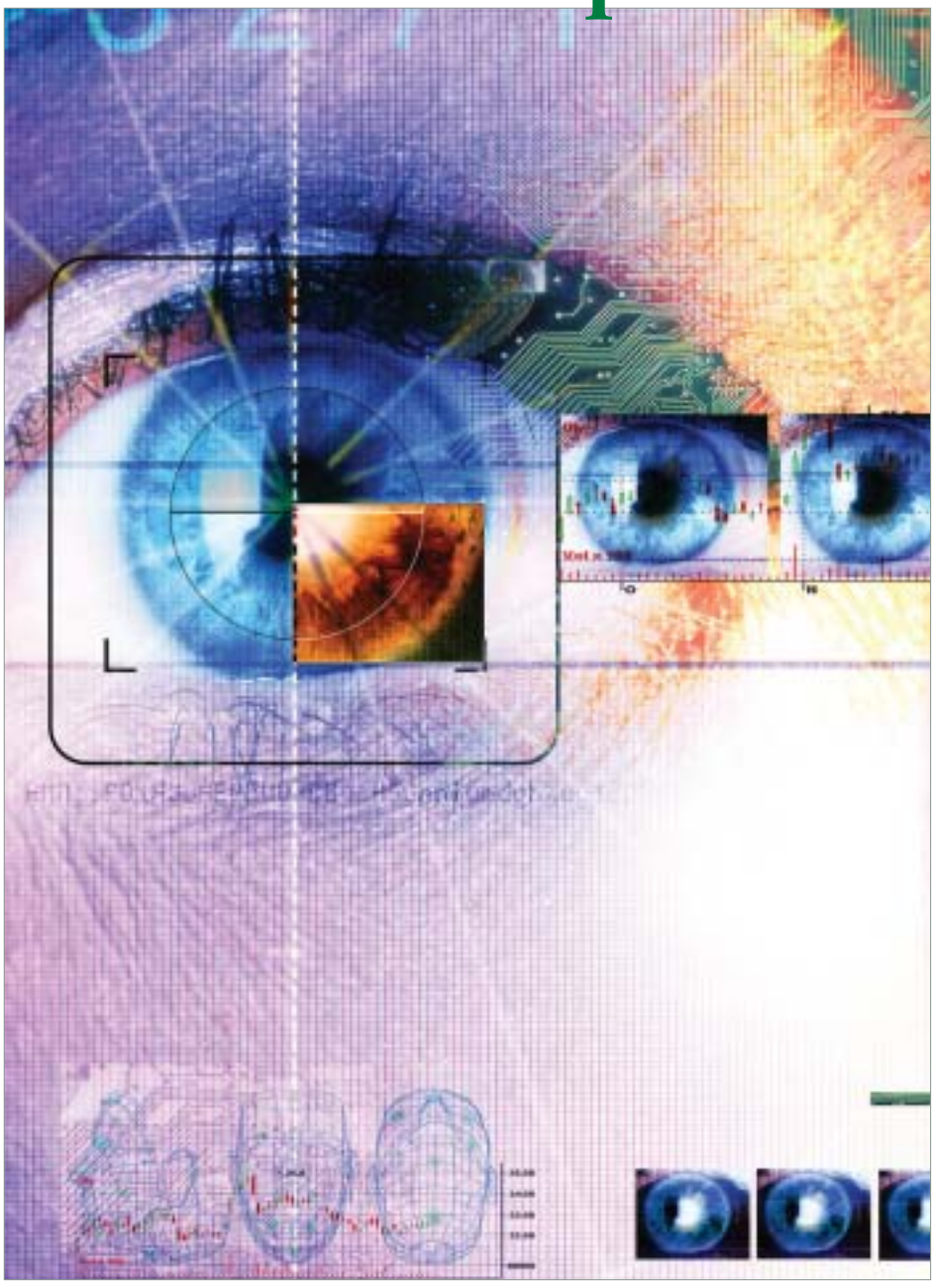
Identity Linkage:
Biometrics and "True Compliance"

By C. Maxine Most



Compliance is about who did what with what data. Identity management can automate and provide audit assistance for much of this process, but it relies on the authentication method used to link an identity to a person. Many types of strong authentication prove only that the person possess the token or knowledge required, and this can be passed to another to use undetectably. Only biometrics prove that an identity matches a person, and compliance significantly elevates the importance of that in enterprise applications.

