Global Information Assurance Certification Paper

Survey of the Status of Security and Emerging Security Innovations for Key Technological Protocols, Recommendations, Specifications and Standards Used in E-commerce

Angela Mozart
GSEC: Assignment Version 1.4b (August 2002), Option 1
November 22, 2003

Abstract

This whitepaper examines the current status of security and emerging security innovations for key technological protocols, recommendations, specifications and standards used in e-commerce. Since the Dot Com crash, it might seem that money and incentive for innovation would dry up. The issue arises as to whether anything substantial technologically speaking is being done to improve or change security in the area of e-commerce. Frankly, I was a little worried. As a regular online customer, I did not see any important noticeable changes. True, I saw Trust-E certification seals and new privacy statements everywhere. However, I did not see any new technological security options being offered to consumers. The most noticeable, prevalent technological security technique remains SSL/TLS. But visibly there was nothing new; technological security innovation seemed stagnant. To satisfy my curiosity and concern, I had to look a lot deeper than the surface of the consumer e-commerce sites that I typically visit. To discover the current status of security and security innovation for e-commerce, one must look behind the scenes as this is where the action is taking place. The first phase of e-commerce which involved bringing e-commerce to the non-mobile Business to Consumer (B2C) arena has already occurred; this was very noticeable and exciting, but security was an afterthought. To see what is really going on in the technological arena for e-commerce security, one must examine the protocols, recommendations, specifications and standards of the various standard setting and recommending bodies which are working to improve Internet security and the Internet in general. Organizations such as the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), the Organization for the Advancement of Structured Information Standards (OASIS), and the Open Mobile Alliance (OMA) in conjunction with the computer industry are all busy formulating the security standards and specifications that will define future e-commerce. This whitepaper examines the work that they have done and are doing for the following: Secure Sockets Layer/Transport Layer Security (SSL/TLS), Electronic Commerce Markup Language (ECML), Platform for Privacy Preferences (P3P), Secure Electronic Transaction (SET), Internet Open Trading Protocol (IOTP), Electronic Data Interchange (EDI)/American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X12, Extensible Markup Language (XML), Simple Object Access Protocol (SOAP)/XML Protocol (XMLP), Web Services Security (WS-Security), Electronic Business Extensible Markup Language (ebXML), and Wireless Access Protocol (WAP): Wireless Transport Layer Security (WTLS)/Wireless Identity Module (WIM). Once the above are examined, one sees global commerce infrastructure building, major work in the B2B arena and a major effort to incorporate transparent security in the m-commerce arena. It also becomes apparent that security is being built in from the ground up as opposed to the original Wild-Wild-West approach in the B2C arena of opening a new frontier and installing law and order afterwards. Naturally the current approach will require more time and effort before dramatic results are seen.

Secure Sockets Layer/Transport Layer Security (SSL/TLS) SSL/TLS are the cornerstone security protocols in the area of protecting online transactions. They are the key means used for encrypting information sent over the Internet, in particular confidential client online transaction information. Essentially all e-commerce requires the end to end encryption afforded by SSL/TLS. It encrypts all user information sent back and forth by the transacting parties. Without it confidential consumer information and other details would be sent in clear text across the Internet and would be visible and accessible to hackers. Historically SSL was developed by Netscape Communications Corporation. It turned the standard over to the Internet Engineering Task Force (IETF) in 1999. The IETF developed TLS Version 1.0 from SSL Version 3.0; see RFC 2246.[1] TLS Version 1.0 is an extremely stable standard, but some improvements have been made to it to incorporate security technological advances since then and to make provision for technological advances in the area of wireless communication. The most important proposed changes and actual changes made in terms of an impact on e-commerce follow. The IETF TLS Working Group has initiated the Internet-Draft "Use of Shared Keys in the TLS Protocol."[2] The reason that this is so important is that is intended to address the issue of low powered mobile handheld devices which much deal with expensive public-key encryption. This Internet-Draft states, "In order to solve these problems, we require a means of eliminating the expensive public-key operations in the TLS handshake, while providing an equivalent level of security using shared symmetric keys." [3] Another Internet-Draft in progress with importance in the area of e-commerce is titled "Transport Layer Security Protocol Compression Methods."[4] The reason that this is so important is that the future of e-commerce innovation is tied to the Extensible Markup Language (XML) which is a technology that requires more information than ever before to be transmitted over the wire. (The future of e-commerce being tied to XML will be discussed further in this paper.) This Internet-Draft states:

