IT'S 2 A.M. DO YOU KNOW WHERE YOUR CERTIFICATES ARE?

Proven tools to help simplify certificate discovery management.

Table of contents

1 **Introduction**
Page 3

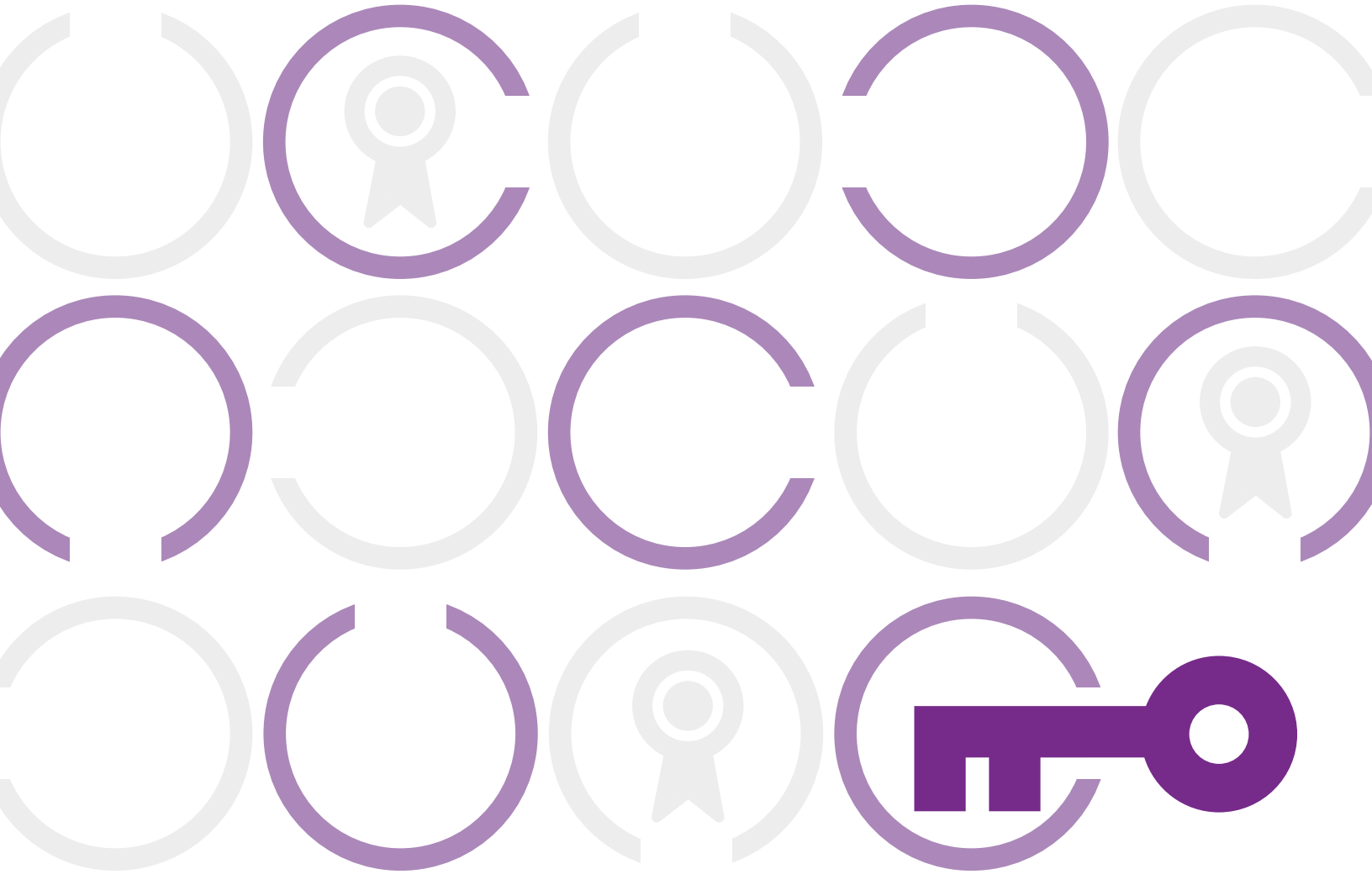
2 **Common Certificate Challenges**
Page 4

3 **Policy Management**
Page 5

4 **Certificate Discovery**
Page 6

5 **Entrust Solution**
Page 6

6 **Conclusion**
Page 7



Introduction

Creating cryptographic keys is a simple matter; many common software applications and operating systems have the ability to do this. Obtaining a certificate for a key from an internal commercial or open-source software certification authority (CA) is also a simple matter.

Even obtaining a certificate from a "publicly trusted" certification authority may be easier than you might expect, as some publicly trusted SSL CAs operate lax controls over the authorization of certificate requests.

In pursuit of sound information governance, responsibility for managing keys and certificates is commonly centralized within an enterprise. But, it can be very difficult for a central authority to enforce key management policy in practice. Even legitimately authorized certificates can be easily copied and mounted on other systems throughout the enterprise.

