Creating a User-Centric Authentication and Identity Platform for the Healthcare Industry

Executive Summary

VASCO
THE AUTHENTICATION COMPANY

iSMG
INFORMATION SECURITY
MEDIA GROUP

In this document

Introduction

Healthcare is in the middle of a major evolution toward digital, personalized medicine and the empowered patient. Ongoing regulatory and monetary incentive programs are driving healthcare providers to increase their EHR and E-Prescribing adoption.

This digital transformation requires a shift in thinking; from “supposedly known users” to “secure and trusted identities.” With many organizations including HIMSS, AHIMA and CHIME calling for a nationwide unique patient identifier with support from the National Strategy for Trusted Identities in Cyberspace’s (NSTIC), a trusted digital identity will likely soon be on your IT agenda.

A recent ISMG webcast took a fresh perspective on digital identity in healthcare and how it can serve healthcare institutions to better satisfy myriad state and federal regulations while deploying a unique, reusable and trusted digital patient credential that provides interoperability and securely links multiple identity providers, different healthcare networks, various payers, and other relying parties via a trust framework.

What is Driving Change in ID Management in Healthcare?

Our Healthcare System is under Attack

According to Michael Magrath, Director of Business Development at VASCO, the healthcare system is increasingly under attack from:

Ransomware. When hackers encrypt a user's files, and then send a message demanding payment — usually in Bitcoin — or the user's files will remain locked.

Keyloggers. The action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored.

Trojan. A packet/software that unleashes damaging code into the computer.

Leapfrog attack. Use of user id and password information obtained illicitly from one host to compromise another host.

Mockingbird. Software that intercepts communications between users and hosts and provides system-like responses to the users while saving their responses (especially account IDs and passwords).

Social Engineering. Tricking people into revealing passwords or other information that compromises a target system's security.

Michael Magrath is a nationally recognized leader in field of healthcare identity management.

Currently, he is Chairman of the HIMSS Identity Management Task Force.

Prior to joining VASCO, Michael served as Director for Identity Solutions for DrFirst and focused on streamlining and securing the identity management process for healthcare providers nationwide and increasing the adoption of electronically prescribing controlled substances (EPCS).

Before DrFirst, Mike lead Gemalto's market and business development activities in the U.S. government and healthcare markets was a contributing member of the Health Record Banking Alliance, WEDI, HIMSS, the Medical Identity Fraud Alliance and the Secure ID Coalition.

He served as Chairman of the Smart Card Alliance's Health & Human Services Council from 2010-2014 where he led initiatives to stimulate the understanding, adoption, use and widespread application of smart card technology in healthcare. He served as an advisor to the American Medical Association supporting a CDC grant to develop and test the viability of a "Health Security Card" to identify and expeditiously treat victims in the event of a disaster.

Mike is also an active member of the IDESG's Healthcare Committee and the Health Record Banking Alliance.

