On Assurance Structures for WWW Commerce

Markus Jakobsson* Moti Yung**

Abstract. We argue that the true potential of the World Wide Web will not be fully unleashed until the web "becomes civilized," by the implementation of *assurance structures*. These structures will complement means for concerns like privacy and transaction enablers like e-payment mechanisms. We first present our position, then we suggest and survey technical mechanisms to reach these goals, and show how these can be put together to provide a backbone (architectural framework) of civilized web commerce. Being a "position paper" we cannot hope to cover all the issues we touch upon in order to convey the needs and goals, neither do we attempt to provide a system design.

1 Introduction

Just like the pioneers settling in the Americas a number of centuries ago, pushing the frontiers and their civilization into the wild and wooly west (www), individuals and businesses are now settling the World Wide Web (WWW)[1]. The WWW opens up new possibilities by its high accessibility and availability, and permits new social and commercial structures to be built. However, we argue that civilization has yet not arrived to the WWW, and the lawlessness hampers further advances. Commercial transactions on the web have not yet become very common, in spite of the great possibility for entrepreneurship opened up by the net. This is because common "rules of the game" are not yet set up, and no one understands yet the business models and how the new medium enables new ways of human activities which involve willingness to spend money. This is also partly because of the lack of a common and working payment system of high reliability and lack of secrecy and other controls in network operation. We argue that both reasons are influenced by the lack of common rules as well as the lack of trust and its maintenance via acceptable infrastructure that must support organized and civilized society.

We observe that, currently, buying goods or information over the web corresponds, security- and liability- wise, to buying merchandise from a street vendor. Until structures for well-defined security and access control are built, the web inhabitants will still be like the crowd we often see in western movies representing

* Information Sciences Research Center, Bell Labs, Murray Hill, NJ 07974. markusj@research.bell-labs.com

** CertCo LLC, New York, NY. moti@cs.columbia.edu

[1] We deliberately do not mention many controversial issues regarding the wild west and our analogy has to be taken with a grain of salt (we admit that we could not resist the "similarity in initials" which has motivated this analogy).

the wild life of the pioneers in the www, i.e., a population where insecurity, lawlessness and arbitrariness rules. (This, of course, excludes the fact that certain known firms and enterprises have established themselves via association with the traditional brand name or via the media, e.g., the first Internet Bookstore is well known, also the manufacturers of Internet technology's web page is highly available and is embedded in various sign-up procedures. In contrast, for massive scale of "new opportunities" and "free enterprise" what we argue above seems to hold).

The WWW is an excellent example of how technology is creating new types of social structures: Suddenly, entrepreneurship and telecommuting are combined, creating a new type of employment opportunities. As another example, spontaneous availability of business to customers is made possible, and self advertising is made easy. More generally, the web changes the nature of communication and creates opportunities for new interactions, some of which can produce new lines of business (which are unpredictable at the moment). However, these will not happen on a large scale until the web becomes civilized. Thus, we need mechanisms that assure certain characteristics of commercial transactions (and related transactions).

We are also aware that the web has a special nature which made it evolve essentially on a voluntary base and that it will continue evolving perhaps dynamically as the population needs change. As a result of such an environment, a general framework with interfaces and service description is what is typically needed (rather than an architecture which dictates specific mechanisms and is cast in concrete). Such frameworks will enable growth and competition within the web environment (and consortiums being created to develop various frameworks). As a negative example, note that recent attempts (by big companies) to dictate commerce via "shopping malls" where merchants gets presented to customers via a special mechanism, seem to have failed. We will therefore avoid getting into detailed designs (this paper should not be mistaken as a specific architecture/ product describing paper). Rather we will concentrate on what our position imply on a generic mechanism and general technical needs level. The suggested framework (ideas) can be in turn included in various paradigms for commercial transactions and the detailed mechanisms themselves can vary. We note that the underlying technology to assure assurance at these more detailed levels is cryptography (the technology assuring integrity and limits in distributed and network environments).

Access control and security: The WWW vs. File Systems In some sense, the problem above can be put in analogy to the simpler problem of "security and access control in file systems". There, different users have different capabilities, and these enable them to access different resources, and in different ways (e.g., read / write/ execute.) While for the file system the access rights are evaluated perhaps statically according to only one strategy in the system, the access rights on the WWW should be evaluated according to dynamic and distributively determined rules. The rules may change according to different strategies, dynamic

state, and risk management philosophies (which dynamically change). Thus, the file system can be viewed as a "closed physical system" whereas the WWW can be viewed as an open one.