As a result, it is difficult to get a complete and accurate view of the totality of keys and certificates in use across an enterprise at a particular point in time.

Common Certificate Challenges

Certificates are used to authenticate and grant access to critical resources. So, improperly managed certificates can result in unauthorized access. On the other hand, if a certificate expires unexpectedly, it can lead to denied access, or, at least, to a change in user experience (e.g., appearance of a trust dialog box in the browser window) that can result in user uncertainty and from there to an increase in support costs. Or worse, a reduction in revenue.

Even if actual expiry can be averted, the inability to form an accurate and up-to-the-minute view of the keys and certificates and their properties, as they exist everywhere in the enterprise, represents a significant obstacle to sound management control — and perhaps even to meeting compliance requirements.

"A common reaction to this problem is to have an administrator manually track known certificates through its various lifecycle stages. But this approach is costly, and results are inevitably incomplete and out-of-date."

Policy Management

Organizations serious about securing information assets and protecting their users develop and implement an information technology security policy that addresses (among other things) the management of keys and certificates. Central to the achievement of an adequate level of assurance is the choice of a well-managed certification authority — whether that is an in-house or out-sourced private authority, or a publicly trusted authority.

The CA is responsible for aspects of key management, including the quality of keys, responsiveness to revocation requests, and rigor in the issuance approval procedure. Other important components of policy include internal procedures, such as assigning authority to request and receive certificates for production systems. These are essential building blocks of both sound management and regulatory compliance.

Even at a relatively modest scale, monitoring compliance with corporate security policy can be a labor-intensive, and therefore costly, function. Hence, compliance-monitoring tools can be a cost-effective approach.

Certificate Discovery

The essential first step to routine and confident certificate management in the enterprise is to obtain a complete and up-to-the-minute view of all the certificates in the enterprise. Once certificates have been located, their properties can be examined, evaluated against applicable policy, and reported to responsible authorities.

Significant certificate properties include: the subject domain name or address; the domain to which they are attached; cryptographic key properties (including algorithm, size, and strength); issuing authority; certificate quality; revocation status; list of subject alt names; and expiry date.

In addition to policy covering which individuals are authorized to manage certificates for the organization, there should be enterprise-wide policy covering all certificate properties. Once reliable reports can be compiled and distributed, it is a simple matter to identify and resolve policy violations. And alerts of imminent outage can be sent for resolution to those responsible for maintaining system availability.

Entrust Solution

Entrust has a proven, world-class solution that solves this challenge — and it's appropriately named Entrust Discovery.

The Entrust Discovery solution comprises several components:

Discovery Agent
An instance of the Discovery Agent is installed on every network segment in order to ensure that all internal machine ports can be examined for the presence of a certificate. The Agent crawls its local network, discovering machine ports that are protected by a certificate. This task can run on a predetermined schedule or ah-hoc. The resulting data is then exported to the Discovery Manager via either a manual or automated process.

Discovery Crypto API (CAPI) Scanner
The CAPI Scanner can be run centrally or distributed, and will query the Crypto API store of machines running Windows. Certificate information is then collected automatically and exported to the Discovery Manager for further analysis.

Discovery Manager
The Discovery Manager consolidates reports from all the agents and scanners in the enterprise, providing the administrator with suitable views into the data. The administrator can immediately identify certificates that are in violation of corporate policy, and those that will require action, such as replacement, in the upcoming period.

An enterprise may operate the Discovery Manager on its own premises, or Entrust can host the Discovery Manager as a service on behalf of a customer.

