Entrust Identity Mobile Smart Credentials

Trusted digital identities for the new workplace

Market Challenge

With the concept of a company supplied and secured workplace fast disappearing, employees need to be able to securely execute their responsibilities from anywhere.

Solution

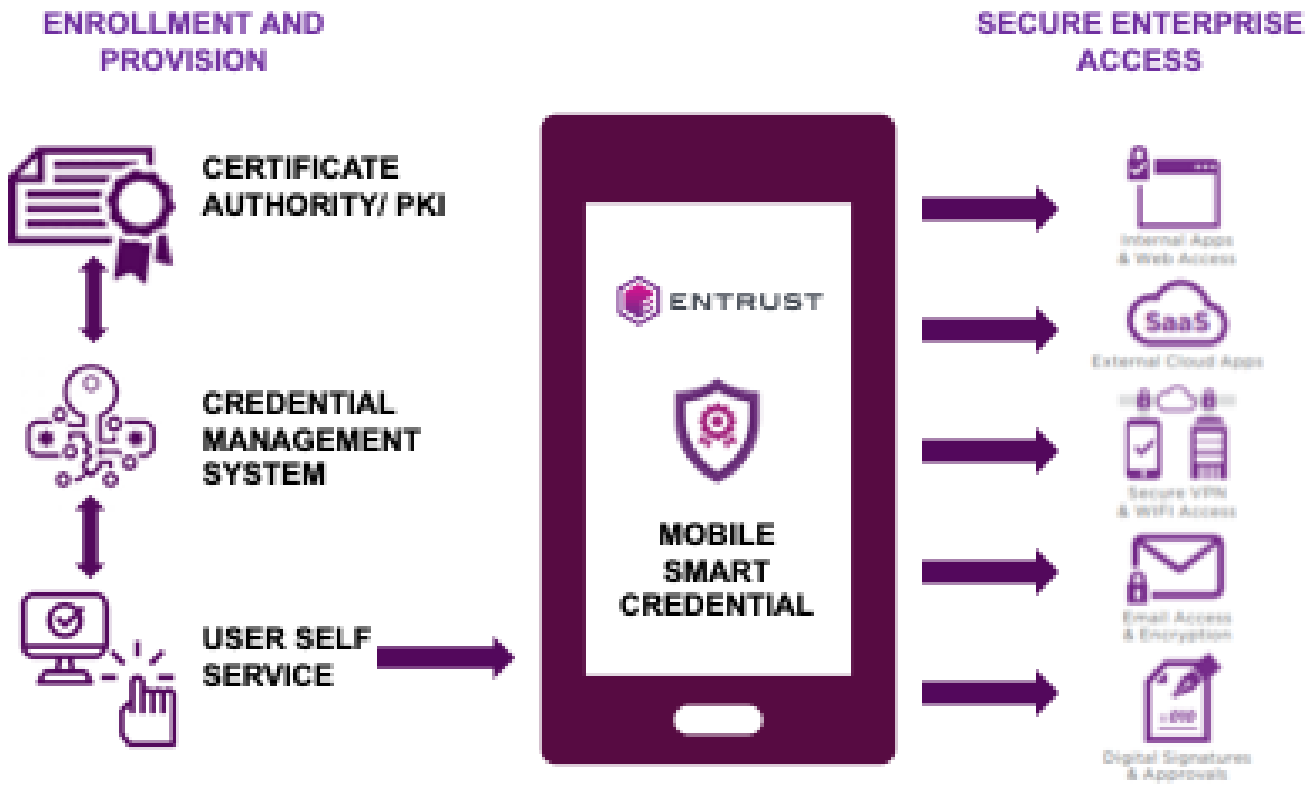
Mobile smart credentials (MSC) from Entrust Identity allows for a secure and productive workforce. Our MSC technology provisions a digital certificate onto the worker's mobile phone, transforming it into their trusted workplace identity, wherever that workplace may be.

BENEFITS

- Enable your secure mobile workforce
- Replace physical smart cards
- Fully integrated with main EMM platforms
- Use CA of choice
- PIV compliant (FIPS 201)

Entrust Identity Mobile Smart Credentials

You can use digital certificates issued by the certificate authority (CA) of your choice, including Entrust and Microsoft CAs. The digital certificates are managed by the roles and policies defined by native or Entrust PKI. Plus, MSCs follow PIV standards (FIPS 201) to meet the stringent security requirements for US federal government employees and contractors.



