TELEBIOMETRIC INFORMATION SECURITY AND SAFETY MANAGEMENT[1]

Phillip H. Griffin, CISM

Booz | Allen | Hamilton, Linthicum, Maryland USA

ABSTRACT

Organizations that rely on human-oriented technologies such as telebiometrics should protect and manage the safety and security of their physical and information assets. Data that documents the safe and secure operation of telebiometric system devices should be collected and captured in an information security and safety event journal. Event journal data provides an audit trail that should be protected using digital signatures, encryption and other safeguards. A system heartbeat record should document and monitor the safety, performance, and availability of telebiometric system devices and alert system administrators to security and safety events and changes. Heartbeat data should provide metrics that inform the continuous improvement of a telebiometric information security and safety management program. A signcryption cryptographic message wrapper should protect event journal, biometric reference template, and other telebiometric information to promote user security and respect for user privacy rights.

Keywords— ASN.1, signcryption, telebiometrics

1. INTRODUCTION

Organizations that rely on telebiometric technology should protect and manage the safety and security of their telebiometric assets [3]. Physical security and personnel security are important telebiometric considerations, and two of the pillars of information security management. The safe operation and performance of telebiometric systems are closely related to availability, a cornerstone of information security. Telebiometric systems safety management and performance monitoring should be integrated into the organization's overall information security management program.

This management program should be based on safety and security policies designed to achieve the objectives of the organization. A risk-based approach should be used to select and impose proper controls and to monitor their effectiveness. A periodic heartbeat message sent from each node of a telebiometric system to a central management collection point should document system compliance to safety and security policies in a secure journal, and help guide operations.

The international biometric information management and security standard, ISO 19092 recommends that compliance of a biometric system "should be periodically validated according to the organizations [*sic*] policy, practices and procedures" [4]. ISO 19092 defines a set of secure event journal records that "should be used in the capture of the validation material" [4]. However, the standard does not define a telebiometric system heartbeat record for monitoring and managing the safety, security and performance of biometric devices in a telebiometric system.

2. DATA SECURITY

Telebiometric information systems are vulnerable to loss of data integrity, origin authenticity, and confidentiality when their biometric data are transferred on "telecommunications network or via wireless communication devices", such as smartphone and tablet computers, using "wireless LAN or Bluetooth" [15]. The raw biometric data in a biometric sample is vulnerable to being "altered or intercepted by an attacker and used for illegal purposes" when being sent "to the signal processing component" [15]. Biometric data is also subject to attack when transmitted for "storage in registration or to the comparison component in authentication" [15].

When biometric devices are used for identification or verification, even when protected by liveness detection, "live-scanned data can be intercepted" during transmission and "replaced by forged biometric data" [15]. If biometric reference templates must be transferred, the confidentiality of their biometric data must be ensured. When templates are stored in a centralized template management system, their authenticity and integrity, as well as the confidentiality of their biometric data, must be protected from purposeful or accidental modification and from attack by trusted insiders.

ITU-T X.1086 proposes "countermeasures to ensure data integrity, mutual authentication, and confidentiality" to

[1] *Paper accepted for presentation at "Building Sustainable Communities" ITU Kaleidoscope Conference, Kyoto, Japan, 22-24 April 2013,* http://itu-kaleidoscope.org/2013

protect telebiometric information and users against threats, such as "hijacking, modification and illegal access" [15], and ITU-T X.1084 specifies a biometric authentication protocol and telebiometric system model profiles [14]. The X.1086 standard requires that personally identifiable biometric data, such as the "faces, fingerprints, irises, and voices" of users, be protected by a confidentiality safeguard and treated as the "providers' private information" [15]. ISO 19092 also requires confidentiality for biometric data and recommends that cryptographic safeguards ensure the integrity and authenticity of biometric objects [4].

Digital signatures based on the certificates in a Public Key Infrastructure (PKI) can be coupled with encryption techniques to protect the confidentiality, integrity, and authenticity of biometric data and associated information. The SignedData cryptographic message used to sign electronic mail can provide data integrity and origin authenticity for an entire biometric object. Once created, the SignedData message can be encapsulated in an EncryptedData message to provide confidentiality for the entire signed object [17].

