KuppingerCole Report

EXECUTIVE VIEW

by Mike Small | October 2017

Entrust IdentityGuard for Enterprise

Securely authenticating users is a major problem given the increasing threats from cyber-crime. Entrust IdentityGuard for Enterprise provides a comprehensive solution for enterprises to select and manage the way in which organizational users are authenticated to access both physical and logical assets.

by **Mike Small**
mike.small@kuppingercole.com
October 2017

Content

Related Research Documents

Leadership Compass: Privilege Management - 72330

Leadership Compass: Identity as a Service: Single Sign-On to the Cloud (IDaaS SSO) - 71141

Leadership Compass: Identity as a Service: Cloud-based Provisioning, Access Governance and Federation (IDaaS B2E) - 70319

Leadership Compass: Cloud Access Security Brokers - 72534

1 Introduction

The threats to organizations from data theft, ransomware and other forms of crime continue to increase. Organizations need to be vigilant and take appropriate precautions to reduce the risk of both physical and cyber-attacks being successful. One critical area that needs to be addressed is that of how individuals and devices are identified; this is known as authentication.

Identity and access management encompasses a range of processes and technologies that are intended to ensure that only authorized people and devices can access the physical and logical infrastructure to which they are entitled. The processes include the vetting of individuals, issuing of credentials, authentication, authorization and monitoring as part of a complete lifecycle management process. One area that needs careful attention is authentication.

Approaches and technologies for authentication have evolved considerably in recent years; however, the use of username and passwords, while known to be weak, is still common. Authentication methods can be summarized as follows:

- Something you know – like a password or PIN.
- Something you have – like a token, smart card or, increasingly, a mobile device
- Something you are – a biometric like a fingerprint.

Mutual authentication extends the authentication process to provide confidence to the user that the system they are attempting to access is genuine to avoid their credentials being revealed to fraudulent or spoofed sites. This often uses the exchange of a random number encrypted using public and private keys. Mutual authentication is inherent where it is based on the use of PKI and X.509 certificates.

The latest mobile devices include a TEE (Trusted Execution Environment). This can be used to hold encryption keys securely making the device as secure as a smart card for authentication. This is exploited by systems such as FIDO[1] (Fast Identity Online). Some mobile devices include fingerprint readers that can be used to provide additional confidence.

MFA (Multi-Factor Authentication) increases assurance combining two or more methods. Adaptive authentication takes account of additional factors based on the risk of the particular transaction to add a further level of assurance. For example, the additional factors used may include the physical location, time of day and device being used to provide additional evidence of identity. NIST SP800-63B[2] defines the levels of assurance that is provided by different forms of authentication.

Many organizations allow partners and suppliers to access their systems relying on the partner to authenticate their employees. This is achieved securely by using the identity federation standards SAML

[1] **https://fidoalliance.org/about/overview/**
[2] **http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf**

2.0[3] and ADFS[4]. This does not remove the need for authentication it merely transfers the responsibility to the partner or the identity provider.

Other standards have been developed for consumer access including OAuth2[5] and OpenID[6]. OAuth is an open standard for access delegation, that is often used as a way for Internet users to grant websites or applications access to their information on other websites without revealing the passwords. This mechanism is used by companies such as Google, Facebook, Microsoft and Twitter to permit the users to share information about their accounts with third party applications or websites.

OpenID allows users to be authenticated by co-operating sites using a third-party service. This eliminates the need for services to each provide their own ad hoc login systems, and allows users to log into multiple unrelated websites without having to have a separate identity and password for each.

In today's world where users are highly mobile and transactions are conducted on the move from a variety of locations, it is no longer appropriate to use a single authentication method based on a fixed view of risk. User names and passwords provide only the lowest level of assurance in the identity of the user. Furthermore, they are very easily compromised and, because of this, have become the target of choice for cyber-criminals to get a foothold into organizational systems. Providing individuals with multiple different authentication methods and devices for use under different circumstances can increase assurance but poses management and usability challenges. Organizations can benefit from a single authentication platform that supports a range of authentication methods for physical, logical and mobile access throughout the enterprise.

2 Product Description

Entrust Datacard is a privately held company that was founded in 1969 with headquarters in Minneapolis, Minnesota, USA. In 2014 Entrust was acquired by the Datacard Group and continues to provide its solutions under the Entrust Datacard brand name.

