architecture a certificate is either "pushed" to the user by the signer, or the certificate is "pulled" from the CA by the user. The "or" is not exclusive due to the possibility of revocation of certificates. For high scalability,

[*] CertCo LLC., montgomeryc,moti@certco.com; moti,yfrankel@cs.columbia.edu

[**] Divx, David.Kravitz@divx.com, Research performed while at CertCo LLC

we will typically have a hierarchy of CA's (CA infrastructure). A user will go up the tree-structure to a CA that it trusts. (The structure does not have to be a hierarchy and may have more semantics; namely various CA's may deal with certain tasks, key types and transactions.)

What we claim is that: a basic CA architecture is there in order to assure that a signature scheme is associated with an identity and its associated static properties. Thus, it will give very good services to transactions where the authenticity of digital signatures is the basic worry. We call such transactions "identity-based".

What has been observed is that once we enter into a commercial setting where financial service support for a transaction is needed, there is much more relevant information in a transaction than what a certificate provides (for example [Froomkin96] describes essential roles for a trusted third party in electronic commerce). We do believe that a certificate is the common information which makes digital signature schemes useful and legally viable [ABA], however we claim there is more which is needed to achieve financial transactions.

Our basic claim is that: once identity is assured, we need to further validate current contextual information which we abstract as a warranty; this validation is the core of smoothly operating business in the electronic world. The granting and validity of warranties should be based on the nature of the transaction, and the characteristics and current states of the parties involved in the transaction. The warranty-granting process can typically be viewed as an augmentation of user certification transactions in a digital signature based context. It melds implicit verification checks on the identity and transaction-specific digital signature authenticity with respect to the subject of the warranty, with access control mechanisms designed to address privacy and warranty-issuance criteria.

We can therefore observe that warranty-granting infrastructure has to support the maintenance of user information and status which is beyond what is provided in a certificate (e.g., it can be built upon anonymity-providing infrastructure). We would also like to mention that a warranty based system might not necessarily be an augmentation of a CA infrastructure. It is rather an infrastructural component with the following properties:

- It is based on pre-established relationships between clients (i.e., users, commercial entities, etc.) and elements of the warranty-granting infrastructure (i.e., banks and financial institutions).
- An established relationship may not exist between clients performing financial transactions.
- The financial transaction may involve more than the clients themselves; e.g., banks may help in controlling risk of transactions.
- Financial institutions may be required to carry users' private and time-sensitive information which may not be appropriate for a public certificate, such as credit rating or financial backing.
- Financial institutions may share information about their clients (shared monetary values and type of fields shared depend on certain circumstances).

- The relevant information per transaction may be dependent upon characteristics of the users performing the transaction, the relationships between them, and the nature of the transaction itself.

The transaction will be associated with a warranty-granting process that precedes the execution of the actual transaction, and is intended to assure that certain terms, conditions, and prerequisites do hold and will make the transaction possible. We assume that connectivity between the clients, and between one of the clients and the system back-end, is available on-line (a varied granularity in which a warranty is given for a transactions which consists of numerous sub-transactions is also possible). The validity of the warranty depends upon the correct representation of information by the clients. Note that the nature of warranty is more refined than that of "authorization certificate" and "transactional certificate" [Froomkin96], as it ties the financial infrastructure with the clients, their state, and the nature of the transaction itself.

2 Requirements

We now list the requirements pertaining to the warranty-granting system, which includes an infrastructure and where users access local representatives of this infrastructure. These requirements follow from the above discussion of properties and connectivity.

1. Each transaction will require access to the supporting infrastructure before a warranty is issued for this transaction. (This is a direct result of the need to obtain current status concerning the subject of the warranty.)
2. The system must provide for high availability and large transaction volume as in any public-key infrastructure that is usable in an electronic commerce environment. Of course, the supporting infrastructure must serve many simultaneous requests including simultaneous requests in which a given client is a requester and others where the given client is the subject of the warranty. This results from the ability of a given client to request service on a new transaction while waiting for a response from a previous transaction, as well as the fact that several clients could request warranties with a single subject of warranty at the same time.
3. The system should support flexible processing in such a way that delays and congestion, which are normally associated with warranty-based systems, can be minimized or avoided. These delays would occur, for instance, when the local representative does (can) not keep all information locally and/or must perform extensive verification with other sources. Accommodation for both completely automated transactions and delayed transactions is an important feature of the system.
4. The payment of fees for services provided by the supporting infrastructure must be consolidated within the supporting infrastructure. This is required both as a throughput issue and in order to ensure payment for services.

