CERTIFICATE MANAGEMENT: POLICY, AUTOMATION AND ENTRUST DATACARD VALUE

Sandy Carielli, Security Technologies Director, Entrust Datacard
INTRODUCTION

PKI is becoming a critical underpinning to help organizations succeed as they roll out new digital business models. Establishing a trusted infrastructure through PKI will help businesses take smart risks, evolve quickly and manage relationships with customers, partners, vendors and employees more effectively.

Certificate management is a crucial part of a robust PKI implementation, ensuring visibility and adherence to policy throughout the certificate lifecycle: from identity vetting, to issuance, to renewal to revocation. As Gartner noted in its recent report, “PKI is Gearing Up for the Internet of Things” (August, 2016):

“Certificate management is the issue for which Gartner clients seek the most guidance, and it is becoming increasingly important.”

Good certificate management is a combination of well-defined policy and the right tools and automation to implement it. In this paper we will discuss some of Entrust Datacard’s best practices for certificate management policy and how Entrust PKI certificate management features and automation can help organizations simplify and streamline their implementation, enabling them to move at a faster pace by trusting their infrastructure and applications.

In order to develop a comprehensive certificate management policy and leverage Entrust Datacard certificate management automation most effectively, let’s start with two questions:

- What are the all of the ways I want to use certificates in my organization?
- For each use of certificates, what is the required assurance level?
CERTIFICATE TYPES

Chances are, you have multiple use cases for PKI. For example, you may be using certificates for mobile devices, remote access, code signing and public-facing web applications via SSL. You may also be issuing certificates for Registration Authorities (RAs) in your organization. Each use case should be defined as a different certificate type (with its own defined key usage and enhanced key usage extensions), to which you will assign a specific assurance level, set of policies and automation behaviors.

Some organizations we’ve worked with have had ten or more different types of certificates to manage, including:

- Windows user and computer certificates
- Non-Windows user and computer certificates (e.g., Mac, Linux, Chrome)
- Mobile device certificates
- SSL certificates
- SSL visibility device certificates (aka HTTPS Proxy)
- Domain controller certificates
- Registration Authority (RA) certificates
- Local RA (LRA) certificates
- WNES server certificates
- Application server certificates
- VPN certificates
- Code signing certificates
- Encryption certificates (email, files, database, etc.)
- Non-repudiation certificates

What is PKI?
For a refresher on the basic concepts and key components of a PKI, please check out https://www.entrust.com/what-is-pki/
DEFINING ASSURANCE LEVELS

At Entrust Datacard, we find it helpful to define a few assurance levels and classify each type of certificate into a level. This helps Entrust Datacard and our customers have a common understanding of the level of automation required during the certificate lifecycle (discussed below). Assurance levels are closely tied to identity vetting, the first stage in the certificate lifecycle.

Our consultants typically define three assurance levels: basic, medium and high.

High
High level assurance requires in-person vetting with a Registration Authority (RA) or Local Registration Authority (LRA). It often requires the person being given the certificate to sign agreement and verification forms. Keys are typically generated and stored in FIPS 140-2 Level 2 hardware cryptographic modules (e.g. smart cards or USB cryptographic modules). It’s important to note that High assurance authentication and signature keys must be generated by the users themselves, rather than a CA, RA or LRA on behalf of the user.

This high level of assurance is not suitable for many certificate types (in person vetting for all mobile device owners, for example, would be unwieldy), but it is critical for your most sensitive and authoritative types, such as RAs and users requiring high levels of assurance (perhaps your CFO and general counsel).

Because high assurance certificates require in-person vetting, the certificate issuance process cannot be fully automated. Renewal and revocation can be fully automated, if the organization so chooses. In some cases, organizations do not want high assurance certificates to be automatically renewed; when it’s time for renewal, these high assurance subscribers must go through the initial enrollment process all over again.

Medium
Medium level assurance will be the choice for most of your certificate types, including many device certificates. For medium level assurance, identity vetting can be in-person or remote; remote vetting can be based on user credentials approved by the PKI Policy Authority, such as AD data. Users and device owners do not have to sign any agreements or verification forms. Software cryptographic modules (or FIPS 140-2 Level 1) are sufficient for generating and storing keys.

Unlike at the High level, medium assurance authentication and signature keys can be generated by the CA, RA or LRA, if necessary (though the user or device often is still the one to generate the keys). At medium level assurance, it is also possible to automate certificate issuance, renewal and revocation.