A user's rule for agreeing to grant access rights to some information can be thought of as a boolean formula of predicates, some of which need to be evaluated in order to satisfy the formula. Typically, these predicates are of the form "someone that I trust, trusts the accessing party," "someone I trust, does not endorse the accessing party," or longer chains of the same formats. Here, the assurances are based on personal trust, legal responsibility, reputation, or monetary responsibility. Whereas in a file system, the evaluation of rights whether to give or deny access, the assessment of predicates in commercial settings may be a quantity calculated based on statistics and other factors, as not all business decisions are based on full knowledge. This is a second difference: we are not performing strict access control but rather we evaluate the trust and risk involved in granting a transaction.

Remark: One problem that is extensively dealt with is the issue of payments. This is an important component of overall commerce, however what we will deal with here is a more general problem of making web commerce trustworthy in more ways than just assuring proper payments.

Organization: The rest of the paper is organized as follows: we start by reviewing positive and negative aspects of the WWW (section 2), then present what we think is needed (section 3), after which we present where, in terms of solutions and problems, we are now (section 4). In section 5, we discuss components for implementing the assurance framework, assemble these into building block, and discuss trust issues. We end, in section 6, by exemplifying transaction scenarios for our proposed generic architecture.

2 Positive vs. Negative Aspects of the WWW

Next we exemplify some basic problems connected with the wide possibilities that the web provides. We believe that by now these issues are well known, but we point at them as a starting point to our position.

The WWW has the capability to supply its users with new services, and makes information collection dramatically easier. The latter is not only true because of the ease of access, but also, with the introduction of payments, by an increased number of service providers. Namely, the web enables small entrepreneurs to find business opportunities without having to go through the bureaucracy and delays of current establishments. Therefore, it will be possible to be a "free-lancer to the masses," instead of going through traditional agencies such as publishers. However, even traditional structures will benefit from the lower costs to access and disseminate information, which can be done across across traditional borders. Thus, new social structures can be built across traditional social and geographical boundaries, benefiting trade and friendship between regions previously isolated from each other, making de-provincialization

and de-isolation easier, boosting business and supporting awareness. The "electronic town-hall" idea, a hot topic during the 1993 U.S. presidential campaign, will find itself a natural host in the World Wide Web. Moreover, the WWW, apart from being very useful for the collection of marketing related information, will also become a tool in making sociological and human research in a scientific way. The ingredients for a successful civilization are definitely present in the WWW!

However, all tools (and especially strong ones like the web) can be abused. In order to prevent this brave new world from becoming that of surveillance of users (bothersome big brotherhood), or the lawlessness of a wild and wooly west, we have to take preventive measures against unwanted practices. The lack of trust is inherent in a distributed system without physical contacts and an agency representing the law. The users must be protected from bad service providers, both those who voluntarily provide a bad service, as those who do it unintentionally. Criminality, both in the sense of the sale of bogus services, and of the kind supporting physical world criminality, must be controlled, as must the distribution of misinformation, and of unwanted information such as recipes for bombs and child pornography. At the same time, which can be a very difficult balance act, the user must be protected with respect to his or her privacy, both from businesses and governments. Just like borrowing Marxist books from the library during the McCarthy area had direct implications on the personal level, accessing certain information may be incriminating in the eyes of some governments. Similarly, extracting and abusing personal information is made easy by businesses with daunty practices. For example, insurance companies may base decisions whether to offer or not to offer life insurance to people on information whether this person may have accessed gay chat lines. Similarly, "sucker lists" containing people known to have a low resistance to buying certain services or products can be established and used to further squeeze these users for money.

3 A Position: What is Basically Needed?

The open-ended nature of the WWW systems makes it necessary to maintain assurance structures that support the dynamic policies, and design processes that employ these structures. Due to its global nature, assurance structures have to be based on "trust infrastructure" that provides "trust relationships" among entities, whereas processes can evaluate "subjectively" the available structure and generate "quantitative access-control entity" that allows for "civilized transaction" to take place. The bottom line is that entities will have the means to assess the "value" and "risk" involved, in a reliable fashion (e.g., a customer is assured that "what you see is what you get!" or an institute is assured that the customer's credentials seem ok given the statistical data about them. The assurance is a combination of evaluating "trust relationships" and perhaps evaluating the evaluation process. Each participant, in turn, may affect the relationship upon participating in a transaction (e.g., via a consumer survey).

