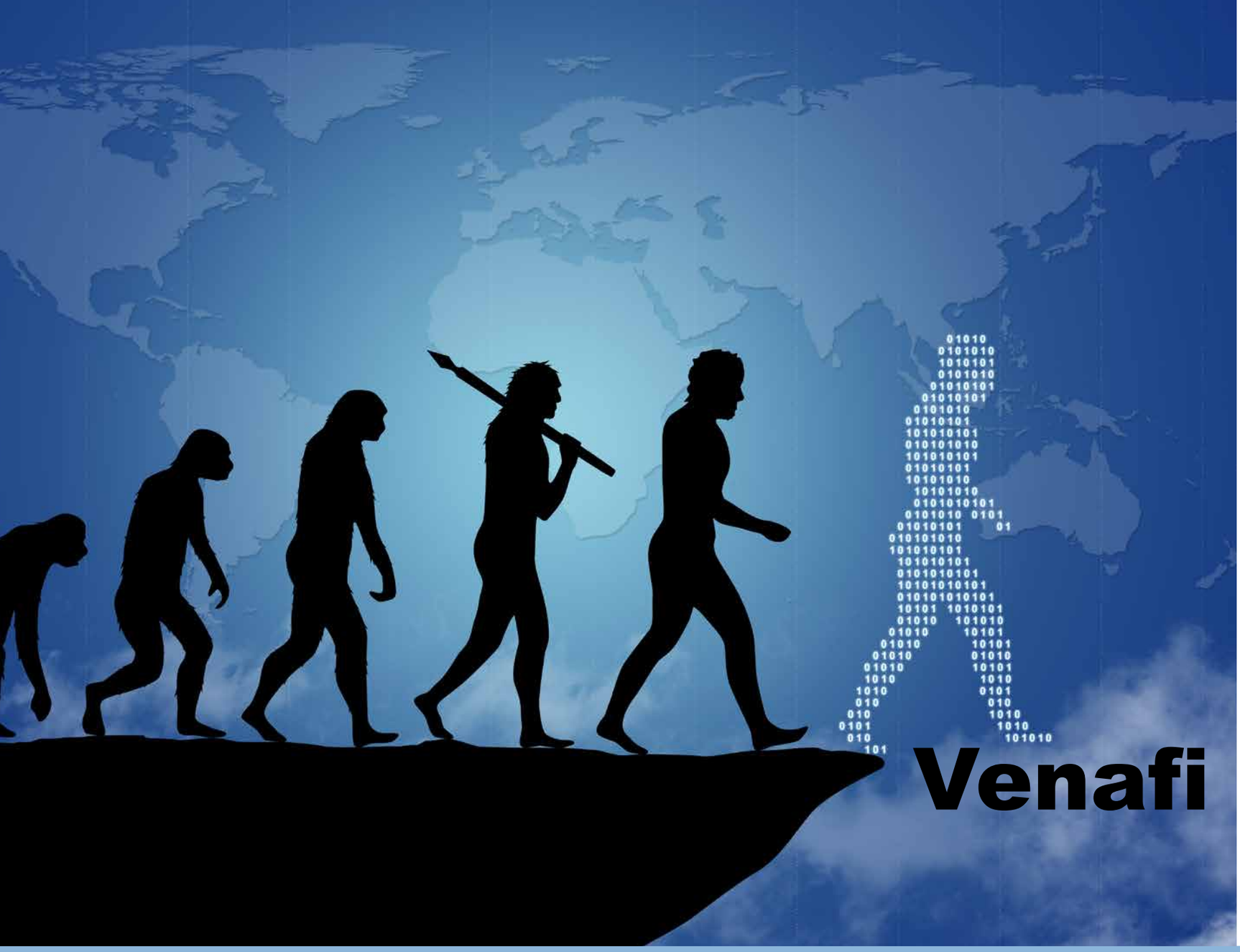

VENAFI®

SHA-1 Migration Guide

To learn more, visit
Venafi.com/contact/SHA-1Migration

Share this whitepaper

How to Migrate to SHA-2 Now

A SHA-1 to SHA-2 7-Step Migration Plan

Now is the time to migrate from SHA-1 to SHA-2 using this guide's 7-step migration plan that provides a comprehensive and achievable approach—even with limited resources.