5. Amongst the users in a transaction, only the warranty requester needs to contact the supporting infrastructure.
6. A client needs to trust only his local representative.
7. The issuance of a warranty requires that the subject of the warranty provide authorization. This is a result of a desire to allow a client to limit and control the delivery of information concerning him as well as limit the scope of warranties issued with him as the subject.
8. The system must support limiting the amount of information provided to the supporting infrastructure to only the information necessary to support a warranty. It is viewed as neither necessary nor desirable to provide the details of the transaction to the system infrastructure unless a claim against the warranty results. (Notice that claims processing is likely to require exposure of the transaction to the supporting infrastructure.)

3 Warranty-Granting General System Description

The completion of operations within a warranty-based system always involves at least the supporting infrastructure and two or more clients. While the supporting infrastructure is viewed as a unit, it in fact consists of the banking system and contains geographically separated units.

Each client is assumed to have a relationship with their local representative of the infrastructure (business or individual client relationship with bank). The client's local representative has connectivity with other local representatives, banks, CA's, insurance companies, underwriters, etc.

It is also assumed that clients, where appropriate, will periodically receive statements concerning outstanding warranties and related information. This will not be provided on a per-transaction basis, and thus will not be shown in the message flows. The local representative may need to also provide for an electronic payment system as well as documentation, timestamping and other services.

A client can take on any of several roles. The client may be the party in need of a warranty in order to allow a transaction to go forward and thus is the warrantee. Another client will be the "subject" of the warranty, that is the assurance or warranty is provided with respect to the "subject". (While it is possible to provide assurance about a party who is not a client such cases are of less interest with respect to this paper.) An additional role that a client may take on is the requester of the warranty. Notice that the "requester" may be either the warrantee or subject of the warranty.

Notice that the relationship between the supporting infrastructure and the clients has two basic cases. In Case 1 (See Figure 1) the interaction is simplified in the sense that the local representative would be able to both determine the ability of Client 2 to meet the requirements of the transaction as well as arrange for payment of any fees associated with providing the warranty. In case 2 (See Figure 2 which contains additional flows) the situation is more complex since Client 1 is paying for the warranty but the ability of Client 2 to support the transaction is the primary issue.

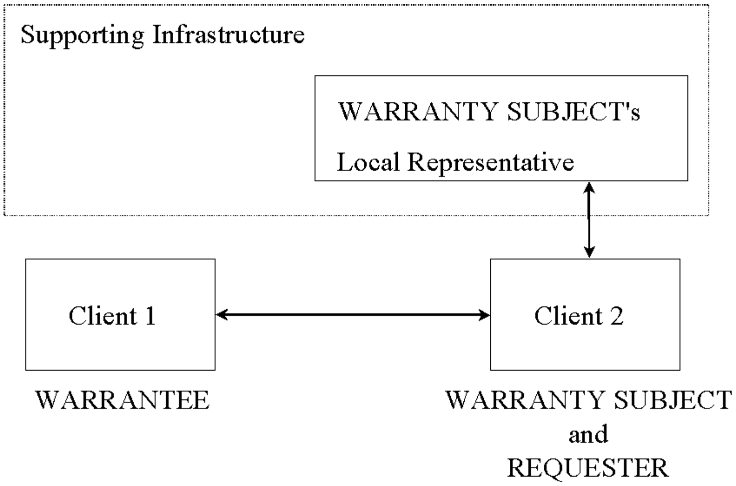

Fig. 1. Case 1: Warranty Subject is the requester for warranty. Client 2 communicates with its own local representative in the supporting infrastructure.

4 Detailed Description

Below we will take a closer look at Case 2 represented by Figure 2. We note that Client 1 has a trust representative in the supporting infrastructure which we call Local Representative 1. Similarly, Client 2 is supported by Local Representative 2. Database 1 is assumed to contain all relevant information on Client 1 and database 2 contains relevant information on Client 2.

It is assumed that any necessary exchange of information required between the WARRANTEE and the WARRANTY SUBJECT to reach agreement on a specific transaction has been completed. Security features required to support this preliminary exchange are not shown.