> TLS is used extensively to secure client-server connections on the World Wide Web. While these connections can often be characterized as short-lived and exchanging relatively small amounts of data, TLS is also being used in environments where connections can be long-lived and the amount of data exchanged can extend into thousands or millions of octets. XML [4], for example, is increasingly being used as a data representation method on the Internet, and XML tends to be verbose. Compression within TLS is one way to help reduce the bandwidth and latency requirements associated with exchanging large amounts of data while preserving the security services provided by TLS.[5]

TLS Version 1.0 has also been now improved by extensions added by RFC 3546[6] which supercedes "The TLS Protocol Version 1.0", RFC 2246. RFC 3546

deals with constraints imposed by wireless TLS clients in the form of memory, bandwidth, power, and battery life limitations.[7] Simultaneously maintenance work is being done on TLS Version 1.1. See Internet-Draft, "The TLS Protocol Version 1.1."[8] Thus it appears that continuous work is being done to keep the most critical protocol used in e-commerce up-to-date and capable of handling future innovations in technology and business.

Electronic Commerce Markup Language (ECML) The purpose of ECML is to overcome the obstacle consumers face when shopping online because they must re-enter payment information for every site they visit. ECML is supposed to standardize digital wallet information, so that information can be passed in a seamless fashion. The IETF in RFC 3106 specifies ECML version 1.1 and obsoletes ECML version 1.0.[9] The draft explicitly states that it did not provide or replace other security standards and that it was leaving open for the next version the possibility of adding fields for privacy.[10] In and of itself ECML is not a security standard for e-commerce. However, it has been coupled with the Platform for Privacy Preferences (P3P) 1.0 Specification.[11], and this is important because of the frequency of the need to transmit consumer transaction information back and forth between and among multiple transacting parties. The objective is to build a P3P compliant wallet, but P3P lacked a standard schema for the wallet contents and ECML 2.0 fills that void. RFC 3505, "Electronic Commerce Modeling Language (ECML): Version 2 Requirements"[12] provides the extension for the P3P fields.

Platform for Privacy Preferences (P3P) The P3P standard creates a standardized machine-readable format for websites to "display" their privacy policies. The World Wide Web Consortium issued P3P 1.0 as a W3C Recommendation on April 16, 2002.[13] While there has been criticism of it, it is definitely a step in the right direction as consumers need to be protected against the enormous potential for various websites to collect a tremendous amount of personal information about them. Without assurances like those provided by the P3P standard, online commerce, particularly in the Business to Consumer (B2C) arena, will be strictly hindered as the politics grow more vocal about the collection of such information. The P3P 1.1 Working Group drafts work on addressing the criticisms and issues that have arisen such as some of the user compatibility issues and providing for environments other than HTTP such as XML.[14] Thus, it looks like P3P is in its infancy but poised for growth.

Secure Electronic Transaction (SET) SET was a security standard which held great promise, but which seems to have fizzled. Its great promise was that it would keep consumer bank information encrypted and inaccessible to the merchant while forwarding it to the customer's bank or credit card company for payment processing. SET was originally created primarily by MasterCard and VISA. The SET website, http://www.setco.org is currently very outdated. Simson Garfinkel in Web Security, Privacy & Commerce[15] succinctly describes SET: "There are three parts to the SET system: an "electronic wallet" that resides on

the user's computer; a server that runs at the merchant's web site; and the SET Payment Server that runs at the merchant's bank." He further goes on to state that it is because of all of this complexity for the consumer and also because of the problem of finding SET enabled websites that it has currently died, but he later states that it might be revived when smartcards become more prevalent. Personally I was very disappointed to see this fail to materialize. I would have loved to have had the opportunity to be able to authenticate myself with a certificate before allowing my credit card to be used and have technological assurance that the merchant's access to my credit card information would be limited. Interestingly, the IETF is still doing some work involving SET. See RFC 3538, "Secure Electronic Transaction (SET) Supplement for the v1.0 Internet Open Trading Protocol (IOTP).[16] The fact that this work is occurring is consistent with the possibility of SET reappearing some day in the future.

Internet Open Trading Protocol (IOTP) The IOTP is described on the IETF Internet Open Trading Protocol (trade) Working Group site as "an interoperable framework for Internet commerce. It is optimized for the case where the buyer and the merchant do not have a prior acquaintance and is payment system independent."[17] It goes on further to describe the anticipated work of the working group which is to create IOTP version 2.0 which will incorporate XML Digital signatures and be compatible with ECML 2.0 as well. It mentions, however, that the mission of IOTP version 2.0 will not be to create an XML messaging layer. The work of the IOTP (trade) Working Group sounds awfully similar to that of E-commerce Business XML (ebXML) since it also involves the creation of a framework for Internet commerce. It is interesting to see that the deadline for the version 2.0 specification has not been met even though some work was done to enable IOTP to use SET, RFC 3538. Thus it appears that ebXML is going to soon supercede this effort. There is also no need to create a messaging layer because Secure Object Access Protocol (SOAP) which will be discussed later covers that as well.