Executive Summary: Why Migration is Important

If your organization hasn't already migrated both internal and external SHA-1 certificates to SHA-2, it's time to start.

- SHA-1 has been vulnerable for years, but is now easy and affordable to exploit.
- Today, leading browsers show security warnings for sites that use SHA-1-based certificates that expire after January 1, 2017.
- Leading browsers will start rejecting SHA-1 certificates as of January 1, 2017—and are considering advancing this date to June or July 2016.
- Likewise, code signed using SHA-1 with a timestamp later than January 1, 2016, will no longer be trusted by Microsoft as of January 1, 2017.
- Both internal and external certificate authorities (CAs) need to be migrated to SHA-2.

Now is the time to migrate from SHA-1 to SHA-2 using this guide's 7-step migration plan that provides a comprehensive and achievable approach—even with limited resources. When you use Venafi as part of your migration plan, the process can be seamless, without any gaps in providing complete visibility, maintaining the trust of your customers, and protecting your business and brand.

To learn more, visit
Venafi.com/contact

Share this whitepaper

SHA-1 Certificates Are Already Impacting Your Business

Cybercriminals can now easily and affordably exploit SHA-1. It has been considered an insecure cryptographic hash algorithm for years, but recently research proved that SHA-1 can be exploited for as little as $75,000 using Amazon Web Services (AWS). As a result, attackers can easily create forged certificates that mimic an original certificate. These forged certificates can be used to perform a multitude of nefarious activities, like man-in-the-middle (MITM) attacks and code-signing malicious binaries.

Because of the weaknesses in SHA-1, a special publication (800-131A) issued by the National Institute of Standards and Technology (NIST) in January 2011 includes a deprecation schedule for digital signatures signed with SHA-1 certificates. However, in November 2015, a revised version of that publication was issued by NIST that no longer shows a deprecation schedule and simply states that SHA-1 is disallowed in digital signature generation except in a TLS handshake.

Even if you put the risk of compromise aside, leading browsers now show security warnings when sites use certificates with SHA-1-based signatures. These warnings can impact your customers and damage your brand.

Because of the weaknesses in SHA-1, in 2014, Google, Microsoft, and Mozilla created their initial SHA-1 deprecation policies and started taking steps to aid end users in understanding the risks. These policies state that sites with end-entity certificates expiring on or after January 1, 2017, which make use of SHA-1, will no longer be accepted as secure. Currently, this means the leading browsers are issuing security warnings in the browser address bar for web services using SHA-1 certificates. These warnings can impact your end-user browser experience.

Figure 1: Example of browser SHA-1 security warnings

Also based on these deprecation policies, leading browsers will go beyond warnings and start rejecting all SHA-1 certificates as of January 1, 2017—or even sooner. In late 2015, when research revealed easier, less expensive ways to exploit SHA-1, the leading browser vendors (e.g., Mozilla and Microsoft), started to consider moving up the SHA-1 cut-off date to as early as June or July 2016. That's right around the corner.

These policies also require certificate authorities (CAs) to stop issuing new SHA-1 certificates after January 1, 2016.

The impact isn't limited to external CAs; the internal CA problem is just as significant. For example, when it comes to code signing, as of January 1, 2017, Microsoft Windows version 7 and higher and Windows Server will no longer trust any code that is signed with SHA-1 and has a timestamp value later than January 1, 2016. Although this goes into effect next year, developers need to start migrating immediately to SHA-2 in preparation. It is also expected that by 2017, all existing code with a timestamp before January 1, 2016, should also be migrated to SHA-2 or risk being flagged as untrustworthy.

