
Defense Standardization Program
Journal
January/March 2013
Biometrics Standardization
Secure Biometric Information
Compact Biometric Messages
The Biometrically Enabled Coalition

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAR 2013		**00-01-2013 to 00-03-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Defense Standardization Program Journal. January/March 2013	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defense Standardization Program Office,8725 John J. Kingman Road, STOP 5100,Fort Belvoir,VA,22060-6220**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

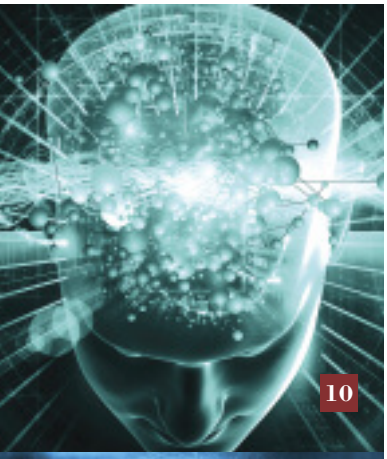
15. SUBJECT TERMS

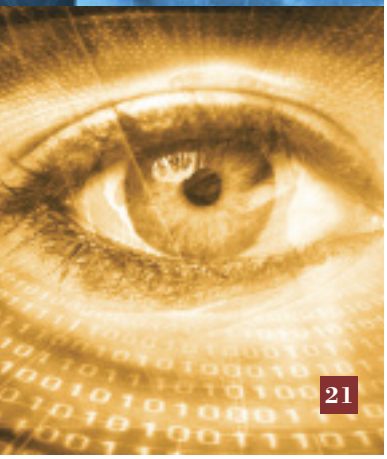
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**48**	

Defense Standardization Program Journal

Contents

January/March 2013





1 **Director's Forum**

3 **Secure Biometric Information**
Extending the DoD Electronic Biometric Transmission Specification

10 **Compact Biometric Messages**
Efficient DoD EBTS Transactions

17 **Supporting the Operational Mission**
Biometric Application Profiles for the DoD Electronic Biometric Transmission Specification

21 **The Biometrically Enabled Coalition**
ABCA Armies Biometric Interoperability Products

26 **Measuring Quality of Biometric Images**
An International Standards-Based Approach to Biometric Image Quality Measurement

Departments

39 Program News 41 Events 42 People

Future issues of the *DSP Journal* will be available only in electronic form.

To receive future issues, please subscribe by sending e-mail to DSP-Editor@DLA.mil with the address you want us to use to notify you when a new issue is posted to the DSP website and type **Add to LISTSERV** in the subject line.

The *Defense Standardization Program Journal* (ISSN 0897-0245) is published four times a year by the Defense Standardization Program Office (DSPO). Opinions represented here are those of the authors and may not represent official policy of the U.S. Department of Defense. Letters, articles, news items, photographs, and other submissions for the *DSP Journal* are welcomed and encouraged. Send all materials to Editor, *DSP Journal*, Defense Standardization Program Office, 8725 John J. Kingman Road, STOP 5100, Fort Belvoir, VA 22060-6220. DSPO is not responsible for unsolicited materials. Materials can be submitted digitally by the following means:

e-mail to DSP-Editor@dla.mil
CD or DVD to *DSP Journal* at the above address.

DSPO reserves the right to modify or reject any submission as deemed appropriate.

Gregory E. Saunders
Director, Defense Standardization Program Office

Tim Koczanski
Editor, Defense Standardization Program Journal

Defense Standardization Program Office
8725 John J. Kingman Road, STOP 5100
Fort Belvoir, VA 22060-6220

703-767-6888
Fax 703-767-6876

dsp.dla.mil

Director's Forum

Very few of the transactions that take place in today's society are done without some form of identity authentication.

Every move we make—whether it's accessing facilities, accessing computer networks, or making simple purchases at the grocery store with a debit card—is tracked. Further, our credentials are authenticated and validated to ensure we are who we say we are. And although authentication and validation are accomplished with relatively simple protective measures (for example, entering PINs, user names, and passwords or showing a photo ID), the risk is much greater than it would be if we used physiological characteristics, or biometrics. Physiological characteristics are inherently unique to an individual and have been proven to be a better measure than the measures currently used for determining individual identity. For example, law enforcement officials and the forensics community have long relied on biometrics data such as fingerprints, DNA, or dental records in the identification of criminals. And DoD has increasingly relied on biometrics data to determine friend from foe while fighting the Global War on Terror. The way we define, capture, store, safeguard, and disseminate biometrics data has been evolving at a rapid rate. To stay vigilant in our security posture, it's important to make sure that we are putting the right standards in place to capitalize on our use of biometric technologies.

Agencies throughout the federal government, in state and local governments, and certain private-sector businesses rely on biometrics to verify and validate identity for many reasons. Over the past decade, the National Institute of Standards and Technology (NIST) has coordinated much of the effort in this area and has been actively involved in the development of specifications for biometrics. By providing guidance on how biometrics systems are to be tested, results calculated, and data reported,

Gregory E. Saunders
Director
Defense Standardization Program Office

NIST has been at the forefront in helping to define methods for accessing high-quality biometrics information, while ensuring that the various biometrics systems used throughout the federal government are interoperable. Though a lot of investment goes into the component technologies that read and store the data, imagine what would happen if data from a DoD system couldn't be read by a system at the Department of Homeland Security. By having NIST manage the development process, we are ensuring the use of a common set of standards and protocols, thus increasing the flexibility and readability of data with different systems at different agencies. Not only is DoD able to use biometrics to validate the identity of good guys, but also to identify bad guys trying to gain access to facilities, computers, and so on. Further, thanks to commonly used standards, we are better able to share the data among our partners and allies as well.

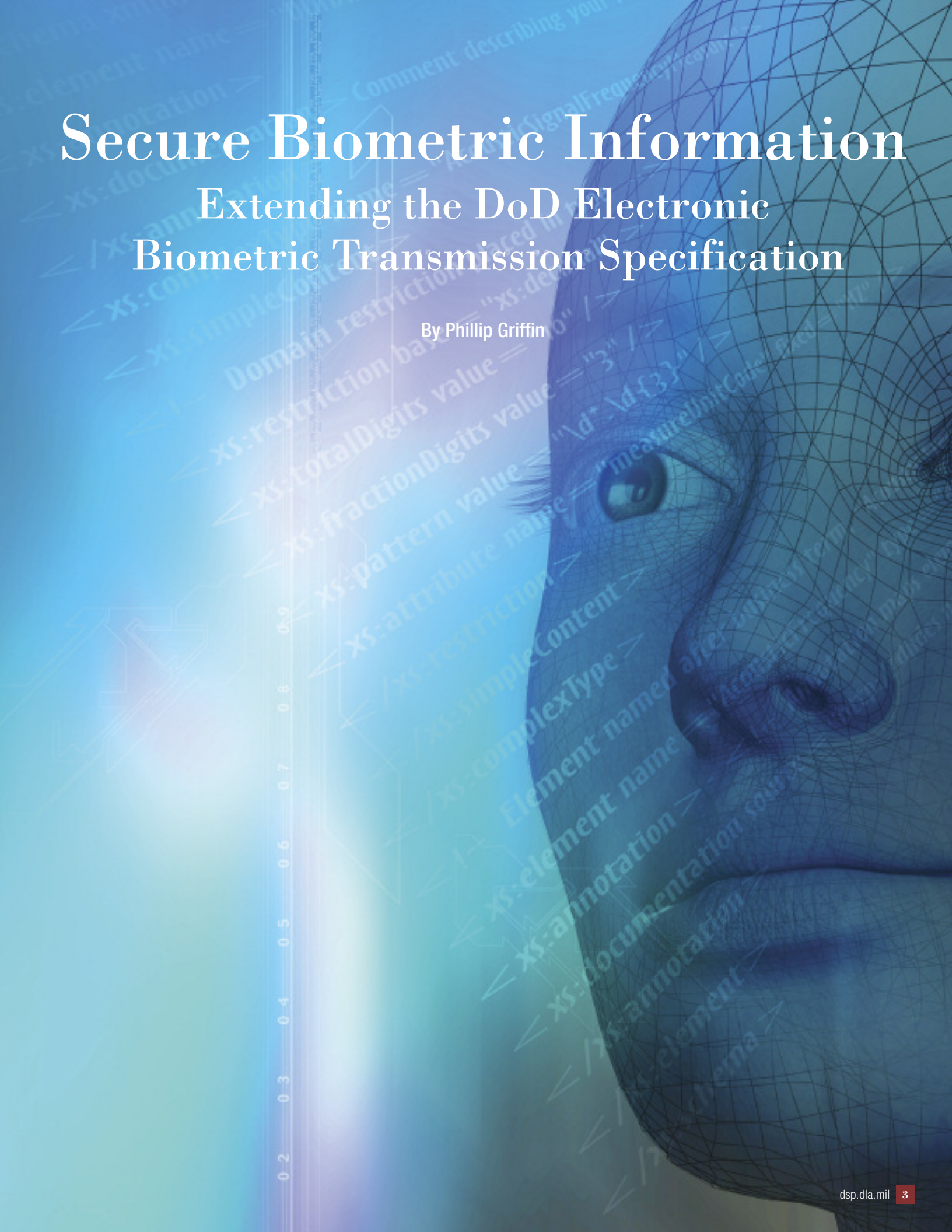
In this issue of the *Defense Standardization Program Journal*, you will learn how the use of various biometric modalities, such as fingerprints, face, and iris, have become key enablers in helping better secure facilities, protect assets, counter fraud, screen individuals, and continue keeping our personnel safe and secure. Many of the articles in this issue are authored by our colleagues at the Army's Biometrics Identification Management Agency (BIMA). They discuss BIMA's work in developing and implementing biometric capabilities for the combatant commands, services, and defense agencies and show how BIMA's work is ensuring interoperability. By incorporating a variety of widely used standards—for example, the ANSI/NIST ITL "Standard on Data Format for the Interchange of Fingerprint, Facial and other Biometric Information"; the ISO/IEC family of standards on "Information Technology–Biometric Data Exchange Formats for Finger Image Data, Facial Image Data, and Iris Image Data"; or the ABCA's "Core Biometrics Collection Standard," which defines best practices and the biometric transmission standards necessary to exchange biometrics data during coalition operations—BIMA is taking the necessary steps to ensure that we are accurately capturing the information we need, managing the information we get, and measuring the accurate quality for the biometric image that were are using.

As you read this issue of the *Journal*, I hope that you'll see how biometrics is helping to keep us both safe and secure and that you'll recognize the critical role played by standards in supporting the accuracy and the interoperability of biometrics data.

Secure Biometric Information

Extending the DoD Electronic Biometric Transmission Specification

By Phillip Griffin



The DoD Biometrics Identity Management Agency (BIMA) is the premier organization dedicated to protecting the nation through the employment of biometric capabilities. BIMA leads DoD activities to program, integrate, and synchronize biometric technologies and capabilities and to operate and maintain an authoritative DoD biometric database to support the national security strategy.

BIMA supports internal DoD business and warfighting needs by collecting biometric samples. These are either enrolled into the system as new samples or matched against previously enrolled samples.[1] BIMA has developed the DoD Electronic Biometric Transmission Specification (EBTS) to enable the exchange of biometric information with other agencies and DoD information-sharing partners in order to ensure mission success.

The latest version of DoD EBTS is based on the American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST) Information Technology Lab (ITL) standard, ANSI/NIST-ITL 2011. The ANSI/NIST-ITL standard also serves as the foundation for biometric information exchange standards developed by Interpol and the Department of Homeland Security. Other specifications, such as the DoD Biometrically Enabled Watch List and the Federal Bureau of Investigation EBTS standard, also rely on ANSI/NIST-ITL–based transactions.

The DoD EBTS standard is used to move biometric data and associated DoD-relevant information from a biometric collection location to a storage, matching, and distribution point. BIMA stores this information and performs biometric matching using its Automated Biometric Identification System (ABIS). ABIS functions as a central matching system by sending matching results and distributing biometrics to DoD information-sharing partners in the form of DoD EBTS transactions.

The DoD EBTS transactions are transferred and stored as messages that may be in one of several traditional formats or represented as Extensible Markup Language (XML). DoD EBTS information integrates the biometrics component into the DoD Identity Management (IdM) strategy. Biometrics enables IdM across four domains: warfighter, business, intelligence, and security and law enforcement. Organizations within these domains make decisions based on the accuracy and reliability of DoD EBTS information that can affect national security. It is crucial that these decision makers receive information that can be shown to be free from tampering and to have originated from a trusted source.

Since publication of the DoD EBTS 3.0 standard in 2011, an increased need to extend and secure DoD EBTS messages has developed. Some users require that the biometrics distributed by ABIS include security classification markings, need-to-know, or geospatial

intelligence information. Other users need to know what security or privacy policies apply to both the biometric data and the other information in a DoD EBTS transaction. As applications and information move out to the global Internet to reduce operating costs and increase organizational agility by utilizing web services, other users need to associate DoD Discovery Metadata Specification terms with biometric information.

