Experiences of establishing trust in a distributed system operated by mutually distrusting parties

Scott Crawford, Enterprise Management Associates, Boulder, CO, USA
Email: scrawford@enterprisemanagement.com
David Chadwick, University of Salford, Salford, England, M5 4WT
Email: d.w.chadwick@salford.ac.uk

Introduction

The organization that is the subject of this case study is engaged in the worldwide monitoring of environmental information. This information provides evidence about the production of contaminants in one country that can be harmful to its neighbors. The project, which started in early 1999, was to develop an IT system that could authenticate data collected from widely distributed sources, in a manner that could be trusted by the participating countries, even though those countries might not trust each other.

Because of the potential political implications of this monitoring activity and the data collected, the subject organization represents the interests of the governments of the participating countries. Therefore, conclusions drawn from the collected data must be based on a reasonable degree of trust in the integrity and authenticity of the data and the data collection, archiving and distribution systems involved.

Because the interests of multiple sovereign and independent nations are involved, none of the participating nations is willing to subordinate its national interest to the subject organization by allowing the organization to speak on its behalf regarding the veracity of the data or any evidentiary conclusions that may be drawn or implied. For example, while a chemical or nuclear accident such as the 1984 Bhopal, India or 1986 Chernobyl disasters could conceivably produce contaminants indicative of hostile military activity, to draw such a conclusion from the data collected from a similar accident would be in error, but not outside the realms of possibility for one nation seeking to thwart the national interest of another nation in which such an accident had taken place. Therefore, one of the principal goals of the data authentication system was to assure that the trust placed in it – and, by extension, in the data itself – be a matter shared amongst, if not all, at least a significant enough number and distribution of participant nations to give a reasonable assurance to the organization as a whole that the integrity and veracity of the data is trustworthy. Each participant nation or any other observer would then be free to draw their own conclusions as they see fit.

To support this goal, the monitoring regime involved in collecting the data was developed along the following lines:

- Its human structure paralleled that of the organization itself. Its policy-making bodies were designed to be democratic and deliberative, and its operational staff developed along lines of proportional representation of participating nations, with oversight by the representative policy-making organs.

- Technical systems were developed to reflect the collective and representative nature of the organization. The data collection system was designed around the placement and distribution of monitoring sites worldwide, with locations distributed among as many participating countries as possible to monitor the global environment as a whole. A number of scientific disciplines were involved, for purposes of confirmation and cross-referencing of data indications.

Monitoring is continuous wherever possible. Monitoring sites have been networked with data management centers to enable timely collection and analysis. The data itself, as well as the data collection, archiving and distribution systems, are open to the scrutiny of all participating nations. The influence of any one or minority of participants on the data – particularly nations hosting monitoring and networking sites – should be minimized as far as possible. This was to be achieved by the participation of representatives of the subject organization in the construction, operation and maintenance of the data collection sites.

System Trust Requirements

These principal considerations influenced the nature of the IT system that was developed to authenticate the veracity and integrity of the collected data. Organizational policy-makers required the authentication system to implement an architecture that distributed the trust among the participants. Policy-makers further required the authentication architecture to parallel the construction of the data collection system and to be open to the highest possible scrutiny and periodic evaluation by representative groups. This requirement, however, had to be balanced against the need to protect the system and its individual sites and components from exploitation. For example, a malicious party seeking to blind the organization to polluting or contaminating activity in a specific location might seek to interfere with the monitoring ability of a site through interfering with its network connectivity or system operation. It also had to be balanced against the risks posed by a pragmatic need to delegate contractual, implementation and operational responsibilities to those having the necessary expertise. Such delegation was, however, subjected wherever possible to oversight by representative groups reflective of the collective nature of the subject organization as a whole. An overriding principle was that no part of the system installation or operation that formed part of the trust infrastructure, should be entrusted to a single individual.

