Hypothesis Nine

Is the legal/business model adequate?

Background

The EMall Pilot, an innovative government initiative, is in line with current business trends toward electronic commerce. Business-to-business electronic commerce (B2B) comprises the vast majority of the emerging digital economy, according to commercial and other data tracked by the U.S. Department of Commerce (see, for example, www.ecommerce.gov for recent government studies). Retail e-commerce may constitute only between seven and fifteen percent of the estimated $102 billion in e-commerce activity in 1998, with the rest conducted between businesses. While this new method of conducting business is already significant and has expanded rapidly by ordinary standards, most commentators predict that we still stand at the cusp of truly remarkable growth in this market. In its 1999 prospectus of the Emerging Digital Economy, the Department of Commerce cites estimates that B2B commerce will top $1.2 trillion by the year 2003. More recent estimates are even more optimistic.

As a Massachusetts state government initiative to facilitate multi-state, web-based procurement, the EMall pilot is a type of business-to-business electronic commerce application. In most ways, the EMall pilot is representative of B2B transactions, however, there are some aspects of this pilot which are not typical of most private sector applications. One of the important ways in which the EMall pilot differs from nearly all other e-commerce is that one party in each transaction is a government, the state buyer, and the other party is a private company, the contracted Supplier. Another way in which the EMall Pilot differs from most e-commerce activity is that it constitutes an aggregation of Buyers who act together within a single technical, business and legal system to effect their online commerce. Finally, the EMall Pilot is distinct in that it has been sponsored, subsidized, and administered by a single government entity, the Commonwealth of Massachusetts.

The following section describes the EMall business and legal model in some detail.

The EMall Legal and Business Model

Existing Context: Procurement Statutes, Regulations and Policies

As the sponsoring state, Massachusetts had to observe applicable procurement rules in the selection of the technology provider, Intelisys, and the integrator, **SAIC**. These companies became the legal entities responsible for the EMall system delivery based upon a competitive selection among Vendors who had already been awarded contracts to provide such products and services to Massachusetts. These "blanket" vendors had already signed standard terms and conditions necessary to establish a relationship with the Commonwealth, including such terms as liability allocation, indemnification and assignment rights.

SAIC became the primary contracted party. SAIC sub-contracted to Intelisys, and Intelisys sub-contracted to Motorola, the company that provided certificate manufacturing services for the EMall pilot. Within these sub-contracting arrangements, the Commonwealth required each party to demonstrate a capacity to meet the business and technical requirements of the EMall pilot prior to permitting them to provide any service or product. Once these government procurement formalities were in place, each vendor agreed to contracts through which they opted into the same types of trading partner Operating Rules as is typical in private e-commerce systems.

The basis of public procurement law in the Commonwealth of Massachusetts is that purchases of goods and services be conducted in an open, fair and competitive fashion. It is a key tenet of the procurement rules that the Commonwealth achieves "best value" as a result of a procurement. This may be achieved by such criteria as attaining the lowest price, or it may be the result of higher levels of quality or an ability to deliver the product or service more quickly - depending upon the circumstances relevant to a given procurement.

Other states also have procurement requirements for competitive bidding prior to awarding a contract, as well as other requirements. Maverick buying and incidental purchases aside, it is typical that no state may purchase goods from a Supplier that has not first been awarded a contract by that state pursuant to applicable procurement processes. Some states will allow the purchase of goods from a Supplier that has been awarded a contract to sell such goods to another state if that state has substantially similar procurement regulations. States that have entered into joint purchasing agreements, also known as cooperative procurement agreements, may also purchase from Suppliers that are primarily associated with another state or with a joint venture among several states (see Hypothesis Two, Existing Cases).

Since the transactions conducted via the EMall system constitute the purchase of goods, it was necessary to assure that the EMall sufficiently accommodate each state's procurement requirements. These requirements created some additional legal and technical overhead beyond what would have been required by non-public buying entities. Although large private organizations also become encumbered by

inordinate and unnecessary layers of processes related to procurement of goods, government remains the widely accepted leader in this area.

The EMall system was designed so that it could support and reflect quite rigorous requirements for any given Buyer without slowing or complicating the procurement process for other Buyers using the same system. Different workflow, approval chains to sign off on purchases, and other unique procurement-related requirements can be flexibly accommodated as part of the core functionality of the Intelysis system. Other requirements necessitated custom coding, kept to a minimum in the pilot, and new business practices surrounding the use of the EMall system.

