Ia
INTERNAL AUDITOR

APRIL 2015

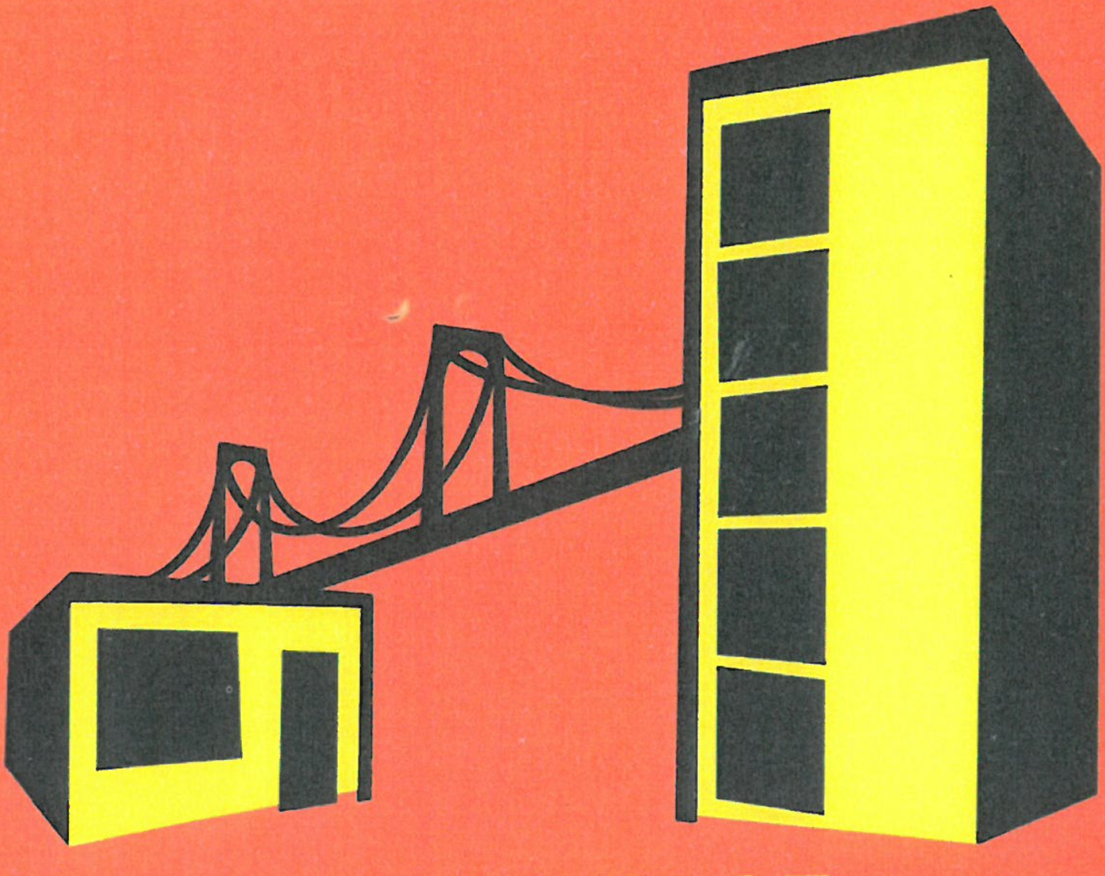
INTERNALAUDITOR.ORG

Deciphering Digital Signatures

Is Your Organization ACA Compliant?

The Internal Auditor as Professional Skeptic

Minimizing Joint Venture Risk



KNOWLEDGE SHARING

Small audit functions can learn a lot about best practices from their larger counterparts, and vice versa.

Digital Signatures Deciphered

Shiva Hullavarad
Russell O'Hare
Ashok Roy

Internal auditors should assess the business processes and risks associated with signing documents digitally.

In today's digital business environment, internal auditors have to assess the risk and security of large volumes of digitally originated transactions and documents. Among the many methods, protocols, and products for securing online transactions are digital signatures. For example, the mortgage industry uses digital signatures for approving real estate negotiations by affixing them to price or contract changes until both parties agree on terms and a price. Once they have reached an agreement, the parties execute the title transfers with a notarized ink signature.

Digital signatures improve efficiency, provide security around transactions, and enhance collective approvals in a fraction of the time compared to conventional ink signatures. Nonetheless, there is always the danger and fear of unauthorized or malicious use of digital signatures. Internal auditors and organizations need to assess the level of risk and to what extent the organization should secure its digital signature platform. Moreover, auditors should consider the trade-off between the level of risk digital signatures pose and the level of authentication required to provide desired levels of assurance while accepting them.