DoD EBTS describes many transaction types composed of different records. One important record is the Type-2 record, which contains a number of user-defined fields. In the past, user-defined fields in the optional Type-2 record have been used to extend DoD EBTS files. This approach has been problematic. Often the content being added had nothing to do with biometric matching, and these extensions increased file size and processing complexity in systems that use biometric information. Extensions made to DoD EBTS using the Type-2 record require continuous changes to the standard. These changes can affect all adopters of DoD EBTS and the systems they use.

DoD EBTS files are not signed objects. Without the protection of a digital signature, data integrity cannot be assured. Digital signatures provide assurance that data have not been modified since it was signed, and they aid in the detection of accidental and malicious changes that might otherwise go undetected. With the increased need for sharing biometrics among dispersed law enforcement agencies and DoD partners, origin authenticity of biometric information becomes crucial for organizations that rely on biometric technology. Origin authenticity can provide assurance that information comes from a trusted source and that information from sources not trusted can be detected.

A partial security solution was provided with the addition of a Type-98 Information Assurance record to the ANSI/NIST-ITL 2011 standard. This optional Type-98 record was incorporated into the latest version of DoD EBTS. The Type-98 record contains a SignedData object, an extensible cryptographic message that provides data integrity and origin authenticity services using a digital signature based on a public key infrastructure. However, Type-98 is not available in all versions of DoD EBTS, and its effectiveness is limited to use in environments in which the optional Type-98 record is required to be present.

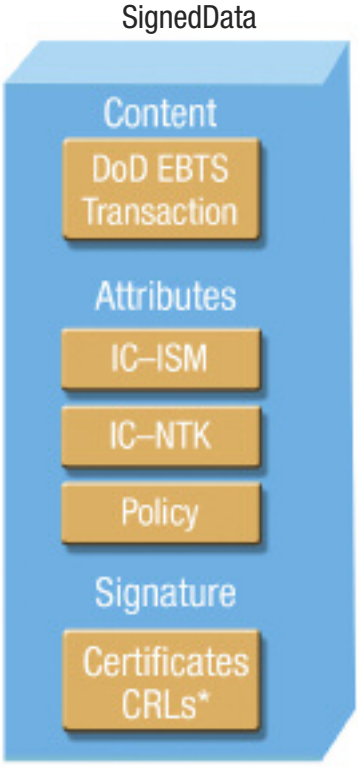
A mechanism is needed that provides security in all environments and for all versions and formats of DoD EBTS. This mechanism should allow any user of DoD EBTS to extend the standard in a way that does not require its revision. Extensions needed by one group should not require implementation by the entire community. This mechanism should enhance the integrity and authenticity of biometric information, and it should isolate the DoD EBTS standard from the revision cycles of other standards.

These requirements can be met using the Type-98 SignedData object as a message wrapper that encapsulates the entire DoD EBTS file. As a message wrapper, SignedData can protect any version or format of DoD EBTS. Associated attributes of any type or format that are needed can be bound to DoD EBTS data using a digital signature to create a secure, one-part message. These signed attributes are external to the DoD EBTS data. They are not embedded in the data, so their use requires no modifications to the DoD EBTS standard.

SignedData is part of a series of messages referred to as Cryptographic Message Syntax (CMS). Several widely used and deployed CMS standards define the SignedData object. The Internet Engineering Task Force (IETF) defines CMS in its Secure Electronic Mail standard. CMS-type SignedData is also used in the ANSI/NIST-ITL 2011 Type-98 security record to protect selected DoD EBTS information.

The financial services also define CMS in their X9.73 standard and extend traditional CMS to provide both compact binary and XML-formatted messages. The X9.73 version of CMS is used to manage biometric information security in the X9.84 Biometric Information Management and Security standard and to protect biometric information using SignedData. It is also widely deployed in ATMs, where it is used to protect critical financial information.

Figure 1. Extended DoD EBTS Transaction



*Certificate Revocation Lists.

As shown in Figure 1, a SignedData wrapper can be used to bind a DoD EBTS transaction to a set of external attributes. A digital signature binds these separate components to form a simple, one-part secure message. Each attribute is external to the transaction content and to the other attributes. This separation allows each message component to be represented in its own format and to conform to its own schema without affecting the validity of the other components.

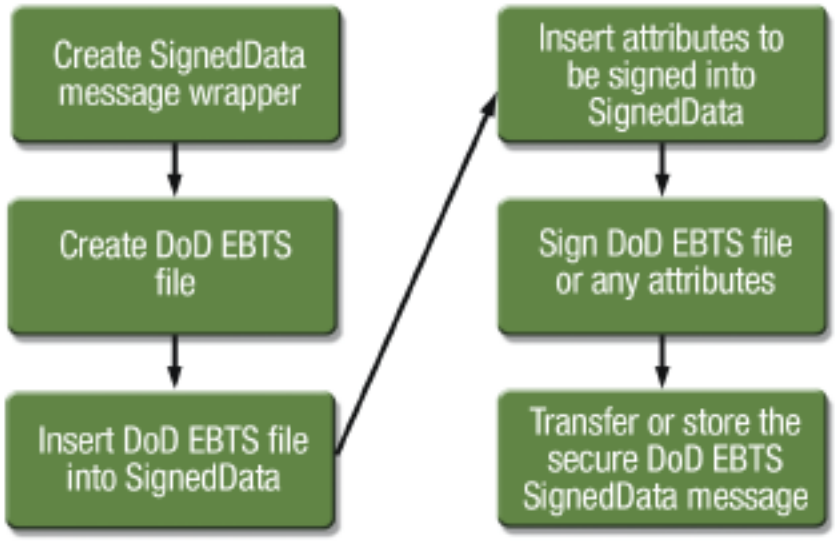
Any version or format of DoD EBTS can have a transaction signed in this manner. Any number of signed attributes of any type or format can be included in the SignedData message wrapper. As component versions change or as new components are needed,

they can be added to the message without affecting the DoD EBTS transaction, the high-level processing of the wrapper, or the SignedData signature verification and validation processing.

Figure 1 shows an Intelligence Community Information Security Marking (IC-ISM), Need-to-Know (IC-NTK), and security policy attributes. Optional certificates and certificate revocation lists may be useful in signature verification and can also be carried in the wrapper.

The CMS SignedData message allows any version and any format of DoD EBTS to be cryptographically bound to any number or kind of associated data. The associated data are in the form of signed attributes. These attributes can carry any type or format of information needed by the DoD EBTS community, including security markings and security and data-handling policy. Figure 2 describes the process of creating a secure extended DoD EBTS message.

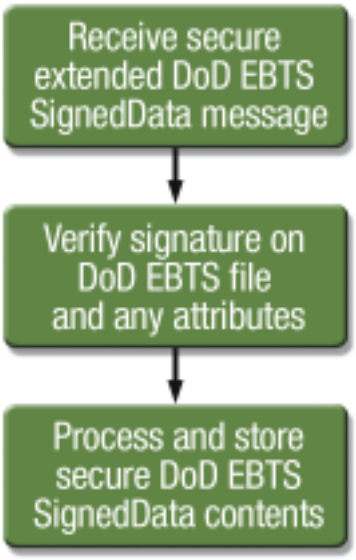
Figure 2. Creation of a Secure Extended DoD EBTS Message



The use of a digital signature allows any change in the signed data to be detected by a relying party during the process of signature verification. Signature verification will fail if even one byte of the data has changed. Public key certificates are used to identify the signer of the information so that the origin of the information can be authenticated. This allows data from nontrusted sources to be identified and rejected. Figure 3 depicts the message processing steps performed by a recipient of a secure extended DoD EBTS SignedData message.

Once the digital signature in the SignedData message has been verified, the attributes and DoD EBTS file content can be processed and stored. The entire message can be

Figure 3. Receipt of a Secure Extended DoD EBTS Message



stored together, or the signature and attributes can be stored together and the DoD EBTS file can be stored separately, perhaps as fields in a single database record. In the future, when a relaying party may need to verify the signature, the entire SignedData message can be reassembled. Its signed components can also be collected and used as input to the signature verification process.

Using SignedData as a DoD EBTS message wrapper allows the entire biometric transaction to be protected, including the optional Type-98 security record. Any attributes included in the wrapper are bound to the DoD EBTS data but are not part of the DoD EBTS standard. The wrapper approach decouples the DoD EBTS standard from the other standards used to define the payloads of each signed attribute.

The attribute payloads are not embedded in the DoD EBTS transactions, and they are not part of the DoD EBTS schema. They are logically bound to DoD EBTS by a digital signature. Their processing is layered on top of the DoD EBTS biometric processing and does not add to the complexity of the biometric matching process.

The X9.73 version of CMS is ideal for use as a message wrapper for extending DoD EBTS transactions. It provides both a compact binary encoding and a human-readable XML version of its SignedData message. The binary version is compatible with the IETF version of CMS that is already in the DoD IT Standards Registry.

X9.73 CMS defines attributes for use in SignedData that carry Security Assertion Markup Language assertions and XML Key Management Specification information. The X9.84 biometric security standard references X9.73 and defines biometric information security management attributes for biometric data that can be leveraged to manage DoD EBTS information. The X9.84 biometric security standard defines CMS attributes that identify biometric security and privacy policies, identify requirements for multifactor authentication using biometrics, and more.

X9.73 SignedData provides a single-part XML message that can be used to ease processing by existing security safeguards and to extend DoD EBTS messages. There is also a "detached" mode of SignedData. This mode allows the DoD EBTS content to be stored separately from the rest of the SignedData message for ease of processing by previously deployed systems not expecting the SignedData message wrapper.

A SignedData cryptographic message wrapper allows any user to easily extend DoD EBTS transactions without changes to the standard. Signed attributes required by one user but not supported by others do not interfere with DoD EBTS information exchange or ABIS biometric match processing. Extending DoD EBTS transactions using a SignedData wrapper enhances biometric information exchange by providing biometric data integrity and assurance that critical identity information comes from a trusted source.

[1]Dale Hapeman, "Biometric Interchange and Interoperability: The DoD Electronic Biometric Transmission Specification," *Defense Standardization Program Journal*, October/December 2008.

About the Author

Phillip Griffin, a Certified Information Security Manager, is a support contractor and subject matter expert for BIMA. He has served as editor of the X9.84 and ISO 19092 biometric information management and security standards. He cofounded and chaired the OASIS XML Common Biometric Format and OASIS Security Standards joint committees. At BIMA, he is responsible for National Information Exchange Model packaging of DoD EBTS and represents BIMA on the OASIS Biometric Identity Assurance Services committee. Mr. Griffin has 15 years of experience in development of information assurance and security standards and secure message protocols.

Compact Biometric Messages

Efficient DoD EBTS Transactions

By Phillip Griffin

The Biometrics Identity Management Agency (BIMA) has developed the DoD Electronic Biometric Transmission Specification (EBTS) to transport, store, and exchange biometric data and DoD-relevant information.[1] Biometrics is the "something you are" identity factor used in authentication and identification systems. Biometrics is a key DoD capability used to identify the enemy and to deny them the anonymity they require to hide among friendly populations where they can launch attacks at will.

Biometric standards enable a wide range of military and business missions that help DoD protect the nation. The most recent version of the DoD EBTS standard defines a set of structured messages as request–response transactions. These transactions support both warfighting and business needs. The structure and content of these messages are defined using the Extensible Markup Language (XML) Schema Definition (XSD) language.

Compact Message Motivation

The XSD schema directly supports a single-message format, representing biometric information in DoD EBTS messages as XML instance documents. This textual format is human readable and machine processable, and it facilitates tagged biometric information exchange using XML markup. However, biometric data have a binary format. The larger size and textual nature of XML documents make them inefficient for use in biometric information storage, transfer, and processing in some DoD environments, such as those faced by soldiers in the field where they are constrained by issues such as limited bandwidth (e.g., wireless and mobile devices) or limited battery life (e.g., handheld biometric collection devices). Warfighter support systems are constrained, and they must support high volumes of transactions over crowded satellite communications links. Other environments may be constrained by limits on the size or cost of storage (e.g., common access cards and personal identity verification cards).

A binary format for DoD EBTS messages is better suited for use in constrained environments. Binary messages are shorter than their XML markup counterparts. DoD EBTS transactions can contain many large binary objects (e.g., iris images, DNA, and fingerprint sets). These objects can be transferred, processed, and validated more quickly in their native binary formats than when represented as XML instance documents.

Information Exchange Options

DoD EBTS 3.0 defines an XML schema for information exchange and data transmission and storage. This schema allows DoD and its partner agencies to share biometric data. When the standard is implemented, derivatives of the published schema can be used to achieve more efficient XML validation and data transfer.

