IoT Identity Management: Build Better Connected Products and Services Into Your Ecosystem

Manage Trusted Relationships Among People, Services, And Things For Scalable Digital Transformation

Introduction

The Internet of Things (IoT) is reshaping almost every industry, from manufacturing and transportation to home automation, telecommunications, and healthcare. By connecting devices with systems, data, and people, businesses can introduce more personalized, automated, and enhanced experiences for their customers. In fact, many emerging business models will drive more revenue through IoT-enabled services than the products through which they're delivered.

The move to IoT involves more than simply adding connectivity to devices. A 'thing' can also be a service, system, application, data source — any thing that interacts with a human operator or organization. These things communicate via cloud, mobile, social, and legacy platforms to request or provide information, send commands, and help manage complex automated processes. As the web of connectivity grows more extensive and complex, critical questions emerge: how will we manage access to all these things and the information they hold? How will we control which people or devices are allowed to do what, with what? And how will we secure the ecosystem as a whole? The time to answer these questions is at the start of your IoT transformation—before growing scale and complexity make them exponentially more challenging to address.

Identity management makes it possible to manage and protect IoT ecosystems at enterprise scale. Providing an essential layer of granular access control and trust, identity management lets companies manage permissions and build trusted relationships among parties including people, services, and things. This includes who and what they can access and communicate with, what commands they're authorized to give, and what data they're authorized to access. By identifying things in their context, identity management also helps organizations more effectively manage, maintain, and extend their IoT ecosystem.

This white paper looks at the essential role and requirements for identity management in IoT.

The Booming IoT Puts The Spotlight On Scalability

The IoT market is growing rapidly, reflecting its central role in digital transformation. Disruptive B2C business models such as connected vehicles, telehealth, wearable technology, smart homes, and smart grids depend on IoT technologies, as do B2B models such as smart manufacturing, smart lighting, and next-generation fleet management.

As the IoT ecosystem diversifies to include more devices, applications, services, and people, the complexity of access itself has increased as well, encompassing:

» Systems such as an event data recorder, motor engine controller, or simple sensors

» Data on usage, events, individual configurations, or current state, distributed across multiple controllers and systems

» Organizations such as a manufacturer, distributor, insurance company, or government agency

» Individuals including employees as well as third-party workers, auditors, and partners

» Events from standard use to violations of defined limits, accidents, and technical failures

Within this dynamic context, the service operator must maintain control over exactly who is allowed to access which data under which event. On one hand, the seamless flow of IoT data is crucial for building rich, end-to-end digital experiences. On the other hand, a lapse in security and control can have devastating consequences, from theft of sensitive personal data to sabotage or ransomware.

Maintaining trusted identities, control, and manageability would be challenging enough for hundreds or thousands of devices, but at enterprise scale, with potentially millions of things connected with dizzying complexity, there's simply no way to make IoT work using manual measures. A robust identity management capability provides the automated access control needed to keep even the most expansive IoT ecosystem well managed.

Strengthening Identity Management to Overcome IoT Challenges

Identity makes it possible to manage access control at scale. For example, a device can call out to an identity store on the network edge to get permission to self-install—a critical capability for installations too large-scale for manual deployment. A technician can access a sensor to retrieve the data it has collected, or the sensor itself can access applications for which it is authorized to upload its data directly.

However, traditional identity management capabilities fall short of what's needed now. In the past, identity was largely a matter of controlling access to applications and systems by people. Consider the evolving variables defining the requirements for modern identity management:

» Identity no longer applies exclusively to people, as in the past; today, things need identities of their own, and engage in their own complex identity relationships.

» Identity management now extends beyond IT's control as multiple identity providers and authenticators co-exist within the same ecosystem, each with its own set of identities to manage.

» Many users will now use different identities or personas to reflect to their current role or tasks, switching among them as their needs change. Both identity and risk vary according to context, calling for a more flexible approach to authorization.

With a more robust identity management capability, identities can be assigned not only to people and devices, but also to services delivered through an edge controller and other elements of the IoT ecosystem. This allows a higher level of control over the interactions among things and data, such as applying different levels of permission for different people and devices. An operator can be given permissions appropriate to their specific role and training; a third-party service technician can be given different rights for different contexts. Fundamentally, identity makes it possible to control and manage the interactions among people, organizations, and things, and their access to systems, components, and data—and to do so at the scale and complexity of an enterprise IoT installation.

How Identity Management Supports IoT Use Cases

At a high level, the IoT market breaks down into two categories of use cases: business optimization and business transformation.

