Setting the standard

Steve Gold, freelance journalist

Steve Gold

Biometrics standards have been around since the mid-1980s, but how important are they in the biometrics industry? And who makes the decisions on standards? Whilst there are standards in all forms of technology to allow for continuity and interoperability between devices, the issue of standards is of paramount importance in the biometrics industry.

This is because biometrics technology has, unknown to many, become pervasive in modern life, with a variety of government agencies, including law enforcement and border control operations, using biometrics-enabled systems.

Then there is the military aspect of biometrics. Military staff – whether air force, army or navy (and quite a few agencies operating in between these categories of defence) – rely on biometrics to provide a unique identifier in situations where people, for various reasons, may not be telling the truth, or, more frequently, cannot communicate their identity in a verifiable form.

Law enforcement

The first biometric standards were in the area of law enforcement, where the need to exchange fingerprint data led the US National Bureau of Standards (now the National Institute of Standards and Technology – NIST) to publish the first biometrics standard in 1986. Since then a growing number of bodies and agencies have joined the biometrics standards bandwagon, with both formal and informal standards.

On the formal standards front there is the American National Standards Institute (ANSI), the British Standards Institute (BSI), and the Japanese Industrial Standards Committee (JISC).

In addition there are international standards development bodies that include the International Organisation for Standardisation (ISO), the International Electro-Technical Commission (IEC), and the International Telecommunications Union (ITU).

Biometrics in Afghanistan: military standards have exacting parameters.

The informal standards bodies have an equally important role to play. It's within bodies such as the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C) and the Organisation for the Advancement of Structured Information Standards (OASIS) that a lot of biometrics development work goes on.

OASIS, in particular, is something of an unsung hero in the field of biometric standards as the not-for-profit consortium that drives the development, convergence and adoption of open standards for the IT industry in general.

In fact, according to OASIS, the consortium that produces more web services standards than any other organisation along with standards for security, e-business, and standardisation efforts in the public sector and for application-specific markets, standards have become of key importance for systems interoperability reasons.

Founded in 1993, OASIS now has more than 5,000 participants representing over 600 organisations and individual members in more than 100 countries.

There's more. Other bodies that have addressed biometrics include the BioAPI Consortium, the JavaCard Forum, and the Voice XML Forum.

Why so many standards?

So why are there so many standards in the biometrics industry? Aside from the cost savings that accrue from a standardised industry, largely thanks to the systems integrators that build solutions from individual technology building blocks, there is a clear need for interoperability.

In April 2010, NATO joined the biometrics standards fray with an announcement that the North Atlantic Treaty Organisation is assessing the long-term capabilities of using biometrics technology in operations as diverse as Afghanistan and humanitarian missions to areas hit by a natural tragedy.

Under the NATO plans, the intelligence directorate (J2) of NATO's Supreme Headquarters Allied Powers Europe (SHAPE) operation has created a working group to look at institutionalising the collation of biometrics information like facial, fingerprint and iris scans.

According to Lt Col Tom Pratt, the military operations branch chief at the Biometrics Identity Management Agency (BIMA), the agency formerly known as the DOD Biometrics Task Force (BTF), there is a move to get all NATO member countries sign up to the biometrics standards plan.

The long-term aim of the BIMA-driven NATO standards working group is to develop standards for sharing biometric database information between member countries and their agencies. These are known as NATO Stanags (standardisation agreements).

"You need standards to ensure that newer equipment and systems will work retroactively with previous generations of systems"

The J2 committee, as it is known, generates a wide variety of biometric requirements, including more mundane issues such as ensuring that members of the armed forces receive their inoculations in a timely manner, using biometric identifiers as a fail-safe method of identification.

One of the driving reasons for the J2 committee to develop biometric standards is the current conflict in Afghanistan, where UK forces are progressively pulling out, to leave their US Army colleagues to maintain law and order, alongside the Afghan army.

According to Thomas D'Agostino, standards branch chief with BIMA, since the spring of 2010, when the BTF became BIMA and also became a permanent US government agency one of his agency's key roles has been to develop standards.

"There are basically four main areas of biometrics identity management: warfare, business, intelligence and security/law enforce-

BIMA aims to get all NATO countries to sign up to standards.

ment," he says, adding that, because biometrics is an evolving industry, there is a strong need for standards.