Proposed Solution

Because the monitoring data could be represented as either a networked bitstream or a discrete message, it was determined that digital signatures could be applied as a means of assuring data authenticity. Pioneered by [DH 76] and elaborated in [RSA 78] and subsequent innovations and standardizations (e.g. the PKCS#1 standard for the RSA algorithm [PKCS 1]), public key cryptography (PKC) implements digital signatures through the combination of public/private keypairs and hash algorithms. Encryption of the data with a private key and successful decryption with the corresponding public key assures that only a specific private key could have performed the encryption. If the encrypted data is a “one-way” hash of the actual subject data, such as provided by the Secure Hash Algorithm (SHA-1, [FIPS 180-1]), it provides a tamper-evident assurance that the data has not been altered since encryption, when the decrypted hash matches one generated over the received data. The authentication system in this application was therefore centered on digital signing of the data at the monitoring site at the time of observation, and as close to the data source as possible so as to limit opportunities for data alteration. Streaming networked data could be divided into discrete transmission frames to which individual digital signatures could be applied.

But while digital signatures may provide a mechanism for authenticating data, of themselves, they do not address the issue of distributing trust amongst the participating nations. For example, a recipient needs to know which private keys have been installed at which data monitoring sites, and that it has the correct corresponding public keys in its possession.

Review of Previous Work

Prior to implementation, other relevant implementations of PKI technology were studied so as to provide insight into how trust can be distributed amongst competing, and possibly mutually distrusting, member organizations. Candidate organizations were multinational organizations involved in international finance, banking and exchange systems. The stakes of individual participants in these multinational organizations, concerning the authenticity of information and data exchange, which represents large sums of money, are at least as significant as the risks borne by the participants in the subject organization.

One of the most significant parallels was found in the establishment of Identrus LLC, which took place at approximately the same time as the early stages of the subject implementation. Founded in April 1999 by eight leading US and European banking and financial institutions, Identrus was created for the purpose of establishing an architecture of trust in electronic transactions between participating banks and institutions, and between their customer businesses as well ([Identrus 98], [Identrus 02a]). One of the original participants in Identrus was the US company CertCo ([Identrus 98]). CertCo was differentiated from its competitors at the time by its implementation (with IBM cryptographers) of threshold public key cryptography ([Ankney 00]). [Desmedt 92] describes the goal of threshold PKC as a scheme "in which the power to perform a certain operation is shared." In a threshold cryptosystem, the factors of a key are *distributed* among a group such that, when the group members contribute their factor components for combination enabling an encryption operation, they do so without divulging their individual components to each other. More to the point, a threshold cryptosystem requires a minimum *threshold* number *m* out of the total number *n* (described as "*t*-out-of-*l*" in [Desmedt 92]) of all possible participants to contribute their components in order to enable the encryption operation.

Threshold cryptography was therefore studied as a possible enabling technology for the distribution of trust between the cooperative yet mutually-distrusting participants in the subject organization. However, a threshold technique posed significant operational complications when considered for application of digital signatures at the data source of an environmental monitoring station. Instead, attention turned to a threshold implementation in the management of the data-signing keys. Because a system of digital signatures relies on the integrity of the private keys used to generate the signatures, a system of management of the corresponding public keys predicated on the then-current X.509v3 standard of digital certificates [X.509] was decided upon. The use of threshold cryptography in generating the digital signatures on the certificates of the issuing certificate authority (CA) was considered.

Threshold cryptography was not, however, a panacea without its own flaws. [Langford 96] illustrated certain vulnerabilities in systems then current: A colluding subgroup of the minimum required number of participants was able to manipulate a forgery of a threshold signature without the knowledge of the other participants (effectively reducing *m* to 2-out-of-*n*, regardless of the intended size of *m*). A malicious participant was able to influence public key generation such that they were enabled to discover the complete private key which is supposed to be unable to be discovered by any participant or used without the threshold number of participants. The conclusion drawn by [Langford 96] was that systems "without a trusted key generation center…are more complicated than those that do allow a single trusted center and are therefore more vulnerable to manipulation." [Desmedt 97] pointed out that not all threshold algorithms had progressed to an equal state of security in their development. In particular, [Desmedt 97] noted that, at the time, "no practical threshold [implementation of] DSS [the

Digital Signature Standard implementation of the Digital Signature Algorithm (DSA), now [FIPS 186-2]]…has been presented so far."