Entrust Datacard offers solutions that range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. This report concerns the Entrust IdentityGuard for Enterprise product.

2.1 Entrust IdentityGuard for Enterprise

Entrust IdentityGuard offers a wide of authenticators from a single software platform. The platform extends to cover smartcards, mobile smart credentials, biometrics and digital certificates. This platform enables organizations to integrate multiple security environments — physical, logical, cloud and mobile and provide consolidated management, cost effectively and with complete view of security.

[3] **http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html**
[4] **https://technet.microsoft.com/en-us/library/cc755226(v=ws.11).aspx**
[5] **https://oauth.net/2/**
[6] **http://openid.net/**

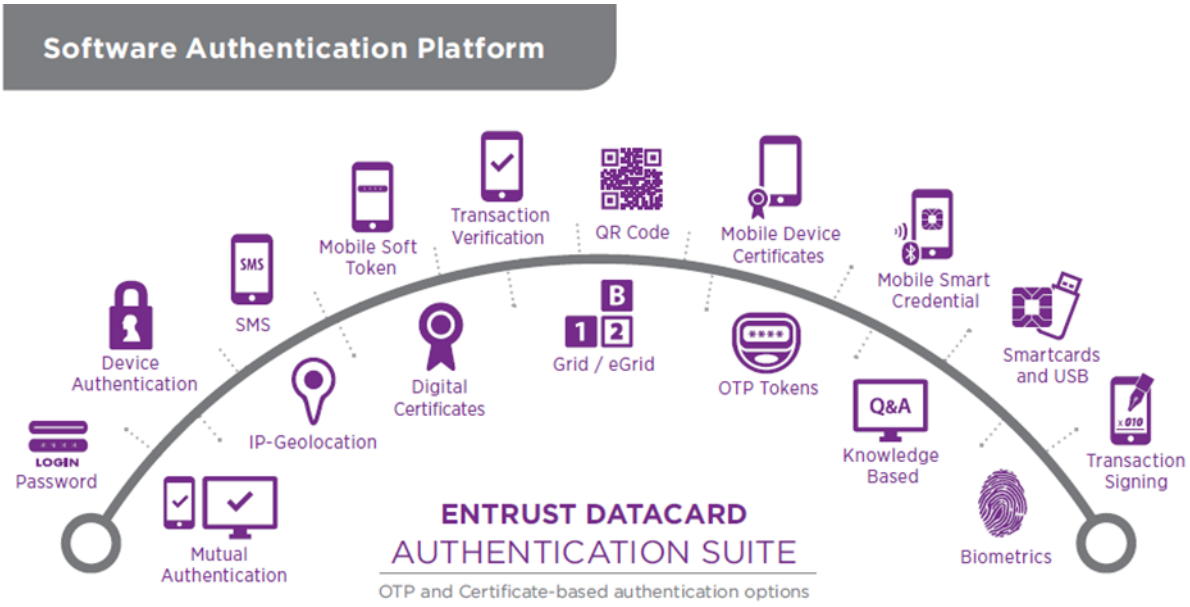

Figure 1: Entrust Datacard Authentication Suite -graphic reproduced with permission from Entrust Datacard

This platform enables organizations to:

- Issue digital certificates, smartcards (from Entrust or third parties), mobile-based smart credentials and a full range of traditional strong authentication options from a single software platform;
- Reduce the number of credentials users are required to have for physical or logical access;
- Implement full lifecycle management of credential environments covering selection, issuance, management and revocation;
- Eliminate the need for physical smartcards by exploiting mobile devices to provide enterprise-grade authentication. These mobile smart credentials may be used with Bluetooth and near-field communication (NFC) technology to provide user convenience;

2.2 Strong Authentication Methods

Entrust IdentityGuard supports a wide range of strong authentication methods with a single point of administration. This makes it easier for organizations to select the authentication method used based on the actual risk involved without increasing administrative costs. Entrust IdentityGuard classifies the authentication methods as follows:

2.2.1 Transparent Authentication

These methods do not require day-to-day involvement and include:

- **Digital Certificates** – these include existing X.509 digital certificates issued from Entrust's managed digital certificate service or a third party to authenticate users. Certificates can be stored locally or on secure devices like smart cards and USB tokens.

Organizations without an in-house PKI can obtain certificates via Entrust's hosted PKI services.

