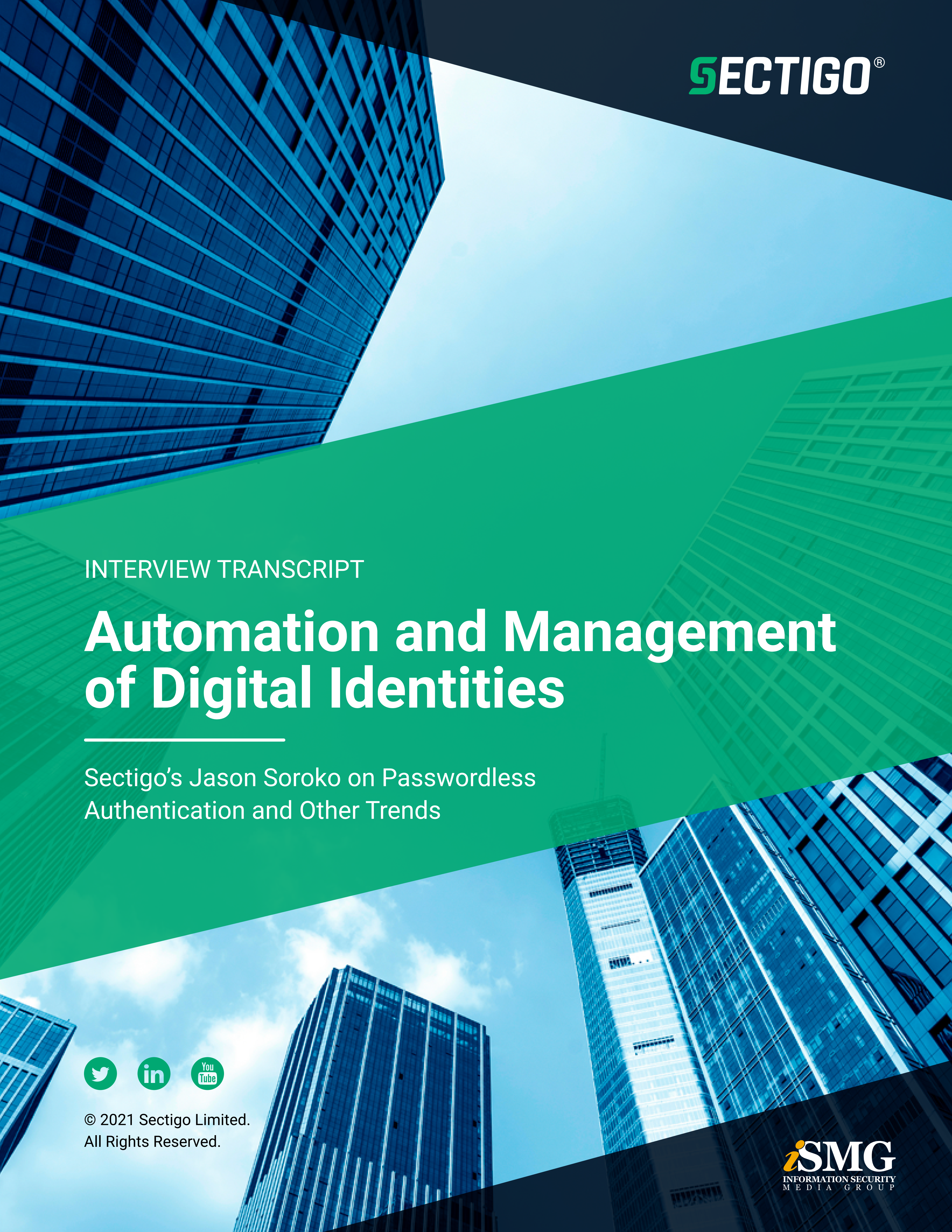

INTERVIEW TRANSCRIPT

Automation and Management of Digital Identities

Sectigo’s Jason Soroko on Passwordless Authentication and Other Trends

Jason Soroko
CTO of PKI, Sectigo

The range of digital identities has evolved into four distinct categories. What role can automation play in managing them? Jason Soroko addresses these and other trends, including the future of passwordless authentication.

In a video interview with Tom Field of Information Security Media Group as part of ISMG's RSA Conference 2021 coverage, Jason Soroko discusses:

- The four categories of digital identities;
- The role of automation in identity management;
- The immediate future of passwordless authentication.

Jason Soroko is an experienced security technology innovator. As CTO of PKI for Sectigo, he is responsible for facing customers, researching, innovating, educating and contributing to strategy, national-level guidance, intellectual property development and consortium standards. He has previous experience in complex data structures and geographic information systems, especially in the fields of climate statistics and spatial mathematics. Jason Soroko worked as an architect and developer of complex data structures and mathematical problems related to GIS systems for the oil and gas industry.

