PRODUCT SHEET

GOOGLE AUTHENTICATOR

Google Authenticator, supported by the Freja authentication appliance, can be deployed to users' smartphones in order to achieve strong 2FA (two-factor authentication) when accessing the corporate network.

Background

New devices such as smart phones and tablet-PC's have brought new opportunities in terms of user experience. Strong authentication can now be issued as a mobile application and provisioned for use with the corporate network. A number of mobile authenticator apps have existed for some time on the market and Freja can support any open standards based mobile device. For several reasons, however, Verisec has opted to propose the Google Authenticator as the mobile solution of choice. Combining the strength of Google Authenticator and Freja Self-Service Portal, users can take advantage of mobile authentication with secure and intuitive provisioning at low cost.

Benefits of open standard

A pre-requisite for any authenticator to work with Freja is that it is built on an open standard for authentication (OATH). This ensures that customers are free, at any point in time, to switch token supplier and thereby achieve greater freedom of choice and a better price point. Google Authenticator supports OATH and has no per user cost associated with it.

Beyond supporting OATH, however, Google Authenticator also allows for an open standard provisioning process. Very often, although solutions are promoted as open standard, when it comes to mobile tokens the provisioning of these tokens is performed through a proprietary provisioning tool.

The Freja Self-Service Portal on the other hand uses an open standards, matrix barcode (QR codes) supported by Google Authenticator to provision the mobile token, i.e. tie the token to a particular user. This avoids the need for proprietary provisioning tools which lock customers into working with a particular vendor or solution. In addition, Freja's provisioning interface allows Google Authenticator provisioning into the customer's own applications.

Google Authenticator advantage

Another big advantage of Google Authenticator is that security aware private users may already have the Google Authenticator app installed on their smartphone, using it for two-factor authentication for their Gmail or Google Apps account. From an end user perspective this allows for a much more user friendly experience, avoiding separate hardware devices by re-using the everpresent smartphone and allowing users to user the same device for authenticating both to the corporate network and to private resources on the Internet.

Google Authenticator gives you two-factor authentication with Freja using the Google Authenticator app for iPhone, iPad, iPod Touch, Android and Blackberry.

Google Authenticator is an open source, free of charge smartphone authenticator. It is a standalone app for smartphones and does not require Google to handle the authentication itself. A common misconception is that

VERISEC

authentication using Google Authenticator takes place in the "cloud" by Google, which to many would indicate lack of control. When used in conjunction with Freja, all authentication takes place in the Freja appliances residing within the customer organization.

Robust security device

From a security standpoint Google Authenticator is a well documented and robust security device. The potential weakness of any mobile authenticator is the fact that it resides on a, relatively speaking, open and interconnected platform. When considering security, an organization needs to determine the criticality of the resources protected by strong authentication. For many user groups accessing primarily corporate mail and similar applications, Google Authenticator can be considered a sufficiently secure solution.

Free of charge license

The license agreement governing Google Authenticator allows for a perpetual and free of charge license meaning that Google will not introduce any costs for the authenticator once a customer has deployed and provisioned its mobile devices.

Mix and match authenticator types

With Freja an organization can mix and match different authenticator types for different user groups depending on the criticality of the resource being accessed. Some may require the highest level of security, using a smart card or PIN protected, hardware based OTP (one-time-password) generators; but for many users the security of the Google Authenticator is sufficient and far superior to any fixed password schemes, which are still all too common in many organizations.

Contact information

For more information regarding Google Authenticator for Freja, please contact sales@verisec.com,
+46 (0)8 723 09 00 or 0800 917 8815 (UK toll-free)