DoD EBTS 3.0 describes two standards-based approaches to enhance transfer, storage, and information exchange efficiency. One approach uses the XML-binary Optimized Packaging (XOP) standard to transfer biometric objects in multiple-part messages.[2] XOP information transfer relies on hybrid messages, with one message part containing XML markup and several other message parts containing binary content.

The XML part of an XOP message contains markup that no longer conforms to the DoD EBTS XML schema and cannot be validated against the published schema. This markup is a derivative of a valid DoD EBTS transaction that is produced by XOP processing. XOP processing modifies a valid transaction and replaces selected binary elements (fingerprints, DNA, face images, etc.) with pointers. Each pointer identifies one of the binary XOP message parts in a multiple-part XOP message.

The DoD EBTS standard describes a second approach for enhancing data transfer, storage, and information exchange efficiency that relies on the Abstract Syntax Notation One (ASN.1) standards. Binary DoD EBTS transactions are based on an international standard, ISO/IEC 8825-5, defined jointly by ISO and the International Electrotechnical Commission (IEC). ASN.1 is also standardized as the X.694 recommendation by the Telecommunication Standardization Sector of the International Telecommunication Union (ITU-T).[3]

The ASN.1 approach produces a simple, single-part binary message. Using ASN.1 XML Encoding Rules, this binary message can be readily converted into valid XML transactions whenever needed. This approach requires less processing overhead than XOP, because using ASN.1 eliminates the need for XOP to convert message components between binary and XML formats during transfer and for applications to manage multiple-part messages.

ASN.1 Compact Messages

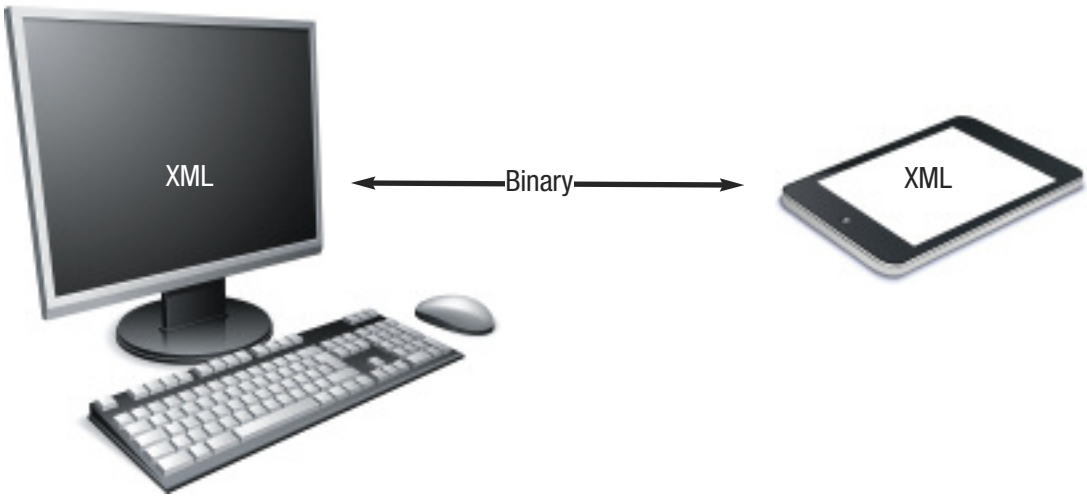
To address message size and processing efficiency concerns, the latest version of the DoD EBTS standard supports a compact binary representation of its XML markup transactions based on the ASN.1 standards. The DoD EBTS XSD schema can be translated into an analogous ASN.1 schema based on the mapping defined in the X.694 standard. Once a mapping from an XSD to an ASN.1 schema exists, ASN.1 encoding rules can be used to validate, send, and receive both compact binary and human-readable XML messages. ASN.1-generated messages in the form of XML markup can exchange information with applications based on the DoD EBTS XML schema.

An X.694-based ASN.1 schema derived from the DoD EBTS XML schema can be directly inputted to programming-language code-generation tools. These tools can automate development and simplify implementation of the standard. Generated DoD EBTS

application programs are ready to be deployed on hundreds of platforms, including devices that run the latest smartphone and tablet operating systems.

From a common XML schema, DoD EBTS implementations can transfer information as XML documents, compact binary messages, or a mix of both formats. DoD EBTS transactions can be transferred and stored in both machine-readable binary and human-readable XML formats. Peer applications can use XML locally, then store or exchange information more efficiently using a compact binary format. Figure 1 depicts the information exchange.

Figure 1. Information Exchange



A common XML schema allows DoD EBTS users to enjoy the many benefits of using XML, yet store and transfer biometric information in a more efficient binary format. Compact binary DoD EBTS transactions can enhance network efficiency of systems that provide critical biometric matching support to warfighters. Common access and personal identity verification cards with limited storage capacity, devices that transfer DoD EBTS data over radio waves or congested communications links, or devices whose period of use may be limited by battery life can all benefit from using compact binary formats based on the DoD EBTS standard and its XML schema.

Having two formats to represent the same data is beneficial. This capability allows applications to use XML locally and a compact binary format for storage or exchange. Biometrics devices that transfer data over radio waves or congested communications links, or whose period of use may be limited by battery life, can benefit from using compact binary formats when needed and still leverage XML for display. Applications that can exchange binary information can also communicate effectively with applications using XML markup.

Compression Results

A DoD EBTS 3.0 Ten-Print Transaction Error (ERRT) message is distributed with the standard as an example of a valid XML instance document. The instance document serves as an example that illustrates proper use of the XML schema (XSD) provided with the DoD EBTS 3.0 standard. The XSD schema and XML examples are packaged according to the requirements of an information exchange standard, the National Information Exchange Model (NIEM), as an Information Exchange Package identified as DoD EBTS IEPD 1.0.

This example transaction is represented using 9,766 characters (bytes) of XML markup. This same message is only 1,316 characters when encoded in binary using ASN.1 encoding rules. During information exchange, 7.42 binary ERRT messages can be transferred at the same time as one XML message. When stored, 7.2 binary ERRT messages require the same space as one XML message. The XML version of the example ERRT message can be derived from the binary form of the message whenever needed.

Programs that can process both XML and binary message formats can be generated using code-generation tools. These tools generate programming language code directly from the DoD EBTS 3.0 XML schema. This requires no programming development, and available tools support more than 250 target platforms, including mainframe, Windows, UNIX, iPhone, and Android operating systems. Programs generated directly from the DoD EBTS schema can be incorporated easily into DoD EBTS applications and systems.

Validation and Transfer

Biometric data, such as fingerprint images, iris scans, and DNA, are commonly stored and processed in a standardized binary format. For use in XML documents, the DoD EBTS schema defines binary information in a verbose character-string format known as Base64.[4] Base64 encoding of binary information causes their size to increase by approximately 33 percent. Larger amounts of information require more storage and transmission time, and computing resources must be used to convert this information between binary and character-string formats.

For binary information represented in character-string format, transfer size and time can be reduced by using the XOP standard. XOP transfers fingerprint images and other binary biometric data in their native binary formats, while XML instance documents that conform to the DoD EBTS schema must represent binary information in a character-string format. However, binary information used in XOP applications must be converted from binary- to character-string format for validation against the DoD EBTS schema.

Systems that use XOP must be capable of processing multipart messages and recognizing the headers that separate message parts, making XOP unsuitable for some DoD environments. XML validation efficiency still suffers when XML tools must process large amounts of unstructured Base64 components to validate an XML document against the DoD EBTS XML schema. The use of XOP addresses binary biometric data transfer efficiency. However, transfer efficiency gains come at a cost of increased data conversion overhead and schema validation issues. XOP use alone does not address the processing required to convert binary biometric information between binary and character-string formats, or the need to validate DoD EBTS transactions efficiently.

An alternative to XOP that addresses these concerns is to use a derivative schema that supports both binary and XML markup formats of DoD EBTS transactions. These formats, based on the X.694 standard, allow an XML document to be transferred and validated in a compact binary form that is then presented to a recipient as the initial XML document.

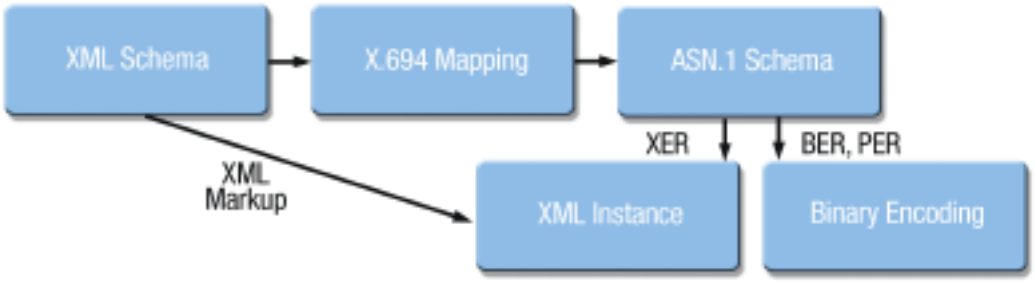
To enable this approach, the DoD EBTS XML schema is translated into an analogous ASN.1 schema based on the mapping defined in X.694. Once a schema mapping has been created, the ASN.1 encoding rules can be used to transfer DoD EBTS documents in binary and XML markup formats. The XML documents produced using a derived ASN.1 schema will be valid DoD EBTS documents.

How ASN.1 Works

Every XML schema has an analogous ASN.1 schema that can be derived using the X.694 standard. A derivative ASN.1 schema can be used to represent DoD EBTS instance document values in both binary and XML markup formats. Using a DoD EBTS ASN.1 schema allows transactions to be transferred as a one-part compact binary message, which can then be presented to a message recipient as XML markup. Schema validation can be performed faster against an ASN.1 schema, because binary versions of instance documents are much smaller, and any large opaque data elements such as fingerprints and iris scans can be quickly skipped over in their binary format. In their XML format, these large image elements must be processed serially, character by character. Figure 2 illustrates the process of creating an ASN.1 derivative of the DoD EBTS schema.

The X.694 standard can be applied to map the DoD EBTS schema into a derivative ASN.1 schema. The mapping provided by X.694 allows biometric applications to produce XML-valid DoD EBTS instance documents or compact binary versions of those documents. Both of these document formats can be transferred in simple, single-part messages as required by some secure DoD systems.

Figure 2. Mapping XSD to the ASN.1 Schema



Source: Biometrics Identity Management Agency, "Electronic Biometric Transmission Specification," 2011.
Notes: BER = Basic Encoding Rules, PER = Packed Encoding Rules, and XER = XML Encoding Rules.

Conclusion

The DoD EBTS schema can be translated directly into an analogous ASN.1 schema to enable fast binary schema validation and compact data transfer. No changes to the DoD EBTS schema are required. The DoD EBTS schema can be translated by hand or used as input to automate XML-to-ASN.1 schema translation tools. Translation is standards based and relies on the X.694 international standard.

The translated ASN.1 DoD EBTS schema can be used as input to computer programming language (C, C++, C#, Java, etc.) code-generation tools. The generated programming language code can then be used to build DoD EBTS applications that can process DoD EBTS transactions in both binary and XML markup formats. These applications will be capable of creating binary versions of DoD EBTS XML instance documents and creating valid DoD EBTS XML instance documents from these binary message formats.

[1]Biometrics Identity Management Agency, "Electronic Biometric Transmission Specification," 2011.

[2]World Wide Web Consortium, "XML-binary Optimized Packaging," W3C Recommendation 25, January 2005 (http://www.w3.org/TR/xop10/).

[3]ISO/IEC 8825-5 and ITU-T Recommendation X.694, "Information Technology—ASN.1 Encoding Rules: Mapping W3C XML Schema Definitions into ASN.1," 2008 (http://www.itu.int/rec/T-REC-X.694-200811-I/en).

[4]RFC 2045, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies," 1996 (http://www.rfc-editor.org/rfc/rfc2045.txt).