It is a central goal of this paper to investigate the need and mechanisms

that allow for predicates and access rights to be first accessed correctly; to be evaluated properly on a first level; and to be dynamically maintained on a second level, by providing the necessary structures and processing techniques.

The components that are needed are:

- **Access structure**: First, there is a need for *categorization for simple access*. This is analogous to the business pages of a phone book, but need not be implemented as a static list, but can favorably be achieved by dynamic searches of links. The potential exponential growth of such a search, if clumsily performed, has drawn a lot of attention to the problem of intelligent search methods in the artificial intelligence community. Self-imposed rating of services, combined with lists provided by endorsement agencies can simplify searches. A specific type of self rating that may be of interest is that of self-censorship by categorization. This is analogous to what the movie industry does, and helps movie-goers select what they want to see.
- **Trust Structure**: Then, we argue that in order to make the World Wide Web an organized and civilized society, we need to build structures to protect its inhabitants against unfair and potentially criminal acts. As mentioned above, one of the issues is to *establish trust* between customers and merchants. This can be achieved using endorsements, either in the form of agencies, or in the form of customer feedback. The former has a physical-world counterpart in the Better Business Bureau, which can be contacted and asked whether they endorse a certain business, or if they have customer complaints on it. The second type, which to a certain degree already exists on the Internet, is a media that allows discussions, warnings and recommendations without any established endorser. The need for a structure permitting endorsement becomes clear in the light of how easy it is to set up a store front, generate some sales, and then "leave town" when the going gets tough, only to resurface under a different alias later. Endorsement structures would not only benefit the buyers, but also make it easier for honest businesses to get established, opening up new commercial possibilities. Licensing and attaching liability via insurance providers may add trust as well. (The issue of provision of such trust in the distributed systems context was first dealt with in [3]). The fact that statistical tools and built-in surveys can generate automatically such a function when the web commerce is used extensively is observed here. The mechanism will associate brand-name recognition and will establish reputation. It has to be assured that only "actual" customers who participated in buying and only a sample of those take part in this action, to prevent competitors from taking part in (or significantly influencing) these automatic actions. In short, the mechanisms apply "access control like" decisions whereas the goal is not to deny access to resources, but rather to assist users and institutes in evaluating quality and liability of required transactions. The model will provide quantitative assessment of commercial actions based on assurances which will be maintained dynamically.
- **Provisions for Individual/Institutional Needs:** The establishment of trust in the context of sales is not the only area where the user needs protec-

tion against malicious businesses. It is easy to see that the WWW allows the individual users access to large amounts of information, and also that the information provider can easily control what information is disseminated. Conversely, it is not true that the individuals surfing the net can control what information the providers are allowed to extract about them. Whereas access patterns of users can be put to great use in making marketing surveys and also help the user directly (via profiling and individual promotions), it is also easy to intrude in the privacy of individuals, as the provider easily can find out the (network) identity of the accessing party. This can be abused in the "real world" for political purposes, to deny services to certain groups of people, overzealous direct marketing, and in the extreme, for blackmail and similar. We see nowadays that anonymous access has been recognized as a major component of web technology and it is aimed at solving such problems. Similar to individual needs, there are needs of institutions where the concerns are analogous. Also, users may want to have various trade-offs of anonymity vs. profiling ability. Like anonymity there should be other protective properties that users and businesses may need. Generally, users need guidance and awareness which allow them to act while they also need shielding from side-effects of their actions.

- **Assurance Structure Maintenance**: The trust and relationships that assure the various needs and access rights, limitations and other controls, need mechanisms to maintain the various relationships in a reliable and authenticated fashion. This will require dynamic processes inside the systems and also outside the systems (in the real world) to assure continuity and growth of the web. There are social, organizational and technical issues related to introducing a law, means for trust, selection and censorship on the World Wide Web, to a large degree using mechanisms already existing in other contexts. Drawing knowledge from analogous mechanisms makes the establishment of a civilized society much easier, and just like the founding fathers of the United States used ideas surfacing during the French revolution when writing the constitution, our suggested methods are inspired by structures in the real world. The maintenance involves dynamic changes as well as adaptation of a given basic structure to various cultures and business models at the same point of time. We will suggest ways and methods of maintaining the structures and making sure it is available in a reliable form to users, both to automated agents and to human interfaces.

