INTERVIEW TRANSCRIPT

Digital Documentation: Authenticity and Integrity

Entrust's Jay Schiavo on New Mindset, New Automated Solutions

ENTRUST

iSMG INFORMATION SECURITY MEDIA GROUP

Jay Schiavo

Schiavo is the vice president of products for the Entrust Certificate Solutions product segment, including PKI, public SSL and digital signing. An industry pioneer and global leader in identity-based digital security, he entered the field in 2004 and was integral in developing the technology that enabled an SSL/TLS offering for hosting companies, service providers and other partners. He and his team are now shaping the future vision and strategy of Entrust, making it easy for customers to consume Entrust solutions across the SSL, PKI and digital signing portfolios.

With the explosion of remote business, we are now digitizing many of our documents and processes. **Jay Schiavo** of Entrust explains what new mindset this shift requires and shares advice for organizations currently making the shift.

In an interview with Anna Delaney of Information Security Media, Schiavo discusses:

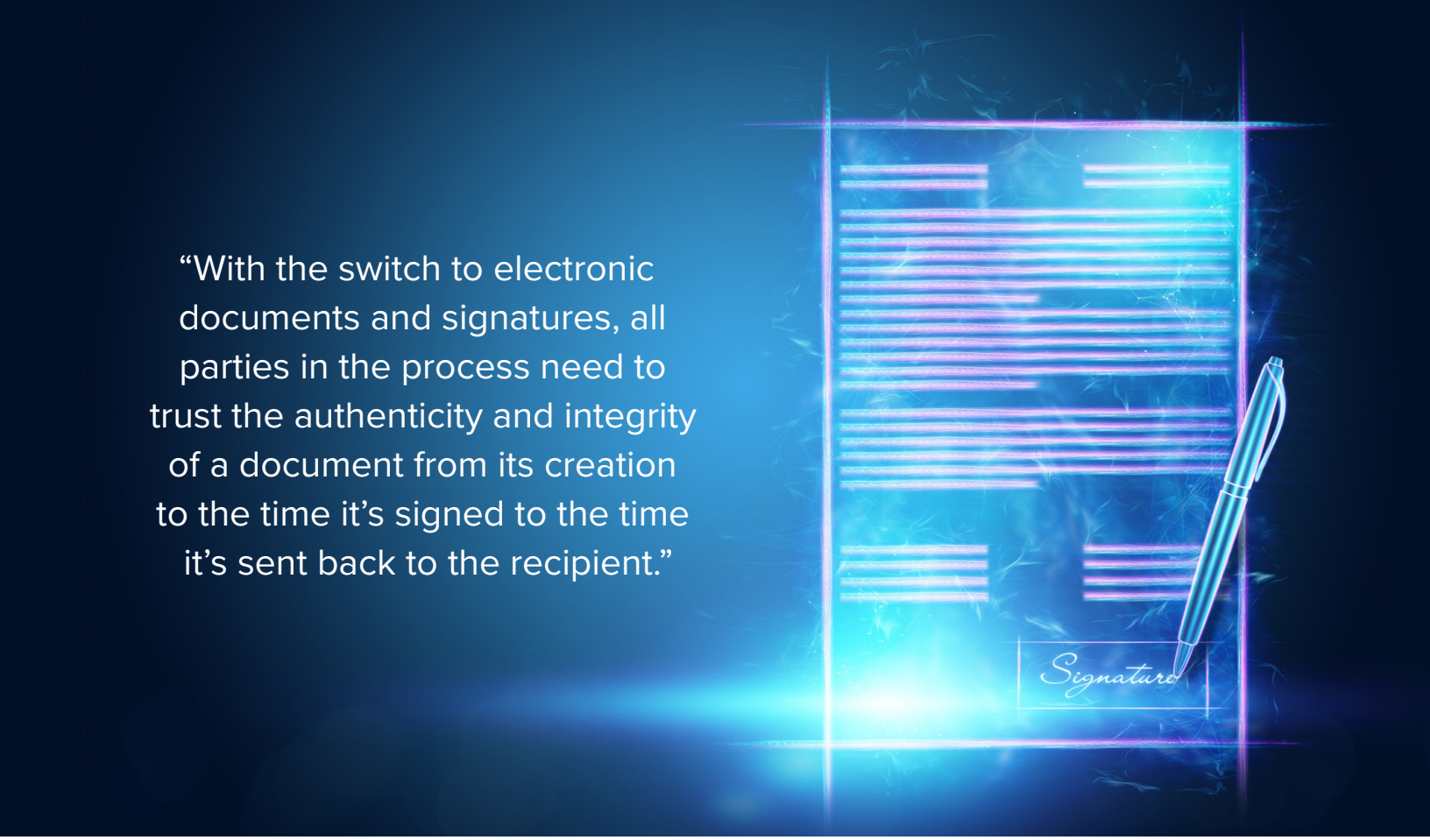
- What's needed to ensure document authenticity and integrity;
- Key pain points for organizations currently making the shift to digitizing documents and processes;
- How Entrust can address these challenges and other security needs.