However, the signature followed by encryption approach employed in electronic mail systems lacks the processing efficiency demanded by modern telebiometric applications. The electronic mail approach also provides insufficient granularity. The entire biometric object must be encrypted, while only a few selected elements in biometric objects might require confidentiality protection. A more efficient, granular alternative for encrypting selected fields in signed telebiometric data is described in this paper.

This granular approach uses a new cryptographic message type, SigncryptedData [3]. This secure message allows a sender to sign and encrypt selected fields in a biometric object, and then to sign the entire object. SigncryptedData can provide confidentiality only where it is needed, and data integrity and origin authenticity over the entire object in a single cryptographic message.

3. PUBLIC SAFETY

3.1 Telebiometrics

Biometric recognition is a key form of automated identification and authentication based on the ability to distinguish individuals by their physiological or behavioral traits. Networked biometric systems are "increasingly used in a wide range of applications" [1] that enhance the quality of human life, including healthcare, law enforcement, border control, and financial services. These applications are enabled by "advanced pattern recognition algorithms applied through powerful ICT" [1] that merge remote biometric sensors and telecommunications.

To interact with biometric recognition applications, a human being must come into physical contact with "telecommunication systems and biometric devices" [13]. During this contact, telebiometric data from one or more sensors is "recorded by a measurement instrument" to collect biometric samples [13]. When "the human body meets electronic or photonic or chemical or material devices capturing biometric" data, the safe operation of these devices must be assured [13].

ITU-T Recommendation X.1081 defines a "framework for identifying and specifying safety aspects of telebiometrics" [13]. This international standard "provides a structure for categorizing the interaction of human beings with telecommunication terminals" [13]. The X.1081 framework can be used to derive "safe limits for the operation of telecommunication systems and biometric devices" [13].

X.1081 defines taxonomy of "all possible human-device interactions" [13]. This taxonomy provides a set of ASN.1 (Abstract Syntax Notation One) [8] information object identifiers whose values can be included in a biometric system heartbeat message that documents system safety and other operational characteristics. These values represent the safety posture of an active telebiometric system at a given point in time. Safety posture can be specified using "quantities and units of measurement based on the ISO/IEC 80000-series of standards" [13]. These values can be compared against device manufacturer recommendations, to ensure safe operation over the life of a device.

3.2 Information Management

Safety posture information that documents the operation of telebiometric system devices should be captured in a secure system event journal. Journal records should provide compliance validation material [4], such as evidence that equipment operation falls within the recommended safety levels for which the equipment manufacturer accepts liability. System safety posture can be used operationally to determine trends in device behavior over time. These trends may indicate that replacement, adjustment, repair, or other corrective action is needed to ensure public safety, system performance, and availability.

Compliance of a telebiometric system to the availability, performance, and safety objectives of the organization should be periodically validated. Secure system event journals should provide validation material that can be used to determine system compliance to organization policies [4]. Independent third parties should use the journal to validate system safety compliance and publish formal reports to ensure public trust in the ethical management and safe operation of telebiometric systems. Metrics gathered from system event journals should be used to inform management decision making, document the safety posture of the organization's biometric devices, and for continuous improvement of the organization's information security and safety management program.

4. FUTURE STANDARDIZATION

4.1 Focus

ITU-T Study Group 17 (SG17) is widely known for its expertise in the development of information and communications technology (ICT) standards. Unlike organizations limited to a single technology domain, such as biometrics or security, SG17 can bridge multiple domains, bringing them together in standards with a cross industry focus that benefit multiple communities. Through its communications process and liaison activities, SG17 engages experts from across the world to standardize solutions that have a global impact. It is well positioned to play a central role in the development of standards that enhance the safety, security, and privacy of individuals and make sustainable communities possible.

SG17 includes experts in biometrics, information security, public key infrastructure, schema definition languages, and telecommunications technologies. The following proposals for standardization will require expertise from all of these disciplines. In particular, the involvement of the abstract syntax, information security, telebiometrics, and Directory experts of SG17 will be needed to ensure the development of high quality solutions that are safe and secure. This combination of expertise and cooperative engagement makes SG17 uniquely suited to lead in the development of the following proposed standards that cross industry boundaries and technology domains.

4.2 Heartbeat message

Telecommunications-enabled biometric devices can support real time remote management and monitoring by system administrators. These devices can send periodic system heartbeat records to alert system administrators of security and safety events, such as changes in device settings or geographic location. Over time, heartbeat records can provide evidence of the safe and secure operation of a telebiometric system.