The perceived need for “browse-only” functionality on the part of some of the participating states illustrates the type of novel legal and business issues raised in the EMall Pilot. The “browse only” Shopper is typically a User who only wants to access a contracted Supplier’s catalog, but does not want to build a shopping basket, return a Requisition or place an Order. Perhaps this User simply wants to compare pricing, or look at specific offerings available from the Supplier.

A work-around was needed within the IEC application to accommodate this role during the pilot period because technically there is no way to distinguish a “browser” from a Shopper, that is, one whose goal it is to place an Order with the Supplier. The work-around relied on Supervisor/Approver intervention through the Cancel Request functionality to enforce the "browse only" rules. The procedure included setting up the “browser” as a Shopper with a zero dollar-spending limit. This meant that the “browser” was allowed to fill a shopping cart and bring it back to the EMall for approval. The IEC application then would route the Order to an appropriate Approver. The Approver would then be required to identify the Order as coming from a "browse only" Supplier and cancel the Order.

Under this work-around, it is possible that an Order could be sent to a Supplier from a "browse-only" User without authorization to conduct a purchase. Due to the risks associated with this work-around, a decision was made to suspend "browse only" implementation during the pilot. If states feel that allowing all EMall Users to access all contracted Suppliers’ sites is a requirement for the production system, then a solution maintaining approval integrity will need to be developed.

In some cases, a Supplier and a State already had an EDI (Electronic Data Interchange) system in place. A version of the Model Trading Partner Agreement of the American Bar Association had been executed between the parties to such systems in the Commonwealth. Upon evaluation, it was determined that these agreements were not suitable as a basis for articulating the legal relationships among EMall Pilot participants. Among other shortcomings, contracts based upon the Model Trading Partner Agreement envision one to one relationships rather than the many-to-many relationships characterizing the EMall system. In addition, these EDI contracts assumed an outsourced value added network acting as a secure and reliable communications intermediary among the trading partners. By contrast, the EMall required

legal arrangements that were responsive to the special risks and processes associated with transferring business information via the Internet. In addition, the EMall legal structure had to be scalable and extensible, that is capable of supporting an ever growing population of users and of supporting dynamic and evolving business practices and modifications in technical processes.

Legal and Business Model Architecture for the Pilot

The legal model was designed primarily to support and reflect the business model for the EMall Pilot, which consisted of a Massachusetts sponsored and run e-procurement system in which other states could participate as buyers and through which a number of private vendors could sell their wares as suppliers. One of the implications of the fact that Massachusetts sponsored this pilot was that executive decisions regarding the technical, legal and business aspects of this project were in the domain of the Commonwealth. Similarly, an implication of the fact that Massachusetts ran the pilot rather than outsourcing the administration of the project was that the Commonwealth also made day-to-day operations and implementation decisions.

During the pilot, Massachusetts served as the Policy Authority, through the EMall Steering Committee, and developed the scope of work for the providers of the technical solution and integrator services as well as the certificate manufacturer. Massachusetts also drafted the Operating Rules that governed the EMall pilot.

Designating Roles and Functions

Though Massachusetts ran the EMall the decision was made to simulate, to the greatest degree practicable, a business and legal model that could be used after the Pilot. Such a model required that one or more additional or alternative parties be capable of carrying out several of the administrative and executive roles that were performed by the Commonwealth. To this end, the major roles were described separately with the various functions grouped accordingly under each role. Likewise, the Operating Rules were crafted with the goal in mind of becoming extensible to different governance combinations among states. Therefore, though the Commonwealth of Massachusetts played several roles in the pilot, each department, division and individual was required to observe all the rights and duties associated with business conducted under each role, just as though a different state or a private sector outsourced entity had performed the role.