The biometrics community has generally considered regulatory compliance to be a key enabler of the widespread commercial adoption of biometrics. However, while regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley (Sarbox) include explicit requirements for privacy

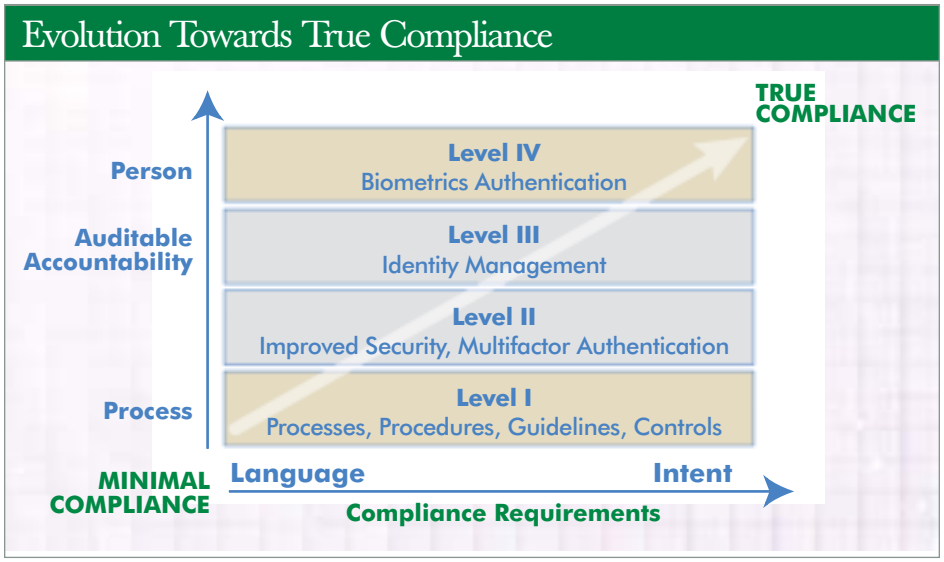
protection, process and data integrity and auditable accountability, they do not explicitly call for the use of biometrics. In fact, many deployed and proposed compliance solutions appear quite committed to steer clear of biometrics altogether.

The outright dismissal of biometrics can be partially attributed to concerns about cost, performance and complexity of implementation. However, is often more a matter of assuming that the use of biometrics is just overkill and therefore unnecessary. While this may seem a reasonable assessment in the near term, this approach may prove short sighted in the long run. Genuine compliance with regulations depends on auditable accountability. This in turn requires non-repudiated identification technology. Biometrics are the only class of technologies capable of providing "true compliance" within the context of establishing non-repudiated identity

Identity Linkage

This linkage between an individual and an electronic process – whether it be completing a health insurance form, entering financial data in a spreadsheet, accessing client files or certifying corporate filings – may seem peripheral to the real work of creating compliant IT systems and networks. However, ultimately it is precisely this identity linkage that ensures the integrity of the entire system.

Unfortunately, this will not be a primary concern until compliance is challenged. At that point the differentiation between simply meeting stated compliance requirements and achieving the actual objectives of compliance may surface with unforeseen and undesirable consequences. It is not enough to know that an individual who possessed the correct password or token accessed a file, completed or certified a transaction or approved mandatory filings; the identity of the individual performing this task must be verified.



Progress – HIPPA & Sarbox

Progress towards biometrics as the defacto identity linkage standard for compliance based applications has along way to go. For the most part, biometrics are still considered an unnecessary fringe technology.

While there are a number of HIPAA deployments that have incorporated biometrics to control physical and logical access at medical facilities, the primary justification for using biometrics is not strong identity linkage. The technology is most often deployed in this environment to enhance convenience for medical professionals or reduce password fatigue and enable single-sign-on (these two are often linked in HIPAA related applications) for hospital administrative and non-medical support staff. So while there has been some use of biometrics in HIPAA solutions, auditable accountability has not been the driving factor. In the healthcare environment far simpler processes, often manual, have been implemented to meet HIPAA compliance rules. This, however, may soon change. Should the Bush administration's call for a healthcare IT overhaul come to fruition, HIPAA compliance would face IT integration challenges similar to those of Sarbox where identity linkage has far reaching implications and "paper pushing" solutions are not enough.