Basic
At the basic level, there is minimal identity vetting and no particular guidelines for key generation and storage. Sounds overly permissive? It is...and it is often limited to test environments. If basic assurance is used in production at all, Entrust Datacard recommends additional controls, such as a short certificate lifetime and manual renewal.
THE CERTIFICATE LIFECYCLE

There are four stages in the lifetime of a certificate, with different policies and automation options for each stage.

CERTIFICATE LIFECYCLE MANAGEMENT

1. VETTING
2. ISSUANCE
3. RENEWAL
4. REVOCATION

Key Decision
Assurance Levels

HIGH
Our root of trust allows for true high-assurance security. Not offered by PKI point solutions.

MEDIUM
The scalability of our PKI solutions lets you scale as your digital business grows.

BASIC
Simplify basic certificate management by consolidating on a single CA.

1. Initial Identity Vetting
How do you assure the identity of the user or device in order to issue the certificate? You might not think about this stage in the lifecycle as frequently, but getting it right is critical to the overall assurance of the system.

The identity vetting stage will certainly be manual for high assurance certificates but can be automated (and even transparent to the user) for medium and basic assurance certificates.

2. Issuance
The actual process of authenticating and approving the certificate request. It can easily be automated for Medium assurance certificates. Entrust Datacard customers can leverage multiple protocols (such as Simple Certificate Enrollment Protocol, which is used by MDMs, Cisco and many mobile devices) and both client-based and client-less options to automate the issuance process.

3. Renewal
Certificate renewals can be completely automated or may require the user to request a renewal. In many cases, the process may be similar to the initial issuance. Entrust PKI can help an organization make the renewal completely transparent to the end user.

4. Revocation
Revocation is usually a manual process — not surprising given the sensitivity of the situations that might result in a revocation. However, Entrust Datacard offers options to automate the revocation process in certain scenarios. (See page 7 sidebar: Automating Revocation)
Entrust PKI allows organizations to configure the level of automation at different stages of the certificate management process. Over the last several years, a vast majority of our customers have opted for extensive automation.

**Entrust Client**
If an organization has an Entrust Client installed on their devices, the client can automate the certificate issuance and renewal processes.

Entrust Datacard offers three options for client-based certificate management automation:

- **Entrust® Entelligence™ Security Provider (ESP) Client**
  The Entrust Entelligence Security Provider (ESP) client is available for Windows and enables automated enrollment and renewal. When combined with the Entrust Auto Enrollment Server (AES), enrollment can be fully automated. The ESP/AES combination can be used to automate verification, issuance and renewal on end-user machines, IIS servers and domain controllers. (Note that beyond certificate management, the ESP offers benefits around key management, ease of deployment and enterprise security features.)

**FROM MANUAL TO AUTOMATED**

While deployments vary based on customer needs and environments, here’s an example of how the process might work:

1. Organization assigns a Group Policy Object (GPO) to a user/device in AD
2. ESP client checks whether the user/device has a certificate
3. If not, ESP client contacts AES
4. AES verifies user/device credential against AD and ensure that user/device is permitted per the GPO
5. AES enrolls user/device with the CA
6. AES pushes Activation Code to ESP client
7. ESP uses Activation Code to get and install the certificate on the device

All of this would be transparent to the user.
Automating Revocation
Certificate revocation is typically a manual function, with users or administrators sending requests and RAs performing the revocation. Entrust Datacard does offer ways to automate some of this process.

For example, Entrust Datacard provides an option that can be deployed on the customer network and monitor AD. If something is removed from AD (a user leaves the organization, or a device is decommissioned), the module picks that up and automatically sends a revocation request to the CA.

If a more manual approach is desired, an RA could manually vet the user in person and then provide Activation Codes (an alphanumeric Authorization Code and an eight digit Reference Number) to them at that time.

Somewhere in the middle is the self-enrollment option, in which users are sent an email with enrollment instructions and then directed to a website where they must provide credentials (Activation Codes, AD credential, passcode, etc.) in order to start the issuance process.

Note that users have the option to self-revoke and self-recover their certificates as well.

▶ Toolkit
Organizations can replicate ESP functionality on other operating systems (Linux, Solaris, etc.) and within applications themselves (such as Smart Card Management Systems) with the Entrust Authority toolkits.