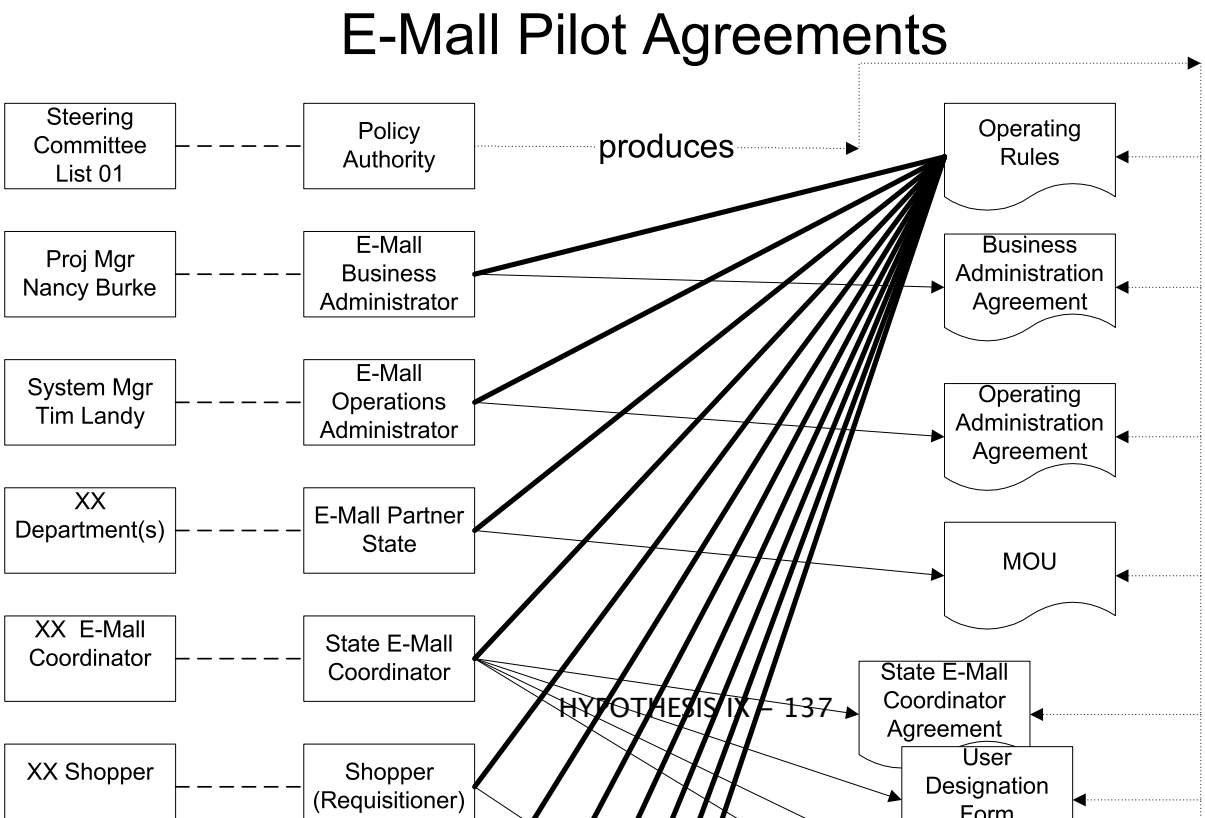
By way of illustration, a number of departments within the Commonwealth agreed to participate as EMall Users. These departments were required to sign the same Memorandum of Agreement as executives from other states and each state employee of each such department was required to sign and observe the same terms and conditions. Similarly, some individuals within the Operational Services Division for the Commonwealth sat both on the Steering Committee for the EMall, which acted in the Role of Policy Authority, and also performed as the Technical Administrator or the Business Administrator. These

individuals were required to sign an agreement and observe security requirements and to create the same audit trails that are similar to what an outsourced third party administration service would have had to sign. Again, these formalities were carried out primarily for the purpose of describing, testing and assessing the problems and prospects associated with carrying out each role within an EMall environment. They also helped us to better prepare a set of Operating Rules that would need minimal revision if other business parties were to assume any executive or administrative role within the system.

