What is SAFE Identity?

SAFE Identity is an industry consortium and certification body operating a Trust Framework for digital identities in healthcare. This standards-based framework is designed to ensure trust and interoperability of digital identities used between healthcare organizations, supply chains, contractors, internet-connected medical devices and more, for digital communication, data exchange, and system access.

The SAFE Trust Framework supports the use of advanced cryptography to support both technical and legal interoperability between all participants in the ecosystem, enabling identity trust, authentication, end-to-end encryption and more. A select group of healthcare leaders and stakeholders, called the Policy Management Authority (PMA), govern the common identity policies that control the security and interoperability of the SAFE Trust Framework, working to meet the needs of the industry, by serving as voting representatives of the industry.
What Can SAFE Do For You?

SAFE Identity facilitates bi-directional trust of digital identities between organizations through a common identity infrastructure shared by all participants. The infrastructure brings value to all parties involved, however, given the different needs of participants throughout the healthcare industry, the value of the SAFE Trust Framework might be different for each participant. Below is a brief articulation of how the SAFE Trust Framework brings value to your organization.

Healthcare Delivery Organizations (HDOs)

Relying on The Trust Framework

Vendors require access to healthcare provider’s systems frequently. Such access takes many forms, ranging from an IT consultant carrying out their work remotely on a hospital’s network, to patients connecting from home in support of telehealth and remote patient monitoring, to network connected medical devices that require network access to function and share updated data. Such a varying set of external users (human or otherwise) requires a unified capability that allows the healthcare provider to leverage a common infrastructure – such as the SAFE Identity Trust Framework – to secure and manage the risk of external users proving their identity in order to gain access to hospital systems.

View the SAFE Identity Supply Chain Executive Brief for more information.
Pharma and Contract Research Organizations (CROs)
Relying on The Trust Framework

Similar to HDOs, vendors supporting a pharma supply chain are extensive, ranging from IT consultants, CROs, Contract Manufacturing Organizations and many others. In some cases, the information exchanged between these organizations is highly confidential intellectual property that must be protected in transit and at rest. Pharma companies also need to support an external facing track and trace system that allows a dispenser to verify the origin and authenticity of a drug as part of the Drug Supply Chain Security Act (DSCSA). The variety of system access and information exchanges between external parties all require strong digital identity credentials to ensure data exchange is secure and the identity of external users can be verified to a high degree of confidence before allowing system access. SAFE Certified Credentials can provide that confidence.

View the SAFE Identity Supply Chain Executive Brief for more information.
Achieving External Trust of Employee Credentials

Just as life sciences companies and other large to mid-size healthcare organizations need to verify the identity of external parties, they also need their employee identities to be trusted externally. Such interoperability is achieved today by federating with external parties, one at a time. This is a resource-intensive effort and limiting approach when used at scale, making it a challenge to unify identity use cases across the organization. An alternative strategy is to leverage a trust framework, such as the SAFE Trust Framework, to federate trust of identity credentials on a life sciences company’s behalf. Such an approach unifies all identity use cases for employee credentials supporting authentication, data integrity and data confidentiality while also supporting external partner and government interoperability at scale in a standards-based way.

View the [SAFE Identity Cross-Certification Executive Brief](#) and the [SAFE Identity Supply Chain Executive Brief](#) for more information.
Medical Device Manufacturers (MDMs)

Achieving External Trust of Device Identities

Medical device manufacturers face a unique challenge when it comes to device security. While all medical device vulnerabilities cannot be traced back to a failure of identity, many vulnerabilities can. The use of passwords on medical devices presents a significant risk not only to the compromise of the medical device itself and by extension, damage the reputation of the manufacturer, but also to the medical device consumers, such as HDOs, labs and radiology centers. Medical devices need a standards-based mechanism for proving their identity over the internet to a consumer in support of strong network authentication and data protection. The device also needs to support a secure update mechanism that allows patches and firmware to be applied with assurance that they have not been modified by a bad actor.