▶ Mobile Smart Credential
Entrust IdentityGuard Mobile Smart Credential enables users to leverage a high assurance credential to generate credentials on their mobile devices. Mobile devices then become virtual smartcards that can be used to access both digital and physical resources and sign and encrypt data. Organizations can install smart credentials on mobile devices to automate certificate enrollment and renewal.
While the various Entrust Clients are very powerful, not every organization wants to install clients on user machines. Entrust Datacard does offer some client-less options to help automate the certificate management process:

**Windows Native Enrollment Server (WNES)**
WNES is a Windows specific option that helps automate the enrollment and renewal processes, essentially translating between the Microsoft CA protocol and the Entrust CA. By configuring AD with a certificate template and a certificate service associated with WNES, you can automate enrollment for user and device certificates in AD.

**Simple Certificate Enrollment Protocol (SCEP), Enrollment over Secure Transport (EST) and Certificate Management Protocol version 2 (CMPv2)**
Devices that communicate using SCEP, EST and CMPv2 can leverage automated certificate issuance and renewal, with Entrust Datacard deploying SCEP, EST or CMPv2 enrollment servers on the customer’s network (customers that already have clients that can enroll via SCEP, EST or CMPv2 can send requests to Entrust Datacard’s SCEP, EST or CMPv2 servers). Devices, MDM software and mobile devices that speak SCEP, EST or CMPv2 can easily leverage these protocols.

**Web Service APIs**
Several Entrust Datacard partners, such as Airwatch and MobileIron, have embedded Entrust Web Service APIs. This enables automated forwarding of certificate requests to CAs from a variety of applications.

**Certificate Expiry Service**
In client-less scenarios, organizations can also leverage Entrust Datacard’s Certificate Expiry Service (CES) to help streamline and automate renewals. CES interacts with the CA database and monitors for certificate expiration dates. Customers can configure CES to notify users and/or admins of upcoming renewal requirements a certain number of days before the certificate is due to expire.
When should an organization install an Entrust Client on devices to help automation, and when should they go with one of the client-less options, such as WNES or SCEP? It depends on the use case, the devices and the operating system.

The most common use case where Entrust Datacard still recommends deploying clients is encryption certificates (i.e. secure email). If, however, an organization wants to use certificates for authentication only, say in a limited VPN environment or for WiFi use case, it may be better and more cost effective to go with a client-less option like the WNES server. The organization can achieve the same certificate management automation without having to deploy clients to their users.

The capabilities of the devices or operating systems also come into play. Organizations managing certificates on devices that don’t run Windows, don’t have integration with the Entrust WS APIs or don’t speak SCEP or similar protocols will still find the client approach to be a powerful option. In those cases, they may need to develop some custom code (either with Entrust Authority toolkits or MDM APIs); Entrust Datacard can advise and support these efforts.

Organizations can also run client and client-less solutions in parallel. Remember that you probably have several certificate types. Some may be well suited to the client-less model, while others may require clients.

**Manual Options**
Finally, while we have focused a great deal on automated issuance, manual methods are still available. The CSR-Requestor/Approver and ESW applications allow users to generate a Certificate Signing Request (CSR) and paste it into a web page to be submitted to the CA. These methods are still popular for issuing certificates to HTTPS servers and may also be used for issuing application server certificates or code signing certificates. The User Registration Service (URS) available in Admin Services allows end users to create and self-manage their accounts and certificates.

**Client Or Client-Less Automation?**

CES may also be useful in a client scenario. Let’s say that an end user hasn’t logged into the ESP client in a while and their certificate is coming up for renewal. CES can send a reminder to the user to log in to ESP; once the user does so, ESP manages the certificate renewal transparently to the user.

CES may also be useful in a client scenario. Let’s say that an end user hasn’t logged into the ESP client in a while and their certificate is coming up for renewal. CES can send a reminder to the user to log in to ESP; once the user does so, ESP manages the certificate renewal transparently to the user.

Finally, while we have focused a great deal on automated issuance, manual methods are still available. The CSR-Requestor/Approver and ESW applications allow users to generate a Certificate Signing Request (CSR) and paste it into a web page to be submitted to the CA. These methods are still popular for issuing certificates to HTTPS servers and may also be used for issuing application server certificates or code signing certificates. The User Registration Service (URS) available in Admin Services allows end users to create and self-manage their accounts and certificates.

When should an organization install an Entrust Client on devices to help automation, and when should they go with one of the client-less options, such as WNES or SCEP? It depends on the use case, the devices and the operating system.