Operating Rules and "Opt In" Agreements

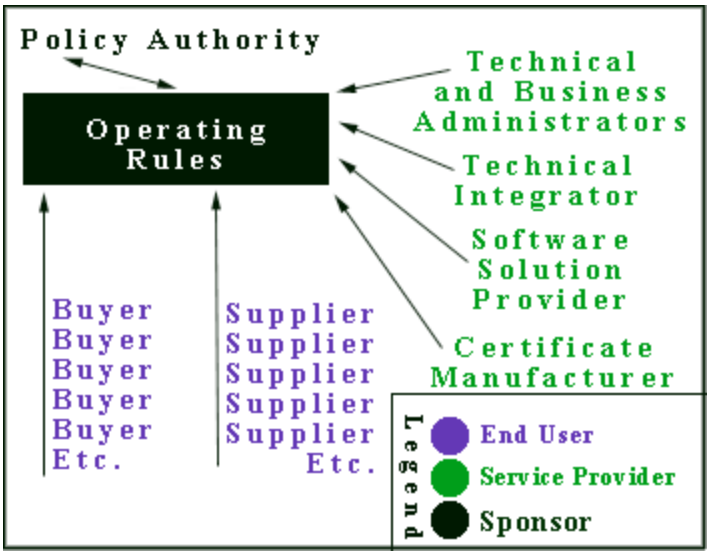
The EMall legal model was premised upon the assumption that parties to this e-commerce system can and should use contractual mechanisms to structure secure, enforceable and reliable business transactions among themselves. To enhance the ease of administration and simplicity of the legal documents, a single overarching set of Operating Rules, rather than many individual long contracts with each participating party, was developed for the EMall Pilot. Each party signed a relatively small "opt in" agreement whereby they agreed to abide by the terms and conditions in the Operating Rules. In this way, as the changing technical or business situations required amendments to the terms and conditions, it was not necessary to re-execute hundreds of individual contracts. Rather, under the "Notice" and amendment provisions of the Operating Rules, every party is given notice of proposed changes and an opportunity to comments and discuss. Once consensus is reached, the Steering Committee (Policy Authority) may execute a change to the Operating Rules. By virtue of each signed opt in agreement, all parties then become subject to the then current terms.

Below, included for purposes of illustration, is a pictorial representation of the interlocking agreements among the parties to the EMall Pilot. Note that any given state actually executes several documents. In



addition, buyers and sellers have pre-existing contracts for the sale of goods upon which the EMall legal arrangements rest.

The illustration below clarifies the types of parties based upon their "role" under the Operating Rules. The parties in green are service providers. During the pilot, some service provision was outsourced to external parties (e.g.: the Integrator SAIC, the Certificate Manufacturer Motorola) and others were performed in-house, such as the Technical and the Business Administrator roles which were conducted by staff from the Massachusetts Operational Services Division. The blue represents end users. The buyers are states and the suppliers are private vendors who have contracts to sell to one or more participating states. The black is the policy authority, which was the Commonwealth of Massachusetts during the pilot because the Commonwealth initiated, subsidized and administered the project. The policy authority produced and also agreed to abide by the Operating Rules. The other parties signed agreements whereby they opted into a promise to abide by the Operating Rules and thereby enjoy the benefits of the EMall system. The arrows pointing toward the Operating Rules designate an agreement to abide by the rules.



Results

This section evaluates the EMall Legal/Business model in light of the pilot experiences. The following observations were made:

- Individual User Opt-In contracts are too cumbersome for this business-to-business e-commerce application
- The flexibility of the model can facilitate potential outsourcing
- The Operating Rules revision and notice process works well
- State digital signature statutes can be a barrier to entry
- The use of client certificates pose unnecessary business, legal and technical problems
- The pre-packaging of public label root certificates in web browsers and servers created business, legal and technical problems

Individual User Opt In Contracts Too Cumbersome for B2B

The legal contracts underlying the EMall were, in retrospect, over inclusive and over numerous in view of the costs, benefits and risks associated with the system. While this has the potential to be a multi-million dollar system, the best models in the private sector of similar scope and depth suggest that there is no need for a central intermediate entity to keep signed contracts for every individual buyer within every participating buying institution. The overhead associated with distributing, retrieving, correcting, storing and accessing each such contract was inordinate. The Pilot was of relatively limited scope and it included hundreds of individual user contracts. An implementation system with thousands or more such contracts would be costly and unnecessary in a B2B environment.

Rather, it seems adequate to include additional provisions within the general contracts executed by the buying institutions wherein the executives agree to manage their users. The executives are made responsible to notify each user of certain relevant facts such as obligations to safeguard passwords, duties to maintain integrity of system, and legally binding result of using system to purchase goods. The institution would also have to agree to stand behind the actions of each of its own users to the extent it created certain types of liabilities within the EMall system. Beyond this point, however, each institution should have the flexibility to manage its own users as it sees fit and in accordance with its existing management and technical support systems. In short, a more distributed legal system for individual end buyers is appropriate for the EMall system because the fundamental legal entities that agree to participate are business or government entities and not individuals. Hence, only the organizations should be dealt with directly in future EMall legal arrangements.