The lack of threshold DSS conflicted directly with the preference of a number of the participant nations for the use of DSS in data signatures. At the time, many national governments had concerns regarding the export of encryption technology, and did not want an organization representing their national interests to be accountable for potentially enabling undesired access, potentially worldwide, to an encryption technology such as RSA, in which either public or private keys could be used to encrypt digital information. DSS was therefore preferred, as DSS private keys could be used (in principle) *only* for signature generation, and the corresponding public keys *only* for signature verification. Thus, non-DSA-based algorithms – including threshold cryptosystems then available – were ruled out.

The example of distributed trust as manifested in *m*-out-of-*n* threshold key management and certificate authority implementations was, however, retained in a requirement to implement a distributed key management system. A "mixed" system of threshold-based certificates of DSS signing keys was briefly considered, but abandoned due to the above-related issues with threshold cryptography and algorithm preference, as well as the problems foreseen for a system of mixed algorithms. Instead, an administrative, rather than technical, implementation of *m*-out-of-*n* signature generation in the issuance of DSA-signed certificates was undertaken. After an evaluation of solution providers worldwide, the UK company Baltimore Technologies was selected to provide tools and systems for implementing an *m*-out-of-*n* key management system predicated on DSA. A number of other vendors from several different nations participated in the implementation of DSA signature generation software at the data sources.

Initial implementation

The Baltimore Technologies implementation was selected, in part, because of its flexibility in "customizing" a CA architecture to the needs of an organization, including its ability to use multiple Registration Authorities (RAs) and Registration Authority Operators (RAOs) to meet the administrative *m*-out-of-*n* requirement in the issuance of digital certificates. In Baltimore's PKI, RAs are client systems that submit requests for an X.509v3 digital certificate to an issuing CA server. RAOs are parties (usually humans) that interact with the RA to enable the approval of a certificate request for forwarding by the RA client to the CA. The certificate request comprises the public key to be certified and other relevant information about the key and its holder, formatted according to the PKCS#10 standard [PKCS 10]. Baltimore's PKI supports both single and multiple RAs interacting with a CA to request a certificate, as well as multiple RAOs interacting with an RA before a request can be sent to the CA. By mandating that multiple RAOs must request the same certificate to be issued for a data monitoring station, effectively distributes the trust placed in the operation of the CA to the number of RAOs that are involved in issuing the certificate requests.

The implementation was staged over periods of preliminary design, pilot testing, final design prior to initial implementation, and the initial implementation itself. Laboratory implementations of the data signing architecture were developed to test the processes of: keypair generation, certificate request and issuance involving *m*-out-of-*n* RAOs, signature of actual data, transmission of data and signatures via networks, management and retrieval of digital certificates, and the use of certificates in signature verification of data. Parameters and issues of general system operation and maintenance were also evaluated.

As preliminary system design took shape, distribution of trust in the system became manifested in a variety of ways beyond key management *per se*. As noted earlier, a number of scientific disciplines were involved in the monitoring regime, to give corroboration and cross-referencing of data supporting indications of specific contaminants and contaminating actions. Thus trust was distributed across a number of monitoring techniques, from measurement of atmospheric compounds to highly sensitive detection of vibrational information transmitted through the earth's oceans and the earth itself. Such multiplicity of data sources and types contribute to the weight of evidence in any given case, even in cases where signature-based authentication at any one monitoring site or minority of sites might be compromised.

Multiple parties were also involved in the construction and deployment of specific monitoring sites as well as the central data collection and management points supporting the system as a whole. In each case, representatives of the entire range of participating nations were involved, reducing the possibility of subversion of critical system components at virtually every key point.

Distributing Responsibility

Such a distribution of responsibility was not, however, without its cost. In the development of the authentication system, at least six, and sometimes more, different contractors spread throughout the world were involved in the detailed technical specification of the various components of authentication. In some cases, different contractors were delegated responsibility for the elaboration of the signature-implementation systems for different monitoring disciplines. Differences in standards were also required for different data transmission techniques (i.e. networked bitstreams versus discrete or "segmented" messages). The organization defined its own standard technique for signing streamed data by allowing a 40-byte space for a DSS signature in each transmission frame. Segmented message-format data had to be signed according to a standard that could be interpreted by both the implementing contractors and the subject organization. The standard chosen was that in most common use at the time, S/MIMEv2 (Secure Multipurpose Internet Mail Extensions) [RFC 2311]. S/MIME defines how to create a MIME body part that has been cryptographically protected according to [PKCS 7]. However, neither S/MIME nor PKCS#7 define the object identifier to be used with the DSA/DSS signing algorithm (they only specify ones for use with RSA). Therefore, accommodation was required among the contractors to enable the DSS signing algorithm. Laboratory implementations were ultimately successful using a variety of tools, including adaptation of open source reference implementations such as OpenSSL (then at version 0.9.5).