The Shift to Digital Documents

ANNA DELANEY: With the explosion of remote business, we are digitizing many of our documents and processes. What new mindset does this shift require?

JAY SCHIAVO: There are three areas in which the mindsets of customers and businesses need to shift. The first is trust. In the past, a lot of the signing of legal agreements was done through face-to-face interactions. With the switch to electronic documents and signatures, all parties in the process need to trust the authenticity and integrity of a document from its creation to the time it's signed to the time it's sent back to the recipient.

There is also a technology aspect. The technology used for electronic documents and signatures needs to fit into your business processes and be compatible with other parts of your business.



"With the switch to electronic documents and signatures, all parties in the process need to trust the authenticity and integrity of a document from its creation to the time it's signed to the time it's sent back to the recipient."

The last piece is security: making sure that as you switch from in-person signatures to electronic signatures, you're tracking who signed what, and when; using time stamping; and authenticating signing and audit logs. These all protect the authenticity and integrity of documents.

Ensuring Authenticity and Integrity

DELANEY: What is needed to ensure document authenticity and integrity?

SCHIAVO: There are three levels when it comes to authenticity. First, we want to verify the identity of the person who's signing the document. The signer could be a legal person, which means an organization or business, or a natural person, which means an individual. Second, we want to verify that the signature has not been altered from transmission. That's usually done through a digital certificate, which is issued through a high-assurance process. And third, we want to make sure that when a user gets access to the keys and applies the signature, it's done in a secure way. That's how we prove authenticity.

Integrity involves the digital certificates. An electronic signature is tied to a digital signature, which is typically done through a PKI-based certificate that cryptographically ties the signature to the certificate. Then, any alteration of that document will break the signature on the document. That's how you ensure integrity.

Addressing the Challenges

DELANEY: What are some of the key pain points for organizations currently making this shift?

SCHIAVO: The first point is legal. In most regions of the world, electronic signatures are valid and are accepted as legal forms of documents. But the type of electronic signature that is accepted varies by region. Organizations need to understand which types of signatures are available and valid for each particular use case.

The second point involves technology. Organizations need to have the signing expertise to ensure that the solutions they're using are properly set up and fit into the business processes.

DELANEY: Entrust has a signing automation service. How does it address these pain points?

SCHIAVO: From the legal side, we provide our customers with trusted advisers. Our technical sales engineers, support teams, product teams and experts within the organization research and understand the legal aspects of digital signature. And we have people from different parts of the world as well, who understand the different aspects within their regions. We help our customers understand the laws, requirements and directives that apply to them.

From the technology side, our solution is completely cloud-based and service-based. We host all aspects of the PKI-based digital

signature that's being applied, and make sure that the technology is properly set up and managed and that the keys are accessed in a secured way. We also have a stringent verification process that every legal person and natural person must go through before they can obtain a certificate that can be used to apply the digital signature. We handle all aspects of that for the customer.

> "We host all aspects of the PKI-based digital signature that's being applied and make sure that the technology is properly set up and managed."

Entrust Signing Automation

DELANEY: How does signing automation address specific security and trust needs?

SCHIAVO: Document seals play a critical role in ensuring the integrity of the origin of corporate documents. Some organizations have to sign tens of thousands of documents. Our signing automation service helps ensure that all those documents are generated in an automated way and signed in a certain way, and that the signatures applied are tamper-proof right from their creation dates. That way, once a document is signed, if it gets altered in any way, the digital signature will break. The seals that we embed with the corporate identity also ensure there's a clear way to find out who owns the document, whether it's a legal person or a natural person. We also assign a time stamping service to all digital signatures to help ensure that the content of the document cannot be repudiated.

DELANEY: Beyond the core services, what are some of the business benefits from signing automation?

SCHIAVO: There are benefits in four areas. One, our signing automation service helps organizations keep control and ownership of their IP. Two, it prevents brand damage from document fraud or abuse. More and more documents are being produced, put out in the internet and downloaded from different places. If that content changes into something that is not favorable to a specific business, that could damage the brand or the company's reputation. Digitally signing these documents creates authenticity and integrity and protects the brand. Three, signing automation provides a high level of confidence in the company's assets and therefore allows the company to perform its business in a much more efficient way. Four, it adds flexibility and efficiency to processes such as quoting and invoicing and improves the way different business functions can get agreements signed. ■

Listen to the full interview:
https://www.bankinfosecurity.com/interviews/digital-documentation-authenticity-integrity-i-4836

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG INFORMATION SECURITY MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io