Again, we wish to remind the reader that this is a position paper, and that there are many opposing positions. Some of these are as follows:

- **Economic Issues:** It may be too costly to implement and maintain the required structure.
- **Legal Issues:** It may be too difficult (and costly) to implement the legal changes and additions needed to support the structure, especially so since the structure geographically encompasses several jurisdictions.
- **Ergonomics:** It may not be possible to design an interface simple enough to be understandable to the average user (e.g., given the intricate decisions

sometimes required for trust evaluation, the average user would not understand how certain settings translate to an acceptable risk). A global system which is culture-independent will be impossible.
- **Anarchistic view:** It may not be desirable to implement the suggested structure.
- **Evolutionary view:** It may not be necessary to make an effort to implement a structure - this will eventually happen by itself[2].

4 Where Are We?

In this section, we discuss the currently used solutions to the problems of the WWW and their shortcomings, and then look at the mechanisms we suggest for civilizing the web.

4.1 Current Solutions

Currently, there is no clear way to judge whether a service provider offers a quality service or not, particularly so for small and unknown providers who do not generate enough sales [3]. However, assume that you are interested in buying a product advertised on the web. *How would you know what the quality of the product is? Can you trust that you will get the merchandise after paying? Can you trust the guarantee?* These are problems also existing in the mail order business, but enlarged by the low costs of a store-front on the web, and the ease with which a new alias can be produced by a criminal shop-keeper. The problem gets even more obvious when the sale of information is considered: Picture a dating company who displays personals and charges for giving out addresses, or a job-search service promising to find you companies where your C.V. has good chances of being successfully reviewed. How can one know that the person or company behind the ad really exists, and is not just a figment of the match making company's imagination?

However, let us assume that you indeed do trust that the merchandise or service you buy from the provider is real. Now, the question is how the payment can be performed. The best existing solutions are based to some degree on sending your credit card information over the network, but leave a lot to wish for. One shortcoming of some solutions of this type is that only registered shops can receive payments, and that it is rather difficult (and expensive) to establish such a status with a credit card company, at least in the perspective of the small entrepreneur. Some solutions overcome this problem by introducing an intermediary, and only this intermediary, run by the provider, needs to be registered as a credit card merchant. Another issue (neglected till recently but

[2] Whereas this is not necessarily a counterpoint, it does not stress the importance of careful analysis of the given possibilities before a choice is made.

[3] One exception is providers of connection to the web, where it is easy to compare the service given between different companies, and also has an anchor in the physical world.

more active recently) is anonymity, both regarding payments and accesses, a problem which is not solved by the introduction of the intermediary, who, on the contrary, obtains large amounts of sale-related information. Furthermore, the service provider can, without the knowledge of the user accessing his service, obtain information about the latter, constituting a breach in the privacy of users.

4.2 Promoting and Protecting

There are two types of methods to promote good service providers and punish bad ones: by direct intervention and through the market forces. Although the web, with its distributed nature, is better suited for a distributed, market force driven legal system, the number of potential victims makes some type of direct intervention desirable.

The market forces would most likely express themselves through hierarchical positive and negative endorsements, the trust in which is based on brand name recognition and reputation: A good service provider does not want to associate with a disreputable endorser, and vice versa, and good endorsers can lose their reputation by endorsing bad services. Similarly, well reputed search engines would rather use reliable endorsers, just as the clients will be likely to favor endorsers and search engines with a good record. Endorsements could be performed either by professional organizations (e.g., IEEE,) by commercial bodies (e.g., Consumer Reports), special-interest organizations or congregations (e.g., labor unions,) or government and other organizational entities (e.g., the Chamber of Commerce.)

The endorsements can either be for free to the inquirer (e.g., endorsement agencies charging their clients, selling statistical information, or providing a free service for the common good) or purchased (e.g., insurance companies setting a price for endorsing a service, where the price of the insurance depends on the provider's previous record and therefore approximating the amount of future complaints and lawsuits). The insurance companies makes it possible for providers without a record to establish themselves, by buying support, thereby transferring trust from the physical world. Again, brand name recognition and reputation would be paramount, but now of the insurance companies, or the endorser of these.

Market forces will punish malicious providers by exclusion from lists of recommended providers, or by increasing insurance costs. Direct punishments, i.e., punishments more severe than the exclusion from a list of recommended providers, are difficult to implement in a distributed system without censuring, but could be achieved through voluntarily used filters, where well-known offenders are filtered out, through blacklisting, and by using "traffic polices;" agents listening in to the page requests, and sending out warnings whenever a service provider with a bad track record is contacted. These filters and "early warning systems" can be either officially run, or run by endorsement agencies as above.