VENAFI®

To learn more, visit
Venafi.com/contact

Share this whitepaper

When it comes to SHA-1 migration, internal certificates are where the challenges are amplified. Internal certificates are harder to discover, manage, secure, and migrate, because typically they are spread throughout the enterprise and owned by different organizational units. Users, systems, applications, and mobile devices all depend upon these internal certificates to secure communications and deploy trusted applications reliably.

SHA-1 security warnings—and soon their rejection—can impact customer confidence, making organizations lose customers and revenue. To avoid these losses and prevent brand damage, businesses need to start migrating to SHA-2 today. But migrating doesn't need to be difficult. This guide outlines a 7-step process that enables organizations to create a SHA-1 migration plan that is comprehensive and achievable—even with limited resources.

The Extent of the Problem

Are your websites using SHA-1? One in four are using this vulnerable standard. The SSL Pulse project found that 24% of the world's top 143,000 HTTPS websites use SHA-1 certificates.

Venafi also conducted research and found over 1.5 million certificates issued since December 31, 2013, with SHA-1 set to expire well beyond the January 1, 2017 deadline when major browsers will stop trusting, and outright reject, these certificates.

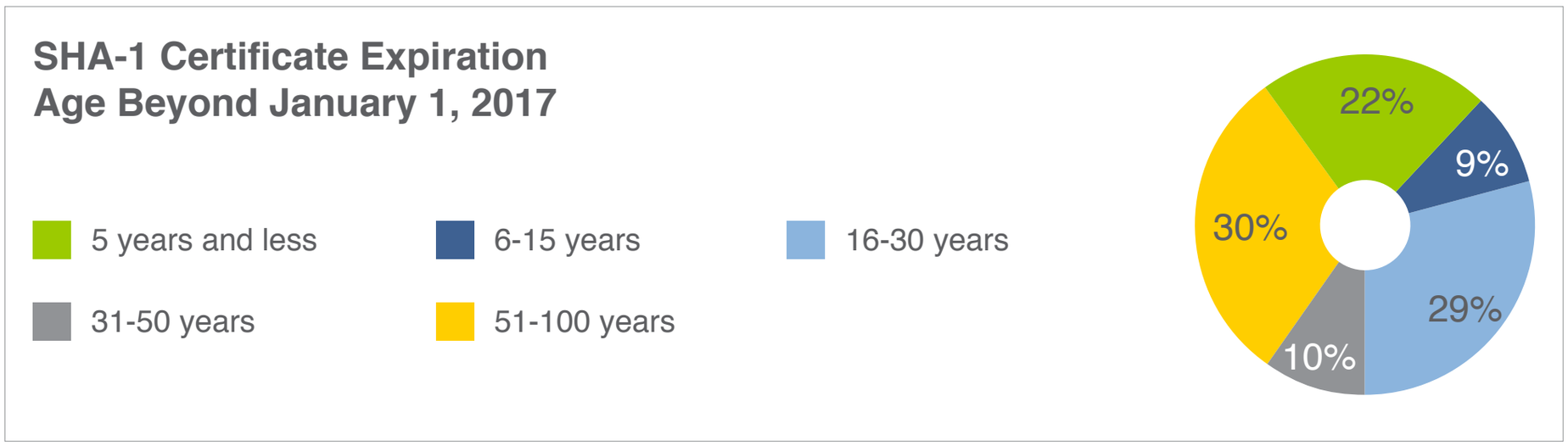

Figure 2: Validity periods for the 1.5 million SHA-1 certificates issued since December 31, 2013

7-Step SHA-1 Migration Plan

If you haven't made the switch to SHA-2 yet, your SHA-1 migration planning needs to begin now. Here is a 7-step process that can assist you with structuring your SHA-1 migration plan. Then, continue reading to learn how Venafi can help you easily and successfully complete this process—even with limited resources.

1. Establish a Migration Team

The use of SHA-1 certificates has a cross-functional impact, affecting both security and operations. Therefore, when you pull together a planning team, it should be comprised of both security and network operations with IT system and application administrators.