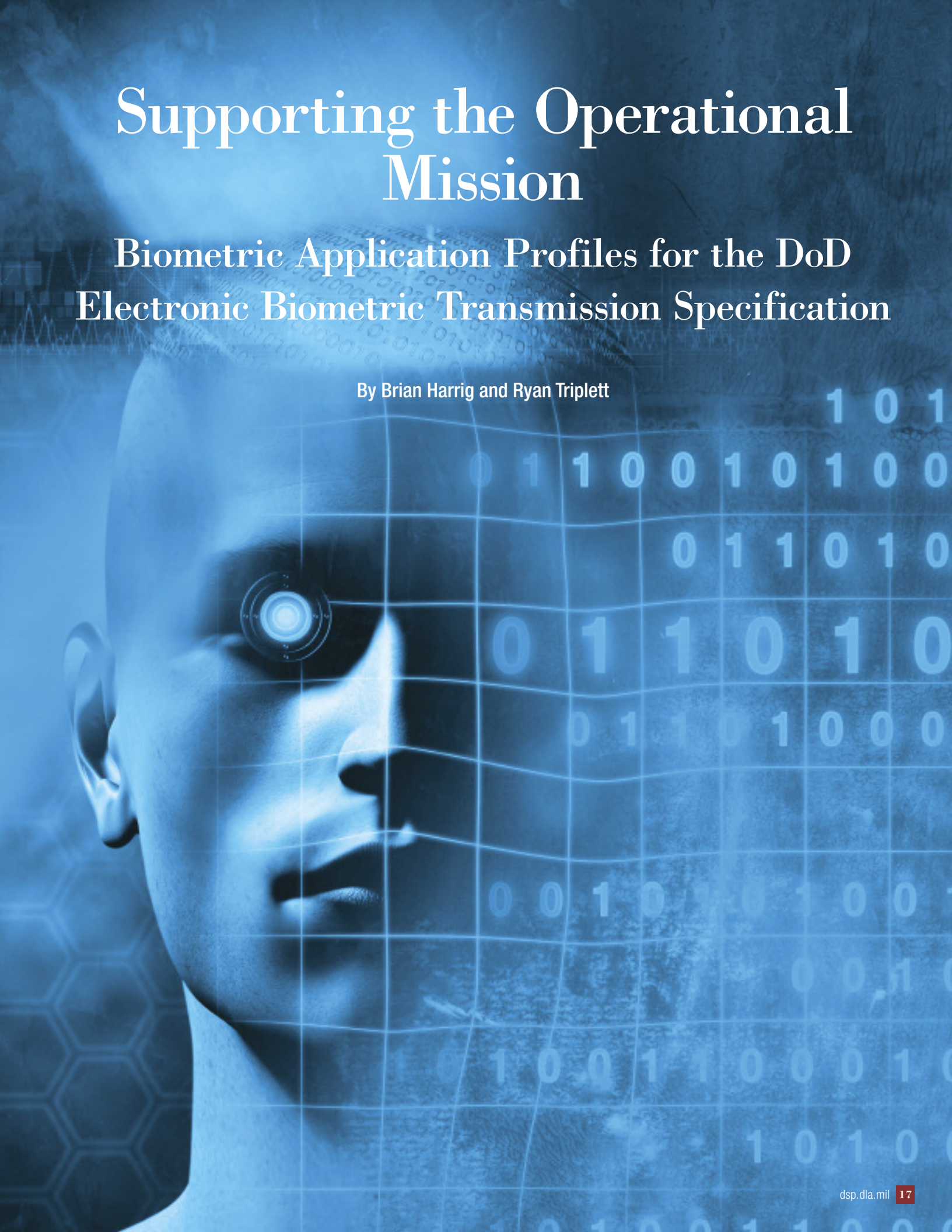
About the Author

Phillip Griffin, a Certified Information Security Manager, is a support contractor and subject matter expert for BIMA. He has served as editor of the X9.84 and ISO 19092 biometric information management and security standards. He cofounded and chaired the OASIS XML Common Biometric Format and OASIS Security Standards joint committees. At BIMA, he is responsible for NIEM packaging of DoD EBTS and represents BIMA on the OASIS Biometric Identity Assurance Services committee. Mr. Griffin has 15 years of experience in development of information assurance and security standards and secure message protocols.

Supporting the Operational Mission

Biometric Application Profiles for the DoD Electronic Biometric Transmission Specification

By Brian Harrig and Ryan Triplett



Interoperability with joint, interagency, intergovernmental, and multinational partners continues to be a topic of significant focus and interest. It is apparent that national and international biometric systems (collection devices and databases) must consistently implement and conform to the appropriate standards for the collection and sharing of biometric data to support interoperability, while at the same time, meeting mission-specific requirements. The DoD Biometrics Identity Management Agency (BIMA) continues to facilitate interoperability through the development of formally adopted biometric transmission standards and supporting documents, such as the DoD Electronic Biometric Transmission Specification (EBTS) 3.0 and the Integrated Data Dictionary (IDD) 5.0, while allowing the end users to meet mission requirements through the concept of standards profiling.

Background

On June 14, 2012, the DoD executive manager for defense biometrics signed a memorandum recommending the adoption and implementation of DoD EBTS 3.0 to reinforce biometric standardization consistency, aid acquisition authorities, and facilitate program planning across the biometrics enterprise. In addition, the executive manager requested the adoption and implementation of multiple application profiles (APs) of DoD EBTS 3.0 to support various operational requirements. The DoD EBTS Baseline Application Profile 1.0 and the IDD 5.0 are significant components of DoD EBTS 3.0, and they serve as reference points for the development of mission-specific APs.

Biometric Application Profiles

By definition, biometric APs (also referred to as biometric profiles or, simply, profiles) are conforming subsets or combinations of one or more base standards or profiles necessary to accomplish particular functions specific to the application and its domain of use. Biometric profiles define specific values or conditions from the range of options described in the relevant base standards and profiles, with the aim of supporting the interchange of data between applications and the interoperability of systems. This definition is derived from ISO/IEC 24713-1:2008 and ISO/IEC TR 10000-1:1998, developed jointly by ISO and the International Electrotechnical Commission (IEC).[1] The authoritative definition of "biometric application profile" will be included in the revision of ISO/IEC 24713-1:2008.

The DoD EBTS standard is used to store and transmit biometric data, biographical information, and associated DoD-relevant information from a biometric collection location to a storage, matching, and distribution point. DoD EBTS 3.0 aligns with the American National Standards Institute/National Institute of Standards and Tech-

nology (ANSI/NIST) Information Technology Lab (ITL) standard, ANSI/NIST-ITL 1-2011, "Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information," and the Federal Bureau of Investigation's EBTS 9.3 specification to help ensure interoperability with interagency biometric systems. The DoD EBTS and associated APs expand upon ANSI/NIST-ITL 1-2011 with a flexible framework for biographical and contextual data, while taking into consideration mission-specific data requirements. These data requirements are representative of the biometric enterprise's critical mission needs; it is essential for BIMA to continue coordinating closely with all biometric programs and aid in defining biometric operational requirements through the development of DoD EBTS APs.

The objective of a biometric AP is to define the DoD EBTS Types of Transactions (ToTs) and data-level requirements. A mission-specific AP will allow organizations to customize their profiles or develop new ToTs, while maintaining conformance with DoD EBTS 3.0. Table 1 contains examples of ToTs used in DoD.

Table 1. Examples of DoD Types of Transactions

ToT	Transaction name	Implementation notes
Submissions		
MAP	Miscellaneous Applicant–Enrollment	Submission used as part of a background check for local nationals and third-country nationals who require access to military installations or other restricted areas. Designator indicates submission based on various mission types.
CAR	Criminal Tenprint Submission (Answer Required)	Submission used for detainees, enemy combatants, enemy prisoners of war, or persons of interest (known or suspected terrorists).
Responses		
SRE	Submission Results–Electronic	This transaction is returned in response to search submissions. The response will always contain the "Ident/Non-Ident" decision.
ERRT	Ten-Print Transaction Error	This transaction is an error response.

A biometric AP also consists of ToTs that define the functionality of each service provided by the AP. The ToTs as defined in the biometric APs will provide the details of how the transmission specification can be applied to the mission or functional need at a data level. Specifically, ToTs define which logical records types (e.g., biometric modalities, contextual information, or file information) are mandatory or optional, which data fields are required within each logical record, and how many occurrences of each are allowed.

Summary

The use of nonstandardized biometric transactions limits the effectiveness of biometric data sharing and decreases the capability to identify possible threats. Biometric standards provide a level of consistency that makes them the cornerstone for interoperability. DoD EBTS 3.0 and its supplemental documents will enable the DoD biometrics enterprise to more efficiently and effectively share biometric data with its stakeholders. The use of APs allows for DoD EBTS 3.0 to be utilized in a variety of operational scenarios.

Consistent with the BIMA mission to "coordinate, integrate, and synchronize" biometric technologies, the IDD provides the authoritative definition of transmission data elements for use by the DoD EBTS stakeholders. The data fields defined in the IDD are available for the development of DoD EBTS APs and new ToTs, as well as for the exchange of standardized biometric data.

BIMA continues to stress the importance of standardization through active participation in biometrics standards bodies to accelerate and advocate DoD interests. BIMA facilitates a net-centric environment across DoD and the Intelligence Community (IC) biometrics enterprise by championing the formal adoption of biometrics standards across DoD and the IC. Among other things, BIMA participates actively in the Joint Enterprise Standards Committee and its various technical working groups, and it chairs multiple biometric standards working groups that develop consensus throughout the biometrics enterprise. BIMA continues to support its enduring biometric standardization capability to promote interoperability and consistent implementation across DoD and the IC enterprise and their joint, interagency, intergovernmental, and multinational partners.

[1]ISO/IEC 24713-1:2008, "Information technology—Biometric profiles for interoperability and data interchange—Part 1: Overview of biometric systems and biometric profiles." ISO/IEC TR 10000-1:1998, "Information technology—Framework and taxonomy of International Standardized Profiles—Part 1: General principles and documentation framework."

About the Authors

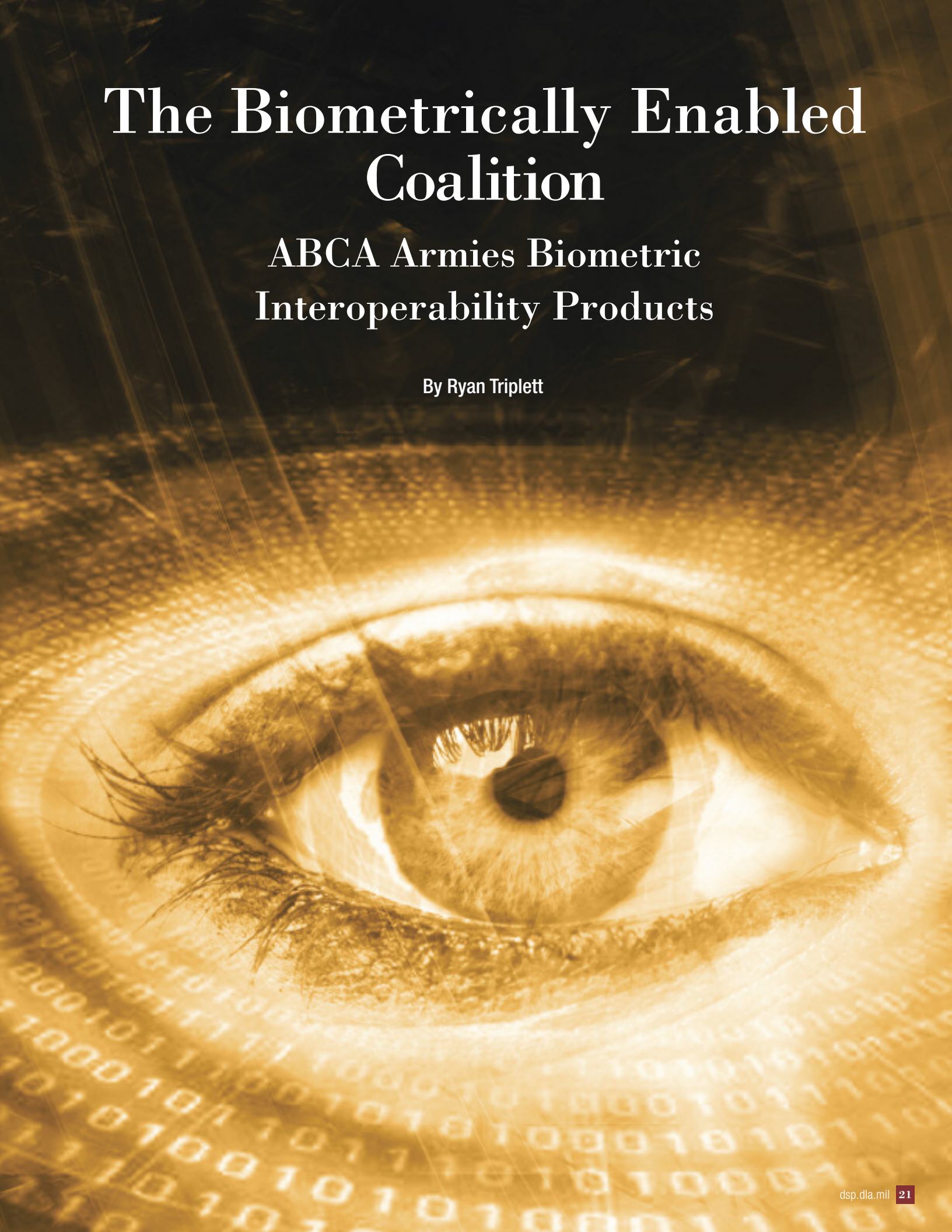
Brian Harrig, a Certified Biometrics Professional, is a support contractor and subject matter expert for BIMA, where he is responsible for the integration of identity management solutions and biometric technology. In this role, Mr. Harrig is the lead developer of the DoD EBTS, coordinates DoD BIMA interests across the federal government to promote interoperability, and coordinates national and international biometric standards for use within the DoD enterprise.