- **IP-Geolocation** - Authenticated users can register locations where they frequently access the corporate network. During subsequent authentications the Entrust IdentityGuard server compares current location data — country, region, city, ISP, latitude and longitude — to those previously registered. Hence organizations can require enhanced authentication only when the values don't match or when the values are outside of policy.
- **Device Authentication** - Authenticated users can register a computer or device that is frequently used to access the organizational network. An encrypted profile of the registered computer is created and stored. During subsequent authentication, the Entrust IdentityGuard server creates a new profile and compares it against the stored value. Step-up authentication is required only when the profiles don't match.
- **Device Reputation** – Encrypted profiles of devices (such as PC's, laptops, tablets and mobile phones) are matched against a repository of over 2 billion devices to assess the likelihood of authentication transactions being fraudulent. Weighted risk scores are based on a sophisticated real-time risk assessment of the device from which the authentication request is made.

2.2.2 Physical Form Factor Authenticators

Physical form factors are physical devices that users carry and use when authenticating. Entrust offers a range of physical authentication devices:

- **One-Time-Passcode Tokens -** Entrust offers two versions of the one-time-passcode (OTP) token. The Entrust IdentityGuard Mini Token is OATH-compliant and generates a secure eight-digit passcode at the press of a button. The OATH-compliant Pocket Token offers additional features including PIN unlock prior to generating the passcode, in addition to a challenge-response mode. OTP tokens are also available with integrated camera; often used where a QR code is displayed in a web browser, ATM screen, Point of Sale terminal, or printed contract. All of these transactions could be digitally signed by the token.
- **Display Card** - The Entrust Display Card provides the same functionality as the token in a credit card format. In addition to providing an OATH-compliant, one-time passcode, the Display Card includes a magnetic stripe and can optionally include a PKI or EMV (Europe Mastercard and Visa) chip.
- **Grid Authentication** - The Entrust-patented grid card is a credit card-sized authenticator consisting of numbers and characters in a row-column format. Upon login, users are presented with a coordinate challenge and must respond with the information in the corresponding cells from the unique grid card they possess.
- **One-Time-Passcode List** - End-users are provisioned with a list of randomly generated passcodes or transaction numbers (TANs) that are typically printed on a sheet of paper and distributed to end-users. Each passcode is used just once.

- **Biometrics** - Entrust leverages biometric fingerprint data to provide a balance between authentication strength and user convenience for Microsoft® Windows® logon. To protect user privacy, fingerprint data is stored in a database or on an Entrust smartcard as an encrypted Hash — and this is compared to the actual fingerprint provided at the time of authentication. This stored Hash cannot be reverse-engineered.

2.2.3 Non-Physical Form Factor Authenticators

Non-physical form factor authentication provides methods of verifying user identities without requiring them to carry an additional physical device.

- **Knowledge-Based Authentication** – (KBA) challenges users to provide information an attacker is unlikely to possess. Questions presented to the user at the time of login are based on information (referred to as authentication secrets) that was supplied by the user at registration or based on previous transactions or relationships. Entrust IdentityGuard allows the administrator to determine the number and type of questions asked.
- **Out-of-Band Authentication** - authentication leverages an independent and pre-existing means to communicate with the user to protect against attacks that have compromised the primary channel. For example, by generating one-time confirmation numbers that can be transmitted along with a transaction summary to the user via email or SMS, or through voice to a registered phone number. OOB Push Transaction Authentication is also available. User options include 'Confirm', 'Deny' and 'Concern'.
- **Entrust IdentityGuard Mobile** – the Entrust IdentityGuard SDKs, which can be used to build this functionality into the customer apps, support mobile authentication, transaction verification, mobile smart credentials, and transparent authentication technology with an advanced software development kit. It supports the OATH standard for time-based OTP, as well as out-of-band transaction signatures.
- **Entrust IdentityGuard Mobile Soft Token** – which is available for Apple and Android - supports OATH time based OTPs, QR Codes, OOB push. A desktop client is also available. Offline OTP authentication is supported on both the mobile and desktop app.
- **Mobile Smart Credentials** - eliminate the need for physical smartcards by transforming popular mobile devices into mobile credentials for enterprise-grade authentication. These credentials can be used with Bluetooth and near-field communication (NFC) technology for greater convenience and secure connectivity.
- **SMS Soft Tokens** – are like the platform's out-of-band authentication capabilities, Entrust IdentityGuard SMS soft tokens, enable the transmission of a configurable number of one-time passcodes (OTP) to a mobile device for use during authentication. This approach delivers the strength of out-of-band authentication without the concern for constant network availability, delivery timing or software deployment to a mobile device.

