Entrust®

+1-888-690-2424
entrust@entrust.com
entrust.com/cloud

@Entrust
+entrust
/EntrustVideo
/EntrustSecurity

DOWNLOAD THIS DATA SHEET

Entrust IdentityGuard Cloud Services Device Certificates

Securing Mobile Identities & Devices

The proliferation of mobile devices presents tremendous opportunities for organizations to empower employees and increase business efficiency.

Entrust cloud-based solutions enable organizations to transparently deploy and manage digital certificates on mobile devices to secure mobile identities and transactions, grant secure access to corporate networks and enable secure email.

Mobility & BYOD

Enterprises face a diverse set of challenges with personal and company-issued mobile devices co-existing within secure corporate infrastructures — all core to enterprise mobility and bring-your-own-device (BYOD) movements. Solve this challenge via certificate-based security on mobile devices issued from Entrust's cloud services.

▶ **entrust.com/mobile**

Certificates from the Cloud

With Entrust cloud-based services, organizations may seamlessly provision and manage device certificates directly to many of the leading mobile platforms. Realize the benefits of certificate-based security without deploying and managing an on-premise PKI/ certification authority (CA).

Secure the Mobile Enterprise

Granting secure access to corporate networks from mobile devices needs a strong and simple approach. Due to low security and unfriendly user experiences, usernames and passwords are no longer sufficient in the mobile world. Organizations need a secure, transparent and simple approach to enabling mobile access.

▶ **entrust.com/enterprise**

Tailored Deployment Models

Digital certificates may be provisioned and managed through a variety of methods. Whether deployed via cloud or on-premise models, organizations may select the method that best suits their security needs, budget and environment.

Solution Benefits

- Enable certificate-based security on mobile devices without deploying a PKI
- Leverage mobile device certificates from the cloud to enable strong device identity
- Eliminate reliance on mobile usernames and passwords for VPN and Wi-Fi access
- Enhance user experience with transparent authentication to VPN and Wi-Fi access points
- Easily provision and manage digital identities and devices in BYOD environments
- Secure mobile devices communicating with customer or enterprise environments
- Leverage mobile device management (MDM) platforms to enable strong device identity
- Simplify management with an easy-to-use interface that allows for anytime, anywhere access

Why Digital Certificates?

As the use of mobile devices and applications grows, so do the rate and sophistication of network and identity attacks on organizations and individuals. This momentum is compounded by the introduction of numerous management and provisioning challenges.

Organizations require a methodical and proven solution to issue and manage mobile devices. Administrators need to know who is accessing corporate networks and what information is stored on the devices.

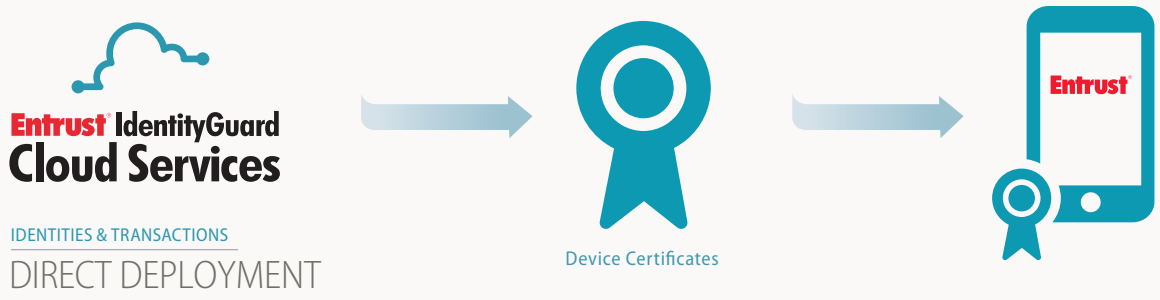
Security-conscious organizations rely on digital certificates as the foundation of their identity-based access and security measures. Digital certificates provide strong device identities to enable secure Wi-Fi or VPN access.

Certificate-based mobile security empowers organizations to defend themselves against unauthorized sharing of Wi-Fi passwords. In fact, certificates are unique for each device and also enable secure email (S/MIME) communication.

Mobile Digital Certificate Management

Entrust helps organizations deploy and manage digital certificates on mobile devices to secure mobile identities and transactions. Entrust digital identities are transparently deployed on mobile devices to grant secure access to corporate networks and enable secure email.

Digital certificates may be provisioned and managed through a variety of methods. Whether deployed via cloud or on-premise models, organizations may select the method that best suits their security needs, budget and environment.