Business optimization focuses on maximizing the value of existing assets and investments, increasing efficiency, and improving operational performance. Examples include predictive maintenance, process automation, factory automation, and building automation. One organization is using IoT to build a trusted and contextual digital workplace. In the first phase, IoT will be used to maximize floor space, work locations, and assets. Future phases will see the introduction of contextual seating maps, smart room technologies, and other services to increase team efficiency and productivity. Identity management supports this use case by:

» Establish a trusted identity to newly connected things

» Building trusted relationships between the users and their things

» Establishing a 360° view

» Enabling fine-grained access management and delegation

Business transformation involves the introduction of new digital services and business models. While business optimization initiatives are internally focused, business transformation delivers new experiences to customers to increase competitive differentiation, customer satisfaction and loyalty, and revenue.

By leveraging identity within the context of IoT, companies can:

» Create rich, omnichannel customer experiences that follow customers across devices, platforms, and contexts to grow top-line revenue

» Deliver more personalized offerings—for example, by applying a user's preferences across a broader range of products and services to design new and potential disruptive business models

» Understand the relationships and interactions among people, services, and things in a given environment

» Collect trusted data that can be used to craft hyper-personalized offers

In a classic example of IoT-enabled business transformation, one connected vehicle provider is using IoT to create trusted vehicle and device identities that enable new mobility services. A customer can:

» Authenticate the owner before authorizing actions such as unlocking, starting, and driving the vehicle

» Share the vehicle safely by setting limitations for the other driver's time of use, geographic range, acceleration, and speed

» Share data on vehicle usage and state with an insurance company to qualify for customized terms, or with a dealer or service station for predictive maintenance

» Remotely authorize a delivery driver from a retail company to open the vehicle for package delivery

» Make payments at a gas pump, drive-through window, or toll booth based on the authenticated driver and their associated payment token

Guiding Principles for IoT Success

Given the scale and complexity of any enterprise IoT ecosystem, it's crucial to take a thoughtful approach to design and execution. One way to think of it is: Think big, act small, move fast.

» **Define a bold, end-to-end vision** for your company's IoT strategy. How will it reshape your relationship with your customers and their relationship with your products and services? What new experiences can you build out from your legacy business model? What's the "smart" version of your business—as in, moving from lighting sales to smart lighting services, or from automobile sales to smart mobility services? This vision will provide a framework around which to build individual initiatives and technologies.

» **Start small** by solving a clearly defined existing problem with a relatively simple solution to build expertise, then continue to expand in line with your guiding vision.

» **Assemble a strong partner ecosystem** of technology vendors and partners. No one can implement IoT alone. In fact, research by James Brehm & Associates shows that there are typically eight systems or companies involved in a sizable IoT project.

- **Avoid creating silos** as you expand. These can complicate subsequent business process digitization efforts.
- **Deliver fast** to prove value, gain buy-in, and start leveraging the IoT's potential for optimization and transformation.

How ForgeRock Modernizes Identity for Successful IoT

ForgeRock helps companies build a foundation for IoT success by applying identity, defining relationships, and establishing trust among all the elements of the ecosystem.

- ForgeRock technologies for identity-based internal and external security have been proven through the deployment of more than one billion identities.
- A single, unified platform breaks down silos, reduces cost, and accelerates time to market for feature upgrades.
- Seamless integration with existing infrastructure lets companies leverage the full value of their current environment while extending it with new IoT capabilities.
- API integration with new and existing business processes helps companies increase automation, efficiency, and control.

The ForgeRock Identity Platform is designed to support a wide variety of IoT use cases including, but not limited to, the following:

- Creating and storing a smart device identity
- Authenticating a smart device to a cloud service
- Authorizing a smart device to access cloud APIs
- Self-registering and IoT user identity
- Customizing the IoT user experience
- Revoking an association between device and user identities
- Protecting IoT resources

Conclusion

The IoT extends and accelerates digital transformation by enabling new services, business models, and operational models for companies in almost every industry. Without an effective way to control the interactions and data flows among things and entities, or to establish trusted relationships across the ecosystem, an IoT installation can become impossible to manage —especially at enterprise scale. Identity provides a way to build access control into the fabric of the ecosystem. Only authorized actions and data access can occur, and only by authenticated entities—whether an operator, a third-party technician, a system or application, or even a data flow. Extending across organizations and systems, the identity-enabled ecosystem gives companies more freedom and flexibility in the types of services they can create, allowing them to achieve even greater differentiation, customer satisfaction, and operational optimization. With a strong identity management solution, companies can move forward with confidence in the quality and scalability of the services they offer.

Find out how ForgeRock manages trusted relationships among people, services, and things here.

/ABOUT FORGEROCK

ForgeRock®, the leader in digital identity management, transforms how organizations build trusted relationships with people, services, and things. Monetize customer relationships, address stringent regulations for privacy and consent (GDPR, HIPAA, Open Banking, etc.), and leverage the internet of things with ForgeRock. We serve hundreds of brands, including Morningstar, Vodafone, GEICO, Toyota, and Pearson, as well as governments like Norway and Canada.

www.forgerock.com