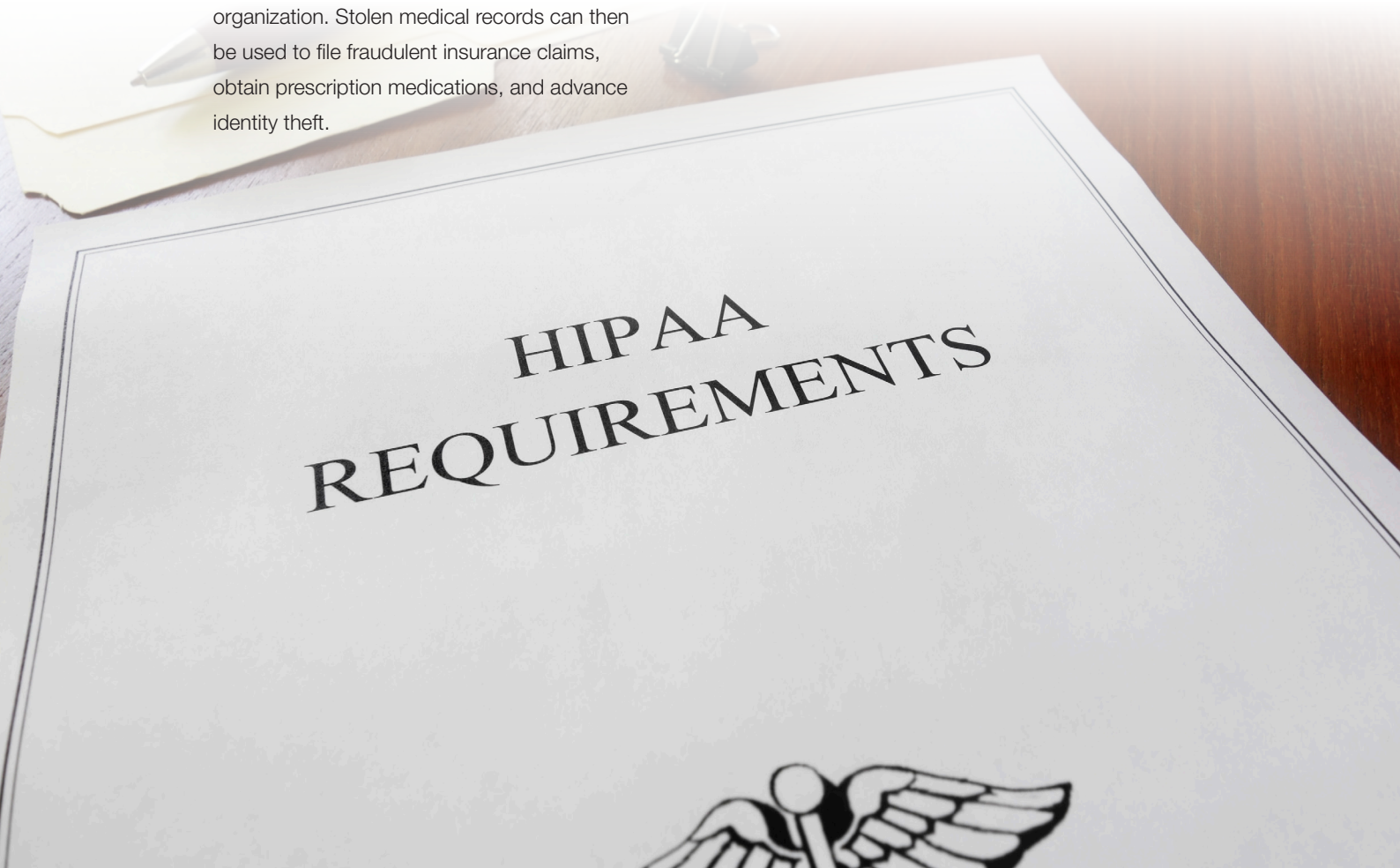
Protecting Health Information: Known users vs. Bad actors

Do you know who is accessing Protected Health Information (PHI) on your network? Is it really the physician, the nurse, the medical staff, the patient or bad actors compromising the hospital's login credentials roaming your network, installing ransomware, viruses, stealing PHI and more? The plain truth is that username and static passwords are no longer sufficient to protect PHI.

Ponemon Institute's 2015 Cost of a Data Breach study determined that a breach in healthcare is by far the most expensive of any industry. At an average of $398 per exposed personally identifiable record, almost any data breach can significantly impact your organization. Stolen medical records can then be used to file fraudulent insurance claims, obtain prescription medications, and advance identity theft.

The HIPAA Audit and the Gamble of Weak Authentication

The United States Department of Health and Human Services Office of Civil Rights (OCR) has begun the process of contacting covered entities and business associates for Phase 2 of the HIPAA Audits. If you have received an email or letter from the OCR and your users are still accessing your network with a username and static password, you are rolling the dice. Further, ONC states that two factor authentication (2FA) is an acceptable method to provide security to ePHI.



Current Initiatives Driving Change in Healthcare

There is a currently a broad range of federally and state mandated regulatory compliance initiatives developing, designed to promote security throughout the institutional and patient security lifecycle via robust identity management programs. These include:

DEA's Final Rule for EPCS. Requires identity proofing (NIST Level 3) and two-factor authentication (FIPS compliant) to be used when electronically prescribing controlled substances where only paper prescriptions were previously required.

