Entrust® Securing Digital Identities & Information

Authentication and Fraud Detection Buyer's Guide

Entrust, Inc.
North America Sales: 1-888-690-2424
entrust@entrust.com
EMEA Sales: +44 (0) 118 953 3000
emea.sales@entrust.com

November 2008

Table of Contents

Introduction

This guide has been developed to assist organizations in identifying their requirements for an authentication and fraud detection solution, and in selecting a solution that meets their security needs. It outlines key questions that should be considered during the selection process to ensure that the chosen solution will address the organization's requirements both from a business and operational perspective.

Organizations are being challenged to implement cost-effective strong authentication and fraud detection solutions that meet the operational needs of their end-users while complying with regulatory requirements. This takes place not only within the context of their internal networks, but increasingly in broader external customer- and partner-network environments.

Whether responding to regulatory compliance pressures, trying to secure collaboration with business partners, looking to reduce costs by using the online channel or simply to strengthen consumer confidence in using this channel, organizations are looking for a solution architected specifically to address such challenges.

This document has been structured to provide an understanding of why authentication and fraud detection is needed and to assist with determining your organization's specific requirements. Things to consider have been provided in the form of questions and checklists in Sections 2 and 3 of this guide to help your organization during the vendor evaluation process.

1 What are Authentication and Fraud Detection? Why Do I Need Them?

Organizations are relying on the online channel more than ever before to reach employees, partners and consumers. At the core of performing online transactions is the need for mutually recognized identities. Users need to feel confident that they are dealing with the intended organization. Likewise, the organization needs to have confidence in the identity of the user. Without this mutual trust, online transactions cannot be completed without significant risk of fraud and negative impacts on service adoption and customer retention rates.

The majority of systems deployed today rely on basic usernames and passwords to protect the online channel. However, it is widely recognized that this is no longer sufficient. Attacks such as phishing, man-in-the-middle or other malware are able to defeat this security, causing a risk to organizations not only because of the financial losses but, more importantly, because user confidence in online services is undermined. This prevents organizations from fully realizing the savings from moving transactions from traditional to online channels.

In addition, simple usernames and passwords are no longer enough to prevent breaches, protect privacy and achieve compliance. Increasing regulatory pressures are dictating that organizations roll out new security systems to achieve regulatory compliance. Such initiatives include:

- PCI-DSS (Payment Card Industry Data Security Standard)
- SOX (Sarbanes-Oxley Public Company Accounting and Investor Protection Act)
- SEPA (Single Euro Payments Area initiative of the European Payments Council (EPC), which also covers the Payment Services Directive (PSD) of the European legislators)
- FPI (Faster Payments regulatory regime in the UK replacing the current three-day clearing process)
- Basel II (Banking laws and regulations issued by the Basel Committee on Banking Supervision to create international banking standards)
- FFIEC (Federal Financial Institutions Examinations Council)
- Red Flag (Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003 (FACTA))

As a result, stronger authentication and fraud detection methods must be deployed to a wider audience, efficiently and cost-effectively.

There are three primary approaches to addressing these issues:

- strong authentication
- fraud detection
- risk-based authentication

Depending on what your organization is trying to accomplish in the online channel, one or more of these approaches will be suitable. Each approach is described in this section, as well as the key business drivers they address.

1.1 Strong Authentication

Strong authentication, also known as multifactor authentication, involves the use of two or more pieces of information to verify a person's identity for security purposes. This identity information, commonly referred to as authentication factors, are:

- Something the user uniquely **has**, such as a hardware or software token
- Something the user uniquely **knows**, such as a password or PIN
- Something the user uniquely **is** or **does**, a biometric such as a fingerprint, a signature or a voice print

Combining two or more of these factors provides higher levels of assurance that the person being authenticated truly is who they claim to be. It also decreases the likelihood that it is an attacker posing as a legitimate user.

Strong authentication is suitable for remote access to corporate networks by employees and business partners, or for consumers carrying out higher-value transactions, such as money transfers in online banking. It also helps to address regulatory requirements.

When considering strong authentication solutions it is important to balance the cost and usability of the solution with the risk involved in the process being protected. For instance, if you are providing access to a low-risk application to a group of technology novices, it does not make sense to deploy a costly and technologically complex authentication solution. However, you may also have another group of users dealing with highly sensitive information or processes for whom a stronger method of authentication is more appropriate. For this reason it important to look for a versatile authentication server; a single authentication platform, which allows you to implement a number of authentication methods to diverse user groups while providing the flexibility to change these authentication methods over time, as threats and user preferences change.