One of the implications of the unique nature of the monitoring regime was the necessity for custom developments in certain monitoring installations. For example, certain subterranean monitoring installations at deep levels below the earth's surface posed special problems for system endurance and form factor, as did underwater detectors placed beneath the ocean's surface. In certain cases, placing signature-generation devices at the *exact* point of data collection were impractical. In many cases significant barriers and challenges had to be overcome. For example, in some installations, the technologies necessary to compose standard certificate requests strictly formatted to PKCS#10 were beyond the physical and technological constraints of the systems at their then-current state of development. The solution to this involved on-site personnel obtaining "raw" public key information from such devices. The absence of a formal PKCS#10 request and an associated signature generated by the corresponding private key (which, when verified by the public key contained within the

PKCS#10 request, is a crucial step in demonstrating certificate request integrity and private key ownership) would be compensated for by the presence of on-site observers who received and verified the integrity of the generated public key from the remote constrained detector. The public key material thus obtained would then be sent in one or more PKCS#7-compliant messages to a key management center by the on-site observers. At the key management center, an adaptation of certificate issuance systems was developed to permit direct submission of such public key material to the CA when verified by the RAOs. Laboratory tests of this combination of techniques were successful in obtaining a certificate for a keypair generated in this manner. Demonstration of the integrity of the process was verified by the auditable recording of participant actions in order to preserve the "chain of trust".

This technique illustrates one example of how the presence and participation of multiple persons at virtually every crucial step of the authentication system became essential to establishing and maintaining the concept of distribution of trust, necessary for the system as a whole. Implicit in such a system, however, is the necessity of informed human participation; but this, after all, is to be expected in a system predicated on trust, which is essentially a human phenomenon. A certificate-authority-based key management architecture is, by definition, based on an assumption of trust in the authority itself. Trust, however, may be interpreted and manifested in a multiplicity of ways ([Mayer et al 95], [AJ 98], [Kramer 99]). Multiple parties may not – perhaps *will* not – all agree on their individual perceptions of what is trustworthy and what is not. However, the assumptions made in the design of this system considered that when a significant number of participants were agreed that they could place their trust in a system consisting of a number of verifiable measures and components, the requirement for trust distribution would be satisfied.

This also, however, implied that a certain number of duplications in implementation would be necessary to assure the necessary participation of multiple parties at significant points in the architecture. No one person could be allowed to operate alone in the presence of crucial system components, when those components might be susceptible to exploitation by an individual. The system would have to enforce multiple authorizations for access, manipulation and control beyond the requirement of *m*-out-of-*n* necessary for certificate issuance. The possibility existed that system operators might be required to be responsible for several components such as smartcards and other tokens necessary to enable operation of certain system elements. Backups of key material would have to be distributed among a number of points, all in an auditable fashion.

To meet these exigencies, a minimum set of qualities were sought as design goals. The threshold number of persons or components among which crucial elements of the system would be distributed would be kept to as practical a minimum as possible without subjecting the system to the susceptibility of individual operators. This did not rule out the actions of a malicious minority in all cases, but the sheer preponderance of numbers of persons and steps toward authentication involved throughout the architecture mitigated the possibility of such isolated actions subverting the system as a whole. Standards of procedure and operation would also be developed, with the intent that persons interacting with the system would be informed and knowledgeable. Operators would be instructed regarding what they would be doing and the reasons why trust in the system would be enabled by their actions, while those depending on the system for trusted demonstrations of authenticity would be aware of how and why the system should be trusted. System operations as well as the signed data itself would be auditable and open to scrutiny by appropriate parties, thus fostering the openness necessary to the development

of trust described in [Mayer et al 95], [AJ 98], [Kramer 99], and others. The use of OpenSSL in bespoke development of authentication components, for example, enabled clear examination of source code used in implementing authentication. Wherever possible, similar cooperation was obtained from contractors, sometimes in the form of "source code escrow," preserving the contractor's proprietary rights in maintaining source code confidentiality while enabling the organization to have the option of source code review should it be desired.