Ryan Triplett is a Certified Biometrics Professional with 15 years of engineering experience, including 8 years in the field of biometrics. At BIMA, he supports biometrics standardization and integration by leading efforts to test, implement, develop, and formally adopt biometrics and identity-related standards across the U.S. government's joint, interagency, and multinational partners. Mr. Triplett also supports BIMA's efforts to facilitate interoperability and data sharing.

The Biometrically Enabled Coalition

ABCA Armies Biometric Interoperability Products

By Ryan Triplett



Our nation's adversaries seek sanctuary among innocent civilians, masking their true identities through false identification and the use of multiple personas. The ability to distinguish these adversaries from legitimate civilians, through the use of biometric capabilities, provides a critical advantage to coalition armies.

Background

The American, British, Canadian, Australian, and New Zealand (ABCA) Armies constitute a product-focused organization whose mission is to optimize coalition interoperability through doctrine, standards, technology, and material solutions. The ABCA Program's working structure consists of capability groups (CGs) that are analytically focused and determine interoperability gaps in accordance with objectives approved by the ABCA Program's national directors (two- and one-star level). The ABCA Sense CG focuses on the interoperability aspects and understanding of the coalition operational environment, especially of adversaries, neutrals, noncombatants, weather, and terrain. To resolve interoperability gaps, the ABCA Sense CG develops mitigation strategies through project teams (PTs), which are product focused. The PTs produce ABCA standards, publications, reports, databases, and architectures.

In September 2007, the ABCA Exercises and Experimentation Support Group held a Coalition Lessons Analysis Workshop (CLAW) to analyze observations, insights, and lessons from all operations and training. The resulting report informed strategic planning by the ABCA Program's Executive Council (four-star level and equivalent) and assisted the CGs with their interoperability gap analyses. Similar CLAW reports were produced in 2009 and 2011, each documenting observations, insights, and lessons. On the basis of the CLAW reports and thorough analysis, the ABCA Sense CG identified the need for biometric-focused PTs to mitigate identified gaps and produce products to enhance biometric interoperability. The following section identifies some of the key products.

ABCA Biometric Products

In 2007, ABCA Report 42, *Coalition Report on Analysis and Findings*, documented the development, by the United States, of biometric tools and techniques for detainee operations and the potential benefits of using those tools and techniques in other areas, such as warfighter operations, force protection, and employee screening. In addition, the report noted a lack of a common biometric data interface across operational theaters down to the lowest tactical level. As a result, ABCA identified a need for a coalition biometrics network that was accessible by the ABCA nations.

The United States has since developed standard operating procedures, doctrine, and guidance on the collection, transmission, and storage of biometric data collected specifi-

cally from detainees. The United States also established networks to transfer coalition biometric data and currently provides a method to ensure national policies and laws are recognized. The DoD Biometrics Identity Management Agency (BIMA), a U.S. biometric lead representative of the ABCA Sense CG, has the authority to share this knowledge through ABCA PTs and to aid in the development of the ABCA Program's biometric-related products.

The ABCA nations had formally recognized that biometric data are a significant source of information and a valuable enabler to the coalition warfighter. However, the lack of terminology and standardization affected the ability to share information efficiently across ABCA nations. Therefore, the ABCA Program took steps to address interoperability gaps.

In 2009, ABCA Report 84, *Biometrics Capabilities*, addressed the biometric capabilities of ABCA nations and noted the lack of coherent and effective standards, national policies, and government guidance to implement and integrate biometric capabilities.

In 2010, a biometric-focused PT published ABCA Report 102, *Biometrics Glossary*, one of the first products focused on optimizing ABCA biometric interoperability by addressing the need to establish a common understanding, among ABCA nations, of biometric definitions. The PT based Report 102 on BIMA's *Biometrics Glossary* and on Standing Document 2, *Harmonized Biometric Vocabulary*, developed by the ISO Joint Technical Committee 1/Subcommittee 37, Biometrics.

Biometric Data Collection

In parallel with the development of ABCA Report 102, the PT produced ABCA Report 104, *Biometrics Architecture*, to outline the concept for a coalition operational-level biometric architecture. The report identifies the key biometric capabilities—collect, store, match, and share—needed to identify individuals and deny anonymity to our nations' adversaries through biometrics.

In 2011, in an effort to expand upon and replace ABCA Reports 84 and 104, the ABCA Sense CG established another biometric-focused PT to produce ABCA Report 138, *Biometrics Interoperability: Systems, Standards and Architectures*. This report informs ABCA nations on current biometric capabilities and provides an in-depth view of each nation's biometric operational architecture. The operational views described in Report 138 detail national biometric implementations and document the data exchange by systems in each nation to provide an integrated perspective of ABCA coalition biometrics.

Biometric Enrollment

In 2012, ABCA Standard 2089(R), "ABCA Core Biometric Collection Standard," underwent ratification. This standard defines best practices and the biometric transmission standards necessary to exchange biometric data during coalition operations. The standard addresses the minimum requirements for biometrics data collection and recommends the use of the DoD Electronic Biometric Transmission Specification (EBTS). It is understood that as biometrics technologies evolve, revisions to the standards are expected and should be adopted, in synchronization, in order to remain interoperable.

Although ABCA Standard 2089(R) established the framework for ABCA nations to exchange standardized biometric data, it did not provide guidance or identify transition periods for nations to take advantage of new functionality and remain interoperable. To ensure all ABCA nations were able to develop, implement, and transition to the appropriate versions of the U.S. DoD EBTS, as the agreed-upon specification to exchange biometric data, the ABCA Sense CG established a biometric-focused PT to develop ABCA Report 161, *Biometrics Roadmap*. This report identifies transition points for the standards recommended in ABCA Standard 2089(R) to guide synchronization of biometric technologies and enable the efficient exchange of biometric data.

To further enhance the sharing of biometric information, the biometrics PT developed Report 156, *Biometrics Application Profile*, to provide guidance for ABCA nations on how to exchange biometric information in a standardized format, while adhering to national laws and policies. Application profiles allow each nation to customize ABCA Standard 2089(R) to meet operational requirements and national caveats or to incorporate business rules such as special handling instructions.

Conclusion

The biometric-focused PTs established by the ABCA Sense CG have made great strides in mitigating biometrics interoperability gaps and have provided significant products for enhancing the exchange of biometric information among ABCA nations. To ensure continued advancement of coalition interoperability in the foreseeable future, it is important for organizations to coordinate and synchronize efforts where possible to establish efficient and integrated coalition biometrics programs. Biometric data exchange and interoperability will continue to advance the ability of ABCA nations to help each other identify national threats and protect our national borders.

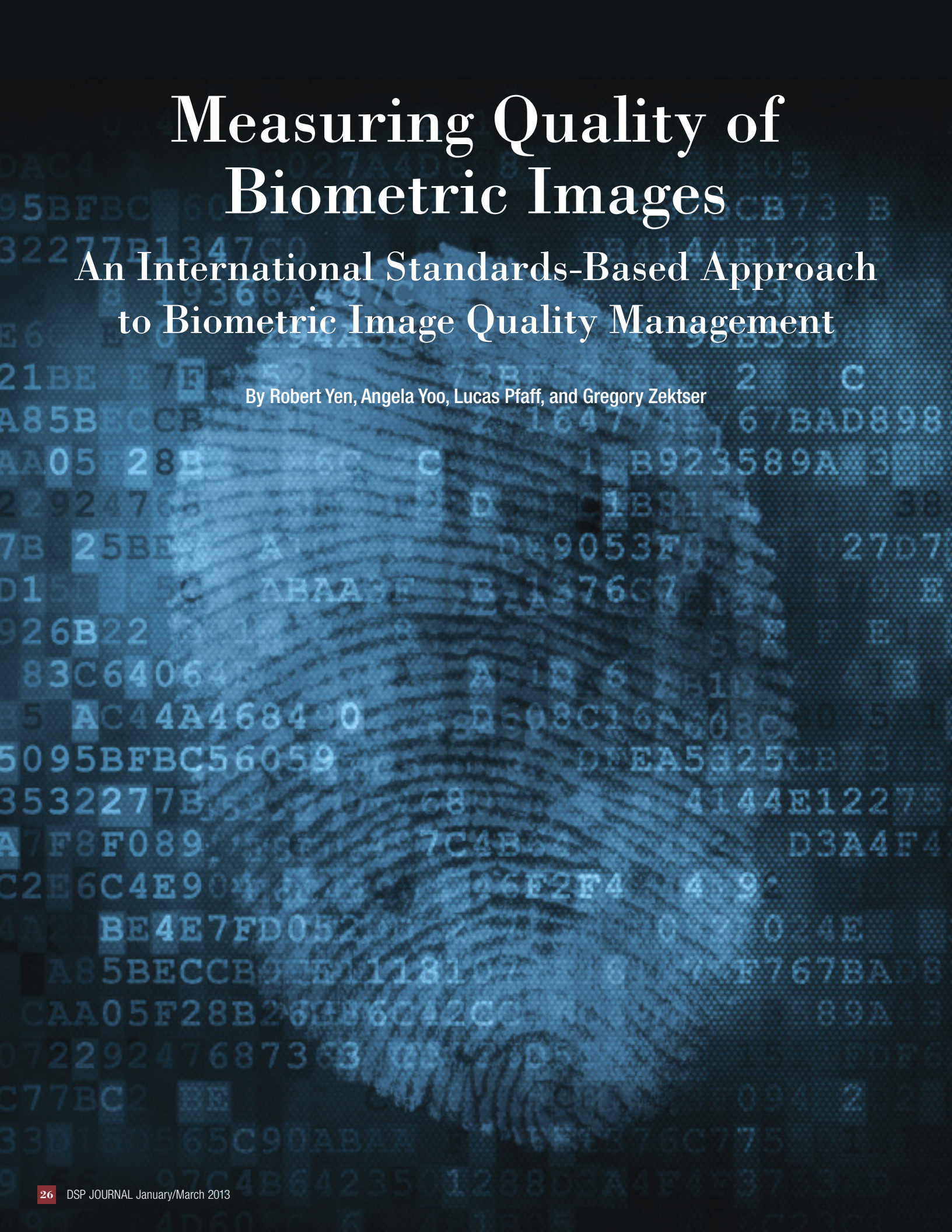
About the Author

Ryan Triplett is a Certified Biometrics Professional with 15 years of engineering experience, including 8 years in the field of biometrics. At BIMA, he supports biometrics standardization and integration by leading efforts to test, implement, develop, and formally adopt biometrics and identity-related standards across the U.S. government's joint, interagency, and multinational partners. Mr. Triplett also supports BIMA's efforts to facilitate interoperability and data sharing.

Measuring Quality of Biometric Images

An International Standards-Based Approach to Biometric Image Quality Management

By Robert Yen, Angela Yoo, Lucas Pfaff, and Gregory Zektser



Real-time biometric image quality is a critical requirement in a number of operational environments. Nonstandardized quality biometric images are commonly captured in the field. Biometric data exchanges among federal agencies suffer loss of data due to nonstandardized quality values. DoD's international standards-based biometric image quality measurement algorithms and tool sets allow the collection and storage of biometric samples that are consistently of high quality. These tools will improve the performance of DoD's biometric systems by providing consistent quality scores across all U.S. government biometric systems.

This article introduces an international standards-based approach that enables real-time quality assessment of biometric images taken from any digital capturing device. This approach uses the features identified in ISO/International Electrotechnical Commission (IEC) standards to determine the quality characteristics of biometric images. The goals are to (1) provide detailed, measured quality data based on the features listed in international standards; (2) determine the quality of an image and provide immediate, near-real-time feedback to the operators to assist them with capturing high-quality biometric samples; (3) provide confidence levels as weighting coefficients for recognition results; and (4) provide federal agencies with interoperable and agnostic quality scores that are independent of vendors' matching algorithms.

Background

In general, biometric recognition systems employ a matching (comparison) algorithm to produce a similarity measurement between probe images and each of the images in the gallery database, which is a set of captured and stored subjects' biometric sample data. A threshold can be set so that a match is reported only when the similarity measurement between the probe and a gallery image exceeds a specified threshold. Obtaining the highest possible biometric image quality is critical when capturing a subject's biometric sample (probe) image in an operational environment. Often, when capturing a biometric image, the operator will use his or her trained knowledge of the image capture process to visually evaluate the quality of the image. However, what may appear acceptable to the operator may be deemed unacceptable or entirely unusable by the biometric matching system. Transmitting and subsequent matching of an image with unacceptable quality may result in a missed chance to recapture the image—a particular concern in field collections where every examination of the image is critically important—or may inconvenience the subject who will have to return for another image capture. Images with unacceptable quality also contaminate the database and affect the performance of matching functions.