Message 1: This message contains the final version of the transaction along with information which forms the basis for warranty request. (Notice that there may have been information exchanged between the WARRANTEE and the WARRANTY SUBJECT prior to message 1 related to specific aspects of the transaction.) It is expected that the information in message 1 (as well as any preceding messages) would be encrypted and possibly signed. However, such protection is not vital to the proposal in this paper and therefore does not receive additional discussion.

Message 2:

Field 2.1. Identification of the WARRANTY SUBJECT: Unique identifier of WARRANTY SUBJECT which also identifies Local Representative 2.

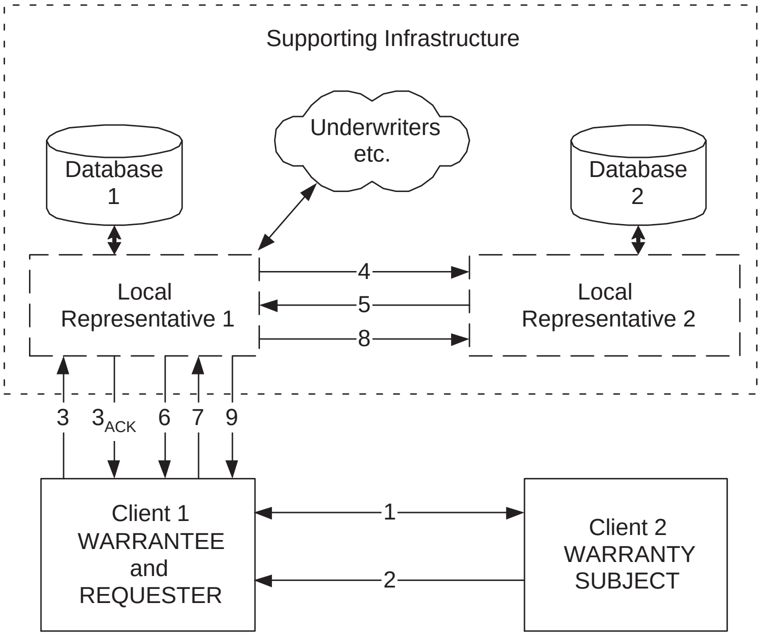

Fig. 2. Case2: WARRANTEE is the requester for warranty. WARRANTEE communicates with its own local representative in the supporting infrastructure.

Field 2.2. Identification of WARRANTEE: Based on information previously received from the WARRANTEE and should support unique identification of the WARRANTEE within the supporting infrastructure.

Field 2.3. Desired class for WARRANTEE: Allows WARRANTY SUBJECT to prescribe minimum standards that the WARRANTEE must meet in order to be issued a warranty on this transaction or to be provided other non-public information about the WARRANTY SUBJECT.

Field 2.4. Transaction count - WARRANTY SUBJECT: A parameter that is meaningful to the WARRANTY SUBJECT and his bank (local representative 2). The WARRANTY SUBJECT will generate the count by increment one from the previous count.

Field 2.5. Warranty parameter categories: Identifies information held by local representative 2 which is believed to be relevant to this transaction. This information is based on such things as the credit rating of the WARRANTY SUBJECT, standing in industry and related information based on the history of the WARRANTY SUBJECT.

Field 2.6. Coverage limit: The warranty coverage limit supported by the WARRANTY SUBJECT for this transaction.

Field 2.7. Effective time period of warranty coverage

Field 2.8. Transaction element categories (discussed below)

Field 2.9. Signature by WARRANTY SUBJECT: The WARRANTY SUBJECT signs the concatenation of fields (2) through (8) and a hash of the transaction. Notice that the hash of the transaction is not included as an element of message 2.

Let us discuss the Transaction element categories now. In some cases the ability to issue a meaningful warranty must take into consideration the contents of the transaction. Since one of the system requirements (see requirement 8) was to limit the information provided to the infrastructure, the "Transaction element categories" field provides a means of providing limited information related to this specific transaction which would be relevant to supporting the warranty. As examples, the identification of the transaction as covering agricultural goods may be relevant to the time period of the warranty (as it would be to a Letter of Credit issued by the Export Import Bank), or the warranty may be sensitive to the possible military use of the goods. Notice that the difference between "Warranty parameter categories" and "Transaction element categories" is that the first field is a direction from the WARRANTY SUBJECT to Local Representative 2 that identifies information on the WARRANTY SUBJECT which may be released for the purposes of supporting this transaction. While this information may support the transaction, it is based not on the transaction, but on the history and status of the WARRANTY SUBJECT, including the record of the WARRANTY SUBJECT's prior executed transactions. Note that it is outside the flow of the presently described system to track the status of transactions beyond the issuance of the warranty. The "Transaction element categories" are related directly to the nature and content of the transaction.

