Journey

Journey's View Of The Future of Secure Trusted Digital Identity

Zero Knowledge, Ephemerality, and Encryption

Privacy, Security and Customer Experience Shouldn't Be Mutually Exclusive

Because the internet was built with no identity layer, the race has been on for decades to provide secure communications between individuals and governments, corporations, and other individuals. There are literally hundreds of companies who have jumped into this space in one way or another, but all of them involve a tradeoff between high security, protection of privacy or a fast, elegant customer experience.

The standard has been, as everyone knows first-hand, knowledge-based authentication (KBA). Over 90% of companies still use this methodology - in fact, it is hard to think of any company that we have interacted with that doesn't lean on username, password, silly "security" questions, or in some cases, dynamic KBA based on information from credit reports. The Equifax breach of complete credit reports of half the population of the US shows just how inadequate even dynamic KBA is. Oh, and it's very costly for companies to use. So KBA doesn't cut it.

Biometrics are emerging as a more secure way to connect an identity digitally to the rightful individual, but it really depends on how biometrics are deployed. Voice biometrics are only 92% effective (and are also extremely expensive and take up to 2 years to implement), and some facial recognition software is insufficient, especially for certain races or ethnicities.

Meanwhile, reports of data breaches and global attacks have remained headline news. Every breach out there has compounded the problem. With security being a top priority for everyone, whether you're concerned about

Journey Proprietary - All Rights Reserved

your own identity or responsible for the protection of your customers or citizens, we need something better. Something that provides a high degree of security, privacy, and an easy, foolproof, and fast user experience.

Many security experts within companies and governments have decided that they cannot trust others to secure their most critical information and conversations. They break IT governance rules by setting up their own email servers to reliably manage what is retained and for how long. This is a bigger problem than many would think - it's common in the public domain as well as in companies, and frankly that is worrisome.

Okay, So What's the Answer?

In short, we need a new way of tackling the problem, and thanks to the advent of powerful sensors in laptops and mobile devices, and advancement of key cryptographic innovations, there is a solution.

Journey, a trusted digital identity company, has developed an award-winning and patent-pending solution that consists of ephemerality, encryption, and the "zero knowledge proof"; therefore enabling a high degree of both security and personal privacy. It leverages the smartphone or laptop to layer several types of identification modalities, but is so fast and easy to use that customers can verify their identity for even the most sensitive transactions in moments.

Zero Knowledge - Journey has built a network based on the cryptographic technique called the zero knowledge proof, which enables the customer to prove who they are without divulging the actual Personally Identifiable information (PII) to the agent. Our Zero Knowledge Network verifies that proof points are accurate, but doesn't actually show them to the agent.

Ephemerality

Centrally managed customer databases, email and messaging systems should be avoided until IT organizations can truly protect data and provide privacy. It matters who touches customer/citizen data, where it resides, and how long it lives. To this end, individuals, governments and corporations will increasingly turn to ephemeral communications as a critical data protection mechanism because the data that isn't stored in a "honeypot" cannot be compromised.

Journey Proprietary - All Rights Reserved

This is why ephemeral communications between individuals have become so popular, but enterprises would do well to adopt identity solutions that enable ephemerality to protect customer data as well.

Encryption

Journey individually encrypts each session with an individual, making it much better at thwarting insider or synthetic fraud attacks.

The Four Underpinnings of Journey's Secure Identity Solution

1. **Privacy**: We are committed to building solutions in a way that ensures that no third party, including Journey, has access to user data. Many companies in this space monetize their data, selling it to 3rd parties for marketing purposes... or other uses that the individual might object to. Journey is fundamentally against this and has architected a solution that provides personal privacy and builds trust.
2. **Transparency**: Journey will continue to operate with full transparency about our product security, user privacy, and public policies. We are committed to strengthening the ongoing collaboration with our user community and more broadly with our network of security and privacy practitioners.
3. **Security Innovation:** User needs will always be at the core of our engineering and design efforts focused on perfecting products and protocols against emerging risks. Our use of the most secure methods of biometrics, IDs and credentials, liveness detection and other inputs meets the most stringent security standards.
4. **Seamless Customer Experience:** It should be fast and easy to prove your identity digitally. This has obvious implications for the customers themselves, but it also provides profound benefits of cost, risk, efficiency and CSAT for the business or entity needing to verify identity for any number of interactions.

The new frontier for proving digital identity is here. There is no need to risk the privacy, security or experience of your customers, or to expose yourself to the notoriety of a breach.

To learn more or schedule a demo, visit us at www.journey.ai

Journey Proprietary - All Rights Reserved