In aggregate, heartbeat record data provides a measure of the performance and availability of the devices in a system. Coupled with security event information, this data can be used to present a dashboard view of the security and safety posture of the system. When compared against policy requirements, metrics derived from heartbeat record data can indicate whether operations are achieving the policy objectives of the organization.

The safe and secure operation of telebiometric systems can be affected by "real-world factors such as 1) Human factors, 2) External environmental conditions, 3) System related issues" [9]. Heartbeat records logged in a secure telebiometric event journal provide an audit trail that document the safety and security posture of system devices. Metrics collected from journal records can inform the continuous improvement of a telebiometric information security and safety management program.

An ASN.1 schema for a telebiometric system heartbeat message should be standardized by ITU-T. This message should be recorded in a secure telebiometric system event journal. Data values that measure device operational safety should be included in the heartbeat message. These values should be associated with those identified in the X.1081 taxonomy [13]. Security and performance information on the quality of a remote verification process of a biometric device should be defined as an optional heartbeat message field that carries an ISO/IEC 24761 report [6]. The report would not be used in this context for making an informed access control decision, but to provide operational values useful for system administration and for information security and safety management.

4.3 Telebiometric event journal

ITU-T Study Group 17 should develop a standard telebiometric event journal. This effort should provide an extensible ASN.1 schema [12] for journal records that makes widespread information exchange possible. A standardized schema would facilitate the development of interoperable applications from multiple vendors. Extensibility would support sustainable, flexible systems that can evolve over time, and allow any adopting community with a need to extend the schema.

This ASN.1 schema should support both compact binary and XML journal formats. Providing two ways to represent journal records would allow peer applications to support either or both formats. Application designers could choose the format best suited for use in a given context. They might use XML locally, then store or exchange telebiometric information efficiently using a compact binary format as depicted in Figure 1.

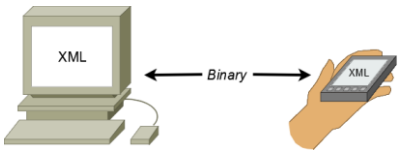

Figure 1. XML and binary information exchange

Binary event journal messages are appropriate for use in environments constrained by mobility, limited battery life, or bandwidth (e.g., wireless communications using hand held and personal devices). Compact binary journals are needed when there are high volumes of transactions (e.g., mobile internet commerce) or limited storage capacity (e.g., common access (CAC), personal identity verification (PIV), and other smart cards). Telebiometric system devices that must transfer data over radio waves or congested communications links or with devices whose period of use

may be limited by battery life can benefit from using compact binary formats, and still leverage XML markup when needed.

A standard for a telebiometric event journal should build upon the event journal defined in the ISO 19092 biometric information management and security standard. This standard predates the emergence of cloud computing, smart phones and tablets, and the convergence of wireless telecommunications and biometric technologies. A new ITU-T standard could build on the security requirements of ISO 19092 to improve the security, privacy and safety of modern telecommunications users. Extensions could include support for system availability and performance monitoring and the safe operation of telebiometric devices.

Telebiometric event journals and records should be signed objects. Without the protection of a digital signature, the integrity of telebiometric information cannot be assured. Digital signatures can provide integrity assurance that information has not been altered since being signed. Signature verification can also provide evidence of data modifications that might otherwise go undetected. With PKI-based X.509 certificates [11], the origin of a signer can be determined. This determination can provide assurance that the information source can be trusted and allow sources that are not trusted to be detected.

Multimodal biometrics applications depend on reliable data collected from multiple sensor locations and vendors. International travel that depends on biometric enabled passports has led to an increasing need for sharing biometric and other personal information across legal and regulatory boundaries. Persons charged with maintaining our safety and security require reliable telebiometric information to make informed decisions. This reliance on technology makes origin authenticity and data integrity crucial for ensuring our communities are sustainable.

4.4 Cryptographic schema

Telebiometric information should be protected using appropriate cryptographic safeguards and other securitymeasures. System managers, regulators, and the public should be confident of the integrity and authenticity of the telebiometric information used by decision makers to ensure public safety and security. Information assets that should be protected include the biometric data of system users, personally identifiable subscriber information, and event journal data used to improve information security and safety management programs. These objects should be signed using a digital signature associated with a PKI using an ASN.1 SignedData cryptographic message.