Manufacturers have increasingly taken on a role of updating and managing devices on behalf of consumers. This service often requires network access to the consumer’s environment, which means medical devices manufactures not only need to provide the identity of their devices, but also the staff that will be responsible for maintaining the device. Such extensive external coordination is best facilitated through the use of the SAFE Trust Framework to facilitate interoperability and trust of digital identity credentials between external businesses at scale.

View the SAFE Identity Cross-Certification Executive Brief for more information.
How Do I Put SAFE to Work in My Organization?

Organizations aiming to have their employee’s credentials trusted externally can take advantage of the SAFE ecosystem by purchasing a SAFE Certified Credential that can be trusted and easily accepted across organizations, or by issuing trusted and certified credentials themselves.

When organizations connect to a Bridge CA, such as the one administered by SAFE, the digital certificates within its hierarchy become federated into a larger PKI community. The SAFE Bridge facilitates trust between every organization it is connected to. Organizations that do not maintain a federated Certificate Authority can rely on the SAFE Trust Framework by depending on the freely available SAFE Trust Anchor which can be installed through Active Directory or configured in a wide variety of applications that support standards in PKI. By utilizing a Trust Framework, participants can prevent vendor lock-in, enjoy enhanced legal and technical interoperability and avoid price gouging by leveraging standards in identity rather than proprietary systems.

Visit the SAFE website to learn more about purchasing SAFE Certified Credentials.

How does SAFE help with making good buying decisions for identity-related products?

The SAFE QPL is a public list of identity-related applications and products that have undergone cryptographic lab testing based on industry adopted specifications through SAFE Identity. Listing on the QPL confirms that a solution uses digital identities in the way holders, issuers and relying parties expect, and are interoperable within the SAFE ecosystem.

Healthcare organizations can consult the SAFE QPL to make informed decisions on which identity products and applications for digital signatures, encryption and authentication best meet their needs. This service includes mapping features, so buyers can determine appropriate, equivalent cryptographic requirements for different vendors for the assurance level they need. Each product undergoes diverse and rigorous testing to ensure it properly implements cryptography and correctly processes identity, along with meeting certain requirements for usability.

Download the SAFE QPL brief for more info.
What other services does SAFE provide to help healthcare organizations?

In addition to the Trust Framework, the QPL and cross-certification, SAFE offers numerous services to make trust simpler. Another service SAFE offers is PMA membership, in which an organization can join a group comprised of leading individuals representing their respective organizations in the health industry to vote on the policies that govern the SAFE Identity Trust Framework. These decisions are made with industry challenges in mind, as well as to suit the needs of PMA member organizations. Members of the PMA include healthcare organizations that rely on SAFE Certified Credentials, organizations that purchase SAFE Certified Credentials, and SAFE Certified Credential Providers (both commercial and enterprise). Members set the topics and gain access to all of SAFE’s technical working groups to solve challenges related to identity and cryptography.

SAFE also offers certification of identity providers, to facilitate external interoperability. All SAFE Certified Credential Providers can be trusted by those relying on the SAFE Trust Framework. These providers are listed on the SAFE website and the SAFE Identity Qualified Products List (QPL).

Another service SAFE offers is various certifications of identity-related software products and services. SAFE certifies products in its lab against widely adopted industry standards. SAFE provides the guidelines for meeting these requirements, as well as transparency into the vendor-agnostic testing processes. These products are tested to ensure interoperable with identities in the SAFE ecosystem and with other credentials that adhere to industry standards in PKI and cryptography. All SAFE certified products and services are publicly listed on the SAFE Identity QPL.

Who is behind SAFE?

SAFE Identity’s leadership team is composed of diverse experts from a wide variety of experiences and backgrounds. Our membership includes some of the 50 largest pharma companies globally, as well as several Fortune 500 companies. This breadth of expertise enables us to tackle the many complexities in the highly dynamic environment of digital identity. We facilitate innovative solutions through our community and our employees.

Interested in learning more?

- Get involved
- Visit Our Website
- Contact Us