The most common use case where Entrust Datacard still recommends deploying clients is encryption certificates (i.e. secure email). If, however, an organization wants to use certificates for authentication only, say in a limited VPN environment or for WiFi use case, it may be better and more cost effective to go with a client-less option like the WNES server. The organization can achieve the same certificate management automation without having to deploy clients to their users.

The capabilities of the devices or operating systems also come into play. Organizations managing certificates on devices that don’t run Windows, don’t have integration with the Entrust WS APIs or don’t speak SCEP or similar protocols will still find the client approach to be a powerful option. In those cases, they may need to develop some custom code (either with Entrust Authority toolkits or MDM APIs); Entrust Datacard can advise and support these efforts.

Organizations can also run client and client-less solutions in parallel. Remember that you probably have several certificate types. Some may be well suited to the client-less model, while others may require clients.
Certificate Modification

What if you need to modify a certificate while it’s still active? For example, you may need to change or add to the Subject Alternative Name (SAN), Distinguished Name (DN) or Extended Key Usage (EKU) fields. Rather than issuing a new certificate, you’d like to modify the existing certificate with these sorts of changes.

Can this take place in a seamless, automated manner? Yes. The Entrust Entelligence Security Provider (ESP) client and the Entrust Authority toolkits can manage certificate updates with the same automation options as they manage issuance and renewal.

CERTIFICATE DISCOVERY AND MIGRATION

It’s one thing to manage certificates that you are newly generating. What about certificates that may already sit in your environment today – not currently managed, perhaps not even fully identified, or from an assortment of other vendors? Some organizations find that they have hundreds (or thousands) of certificates in their infrastructure that they weren’t aware of, from a mishmash of vendors and products, perhaps due to corporate acquisitions or prior, aborted PKI implementations.

Some Entrust Datacard customers use Entrust Datacard’s Certificate Discovery offering to scan their environment and identify all certificates that reside in their organization. This provides an excellent starting point; with that complete list of certificates, you can then decide which you need and how to manage them. You might want to partially manage non-Entrust certificates through Entrust Certificate Discovery. You will probably opt to delete unneeded certificates. Or you can migrate certificates from these various unmanaged sources so they are issued, renewed and managed by Entrust Datacard.

Certificates and keys can be migrated to Entrust PKI so long as they can be exported to a P12 file.

If an organization is running another PKI (such as a Microsoft CA) and does not wish to maintain multiple PKIs, they can opt to migrate an entire database of certificates and keys, exporting them all to P12 files and then uploading them to their Entrust Datacard CA. Once all of the certificates and keys have been moved, the organization can shut down their old CA and manage all certificates with Entrust Datacard.
CONCLUSIONS

Certificate management can seem overwhelming, especially in an environment with multiple types of certificates. Clear understanding of the different uses can help organizations apply automation sensibly and minimize the complexity while ensuring that the right levels of identity vetting remain. Your Entrust Datacard team can advise you as you develop your certificate management policy and leverage Entrust PKI, integrations and toolkits to streamline the processes.
WHY CHOOSE ENTRUST DATACARD FOR PKI

Entrust Datacard pioneered PKI more than 20 years ago for enterprise and government customers who understood the potential cost of a breach — and the potential upside of becoming a highly proficient digital business. Since then, we have shaped PKI into the most cost-effective technology for addressing the security risks introduced by expanding cloud, mobile and IOT environments. You can choose from on-premises or managed service models depending on your needs. Both solutions are platform agnostic and both align with the way you choose to do business. Our consultative PKI Black Belts, with 800+ deployments to their credit, support you every step of the way, from needs analysis to deployment to ongoing optimization.

ABOUT ENTRUST DATACARD

Employees, citizens and consumers increasingly expect anywhere-anytime experiences — whether they are logging onto corporate networks, crossing borders, accessing e-gov services or making purchases. They also expect the ecosystems that allow this freedom and flexibility to be entirely reliable and secure. Entrust Datacard offers the trusted identity and secure transaction technologies that make these ecosystems possible. Our 45+ years of industry-leading expertise and experience spans the globe, with more than 2,000 employees serving customers in 150 countries worldwide.

For more information, visit www.entrust.com/pki

Thanks to Martin Bouchard, Matt Hur, Josh Jabs, Janet Davis and Tim Moses for their inputs and reviews.