Flexibility of Model Can Facilitate Potential Outsourcing

As has been noted, the Operating Rules and the business relationships were designed to allow maximum flexibility in mixing and matching different parties to different roles within the EMall. Outsourcing some of these functions, where economically advantageous, should be eased by the flexible design built into the model.

With the prospect of significant growth in the number of EMall participants in a production system, it may be desirable for the administrative roles such as business manager and technical administrator to be outsourced in a future implementation. The functional processes required for each role have already been established through the course of the pilot, a fact that should ease any potential outsourcing of these roles. It should be noted that the execution of these administrative duties is different from the executive decision making duties associated with the role of Policy Authority - which can not and should not be outsourced. However, a future implementation model may require that additional parties join directly or indirectly through advisory or other committees in the duties of the policy authority.

Operating Rules Revision and Notice Process Works Well

The EMall Operating Rules went through a revision process from version 1.1 to version 2.0 of the Operating Rules during the course of the Pilot. The system notice and comment period operated in a timely and efficient manner. The current version of the Operating Rules is 2.0. It may be advisable to facilitate further automation of the notice, comment and approval process for revision of the Operating Rules through use of e-mail (pushed) and web (pulled) notices, as well as web-based discussion. More automated processes should also be reviewed as part of the contractual opt in process for agreeing to the Operating Rules.

State Digital Signature Statutes Can Be a Barrier to Entry

When the state of Washington was considering joining the EMall pilot, its digital signature legislation posed problems because it required that a licensed "certificate authority" be used to issue certificates for any official business conducted with the state in which a digital certificate was used. The general business and legal model underlying a "certificate authority" is different from the B2B business and legal models that characterize the EMall Pilot.

The B2B relationships in the EMall rely on contracts, agreements and Operating Rules that describe the duties, processes, liabilities and rights of each party. In order to use a Washington state-licensed CA, parties must become subject to the legal rules governing the use of certificates under the digital signature law of that state. That law would create non-standard and problematic legal terms that would conflict with the desired and contracted terms for B2B commerce under the EMall Pilot. Following are some examples:

- The Washington law would require that there be a rebuttable presumption that a document was digitally signed under certain circumstances. The EMall Operating Rules set the terms differently.
- The Washington law would have created a liability limitation for the entity issuing certificates. The EMall contracts set the liabilities differently based on the negotiated terms between the parties.
- The Washington law envisions an "open" use of issued certificates with potentially any party in the world. These terms were different from the bounded and closed use of certificates within the EMall system - where parties are supposed to limit use of certificates only to use with other authorized EMall Parties.
- None of the nationally known certificate providers with whom the EMall Steering Committee discussed outsourcing certificate services have chosen to become licensed under the Washington law. The market has not generally opted to follow the regulatory direction of the Washington law.

Since Washington law restricted their state government from conducting official state business with certificates issued by companies that were not licensed under the law of that state, Washington was unable to participate. The other states that participated in or observed the EMall have no such restrictions and were fully able to agree to the business agreements with the private suppliers and the other participating states. In fact, as far as we know, Washington is the only state that requires that a licensed CA be used with their state government. It is unclear whether Washington would have opted to join the EMall even if the CA problem had been overcome, however, that became a moot point in view of the restrictions under Washington law.

The underlying purpose of these regulatory, technology-specific laws was to bolster use of public-label certificate authorities. The EMall pilot revealed that use of such public label root certificates is itself problematic in a bounded B2B e-commerce environment, as detailed later in this Section of the Evaluation. This session of Congress, legislation in both the U.S. House and the U.S. Senate has been filed and has been reported out of sub-committees which would have the effect of preempting certain types of digital signature specific state statutes. Massachusetts has sent representatives to both chambers of Congress to testify in favor of such a legislative result. Florida has recently captured the distinction of being the first state to voluntarily repeal its CA licensing statute. Though only a few states have such laws in effect, the repeal of the remaining such statutes would simplify and improve the legal environment surrounding use of public key certificate systems like the EMall.