2. Discover All SHA-1 Certificates

First, all certificates that use SHA-1-based signatures need to be identified. This is not necessarily an easy task—the average enterprise has over 23,000 certificates and 54% admit to not knowing where all of their certificates are located, how they are used, or who owns them. However, complete discovery, including detailed information on each certificate, is needed to enable comprehensive SHA-1 migration.

3. Consider the Impact of a SHA-1 Migration

Once all SHA-1 certificates are identified, your team must consider what impact a SHA-1 migration across these certificates will have on your infrastructure, including impacts to hardware and software compatibility with SHA-2. You'll need to check all applications to see if they support a certificate chain or revocation checks against Certificate Revocation Lists (CRLs) for certificates that have been signed with SHA-2.

Some systems will need to be upgraded or patched, while others may not support the migration to SHA-2 at all, requiring broader system changes before the January 1, 2017 deadline. You may initially need to run two internal Public Key Infrastructure (PKI) systems in parallel, one that supports SHA-1 and one that supports SHA-2, and slowly upgrade applications, allowing more systems to migrate to the SHA-2 PKI system over time.

4. Automate the Migration of SHA-1 Certificates to SHA-2

Once the impact is assessed, your team can narrow in on the SHA-1 certificates that need to be updated and prioritize migration in stages, if needed.

Manual remediation is not ideal, regardless of the size of the enterprise, not only because of the cost of resources, but also because of the risk introduced through human error. Instead, relying on a policy-enforced, automated renewal schedule removes human-error and ensures the consistent application of specific security attributes.

5. Create Enforceable SHA-2 Policies

Your security and operations teams need to establish policies that not only guide the initial migration, but will automatically ensure any new certificates are SHA-2 compliant based on your network requirements. Your approach should introduce a frequent certificate

rotation policy that ensures SHA-2 usage and standardizes certificate lifecycle through automation and workflow requirements.

6. Facilitate Change Control

While automation can remove human error, change control enforces an approval process to ensure accuracy and compliance. The renewal policy should include change control authority for oversight and accountability.

7. Validate Replacement

As part of your SHA-1 migration plan, you need to ensure that you can validate your progress and achieve audit success. How will you know if the SHA-1 certificates have been replaced and the new SHA-2 certificates are installed and working properly? You need to define a migration report that details which certificates have been migrated and which are still at risk, and be able to deliver this information to key stakeholders in a timely fashion.

The deprecation of SHA-1 is now part of many compliance and governance standards. When establishing a method of validation, ensure that it provides the details needed to support your audit processes.

VENAFI®

To learn more, visit
Venafi.com/contact

Share this whitepaper

Venafi Makes the Process Easy

You don't need to start your SHA-1 migration process in the dark. Tools and expertise from Venafi will help you migrate from SHA-1 to SHA-2 with speed, accuracy, and reliability—without requiring additional resources.

"Venafi is the only company that finds and remediates SHA-1 keys and certificates for any CA and fully automates replacement, reducing cost and risk to your organization."

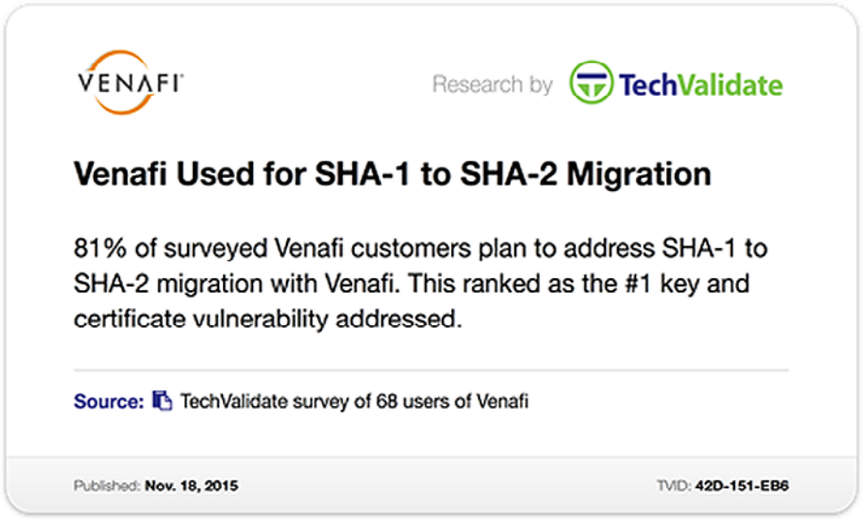

Figure 3: Percentage of Venafi customers using the Venafi solution to address SHA-1 migration.