SignedData is an extensible cryptographic message that provides data integrity and origin authenticity services using a PKI-based digital signature. SignedData is used in many network security protocols. One variation of the message is used to distribute X.509 certificates and certificate revocation lists (CRLs). SignedData is one of a set of cryptographic key management messages referred to as Cryptographic Message Syntax (CMS) [17].

SignedData is widely deployed in network security protocols, including Secure Sockets Layer (SSL) and Transport Layer Security (TLS). SignedData is used to distribute X.509 certificates in the Organization for the Advancement of Structured Information Standards (OASIS) Web Services Security (WSS) X.509 Security Token. SignedData is included in tool kits on a number of popular operating systems, including several versions of Windows and Unix servers.

Several widely deployed CMS standards define a SignedData message. These include the RSA Public Key Cryptography Standard (PKCS) #7, the Secure Electronic Mail (S/MIME) CMS standard defined by the Internet Engineering Task Force (IETF), and the X9.73 Cryptographic Message Syntax: ASN.1 and XML standard [17]. However, there is no international CMS standard that uses valid ASN.1 syntax to define its message schema.

The data security of a number of international biometric standards depends on the cryptographic schema defined in the IETF CMS standard. IETF CMS SignedData is used in the "International Civil Aviation Organization (ICAO) standard for machine-readable travel documents (MRTD) including electronic passports" [1], the ISO/IEC 24761 Authentication context for biometrics, and the ISO/IEC 19785-4 Common Biometric Exchange Format Framework (CBEFF) – Security block format specifications.

Two informational IETF CMS publications contain valid schema definitions. The message schema specified in the normative IETF 3852 CMS standard [16] does not contain valid ASN.1 syntax. Though the standard lists the current ASN.1 standards in its reference section, these versions of the ASN.1 standards are not used. Instead, the IETF 3852 CMS schema is based on X.208, the deprecated 1988 version of ASN.1 that was withdrawn as a standard in 2002 [10]. The known defects in X.208 were never corrected before it was abandoned. These defects were corrected in the current ASN.1 standards [8].

New types to support national languages were never added to X.208. The Distinguished and XML Encoding Rules were never defined for use with the X.208 syntax. The IETF CMS schema attempts to mix X.208 syntax with syntax from post-1988 versions of ASN.1 in the same ASN.1 module, which is not allowed in the ASN.1 standards. Based on this ambiguous syntax, tools that implement the ASN.1 standards are not able to generate applications that conform to any version of the ASN.1 standards. The reliance on invalid cryptographic syntax for data security in the ICAO, ACBio, and CBEFF standards does not enhance the ability of these important biometric standards to provide information assurance and security.

ITU-T should create an international Cryptographic Message Syntax standard. This work should be developed by the security, PKI, and schema language experts in Study Group 17 (SG17). A new CMS standard should be created as a generic application of ASN.1 in the X.890-series of recommendations and standardized jointly with ISO and IEC. The new CMS standard should contain valid ASN.1 syntax and its schema should support all of the compact binary and XML encoding rules.

The X9.73 CMS standard contains valid syntax whose binary encodings are valid IETF CMS binary values. To the greatest degree possible, XML encoded values of the X9.73 CMS standard should be valid encodings in the new ITU-T CMS standard. The ITU-T standard should follow the approach of the X9.73 standard and collect in a single set of ASN.1 modules the schema for all of the key management techniques defined in CMS. These techniques include key agreement, password-based encryption, and constructive key management.

4.5 Signcryption message

Signcryption is a relatively new cryptographic primitive standardized in ISO/IEC 29150 [7]. Signcryption uses a special algorithm that blends together signature and encryption schemes to perform digital signature and asymmetric encryption functions simultaneously. This hybrid cryptographic technique provides confidentiality, data integrity, and origin authenticity in a single, efficient operation.

Efficient cryptographic protection methods are needed in telebiometric systems if they are to empower human users and manage their safety and security risk. Such methods help to ensure that telebiometric systems provide the privacy and security citizens need to build sustainable communities, and the reliable management information system providers need to ensure high quality, safe, reliable service.

