



It's 2 a.m. Do you know where your certificates are?

Proven tools to help simplify certificate discovery, management

Get this
White Paper





Contents

Introduction	3
Policy Management.....	4
Certificate Discovery.....	5
Entrust Solution	6
Discovery Agent	6
Discovery Crypto API (CAPI) Scanner.....	6
Discovery Manager	6
Certificate Revocation	7
Conclusion.....	8
Entrust & You	9



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.

“

... 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.

”



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.

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.

“

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.

”



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 agents and scanners in the enterprise, providing the administrator with suitable data views.

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.



Certificate Revocation

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.

Entrust		Discovery Manager					License Info: Entrust Demo (Premises) 389 Available 111 In Use Expiry Date: 15 Jan 2013	
Home	Summary ▼	Certificates ▼	Agents	Upload ▼	Options ▼	entconfig - SuperAdmin ▼ Logout		
Registered & Monitored Certificate Summary								
Issuer	Total	Expired	1 - 30 Days	31 - 60 Days	61 - 120 Days	121 - 365 Days	Later	
Entrust Public CAs	38	5	1	9		2	21	
Entrust Certification Authority - L1B	10	4		6				
Entrust Certification Authority - L1C	15	1	1	3		2	8	
Entrust.net Secure Server Certification Authority	13						13	
Entrust Non-Public CAs	2					1	1	
O=YCEMSPKI	2					1	1	
Other Public CAs	60	15	5	5	9	12	14	
VeriSign Class 3 Secure Server CA - G3	10	1	2	2	4	1		
Go Daddy Secure Certification Authority	17	5	1	1	1	3	6	
OU=Equifax Secure Certificate Authority, O=Equifax, C=US	10	7	2		1			
DigiCert High Assurance CA-3	14	1			1	6	6	
COMODO Extended Validation Secure Server CA	3			1	1		1	
Akamai Subordinate CA 3	1	1						
Thawte Server CA	2					1	1	
GeoTrust SSL CA	3			1	1	1		
Other Non-Public CAs	11	1		1	3	2	4	
[user1]	1						1	
Automated Server Key CA	1			1				
[user2]	1						1	
sedemoidg10.yourcorp.com	1						1	
Apple iPhone Device CA	1				1			
Entrust Code Signing Certification Authority - L1D	4				1	2	1	

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



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.



Entrust & You

More than ever, Entrust understands your organization's security pain points. Whether it's the protection of information, securing online customers, regulatory compliance or large-scale government projects, Entrust provides identity-based security solutions that are not only proven in real-world environments, but cost-effective in today's uncertain economic climate.

A trusted provider of identity-based security solutions, Entrust empowers 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 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, Texas 75240

Sales

North America: 1-888-690-2424
EMEA: +44 (0) 118 953 3000
Email: entrust@entrust.com

follow us on
twitter  **tweet**