The establishment of maps of the web landscape is closely related to the promotion of good providers, and can be obtained using the same vehicles,

namely endorsers, directories, and search engines, which will establish pointers to providers that are likely to please the client.

4.3 Data Mining for Marketing and Research

Just as the WWW provides users with a valuable and easy accessible source of information, the users can in turn provide service providers and others with valuable statistical information. By observing user behavior and purchase patterns, a lot of very precise marketing information can be automatically collected, and marketing approaches tested on a large population for a small cost. Similarly, researchers can will be able to collect important information of a similar kind from access and purchase patterns, and performing experiments whose results are easily quantified through the precise collection of data and the large sample size, making the web population the ultimate ant-farm of social studies. (However, and as earlier pointed out, the goals of the marketers can sometimes be in conflict with the goals of supporters of privacy, making it important to regulate what type of information can be obtained without a previous agreement.)

4.4 Enforcing Policies

Currently, one may use the off-line mechanisms to complain and to assure trust. However, such traditional enforcement mechanisms may become a bottleneck. (In fact we see that such services also made themselves available on the web).

We are aware that it will take a lot of user education to assure that users and institutions use automatic tools to assure commercial transactions (and other transactions). We therefore assume that the sooner we think about them, the easier it will be for new and unpredictable commerce to find its way to the web (e.g., the intergalactic paradigm put by Rivest [4] hints about such unpredictabilities).

We next start describing the framework we try to put forth here.

5 Assurance Framework: Components

Here, we concentrate on technical solutions to implement the mechanisms of civilization. After introducing all the building blocks, we look at how these can be assembled to produce the desired structures.

5.1 Building Blocks

In order to achieve the goals, we suggest the following building blocks:

- *Endorsing Agencies and Rating Agencies*
  In order for consumers to know what businesses to trust and which ones to avoid, different types of endorsing agencies can be employed. Here, it is possible to picture an active agency who goes out and samples the services,

in order to produce what compares to the Michelin guide rating of good restaurants. This agency can then either produce a time-stamped certification (using digital signatures and related standard cryptographic methods) that the business could display, or could make itself available on-line for advice. Alternatively, a parallel to the Better Business Bureau or the Chamber of Commerce could be established, keeping statistics of user complaints and endorsing (either off-line or on-line, as above) businesses with a good track record. The collection of consumer opinions could be automated by asking for user feedback after each major transaction, or could solely rely on negative feedback in the form of complaints. Furthermore, a forum for user opinions can be useful guidance. This can either be organized and centralized (as a digital version of *Consumer Reports*) or distributed and open for discussions (as many newsgroups currently are.) In those cases where feedback is given by users it has to be made certain that the feedback is valid, e.g., does not originate from the organization judged or a competitor, or at least not to a significant share.

- *Insurance Companies*

  Another way trust can be established is by the endorsement of a third party in the sense that if the service provider fails to provide the promised service (by accident or intention) then the third party, the *insurance company*, will pay the customer for its damages. The cost of buying insurance will depend on the history of the service provider, the expected risks and the extent of the insurance, just as for "real world" insurance companies. Furthermore, insurance companies may be structured hierarchically to establish trust and ascertain availability of funds for payments. This issue is treated in detail in [3].

- *Directories*

  In order to allow the users to find the services they are interested in, directories of services will be useful. These can as part of their function perform a selection of services that have been well received by previous users, and therefore take part in the quality control practiced by the endorsement and rating agencies. Individual directory services may interface each other, exchanging information and enabling searches. An example of a service of this type, already existing on the web, is dating services.

- *Brokerages*

  Brokerages are institutions devoted to find information, services and merchandise for their customers, and are related to the directories in functionality, although they may not themselves have any information, only the capability of finding it. Examples of such services that already exist on the net are general search engines and job-finding agencies (some of which are more closely related to directory services.)

- *Banks*

  In order for commerce to be made possible, there must exist means for exchanging tokens denoting value electronically. Several different approaches to solve this problem have been suggested, and financial institutions are show-

ing the issue much attention. There are many systems suggested, extending the use of cash or credit cards. Extension of cash allow a high or perfect degree of anonymity, but at the same time, many schemes of this type introduce possibilities for crimes like money laundering and blackmail using the perfect anonymity. Recently, the cryptographic community has given attention to payment forms implementing an anonymity that can be revoked in special cases of suspected criminal behavior, thereby removing this problem.