It would be inevitable that, beyond outright exploit, human as well as technical errors would eventually begin to be manifested in such a system, perhaps posing a more significant threat than malicious exploit. Again, however, the preponderance of the number of monitoring sites, the numbers of points throughout the architecture in which multiple parties would be involved, and the numbers of persons involved in critical operations, mitigated the potential consequences of any one error or a small number of errors. Added to these factors are data management systems at the data centers receiving the signed data that are able to alert operators when signature verification failures occur. The data centers hosted by individual participating nations help to verify the validity of such incidents and may themselves track such occurrences independently, thus helping to keep them from being hidden in a possible exploit scenario. Thus, a general development of "trust by consensus" in which the number of individual actions and steps in data authentication accumulate towards a body of data supporting trust, began to emerge as the system design progressed.

In summary, a description of the initial implementation proposed for the distributed management of trust is as follows. At the time a monitoring site is to be enabled with a digital signature capability, an on-site team of operators generates the keypair. If satisfied with the key generation process and the integrity of the resulting keypair, the on-site team then forwards the resulting public key to the key management center in one or more PKCS#7-compliant messages bearing the digital signatures of the on-site observers. At the key management center, the signatures of the received messages are verified against the signer's certificate(s) by a group of authorized RAOs. If a minimum *m* out of a total number of *n* RAOs agree that the signed message(s) containing the submitted public key are trustworthy based on signature verification and other verifications of the on-site observers' presence at the site, the RAOs approve the certificate request, and the certificate is duly issued by the CA. Signed data thereafter received from the site is verified on receipt at the data management center by signature verification using the issued certificate accessed from a local directory of certificates and certificate revocation lists (CRLs are as defined in edition 3 of X.509 [X.509]). This directory is accessed according to the Lightweight Directory Access Protocol (LDAP) described in [RFC 1777] and [RFC 2251], with an organizational namespace rooted on the name of the organization itself (being, as it is, an international entity).

System Maintenance

Yet to be fully elaborated are issues of key rollover and replacement of valid keys. The assumption to date has been that as the current key lifetimes reach their pre-determined limit (set to a minimum of 5 years) PKC technology will have matured to the point where a more evolved implementation may be indicated. Regardless, a preliminary protocol has been worked out, in which a currently trusted signing key is used to "countersign" the certificate request generated for a new keypair. Thus, a data generating system needs to be able to "cache" a currently valid keypair while awaiting issuance of the replacement keypair's certificate and authorization to use the new signing key. In cases where such caching is not possible, data would need to be signed

immediately with the new signing key. Authentication by the recipient is then contingent upon the issuance of the replacement certificate for the new keypair, during which time the validity of the site's data would be in a state of suspension. In any event, under such a scheme a new keypair would not be generated except on the site's receipt of an authenticated (digitally-signed) command issued by a minimum number of authorized parties, identified by certificates available to the site itself. Unauthorized keypair generation messages would be detected when data signed by an unauthorized key is received at the data management center. No authorized certificate would be available for data verification, and authentication would fail. In this case data from such a site would be "suspended" from authentication until on-site remediation was undertaken to restore the site to a trusted state.

In such a scenario, monitoring sites would need to have certificates of authorized command-issuers available to them, in order to enable command authentication. For any site installation, a certain number of individuals and groups must be delegated the responsibility for trusted operations on the site. Again, the limits of trust related to the number of individuals authorized to operate at a site is mitigated by the numbers of sites, the numbers of persons involved, and the oversight of such operations made possible by open scrutiny and the auditability of actions. In its role as the facilitating entity for the regime as a whole, the subject organization is able to call on on-site representatives and other means to monitor and corroborate site changes. It is also able to track any site changes that are authorized, thereby further mitigating the risks arising from trust placed in the site.