I-STOP LAW. New York's Internet System for Tracking Over-Prescribing (or I-STOP) Law, requires all providers to check state prescription drug monitoring program prior to writing a controlled substance prescription. Additionally, it also requires all prescriptions (controlled and non-controlled) be sent electronically; paper is no longer permitted.

White House's Cybersecurity National Action Plan (CNAP). CNAP empowers Americans to secure their online accounts by moving beyond passwords and adding an extra layer of security to protect them in an increasingly digital world.

White House's Precision Medicine Initiative (PMI). Research cohort that will engage a million or more Americans who volunteer to contribute their health data over many years to improve health outcomes, fuel the development of new treatments for disease, and catalyze a new era of data-based and more precise preventive care and medical treatment. Securing patient data is a high priority for the PMI which is utilizing the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, including:

1. **Identity Proofing.** Organizations should develop a policy for verifying the identity of users and contributors (e.g., participants and healthcare provider organizations), prior to granting credentials for access to or contribution of PMI data.
2. **Credentials.** PMI organizations should use innovative approaches for authentication so they do not rely on username and password alone, and should use strong multi-factor authentication for users of PMI data.
3. **Authentication.** Risk-based authentication controls should flow from the PMI organization's security risk assessment, and should be commensurate with the type of data, level of sensitivity of the information, and user type.
4. **Authorization.** Authorization controls should be granular enough to support participant consent that has been captured by the PMI organization and should limit access, use, or disclosure based on what is necessary to satisfy a particular purpose or carry out a function.

ONC's Shared Nationwide Interoperability Roadmap

To advance interoperability of the exchange electronic health information the Office of the National Coordinator for Health Information Technology (ONC) published a shared nationwide interoperability roadmap. This includes specific milestones, calls to action and commitments which include identity proofing and authentication best practices to verify the identity of all participants including providers, staff and patients.

National Strategy for Trusted Identities in Cyberspace (NSTIC)

NSTIC has developed a series of standards needed to secure healthcare information, especially in cyberspace. These efforts to promote consumer identity standards in healthcare will benefit both consumers and providers.

HIMSS Identity Management Task Force

The Healthcare Information and Management Systems Society (HIMSS) has initiated guidelines to protect electronic access by patients to their own protected health information. These guidelines state that such information must be capable of employing user identity proofing and authentication at a high level of confidence, greater than or equal to NIST Level of Assurance (LoA) 3 or equivalent.

Trusted Digital Identities as Foundation for Interoperability

Bridging the Gap in Healthcare Compliance

Andrew Showstead, Director of Technical Consultancy and Market Solutions at VASCO believes that narrowing the gap between ongoing healthcare compliance with new regulations including I-STOP enables healthcare as well as technology providers to better align with the ONC shared interoperability roadmap resulting in solutions that are secure, resilient, cost effective and easy to use. This includes, significantly, developing online digital identities for physicians and patients alike and consisting of the following typical data attributes:

- Username and password
- Online search activities, like electronic transactions
- Date of birth
- Social security number
- Medical history
- Purchasing history or behavior

To foster this outcome, VASCO experts recommend examining the entire ecosystem associated with managing online identities: from the initial identity proofing of a patient or physician to the ongoing security of the channel they're using to interact with their health records or patient data.

As a result, providers can no longer rely simply on a password only. They need to combine them with other factors, such as a card, a key or a token. Or even biometric measures like fingerprints, iris scans or facial recognition.

Andrew Showstead
Director of Technical Consultancy and Market Solutions
VASCO Data Security

Andrew Showstead is the Director of Technical Consultancy and Market Solutions at VASCO. In this role, Andrew oversees engineering and product implementation aspects of multi-factor authentication and application security projects for large enterprise clients in North America. While at VASCO, Andrew has been leading a cross functional team tasked with developing cutting edge security solutions for evolving markets. Currently, Andrew and his team focus on creating a trusted digital identity ecosystem for financial, healthcare and government sectors.

