BILLION™

BiGuard OTP

Two-Factor Authentication with One-Time Password

BiGuard OTP

The BiGuard OTP is a chip-based, 6-digit numeric PIN token to be used in combination with a password for a strong two-factor authentication. This powerful solution provides single password authentication for remote VPN, LAN and web access through the use of an ASAS back-end server. Each BiGuard OTP token is unique and has been assigned an Electronic Serial Number (ESN) and identification seed, so that the authentication cannot be reproduced. The BiGuard OTP continuously changes its PIN number, which, compared to a relatively easy-to-crack static password, dramatically increases access security and greatly reduces the risk of unauthorized access to corporate network resources by intruders. The car key-sized token is extremely portable, offering total mobility and maximum flexibility for remote network access.

- Dynamic One-Time Password
- Event-based Algorithm Token
- Strong Two-factor Authentication
- Easy installation and management
- Car key-sized for extreme mobility
- One-click easy-to-use system
- Compatible with BiGuard SSL VPN series equipment

Strong Two-Factor Authentication

The traditional user login method is to simply enter a fixed static password. This could pose a grave risk when used in public areas such as Internet cafes, airports and other public areas, because people nearby may be able to obtain the static password you use to log into your company's network. The BiGuard OTP allows you to create a strong, two-factor authentication by using a dynamically generated 6-digit PIN, and combine this with your existing static password. Even if the token is lost or stolen, it's useless to anyone but its owner and your company's system administrator.

One-Time Password for Multiple Applications

Prior to launching authentication systems, administrators were required to synchronize each BiGuard OTP token with an ASAS RADIUS-standard server which stored the ESN of each token. The BiGuard OTP token is flexible enough to adopt various algorithms, including OATH (Open AuTHentication) event-based algorithms. Whenever access to LAN, Web or remote VPN is needed, users simply click on the token button to obtain a one-time password called a dynamic PIN. This action will start the two-factor authentication process between the BiGuard SSL VPN equipment and the ASAS server, resulting in the server either accepting, rejecting or challenging the authentication request.

Easy Installation and Management

The ASAS server provides administrators with a friendly management interface, which includes account management, adding new tokens, etc. The step-by-step server installation is as easy as any normal commercial software. The administrator can use any web browser, anywhere, any time, to login to the ASAS management server, without having to pre-install any client software.

Ease of Use Anywhere at Any Time

Its simple interactive interface is easy to understand and use. A simple, single click on the button of the BiGuard OTP token generates a six-digit OTP number. Pressing and holding the button produces the token's Electronic Serial Number (ESN), a number used to identify each token. Bars in the lower right corner of the LCD screen display battery strength - 3 bars for a fully charged battery. Its car key-sized design makes it extremely portable. Wherever you need to access the company's network resources, the BiGuard OTP offers you better security level of authentication process to login the networks, even when on the road, or from an airport paid terminal.

Economic Authentication Solution

Unlike others solutions, BiGuard's OTP solution includes an ASAS server, so there is no need to renew the service, reconfigure user setting or renew tokens. The battery inside a BiGuard OTP token will last up to 3 years, so no hassle of replacing batteries.
The BiGuard OTP: a truly economic authentication solution.

Features & Specifications

Standard Compliance

• OATH Algorithm

Supported Software

• Remote Access (With Authenex ASAS Authentication Server)
  - Any ASAS system-compatible remote access system
  - OTP-capable VPNs
  - SSL VPN
• Authentication Interoperability
  - Secure Web Access (MS Internet Explorer and Netscape Communicator)
  - RADIUS
• OTP Number Generation
  - OATH Algorithm
  - 160-bit

Minimum System Requirements

• Client Browser: Microsoft IE 6.0 or newer versions
• ASAS Server Requirements:
  - Hardware:
    CPU: Pentium IV 1.4GHz or above
    Disk space: 8GB of free hard disk space
    Memory: 512MB or more
  - Software:
    Microsoft Windows 2000/2003 Server Edition
    Microsoft Windows 2000 Server Pack 3 or above

ASAS Server Software

• OATH Algorithm Authentication Server:
• RADIUS Standard Server (ASAS Server)
• Easy Administration through Web Management GUI
• Easy to integrate into existing network infrastructure
• Use a Web browser to manage ASAS any time, from anywhere

Hardware Specifications

• Display: 6-Digit Numeric LCD Display
• Casing: Polycarbonate
• Power: Internal battery
• Dimension: 55mm (W) x 25mm (D) x 12.2mm (H)

Operation Environment

• Operating Temperature: -5° to 50° C
• Storage Temperature: 10° to 50° C

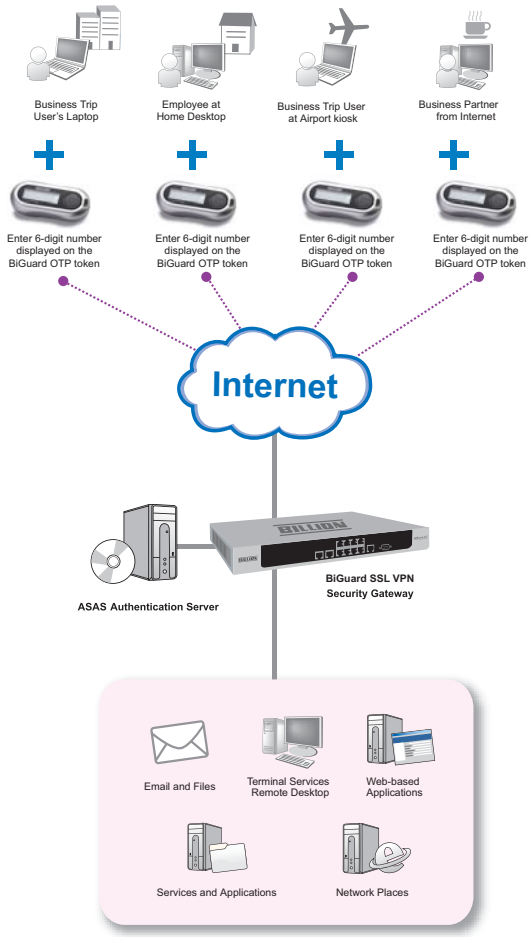
Supported Equipment

• BiGuard SSL VPN series equipment

Available Packages

• BiGuard OTP Starter Kit (2 OTP tokens)
• BiGuard OTP 5U (5 OTP tokens)
• BiGuard OTP 10U (10 OTP tokens)

Application Diagram



The specifications in this datasheet are subject to change without prior notice.

V.083007

Billion Electric Co., Ltd.
8F, No.192, Sec.2, Chung Hsing Road,
Hsin Tien City, Taipei Hsien, Taiwan

TEL : +886-2-2914-5665
FAX : +866-2-2918-6731,+886-2-2918-2895
E-mail : sales@billion.com

www.billion.com