Electronic Data Interchange (EDI)/American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X12 The Accredited Standards Committee (ASC) X12 is the approved subcommittee of the American National Standards Institute and approved standards setting body for Electronic Data Interchange (EDI), the current workhorse for B2B commerce.[18] Although EDI may have a stodgy reputation in the face of the Internet business revolution, it is in no way going away.[19] When one examines the agenda for the ASC X12 committee trimester meetings for 2004,[20] one can see that they are very actively doing continuing work. Most of this work involves enabling EDI for XML and ebXML. In addition to this, earlier this year ASC X12 created a draft proposal to update the already approved ANSI X12.58-1997 security standard. The dpANS X12.58-February 6, 2003 is the draft proposed American National Standards for Electronic Data Interchange on Security Structures.[21] The stated purpose and scope of the draft are "to define the data formats for authentication, encryption, and assurances in order to provide integrity, confidentiality, and verification and non-repudiation of origin for two levels of exchange of Electronic Data

Interchange (EDI) formatted data defined by Accredited Standards Committee (ASC) X12. These security services can be applied at either the functional group level or the transaction set level or both."[22] Thus, it is clear that ASC X12 and EDI are not unaware of the current environment which demands a much stronger security awareness than when EDI was originally developed and designed to be transported across private lines and networks alone. Additionally the Value Added Networks (VAN)s who have been using the Internet to handle EDI communications for their customers have definitely had to consider security implications of using a public network. The future for EDI definitely appears to be a blend of old-style EDI, new-style XML/ebXML and a mixture of private and public networks to transport the data and communications. However, this seemingly stodgy arena of B2B commerce is going to be the next big thing in terms of innovation because of XML and its potential to make a major revolutionary improvement in the way business is done. B2C already has had its major revolution; it is now time for B2B.

Extensible Markup Language (XML) XML is the technology that is providing the next revolutionary usage of the Internet. It is truly classified as a disruptive technology.[23] The first Working Draft for XML was created by the World Wide Web Consortium (W3C) SGML Working Group on November 14, 1996.[24] Since this original draft, work has steadily proceeded by the W3C committees and by business, government and every conceivable industry in the world. The latest invocation of the original XML standard is the "Extensible Markup Language (XML) 1.1 W3C Proposed Recommendation 05 November 2003".[25] Its abstract states, "The Extensible Markup Language (XML) is a subset of SGML that is completely described in this document. Its goal is to enable generic SGML to be served, received, and processed on the Web in the way that is now possible with HTML."[26] XML itself is not a markup language but rather a meta-language for describing in a standardized fashion business documents at a minimum and more opportunistically queries, processes, protocols, links and security measures like encryption, digital signatures, and authenticated access. XML's primary security specifications are XML Encryption, XML Key Management, XML Signature and Security Assertion Markup Language (SAML). One of the best things about these security specifications is the fact that they are being built from the start rather than as an afterthought. They will give the XML technology all it needs to deliver heavy-duty security to the B2B world. Right now the B2C world has SSL/TLS which is fantastic, but because of the complexity of more stringent solutions such as client authentication by way of client certificates as one example, online sites and credit card vendors are forced to offer limited liability guarantees instead utilizing all the hard-core security technology possible. This may be fine at a certain transactional level, but it is very limiting in the B2B context where thousands and millions of dollars worth of transactions need to be conducted. Thus, the forward-looking XML security specifications are more important than ever.

The XML Encryption (XML-ENC) Recommendation of the W3C was made on December 10, 2002.[27] It was created by the XML Encryption Working Group. It provides for confidentiality when using XML. The most important thing it does is to allow for granularity of encryption as opposed to the all or nothing approach of SSL/TLS. This in turn allows for one party to see one piece and not another and vice versa. The other important point about XML Encryption is that it does not create any new encryption techniques or features but rather it allows existing encryption techniques and standards to be modeled in XML.