Venafi uses network discovery features to quickly identify both known and unknown certificates throughout your enterprise. Odds are you have many more certificates than you realize—including certificates that still use SHA-1. Research conducted by TechValidate in 2015 revealed that Venafi customers discovered an average of over 16,500 unknown keys and certificates. With Venafi, you significantly increase your visibility and ensure a more comprehensive SHA-1 migration.

Venafi inventories and categorizes certificates based on certificate attributes such as SHA-1. This capability provides immediate visibility into vulnerable keys and certificates and shows which certificates need to be migrated for faster protection of your organization.

Figure 4: With Venafi, dashboard metrics display those certificates detected with weak algorithms to help quickly identify certificates that are at risk.

To learn more, visit
Venafi.com/contact

Share this whitepaper

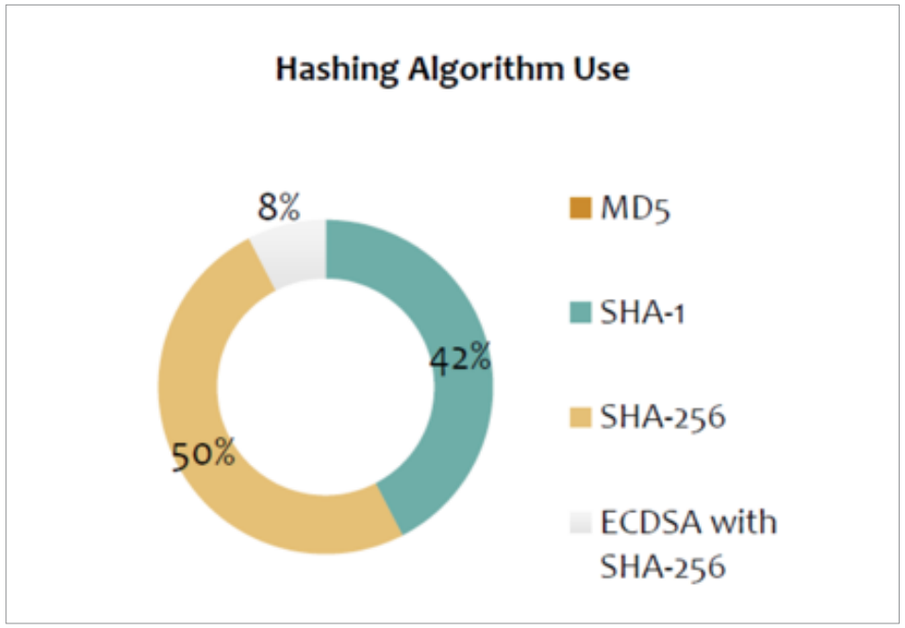

Figure 5: Additional dashboard indicators provide instant visibility into an enterprise's security posture and are interactive, allowing administrators to click and quickly filter and display a list of related certificates.

