Symantec™ Secure App Service

Hosted Code Signing Service

Datasheet: Symantec Secure App Service

Overview

Traditional code signing provides a way for software publishers to assure their customers that the apps and files they have downloaded are, indeed, from them and have not been tampered with. Unfortunately, inadequate controls around this process can lead to malware propagation. According to IDG News Service, "Malware authors are signing their malicious creations with stolen digital certificates to bypass antivirus detection and defense mechanisms" (IDG News, March 15, 2012).

Compromised certificates make news headlines and can lead to poor reputation for your company, and revoking these certificates could result in your distributed applications to suddenly appear as untrusted.

Symantec Secure App Service is a cloud-based code signing and management solution with a complete range of services to help enterprises control and secure their code signing activities and keys easily. Services include vetting and approval of software publishers, code signing, key protection and revocation, administrative controls, reporting and audit logs.

Symantec Secure App Service offers a complete range of code signing management services to protect your business and your users

Key Benefits

Maintain Integrity of Files and Apps

- Eliminate issues from lost and stolen signing keys by leveraging Symantec's secure cloud-based service
- Maintain control with role-based authorization
- Avoid fraud by using authentication by IP address(es)
- Minimize non-compliance and enforce accountability with detailed reports and audit logs on signing activities

Maintain Business Continuity

- Minimize adverse business impacts when keys are revoked by deploying unique keys and automatic time stamping
- Maintain reputation rating in Microsoft's application reputation model and adopt best practices by deploying rotating keys
- Utilize Symantec's world class vetting services for developers

Drive Business Agility

- Support all major file types and integrate with third-party test houses
- Expedite process time with batch update of apps
- Flexibility to use Private Roots or to chain to a Trusted Root
- Integrate with other systems and activities via full set of SOAP APIs
- Customize email notifications to meet business needs

Symantec™

Maintain Integrity of Files and Apps, and Secure Keys

Traditional code signing requires companies to have tight management controls over their code signing activities and keys. Without proper security and controls, there is no tracking of signing activity or auditing, no accountability for signing, no rights management, and the signing keys are often vulnerable to theft or can easily be lost.

Symantec Secure App Service provides security and convenience: you can sign desktop files and apps and then secure the keys in the same cloud service. This helps prevent keys from being stolen and deployed for nefarious purposes while ensuring the integrity of files downloaded by users.

Maintain Business Continuity with Rotating Keys and Unique Keys

Contrary to industry best practices, some companies use the same key to sign many of their files and apps. If the key is compromised and needs to be revoked, all the files and apps signed using that key will have to be recalled and will not be available to users. Companies may experience a ripple effect in terms of costs associated with unavailability of these assets to their users as well as additional resources required to track and re-secure the assets.

With Symantec Secure App Service, companies can deploy unique keys to minimize adverse business impacts in the event a key is revoked. In addition, for publishers on Windows®, they are provided with a pool of keys to sign and rotate through. This allows them to maintain their ranking with Microsoft SmartScreen® Filter while minimizing the business impact if a key has to be revoked.

Enforce accountability with reports, and audit logs

Traditional code signing warns users when files and apps are tampered prior to download and protects users and businesses from malware. In order to attain an enterprise-wide view of keys and code signing activities, administrators would have to spend additional resources to discover and track that information.

Symantec Secure App Service provides reports and audit logs so that administrators can easily track and monitor activities. The availability of reports and audit logs helps companies enforce accountability and compliance. Companies have access to reports and logs on all signing activities in one area providing them with insight and data for risk analysis, forecasting and resourcing.