- *Drive-through Booths*

  In order to achieve anonymity, we must provide means to access a service under an alias, since it is possible for a service provider to read the IP address of an individual accessing the service, and also to query the gateway of the accessing party in order to obtain more information about the user. We call this service the *drive-through booth*, as it would funnel all its traffic through, establishing an alias for outgoing traffic, and de-anonymize returning traffic in order to send it to the accessing party. This way, using one or more drive-through boots on the way to a service provider, it will be possible to implement anonymity. An example of such a service is [2]. We note that, in the context of digital cash, it does not make sense to implement a higher degree of anonymity in the payment scheme than is obtained by the use of (possibly multiple) drive-through booths. High throughput is an issue of major importance to the drive-through booths, as they would otherwise constitute unnecessary bottlenecks. Therefore, it makes sense to combine the drive-through booths with a directory service, an on-line service provider, etc., i.e., where the traffic goes through anyway. To obtain further privacy, encryption can be employed.

- *Toll Booths*

  A toll-booth is a service that allows charging for traffic. In order to make sure that over-charging by a service provider does not take place, the toll both will constitute the trusted interface between the user and the merchant, making sure that the proper amount is charged and clearly displaying this to the customer. The honesty of the toll booths, in its turn, can be inspected and kept track of by endorsement agencies. The toll booths may have the added functionality of recording transactions in order to enable legal actions to be taken, should the service paid for not be what was promised. We note that this does not need to compromise anonymity, as the transactions can be recorded w.r.t. the secret alias used. With the help of the drive-through booth, the user would still, however, be able to show that a certain payment took place.

- *Arbitrage Agencies*

  An arbitrage agency implements the legal function of a judge, receiving complaints, ruling in specific cases, and making policy decisions. The decisions of such a judge can be implemented in a distributed system like the WWW by voluntary agreement to its decisions by service providers such as network providers, directories, endorsement agencies and similar. Since a working society is in the common interest of the majority of the players, the rulings of

arbitrage agencies will be meaningful.

- *Certification Agency*

  Users will have a need to identify themselves, sign contracts, etc. In order to achieve this, each user will select a secret key and calculate the corresponding public key. Knowledge of a secret key corresponding to a certain public key allows the user to prove his identity as that of the owner of the public key, sign documents with the name connected to the public key, etc. The certification agency certifies the public keys connected to the name of participants, using digital signatures.

  One recent idea of relevance is Blaze, Feigenbaum and Lacy's [1] work which identified the issue of "trust management" and suggested mechanisms to achieve it in the context of network services via certification authorities of extended roles. Another related idea is the distributed security infrastructure suggestion by Rivest and Lampson [5] which suggests grouping. Indeed, assurance structured are processes which should be supported by trust management and aggregation mechanisms which become part of the processes as will be described in this work.

- *Traffic Polices*

  The traffic police could implement a warning system, where users accessing the pages of known offenders could be warned, and pointers to complaints and lawsuits be given. This can be implemented in conjunction with e.g., drive-through booths, or by agents residing in the physical switchboards of the net, listening in to the page requests.

- *Tax Collectors*

  When commerce becomes common on the WWW, it will become of importance for the local authorities to be able to derive the amount of income from transactions on the network, so that they can tax the related companies and individuals correspondingly. In order to achieve this, one possibility is to obtain revenue information from the toll-booths. Although sales can take place without the toll-booths taking part in it, in order to evade taxes, it may not be wanted by the customer since the toll-booth gives security to him by overseeing and possibly also recording the transaction. We note that the existence of tax collectors further motivates the use of toll booths. Another way of taxing (with a flat rate) would be to let all coins in an e-cash setting lose value between withdrawal and deposit.

- *Customs*

  The customs make sure that the transfer of information and funds is performed according to the rules. This may include the banning of certain services into the country, taxation of others, and the control of money flow in order to prevent tax evasion.

- *Marketing Agencies*

  The marketing agencies, who with advantage can cooperate with the directory agencies, brokerage agencies and endorsing agencies, perform market surveys and do research on consumer behavior. The amount of information given to them can be controlled by means of the drive-through booths, mak-

ing sure that no personal information is used without the agreement of the provider of the marketing information (i.e., the user). As noted before, the value of web-based surveys can give be very high, given the high precision of the experiments, aided by the objective measurability, and the high throughput of the media used.

- *Standardization Body and Form Providers*
  The standardization body decides on the proper format for queries of different types. There may (although there is no direct benefit) be several co-existing standards, in which case we can envision a type of party that "translates" queries between different formats. The proper formats may be provided by "form providers". Note here that the proper format may be an executable description of the expected merchandise, and that these descriptions then can be both provided and certified by such an entity.