To learn more, visit
Venafi.com/contact

Share this whitepaper

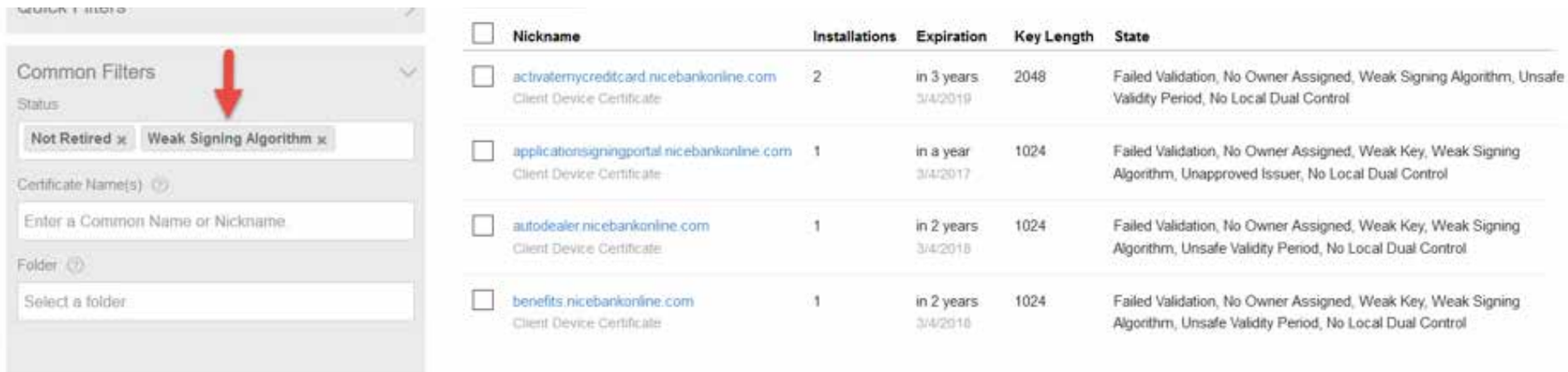

Figure 6: Reports provide much greater detail and the context needed to identify and prioritize specific certificates. Results can be further filtered and/or grouped for review and processing.

After Venafi identifies SHA-1 certificates, Venafi security policy templates can create an automated renewal schedule to ensure a seamless migration to SHA-2. Venafi streamlines migration and provides ongoing certificate lifecycle management through automation, policy enforcement, workflow capabilities, and system integration. All of these help you enforce the use of SHA-2 and other security attributes and ensure change control.