Signcryption offers a smaller message size and faster processing speed compared to *sign-then-encrypt* signature followed by encryption techniques [2]. Unlike safeguards that rely on symmetric keys, the reliance of signcryption on asymmetric cryptography makes non-repudiation possible. These features make signcryption ideal for protecting telebiometric system information, such as ISO/IEC 19785 templates, ISO/IEC 24761 reports, and ISO 19092 journals.

In the paper *Protecting Biometrics Using Signcryption* presented at the 2012 ID360 Global Forum on Identity [3], an ASN.1 schema for a signcryption message is defined. The paper proposes that a new SigncryptedData type be added to the X9.73 CMS [17] standard to extend CMS functionality. The proposed schema is based on the familiar SignedData type used to protect "electronic mail, biometric enabled watch lists, biometric reference templates, and [*sic*] biometric elements in the Electronic Biometric Transmission Specification (EBTS)" [3] transactions used by law enforcement.

The SigncryptedData type allows biometric information objects to be signed, and for selected elements within these objects to be encrypted. In the *signcrypted-components* mode, one of three proposed modes of operation, one or more elements of an information object are signcrypted. The resulting object is then cryptographically bound to one or more attributes under a digital signature. These signed attributes must include a manifest of all of the elements in the information object that have been signcrypted.

This field-level encryption capability coupled with a digital signature makes the SigncryptedData type ideal for use in managing the safety and security of telebiometric systems, and for protecting the sensitive elements found in biometric templates, verification reports, and event journals. Using SigncryptedData, a biometric reference template can be signed, and the biometric data component within the template can be signcrypted using the same cryptographic keys. While there is security risk that must be managed when using cryptographic keys for more than one purpose, this solution meets the security requirements of ISO 19092 by ensuring the user's biometric data remains confidential within a reference template having origin authenticity and data integrity protection.

Rather than including SigncryptedData in the optional signature block defined in the ISO/IEC 19785 CBEFF standard, stronger protection of biometric templates can be achieved when SigncryptedData is used as a message wrapper that encapsulates the entire template. A message wrapper approach allows a trivial attack on reference templates to be detected using signature verification. In environments in which the optional signature block is not required to be present, it is possible for a low skill attacker to remove the entire signature block to thwart the signature safeguard's effectiveness. Telebiometric systems that serve global communities of mobile users should ensure the effectiveness of security safeguards in all usage contexts.

When a biometric verification process is performed at a remote location, identification and access management (IdAM) systems must make authentication decisions using devices in an uncontrolled environment. Relying parties may lack administrative control over the remote biometric devices used to authenticate users that access their systems. Remote biometric systems owned or operated by others may not be subject to the security and privacy policies of the resource owners.

The ISO/IEC 24761 (ACBio) standard [6] provides relying parties security and performance information on the quality of a remote biometric verification process. ACBio transfers a biometric verification process report to the relying party. A digital signature associated with a SignedData message

protects this report. However, in the current version of ACBio, this SignedData message is based on an IETF CMS schema, which does not conform to any version of the ASN.1 standards.
Verifying the signature and validating the certification path from a report signer to a trust anchor provides the report recipient data integrity and origin authenticity assurance. The report itself gives a relying party assurance that the match decision returned by a remote biometric verification system can be trusted. ACBio provides a means for "falsified reference templates, forged raw data" and "unreliable biometric devices" [6] to be detected. ACBio reports allow the security risk associated with remote biometric verification to be managed. The SignedData message provides integrity and authenticity protection, but does not protect the confidentiality of ACBio information.

ACBio respects human values by ensuring that its reports do not contain personally identifiable information, such as biometric data from a biometric reference template or the biometric sample of an identity claimant. However, the SignedData message wrapper does not prevent ACBio device identification and operational information from being collected and viewed by an eavesdropper or by a trusted insider. Transport layer encryption could be used to provide point-to-point protection, but that approach does not provide an end-to-end confidentiality solution.

ACBio reports contain biometric device identification, match control configuration settings, and match processing information that might benefit an attacker. This information could be aggregated over time to help plan attacks or to identify a weakness in a biometric system. Replacing the SignedData wrapper with a SigncryptedData [3] wrapper would add confidentiality services to the data integrity and origin authenticity services provided by SignedData. This would extend the usefulness of ACBio to law enforcement, defense and intelligence environments, where access to system operational information may be restricted by security classification level or on a need-to-know basis.