Message 3: This message may be structured so as to address encryption / authentication aspects of this message and/or subsequent messages between Local Representative 1 and the WARRANTEE. Notice that the Local Representative 1 can uniquely identify the WARRANTEE by the information contained in field 3.5.

The signed message from the WARRANTEE contains:

Field 3.1. Identification - WARRANTY SUBJECT

Field 3.2. Transaction count WARRANTEE: A parameter that is meaningful to the WARRANTEE and his bank (local representative 1). The WARRANTEE will generate the count by incrementing one from the previous count.

Field 3.3. Coverage limit requested: This is warranty coverage desired by the WARRANTEE.

Field 3.4. Hash of transaction: A hash of his copy of the final transaction agreement. This hash should be identical to the hash formed by the WARRANTY SUBJECT as a part of computing the signature for message 2.

Field 3.5. Signed portion (i.e., fields 2.2 - 2.9) from WARRANTY SUBJECT

Field 3.6. WARRANTEE Transaction element descriptions. (See below)

In cases in which the agreement or the warranty is based on underlying details contained in the transaction, those elements of the transaction which are important to the WARRANTEE and the usefulness of the warranty he will receive will be listed in the 'WARRANTEE Transaction element descriptions'. It is assumed that the form of this information was based on information obtained from the WARRANTY SUBJECT during negotiation of the transaction, and is related to the 'transaction element categories' identified by the WARRANTY SUBJECT in message 2. These WARRANTEE Transaction element descriptions may be transmitted within message 1. It is in the WARRANTEE's interest to ensure that these descriptions depict an accurate summary of all of the salient characteristics of the transaction. An "illicit" transaction may result in rejection of a warranty claim.

Message 3_{ACK}: Message 3 acknowledgment is provided to the WARRANTEE as an indication that message 3 was received and that it contained the required information from the client to support processing. It also would provide a path for immediately indicating that a warranty would not be issued if Local Representative 1 could determine this without additional information. An example of such a situation would be Client 2's identification appearing on a list held by Local Representative 1, which identified clients that were barred from being WARRANTY SUBJECT's.

In the case of complex transactions the time span between the WARRANTEE receiving message 3_{ACK} and message 6 may be unpredictable. This is due to the possible need for Local Representative 1 to obtain additional support for the warranty (such as underwriter support) as well as the possibility that Local Representative 2 may require time in order to obtain additional information. In many cases this additional support may require review by humans and would not be fully automated. To the extent possible, message 3_{ACK} should provide an estimate of the required processing time as well as providing the necessary communication and security basis for future messages. In particular messages from Local Representative 1 to the WARRANTEE would require encryption in order to provide adequate protection of information about the WARRANTY SUBJECT. Of course it is expected that any such information provided to the WARRANTEE would be held as sensitive information. (The WARRANTEE would have agreed to this as part of a contract with his local representative. This could be augmented by signed information within message 3.) This structure for the messages allows fast response where possible while still accommodating delayed responses where required.

Message 4:[1] This message includes the components from message 2 as created by the WARRANTY SUBJECT plus the hash of the transaction created contained in message 3 as created by the WARRANTEE. Notice that since the hash of the transaction as created by the WARRANTEE should be identical to the hash of the transaction as created by the WARRANTY SUBJECT, the signature on this information as created by the WARRANTY SUBJECT should be

[1] This message is internal to the supporting infrastructure and as such its security is assumed to be provided by infrastructure components which are not described in this paper.

correct. Message 4 contains:

Field 4.1. Signed message 2 from WARRANTY SUBJECT
Field 4.2. Identification - WARRANTY SUBJECT
Field 4.3. Transaction count WARRANTEE
Field 4.4. Information related to the WARRANTEE

Let us now discuss some of the processing performed at Local Representative 2. The signature on message 2 is verified. In order to detect the presence of a repeated message the database maintains a list of the N most recently processed transaction count values for each client. A message is not considered to be a valid new request unless the 'Transaction count - WARRANTY SUBJECT' is not contained in the database and is greater in value than the lowest transaction count retained in the database.