The XML Key Management Specification (XKMS), Version 2.0, 18 April 2003, is a W3C Working Draft produced by the XKMS Working Group.[28] It facilitates key exchange for web services which will allow for authentication of parties and integrity, confidentiality and non-repudiation of messages. XKMS is an extremely important innovation for commerce because it allows web services to handle complex PKI infrastructure rather than requiring each system to deploy its own.[29] In particular it also facilitates m-commerce. Ramesh Nagappan, Robert Skoczylas and Rima Patel Sriganesh in Developing Java Web Services write, "XKMS presents a possibility for a thin device, such as a PDA, to register its certificate by consuming the Web services of a trust services provider, with nothing more than support for a plain XML parser and minimal footprint for XML Encryption and XML Signature implementations present on the device."[30]

The XML Signature (XML-SIG) Specification is a product of the joint effort of the IETF and the W3C XML Signature Working Group. The W3C calls it the "XML-Signature Syntax and Processing W3C Recommendation 12 February 2002."[31] At the IETF it is known as RFC 3275, "(Extensible Markup Language) XML-Signature Syntax and Processing."[32] This specification has achieved the highest levels possible within both organizations which are not per se standards settings bodies themselves but recommending bodies. While that may be true in a *de jure* sense, both bodies are quite powerful in a *de facto* sense. The RFC 3275 Abstract states, "XML Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere."[33] Thus it affords great flexibility and more importantly opens an enormous cost savings opportunity. Encryption is expensive in terms of processing power; SSL accelerators are not installed without good reason. Since XML-SIG allows selective encryption, businesses will be able to choose what to encrypt and what not to encrypt depending upon security needs. This will reduce costs since not everything will need to be encrypted. Like XML-ENC it does not create any new digital signature technology but rather enables the existing signature technology through XML.

Security Assertion Markup Language (SAML) provides Single Sign On in the XML framework. The SAML V1.1 Organization for the Advancement of Structured Information Standards (OASIS) standard is an open e-business standard that was approved on September 22, 2003.[34] Webopedia defines

SAML as “an XML-based framework for ensuring that transmitted communications are secure. SAML defines mechanisms to exchange authentication, authorization and non-repudiation information, allowing single sign on capabilities for web services.”[35] This allows companies and organizations to create contractual federations and for browsing end-users or other web services to reach those entities’ services using a SSO with appropriate authentication and authorization information. Again the SAML technology does not define any new authentication techniques itself but rather enables the existing technology for the same in XML. Thus, another critical piece is in place to deliver the technology needed for online B2B commerce.

Simple Object Access Protocol (SOAP)/ XML Protocol (XMLP) Webopedia defines SOAP as “a lightweight XML-based messaging protocol used to encode the information in Web service request and response messages before sending them over a network. SOAP messages are independent of any operating system or protocol and may be transported using a variety of Internet protocols, including SMTP, MIME, and HTTP.”[36] The latest standard for SOAP is the W3C XML Protocol (XMLP) Working Group’s SOAP Version 1.2 Recommendation which was made on June 24, 2003.[37] SOAP is the communications protocol of choice for distributed computing. It is SOAP which allows application calls in the heterogeneous, revolutionary world of web services. SOAP over HTTP allows all of this application communication for e-commerce to flow through everyone’s firewall port 80 unhindered. This, of course, has the potential for good and bad. It is a great enabler for e-commerce and web services in general. It is a bad thing when one thinks of the potential security problems. In and of itself, SOAP is not secure, but it is extensible. The SOAP Version 1.2 Recommendation explicitly states “The SOAP Messaging Framework does not directly provide any mechanisms for dealing with access control, confidentiality, integrity and non-repudiation. Such mechanisms can be provided as SOAP extensions using the SOAP extensibility model...”[38] Then the Recommendation further directs developers how to check for the security of SOAP nodes, SOAP intermediaries and the underlying protocol bindings. Thus, given the extensibility of SOAP, there is a way to secure e-commerce communications made using web services.

Web Services Security Specification (WS-Security) Microsoft and IBM created a roadmap for WS-Security entitled “Security in a Web Services World: A Proposed Architecture and Roadmap” on April 7, 2002.[39] The whole purpose of this roadmap is to deal with the above issue of extending SOAP in order to secure web services. The base layer of the roadmap is WS-Security, and it sits on top of a SOAP foundation. Above this layer are WS-Policy, WS-Trust, WS-Privacy, WS-SecureConversation, WS-Federation and WS-Authorization. On June 27, 2002, Microsoft, IBM and Verisign handed over the WS-Security piece of the roadmap to OASIS.[40] The pieces of the roadmap are described as follows on Cover Pages which is hosted by OASIS:

WS Specifications:

Initial Specifications

- **WS-Security**: describes how to attach signature and encryption headers to SOAP messages. In addition, it describes how to attach security tokens, including binary security tokens such as X.509 certificates and Kerberos tickets, to messages.

- **WS-Policy**: will describe the capabilities and constraints of the security (and other business) policies on intermediaries and endpoints (*e.g.*, required security tokens, supported encryption algorithms, privacy rules).

- **WS-Trust**: will describe a framework for trust models that enables Web services to securely interoperate.