The SigncryptedData message could extend ACBio with support for additional signed attributes added by any user with a need. These attributes might include system heartbeat information, operational safety and performance reports, security classification markings or security and privacy policy. For stationary equipment, a geolocation attribute could be used to monitor and detect unexpected relocation of a system device.

5. CONCLUSION

ITU-T should create a standard telebiometric event journal whose records are defined in an ASN.1 schema. Records should document biometric system security events following the events defined in ISO 19092 [4]. Event journals should be signed objects. When necessary, event journal records should also be signed, and selected fields should be encrypted to protect the privacy of human beings.

A system heartbeat journal record should be defined along with one or more records containing useful metrics collected from journal entries. A field in this heartbeat record should allow optional inclusion of an ACBio system verification report.

ITU-T should create a new Cryptographic Message Syntax (CMS) security standard whose messages are defined using valid ASN.1 syntax. This new generic application of ASN.1 should be standardized jointly with ISO/IEC. ITU-T experts should promote its adoption in international standards that are important for securing telebiometric information, such as ICAO, ISO/IEC 19785 and ISO/IEC 24761. Improving security standards that contain invalid ASN.1 syntax can enhance the safety, security, and privacy of telebiometric system users.

ITU-T should standardize the schema and associated cryptographic processing of a new SigncryptedData type. This new type should be added to an ITU-T CMS standard. All of the signcryption mechanisms and cryptographic algorithm identifiers defined in the ISO/IEC 29150 standard [7] should be supported. Though signcryption is not intended for use in signing X.509 certificates, the Directory standards should be examined to determine whether modifications are needed to support signcryption operations.

REFERENCES

[1] Biometrics and Standards. ITU-T Technology Watch Report #12, December 2009. Retrieved November 21, 2012 from http://www.itu.int/oth/T230100000D/en

[2] Dent, Alexander W. (2004). Hybrid cryptography, Cryptology ePrint Archive Report 2004/210. Retrieved November 21, 2012, from http://www.signcryption.org/publications/pdffiles/Dent-survey-eprint-04-210.pdf

[3] Griffin, Phillip H., *Protecting Biometrics Using Signcryption*. Proceedings of ID360: The Global Forum on Identity, the Center for Identity, University of Texas at Austin, 2012. Retrieved November 21, 2012, from http://phillipgriffin.com/innovation.htm#ID360

[4] ISO 19092:2008 Financial services – Biometrics – Security framework.

[5] ISO/IEC 19785-1, Common Biometric Exchange Formats Framework – Part 1: Data element specification

[6] ISO/IEC 24761 (2009), *Authentication context for biometrics*.

[7] ISO/IEC 29150 (2011), *Signcryption*.

[8] Larmouth, John, *ASN.1 complete*. San Francisco: Morgan Kaufmann Publishers, 2000. Retrieved November 21, 2012, from http://www.oss.com/asn1/resources/books-whitepapers-pubs/larmouth-asn1-book.pdf

[9] Pour, Babak Goudarzi, There's A Metric for That': How 'Big Data' Impacts Biometrics Market and Industry, June 16, 2012. Retrieved November 21, 2012, from http://biouptime.com/2012/06/16/the-business-impact-of-big-data-on-biometrics/

[10] Recommendation ITU-T X.208 (1988). *Specification of Abstract Syntax Notation One (ASN.1)*.

[11] Recommendation ITU-T X.509 (2008). The Directory: Public-key and attribute certificate frameworks.

[12] Recommendation ITU-T X.680 (2008). *Abstract Syntax Notation One (ASN.1): Specification of basic notation*.

[13] Recommendation ITU-T X.1081 (2011). *The telebiometric multimodal model – A framework for the specification of security and safety aspects of telebiometrics*.

[14] Recommendation ITU-T X.1084 (2008). *The telebiometrics system mechanism - Part 1: General biometric authentication protocol and system model profiles for telecommunications systems*.

[15] Recommendation ITU-T X.1086 (2008). *Telebiometrics protection procedures – Part 1: A guideline to technical and managerial countermeasures for biometric data*.

[16] RFC 3852 *Cryptographic Message Syntax* (2004). Internet Engineering Task Force (IETF). Retrieved November 21, 2012, from https://www.ietf.org/rfc/rfc3852.txt

[17] X9.73-2010 *Cryptographic Message Syntax – ASN.1 and XML*. U.S.A.: American National Standards Institute (ANSI).