5.2 Assembling the Building Blocks

We show one example of how the above building blocks can be put together to form service units, which together obtain the means for trust, payments, privacy and structure that we require.

1. *Connection unit*
   The Internet access provider can at the same time as providing a connection implement the functions of directories, brokerages, banks, drive-through booths, toll booths, certification agencies, marketing agencies and form providers. Furthermore, they can to some degree be endorsing agencies, and insurance companies to its users.
2. *Commercial unit*
   We combine directories, brokerages, drive-through booths and marketing agencies to form a commercial unit. Such a unit provides information about services, implements anonymity, and uses access patterns of users for marketing surveys.
3. *Charging unit*
   We can combine banks, drive-through booths and toll booths, tax collectors and customs to a unit supervising payments, implementing anonymity, and verifying that no "illegal material" is imported.
4. *Endorsement unit*
   The endorsement unit contains endorsement and licensing agencies, possibly combined with directories and brokerages. If the endorsement unit provides traffic through it (and not only is a consulary service) then it will also implement a drive-through booth.
5. *Privacy Unit*
   The privacy unit solely implements a drive-through booth, enabling users concerned with privacy to access information anonymously. The privacy unit would not have any conflict of interests, would be run by privacy advocates, and would therefore give a more trustworthy anonymity than the other units

implementing drive-through booths. We note that a multiplicity of privacy units may be employed to strengthen the degree of privacy.

6. *Legal unit*
   We combine arbitrage agencies and certification agencies to form a legal unit. This unit may also implement a directory of legal services, and similar.

5.3 Trust between Components

The establishing of trust is central to the issue of obtaining secure WWW commerce. There are three types of trust involved: (1) the trust each entity has to put in his or her own machine, (2) the static trust between entities, and (3) dynamically established trust. Let us consider these one by one:

1. **"Self" trust**
   Each participant needs to trust the operating system on his or her machine to give access appropriately. For example, a charging unit will be allowed to open a window with a certain appearance (indicating its authenticity) and interact with the wallet of the participant. The same access rights must of course not be given to a merchant. The operating system should use the so called sandbox concept, in which different processes are given a "sandbox" of their own, in which they may access any information, but from which they are not allowed to leave.
2. **Static trust**
   The user needs to trust the different parties differently; with money (his bank, and to some extent the charging unit, and indirectly, the endorsement unit), with privacy (that not all drive-through boot units on the path collaborate against him), and with "good advice" (that all units giving referrals or recommendations are properly updated and maintained.) The money related trust and the trust of "good advice" are related in the sense that entities giving bad advice may be economically liable for this.
3. **Dynamic trust**
   During any transaction, the user will have to establish a chain of trust, based on a hierarchy of positive endorsements or a lack of negative endorsements (two paths with different risks associated with themselves.) This process is partially automatic (by automatic verification of credentials and endorsements, some of which may require communication with other entities) and partially manual (driven by user decisions based on the user's own business decisions and preferences.)

6 Assurance Framework: Generic Architecture

Once the building blocks are identified, relationships and interactions between them can be designed and then "transaction scenarios" can be built. We will exemplify some of those.

We want to envision the establishment of trust in a setting using generic access mechanisms with standardized protocols for interacting with each other.

For example, we want not to restrict the type of payment scheme used, the type of browser, or the root of the trust in the establishment of trust. We give three examples of flows of information, closely related to chains of trust, in figures 1 to 3. In these figures, we sketch how three common types of transactions can be viewed. These are *searching for a product* (figure 1), *performing a barter* (figure 2), and *filing a complaint* (figure 3.) In these figures, filled lines indicate communication; dotted lines indicate endorsement; and flash-lines the potential revocation of endorsements.

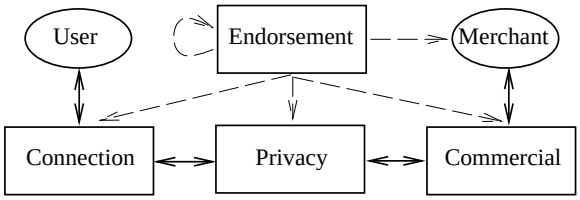

Fig. 1. Searching for a product.