- **WS-Privacy**: will describe a model for how Web services and requesters state privacy preferences and organizational privacy practice statements.

Follow-On Specifications

- **WS-SecureConversation**: will describe how to manage and authenticate message exchanges between parties including security context exchange and establishing and deriving session keys.

- **WS-Federation**: will describe how to manage and broker the trust relationships in a heterogeneous federated environment including support for federated identities.

- **WS-Authorization**: will describe how to manage authorization data and authorization policies.[41]

The OASIS Web Services Security (WSS) Technical Committee has created the "Web Services Security: SOAP Message Security Working Draft 17," dated Wednesday, August 27, 2003.[42] As of October 19, 2003 the review phase for this draft ended, and the draft is currently back in the hands of the WSS Technical Committee. Allen Bernard has written a very interesting article entitled "WS Security and Adoption."[43] The article points out that on the one hand some software companies have already started implementing WS-Security assuming that the draft will be passed as currently written. However, on the other hand, it points out that it is going to be a long time for web services to actually be accepted by customers because of the fact that the security standards for it have not in fact been worked out. The fact that work is now only being done on the WS-Security foundational layer but that nothing has been done yet from a standards perspective for the other upper layers mentioned in the roadmap has been called instead a roadblock. In fact, the security problem is so severe that customers are not implementing web services outside of the firewall, but are merely using them for integration purposes instead. Thus, it appears that web

services security is still very much a work in progress and that it must first be ironed out before widespread implementation will occur.

Electronic Business Extensible Markup Language (ebXML) ebXML is a standard that was introduced in 1999 and designed to provide a framework for global e-commerce for enterprises ranging in all sizes. It is specifically designed to overcome the barriers of EDI, so that Small-to-Medium Enterprises (SME) can participate as well. The ebXML specifications are a joint effort of United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) and OASIS.[44] OASIS handles the Messaging Services, Registries and Repositories, Collaborative Protocol File, and Implementation, Interoperability and Conformance pieces. UN/CEFACT handles the Core Components and Business Process Models pieces. The OASIS ebXML Message Service Specification v. 2.0 (ebMS) was approved in August 2002.[45] This is the piece of the specification where security issues are predominant. It is interesting because both ebMS and WS-Security both provide extensibility of SOAP. In an IEEE article entitled "ebXML and Web Services," Sanjay Patil and Eric Newcomer compare the two concepts.[46] They say that ebXML is a top-down overall design framework approach while the web services including WS-Security approach is a bottom up approach, and that these two meet in the middle at SOAP. Perhaps the key difference between ebMS and WS-Security is that ebMS is a comparatively mature standard whereas WS-Security is just now going through the final approval process. A Sun Open Net Environment (Sun ONE) technical sales article on the Sun website notes that the ebXML messaging solution is ready today.[47]

Wireless Access Protocol (WAP): Wireless Transport Layer Security (WTLS)/Wireless Identity Module (WIM) The WAP 2.0 specification, which is what is currently being used, was approved by the WAP Forum on January 18, 2001.[48] Two of the numerous security specifications that WAP 2.0 includes are WTLS and WIM. In June 2002, the WAP Forum was merged into the newly formed global organization called Open Mobile Alliance (OMA).[49] OMA has taken over WAP 2.0 and the specifications which comprise it. OMA has several working groups; the ones that are in closest contact with security issues are the Security Working Group and the M-Commerce Working Group. Generally, WAP 2.0 is rather stable and very few changes have been made to it.

The WTLS specification which was created by the WAP Forum is dated April 6, 2001.[50] It exists largely as it was originally created. It sits between the Transaction Layer (WTP) and the Transport Layer (WDP/UDP/IP) in the WAP protocol stack. WTLS is very similar to SSL/TLS, but it had to be designed differently in some respects for wireless constraints such as low-bandwidth, less computing power, and limited memory. Another key difference is the fact of the "WAP gap." With the legacy WAP stack there must be a protocol conversion that takes place between the WAP client and the web server; this necessitates a WAP gateway which makes end-to-end security impossible.[51] However, with

WAP 2.0 and the newer, faster 2.5G and 3G bearer services, it is now possible to bypass the gateway requirement.[52] It is the WAP 2.0 Wireless Profiled TCP (WP-TCP), Wireless Profiled TLS and Wireless Profiled HTTP standards that make this possible.[53]

The WIM specification was originally created by the WAP form on July 12, 2001.[54] It has since been revised by OMA to WIM version 1.1 on October 24, 2002, and is listed on their website under Specifications for Public Comment.[55] This standard furthers the usage of a tamper-resistant storage area for private keys. The whole idea is to make security transparent to the user. The user will be able to either insert an external smart card or have the same information stored in the Subscriber Identity Module (SIM) card.

