Digital Identity

Kim Maida, Previously Head of Developer Relations at Auth0
Roger Tipping, VP of Client Success at BrieBug

What is “digital identity”?

Identifying users and authorizing access to resources. The digital identity of a user is dependent on the context of an application.

Digital identity includes:

- Authentication
- Authorization
- Access management
- User management

Managing identity is complex

"You don't know what you don't know"

Misinformation about authentication can lead to serious consequences in applications.

- Current web resources are not sufficient to teach developers to implement authorization safely, securely, effectively, and efficiently.
- Distinguishing correct, up-to-date information and best practices is not easy without a background in identity, even for experienced developers.

If implemented incorrectly

Failure to follow best practices when developing digital identity can be catastrophic to an organization.

- Data breaches - Jeopardizes an organization's credibility and the trust of their customers.
- Waste of time - Time is spent trying to understand identity's nuances without minimizing risk of critical errors due to misinformation.
- Uncertainty - Teams are not confident about following best practices. Disagreements may arise as to how to implement authentication.

Using Identity as a Service (“IDaaS”)

Trusting in an identity service to implement authentication ensures:

- Reduces risk - Stays up to date on best practices to ensure security
- Out of the box - Powerful and adaptive feature set for any application
- Scalability - Add new features easily as users scale from 100 to 100,000
- User experience - Experts focus on building quality and reliable identity
- Time savings - Developers focus on other key parts of the application while experts take care of identity

TRANSLATING TECHNOBABBLE

TRANSLATINGTECHNOBABBLE.COM