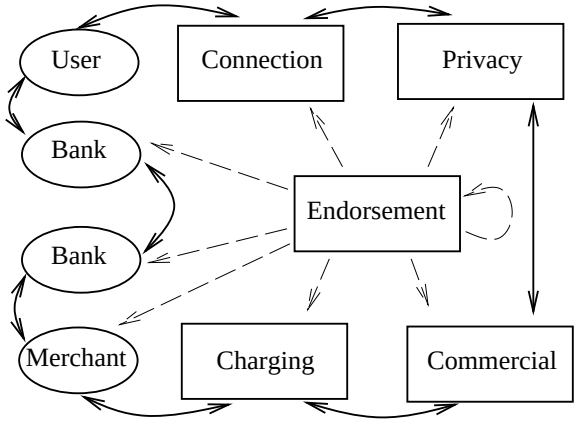

Fig. 2. Performing a barter.

1. **Searching for a product** *(Figure 1.)*
   When searching for a product, the user connects through the connection unit, where he obtains forms for the query, and pointers to appropriate commercial units, after which he goes through a drive-through booth for privacy. Second,

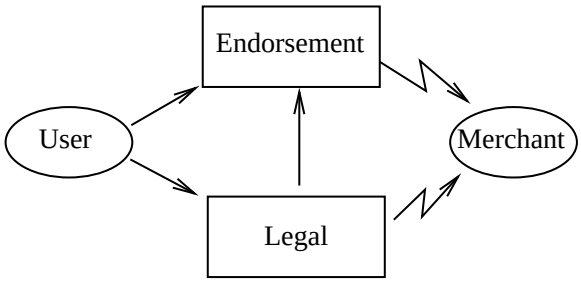

Fig. 3. Filing a complaint.

he may go through a privacy unit to further improve the privacy (the degree of privacy wanted can be set by the user). This anonnymizes his request for information from the commercial units he received pointers to by his connection unit. The commercial units compile answers to the requests, possibly using other commercial services, and possibly in cooperation with different merchants. These answers are returned to the user through the privacy unit and his connection unit. The process may be interactive, and the above may be repeated several times. All the different units above may be positively endorsed (or negatively, in which case that will be taken into consideration when the information obtained is evaluated) by a set of endorsement units, potentially hierarchically arranged.

2. **Performing a barter** *(Figure 2.)*
   When the user has found a product, he wants to establish a price for the product (if this is not already done) and procure it. Backed by a bank, he has some digital currency issued (or, in a more general case, something that the merchant desires from the barter). He connects through his connection unit, which again funnels the traffic through a privacy unit, if desired. The request is then sent to a commercial unit, which forwards it to the merchant through a charging unit. The charging unit performs the barter after both parties have agreed to the terms (this may be performed automatically or manually). The information is exchanged by sending the obtained merchandise to the acquiring party, who then deposits it in his bank (where applicable.) The banks of the two traders balance their accounts to complete the transaction, after they have verified availability of funds (this may be done in a way that is supervised by the charging unit in order to establish availability of funds for both traders before the barter is performed.) As before, all units may be endorsed.
3. **Filing a complaint** *(Figure 3.)*
   If a user (or more general, any participant) is unhappy with the service he or she received from another participant, he can file a complaint. This may be done with the appropriate endorsement agencies, and with the appropriate legal units. These consider the complaint, and the history of complaints

on the potentially misbehaving party, and takes appropriate action. This may involve the issuing of negative endorsements, or the refusal to perform positive endorsements onwards. This is a process of strongly hierarchical nature, where one entity may suggest another to change its future behavior (e.g., in terms of referrals) in order for the first entity to continue to trust the second.

References

1. M. Blaze, J. Feigenbaum and J. Lacey, "Decentralized Trust Management," IEEE Security and Privacy, 1996
2. E. Gabber, P. Gibbons, Y. Matias, A. Mayer, "How to make personalized web browsing simple, secure, and anonymous," Financial Cryptography '97, pp. 17 - 31.
3. C. Lai, G. Medvinsky, B.C. Neuman, "Endorsements, Licensing, and Insurance for Distributed System Services," 2nd ACM Conference on Computer and Communications Security, pp. 170-175
4. R. Rivest, "Perspectives on Finacial Cryptography," Financial Cryptography '97, pp. 145 - 149.
5. R. Rivest and B. Lampson, "SDSI– A simple distributed security infrastructure."
6. J. M. Tenenbaum, C. Medich, A. M. Schiffman, and W. T. Wong, "CommerceNet: Spontaneous Electronic Commerce on the Internet," Compcon '95, pp. 38-43