There are other security specifications in WAP 2.0 which the Security Group Charter lists, but there have been no specifications changes made to them yet. The scope of the Security Group charter, dated December 6, 2002, lists the following other specifications for which they are responsible: Wireless Profile of Transport Layer Security ("TLS Prof"), WMLScript Crypto Library ("Crypto API", and extensions), ECMAScript Crypto object (ECMACR), Wireless Public Key Infrastructure (WPKI), Wireless Certificate Profile ("CertProf"), Signed Content (SCONT), and Online Certificate Status Protocol ("OCSP").[56]

The M-Commerce Working Group which is concerned with web services has not yet released any deliverables. The fact that WAP 2.0 is XHTML Mobile Profile (XHTML MP) compatible[57] starts to open wireless devices to the world of XML, web services and all of its accompanying work in progress as stated earlier in this whitepaper. This combination of work being done in the presentation area by way of XHTML MP and the ability to access web services providing what would otherwise be processor intensive security services is what will truly assist in opening the m-commerce door.

Note: There is, however, one other great obstacle to m-commerce which does not involve security and that is bandwidth. The transition from Second Generation (2G) to (2.5G) networks and eventually from (2.5G) to Third Generation (3G) networks must be made. Progress is being made; for example, AT&T Wireless just made the announcement of their upgrade to Enhanced Data GSM Environment (EDGE).[58] This takes the subscriber's bandwidth to the 100 to 130 kbps range. Full 3G capability promises about 2000 kbps.[59]

Conclusion

Technological security innovation for e-commerce is not dead; it is just less visible to the casual observer. It is less visible for three main reasons. Firstly, it is because the innovation is in the area of infrastructure building such as ebXML framework creation and the securing of web services. (Visibility would not be desirable here anyway.) Secondly, with the exception of m-commerce, it is because the next major wave of e-commerce will take place in the B2B arena as opposed to the B2C arena once the more heavy-duty security technology is in

place to allow larger and more varied B2B transactions to take place. Thirdly, for security in the area of m-commerce, transparency is the whole idea, so that the user will not have to keep re-entering cumbersome security information to complete his or her transactions. Given enough time, the security protocols, recommendations, specifications and standards that everyone is working on will help usher in the next phase of e-commerce growth.

Endnotes

[1] Dierks, T., et al. "The TLS Protocol Version 1.0." Internet Engineering Task Force Request for Comments: 2246. January 1999. URL: http://www.ietf.org/rfc/rfc2246.txt (14 November 2003).
[2] Gutmann, P. "Use of Shared Keys in the TLS Protocol." Internet Engineering Task Force Internet-Draft: draft-ietf-tls-sharedkeys-02. October 2003. URL: http://www.ietf.org/internet-drafts/draft-ietf-tls-sharedkeys-02.txt (14 November 2003).
[3] Gutmann, P.
[4] Hollenbeck, S. "Transport Layer Security Protocol Compression Methods." Internet Engineering Task Force Internet-Draft: draft-ietf-tls-compression-06. November 20, 2003. URL: http://www.ietf.org/internet-drafts/draft-ietf-tls-compression-06.txt (21 November 2003).
[5] Hollenbeck, S.
[6] Blake-Wilson, S., et al. "Transport Layer Security (TLS) Extensions" Internet Engineering Task Force Request for Comments: 3546. June 2003. URL: http://www.ietf.org/rfc/rfc3546.txt (14 November 2003).
[7] Blake-Wilson, S., et al.
[8] Dierks, T. et al. "The TLS Protocol Version 1.1" . Internet Engineering Task Force Internet-Draft: draft-ietf-tls-rfc2246-bis-05.txt. June 2003. URL: http://www.ietf.org/internet-drafts/draft-ietf-tls-rfc2246-bis-05.txt (14 November 2003).
[9] Eastlake, D., et al. "ECML v1.1: Field Specifications for E-Commerce." Internet Engineering Task Force Request for Comments: 3106. April 2001. URL: ftp://ftp.isi.edu/in-notes/rfc3106.txt (14 November 2003).
[10] Eastlake, D. et al.
[11] Cranor, Elaine, et al. "The Platform for Privacy Preferences 1.0 (P3P1.0) Specification." World Wide Web Consortium. 16 April 2002. URL: http://www.w3.org/TR/P3P/ (21 November 2003).
[12] Eastlake, D. and Motorola. "Electronic Commerce Modeling Language (ECML): Version 2 Requirements." Internet Engineering Task Force Request for Comments: 3505. March 2003. URL: ftp://ftp.rfc-editor.org/in-notes/rfc3505.txt (14 November 2003).
[13] World Wide Web Consortium. "World Wide Web Consortium Issues P3P 1.0 as a W3C Recommendation." 16 April 2002. URL: http://www.w3.org/2002/04/p3p-pressrelease (14 November 2003).
[14] World Wide Web Consortium. "P3P Specification Working Group List of Documents." 6 November 2003. URL: http://www.w3.org/P3P/1.1/documents.html (14 November 2003).
[15] Garfinkel, Simson. Web Security, Privacy & Commerce. Sebastopol: O'Reilly & Associates, Inc. 2002: p. 86.
[16] Kawatsura, K. and Hitachi. "Secure Electronic Transaction (SET) Supplement for the v.1.0 Internet Open Trading Protocol (IOTP)." Internet Engineering Task Force Request for Comment: 3538. June 2003. URL: http://www.ietf.org/rfc/rfc3538.txt?number=3538 (14 November 2003).

