

Company Background

Oct 2017





Intercede is a global leader in cybersecurity with global clients such as Boeing, Lockheed Martin, TELUS, Interpay, the UK Government and the US Federal Government, plus the tier one relationships with Intel, ARM and Microsoft. Intercede's heritage is in securing some of the world's most sensitive data assets for organizations in the most data critical industries including defence, aerospace, government and financial institutions. For two decades, the company's software has ensured that access to physical infrastructure, networks, applications and data is restricted to people and machines that are both positively identified and authorized.

A Growing Threat

Today, few companies can afford to ignore the requirement to more effectively establish digital identity and create the trust relationships that enable 21st century commerce. The volume of data held has increased dramatically, the regulatory requirements are much more onerous and cybercrime is sophisticated and widespread. Despite that situation, much of the world's data is protected by little more than a username and password combination, an approach continually shown to be profoundly flawed. In that environment, it shouldn't come as a surprise that 80% of hacking related breaches exploit stolen or weak passwords and the potential for catastrophic business impact is real.

Whilst much of the industry has focused on pleading with users to use ever more complex passwords, or adding basic two factor authentication, Intercede has developed its core technologies to apply to a much wider range of sectors and implementations. Working directly and with partners, Intercede has created solutions to address the requirement in enterprise and consumer markets and to take a lead in the developing IoT sector.

Developing Digital Trust

Digital trust is defined as knowing that the people or 'things' connecting to a device or service are who or what they claim to be. That trust is predicated on establishing and verifying a unique digital identity. Without it, trust can't be established and data breaches are not only possible, but probable. In today's digital economy and hyper-connected world, trust and privacy are no longer a nicety, they are an essential requirement. Organisations ignore this at their peril.

The digital identities created by Intercede, and consisting of a unique private 'key' that cannot be copied, coupled with a 'certificate' issued by a trusted authority, allow identity to be verified with confidence. When combined with a second authentication factor, identity can be verified and you can be sure that whoever or whatever is requesting service access is authorized to do so.

Something You Know, Something You Have

At the heart of Intercede's approach is a requirement that someone attempting to make a digital connection, as well as knowing something, must also have

something and that something must be equipped with a secure digital identity. In the case of a person accessing a service online those two requirements can be satisfied with a simple PIN (or biometric such as a fingerprint) and their identity equipped smartphone. Neither the PIN nor the smartphone can be used in isolation.

Digital identities are far more secure and convenient than passwords and they protect services and devices from exposure to the most common form of data breach. Whilst the cryptology behind the approach is very advanced, the user experience is extremely convenient and there is no requirement to define and remember complex passwords.

*Intercede identity authentication solutions ensure that users, devices and apps are who and what they claim to be. It's what we call **DIGITAL TRUST**.*



Product portfolio

Employee IDs

Secure enterprise access has never been a more critical requirement for protection from growing threats. MyID enables enterprises to replace employee passwords with more secure and more convenient digital identities: providing protection against the number one cause of data breaches - weak or compromised user credentials.

Once deployed, MyID is connected to existing infrastructure to issue trusted digital identities to employees across a wide range of devices including smart cards, virtual smart cards and mobile handsets. It complies with specific regulatory requirements such as FIPS 201 and SP 800-171 in the US and GDPR in Europe and can be provided as an on-premise or private cloud solution. Administrators manage the lifecycle of credentials, for example automatically revoking them if a user leaves the organization, or updating them in advance of them expiring.

All credential issuance and lifecycle events are recorded within MyID allowing full visibility of who has active access credentials, and the built-in audit enquiries and reports are often used as part of a compliance audit to show an organization is in control of who can access their systems.

Consumer IDs

Consumers are fed up with being told to remember an increasing number of complex passwords and the hardware tokens that are commonly seen in banking applications are universally disliked and costly. MyID is the alternative – a secure, easy to implement two-factor authentication service for mobile apps and cloud services. It allows service providers to quickly deploy strong authentication to services from mobile apps, with minimal effort and cost. MyID has relevance in a variety of sectors including banking, retail, healthcare, social media, gaming and TV/media services.

MyID uses PKI certificates with two-way SSL to secure trust between the mobile device and the service without the need for additional SMS verification or 'one-time' passwords. The result is a frictionless solution for service provider and customer.

MyID dramatically enhances application security with quick and secure two-factor identity authentication, that simultaneously improves the user's experience by eliminating passwords from the equation. As well as authenticating customers without passwords, MyID credentials can also be used for additional security capabilities, such as digitally signing transactions. A prime regulatory market in the payments space solved by MyID is PSD2.

Intercede partners with the world's best known companies in silicon and security - ARM, Citrix, Gemalto, Blackberry, Intel, Microsoft, IDEMIA, Symantec, Trustonic..