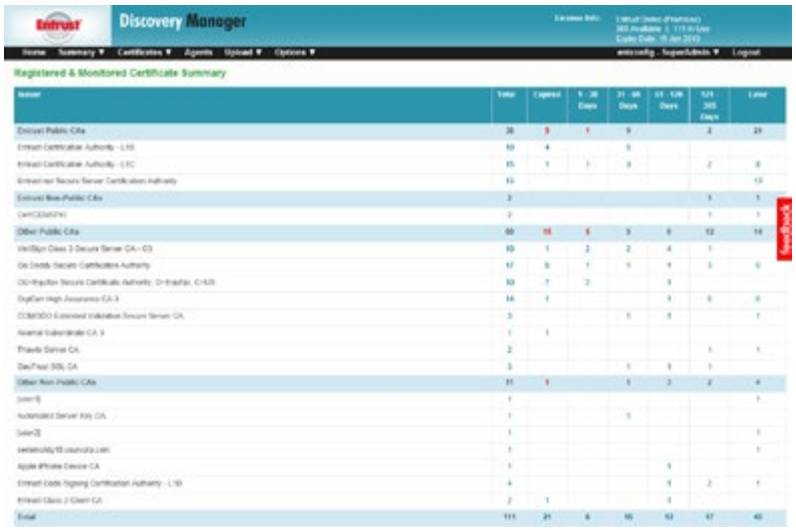


Figure 1:
Entrust Discovery's easy-to-use interface

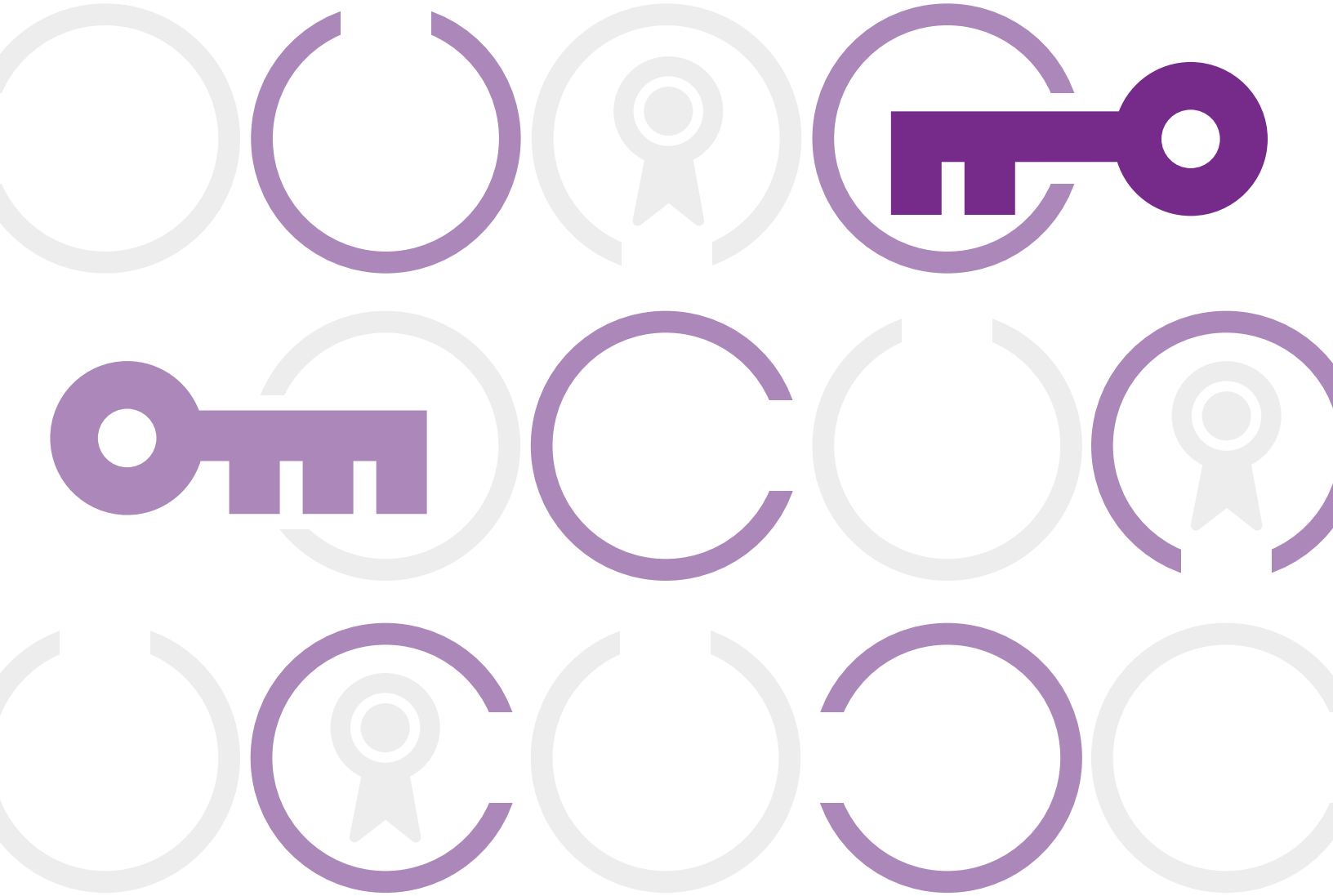
In the case of non-conformant certificates, the private key can be deleted and the issuing authority asked to revoke them. If certificates are discovered that have been issued by an unapproved authority, then timely corrective action can be taken.

Similarly, if weak keys are discovered, these can be rapidly replaced by keys of acceptable strength.

Conclusion

The tools to create keys and certificates are readily available. Yet, managing cryptographic keys and certificates is deceptively complicated. And, the consequences of a failure can be anything from a service outage to a compliance violation.

Nevertheless, these issues can be addressed by relatively simple measures. Tools are available to report on certificates and their properties wherever they may be deployed in the enterprise. The discovery tools available from Entrust offer one of the most cost-effective solutions to these problems.



About Entrust Datacard

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide. For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

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

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

Twitter Facebook Youtube LinkedIn Google+ RSS