The ideal biometric image has recognizable features, such as defined ridges and valleys of a fingerprint image and clear eyes and mouth location of a facial image. These clear,

computer-readable features are what make each biometric image unique. A good quality biometric image enhances the performance of automatic recognition systems during the matching and identification process. Often, however, the image quality is poor due to the environment (lighting, deteriorating equipment, inadequate collection processes, and so on) in which the image is captured.

In March 2006 and November 2007, the National Institute of Standards and Technology (NIST)—seeking to improve the accuracy of biometric systems by incorporating quality assessment technologies into the sample acquisition process—held a series of biometric quality workshops. The purpose of the workshops was to assess the existing quality measurement capabilities and to identify technologies, factors, operational paradigms, and standards that can measurably improve image quality and the recognition rate. NIST also conducted an Iris Challenge Evaluation (ICE) study, the first large-scale, open, and independent evaluation of iris recognition technology. The primary goals of the ICE study were to promote the development and advancement of iris recognition technology and to assess its state-of-the-art capability.[1] NIST also initiated IREX 2008, a project for the development of exchangeable iris imagery in support of the compact interoperable ISO/IEC iris data record standard. NIST's motivation in undertaking IREX 2008 included the establishment of a standardized, accurate, interoperable, and compact iris image format suitable for large-scale identity management applications.

International Standards

The ISO/IEC biometric data interchange formats and sample quality standards related to the fingerprint, facial, and iris modalities are as follows:

- Fingerprint modality
  - ISO/IEC 19794-4:2011, "Information technology—Biometric data interchange formats—Part 4: Finger image data," Section 7: Image acquisition requirements, and Annex A: Image quality specifications
  - ISO/IEC TR 29794-4:2010, "Information technology—Biometric sample quality—Part 4: Finger image data"
- Facial modality
  - ISO/IEC 19794-5:2011, "Information technology—Biometric data interchange formats—Part 5: Facial image data," Section 7: The frontal face image type, and Annex A (Informative): Best practices for face images
  - ISO/IEC TR 29794-5:2010, "Information technology—Biometric sample quality—Part 5: Face image data"
- Iris modality
  - ISO/IEC 19794-6:2011, "Information technology—Biometric data interchange

formats—Part 6: Iris image data," Annex A (Informative): Iris image capture

- ISO/IEC CD 29794-6, "Information technology—Biometric sample quality—Part 6: Iris image data," Section 6: Iris image quality metrics.

Standardized Algorithms for Operational Environment

High-quality images are conducive to automatic recognition/identification systems, such as DoD's Automated Biometric Identification System. With current technologies, it is possible to implement a real-time image quality checking subsystem in which the system storing or transmitting the images can automatically and immediately indicate the status of the scan, such as "accepted," "failed," or "rescan."

Over the past several years, new methods have been developed to measure the quality of a single biometric image. Although significant progress in biometric recognition has been made, many researchers agree that the need still exists to do the following:

- Define standardized, interoperable, and computable features for use in determining the quality of images.
- Establish standardized methods to measure identified features.
- Define standardized quality scores that can be used to predict the matching behavior before the matching engine is applied.

In a fingerprint or facial image capture process, the human visual perception model should be at the core of a quantitative and automatic image quality evaluation system. The human visual perception has a remarkable ability to detect the edges (high-frequency signals) in a processed visual image and interpreted edge information. Clear edge information within a local area is interpreted as high quality.

Biometric image quality assessment is a challenging task that should be based on a standardized approach, and the quality score of an image should be interoperable among all users. Recognition of those needs has resulted in an increase in the interest in and demand for developing standards-based biometric image quality assessments tools.

DoD Biometric Image Quality Measurement Algorithms

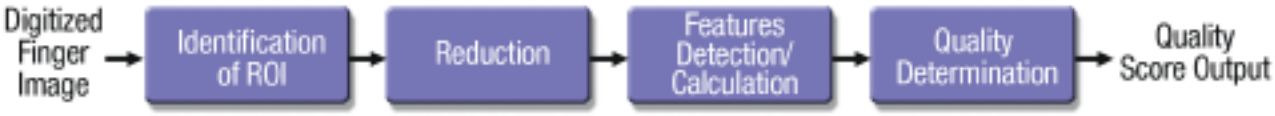
DoD's fingerprint quality measurement (FIQM) and facial image quality measurement (FaceQM) algorithms and tool sets were designed by the Biometrics Identity Management Agency (BIMA) to analyze the quality of fingerprint and facial images. The tools are implemented to run in a single executable mode (based on graphical user interface or command line), as well as to be called via an application programming interface. This section contains details about the FIQM and FaceQM tools, and it proposes an approach to iris image quality measurement (IrisQM).

DOD FINGERPRINT IMAGE QUALITY MEASUREMENT

Figure 1 depicts the process for determining the quality score for digitized finger images.[2] As the figure shows, FIQM has four modules:

- *Identification of region of interest (ROI).* This module identifies the target area ROI of a fingerprint image for quality measurement.
- *Reduction.* This module establishes multi-resolution layers, removing redundant and noisy pixels from the ROI.
- *Features detection/calculation.* This module is based on computational features described in ISO/IEC 19794-4:2011 and ISO/IEC TR 29794-4:2010. The FIQM produces an image quality score between 0 and 100 for each compressed Wavelet Scalar Quantization (WSQ) or uncompressed bitmap (BMP) or portable graymap (PGM) image with scanned resolutions of 500 or 1,000 pixels per inch (ppi). Higher scores correspond to higher quality. Table 1 lists all of the output parameters.
- *Quality determination.* This module produces a quality score to represent the entire fingerprint image and a quality vector, including data on all measured parameters.

Figure 1. FIQM Process



FIQM can process 500 ppi slap (four fingers) images as well. For each slap finger image, a segmentation function can be called to segment each single finger. Then, the same process of measuring the quality of a single finger image is applied to each segmented finger. The output includes a fused quality score that represents the entire slap image and output parameters for each segmented finger. The type of finger can be determined based on the detected cores and deltas (numbers of cores and deltas, locations, relationships).

Figure 2 demonstrates an application of FIQM, qExamine, which allows up to three examiners to "guess" the quality of a fingerprint image with a rating of high, medium, or low. Comparison of the guessed score to a consistent FIQM quality score will allow users to become familiar with FIQM quality zones.

DOD FACIAL IMAGE QUALITY MEASUREMENT

Figure 3 depicts the process for determining the quality score for digitized facial images.[3] Like FIQM, FaceQM has four modules:

- *Validation.* This module validates the image header information against the requirements of ISO/IEC 19794-5:2011. Each image usually has a header section providing

Table 1. FIQM Output Parameters

Parameter	Description
Input finger file name	Name of image file name (FIQM can accept images as compressed WSQ files, uncompressed BMP or PGM files, or data blocks/byte arrays)
Image width	Width of input image in pixels
Image height	Height of input image in pixels
File size	Size of input image file in bytes
Image quality score (0–100)	Estimated quality score based on the average of converted majority orientation directions probability from the measured area
Position score	Comparison of the midpoint of an image (in both horizontal and vertical directions) to the actual center of the image in both directions
Dynamic range	Computation based on the detected number of gray levels presented in the measured area
Dynamic range score	Computation based on the ISO/IEC standard
Number of cores	Detected cores based on the combination of the Poincare indices, orientation zone coherences, entropy of local orientations, and core orientation field masks
Number of deltas	Detected deltas based on the combination of the Poincare indices, orientation zone coherences, entropy of local orientations, and delta orientation field masks
Number of minutiae	Minutiae count detected using FingerJetFX's open source algorithm[a]
Ridge orientation distribution	Calculated entropy number representing the overall orientation distribution of major finger area; used to distinguish whether the input image is a finger or an artificial pattern
Measured width	Width of identified major finger area in pixels
Measured height	Height of identified major finger area in pixels
Measured area percentage	Calculated percentage of the region of interest in comparison to the entire image
Measured area ratio	Computation of the ratio of the width to the height of the measured area
Low-quality zone percentage	Number of cells in the measured area whose quality scores are lower than the defined low-quality threshold value, as a percentage of total cells
Medium-quality zone percentage	Number of cells in the measured area whose quality scores are between the defined low- and high-quality threshold values, as a percentage of total cells
High-quality zone percentage	Number of cells in the measured area whose quality scores are higher than the defined high-quality threshold value, as a percentage of total cells

[a]See http://www.digitalpersona.com/fingerjetfx.

Figure 2. qExamine's Main Window

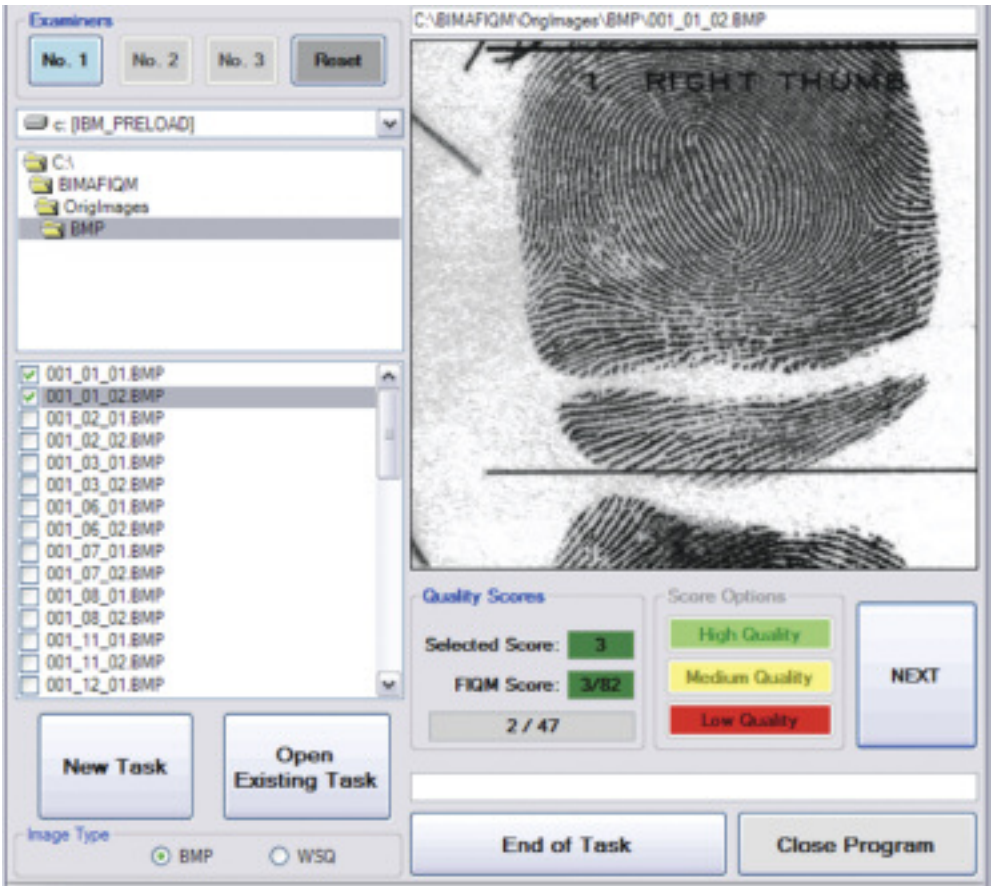
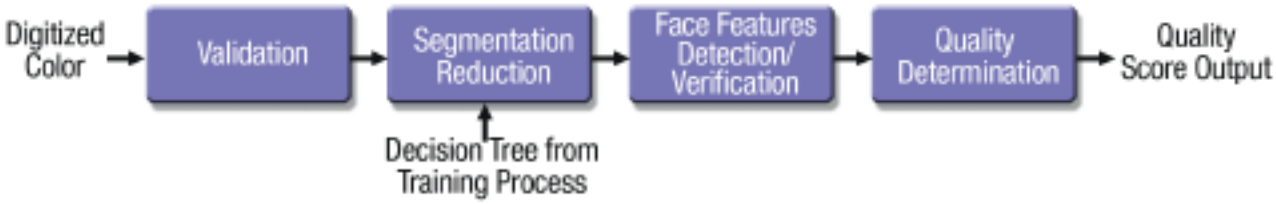


Figure 3. FaceQM Process



the detailed information in each field, for example, scanned resolution, number of rows, number of columns, and size of image. The module filters out nonconformant facial images.

- *Segmentation reduction.* Segmentation is a real-time process for each input image. The purpose of the segmentation process is to attempt to identify skin areas from the input image. The process is based on a decision tree that applies each color feature vector to identify and verify skin areas. This module segments the face region from the entry image by the decision tree that is built from training data with the Non-Uniform Binary Splitting, or NUBS, algorithm.[4] This module segments the face area as an ROI that will be applied to all measurement calculations.
- *Face features detection/verification.* Various facial features—the most important being eyes, mouth, and ears—will be detected from the segmented face area. The constraints

of computational features are described in ISO/IEC 19794-5:2011 and ISO/IEC TR 29794-5:2010. Table 2 lists the facial features that are measured.