- **eGrid** - An alternative to hardware tokens, eGrid cards are sent to users via the Web or as a PDF, which can be stored on a machine or mobile device for access, eliminating the need to carry a physical form factor.
- **Strong Username & Password** - Entrust IdentityGuard can provide a strong second factor of authentication to an organization's existing username and password infrastructure.

2.2.4 Mutual Authentication

Mutual authentication provides a mechanism for the user to be confident that the system that they are logging onto is genuine so that they do not divulge their credentials to a fraudulent or spoofed entity. Entrust IdentityGuard provides the following mutual authentication methods:

- **Image & Message Replay** - Upon registration, the user selects an image from an image bank and creates a message. During subsequent logins the image and message are presented to the user.
- **Grid Serial Number Replay** - During login, the serial number of the user's unique grid card is presented to the user.
- **Grid Location Replay** - During login, the user is presented with the values of several cells from their unique grid card.
- **Entrust EV Multi-Domain SSL Certificates** - Organizations can deploy Extended Validation (EV) SSL certificates, which confirm the Web site's authenticity by displaying a green address bar — an obvious trust indicator for the end-user.

2.2.5 Adaptive Authentication

The Entrust IdentityGuard platform supports adaptive authentication. The toolkit allows organization to evaluate a broad range of contextual attributes, including the identity of mobile devices or PCs, geo-location, geo-velocity, user behaviour and user credentials. It can also consider inputs from device reputation, external fraud and analytics sources.

2.3 Integration with Enterprise Infrastructure

The Entrust IdentityGuard platform works within the organization's existing infrastructure. The platform can run as a stand-alone authentication server or be deployed into leading application servers, including IBM and Oracle, interfacing to current sign-on applications via Web services. This allows integration with current applications built on J2EE, .NET and legacy platforms.

It does not require additional client or server software for VPN remote access. It interoperates with various IP-SEC and SSL VPN applications from Cisco, Checkpoint, Juniper Networks, F5 and others. The solution also includes 802.1x native support.

Organizations can exploit standard Web service APIs to directly integrate into an enterprise portal, or use the suite of integrated applications such as Microsoft® Outlook® Web Access, Citrix Xen App, or WAM (Web Access Managers) such CA Single Sign-on, IBM Tivoli Access Manager or Oracle Access Manager.

The solution uses existing repositories for storing identity information including support for LDAP directories such as Oracle Directory Server, Microsoft Active Directory, Novell, and databases from Oracle, IBM and Microsoft.