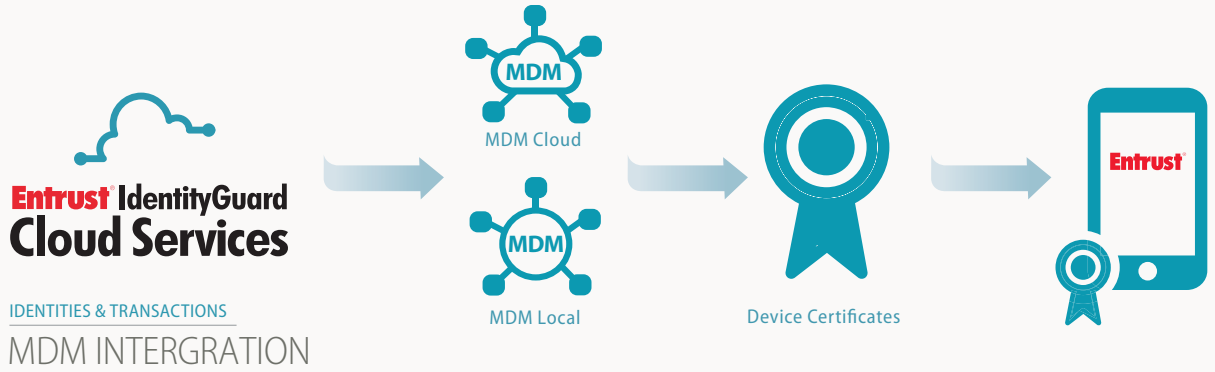
Mobile Device Certificates — Right From the Cloud

With Entrust cloud-based services, organizations may seamlessly provision and manage device certificates directly to many of the leading mobile platforms.

Realize the benefits of certificate-based security without the burden of deploying and managing an on-premise PKI/certification authority (CA).

The solution streamlines the management and delivery of device certificates, which may be delivered directly to mobile devices without the need for client software.

This is all accomplished through an easy-to-use interface that can be accessed anytime and from anywhere. This approach reduces costs, increases efficiency and simplifies setup and deployment.



MDM Integration

Today's leading mobile device management (MDM) solutions offer organizations the ability to manage mobile platforms, enforce policy and ultimately empower organizations to enable enterprise mobility.

However, granting secure access to corporate networks from mobile devices needs a strong and simple approach. Due to low security and unfriendly user experiences, usernames and passwords no longer suffice in the mobile world.

Security-conscious organizations realize the benefits of MDM solutions and certificate-based security. It is imperative organizations leverage their investment by allowing their MDM solution to seamlessly provision and manage device certificates. This provides a secure, transparent and simple approach for mobile access. Entrust transparently delivers device certificates to mobile devices through a variety of leading cloud and on-premise MDM solutions.

Secure Mobile, Leverage Mobile

Entrust solutions help secure mobile identities and transactions, but also allow organizations to leverage mobile devices to improve overall security.

Whether to enhance strong authentication or eliminate usernames and passwords, Entrust helps organizations secure their mobile devices and subsequently leverage them to strengthen identity-based security

ENTRUST MOBILE SECURITY SOLUTIONS

IDENTITIES, DEVICES & TRANSACTIONS

- STRONG AUTHENTICATION
- DEVICE CERTIFICATES
- MDM INTEGRATION
- DESKTOP MALWARE PROTECTION
- MOBILE SMART CREDENTIAL
- TRANSACTION-SIGNING
- APPLICATION PROTECTION
- ANALYTICS

Entrust IdentityGuard Cloud Services

Entrust IdentityGuard Cloud Services is a comprehensive cloud-based solution that offers Entrust's complete line of identity-based security solutions. Manage all identities and certificates — related to SSL, smart credentials, device certificates, PKI and certificate discovery — right from a single cloud interface.

This approach provides a simple, strong and easy solution to issue and manage identities through their lifecycle via the cloud.

A trusted provider of identity-based security solutions, Entrust secures governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries.

Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL.

For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Company Facts
Website: www.entrust.com
Employees: 359
Customers: 5,000
Offices: 10 globally

Headquarters
Three Lincoln Centre
5430 LBJ Freeway, Suite 1250
Dallas, TX 75240 USA

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. In Canada, Entrust is a registered trademark of Entrust Limited. All other Entrust product names and service names are trademarks or registered trademarks of Entrust, Inc. or Entrust Limited in certain countries. All other company names, product names and logos are trademarks or registered trademarks of their respective owners. © 2014 Entrust. All rights reserved.

24710/1-14