1.2 Fraud Detection

Fraud detection refers to the process of monitoring, detecting and preventing fraudulent activities by looking for anomalies in users' behaviors and transactions. This is done by examining:

- **Access** – fraud detection determines where and when the user is logging in and compares this to typical access patterns to find anomalies.
- **Transaction** – fraud detection looks for unusual transactions, such as those involving high values or large bill payments to new payees.
- **Behavior** – robust fraud detection solutions monitor the sequence of transactions within and across user sessions to spot fraudulent activity patterns (e.g., completing a change of address and then ordering new checks). It also examines and compares user behaviors. For

instance, fraud detection will monitor how a user navigates a site and compare this to previous navigational sequences to identify if the user is logging in at an unusual time of day, performing an unusual transaction, etc.

Fraud detection provides transparent monitoring and can help stop suspicious transactions by proactively contacting customers, blocking access or requesting additional authentication. It is also invisible to attackers and difficult to circumvent.

This approach is most suitable for transaction-based online applications, such as banking where the risk of financial loss is high, as is the risk of loss of consumer confidence in the organization's brand.

1.3 Risk-Based Authentication

Risk-based authentication allows an organization to apply the appropriate amount of authentication and fraud detection based on the risk associated with the user's transaction while minimizing the impact on the end-user experience. With risk-based authentication, an end-user is only interrupted when there is an increased concern about the session based on risk, transaction and behavior patterns. End-users are not faced with stronger interactive authentication mechanisms when they are completing routine transactions, only when the risk of the transaction warrants stronger or "stepped-up" authentication.

Risk-based authentication is suitable for transaction-based online applications, such as online banking where customer authentication should be as simple and transparent as possible unless suspicion of fraud exists.

2 Determining Your Requirements

In order to assess a vendor's solution, you must first determine your specific business and security requirements. Listed below are some guiding questions to assist you with determining your organization's needs from a strong authentication and fraud detection perspective. These questions will also enable you to build a profile of your organization and its users that will assist in the assessment of what solution best fits your users' needs. These questions are provided in a convenient self-assessment table with checkboxes to help you identify your requirements.

Note: This is not intended to be an exhaustive list. It is meant as a starting place to assist you in your requirements gathering process. Blank spaces have been left at the end of the table for additional criteria.

Criteria	Yes	No	Notes
What end-user diversity do I have?			
• Customers/Consumers			
• Partners			
• Employees			
• Contractors			
• Other:			
Where are my end-users located?			
• In the same location			
• In remote locations			
• Internal to the corporate network			
• External to the corporate network			
• Other:			
Do I have control over the users and their computers?			
• Am I able to deploy client side software?			
• Can I mandate end-user security policy and authentication methods?			
• Does control vary across my user groups (e.g., consumers, eternal business partners, etc.)?			
• Other:			

Criteria	Yes	No	Notes
What are the users going to be doing?			
• Accessing information			
• Completing financial transactions online			
• Purchasing merchandise online			
• Online-banking			
• Sending and receiving sensitive and/or personal information			
• Other:			
What am I trying to protect?			
• Remote access to my network			
• Desktops			
• Web applications like OWA			
• Network admin access			
• Other:			
What is the profile of my users?			
• Technologically aware			
• Little to no awareness			
• Diverse technical capability			
What do I want my user experience to be?			
• Do I want the authentication to be transparent?			
• Will my users accept a physical factor for authentication?			
• Do I want to leverage something the user already has, such as a cell phone?			
• Do I want to offer my users a choice of authenticators?			
How will my organization change over time?			
• Do I want/expect to extend access to a broader group in the future?			
• Do I need the flexibility to change or augment the method of authentication in the future?			

Criteria	Yes	No	Notes
Are my security needs across the different user groups the same?			
• Does each group access equally sensitive material (Admin vs. HR, Finance vs. Executive, Consumer vs. Partners)?			
• Is the impact of a breach significant enough to justify stronger authenticator for certain groups (e.g., high-net value clients vs. regular clients)?			
What are my project requirements?			
• Do I have existing infrastructure that I need to leverage?			
o Applications			
o Authentication			
o Other:			
Additional Criteria:			
•			
•			
•			
•			
•			
•			
•			

3 Key Considerations When Selecting a Strong Authentication and Fraud Detection Solution

The following questions have been provided to assist your internal project team to determine what questions need to be asked of a potential vendor. This is not intended to be an exhaustive list. It is meant as a starting place to assist you in your review process.

3.1 Flexible Authentication Methods

3.1.1 Is there a requirement for specialized authentication hardware?

3.1.2 Does the solution provide a single authenticator or a broad range of authentication choices to meet the needs of a diverse user population?

3.1.3 If the solution does support more than one type of authenticator, is there a variety of authenticators to address varying security requirements? List which types?

3.1.4 Are there transparent authentication methods available for minimal user impact?

3.1.5 Does the solution offer stronger interactive authentication capabilities if "stepped up" or stronger authentication is required?

3.1.6 Does the solution offer second-factor authentication options for high-risk transactions?

3.1.7 Are these authenticators supported by a single platform? If so, is this platform architected to easily incorporate new authentication methods?