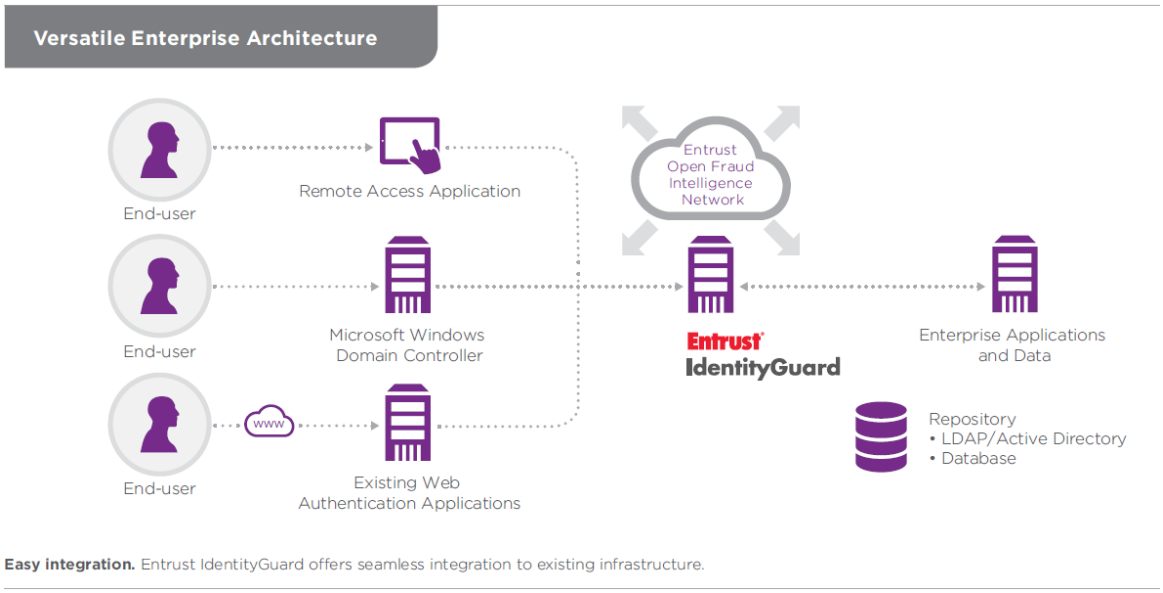

Figure 2: Entrust IdentityGuard Architecture (reproduced with permission from Entrust Datacard)

2.4 Management Interface

Entrust IdentityGuard provides an administrative dashboard that for managing user enrolment, roles, group and policy management, bulk operations and more. It enables authorized managers to generate usage reports, assign and manage certificates, and oversee any IP blacklists used for risk-based authentication.

2.5 US PIV Standard

The NIST standard FIPS 201 specifies Personal Identity Verification (PIV) requirements for US Federal employees and contractors. Entrust Datacard is a US Federal government-approved provider of PIV and PIV-I credentials.

3 Strengths and Challenges

Securely authenticating users is a major problem given the increasing threats from cyber-crime. Entrust IdentityGuard for Enterprise provides a comprehensive solution for enterprises to select and manage the way in which organizational users are authenticated to access both physical and logical assets. The company has thousands of customers across the globe, serving millions of users, in both the B2C and B2E space. A significant portion of its customer base is banking/finance.

It consolidates the management of identities and credentials into a single software platform. This covers the processes of selecting the appropriate authentication method, issuing credentials, on-going management and finally revocation. This helps to simplify management and reduce costs.

Entrust IdentityGuard is a full-featured adaptive authentication solution that supports a wide range of authenticators, including Knowledge Based Authentication, out-of-band push mobile apps, OATH OTPs, biometrics, and 3rd party authenticators. It also connects to WAM and federation systems via SAML, RADIUS, and Kerberos.

Entrust IdentityGuard's risk analytics engine can evaluate up to 50 different risk-related data points. Administrators can rate and weight the factors via policies. The product also allows user behavioural profiling. The risk engine also can integrate with 3rd party Cyber Threat Intelligence providers. Entrust has an aggressive schedule for on-boarding additional Cyber Threat Intelligence providers, giving it an edge in the security innovation area.

However, although Entrust IdentityGuard integrates with Entrust Open Fraud Intelligence Network it does not contain inbuilt user and entity behaviour analytics. This is increasingly an important requirement since most cyber-crime involves the use of hijacked or stolen credentials. In addition, it does not contain its own inbuilt directory, but it does integrate with most directory services commonly found in use in organizations.

Authentication is only one of the many processes involved in identity and access management and so integration with tools that support the other processes is important. Entrust IdentityGuard integrates with a range of widely used third party tools and technologies. IdentityGuard can output data via syslog to SIEM and RTSI systems. It also offers integration to GRC partner SailPoint. It does not provide out-of-the-box integration with Service Request Management systems, which could be an issue for some potential deployments. Support for FIDO authentication is planned.

Entrust IdentityGuard provides a well-rounded adaptive authentication feature set. Entrust is also responsive to customer's requirements. Its support for a wide range of authentication mechanisms, an advanced risk engine, and the inclusion of cyber threat intelligence put IdentityGuard on the short list for organizations looking for adaptive authentication capabilities.

Strengths	Challenges
• Single software platform supports a wide range of authentication methods; • Large selection of innovative authentication mechanisms, including biometrics, OTP, push out of the box; • Standalone, but with identity federation support and WAM integration available; • Sophisticated risk analytics engine • Integration with cyber-threat intelligence providers; • Manages the full lifecycle for credentials from a single point; • Integrates with a range of third party products that support the other identity and access management processes.	• Lacks integration with Service Request Management systems; • Some solutions offered as specifically tailored for banking and finance, this can limit its appeal for use in other verticals; • Lack of built in analytics for user activity; • Does not include an inbuilt directory but provides integration with a range of common directory services.

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

Kuppinger Cole Ltd.
Sonnenberger Strasse 16
65193 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com