[17] Internet Engineering Task Force. "Internet Open Trading Protocol (trade): Description of Working Group." 1 October 2003. URL: http://www.ietf.org/html.charters/trade-charter.html (14 November 2003).
[18] Accredited Standards Committee (ASC) X12. "Frequently Asked Questions." 31 October 2003. URL: http://www.x12.org/x12org/about/faqs.cfm#b1 (15 November 2003).
[19] Gibb, Brian, and Suresh Damodaran. ebXMConcepts and Application . Indianapolis: Wiley Publishing, Inc., 2003: p. 25.
[20] Accredited Standards Committee (ASC) X12. "Meeting Agenda." URL: http://www.x12.org/x12org/meetings/meeting_agenda.cfm?sortby=date (15 November 2003).
[21] Accredited Standards Committee (ASC) X12. "dpANS X12.58-Feburary 6, 2003: Draft Proposed American National Standards for Electronic Data Interchange on Security Structures." 6 February 2003. URL: http://www.w12.org/x12org/subcommittees/dev/pdf/V5_x1258.pdf (15 November 2003).
[22] Accredited Standards Committee (ASC) X12, at p. 2.
[23] Gibb, Brian, and Suresh Damodaran, at p. 62.
[24] World Wide Web Consortium. "Extensible Markup Language (XML) WC3 Working Draft 14-Nov-96." 14 November 1996. URL: http://www.w3.org/TR/WD-xml-961114.html#dt-xml-doc (15 November 2003).
[25] Bray, Tim, et al. "Extensible Markup Language (XML) 1.1 W3C Proposed Recommendation 05 November 2003." World Wide Web Consortium. 5 November 2003. URL: http://www.w3.org/TR/2003/PR-xml11-20031105/ (15 November 2003).
[26] Bray, Tim, et al, at heading.
[27] Imamura, Takeshi, et al. "XML Encryption Syntax and Processing W3C Recommendation 10 December 2002." World Wide Web Consortium. 10 December 2002. URL: http://www.w3.org/TR/xmlenc-core/ (15 November 2003).
[28] Hallam-Baker, Phillip. "XML Key Management Specification (XKMS) Version 2.0 W3C Working Draft 18 April 2003." World Wide Web Consortium. 18 April 2003. URL: http://www.w3.org/TR/xkms2/ (15 November 2003).
[29] Nagappan, Ramesh, Robert Skoczylas and Rima Patel Sriganesh. Developing Java Web Services. Indianapolis: Wiley Publishing, Inc. 2003: p. 668.
[30] Nagappan, Ramesh, Robert Skoczylas and Rima Patel Sriganesh, at p. 669.
[31] Bartel, Mark, et al. "XML-Signature Syntax and Processing W3C Recommendation 12 February 2002." World Wide Web Consortium. 12 February 2002. URL: http://www.w3.org/TR/xmldsig-core/ (16 November 2003).
[32] Eastlake, D. et al. "(Extensible Markup Language) XML-Signature Syntax and Processing." Internet Engineering Task Force. March 2002. URL: http://www.ietf.org/rfc/rfc3275.txt?number=3275 (16 November 2003).
[33] Eastlake, D. et al.
[34] Organization for the Advancement of Structured Information Standards. "Security Assertion Markup Language (SAML) Version 1.1 Ratified as OASIS