Andrew comes back to VASCO after serving as a Chief Technology Officer for nJuvo Inc. where he led the development of an Internet security product for payment fraud prevention.

Andrew holds a B.S. in Electrical Engineering from Purdue University ('95). He brings over 20 years of experience in engineering and product development from Eastman Kodak, Creo Inc., nJuvo and other technology companies. His research interests include identity federation and the use of embedded technologies to simplify security.

How to Get It Done

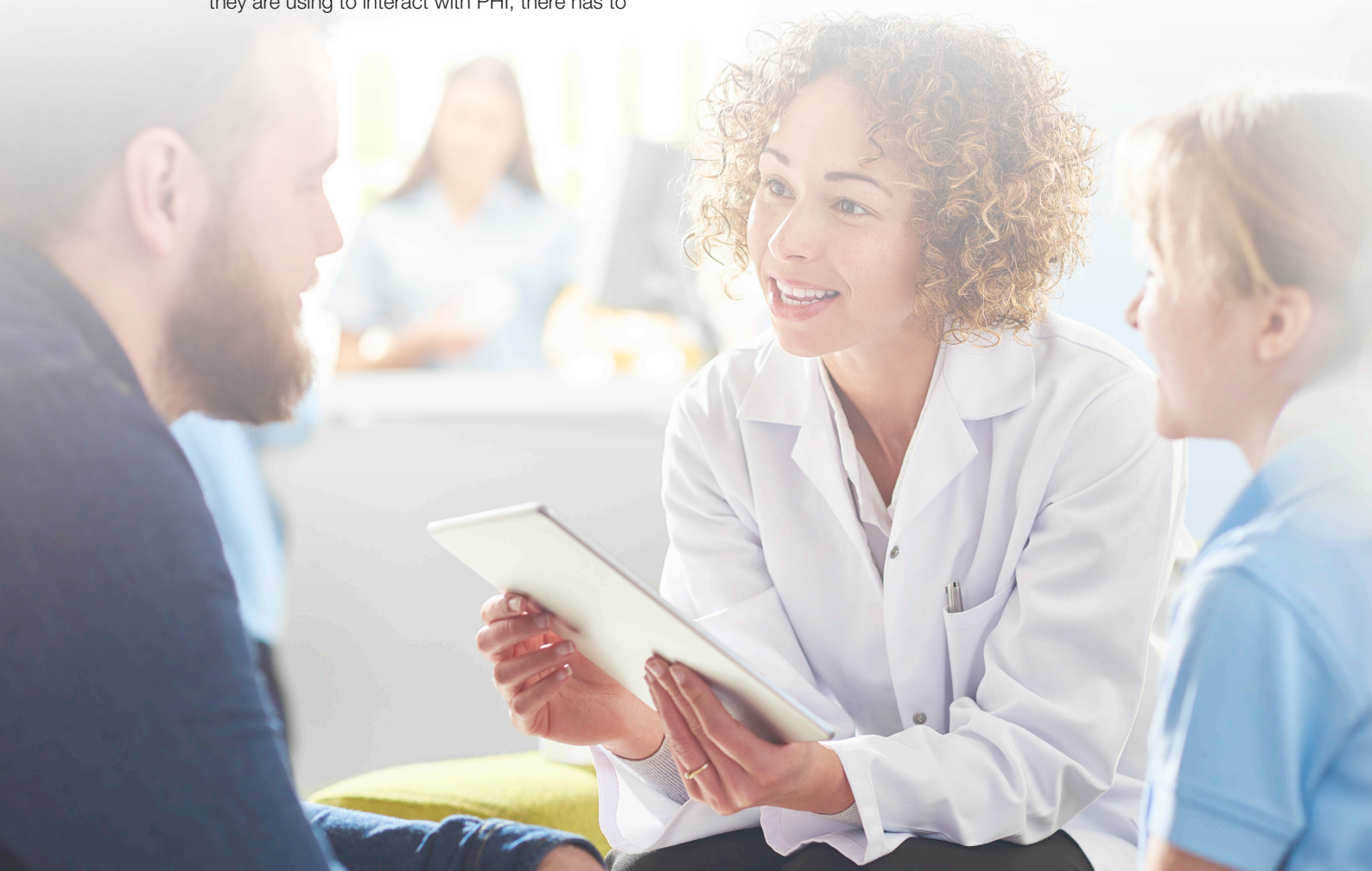
Technological Advancements Behind Digital Trust