- *Quality determination.* This module determines the quality score—translated as "good image" or "need to rescan"—for each facial image, based on verification results of facial features. Each facial feature has its own constraint. The "good image" quality score means that all detected facial features of the facial image satisfy all constraints. Any undetected or unsatisfied features will cause the measured facial image to have a "need to rescan" quality score. The 5 percent tolerance in some features' constraints allows for variations that might occur during the image-capturing process.

Table 2. FaceQM Measured Features

Feature	Description
Eyes' locations	Coordinates of detected eyes from facial area
Mouth's location	Coordinates of detected mouth from facial area
Ears' locations	Coordinates of detected ears from facial area
Bits count	Number of 24-bit color or 8-bit gray scale from input image header
Red-eye detection	"True" or "false" evaluation of red-eye possibility
Blurriness detection	Calculations of "blur percentage" and "blur extent" from a three-layer wavelet coefficient, with a high level indicating lower estimated blurriness
Near/far	Estimated distance between the face and the image capture device
Centered	Distance between the center of the face and the center of the image
High/low	Height of the eyes from the bottom of the image
Roll angle	Rotation about the horizontal axis
Yaw angle	Rotation about the vertical axis
Pose symmetry	Homogeneity between the left and right sides of the face
Contrast–co-occurrence	Contrast calculation from the co-occurrence matrix with neighborhood distance of 1 pixel
Contrast–Michelson	Measure of where bright and dark features are equivalent
Contrast–RMS	Measure of the standard deviation of the pixel intensities
Contrast–Weber	Measured luminance difference between features and background
GCF	Measure of the weighted sums of overall local contrast for different resolutions
Contrast–Hess	Measure of the sum of all frequencies for height and width of image
Exposure	Measure of all image pixel values distributed over the gray scale or over the range of values available in each color component
Sharpness	Entire image gradient
Brightness	Entire image differences in luminance
Lightening symmetry	Measure of lighting pose from left and right sides of the face
Luminance dynamic range	Measure of luminance dynamic range of the detected face area
Vertical saturation ratio	Measure of the brightness ratio in the vertical direction
Horizontal saturation ratio	Measure of the brightness ratio in the horizontal direction

For each JPEG compressed or uncompressed BMP image, the quality score is presented in three forms: a C-Score, a D-Score, and an E-Score. The C-Score is the minimum value of the 22 facial features' quality levels; each feature's quality level is converted from a measured value with predefined piece-wise mapping functions. The D-Score is the total number of facial features that satisfy the constraints; the maximum quality score is 22, which means all of the evaluated values of the 22 features satisfy all constraints, and the minimum score is 0, which means none of the evaluated values of the 22 features satisfy constraints. The E-Score is calculated based on the located eyes' coordinates and the constraints from international standards.

Figure 4 shows a frontal facial image that was determined to have unacceptable quality score (C-Score = 44, D-Score = 21, and E-Score = 73) and therefore needs to be rescanned. This result is based on the determination that the subject's yaw pose angle is toward the left and greater than the constraint, and the evaluation of pose asymmetry is lower than the constraint.

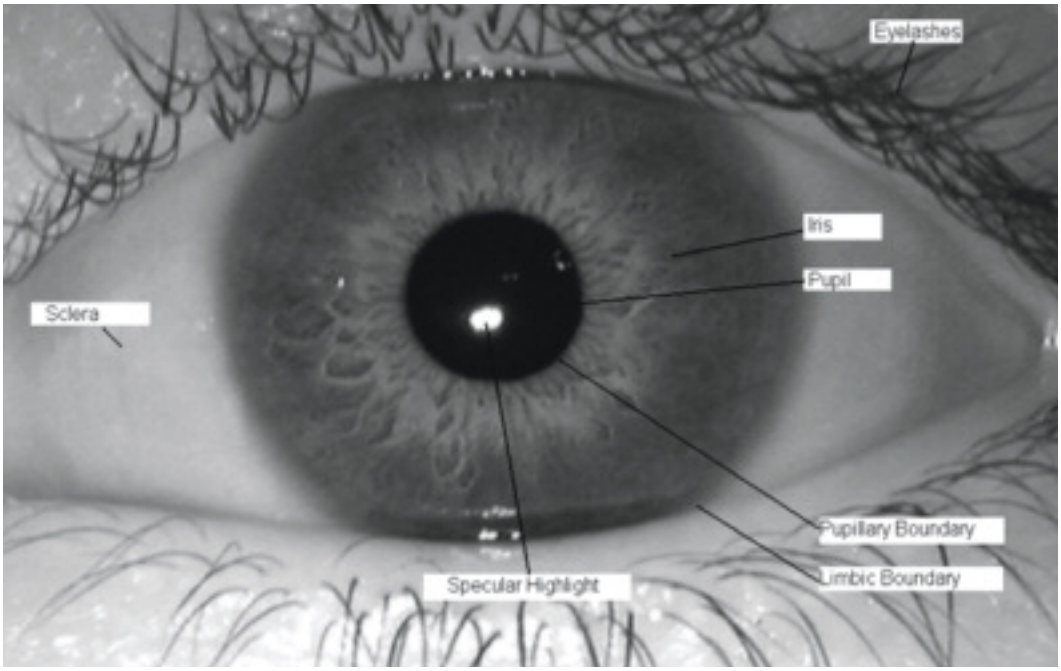
Figure 4. Read/Process Image Mode: "Need to Rescan"

DOD IRIS IMAGE QUALITY MEASUREMENT

Iris recognition is considered to be one of the most reliable biometrics in terms of recognition and identification. The recognition process involves comparing the features of the iris image against the features of a sample or samples stored in a database of iris images. Iris recognition requires detecting an iris area through a process of segmentation. Next, the iris features are encoded as a template. The iris image is preprocessed to account for factors such as illumination and characteristic and to detect particular features of the iris, and then it is encoded as an iris template to represent the iris image. The iris template data from the probe image are then matched against the template entries in the gallery.

The iris lies between pupillary and limbic boundaries, and its shape is conical with the pupillary boundary. Figure 5 shows a front view of the human eye. Like the quality of finger and facial images, iris image quality significantly affects the performance of automatic iris recognition systems during the matching (comparing) and identification/verification processes. However, human visual perception could not assist with evaluating the quality of an iris image during the capturing process because the tiny features of an iris are outside the scope of a normal human visual system.

Figure 5. A Front View of the Human Eye



So far, no robust, vendor-agnostic, and large-scale iris image quality measurement tool is available in the market. The various quality factors listed in ISO/IEC 19794-6:2011 and ISO/IEC CD 29794-6 show that the standardized features are highly correlated with recognition accuracy and are capable of predicting the recognition results.

On the basis of the recommendations of a DoD BIMA technical report, DoD IrisQM should be a government-owned, standards-based, vendor-agnostic, and robust iris image quality measure tool.[5] The DoD IrisQM algorithm is being developed by BIMA to meet DoD requirements and, as shown in Figure 6, will have three modules: (1) a module providing iris segmentation, (2) a feature extraction module providing feature information relating to the recognition, and (3) a quality determination module providing a quality score calculated from feature information. This score can be used to predict the performance of recognition.

Figure 6. IrisQM Process

Various iris features will be extracted from the segmented iris area. The constraints of the computational features are described in ISO/IEC 19794-6:2011 and ISO/IEC CD 29794-6. Table 3 lists ISO/IEC CD 29794-6 factors that relate to iris image quality. The factors represent the baseline that will be used by DoD IrisQM to measure the quality of iris images. (DoD BIMA expects to release IrisQM in fall 2013.)

Key Benefits

The DoD international standards-based approach includes calculating the standardized features listed in ISO/IEC 29794 series standards. Applying DoD international standards-based biometric quality measurement tools to biometric recognition systems has several key benefits:

- Quality measurement algorithms are vendor agnostic (i.e., vendor independent) and do not depend on the design of matching algorithms or the captured conditions.
- Quality score of a fingerprint or facial image simulates a human's visual perception.
- Quality score can be used as a predictor for matching behavior before matchers are applied.
- Quality score can be customized (or mapped) to other scoring systems (for example, Good–Medium–Poor or Acceptance–Rejection).
- Quality score vector provides detailed, measured quality data.
- Quality score can be used as a confidence index that supports the matching results.
- Quality score can be used as a weighting coefficient that supports the fusing matching score calculation in a multimodal recognition system.
- Quality parameters can be used to evaluate the performance of a recognition matching algorithm, that is, to determine the "sensitivity" of individual matchers to specific quality parameters.

Table 3. ISO/IEC CD 29794-6 Factors Relating to Iris Image Quality

Factor	Description
Usable iris area	Portion of the iris image that is usable (i.e., not occluded by eyelids, eyelashes, or saturating specular reflections), expressed as a percentage of the area of an annulus modeling the iris without such occlusions
Iris-sclera boundary contrast	Image characteristics at the boundary between the iris region and the sclera (sufficient contrast is needed in many implementations of iris segmentation algorithms; low or insufficient contrast may result in a failure to process an iris image during feature extraction)
Iris-pupil boundary contrast	Image characteristics at the boundary between the iris region and the pupil (sufficient contrast is needed in many implementations of iris segmentation algorithms; low or insufficient contrast may result in a failure to process an iris image during feature extraction)
Pupil boundary shape	Eccentricity or other measures of deviation from circularity of iris-sclera and iris-pupil boundaries
Sharpness (defocus)	Degree of defocus present in the image
Frontal gaze–elevation	Degree of vertical displacement between the optical axis of the camera and the optical axis of the eye
Frontal gaze–azimuth	Degree of horizontal displacement between the optical axis of the camera and the optical axis of the eye
Gray-scale utilization	Measure of the dynamic range of the gray scale (a useful iris image should have a dynamic range of at least 256 gray levels, allocating at least 8 bits, with a minimum of 7 bits, of useful information)
Iris radius	Measure, in the image plane, representing half the distance across the iris along the horizontal
Pupil-to-iris ratio	Degree to which the pupil is dilated or constricted
Iris-pupil concentricity	Degree to which the pupil center and the iris center are in the same location
Margin	Degree to which the image achieves positioning of the iris portion of this image relative to the edges of the entire image
Motion blur	Degree of distortion in the image due to motion

- Quality parameters enable the user or the capturing system to adjust images to provide higher quality score images for use in recognition.

Conclusion

The DoD standards-based biometric image quality measurement algorithms and tool sets provide detailed, measured quality data based on features listed in the ISO/IEC biometric quality standards. The tool sets determine the quality of an image and provide feedback to the operator to help capture the best possible images in real time. The quality scores provide confidence levels to the recognition results. The tool sets also provide interoperable and consistent agnostic quality scores that are independent of the vendors' matching algorithms across all U.S. government international biometric systems. They

allow for the collection and storage of consistently high-quality biometric samples and will improve the overall performance of the DoD biometric systems.

[1]NIST, *FRVT 2006 and ICE 2006 Large-Scale Results*, NISTIR 7408, March 2007 (available at http://iris.nist.gov/ice).

[2]The current version (6.0) of the DoD FIQM tool set is based on an approach described by R. Yen and J. Guzman in "Fingerprint Image Quality Measurement Algorithm," *Journal of Forensic Identification*, Vol. 57, No. 2, March/April 2007.

[3]The current version (4.0) of the DoD FaceQM tool set is based on an approach described by R. Yen and G. Zektser in "A New Approach for Measuring Facial Image Quality," *Defense Standardization Program Journal*, October/December 2008.

[4]For additional information about face recognition algorithms, see P. J. Phillips, H. Wechsler, J. Huang, and P. Rauss, "The FERET Database and Evaluation Procedure for Face Recognition Algorithms," *Image and Vision Computing*, Vol. 16, No. 5 (1998), and P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss, "The FERET Evaluation Methodology for Face Recognition Algorithms," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 22 (2000).

[5]R. Yen and G. Zektser, *Iris Image Quality Measurement Algorithms Study and Comparative Analysis*, DoD BIMA Technical Report, December 2009.

About the Authors

Robert Yen, Angela Yoo, Lucas Pfaff, and Gregory Zektser were support contractors and subject matter experts working with the standards branch within DoD's BIMA.

Dr. Yen leads the development and assessment of all biometric image quality-related tasks. He has 20 years of experience developing real-time imaging systems, including optical/intelligent character recognition, biometric imaging, and medical imaging.

Ms. Yoo's responsibilities include the development and testing of the FIQM algorithms and supporting software. She has 7 years of software development experience on numerous platforms and frameworks.

Mr. Pfaff develops and tests the FaceQM algorithms and supporting software. He has 12 years of software development experience on numerous platforms and frameworks.

Mr. Zektser's responsibilities include working on biometric standards and test and evaluation. He has 20 years of experience in various areas of systems engineering, technical standards development, quality management, and biometrics.