PROOF OF AUTHENTICITY

A digital signature is an electronic sound, symbol, or process attached to or logically associated with a record and executed by a person with the intent to sign the record. In layman's terms, it is a person's electronic expression of agreement to the terms of a particular document with the intent to sign. A scanned or photographed image of a written signature does not constitute a digital signature, as it is analogous to affixing a rubber stamp of the signature that can be duplicated or misused without the signer's knowledge. Instead, digital signatures provide a secure encryption environment for the data associated with a signed document and verify the authenticity of a signed record.

To authorize transactions, digital signatures use a combination of content capture, method of signing, data, and user authentication. They use electronic authentication to establish confidence in user identities that are electronically presented to an information system. Individual authentication is the process of establishing an accepted level of confidence and assurance for an accepted level of risk.

There is a direct relationship between the associated risk and the complexity of authentication needed to provide a higher degree of assurance in the use of digital signatures. Higher levels of assurance need complex, multifactor authentication methods that, in turn, require a secure IT infrastructure and user training. This correlation poses a trade-off challenge to auditors and organizations willing to accept digital signatures, thereby compelling them to identify those business processes that require an optimum level of authentication to offset risks.

Digital signatures are built on an encryption/decryption technology that a) collects evidence of the document such as metadata and IP address, b) verifies the identity of a signer and receiver, and c) provides an audit trail of the transactions. This technology uses a public key infrastructure (PKI)

TO COMMENT on this article, EMAIL the author at shiva.hullavarad@theiia.org

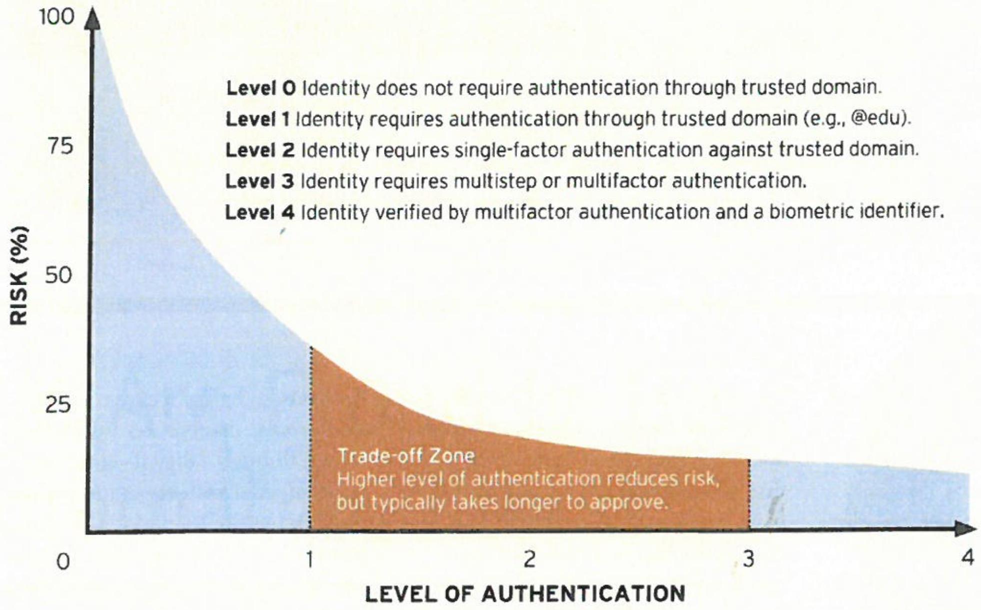
HOW DIGITAL SIGNATURES WORK

Digital signatures use private/public keys and hash results of the original and destination documents. The digital representation or summary of the document unique to a message *origin-hash result* (OHR) is created by the hash function of the digital signature software. In turn, this software uses the signer's *private key* to transform the hash result into a digital signature that is unique to the message. Upon receipt of the document, the transmitted message computes a new *destination-hash result* (DHR) by using the same hash function used to create the digital signature. Using the corresponding *public key* and DHR, the receiving computer confirms whether the affixed digital signature was created using the matching private key and whether both the OHR and DHR match. If both the keys and hash results are a match and confirmed, the validity of the message, signer, and receiver are verified.

81% of digital signature projects achieved return on investment within one year, according to the 2013 Digital Signatures survey by the Association for Information and Image Management.

DIGITAL SIGNATURE RISK TO AUTHENTICATION

The chart below illustrates the digital signature risk-to-authentication model. This model provides a semi-quantitative approach to assess the associated risk for a given level of authentication used to provide a digital signature.