"When considering the concept of digital trust, one cannot simply rely on a [single] technology to make it work. We must look at the entire ecosystem of technologies and products involved in the lifecycle of a secure digital identity," says Andrew Showstead, Director of Technical Consultancy and Market Solutions at VASCO.

From initial onboarding and identity proofing for doctors and patients, to the security of channel they are using to interact with PHI, there has to be an established and continuous trust. The key term here is "ongoing." We need have ongoing positive identification, ongoing positive authentication and a continuous process behind the scenes where we can monitor risk and behavior on an ongoing basis.

Achieving trust occurs throughout an end-to-end solution, comprised of the following elements:

- identity proofing
- multi-factor authentication
- mobile application security
- fraud prevention
- ongoing monitoring



Seven Steps to Achieving Digital Trust in Healthcare

The steps below outline how to achieve digital trust for the entire healthcare organization.

1 Easy onboarding

Trust starts with the proofing and validation of the person. Ask yourself: are you absolutely and unconditionally certain your user is who you think it is? How do you distinguish this user? By their user name? By application type? The transition of trust (ID proofing) credentials has implied value between users as well as systems and forms the basis of delivering a resilient online identity. Limit impact on end users and physicians alike by delivering a high level of assurance you are proofing the right user.

Solution: MYDIGIPASS for Healthcare – a FICAM Certified Identity Proofing Service offers easy onboarding through self-service portal.

2 Compliant identity proofing

For compliance purposes, always rely on the ID proofing method. For instance, in some cases it will be enough to require a user to answer a series of knowledge based questions. But, in other cases, you may want to use a live video conference session to ensure and confirm the user's credentials.

Solution: VASCO offers several methods of remote ID proofing for patients and physicians through its MYDIGIPASS for Healthcare Service including KBA or live video call

3

Secure Provisioning of a Secure Credential

Once the user has been identified, a secure credential (hardware or software token, mobile token, other secure credentials that can be later used for authentication) can be provisioned, but only to a secure device. This secure device can come in a form of an out-of-band (unconnected and encrypted hardware authenticator or token) or in a form of an encrypted and securely provisioned app to a mobile device for which a user is already in possession.

Solution: VASCO's MYDIGIPAS for Healthcare offers a secure, automated provisioning process for mobile and hardware credentials, as well as fully integrated inventory management, logistical support and delivery of hardware credentials (tokens) to patients and physicians.

What is a Secure Credential? A credential is a "document or certificate proving a person's identity or qualifications." In case of multi-factor authentication, a Secure Credential constitutes a hardware authenticator (one-time password token), a USB token, a soft token installed on a mobile device in a secure fashion, that is not compromised or altered during installation, cannot be copied or replicated, a process that ensures it is secure is called secure provisioning.

What is cross-channel multi-factor authentication? A simple push button hardware authenticator or token can qualify as a cross-channel authentication device. It is also compliant with all existing DEA and NSTIC regulations on identity proofing and authentication. Such devices can be used in the same fashion to positively identify a user in each of the following scenarios:

- PC or laptop at the office or at home
- Mobile phone or tablet anywhere
- Phone conversation

4

Delivering trust to the device

Before delivering the credential to the mobile device we must ensure the device is healthy (not jailbroken, hasn't been rooted, has no malicious processes running on it). Once this health check is passed, you can then build trust in the device by binding that device to the user.

Solution: VASCO DIGIPASS for APPS checks the mobile device for multiple vulnerabilities such as jailbreak, rooting, malware, geolocation check, and also binds a mobile device to a specific user to avoid device cloning. We want to make sure the entire communication is secure. The protocol in use needs to include encryption. The actual mobile device, now trusted, can then be checked on throughout the lifecycle of the mobile app.