Key Features

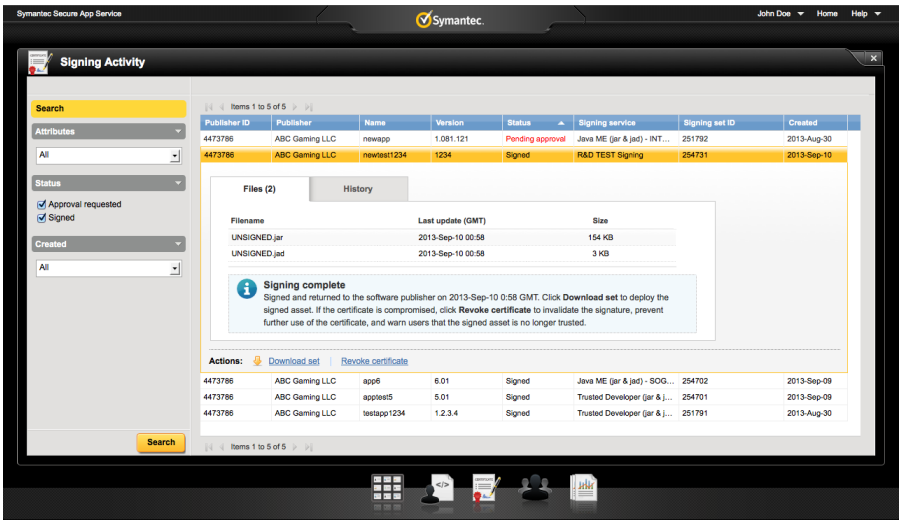
- Cloud-based, with easy-to-use dashboard for code signing and management of keys and signing requests
- Role-based access control on code signing
- Access restriction by IP range and IP logging when applications are signed
- Unique signing keys
- Rotating pool of keys
- Support for all major file types: Microsoft, Java desktop, Java mobile, Android, file hashes and others
- Unlimited test signings and capability to integrate with third-party test houses
- Option for automatic time stamping (RFC 3161 or Authenticode)
- Capability for Admins to approve or reject signing requests
- Option to use Private Roots or chain to a Trusted Root
- SOAP APIs for integration with other systems and workflows
- Reports and audit logs to track signed code and activities
- Capability to customize email notification by language as well as enable/disable emails
- Assign signing/services to developers
- Option for developer vetting

Symantec™

Maintain Tight Control with Approval Queue and Role-based Access

As part of industry best practices, companies should maintain tight control over who should have access to sign apps and files as well as the access level based on the role of an individual. With proper access control, companies can minimize security risks and avoid business disruptions.

Symantec Secure App Service provides the capability for companies to manage and maintain control over their publishers. With this Service, administrators can approve or revoke access. Access can be granted based on roles and responsibilities. When a publisher leaves the company or changes roles, access can be revoked or adjusted accordingly.



Symantec Secure App Service, a cloud-based service, maintains and tracks all code signing activities in an integrated web-based portal, or via API

Symantec™

More Information

Visit our website

North America: http://go.symantec.com/code-signing
EMEA: http://www.symantec.com/en/uk/code-signing
APAC: http://www.symantec.com/en/aa/code-signing

Speak with a product specialist

North America:	+1 (866) 893-6565 or +1 (650) 426-5112	codesigning@symantec.com
U.K. and Ireland:	+0800 032 2101	talk2us-uk@symantec.com
Rest of EMEA:	+353 1 850 2628 or +41 (0) 26 429 7929	talk2us-ch@symantec.com
Australia:	+61 3 9674 5500	ssl_sales_au@symantec.com
New Zealand:	+64 9912 7201	ssl_sales_au@symantec.com
Hong Kong:	+852 30 114 683	ssl_sales_asia@symantec.com
Singapore:	+65 6622 1638	ssl_sales_asia@symantec.com
Taiwan:	+886 2 2162 1992	ssl_sales_asia@symantec.com

To speak with a Product Specialist outside the U.S.

To speak with additional product specialists around the world, visit our website for specific offices and contact numbers.

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device to the enterprise data center to cloud-based systems. Our industry leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at: go.symantec.com/ socialmedia.

Symantec World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
1-866-893-6565
www.symantec.com

UID: 206/10/13