The "Desired class for WARRANTEE" from message 2 is compared with information provided in Field 4. This will be used by local representative 2 to make a support/non-support decision.

The data available for the WARRANTY SUBJECT will be reviewed for compatibility with maximum reasonable warranty coverage limits as well as the total coverage limits outstanding. This will require that all pending requests for warranties and the related status of these requests (as reported in previous messages of type 8) have been accounted for. As a result a support/not-support decision can be reached.

Notice that the actual processing of the transaction is outside the exchanges covered by this document. As a result the decision process may include consideration of warranties which were issued but did not actually result in completion of the associated transactions. It is expected that the local representatives will use knowledge concerning their clients which is verifiable outside of the exchanges of this system. This is necessary since the system does not in general follow the details of the transaction through its completion.

If the issuing of a warranty is supported, the Transaction element categories will be used to form the 'Database Transaction element descriptions'.

Message 5: [1]

Field 5.1. Identification of WARRANTEE
Field 5.2. Transaction count WARRANTEE
Field 5.3. Support/not-support decision
Field 5.4. Warranty parameters as listed in the warranty parameters categories
Field 5.5. Coverage limit authorized (Not Applicable if not supported)
Field 5.6. Database Transaction element descriptions. (Not Applicable if not supported)
Field 5.7. Reason for a not-support decision (Not Applicable if supported)

Let us now briefly discuss the processing at Local Representative 1. Assuming that message 5 indicated that the transaction is to be supported a comparison will be made between the WARRANTEE Transaction element descriptions (message 3) and Database Transaction element descriptions (message 5).

A discrepancy will prevent providing a warranty. Information available to Local Representative 1 may also be used to adjust relevant parameters (such as time period) in the warranty.

Message 6: The status of the warranty is provided in this message. Assuming that issuance of the warranty has been approved, it can also provide cost information associated with the warranty as well as any information required to initiate receiving of the warranty as well as any restrictions on the purchase of the warranty (for example time limit for purchase). In addition, message 6 will provide a report based on the warranty parameters as provided by the WARRANTY SUBJECT's Local Representative (as extracted from message 5) and may also provide relevant information related to the Database Transaction element descriptions (as extracted from message 5) and contrasted against the WARRANTEE Transaction element descriptions.

In accordance with requirement 7, the transfer of information relevant to the WARRANTY SUBJECT is limited as defined by the Warranty parameter categories and Transaction element categories contained in message 2.

It is important to note that message 6 is not the warranty but is an offer to sell the warranty. It is constructed such that misinterpretation is unlikely.

Message 7: Agreement by the WARRANTEE to accept (and pay for) the warranty is provided by this message.

Message 8: [1]

Field 8.1. Identification - WARRANTY SUBJECT
Field 8.2. Transaction count
Field 8.3. A statement of issued/non-issued status of the requested warranty.
Field 8.4. Final coverage value

Message 9: Message 9 is a signed indication of the warranty. It contains:

Field 9.1. Identification - WARRANTY SUBJECT
Field 9.2. Identification - WARRANTEE
Field 9.3. Transaction count (used with Identification - WARRANTY SUBJECT as pointer in database 2)
Field 9.4. Transaction count WARRANTEE (used with Identification - WARRANTEE as pointer in database 1)
Field 9.5. Hash of transaction
Field 9.6. Final coverage value.
Field 9.7. Time period of coverage

Message 9 may also contain information relating to specific aspects of coverage, such as the warranty parameters, if these values are guaranteed to be "accurate" at the time they were compiled, where the determination of accuracy is in accordance with the initial contract between Local Representative 1 and Client 1, the WARRANTEE.

5 Fees to the Supporting Infrastructure

It is envisioned that a fee will be charged to the REQUESTER (the WARRANTEE in the case under consideration) only if a warranty was approved and issued. While this practice does not provide fees for requests which are either denied by the system or not acceptable to the WARRANTEE it does prevent inappropriate fees from being charged to the REQUESTER as a result of requests involving security shortcomings in security structures outside of this system (e.g. an imposter posing as the WARRANTY SUBJECT).

The collection of the fee is enabled by the ability of Local Representative 1 to consolidate payments for services provided (with appropriate payment-authorization provided by the client which directly contacts the warranty-granting infrastructure back-end). No charge is made to the other client involved in the transaction.