Standard." 22 September 2003. URL: http://www.oasis-open.org/news/oasis_news_09_22_03.php (17 November 2003).
[35] Webopedia. "SAML." 25 June 2002. URL: http://www.webopedia.com/TERM/S/SAML.html (17 November 2003).
[36] Webopedia. "SOAP." 12 March 2003. URL: http://www.webopedia.com/TERM/S/SOAP.html (17 November 2003).
[37] World Wide Web Consortium. "XML Protocol Working Group." 21 November 2003. URL: http://www.w3.org//2000/xp/Group/ (22 November 2003).
[38] Gudgin, Martin, et al. "SOAP Version 1.2 Part 1: Messaging Framework." World Wide Web Consortium. 24 June 2003. URL: http://www.w3.org/TR/2003/REC-soap12-part1-20030624/#secconsiderations (17 November 2003).
[39] International Business Machines Corporation and Microsoft Corporation. "Security in a Web Services World: A Proposed Architecture and Roadmap." 7 April 2002. URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnwssecur/html/securitywhitepaper.asp (17 November 2003).
[40] Organization for the Advancement of Structured Information Standards. "Technology News." Cover Pages 9 September 2003. URL: http://xml.coverpages.org/ws-security.html#articles (17 November 2003).
[41] Organization for the Advancement of Structured Information Standards."Technology News." Cover Pages 9 September 2003. URL: http://xml.coverpages.org/ws-security.html (17 November 2003).
[42] Nadalin, Anthony, et al. "Web Services Security : SOAP Message Security Working Draft 17, Wednesday, August 27, 2003." Organization for the Advancement of Structured Information Standards. 27 August 2003. URL: http://www.oasis-open.org/committees/download.php/3281/WSS-SOAPMessageSecurity-17-082703-merged.pdf (17 November 2003).
[43] Bernard, Allen. "WS Security and Adoption." EarthWeb. 15 August 2003. URL: http://itmanagement.earthweb.com/secu/article.php/3064501 (17 November 2003).
[44] Organization for the Advancement of Structured Information Standards. "ebXML Technical Work." URL: http://www.ebxml.org/technical_work.htm (17 November 2003).
[45] Organization for the Advancement of Structured Information Standards. "Message Service Specification Version 2.0 OASIS ebXML Messaging Services Technical Committee 1 April 2002." 1 April 2002. URL: http://www.ebxml.org/specs/ebMS2.pdf (18 November 2003).
[46] Patil, Sanjay and Eric Newcomer. "ebXML and Web Services." IEEE Distributed Systems Online. May 2003. URL: http://dsonline.computer.org/0305/f/wp3spot.htm (18 November 2003).
[47] Malks, Dan and Marina Sum. "Developing Web Services with ebXML and SOAP: An Overview." Sun Microsystems, Inc. March 3, 2003. URL: http://developers.sun.com/sw/building/tech_articles/collab.html (18 November 2003).

[48] WAP Forum. "The WAP 2.0 Conformance Release." 18 January 2001. URL: http://www.openmobilealliance.org/wapdownload.html (19 November 2003).
[49] Open Mobile Alliance. "New Global Organization, the Open Mobile Alliance, Formed to Foster Worldwide Growth in the Mobile Services Market." 12 June 2002. URL: http://www.wapforum.org/new/20020612433New.htm (19 November 2003).
[50] WAP Forum. "Wireless Transport Layer Security." 6 April 2001. URL: http://www.openmobilealliance.org/wapdocs/wap-261-wtls-20010406-a.pdf (19 November 2003).
[51] Sadeh, Norman. M-Commerce Technologies, Services, and Business Models. New York: Wiley Publishing, Inc. 2002: p. 115.
[52] Sadeh, Norman, at p. 113.
[53] Sadeh, Norman, at pp. 117-118., Open Mobile Alliance. "The WAP 2.0 Conformance Release." 18 January 2001. URL: http://www.openmobilealliance.org/wapdownload.html (19 November 2003).
[54] WAP Forum. "Wireless Identity Module Part: Security Version 12-July-2001." 12 July 2001. URL: http://www.openmobilealliance.org/wapdocs/wap-260-wim-20010712-a.pdf (19 November 2003).
[55] Open Mobile Alliance. "Technical Releases and Specifications of the Open Mobile Alliance." 24 October 2002. URL: http://www.openmobilealliance.org/documents.html (19 November 2003).
[56] Open Mobile Alliance. "Security Working Group Charter." 6 December 2002. URL: http://www.openmobilealliance.org/security.html##secCharter (19 November 2003).
[57] Openwave Systems, Inc. "History of XHTML Mobile Profile." URL: http://developer.openwave.com/omdt/xhtml-mp-styleguide/Chapter1.html#pgfId-998393 (21 November 2003).
[58] AT&T Wireless. November 2003. "URL: http://www.attwireless.com/speed/ (21 November 2003).
[59] Sadeh, Norman, at p.94.