At the site, authorized signed commands are distinguished by the positive identification of the command-issuer through verification of the issuer's digital certificate. Without such verification, commands are ignored. To maintain the availability of the most up-to-date certificates, as well as information regarding suspended or revoked certificates, two methodologies were proposed. One was network-based access to directories containing certificates and CRLs; the other was on-site storage and maintenance of the necessary certificates and CRLs. The ultimate goal in the future is network enablement of certificate status checking for the most timely validation by the monitoring sites, using a protocol such as OCSP ([RFC 2560]). However, not all sites are currently capable of supporting such technological demands. On-site storage of current necessary certificates and CRLs will supplement such sites. In such cases, it is possible that, for example, an authorized individual whose authorization has been revoked may command a site as yet unaware of the revocation. Such cases are mitigated by limitations on access to the command-and-control functionality itself, and by requiring more than one individual to issue the same command (but this latter functionality has not been implemented yet). Also, the number of sites and persons involved spreads the individual risks. In no case would any one individual be authorized to command more than a significant minority of sites.

Local vulnerabilities in the monitoring sites are mitigated through a number of measures intended to develop tamper-evident installations that generate alerts whenever a site exploit is attempted. This is enabled through the triggering of functionality that includes site ill-state-of-health information in the data flow indicating that the site has been accessed. Cutting off the site's network connectivity in order to "blind" either the subject organization to an exploit or the site to the existence of, e.g., revoked command-issuer certificates, is detected by the absence of expected data from the site. This data cannot be mimicked to obscure the exploit without the attacker having access to the signing keys. Replay of valid data is not an option either, since the data contains replay detection information. Even scheduled maintenance may produce alerts of site intrusion, but such alerts are verified as scheduled maintenance from published operational

plans. There are, of course, limitations to the amount of trust that can be placed in such measures, but the "trust horizon" relative to the number of persons involved and their motivation to exploit is limited to the extent practical to the maintenance and purpose of the organization itself.

Initial results of implementation

At the time of writing, approximately one-fourth to one-third of monitoring sites have been equipped with the initial implementation of digital signatures and are sending authenticated data to the data management centers. While authentication of data in these cases has been successful, some of the most significant results are as follows.

The human interaction necessary to enable the system operation described above has been considerable. In particular, one of the author's personal experience in orienting operational staff and users to the system indicates that the learning curve alone is significant. Simply orienting users to the nature and operation of public key cryptography has been an abstraction difficult to communicate in many cases. Compensating for such challenges has been the high motivation and dedication of the subject organization's participants to fully understand the system. Thus, it is our subjective opinion that motivation is a significant factor in the success of such a trust-based system. In addition the aptitude of users to understand the operation of public key cryptography, as well as the ability of system developers to communicate the information essential to understanding, are essential to success.

The burden authentication technology places on data management systems themselves should not be overlooked. Performance measures of the time and resources necessary to authenticate a large number of DSS signatures received from stations continuously transmitting proprietary data protocol frames is not insignificant. System capacity planning and development is still taking shape to accommodate such demands. Computational and network resources are not the only demands placed on an organization seeking to implement a system such as this. Measures necessary to assure the security of all aspects of the implementation also take a toll on both human and material resources. A higher degree of vigilance and standardization of operational policies and procedures is necessary to assure the integrity of the system itself.

Nevertheless, the general consensus among users at this point appears to be divided between those who feel they understand the authentication system and those who do not. Surveys of users are currently underway to establish quantitative measures of success or failure of the implementation. Until they are received and analyzed, interviews with current system participants indicate that those who manifest an understanding of the system are satisfied that the system is functioning successfully. Nevertheless, they are not happy with the burden imposed by both the procedural and computational requirements of this distributed-trust implementation of digital-signature-based authentication. They are also less than satisfied with the "usability" of the human-interactive components of the system, which can be cumbersome and require the necessary understandings which can be challenging to communicate effectively to the involved personnel, as described above. Among those who do not express a high understanding of the system, the above-described burdens appear to be regarded as excessive relative to the benefits that are derived. It is not yet clear whether further education and dissemination of information regarding the system and its necessity to the requirements of the organization would help alleviate such concerns. However, future developments in the system will almost certainly take such measures into account.