3.2 Fraud Detection Capabilities

3.2.1 Does the solution require integration or changes to back-end applications to identify what data to capture?

3.2.2 Does the solution capture all data from the channel monitored or only a subset?

3.2.3 Does the solution monitor all transactions? If not, list which are and which are not.

3.2.4 Does the solution monitor within the application? Does an event need to be triggered before the analysis takes place?

3.2.5 Where does fraud detection monitoring take place? At the application level? At the network level?

3.2.6 How does the solution adapt to new fraud patterns? How quickly can it start catching these new fraud patterns?

3.2.7 Does the data captured for analysis stay in the control of the organization? If not, what data leaves the organization? Does that data leave the country?

3.2.8 Is there a method of sharing or receiving information regarding new fraud patterns with others? If so, what information does it include?

3.2.9 Are the fraud rules updated on an ongoing basis?

3.2.10 Are alerts and historical analysis included?

3.2.11 Can other channels be monitored in addition to the online channel? If so, which ones?

3.2.12 How quickly can a fraudulent transaction be stopped?

3.2.13 Can the transaction be blocked?

3.2.14 Can alerts be triggered?

3.2.15 Can the transaction be stopped pending a fraud analyst's review?

3.2.16 Can "step-up" or stronger second-factor authentication be triggered based on risk score?

3.2.17 Can forensics be carried out on historical transactions to find additional incidents of an identified pattern?

3.2.18 Does the solution provide complete transaction records?

3.2.19 Does the solution provide data mining capabilities?

3.2.20 Does the solution replay historical data against new rule sets?

3.2.21 Does the solution provide enough audit information to take all appropriate action?

3.2.22 Does the solution provide both access and behavioral fraud detection?

3.2.23 Does the solution provide real-time analysis of transactions as they occur?

3.3 Deployment and Usability

3.3.1 Does the solution easily integrated into an organization's environment with minimal impact to existing infrastructure?

3.3.2 Does the solution integrate with existing authentication applications, Web access control solutions and user repositories?

3.3.3 Is the solution intuitive for administrators and end-users?

3.3.4 Are the available authentication methods easily understood across diverse communities?

3.3.5 Does the solution leverage existing devices and knowledge already possessed by the user?

3.3.6 How does the solution ensure minimum impact to users unless there is a high risk of fraud?

3.3.7 Does the solution cost-scale with you business use and volume or do you incur significant up-front costs regardless of deployment size?

3.3.8 Are there different costs associated with different authentication methods?

3.3.9 Can different user groups be provided with different authentication methods (e.g., tokens for higher-risk transactions and lower cost grid cards for lower-risk transactions)?

3.3.10 Can different authenticators be added to the solution as new methods are developed?

3.3.11 Does the solution provide centralized points of security policy administration and enforcement?

3.3.12 How are new rules created or modified to respond to new attacks? Who must be involved? How quickly can this done?

3.3.13 What type of self-service capabilities are offered?

3.3.14 What type of reporting and auditing is possible? Who controls these capabilities?

3.3.15 Does the solution have a range of methods to catch fraud besides simply looking at the device profile of the user's system?

3.3.16 Is the solution offered as a hosted service? If so, what happens if the service is discontinued or the customer wants to migrate to a new solution?

3.3.17 Is the solution kept up to date with real-time world event data? Is there a means of collecting and feeding this information into the system? If so, is this information limited in any way?

3.3.18 Is transactional data collected even if no fraud alerts are triggered? If so, is it possible to look at past history to investigate fraud or test new rules?

3.3.19 How does the solution integrate within your banking application? Do I need to change my application right from the outset?

3.3.20 How is transactional data collected? Does the solution require the deployment of Web filters on all existing Web servers? Is a non-intrusive network-based method supported, or does the data have to be collected within each application being protected?

4 Vendor

4.1 Corporate Information — briefly describe the following:

4.1.1 Corporate profile

4.1.2 Number of employees

4.1.3 Corporate headquarters and other office locations

4.1.4 Financials (copy of 10K report or annual report)

4.1.5 List any product awards won in the last five years

4.1.6 List any relevant experience and customer deployments. Are these customers referencable?

4.1.7 Describe your corporate quality and security assurance process.

4.2 Technical Support

4.2.1 Describe your technical support options, policies and procedures.

4.3 Documentation and Training

4.3.1 Describe your method of providing documentation and training for your products.

4.4 Strategic Partnerships

4.4.1 Describe your strategic relationships or vendor alliances you have regarding the delivery of digital signatures, authentication, fraud detection and encryption products and services.

4.5 Services

4.5.1 Does your company provide professional services capabilities on a global basis?

4.5.2 Does your company have a dedicated solution design and deployment team to enable customer input to product enhancements?