Entrust Identity Mobile Smart Credentials

Features

High assurance workforce solutions

MSCs verify the user AND authenticate the device, creating the worker's trusted workplace identity. With our larger Entrust Identity portfolio, we provide added layers of assurance with additional authenticators (i.e. biometrics), single sign-on (SSO), and adaptive risk-based authentication. Learn more about Entrust Identity.

Go passwordless

By combining MSCs with smartphone biometrics, workers are able to securely access company resources passwordlessly on their phone and workstation. For the latter, when the worker is in close proximity of their workstation and the phone is unlocked with their biometric, they are automatically logged in via a secure Bluetooth connection or near field communications (NFC) and logged out when they walk away – a critical capability for organizations with shared workstations (e.g., doctors, stock traders). With Identity as a Service, password-less access includes SSO for a truly frictionless user experience.

Secure digital signing

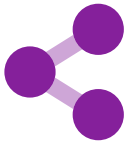
Legally binding digital signatures are fundamental to many day-to-day operations. MSCs verify the signer's identity for a strong, non-repudiated digital signature – right from their mobile device.

Encrypt email communications

MSCs can be used to encrypt emails for secure transmission over the internet. Before an email leaves the outbox, the certificate-based credential digitally signs the email to verify the sender's identity and encrypts the plain text using asymmetric encryption (with the public key of the recipient). Only the recipient who has the matching private key can decrypt the contents of the email.

Reduce IT costs

With streamlined user provisioning, user self-service tools, and no need for physical smartcards, card-printing, and personalization systems, Entrust Identity with MSCs reduces your IT administration and associated costs.



Ease of integration

MSCs can be easily provisioned from client mobile applications or EMM platforms. MSCs offer built-in integration for simple deployment, regardless of the mobile operating systems used within your environment. This flexibility enables IT organizations to work with end-users and provide BYOD security.

Entrust Identity Mobile Smart Credentials

MSC deployment options

In-application

Entrust Identity lets you embed MSCs directly within an application or application suite. This use case is generally deployed in three different ways:

Enterprise mobility management platforms
Entrust has established partnerships with top EMM vendors like Blackberry, MobileIron, Citrix, Microsoft Intune, IBM MaaS360, and VMware AirWatch. This enables the MSC to be fully integrated with the EMM mobile client.

Internally developed applications
For custom enterprise applications or internal portals, there is an SDK which integrates MSCs within the internal mobile client.

Accessing public cloud apps via identity protocols like SAML, OIDC, OAuth, or LDAP
Entrust Identity integrates with established identity providers such as Microsoft Active Directory Federation Services (ADFS), enterprise SSO platforms, and the Entrust Federation module to extend secure mobile access to any browser-accessible SaaS application.

Frictionless user experience
User opens a mobile browser, enters the desired URL, and is prompted for an authentication (Touch ID, PIN, etc.). There is no need to authenticate again and no passwords or tokens are required.

Outside-of-application

MSCs can also be leveraged via the Entrust Identity mobile application. This app accommodates a range of authentication scenarios including:

- Accessing applications using **federated identity protocols like SAML, OIDC, or OAuth.** This use case does not depend on technical partnerships between the mobile identity provider (Entrust) and the application provider.
- For **server-side applications that do not support SAML/SSO,** the Entrust Identity mobile app can be directly integrated through APIs. This scenario requires additional setup but ensures a seamless experience.
- The Entrust Identity mobile app communicates with an **SSO portal** (such as Oracle Access Manager). Sign-on creates a secure web connection that enables seamless access to all web apps protected with the SSO portal.

Frictionless user experience
Since the MSC is not fully integrated with the application, the initial setup will have the following few additional steps for users:

- User opens the mobile browser and enters the desired URL
- User then enters their username in the app login (this can also be auto-populated based on the embedded PKI certificate)
- User is prompted to authenticate via a Push notification, PIN, or Touch ID
- User confirms the session with a click / swipe

About Entrust Identity

Entrust Identity is the unified portfolio that addresses all of your organization's Identity and Access Management (IAM) requirements. Entrust Identity protects and verifies the identities of workers, consumers, and citizens so you can establish secure access and communications with these different user communities, when and where needed.

Learn more at
entrust.com

Entrust and the Hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer.
©2020 Entrust Corporation. All rights reserved. IA21Q3-entrust-identity-mobile-smart-credentials-ds

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com entrust.com/contact