“Passwordless can kill two birds with one stone: It can get rid of the password, which was always a bad idea, and it can solve the provisioning problem of getting the digital identity to where it needs to be.”

The Need for Digital Identity

TOM FIELD: Talk about the range of digital identities and how they’ve evolved into four distinct categories and the nuances that separate them.

JASON SOROKO: Digital identities have really proliferated over the years. Those of you who remember the use cases from the 1990s know that SSL is a term we still use even though that’s been deprecated with TLS. Because of the number of devices, including devices that are held by people or are associated with people, everything needs a digital identity anytime you have to cross a hostile network boundary. And that happens a lot more than it used to because of the cloud and the way that we all interact now. Digital identity provides all that secret sauce that PKI does: encryption of data in transit, encryption of data at rest, authentication and signing. All the standard use cases that are important require digital identities, and it is most helpful to think of them in terms of four distinct categories: server identities, user identities, device identities, and software identities.

Managing Digital Identities With Automation

FIELD: What role does automation play in managing digital identities?

SOROKO: The hardest part of dealing with device categories is getting the digital identity to the actual entity, the node, and then renewing it and automating it. In the SSL use case I talked about earlier, the biggest problem was that, in the past, only a Linux administrator would manually provision that digital identity. Now, you might have dozens or hundreds or thousands of websites, so it has to be automated. In use cases such as IoT, DevOps or any of those machine-type identities, the lifespans of the digital identities are now down to minutes. Therefore, automation is an absolute must.

> ***"Using a strong digital identity and crossing that hostile network boundary in a truly encrypted session with mutual authentication is the key to making life a lot more difficult for attackers. Unfortunately, a lot of heritage, legacy environments are just not there yet."***

The Future of Passwordless Authentication

FIELD: How do you see the future of passwordless authentication coming to bear?

SOROKO: We've been doing certificate-based authentication for users for a very long time; it's not new. We had to come up with passwordless because there's just so much remote work now. There's so much more business-to-consumer activity. Between the pandemic and the need for a digital identity in the hands of your partners and your customers, passwordless can kill two birds with one stone. It can get rid of the password, which was always a bad idea, and it can solve the provisioning problem of getting the digital identity to where it needs to be. Once you're done that, the range of secure use cases you can do becomes a lot greater. Passwordless provides a lot of value.

Digital Identity Management Gaps

FIELD: Where do you see gaps in how organizations are trying to manage digital identities today?

SOROKO: As late as last year, we still saw major outages on web applications because of expired certificates that were manually managed. The legacy of unmanaged certificates is still there, and the management has to be automated.

FIELD: How has the adversary taken advantage of this?

SOROKO: To this day, you read about attacks against passwords, because there are still so many weak forms of authentication. We have deprecated SMS, and we are deprecating some of the weaker forms of the one-time-password type of multifactor authentication methods. The attackers' technology pipeline is much farther ahead than most people think. But using a strong digital identity and crossing that hostile network boundary in a truly encrypted session with mutual authentication is the key to making life a lot more difficult for them. Unfortunately, a lot of heritage, legacy environments are just not there yet.

The Sectigo Approach

FIELD: How is Sectigo helping its customers get a better handle on securing their digital identities?

SOROKO: Because we're a public certificate authority, our customers source a lot of certificates from us, but now they are also concerned about the management of those certificates. We are bringing a lot of open standards to our customers, instead of closed proprietary standards of getting certificates to them. We're not locking customers into things and that's the future. We use open technologies that have been battle-hardened. Customers like to have a lot of options. They're already dealing with a security partner. Why would we want to lock them in any further? We are also future-proofing our customers, for example, with Sectigo Quantum Labs, which helps organizations prepare for the time when quantum computers render existing standard encryption algorithms obsolete. That's going to become important in the next little while. ■

Sectigo is a leading cybersecurity provider of digital identity solutions, including TLS / SSL certificates, DevOps, IoT, and enterprise-grade PKI management, as well as multi-layered web security. As a large global Certificate Authority (CA) with more than 700,000 customers and over 20 years of online trust experience, Sectigo partners with organizations of all sizes to deliver automated public and private PKI solutions to secure web servers and user access, connected devices, and applications. Recognized for its award-winning innovation and best-in-class global customer support, Sectigo has the proven performance needed to secure the digital landscape of today and tomorrow. For more information, visit **www.sectigo.com** and follow **@SectigoHQ**.

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

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

ISMG
INFORMATION SECURITY
MEDIA GROUP

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