Summary and conclusions

The most obvious conclusion drawn from this experience is that "distributed trust" means, first and foremost, distribution among people. While that statement may seem so apparent as not to even require being made, consider that first- and second-generation public key infrastructures (PKIs) such as this almost universally began as technological exercises. Focus on the algorithms and the technology of encryption and digital signature led to a number of implementations which did not sufficiently consider the human factors of trust, as well as other human factors such as how people perceive technology, how such perceptions affect their use of technology, and the relationship of such perceptions to assumptions – correct or not – made by system planners and developers, particularly as affects the success or failure of security technologies. This, in turn, led to the development of a framework for certification practice and certificate policies such as that described in [RFC 2527], but policies alone are not enough to compensate for the involvement of human beings in the technology of trust. Studies of human factors in security implementations such as [WT 98] and [WT 99] demonstrate that what often begins as a technology exercise often ends, successfully or not, as an exercise in implementing an appropriate understanding of the human factors involved. It is our belief that the technological limits of security implementation are often subject to the fact that both security and trust are fundamentally human concepts.

In the case of this implementation, the key goal was to implement a system in which all participants could trust the distributed data as far as it was possible and practical, notwithstanding the political nature of the organization and the lack of trust between the participants. It was essential to prevent a minority of persons with malicious intent from being able to subvert or exploit the data authentication system. Initially, this effort focused on the technology of distributing trust as manifested in the threshold cryptography system of digital signatures. Ultimately, the system has become one where trust is dependent upon the sheer numbers of people and systems that are involved, viz.: the number of points of data collection and their worldwide distribution necessary to obtain a reasonable number of overlapping systems and techniques of measurement; the numbers of participating nations and their representatives; the numbers of individuals involved in critical steps in the authentication process; and the volume of data itself. It must be noted that each of these factors was in existence in this organization before the authentication system itself was undertaken. Therefore, it would seem that authentication is dependent on the existence of the underlying factors that enable the necessary distribution of trust; the authentication system itself does not enable or distribute trust independent of these pre-existing factors.

Nevertheless, the system may at this point be judged a qualified success, in so far as it has succeeded in enabling a tangible measure of trust in the authenticity of the signed data, through the participation of a number of capable systems and motivated, knowledgeable individuals. However, the organization is distinguished as one which attracts individuals from throughout the world who are motivated to see it succeed. While this may in many respects be true of most professional organizations, the subject organization is able to call on the resources of national governments owing to the political nature of its existence. While environmental monitoring may not be a high priority with many participating governments, it nevertheless distinguishes the organization from, for example, those in the private sector with more limited resources. Only those organizations not just capable of, but also having a mandate for, fielding the necessary resources in terms of motivated, knowledgeable staff and technological capacity and development would likely be interested in such an undertaking. It is therefore not surprising

that architectures for building trust into distributed systems run by mutually distrusting or wary parties have to date only been undertaken primarily by banks, international financial institutions and other entities operating in the arena of marketing top-level trust assurance. More recently, international military coalitions [FRD 02] have also been shown to have the resources and mission to do so. This may be at least partly attributable to the potentially cumbersome nature of X.509-based hierarchical PKIs and their related technologies. Developments such as SPKI [IETF 01], authorization-based certificates and "federated" trust architectures such as the Internet2 Shibboleth project [I2 03] may succeed in helping to shape trust technology more closely to the realities of human use and interaction, particularly in more common, less well-endowed environments, but as yet it is too early to say so conclusively.

As a final note, the authors wish to state that the content of this paper represents the authors' own views. The authors do not represent or speak for or on behalf of the subject organization, nor should any statement in this paper be so construed.

References

[AJ 98]: P. J. Ambrose, G. J. Johnson. A Trust Based Model of Buying Behavior in Electronic Retailing. Association for Information Systems 1998 Americas Conference Proceedings, pp. 263-265. In http://www.isworld.org/ais.ac.98/proceedings/track06/ambrose.pdf.

[Ankney 00]: R. C. Ankney. Certificate management standards. CertCo, Inc., 2000, in http://www.certco.com/pdf/cms.pdf.

[Desmedt 92]: Y. Desmedt. Threshold cryptosystems. In J. Seberry, Y. Zheng, eds. AUSCRYPT '92. Lecture Notes in Computer Science 718. Springer-Verlag, Berlin/Heidelberg/New York, 1993, pp. 3-14.

[DH 76]: W. Diffie, M. E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, IT-22:644–654, 1976.

[FIPS 180-1]: National Institute of Standards and Technology, US Department of Commerce. Secure Hash Standard. 17 April 1995, in http://csrc.nist.gov/publications/fips/fips180-1/fips180-1.pdf.