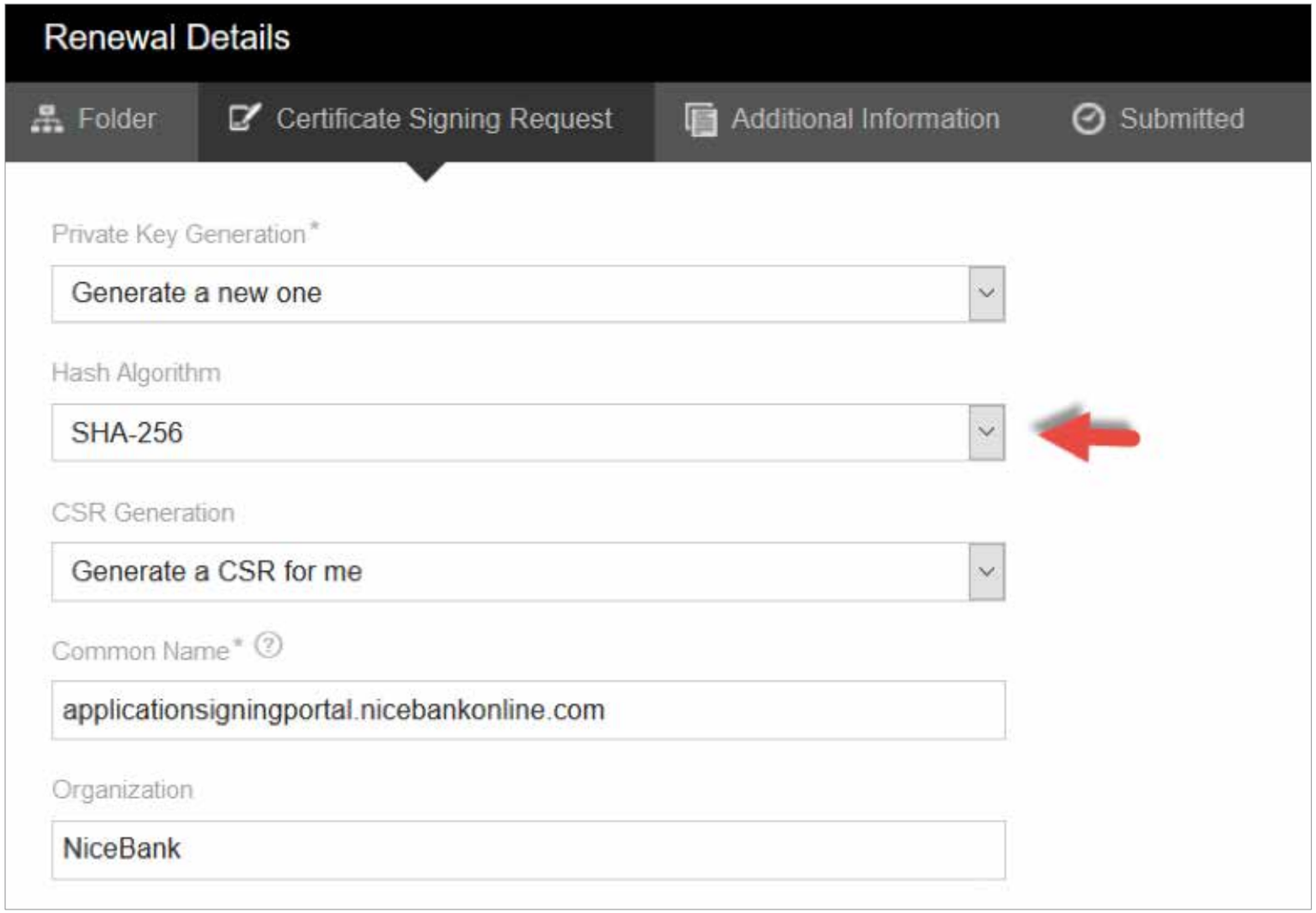

Figure 7: Security policies can be created to enforce automated controls and ensure that all future certificates are signed with SHA-2 or greater algorithms.

To learn more, visit
Venafi.com/contact

Share this whitepaper

Venafi doesn't limit the number of policies that you can define as part of your migration—the process can be customized on a per-certificate basis or by security policy. Security polices allow your migration to proceed quickly and accurately, reducing risk and the reliance on error-prone human interaction. Vulnerable SHA-1 keys and certificates are quickly identified and automatically replaced so that system administrators don't have to perform the task manually, speeding replacement and eliminating errors.

If you decide to maintain two separate PKI environments in parallel—one based on SHA-1 and one based on SHA-2—Venafi can manage both of these environments and allow you to phase out your SHA-1 PKI environment in a time frame that makes sense for your infrastructure and your business.

Upon completion of your migration project (or at any point along the way), Venafi easily generates audit reports to show your progress—validating that certificates have been successfully replaced with ones using SHA-2. These reports can be customized to include all migration details required to meet your compliance and governance needs.

Get Started—Stop Your SHA-1 Risk Now

Venafi is the only solution that helps reduce the cost and impact of SHA-1 migration without the need for any additional resources. Contact Venafi for a certificate assessment to determine the extent of your SHA-1 risk or for support with your migration efforts.

Venafi.com/contact/SHA-1Migration

VENAFI®

To learn more, visit
Venafi.com/contact

Share this whitepaper

Trusted by the Top

Implemented Venafi solution

4 of the top 5 U.S. Retailers
5 of the top 5 U.S. Health Insurers
4 of the top 5 U.S. Banks
3 of the top 5 U.K. Banks
4 of the top 5 S. African Banks

About Venafi

Venafi is the Immune System for the Internet™ that protects the foundation of all cybersecurity—keys and certificates—so they can't be misused by bad guys in attacks. Venafi constantly assesses which keys and certificates are trusted, protects those that should be trusted, and fixes or blocks those that are not.

Part number: 1-0050-0116