While not envisioned as the primary method for providing fees for the supporting infrastructure, a more general fee structure could support a fee for three levels of service. The first level would be a small fee assuming the process ended with the message 3 acknowledgment. The second level would be if the process ended at message 6 without the issuance of a warranty. The third level would include the issuance of the requested warranty.

We remark that the system under discussion does not address any confidentiality requirements between the clients (which is an orthogonal issue in our context. It can, however, be provided as an additional layer).

6 An Exemplifying Scenario

As a conclusion we provide an example warranty issue process. Of course, this is one of many possible examples but was chosen to represent some of the capabilities of the described system.

In this example the WARRANTY SUBJECT is known by the supporting infrastructure to be a provider of software and cryptography. It will also be assumed that the WARRANTY SUBJECT is a company in the US and therefore subject to export controls for the delivery of cryptography outside the US. In this example it will be assumed that the WARRANTEE is a non-US company.

The transaction developed between the WARRANTY SUBJECT and WARRANTEE will be for the delivery of software which contains cryptographic capability. In addition it will be assumed that the WARRANTY SUBJECT is attempting to cheat and has not obtained the necessary US export authorization.

In this case the WARRANTY SUBJECT would include in the "transaction element categories" of message 2 only the category for software and not include the fact that the software also contains cryptography. In message 3 the WARRANTEE should ensure that the "WARRANTEE Transaction element descriptions" include all descriptors which he feels are important to the transaction. It is assumed here that he included both cryptography and software as descriptors.

Message 4 will contain the transaction element categories of message 2 and will return in message 5 matching database transaction element descriptions. Upon receiving message 5 local representative 1 will check for a discrepancy between the "database transaction element descriptions" of message 5 and the "WARRANTEE Transaction element descriptions" of message 3. In this example the discrepancy would prevent a warranty from being issued.

Notice that the WARRANTEE has the burden of insuring that the "WARRANTEE Transaction element descriptions" of message 3 was sufficiently complete to provide protection. If the WARRANTEE had included only software in the "WARRANTEE Transaction element descriptions" the warranty would have been issued. If the transaction had later failed to complete (perhaps as a result of the export controls) the WARRANTEE might have tried to make a claim against the warranty. In processing the claim the supporting infrastructure would have obtained the complete transaction and discovered that it was in violation of law and therefore not subject to warranty protection.

On the other hand if the WARRANTY SUBJECT had included the cryptographic "Transaction element category" in message 2, this along with "information related to the WARRANTEE" of message 4 would allow local representative 2 to detect a questionable transaction, in this case because of the non-US status of the WARRANTEE.

It should be noted that the issue here is not one of export control, but rather the legitimacy or legality of the transaction in the context of warranty coverage as defined in contracts between local representative 1 and client 1 and between local representative 2 and client 2. The extent of the actual coverage provisions may vary. For example, coverage may deal strictly with guaranteeing the accuracy of the delivered warranty parameter information, or may guarantee certain aspects of actual transaction fulfillment to be carried out by the WARRANTY SUBJECT. Even if certain transaction aspects are guaranteed, the WARRANTEE may want to use warranty parameter information to make a judgment on whether to expend the resources necessary to further pursue the transaction. In fact, the entire warranty process, as defined in the message flows, may be iterated during the transaction negotiation between the two clients. The incorporation of transaction element and warranty parameter categories enables automation and facilitates handling of access control and privacy requirements.

Other exemplifying scenarios may deal with the sale and delivery of morphine to licensed pharmacies, or with the shipment of hazardous waste materials to sites which must be licensed as demonstrable proof that they are equipped to deal with containment.

References

[Froomkin96] A. M. Froomkin, "The essential role of trusted third parties in electronic commerce", 75 Oregon L. Rev. 49, 1996. (See also http://www.law.miami.edu/ froomkin/articles/trustedno.htm)

[X509] CCITT, Recommendation X.509, "The directory-authentication framework," Consultation Committee, International Telephone and Telegraph, International Telecommunications Union, Geneva, 1989.

[ABA] American Bar Association, "Draft Digital Signature Guidelines", Information Security Committee of the Section on Science and Technology, 1996 (Available online: http://www.state.ut.us/ccjj/digsig/dsut-gl.htm)