[FIPS 186-2]: National Institute of Standards and Technology, US Department of Commerce. Digital Signature Standard. 27 January 2000, in http://csrc.nist.gov/publications/fips/fips186-2/fips186-2.pdf.

[FRD 02]: G. Fink, S. Raiszadeh, T. Dean. Experiences establishing an international coalition public key infrastructure. 1st International PKI Research Workshop – Proceedings. April 2002, pp. 193-206, in http://www.cs.dartmouth.edu/~pki02/Fink/paper.pdf.

[I2 03]: Internet2 Consortium. Shibboleth project. July 2003, in http://shibboleth.internet2.edu.

[Identrus 98]: Identrus LLC press release. Major financial institutions announce new company to provide businesses globally with a single electronic identity. 21 October 1998, in http://204.141.53.14/knowledge/releases/us/release_102198.xml.

[Identrus 02a]: Identrus LLC. About Identrus. 2002, in http://www.identrus.com/community/index.xml.

[IETF 01]: Internet Engineering Task Force. Simple Public Key Infrastructure (spki). IETF Charter, 16 January 2001, in http://www.ietf.org/html.charters/spki-charter.html.

[Kramer 99]: R. M. Kramer. Trust and distrust in organizations: Emerging perspectives, enduring questions. Annual Review of Psychology, vol. 50, pp. 569-598. Annual Reviews, Palo Alto, CA, 1999.

[Langford 96]: S. K. Langford. Weaknesses in some threshold cryptosystems. In N. Koblitz, ed. CRYPTO '96. Lecture Notes in Computer Science 1109. Springer-Verlag, Berlin/Heidelberg/New York, 1996, pp. 74-82.

[Mayer et al 95]: R. C. Mayer, J. H. Davis, F. D. Schoorman. An integrative model of organizational trust. Academy of Management Review. Vol. 20 no. 3, 1995, pp. 709-734.

[PKCS 1]: RSA Laboratories, Inc. PKCS #1 v2.1: RSA cryptography standard. 14 June 2002, in ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.doc.

[PKCS 7]: B. Kaliski. PKCS #7: Cryptographic message syntax version 1.5. Request for Comments 2315. IETF Network Working Group, March 1998, in http://www.ietf.org/rfc/rfc2315.txt.

[PKCS 10]: M. Nystrom, B. Kaliski. PKCS #10: Certification request syntax specification version 1.7. Request for Comments 2986. IETF Network Working Group, November 2000, in http://www.ietf.org/rfc/rfc2986.txt.
[RFC 2311]: S. Dusse et al. S/MIME Version 2 Message Specification. Request for Comments 2311. IETF Network Working Group, March 1998, in http://www.ietf.org/rfc/rfc2311.txt.
[RFC 2527]: S. Chokhani, W. Ford. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. Request for Comments 2527. IETF Network Working Group, March 1999, in http://www.ietf.org/rfc/rfc2527.txt.
[RFC 2560] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams. X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP. Request for Comments 2560. IETF Network Working Group, June 1999, in http://www.ietf.org/rfc/rfc2527.txt.
[RSA 78]: R. Rivest, A. Shamir, L. Adelman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21 (2), pp. 120-126, February 1978.
[WT 98]: A. Whitten, J. D. Tygar. Usability of Security: A Case Study. Carnegie Mellon University School of Computer Science Technical Report CMU-CS-98-155, December 1998, in http://reports-archive.adm.cs.cmu.edu/anon/1998/CMU-CS-98-155.pdf.
[WT 99]: A. Whitten, J. D. Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. Proceedings of the 8th USENIX Security Symposium, August 1999, in http://www.usenix.org/publications/library/proceedings/sec99/whitten.html.
[X.500]: ITU-T (formerly CCITT) Recommendation X.500 / ISO/IEC/ITU Standard 9594 (series). Information Technology – Open Systems Interconnection – The Directory. 1988.
[X.509]: ITU-T (formerly CCITT) Recommendation X.509 (1997 E) / ISO/IEC/ITU Standard 9594-8. Information Technology – Open Systems Interconnection – The Directory, Part 8: Authentication Framework. June 1997.