Program News

Topical Information on Standardization Programs

DSP Announces 2012 Award Winners

Annually, DSP awards teams and individuals for their efforts in playing an integral part in keeping our men and women in uniform safe and in providing them the tools they need to get the job done. The FY12 awards went to five teams and one individual:

Army

- Fred Lafferman, John Escarsega, Bernard Hart, and William Lum, from the U.S. Army Research Laboratory Organic Coatings team, for developing a suite of coating specifications to provide a family of qualified coating products that are more environmentally friendly and durable and will result in a life-cycle cost avoidance of nearly $1 billion.
- Thomas Kozlowski, from the U.S. Army Materiel Command Packaging, Storage, and Containerization Center, for leading the effort to develop a NATO standardization agreement (STANAG) for NATO land forces on the proper return of stores and equipment to designated storage, repair, recycling, supply, and disposal points. Implementation of this NATO STANAG will result in significant cost savings, safety improvements, a reduced logistics footprint, and more efficient and effective use of resources.
- Richard Squillacioti and Brian Scott, from the U.S. Army Research Laboratory Weapons and Materials Research Directorate, for developing specifications to evaluate the effectiveness of newly developed composite materials for armor vehicles and ensuring the safety of our warfighters by reducing the possibility of counterfeit or noncompliant materials being used.

Navy

- Robert Matthews, Robert Sweeney, Scott Dennis, Marcell Padilla, and Deborah Mooradian, from the Naval Air Systems Command Future Airborne Capability Environment team, for developing a technical standard that provides a common software environment to allow the reuse of software capabilities across platforms and services. Use of the standard will result in a cost avoidance of $29.1 million each time the capability is implemented on a different platform.

Air Force

- Cheryl McCormick, Benet Curtis, Thomas Burris, Donald Phelps, and Captain Daniel DeVirgilio, from the Air Force Petroleum Agency Fuel System Icing Inhibitor team, for demonstrating that fuel-system icing-inhibitor additive could be lowered without affecting air worthiness. The team's work allowed changes to the JP-8 aviation fuel specification that will save the Department $5.3 million annually and prevent fuel tank topcoat peeling.

Defense Logistics Agency

- Earnest Brown, Maurice Womack, William Carpenter, and Mitchell Ranck, from the Defense Logistics Agency Land and Maritime Interconnection team, for developing a suite of adapter fitting specifications and working with industry to develop SAE International standards that will minimize the risk of operational failure due to leaks in fuel, hydraulic, and pneumatic systems. That, in turn, will reduce pollution and hazardous material spills and will preclude a minimum of 100 nonstandard parts annually from entering DoD inventory, resulting in a cost avoidance of over $2 million a year, while shortening procurement lead-times, increasing operational readiness, and reducing the logistics footprint.

DSPO and ANSI Will Host MSHT Meeting

On June 4–7, 2013, DSPO and the American National Standards Institute (ANSI) will cosponsor the spring Materiel Standardization and Harmonization Team (MSHT) meeting in Washington, DC. The 4-day meeting will allow senior-level international standardization managers from the European Union, NATO, and the United States to network with defense personnel and industry subject matter experts, to address the standardization shortfalls affecting multinational military operations, and to learn about materiel standardization solutions that could prove helpful to the nations attending the meeting.

MSHT, an expert body composed primarily of defense standardization management experts and regional organizations, such as NATO, the European Defense Agency, and so on, aims to improve national, regional, and international defense standardization management.

Each day, the meeting will have a different agenda and focus, but will include a five-nation meeting, industry day, and general body meeting that is open to participation by industry and standards developing organizations. This is the first year for the United States to host the MSHT meeting. The meeting cosponsors anticipate a successful and educational event for all those in attendance.

Participation at this meeting is by invitation only. If you are interested in attending, contact Ms. Latasha Beckman at latasha.beckman@dla.mil, 703-767-6872.

Events

Upcoming Events and Information

May 29–31, 2013, Fort Belvoir, VA

Defense Standardization Workshop (SYS 120)

SYS 120 (formerly PQM 103) will be offered May 29–31, 2013, at DAU's Fort Belvoir campus. SYS 120 covers DoD policies and procedures for the development, management, and use of nongovernment standards, commercial item descriptions, and specifications and standards. Individual and group practical exercises emphasize the application of standardization tools, policies, and procedures described in three prerequisite courses: CLE 028, Market Research for Technical Personnel; CLE 064, Standardization in the Acquisition Lifecycle; and CLE 065, Standardization Documents. All three prerequisite courses must be completed before enrolling in SYS 120. For more information or to register, go to http://www.dau.mil; click "Training" and then click "Course Registration/Cancellation." You may also register by calling the DAU Help Desk at 703-805-3459 or toll free at 1-866-568-6924.

June 24–27, 2013, Philadelphia, PA

23rd Annual INCOSE International Symposium

The International Council on Systems Engineering (INCOSE) is holding this year's international symposium on June 24–27, 2013, at the Philadelphia Marriott Downtown. The INCOSE International Symposium is the premier international forum for systems engineering. Participants network; share ideas, knowledge, and practices; and learn more about the most recent systems engineering innovations, trends, experiences, and issues. Presentations and tutorials will address ways in which systems engineering principles, processes, and perspectives are addressed today and how systems engineering might influence our future. Topics include technology insertion, process improvements, and organizational governance of the systems we make, manage, operate, and maintain over their life cycle.

September 16–20, 2013, Orlando, FL

Fall 2013 SISO Simulation Interoperability Workshop

The Simulation Interoperability Workshop is a semiannual event sponsored by the Simulation Interoperability Standards Organization (SISO). The fall workshop will be held at the Florida Mall Conference Center. The SISO workshops encompass a broad range of model and simulation issues, applications, and communities. The workshops consist of a series of forums and special sessions addressing interoperability issues and proposed solutions; tutorials on state-of-the-art methods, tools, and techniques; and exhibits displaying the latest technological advances.

October 28–31, 2013, Arlington, VA

16th Annual NDIA Systems Engineering Conference

This conference is sponsored by the National Defense Industrial Association (NDIA) Systems Engineering Division, with technical cosponsorship by the IEEE Aerospace and Electronic Systems Society, the IEEE Systems Council, and the International Council on Systems Engineering. To be held at the Hyatt Regency Crystal City, the conference will focus on improving acquisition and performance of defense programs and systems, including network-centric operations and data/information interoperability, systems engineering, and all aspects of system sustainment. The conference is supported by the Deputy Assistant Secretary of Defense for Systems Engineering, OUSD(AT&L), and the Office of the DoD Chief Information Officer.

People

People in the Standardization Community

Welcome

Lilibeth de los Santos of Defense Logistics Agency (DLA) Aviation, Richmond, VA, was reassigned to the standardization team from the Data Management Division. She assumed Preparing Activity (PA) responsibilities for the standardization documents under standardization code DLA-GS1. She has 27 years of federal service, with a wealth of experience from other government agencies.

Edward Disselkamp joined the Standardization Program Branch at DLA Aviation as a mechanical engineer. He assumed PA responsibilities for the standardization documents under standardization codes DLA-GS4 and DLA-GS6. Mr. Disselkamp came with a background in specifications, standards, and drawings related to aviation armament equipment. He has served as a team leader at the Naval Air Warfare Center, Indianapolis, IN; a project manager in the Aircraft Sustainment Engineering Branch at DLA Aviation, working on improving targeted DLA aircraft parts and assemblies; and as a mechanical engineer for General Electric, working in the appliance design and development area of refrigeration.

Dominique Stutts joined the Standardization Program Branch at DLA Aviation. She has an extensive chemical background, which includes chemical research at the National Aeronautics and Space Administration's Langley Research Center, where she assisted with a study of alternative fuels for aircraft, and at Brookhaven National Laboratory, where she worked on radiotracer development for use in positron emission tomography. Ms. Stutts also assisted as a chemist with the startup of Dominion Virginia Power's Virginia City Hybrid Energy Center, a coal- and biomass-fueled power station.

Karolina Koller, a materials engineer, recently joined the Standardization Program Branch at DLA Aviation. She has a wealth of knowledge in fiber-optic connectors gained in medical, petrochemical, and military research from private industry. Ms. Koller is assigned to standardization code DLA-GS2, which includes parachutes, instrumental light panels, lighting fixtures for vehicles, electrical lamps, nonelectrical lighting fixtures, and electrical connectors.

People

People in the Standardization Community

Thomas Kennedy of DLA Aviation was promoted to chief of the Engineering and Technology Division from his previous position as chief of the Standardization Program Branch. As the division chief, he has oversight of the Standardization Branch, as well as DLA Aviation's value management, should-cost, sourcing, reverse engineering, casting and forging, and organic manufacturing functions. Starting as a member of the standardization team in 2004, Mr. Kennedy had PA responsibilities for standardization codes DLA-GS4 and DLA-GS8. He worked with diverse commodities, such as mechanical speedometers and tachometers, graphitic electrodes, and aircraft tie-down chains used to secure cargo. He has been an active member of several non-government standardization organizations, such as ASTM International and SAE International.

Miguel Lopez-Oquendo was promoted to chief of the Standardization Program Branch within the Engineering and Technology Division at DLA Aviation. He started his career with DLA Aviation in January 2004, working as an industrial engineer on the standardization team. He had PA responsibilities for gas cylinders, parachutes, liquid and gas flow, mechanical motion measuring instruments, lighting fixtures for vehicles, portable and hand electrical lamps, and nonelectrical lighting fixtures. In addition, he has been one of the lead audit engineers assigned to DLA Aviation's qualified products list program.

Farewell

Glen Hoffman, from the Naval Surface Warfare Center (NSWC), Corona Division (Norco, CA), retired in September 2012 after 30 years of civilian service to the U.S. Navy. Early in his career, he was awarded the Naval Sea Systems Command's "Engineer of the Year." For more than 20 years of his career, Mr. Hoffman was an integral member of the Government-Industry Data Exchange Program's (GIDEP's) information technology (IT) team. His major responsibilities included serving as GIDEP's Unix system administrator, maintaining day-to-day system operations and resolving any internal/external connectivity issues. Mr. Hoffman also contributed significantly to the development of GIDEP's Push Mail, a service that helps users keep current on new data being entered into the database. Through the years, he helped GIDEP transition from the days of modem access to the current worldwide web.

People

People in the Standardization Community

Roger Mansfield retired from NSWC, Corona Division, in December 2012 after 23 years of civilian service to the Navy. For more than 20 years of his career, he was an integral member of the GIDEP IT team. His major responsibilities included serving as GIDEP's Web Server administrator. He was also GIDEP's subject matter expert for web security, ensuring the integrity of GIDEP web access and resolving any issues or questions regarding web access. Another major accomplishment was his creation of GIDEP's database search engine, which serves as the online web interface used by the GIDEP community to access and download GIDEP documents. Mr. Mansfield helped GIDEP's transition to the worldwide web.

William Sindelar retired in December 2012 from DLA Land and Maritime, Columbus, OH. He served the federal government for more than 37 years. For the last 15 years, he supported the DSP for circuit protection devices, oscillators, and batteries. Mr. Sindelar had a wealth of knowledge from his broad work experience, which included the Kennedy Space Center, Robins Air Force Base, Newark Air Force Base (Aerospace Guidance and Metrology Center), and Defense Contract Management Agency. We wish him well in retirement.

Eugene Ebert, DLA Land and Maritime, retired in January 2013 with more than 27 years of federal service. For the last 10 years, he supported the DSP for fiber optics. He worked actively with all services to improve the standard fiber-optic components available to the services. One of his many accomplishments was the creation of MIL-STD-1678, "Fiber Optics Test Methods and Instrumentation." Mr. Ebert was very dedicated and went to great lengths to make sure his many military and industry customers were satisfied. We wish him well in retirement.

Joseph Kerby retired from DLA Land and Maritime with more than 26 years of federal service. As an electronics technician in the Document Standardization Division, he worked on military specifications and standard microcircuit drawings in the complementary metal–oxide–semiconductor microcircuit area of MIL-PRF-38535, "Integrated Circuits (Microcircuits) Manufacturing." His wealth of knowledge, dedication, and work ethic will be greatly missed. We all wish him well in his retirement.

Upcoming Issues
Call for Contributors

We are always seeking articles that relate to our themes or other standardization topics. We invite anyone involved in standardization—government employees, military personnel, industry leaders, members of academia, and others—to submit proposed articles for use in the *DSP Journal*. Please let us know if you would like to contribute.

Following are our themes for upcoming issues:

Issue	Theme
April/June 2013	Standardization Stars
July/September 2013	Interoperability
October/December 2013	Counterfeits

If you have ideas for articles or want more information, contact Tim Koczanski, Editor, *DSP Journal*, Defense Standardization Program Office, 8725 John J. Kingman Road, STOP 5100, Fort Belvoir, VA 22060-6220 or e-mail DSP-Editor@dla.mil.

Our office reserves the right to modify or reject any submission as deemed appropriate. We will be glad to send out our editorial guidelines and work with any author to get his or her material shaped into an article.


DEFENSE STANDARDIZATION PROGRAM
WHERE SYSTEMS WORK TOGETHER