When we know it's a healthy device we can establish a secure communication channel between the device and the user ensuring that the credential obtained during the ID proofing process is secure on that device at all times. This is called binding.

5

Delivering trust to the application

Once you ensure your device is secure, it is now time to do a health check on your application to prevent hacker attacks on your specific apps, or delivering malicious apps to your users through an update. That malicious application can harvest information about the credential and the user that you just worked so hard to secure.

Solution: VASCO DIGIPASS for APPS includes a technology named RASP (runtime application self-protection) that helps prevent screen scraping, debugging, and other malicious attacks on mobile apps. With that, you then have a trusted device, as well as a trusted application bound to that user.

6

Allowing the trust to continue

Once we have established trust all the way from user identification through health checks performed on the mobile device (or secured hardware authenticator) and the mobile app with a secure communication channel, we need to make sure we maintain this continuity. Continuously checking user authentication and to foster an ongoing process to positively authenticate a user sustains ongoing trust.

Solution: User authentication can come in many forms and flavors, based on the previous intelligence data coming from the user device, mobile app, behavior, geolocation and other factors. High risk login requests may require a positive user authentication via a hardware token, or mobile authenticator every time; but login requests that have low risk (haven't been flagged by the system) will pass through frictionless user authentication running in the background. With that, you have a continuous level of trust while maintaining a positive user experience.

7

Delivering frictionless security to the user

Establishing digital trust allows healthcare organizations to open more doors to patients and physicians alike making their online and mobile experience easier.

Solution: Multiple delivery channels can be used for better user experience.

- **QR codes.** VASCO offer frictionless access to a healthcare portal using trusted digital identity bound to a mobile device. A QR code based authentication solution limits the amount of data a user needs to enter during login. All they need to do is to scan a QR code, and they are logged in.
- **Bluetooth.** You don't need to sacrifice mobility for compliance. A Bluetooth based authentication device will communicate securely with a mobile phone and a PC.
- **Secure "PUSH."** When a user tries to access a web site, they receive a notification on their mobile phone asking if they want to login and authenticate to that web site. All they need to do is to login to their device and their healthcare provider app and confirm that request. Unlike with other similar implementations of mobile push, the true multi-factor authentication happens behind the scenes using established and trusted digital credentials bound to a specific user and their specific mobile phone.
- **Facial Biometrics.** This method significantly enhances user convenience without sacrificing security. Users can walk up to a kiosk or pull out their mobile device, perform a quick visual authentication and log in.

Looking into the Future

Federated Identity in Healthcare

The question frequently asked by healthcare organizations is “Can we use established user authentication processes in more than one location not connected by a common IT network or infrastructure and often between separate entities and healthcare networks?” Federated identity is one of the answers that will help healthcare organizations to have easier access to information and start them on the road to interoperability.

What is federated identity?