Use of Client Certificates Pose Unnecessary Problems

The use of client certificates presented several difficult and unnecessary legal, business and technical problems. In short, the end user software is not sufficiently mature to warrant use of this technology nor are the business practices. For a full discussion of the use of digital certificates in the EMall please see

Hypothesis Eight. This discussion will concentrate on the legal and business issues raised by the use of client certificates.

Because the pilot used client certificates in its security implementation it became necessary to develop appropriate content for each field in the certificate such as the syntax of the name, the place, and the associated organizations. It quickly became apparent that the X.509v3 field definitions raise far more questions then they answer. For instance, there are no generally recognized conventions regarding the type of content that is supposed to occupy several fields or what that content is supposed to mean. The country code for an institution, for instance, may mean the place it is incorporated, or its primary place of business, or where a particular computer resides, or any other semantic meaning an individual chooses to assume when filling that field with data.

An even clearer example of this difficulty was illustrated in a recent debate among technologists, academics and lawyers participating in the Internet Engineering Task Force PKI group and related groups' e-mail lists on the topic of the "non-repudiation" bit field in an X509v3 digital certificates. If a certificate had the field turned "on" one might wonder if transactions associated with the certificate could not be repudiated. Perhaps even more interestingly, if the field is "off" - does that mean transactions may, will or must be repudiated?

The question of whether a transaction may or may not be repudiated depends on a complex and voluminous array of factors, and the existence of a single bit (on or off) with no additional context is likely to obfuscate rather than clarify the expectation of the parties. A person receiving a certificate with such information out of context in a public system may not correctly guess the meaning intended by the user or issuer of that certificate. It should be noted that this is not as likely in a bounded system, like the EMall, where a finite number of parties agree to details of meanings and processes. The confusion surrounding the presence of these types of fields demonstrates the relatively immature state of public key certificate usage in open systems.
In short, the semantics of the X.509 certificate profiles are not widely understood or accepted and had the effect of slowing rather than facilitating secure electronic commerce in the case of the EMall. In the end, the EMall system used pseudonyms to designate each user rather than using the person's real name. The pseudonym was a user number given by the EMall system much like an account number associated with a bank account.

The Pre-Packaging of Public Label Root Certificates Creates Business, Legal and Technical Problems

The EMall pilot encountered significant difficulties as a result of the inclusion of so called "trusted roots" in off-the-shelf web software. This issue is related to the decision by the major Web browser manufacturers and Web server manufacturers to include root certificates in their software. The result of this decision is that web communications that are authenticated by use of a digital certificate issued by one of the

companies with an embedded root are automatically "trusted." In other words, the web server and/or web browser will indicate that the digital certificate has been issued by a trusted entity and, by implication, may legitimately be relied upon.

This assumption is false in the context of the typical bounded B2B system, and it caused business and legal disruptions in the Pilot. In the EMall, the EMall server and supplier servers use certificates from public label CAs. The primary criteria for judging whether a person or entity is "trusted" to do business within the EMall is whether they have agreed to abide by the Operating Rules and whether they have been accepted by the EMall Administrators as a business partner after due diligence review of application materials. Nothing in the issuance or use of a public label digital certificate qualifies a person or entity to do business within the EMall or to be considered "trusted" in any way. More information on the definitions and implications of public label, or "open" versus "bounded" certificate systems, can be found in the Certificate Authority Rating and Trust Guidelines, issued by NACHA, and available through http://www.state.ma.us/itd/legal.

The mere fact that a certificate has been issued by one of the several entities that happen to have a root certificate embedded in commercially available software does not in any way qualify the user of such a certificate to do business in the EMall system. As a business grade application, the EMall requires that parties sign contracts, accept certain liabilities, and otherwise conform to an array of duties and expectations. The use of a certificate was intended to bolster the authentication of parties who were already part of the EMall system.

Even if a so-called "public certificate authority" had issued a certificate to an entity called, say, Universal, Inc., which would not necessarily mean that entity was the same Universal, Inc. with whom the EMall has a business relationship. There are many other such companies that legitimately use the same name such as Universal Studios, Universal Plumbing, and Universal Software Company. The other data beyond the name which may be gleaned from a certificate such as date of issue, and country code does not provide sufficient information from which to make a judgement about whether to rely upon the certificate.

In a non-trivial application like the EMall that supports hundreds of thousands of dollars in trade among hundreds of entities, parties conduct transactions based on trust. Trust-worthiness is determined through actual business reputation, prior course of dealing, recommendation by peers, pre-determined liability allocation and other elements upon which trust is built. A generic public label certificate cannot impart this type of trust.