Level 0 Identity does not require authentication through trusted domain.
Level 1 Identity requires authentication through trusted domain (e.g., @edu).
Level 2 Identity requires single-factor authentication against trusted domain.
Level 3 Identity requires multistep or multifactor authentication.
Level 4 Identity verified by multifactor authentication and a biometric identifier.

in which the signer uses his or her private key to encrypt the document and the recipient uses the corresponding public key to decrypt it (see "How Digital Signatures Work" on page 36). A digital signature requires a signer to establish a certificate-based digital ID, commonly enclosed in a token, smart card, or other physical device, to provide a high level of authentication, integrity, and security to the transaction and the identity of the parties signing. The executor or signer is presumed to be legally responsible for any document signed with a private key.

The important consideration when assessing the risk for digital signatures is their provisioning through e-mail communications, which makes Internet security critical. If the e-mail platform is compromised, the digital signature and PKI lose their authenticity and validity.

THE RISK-ASSURANCE TRADE-OFF

"Digital Signature Risk to Authentication" on this page depicts the trajectory for risk tolerance versus level of authentication for a typical business process. The trajectory slope may vary with the nature of the business process. For example, financial transactions, approvals, or decisions generally have a higher degree of risk, based on their monetary value, than administrative functions such as leave requests.

The digital signature risk-to-authentication (SRA) model depicted in the chart provides a framework for internal auditors to establish the desired level of trust for an electronic transaction, as well as the authenticity, integrity, and reliability of such transactions. This can be accomplished through a quantitative risk assessment for each transaction specific to a functional unit by estimating the risk and the likelihood of occurrence. Use of the SRA model can give internal auditors an understanding of internal controls and security needed when their organization implements digital signatures.

The SRA model provides a semi-quantitative approach to assessing the risk associated with a given level of authentication used to provide a digital signature. As a general rule, the higher the level of authentication, the lower the likelihood that an incident, or breach, will occur and the

AUTHENTICATION LEVELS

Authentication focuses on confirming the authenticity of the document and the validity of the signer based on pre-established and verified credentials. This table shows the authentication levels, equivalent electronic modes of authentication, and risk of compromise.

Level	Signer's Identity Verification Description	Electronic method	Risk of compromise
0	Unknown	Unknown domain email, suspicious email domains.	High
1	Requires validation with IT	Organization employee directory generated user ID and password or organization email.	Medium
2	Level 1 + single factor	Organization email + digital signature (PKI).	Low
3	Level 2 + double factor	Organization email + digital signature + workflow.	Lower
4	Level 3 + biometric	Organization email + digital signature + workflow + approver.	Lowest

lower the risk. Although the nature of the risk versus authentication curve may be different for different business processes, the pattern will tend to follow the path of reduced risks for higher authentication. Internal auditors or management can develop a risk chart based on the formula: *Risk (R) = Likelihood of occurrence of event (L) x Magnitude (M).*

To illustrate the formula, assume that one in 30 email accounts are hacked. Based on this assumption, the risk can be calculated by assessing the monetary magnitude of the effect of hacked emails on an organization. The trade-off zone depicted in the chart provides an opportunity window to secure the digital signature environment to achieve the desired level of assurance, thereby enabling organizations to identify those processes that require optimum levels of authentication to offset risks.

The key factor to consider in implementing digital signatures is to identify the level of risk tolerance and the associated risk for a business process. Institutional risks may involve financial, brand-value reputation, and other key administrative communication. Based on the various types of business processes and the level of severity, the assurance levels—which are a combination of authentication and validation—as well as the trust levels must be established by the appropriate business-unit management. To secure an electronically signed document as evidence, auditors should consider the risks associated with the signing process and with the significance of the information. Security must be approached with the objective of managing potential risks and should be weighed against the level of authentication needed to achieve the desired level of risk tolerance (see "Authentication Levels" on this page).

Internal auditors can use this model to assess the risk/assurance needed for digital signatures. Because systems are imperfect, auditors should consider the reliability of the information obtained through the digital signature validation process. For example, they should consider whether digital signatures can enhance internal control over online sales orders by authenticating the validity of customers.

DIGITAL ASSURANCE

As the Internet is an essential tool for transmitting digital signatures, it is necessary to have a secure transmission process that ensures a document signed through a digital signature is not tampered with by a third person and reaches the recipient in the form in which it left the signatory. Organizations also need to determine which business processes are not appropriate for digital signatures, such as creating wills, testamentary results, and certain types of contracts.

Internal auditors and their organizations need to identify the various processes for which they plan to use digital signatures, as well as perform a comprehensive risk assessment of those processes. The digital signature risk to authentication model can help auditors assess the level of authentication suggested for a specific business process to ensure it provides the desired level of assurance.

SHIVA HULLAVARAD, PHD, *is statewide ECM/ERM System Administrator with the University of Alaska System in Fairbanks.*
RUSSELL O'HARE, EDD, CRM, *is chief records officer with the University of Alaska System.*
ASHOK ROY, PHD, CIA, CFSA, CBA, *is vice president for finance and administration with the University of Alaska System.*