DATASHEET

Sectigo Identity for Chromebooks

Google has broken the duopoly of Apple and Microsoft in personal computing with its success of the Chromebook. A low-cost device that is easily managed and resilient to cyberattacks, Chromebooks have proven popular for schools, colleges, and some enterprises.

Most webservices and network services like VPN and Wi-Fi require a level of authentication for access which is usually password centric, often with the addition of Multi Factor Authentication (MFA). More services, more networks and more applications together mean more passwords, and invariably result in significant levels of password reuse, a big risk for everyone. There's a considerable cost associated with supporting these passwords and corresponding password resets. The World Economic Forum estimates that "nearly 50% of IT help desk costs are allocated to password resets."

The cybersecurity industry no longer considers passwords to be a strong authentication mechanism. Passwords are easy for cybercriminals to steal and exploit, they are difficult for users to remember and manage, and they don't support all digital identity use-cases.

> "nearly 50% of IT help desk costs are allocated to password resets."

Simplifying the user experience is key for many IT departments and the elimination of passwords is a compelling proposition. Gartner has identified passwordless authentication as an immediate emerging technology especially in support of employee use cases.

Reduce IT Costs and Simplify Secure Access to Applications

Sectigo Identity for Chromebooks, a passwordless solution, reduces the burden of user and machine authentication, streamlining the user interaction and simplifying IT management.

Sectigo enables certificate-based authentication which uses asymmetric keys and eliminates the need for passwords to be exchanged between the client and web-based services. Digital certificates are widely supported and can be managed by Sectigo Certificate Manager. Certificates can be automatically installed, renewed, and revoked, making management of the authentication ecosystem efficient and straightforward.

With certificate-based authentication, the Chromebook sends proof that it possesses the digital identify rather than the digital identity itself. Unlike passwords, the digital identity never leaves the Chromebook, so it cannot be stolen.

Chromebooks work hand in glove with Google Workspace, including administration and software deployment tools. Likewise, Google Workspace is central to the Sectigo solution for Chromebooks. Using Sectigo tools Chromebooks can be easily configured with user or device certificates, embedded in the TPM (Trusted Platform Module) on each device.

Trusted Platform Module (TPM)

TPM is an industry standard (ISO/IEC 11889) for protecting an identity from theft and duplication using dedicated hardware. This enables certainty that it really is that person or that machine. Most devices including Windows PCs and Chromebooks now include a TPM.

Sectigo Identity for Chromebooks Provides the Following Benefits:

- Greater convenience for users in not having to remember passwords for multiple web and network services
- Improved security across the entire network
- Ease of management of certificates including the ability to assign, deploy, renew and revoke
- Low touch enrolment for client and device certificates
- Secure enrolment using standard SCEP protocol
- Administrator convenience using Google Workspace for client configuration and certificate policy

How is this Solution Implemented?

- All users must have a Google Workspace account. Google requires this to access the TPM on the device.
- The TPM is used to securely generate and store the private key on the device allowing applications to use it but not remove or export it from the device.
- The IT department installs the Sectigo Identity extension onto the device via Google Workspace.
- The IT department configures the identity policy in Google Workspace.

For enterprises and IT departments using Chromebooks, this solution offers a clear path to reduced IT overhead and greater security. By adopting a passwordless authentication strategy users will have no passwords to remember, and more robust authentication policies can be easily implemented, facilitating a move towards a Zero Trust Network Architecture (ZTNA). Sectigo offers a range of Passwordless Authentication solutions which provide greater flexibility and increased security for the network of the future.

About Sectigo©

Sectigo is a leading provider of digital certificates and automated certificate lifecycle management solutions to leading brands globally. As one of the longest-standing and largest Certificate Authorities (CA), Sectigo has over 20 years of experience delivering innovative security solutions to over 700,000 businesses worldwide. Sectigo is the leading certificate lifecycle management provider supporting multiple CA vendors and integrating with the largest software ecosystems in the world.