"We need the right standards for the simple reason it's an evolving market. It's evolving and maturing at the same time, meaning that old biometric identifiers, such as fingerprints, are giving way to new biometric technologies, such as DNA," he says.

"And it's also important to realise that the biometrics technology that we are all using is improving significantly. That's why you need standards, to ensure that newer equipment and systems will work retroactively with previous generations of systems," he adds.

Coupled with the fact that biometrics technology can be used in a very wide variety of applications today, D'Agostino points out that there are now different parameters for different applications, with the exacting parameters required in, for example, a military biometrics application, differing greatly to, say, a fingerprint scan system on an personal computer.

Military specs

Does this mean that biometric standards are more rigorous for military applications than for civilian ones? "The core structure that both applications use is quite strong. We all use the ISO standards, but there is always going to a difference between the standard and its implementation," he explains. And, he went on to say, there is also the military specification that the US government in common with all governments imposes on its suppliers, and not just for biometrics technology.

Military specifications, he says, transcend the standards in that they are a requirement for a given piece of military technology. Put simply, this means that the specifications may be a lot tighter for a piece of biometric hardware required for the military than a similar system, which has a civilian application.

BIMA, he went on to say, has around 300 staff at various locations across the US, with just six people working on standards issues, a number that the BIMA standards branch chief says greatly simplifies the task of staff keeping up with each other's activities and the development of standards in the industry. Even so, he told BTT that interoperability is a challenge for the agency, so it's important that they all work together.

Standards jigsaw

So where do the other standards bodies fit into the BIMA element of the standards jigsaw? "We work very closely with our colleagues on the ISO committee. We're very close to the ISO standards people, including the ISO/IEC SC37 committee, and we also work with Interpol, the international police agency, which also has a say in standards in technology," he says.

"In addition, there are the Stanags, the standardisation agreements, that NATO co-ordinates between member countries," he adds.

Stanags, says D'Agostino, are standardisation agreements for procedures and systems plus equipment components. Developed and promulgated by the NATO Standardisation Agency in conjunction with the Conference of National Armaments Directors and a number of other authorities, the Stanags are a crucial set of standards that are used by NATO members to ensure one armed force's set of kit interoperates with that of another member nation.

Whilst there are several NATO Stanags that have integral biometrics specifications, BIMA has been working with NATO since September 2008 on developing a Stanag for biometrics.

According to NATO, BTF officials met with their counterparts from the Joint Capability Group for Intelligence, Surveillance and Reconnaissance (JCGISR) within NATO in September 2009, since when the BTF has been working on three JCGISR technical working groups to ratify the biometrics Stanag.

"Sources close to NATO suggest that agreement on the biometrics Stanag is close"

Although details of the process are classified, sources close to NATO suggest that agreement on the biometrics Stanag is close, with two of the working groups – the human intelligence (Humint) and measurement and signal intelligence (Masint) – having already submitted their recommendations.

If you've read this far and have not been overwhelmed with the acronyms that inhabit the military side of the biometrics standards arena, it's time to ask the question: where do standards fit into the UK side of the biometrics business and the commercial world of the industry?

Thomas D'Agostino: military specs transcend standards.

Whilst standards are clearly important when it comes to UK applications, the main focus of UK standards developments falls squarely on the shoulders of the British Standards Institute (BSI) where the ISO and IEC have established a joint committee for information technology standards known as JTC1. In 2002, the ISO/IEC JTC1 established the SC37 sub committee to develop biometric standards.

According to the BSI, the sub committee consists of six working groups each addressing a specific area of work: harmonised vocabulary, technical interfaces, data interchange formats, biometric profiles, performance testing and reporting and cross-jurisdictional and societal aspects of biometrics

Commercial

The commercial side of standards development is carried out by the BSI IST/44 biometrics standardisation committee. The membership of IST/44 consists of UK government agencies, such as the UK's Ministry of Defence, the Department of Transport and Home Office Scientific Development Branch, and a number of other bodies including the UK's Biometrics Working Group (BWG), ISACA and the British Computer Society, to mention but a few.

About the author

Steve Gold has been a business journalist and technology writer for 26 years. A qualified accountant and former auditor, he has specialised in IT security, business matters, the Internet and communications for most of that time. He is technical editor of Infosecurity and lectures regularly on criminal psychology and cybercrime.