Just because a certificate authority issued a certificate to an entity with which the EMall has no prior course of dealing, the software should not create an assumption that the person's digital certificate is "trusted" for any business transaction. That person or entity must first be accepted as a business partner,

must sign an agreement to abide by the rules of the system and otherwise meet certain minimal due diligence requirements.

Similarly, even if a certificate were issued by a public CA to an individual or business that had already been accepted as a business partner in the EMall, unless that CA itself agreed to follow the business rules of the EMall, it would be nearly impossible to correlate the issued certificate to the business partner. How many people by the name of John Smith exist in the United States? The underlying agreements for every CA to use the same unique identifier for every individual are years away from coming into existence.

Further, current wisdom regarding privacy of individual information suggests that a single identifier for every individual poses more problems that it solves. Rather, it seems more cost effective and consistent with sound public policy to issue certificates based upon pre-existing relationships. For instance, the EMall came to agreement with an entity, Motorola, to issue unique branded "EMall" certificates to the users of this system. Only legitimate users are entitled to receive EMall certificates for authentication, as with an EMall password.

The premise underlying this decision is that certificates should follow trust, and trust should not follow from a certificate alone. That is, after a business trust relationship is demonstrated, a certificate and other technical means of authentication are appropriate to confirm the identity of the individual or entity that was deemed trusted. No external "third party" certificate authority can make the determination of who or what the EMall will deem as trusted. The definition of a "third party" public certificate authority is antithetical to the business grade requirements of an e-commerce application like the EMall. Only first or second parties to the system have the knowledge to identify any given party as trusted or not trusted.

EMall Server Root Certificate Issues

One of the several difficulties that emerged from the inclusion of trusted roots within server software was that any certificate that was issued by one of the several included CAs would automatically be accepted. Additional custom programming was necessary to block out non-EMall authorized certificate manufacturers. In one test, a VeriSign certificate was acquired in which the name field included the same name as an accepted EMall user. In a test, that certificate was accepted into the EMall application on the EMall server. This was considered to be a serious flaw, since no public label CA does or should restrict issuance of certificates that happen to contain the same names as are correlated to EMall users. However, only legitimate EMall users may gain access to the EMall system.

The EMall system was designed to allow users from across the country and in large numbers to opt into the project. The scalability requirements, however, do not mean that a public label CA is in any way adequate or appropriate to fulfill the business and legal requirements of the EMall. Rather, a genuinely

trusted certificate manufacturer is needed - one that is trusted because it agrees to abide by the business, technical and legal practices designated by the Policy Authority for the commercial system. The critical point here is that if a public label CA were to agree to such requirements, and if it were accepted as a partner, then it would actually be a Certificate Manufacturer and not a Certificate Authority. This is because the "Authority" in a bounded B2B system does not reside with the party that happens to make certificates, rather it resides with the Policy Authority, whom pays for and governs the technical and business processes. Again, for more information on these models and definitions, please see the Certificate Authority Ratings and Trust (CARAT) Guidelines, at www.state.ma.us/itd/legal.

EMall Supplier Public Label Server Certificates and Public Label Roots in User Browsers

The only context in which public label certificates and roots were not problematic involved creation of secure sessions between users with browsers and some web servers of suppliers. In order to set up an encrypted session between the user's browser and the supplier's server, Secure Sockets Layer (SSL) encryption was implemented. Supplier servers with public label server certificates like VeriSign or GTEI CyberTrust could create an SSL session with any commercial off the shelf browser, since the browser already had the root certificate of the public label CA pre-packaged into the software. In this case, however, all that is really needed is encryption and the data in the server certificate was not especially important to users which is typical among all browser users connecting to public label server certificates. Nonetheless, since SSL does not allow encrypted sessions without a server certificate (browser certificates are optional), it was generally easier to use the public label server certificates since they did not require installation of yet another root on each desk top PC of each user in the EMall pilot.

EMall Transaction Server Certificate Issues

In order for an EMall purchase order - also referred to as an "OBI Order" under our technical specifications - to be legally binding, a supplier must be able to determine that it originated from the EMall transaction server. In addition to such data as the IP address and certain message content in the OBI Order, suppliers were directed to check the certificate of the EMall transaction server to assure authentication of origin. The EMall Operating Rules clearly spell out the timing and circumstances upon which allocation of loss rules will shift the legal burden to make good on orders from the seller to the buyer. After an order has been received in accordance with the technical specifications discussed in the Operating Rules, the buyers are "on the hook" to be bound by the transaction.