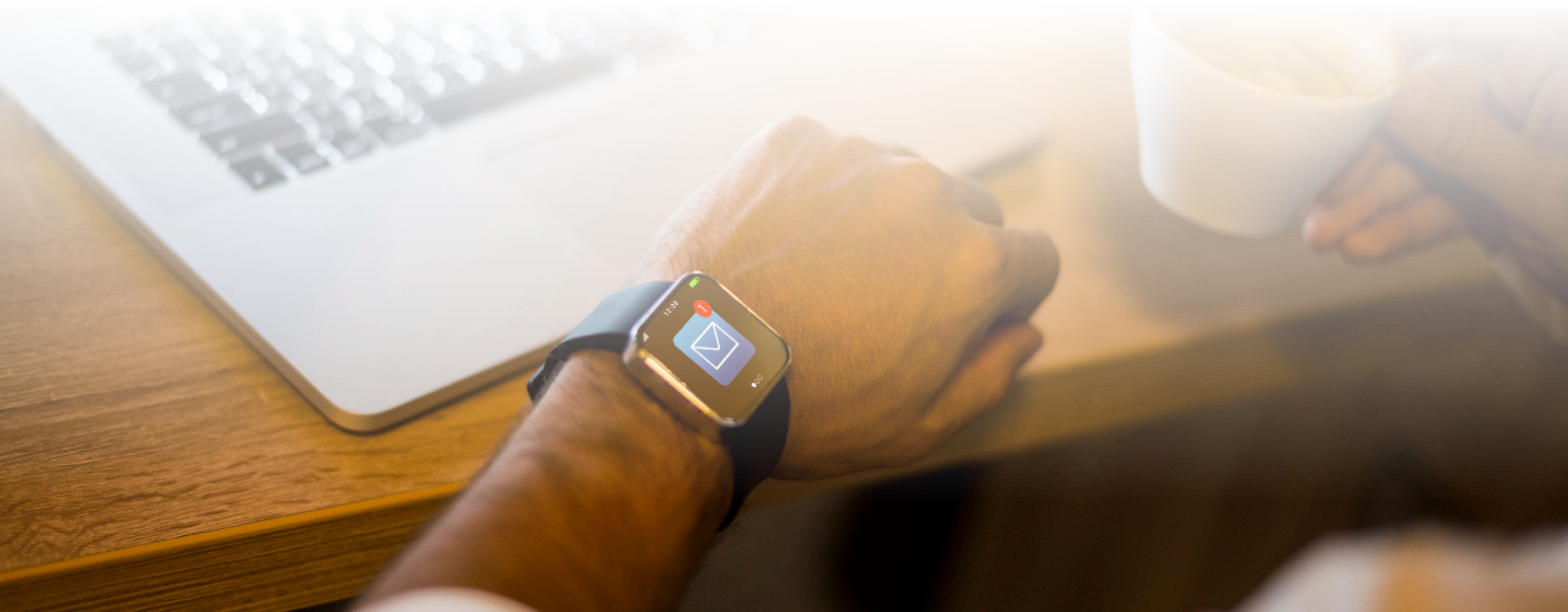
It is the ability to trust ID proofing and authentication provided by other entities, and then leverage it elsewhere. This is a centralized and distributed identity system at the same time. You have an established trust between identity providers so multiple service providers can leverage that bound credential and get attributes from users requesting authentication. “As a result, your healthcare organization can have the benefits of established digital trust for a specific user (e.g. physician or patient) without having to go through the ID proofing and authentication of that person yourself, thus reducing the burden on your IT department”, says Andrew Showstead at VASCO.

Wearables

Many future-looking initiatives are focused around using wearable technology for frictionless authentication. These include leveraging health risk bands as second factors of authentication. VASCO is also seeing the convergence of biometrics and speech to text technology where, for example, if/when you need a prescription, it is displayed on your device, you read it out loud and then, in a single step, positively authenticate your identity.

Conclusion: The Identity Lifecycle

By thinking of a digital identity in terms of an entire lifecycle, said Mr. Showstead, VASCO delivers a usable, resilient and secure solution for ongoing compliance that not only satisfies today’s regulatory requirements, but also anticipates future organizational outcomes.



About VASCO

VASCO is the world leader in providing two-factor authentication and digital signature solutions to financial institutions. More than half of the Top 100 global banks rely on VASCO solutions to enhance security, protect mobile applications and meet regulatory requirements. VASCO also secures access to data and applications in the cloud, and provides tools for application developers to easily integrate security functions into their web-based and mobile applications. VASCO enables more than 10,000 customers in 100 countries to secure access, manage identities, verify transactions, and protect assets across financial, enterprise, E-commerce, government and healthcare markets.

Learn more about VASCO at www.vasco.com or visit blog.vasco.com

About iSMG

ISMG is the largest media company solely focused on Information Security, Risk Management, Fraud, Compliance and other related topics. The firm's footprint and the subscriber-base extends from the North American markets to Europe, Asia and Australia.

Learn more about iSMG at www.ismgcorp.com

VASCO®
THE AUTHENTICATION COMPANY