Sarbox compliance is integrally liked with IT operations and therefore ultimately to strong identity linkage. This has led to compelling arguments for identity centric IT models among those addressing Sarbox compliance. The Sarbox Act's Section 404 – Management Assessment of Internal Controls – is to a large extent driving this argument. Section 404 requires mandatory control, security and accountability for sensitive information. It compels companies to identify key business processes, the controls overriding the processes, and any vulnerabilities in these controls. This includes monitoring and auditing access to all financial, confidential, trade secret information and communications with customers, suppliers and partners. As the unwieldiness of meeting Sarbox rules becomes increasingly more evident, identity seems to provide the best, if not the only viable framework for deploying compliant IT infrastructures which leverage use of identity linkage technologies that ensure auditable accountability.

Sarbox Reality

A colleague providing consulting services on a Sarbox implementation for a large real estate developer and finance company (whose contractual relationship requires anonymity) reported the evolution of her own thinking on the implications of identi-

ty and compliance. After spending several months developing and implementing Sarbox compliant processes and control guidelines for her client, she concluded that without a sophisticated identity management system bolstered by biometrics verification, much of her hard work was for naught. The security procedures built into the system were simply not adequate to ensure process and data integrity. Even with added security measures, the lack of robust provisioning, strict access controls and non-repudiated user authentication, prevented genuine compliance objectives from being achieved.

This particular client ended up developing basic identity management functionality in-house. They were unwilling to invest in a major IT overhaul and were severely limited by their existing IBM AS4000 based infrastructure which prevented them from using readily available identity management products.. Instead, they settled on limited improvements in provisioning, access controls and security measures that while technically adequate for compliance will most likely not achieve true Sarbox objectives. Unfortunately, this scenario is fairly representative of the state of Sarbox compliance efforts today.

Estimates from AMR Research put Sarbox compliance expenditures at $5.5 billion for 2004 growing to over $6 billion in 2005. It is disillusioning at best to consider that this level of IT investment is going being made 1) without developing solutions that provide genuine compliance – not just with the language of the regulations but with the true intent of the law, and 2)while failing to provide real IT infrastructure improvements, such as the adoption of identity management frameworks, which enhance core business process, increase flexibility, reduce security risks and liabilities and protect against fraud and corporate malfeasance.

Linking individuals to an identity and linking that identity to access rights, privileges and/or legal accountability will be an essential element for a wide variety of compliance applications.

Biometric Value Add

It is easy to understand how in this context, biometrics technology seems at best insignificant, and at worst irrelevant. Even within the identity management community, little attention has been paid to biometrics. The technology is considered an afterthought, if it is considered at all (for more on this see Digital ID World Magazine, March/April 2004, Collision Course: Biometrics and Rights Management). However, as reported in White Castle Hands Employees Self Service (Digital ID World, January/February 2005), though biometric technology may indeed be irrelevant to the primary drivers and the mechanics of implementing core IT solutions, it sometimes provides a key element that makes the whole solution viable.

In the White Castle example, the company was determined to address a costly and cumbersome employee benefits paperwork process. They wanted to move to electronic forms on a kiosk-based system but faced significant challenges including legally binding signatures. Biometrics were not central to the paperwork reduction process that drove the development of the application, nor was this particular application directly driven by compliance requirements. However, in the end biometrics proved the crucial factor in making the process legally binding, compliant and therefore deployable. The initial application for the benefits kiosk was healthcare enrollment. Without biometrics, the automation of this HIPAA regulated process would not have been possible.

The Relevance of Verifiable Identity

Biometrics may continue to be considered "irrelevant" in the world of compliance for some time to come. However, ultimately, as the larger IT infrastructure issues are resolved , the role of identity as a central organizing principal of compliance efforts becomes mainstream, and the nitty-gritty work of building and challenging deployable solutions commences in earnest, the relevance of biometrics is inevitable.

The linking of individuals to an identity and the linking of that identity to access rights, privileges and/or legal accountability will be an essential element for a wide variety of compliance applications. Whether compliance will be a driving force in the evolution of this linkage or whether it will simply be swept along as part of a greater move towards biometric identification remains to be seen. Either way, however, the need to irrefutably verify and protect identity will make biometric technology not only relevant but ultimately essential to maintaining efficient, secure and trustworthy complaint IT systems. ■

C. Maxine Most is the Principal of Acuity Market Intelligence (www.acuity-mi.com), an emerging technology market consultancy as well as the Editor of the Biometric Market Intelligence eUpdate (www.biometricsmi.com) a free newsletter providing insight and analysis for the biometric industry. Ms. Most may be reached at max@acuity-mi.com.