A public label certificate was used to authenticate the transaction server because a Motorola certificate could not be embedded in the transaction server due to technical configuration limitations. The result of using this public label certificate was that the transaction servers of the suppliers would automatically accept as "trusted" any facially valid order of goods that was transmitted from a source that happened to have a certificate from this public label CA. The public label CA does not constrain its practices to check whether a certificate applicant is a member of the EMall, nor does the public CA accept liability for

transactions gone bad as a result of such reliance. This made it especially worrisome that any EMall supplier may actually trust the so-called "trusted" root. This security and risk-management problem was handled during the pilot by adding certain internal controls and through specially crafted multi-party agreements specifying confidential data associated with valid OBI EMall orders.

The “trusted” roots, in practice, designate certificates that should NOT be trusted, in the context of the EMall Pilot. Ultimately, it was required that the suppliers spend more resources for additional custom programming to parse the certificates in order to distinguish the valid EMall certificate from all others issued by the public label CA. If the public label CA happens to issue another certificate with the same name as the EMall transaction server, then this control will be useless. Whether the public label CA does issue such a certificate is totally out of the control of the Policy Authority or any of the parties participating in the EMall. Motorola, the Certificate Manufacturer for the EMall agreed by contract to stand behind relevant business and technical practices and issued certificates that conformed to the policy requirements of this e-commerce application.

Summary

The advent of e-commerce and the new digital economy is causing a fundamental restructuring of institutions and practices in the public and private sectors. In many ways, the EMall pilot reflects these broader changes in prevailing business models and novel relationships between commercial parties.

The Pilot has shown that the new general business/legal framework developed for the EMall implemented through the Operating Rules and Opt-In Agreements has worked well. The most significant business, legal and technical issues encountered during the Pilot are attributable to the implementation of client and server digital certificates. Following are the specific observations that can be made as a result of the Pilot experience:

- Individual Opt-In contracts are too cumbersome for business-to-business e-commerce
- The flexibility of the model can facilitate potential outsourcing
- The Operating Rules revision and notice process works well
- State digital signature statutes can be a barrier to entry
- The use of client certificates pose unnecessary business, legal and technical problems
- The pre-packaging of public label root certificates in web browsers and servers creates business, legal and technical problems

Recommendations

1. The EMall business/legal framework of Operating Rules and Opt-In Agreements should be retained with appropriate modifications.

The EMall business/legal framework appeared to work well under the Pilot and should be followed in a production system. For purposes of streamlining the process, it is desirable to require opt in contracts only from the participating institutions and not from each individual employee. The institution's contract should include clauses regarding minimum duties with respect to the management of their internal users.

2. The use of digital certificates should be carefully reconsidered

The use of certificates presented inordinate legal and business problems and should be completely re-examined based upon an analysis of the benefits and the costs of such technology as well as the underlying transaction risks associated with the business. The use of internal passwords for users within an institution and of institution to institution authentication (such as with the IPSEC protocol) may be sufficient. Use of certificates simply to authenticate institutional servers, such as with IPSec, server to server SSL and the like, does not involve the same administrative overhead and can be limited to private label certificates with ease. In this way, local IT administrators may continue to handle individual internal passwords for various systems on their site, but such data as the identities, private authentication data and sensitive security information related to individuals will not flow beyond each institution.

If certificates are used more broadly, it will be important to avoid use or acceptance of so called "public label" certificates or any so-called "trusted root" that is pre-installed in software. Rather, it is important to bring the entity that issues certificates under contract to abide by the policies and business practices associated with the EMall system. Finally, the possibility of using online dispute resolution as provided under the current Operating Rules should be more fully explored as a way to manage risks and to reduce costs.

3. Contractual agreements for EMall products and services will have to be revised.

The contractual agreements through which EMall products and services are provided will have to be considerably revised in view of the fact that the scope of work contemplated was carefully tailored for a pilot only. The need to revisit these underlying contracts will be especially pronounced if a future implementation will entail any change in any product or service provider, or if the Commonwealth is no longer the primary or sole entity responsible for procuring these products or services.